Tool ONTAP per la documentazione di VMware vSphere 10,2

ONTAP tools for VMware vSphere 10.2

NetApp
January 18, 2025

Sommario

Tool ONTAP per la documentazione di VMware vSphere 10,2

Note di rilascio

Note di rilascio

Scopri le nuove e migliorate funzioni disponibili nei tool ONTAP per VMware vSphere 10,2.

Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere Novità dei tool ONTAP per VMware vSphere 10,2.

Per ulteriori informazioni sull'opportunità di eseguire la migrazione dagli strumenti ONTAP per VMware vSphere 9 agli strumenti ONTAP 10,2, 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 le release VMware vSphere 9.10D2, 9.11D4, 9,12 e 9,13 agli strumenti ONTAP 10,2.

Per ulteriori informazioni, vedere "Note sulla versione dei tool ONTAP per VMware vSphere 10,2". Per accedere alle Note di rilascio, è necessario accedere con l'account NetApp o creare un account.

Novità dei tool ONTAP per VMware vSphere 10,2

Scopri le nuove funzionalità disponibili nei tool ONTAP per VMware vSphere 10,2.

Aggiornare	Descrizione
Supporto del protocollo NVMe	I tool ONTAP per VMware vSphere 10,2 supportano sia i protocolli NVMe/FC che NVMe/TCP per il provisioning dei datastore VMFS. I workflow integrati senza problemi all'interno dell'interfaccia vCenter semplificano il provisioning dei datastore. I vantaggi dell'utilizzo dei protocolli NVMe/FC e NVMe/TCP per il provisioning dei datastore VMFS includono performance ottimizzate, elevata scalabilità e gestione efficiente di richieste di dati multiple, significative riduzioni della latenza e una gestione delle risorse efficiente. L'io storage basato su NVMe ha un utilizzo della CPU inferiore fino al 50% rispetto ai protocolli dati legacy.
Supporto del protocollo Fibre Channel (FC)	I tool ONTAP per VMware vSphere 10,2 supportano il protocollo FC per il provisioning di datastore vVol e VMFS. I vantaggi del supporto del protocollo FC includono prestazioni elevate, affidabilità e stabilità, scalabilità, protezione avanzata e gestione efficiente delle risorse.

Aggiornare	Descrizione
Sincronizzazione attiva di SnapMirror	Il supporto della sincronizzazione attiva di SnapMirror con i tool ONTAP per VMware vSphere 10,2 include una funzionalità del cluster di protezione completamente nuova che fornisce un workflow di configurazione end-to-end per la costruzione di un vSphere Metro Storage all'interno dell'interfaccia utente di vCenter. Ciò consente configurazioni cluster stretched in cui i servizi business continuano a operare anche attraverso un guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. La procedura guidata SnapMirror può configurare SnapMirror asincrono e sincronizzato oltre alla sincronizzazione attiva di SnapMirror.
Miglioramenti di Storage Replication Adapter (SRA)	SRA implementa la soluzione di disaster recovery (DR) basata sulle specifiche di VMware Site Recovery Manager (SRM). La sincronizzazione attiva di SnapMirror tramite l'integrazione di SRM supporta la pianificazione del disaster recovery e la soluzione di orchestrazione per fornire un failover dell'applicazione trasparente.

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 VMware vSphere 10,2 è la soluzione giusta per te. Per informazioni aggiornate sulla compatibilità, vedere "Tool di matrice di interoperabilità NetApp".

Funzione	Strumenti ONTAP 9,13	Strumenti ONTAP 10,1	Strumenti ONTAP 10,2
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 SRM a tre siti
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
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

Funzione	Strumenti ONTAP 9,13	Strumenti ONTAP 10,1	Strumenti ONTAP 10,2
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
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 SRM.
Supporto di 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)

Concetti e termini chiave

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

Autorità di certificazione (CA)

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

Gruppo di coerenza

Un gruppo di coerenza è 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.

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".

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

Panoramica sul role-based access control nei tool ONTAP per VMware vSphere

VCenter Server fornisce il role-based access control (RBAC) che consente di controllare l'accesso agli oggetti vSphere. VCenter Server fornisce servizi di autenticazione e

autorizzazione centralizzati a molti livelli diversi all'interno del proprio inventario, utilizzando i diritti di utenti e gruppi con ruoli e Privileges. VCenter Server include cinque componenti principali per la gestione di RBAC:

Componenti	Descrizione
Privilegi	Un privilegio abilita o nega l'accesso per eseguire azioni in vSphere.
Ruoli	Un ruolo contiene uno o più privilegi di sistema in cui ogni privilegio definisce un diritto amministrativo per un determinato oggetto o tipo di oggetto nel sistema. Assegnando a un utente un ruolo, l'utente eredita le capacità dei privilegi definiti in quel ruolo.
Utenti e gruppi	Gli utenti e i gruppi vengono utilizzati nelle autorizzazioni per assegnare i ruoli da Active Directory (ad). VCenter Server dispone di propri utenti e gruppi locali che è possibile utilizzare.
Permessi	Le autorizzazioni consentono di assegnare Privileges a utenti o gruppi per eseguire determinate azioni e apportare modifiche agli oggetti all'interno di vCenter Server. Le autorizzazioni di vCenter Server interessano solo gli utenti che accedono a vCenter Server anziché gli utenti che accedono direttamente a un host ESXi.
Oggetto	Un'entità su cui vengono eseguite le azioni. Gli oggetti VMware vCenter sono data center, cartelle, pool di risorse, cluster, host, e VM

Per completare correttamente un'attività, è necessario disporre dei ruoli vCenter Server RBAC appropriati. Durante un'attività, gli strumenti ONTAP per VMware vSphere controllano i ruoli vCenter Server di un utente prima di controllare i privilegi ONTAP dell'utente.

I ruoli di vCenter Server si applicano agli strumenti ONTAP per gli utenti di VMware vSphere vCenter, non agli amministratori. Per impostazione predefinita, gli amministratori hanno accesso completo al prodotto e non richiedono l'assegnazione di ruoli.

Gli utenti e i gruppi accedono a un ruolo facendo parte di un ruolo vCenter Server.

Punti chiave sull'assegnazione e la modifica di ruoli per vCenter Server

È necessario impostare i ruoli di vCenter Server solo se si desidera limitare l'accesso a oggetti e task vSphere. In caso contrario, è possibile accedere come amministratore. Questo login consente di accedere automaticamente a tutti gli oggetti vSphere.

L'assegnazione di un ruolo determina gli strumenti ONTAP per le attività di VMware vSphere che un utente può eseguire. È possibile modificare un ruolo alla volta. Se si modificano i privilegi all'interno di un ruolo, l'utente associato a tale ruolo dovrebbe disconnettersi e quindi riconnettersi per abilitare il ruolo aggiornato.

Ruoli standard forniti con strumenti ONTAP per VMware vSphere

Per semplificare l'utilizzo dei privilegi di vCenter Server e RBAC, i tool ONTAP per VMware vSphere forniscono

tool ONTAP standard per i ruoli VMware vSphere che consentono di eseguire tool ONTAP chiave per i task VMware vSphere. Esiste anche un ruolo di sola lettura che consente di visualizzare le informazioni, ma non di eseguire attività.

È possibile visualizzare gli strumenti ONTAP per i ruoli standard di VMware vSphere facendo clic su **ruoli** nella home page del client vSphere. I ruoli forniti dai tool ONTAP per VMware vSphere consentono di eseguire le seguenti attività:

Ruolo	Descrizione
Strumenti NetApp ONTAP per l'amministratore di VMware vSphere	Fornisce tutti i privilegi nativi di vCenter Server e i privilegi specifici degli strumenti ONTAP necessari per eseguire alcuni degli strumenti ONTAP per le attività 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

Il ruolo di amministratore di ONTAP Tools Manager non è registrato in vCenter Server. Questo ruolo è specifico del gestore strumenti ONTAP.

Se la tua azienda richiede l'implementazione di ruoli più restrittivi degli strumenti ONTAP standard per i ruoli VMware vSphere, puoi utilizzare gli strumenti ONTAP per i ruoli VMware vSphere per creare nuovi ruoli.

In questo caso, è necessario clonare gli strumenti ONTAP necessari per i ruoli VMware vSphere e quindi modificare il ruolo clonato in modo che disponga solo dei privilegi richiesti dall'utente.

Autorizzazioni per backend di storage ONTAP e oggetti vSphere

Se l'autorizzazione vCenter Server è sufficiente, gli strumenti ONTAP per VMware vSphere controllano quindi i privilegi RBAC di ONTAP (il ruolo ONTAP) associati alle credenziali backend di storage (il nome utente e la password) per determinare se si dispone di privilegi sufficienti per eseguire le operazioni di storage richieste dai tool ONTAP per l'attività VMware vSphere su quel backend dello storage. Se disponi del ONTAP Privileges corretto, puoi accedere ai backend di storage ed eseguire i tool ONTAP per i task di VMware vSphere. I ruoli ONTAP determinano i tool ONTAP per i task VMware vSphere che puoi eseguire sul backend dello storage.

Componenti delle autorizzazioni vCenter Server

VCenter Server riconosce le autorizzazioni e non i privilegi. Ogni autorizzazione vCenter Server è composta da tre componenti.

VCenter Server include i seguenti componenti:

- Uno o più privilegi (il ruolo)

  I privilegi definiscono le attività che un utente può eseguire.

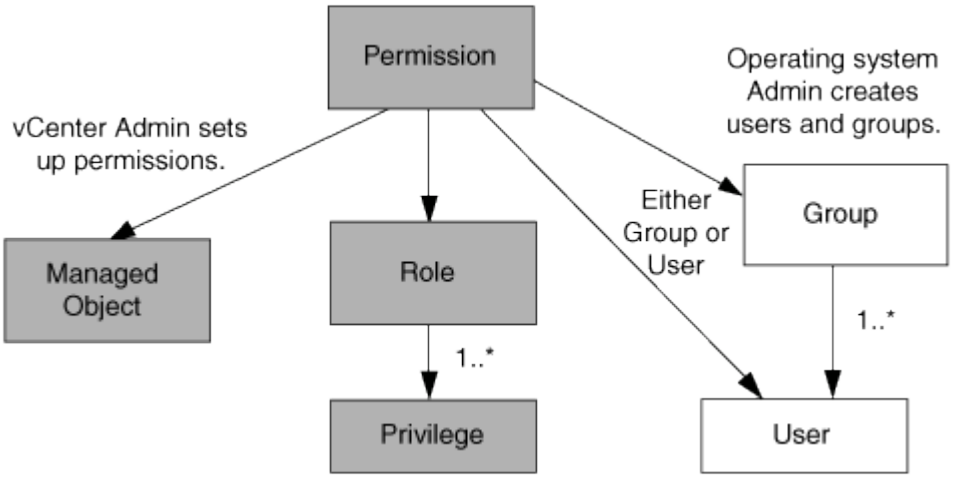
- Un oggetto vSphere

  L'oggetto è la destinazione delle attività.

- Un utente o un gruppo

  L'utente o il gruppo definisce chi può eseguire l'attività.

In questo diagramma, le caselle grigie indicano i componenti presenti in vCenter Server e le caselle bianche indicano i componenti presenti nel sistema operativo in cui è in esecuzione vCenter Server.



Privilegi

Due tipi di privilegi sono associati ai tool ONTAP per VMware vSphere:

- Privilegi vCenter Server nativi

  Questi privilegi vengono forniti con vCenter Server.

- Privilegi specifici per i tool ONTAP

  Questi privilegi sono definiti per strumenti ONTAP specifici per le attività VMware vSphere. Sono esclusivi dei tool ONTAP per VMware vSphere.

Gli strumenti ONTAP per le attività VMware vSphere richiedono privilegi specifici di ONTAP e privilegi nativi di vCenter Server. Questi privilegi costituiscono "role" per l'utente. Un'autorizzazione può avere più privilegi. Questi privilegi sono riservati a un utente che ha effettuato l'accesso a vCenter Server.

Per semplificare le operazioni con vCenter Server RBAC, gli strumenti ONTAP per VMware vSphere forniscono diversi ruoli standard che contengono tutti i privilegi nativi e specifici degli strumenti ONTAP necessari per eseguire gli strumenti ONTAP per i task VMware vSphere.

Se si modificano i privilegi all'interno di un'autorizzazione, l'utente associato a tale autorizzazione deve

disconnettersi e quindi accedere per attivare l'autorizzazione aggiornata.

Oggetti vSphere

Le autorizzazioni sono associate agli oggetti vSphere, come vCenter Server, host ESXi, macchine virtuali, datastore, data center, e cartelle. È possibile assegnare autorizzazioni a qualsiasi oggetto vSphere. In base all'autorizzazione assegnata a un oggetto vSphere, vCenter Server determina chi può eseguire le attività su tale oggetto. Per gli strumenti ONTAP per attività specifiche di VMware vSphere, le autorizzazioni vengono assegnate e convalidate solo a livello di cartella principale (vCenter Server) e non su altre entità. Ad eccezione del funzionamento del plug-in VAAI, in cui le autorizzazioni vengono convalidate per l'host ESXi interessato.

Utenti e gruppi

È possibile utilizzare Active Directory (o la macchina vCenter Server locale) per configurare utenti e gruppi di utenti. È quindi possibile utilizzare le autorizzazioni di vCenter Server per concedere l'accesso a questi utenti o gruppi per consentire loro di eseguire strumenti ONTAP specifici per i task di VMware vSphere.

> ⓘ Queste autorizzazioni di vCenter Server si applicano agli strumenti ONTAP per gli utenti di VMware vSphere vCenter, non agli strumenti ONTAP per gli amministratori di VMware vSphere. Per impostazione predefinita, gli strumenti ONTAP per gli amministratori di VMware vSphere dispongono dell'accesso completo al prodotto e non richiedono le autorizzazioni assegnate.

Gli utenti e i gruppi non hanno ruoli assegnati. Ottengono l'accesso a un ruolo facendo parte di un'autorizzazione vCenter Server.

Assegnare e modificare le autorizzazioni per vCenter Server

Esistono diversi punti chiave da tenere a mente quando si utilizzano le autorizzazioni di vCenter Server. Il successo di un'attività di ONTAP Tools per VMware vSphere dipende dalla posizione in cui è stata assegnata un'autorizzazione o dalle azioni intraprese da un utente dopo la modifica di un'autorizzazione.

Assegnazione delle autorizzazioni

È necessario impostare le autorizzazioni di vCenter Server solo se si desidera limitare l'accesso agli oggetti e alle attività di vSphere. In caso contrario, è possibile accedere come amministratore. Questo login consente di accedere automaticamente a tutti gli oggetti vSphere.

Il punto in cui si assegna l'autorizzazione determina gli strumenti ONTAP per le attività di VMware vSphere che un utente può eseguire.

A volte, per garantire il completamento di un'attività, è necessario assegnare un'autorizzazione a un livello superiore, ad esempio l'oggetto root. Questo accade quando un'attività richiede un privilegio che non si applica a un oggetto vSphere specifico (ad esempio, il monitoraggio dell'attività) o quando un privilegio richiesto si applica a un oggetto non vSphere (ad esempio, un sistema storage).

In questi casi, è possibile impostare un'autorizzazione in modo che venga ereditata dalle entità figlio. È inoltre possibile assegnare altre autorizzazioni alle entità figlio. L'autorizzazione assegnata a un'entità figlio sovrascrive sempre l'autorizzazione ereditata dall'entità padre. Ciò significa che è possibile assegnare autorizzazioni a un'entità figlio per limitare l'ambito di un'autorizzazione assegnata a un oggetto radice e ereditata dall'entità figlio.

A meno che le policy di sicurezza aziendali non richiedano autorizzazioni più restrittive, è consigliabile assegnare autorizzazioni all'oggetto root (anche noto come cartella root).

Permessi e oggetti non vSphere

L'autorizzazione creata viene applicata a un oggetto non vSphere. Ad esempio, un sistema storage non è un oggetto vSphere. Se un privilegio si applica a un sistema di storage, è necessario assegnare l'autorizzazione contenente tale privilegio 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 come gli strumenti ONTAP per il privilegio "Aggiungi/Modifica/Salta sistemi di archiviazione" di VMware vSphere deve essere assegnata a livello dell'oggetto principale.

Modifica delle autorizzazioni

È possibile modificare un'autorizzazione alla volta.

Se si modificano i privilegi all'interno di un'autorizzazione, l'utente associato a tale autorizzazione deve disconnettersi e quindi accedere nuovamente per attivare l'autorizzazione aggiornata.

Privilegi richiesti per gli strumenti ONTAP per le attività VMware vSphere

I diversi strumenti ONTAP per le attività VMware vSphere richiedono diverse combinazioni di privilegi specifici per gli strumenti ONTAP per VMware vSphere e i privilegi nativi di vCenter Server.

Per accedere agli strumenti ONTAP per la GUI di VMware vSphere, è necessario disporre del privilegio View specifico dei tool ONTAP a livello di prodotto assegnato al livello di oggetto vSphere corretto. Se si accede senza questo privilegio, gli strumenti ONTAP per VMware vSphere visualizzano un messaggio di errore quando si fa clic sull'icona NetApp e si impedisce l'accesso agli strumenti ONTAP.

Nel privilegio **View**, è possibile accedere agli strumenti ONTAP per VMware vSphere. Questo privilegio non consente di eseguire attività all'interno degli strumenti ONTAP per VMware vSphere. Per eseguire qualsiasi strumento ONTAP per le attività VMware vSphere, è necessario disporre dei privilegi vCenter Server nativi e specifici per gli strumenti ONTAP per tali attività.

Il livello di assegnazione determina le parti dell'interfaccia utente che è possibile visualizzare. L'assegnazione del privilegio Visualizza all'oggetto principale (cartella) consente di accedere agli strumenti ONTAP per VMware vSphere facendo clic sull'icona NetApp.

È possibile assegnare il privilegio View a un altro livello di oggetto vSphere, tuttavia ciò limita gli strumenti ONTAP per i menu VMware vSphere che è possibile visualizzare e utilizzare.

L'oggetto root è la posizione consigliata per assegnare qualsiasi autorizzazione contenente il privilegio View.

Ruoli ONTAP consigliati per i tool ONTAP per VMware vSphere

È possibile impostare diversi ruoli ONTAP consigliati per lavorare con gli strumenti ONTAP per VMware vSphere e RBAC (role-based access control). Questi ruoli contengono i privilegi di ONTAP necessari per eseguire le operazioni di storage eseguite dai tool ONTAP per i task VMware vSphere.

Per creare nuovi ruoli utente, occorre accedere come amministratore dei sistemi storage che eseguono ONTAP. È possibile creare ruoli ONTAP utilizzando Gestione di sistema di ONTAP 9.8P1 o versioni successive.

Ogni ruolo ONTAP dispone di una coppia di nome utente e password associata, che costituiscono le credenziali del ruolo. Se non si effettua l'accesso utilizzando queste credenziali, non è possibile accedere alle operazioni di storage associate al ruolo.

Come misura di sicurezza, gli strumenti ONTAP per i ruoli ONTAP specifici di VMware vSphere sono ordinati gerarchicamente. Ciò significa che il primo ruolo è il più restrittivo e dispone solo dei privilegi associati al set più elementare di tool ONTAP per le operazioni di storage di VMware vSphere. Il ruolo successivo include i propri privilegi e tutti i privilegi associati al ruolo precedente. Ogni ruolo aggiuntivo è meno restrittivo delle operazioni di storage supportate.

Di seguito sono elencati alcuni dei ruoli RBAC di ONTAP consigliati quando si utilizzano i tool ONTAP per VMware vSphere. Dopo aver creato questi ruoli, è possibile assegnarli agli utenti che devono eseguire attività correlate allo storage, ad esempio il provisioning di macchine virtuali.

Ruolo	privilegi
Discovery (rilevamento)	Questo ruolo consente di aggiungere sistemi storage.
Creare storage	Questo ruolo consente di creare storage. Questo ruolo include anche tutti i privilegi associati al ruolo di rilevamento.
Modificare lo storage	Questo ruolo consente di modificare lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo di rilevamento e al ruolo Crea archivio.
Distruggere lo storage	Questo ruolo consente di distruggere lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo di rilevamento, al ruolo Crea archivio e al ruolo Modifica archivio.

Se si utilizzano strumenti ONTAP per VMware vSphere, è necessario impostare anche un ruolo di gestione basata su criteri (PBM, Policy-Based Management). Questo ruolo consente di gestire lo storage utilizzando le policy di storage. Questo ruolo richiede anche la configurazione del ruolo "DDiscovery".

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.

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 attivare o disattivare AutoSupport solo al momento della distribuzione. 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. Per una trasmissione corretta, è necessario includere l'URL 216.240.21.18 // support.netapp.com nella rete.

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.
- Gestione password - Reimposta la password dell'applicazione OVA per l'utente.

Per accedere a ONTAP Tools Manager, avviare il `https://loadBalanceIP:8443/virtualization/ui/` sistema dal browser e accedere con gli strumenti ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.

Implementa i tool ONTAP per VMware vSphere

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**
  - 10 GB per le installazioni con thin provisioning
  - 248 GB per installazioni con thick provisioning
- **I requisiti di dimensionamento del sistema host per nodo** la memoria consigliata in base alla dimensione dell'implementazione e per nodo è indicata nella tabella seguente:

Tipo di distribuzione	CPU	Memoria (GB)
Piccolo (S)	8	16
Medio (M)	12	24
Grande (L)	16	32

Per ulteriori informazioni, consultare la sezione *limiti di configurazione per l'implementazione degli strumenti ONTAP per VMware vSphere* riportata di seguito.

Requisiti minimi di archiviazione e applicazione

Storage, host e applicazioni	Requisiti minimi di versione
ONTAP	Ultima versione delle patch di ONTAP 9.12,1, 9.13.1, 9.14.1 e 9.15.1.
Host ESXi	ESXi 7.0.3
Server vCenter	VCenter 7.0U3
Provider VASA	3,0
Applicazione OVA	10,2

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	Tipo di protocollo
Implementazione semplice	Piccolo (S)	CIRCA 12K MB	32	NFS, iSCSI
Implementazione semplice	Medio (M)	CIRCA 24K MB	64	NFS, iSCSI
Alta disponibilità	Piccolo (S)	CIRCA 24K MB	64	NFS, iSCSI
Alta disponibilità	Medio (M)	circa 50k mb	128	NFS, iSCSI
Alta disponibilità	Grande (L)	circa 100k mb	256 [NOTA] il numero di host nella tabella mostra il numero totale di host da più vCenter.	NFS, iSCSI

Per informazioni dettagliate sui requisiti di dimensionamento del sistema host per nodo, fare riferimento alla "Prerequisiti per la distribuzione degli strumenti ONTAP per VMware vSphere".

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".

Controlli pre-implementazione

Prima di procedere con la distribuzione, accertarsi che siano presenti i seguenti elementi:

- L'ambiente vCenter Server è configurato e configurato.
- (Facoltativo) per l'utente di automazione - NetApp ha fornito Postman collezioni il file JSON è raccolto.
- Le credenziali vCenter Server padre per la distribuzione dell'OVA sono state implementate.

  La password di vCenter Server padre non deve contenere questi caratteri speciali ($, ', ").

- Si dispone delle credenziali di accesso per l'istanza di vCenter Server a cui si connetteranno gli strumenti ONTAP per VMware vSphere dopo la distribuzione, per la registrazione.
- La cache del browser è stata eliminata.
- Assicurati di disporre di tre indirizzi IP gratuiti per l'implementazione non ha: Un indirizzo IP gratuito per il bilanciamento del carico e un indirizzo IP gratuito per il piano di controllo Kubernetes e un indirizzo IP per il nodo. Per l'implementazione ha, insieme a questi tre indirizzi IP, saranno necessari altri due indirizzi IP per il secondo e il terzo nodo. I nomi host devono essere mappati agli indirizzi IP liberi sul DNS prima di assegnare le implementazioni ha e non ha. Tutti i cinque indirizzi IP nell'implementazione ha e i tre indirizzi IP nell'implementazione non ha devono trovarsi sulla stessa VLAN selezionata per l'implementazione.
- Assicurarsi che il nome di dominio su cui viene emesso il certificato sia mappato all'indirizzo IP virtuale in una distribuzione multi-vCenter in cui i certificati CA personalizzati sono obbligatori. *Nslookup* viene eseguito un controllo sul nome di dominio per verificare se il dominio viene risolto all'indirizzo IP desiderato. I certificati devono essere creati con il nome di dominio e l'indirizzo IP dell'indirizzo IP del bilanciatore del carico.
- Prima di installare gli strumenti ONTAP per VMware vSphere 10,2 nella configurazione non ha avanzata e ha, consultare l'articolo della Knowledge base: "Prerequisiti per la configurazione ha e avanzata non-ha"

Implementa i tool ONTAP per VMware vSphere

Puoi implementare i tool ONTAP per VMware vSphere in due configurazioni:

- Configurazione a nodo singolo non ha
- Configurazione HA

Configurazione a nodo singolo non ha

È possibile implementare una configurazione a nodo singolo non ha in configurazioni piccole o medie.

- La configurazione piccola non ha contiene 8 CPU e 16 GB di RAM.
- La configurazione media non ha contiene 12 CPU e 24 GB di RAM.

Prima di iniziare

Assicurarsi che il percorso di rete sia presente. La rete di dati dello storage deve essere accessibile dalla rete di gestione delle macchine virtuali. Ad esempio, accedere a ONTAP > eseguire il comando *network route create -vserver <SVM> -destination 0,0.0.0/0 -gateway <gateway_ip>*

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" .
2. Accedere al server vSphere.
3. Passare al pool di risorse creato, al cluster o all'host in cui si desidera distribuire l'OVA.
4. Fare clic con il pulsante destro del mouse sulla posizione desiderata e selezionare **Deploy OVF template…** (distribuire modello OVF…).

   Non implementare i tool ONTAP per la macchina virtuale VMware vSphere in un datastore vVol gestito dal reparto IT.

5. Selezionare il file OVA tramite l'URL per il file *.ova* o navigare alla cartella in cui è stato salvato il file *.ova*, quindi fare clic su **Avanti**.
6. Selezionare una risorsa di computer e fare clic su **Avanti**.
7. Esaminare i dettagli del modello e fare clic su **Avanti**.
8. Leggere e accettare il contratto di licenza.
9. Selezionare la configurazione di distribuzione e fare clic su **Avanti**.

   Le opzioni di implementazione avanzate utilizzano Trident come provisioner di storage dinamico per ONTAP per creare volumi e la semplice implementazione usa lo storage locale per creare volumi.

10. Selezionare lo spazio di archiviazione per la configurazione e i file del disco e fare clic su **Avanti**.
11. Selezionare la rete di destinazione per ciascuna rete di origine e fare clic su **Avanti**.
12. Nel modello **Personalizza**, immettere i dettagli richiesti e fare clic su **Avanti**
    - Una volta abilitato l'ambito SVM, dovresti aver già abilitato il supporto SVM con l'indirizzo IP di gestione.
    - Le informazioni qui fornite sono convalidate per i modelli corretti durante il processo di installazione. In caso di discrepanza, viene visualizzato un messaggio di errore sulla console Web e viene richiesto di correggere eventuali informazioni errate fornite.
    - I nomi host devono essere costituiti da lettere maiuscole (A-Z), lettere minuscole (a-z), cifre (0-9) o dal trattino (-). Se si desidera configurare lo stack doppio, specificare il nome host mappato all'indirizzo IPv6.

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

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.

Configurazione HA

È possibile configurare tre nodi ha in configurazioni piccole, medie o grandi. L'implementazione HA utilizza Trident per memorizzare i dati dei servizi.

- I tre nodi ha di piccole dimensioni contengono 8 CPU e 16 GB di RAM per nodo.
- I tre nodi ha di medie dimensioni contengono 12 CPU e 24 GB di RAM per nodo.
- I tre nodi ad alta disponibilità di grandi dimensioni contengono 16 CPU e 32 GB di RAM per nodo.

Prima di iniziare

Questa attività offre istruzioni su come installare tre nodi ha in configurazioni piccole, medie o elevate.

La creazione della libreria di contenuti è un prerequisito obbligatorio per la distribuzione della configurazione ha a tre nodi. 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 di un cluster possano accedervi. È necessario creare una libreria di contenuti per memorizzare l'OVA prima di distribuire l'OVA nella configurazione ha.

Il modello della libreria di contenuti una volta caricato non deve essere eliminato dopo la distribuzione, poiché verrà utilizzato durante i riavvii.

Creare la libreria di contenuti utilizzando i seguenti passaggi:

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 utilizzando `https://vcenterip/ui`
3. Selezionare i puntini di sospensione orizzontali accanto al 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.

Assicurati di aver importato il tuo OVA nella tua libreria di contenuti. Tenere a portata di mano il nome della libreria dei contenuti e dell'elemento della libreria fornito all'elemento OVA.

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

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" .
2. Accedere al server vSphere.
3. Passare al pool di risorse creato, al cluster o all'host in cui si desidera distribuire l'OVA.
4. Fare clic con il pulsante destro del mouse sulla posizione desiderata e selezionare **Deploy OVF template…** (distribuire modello OVF…).

   Non implementare i tool ONTAP per la macchina virtuale VMware vSphere in un datastore vVol gestito dal reparto IT.

5. Selezionare il file OVA tramite l'URL per il file *.ova* o navigare alla cartella in cui è stato salvato il file *.ova*, quindi fare clic su **Avanti**.
6. Per implementare i tool ONTAP per VMware vSphere dall'archivio di contenuti:
   a. Vai alla tua libreria di contenuti e fai clic sull'elemento della libreria che desideri distribuire.
   b. Fare clic su **azioni** > **Nuova VM da questo modello**
7. Selezionare una risorsa di computer e fare clic su **Avanti**.
8. Esaminare i dettagli del modello e fare clic su **Avanti**.
9. Leggere e accettare il contratto di licenza e fare clic su **Avanti**.
10. Selezionare la configurazione di distribuzione e fare clic su **Avanti**.
11. Selezionare lo spazio di archiviazione per la configurazione e i file del disco e fare clic su **Avanti**.
12. Selezionare la rete di destinazione per ciascuna rete di origine e fare clic su **Avanti**.
13. Nella finestra **Personalizza modello**, compilare i campi obbligatori e fare clic su **Avanti**.
    - In modalità di implementazione ha, non rinominare i nomi delle VM dopo l'implementazione.
    - Una volta abilitato l'ambito SVM, dovresti aver già abilitato il supporto SVM con l'indirizzo IP di gestione.
    - Le informazioni qui fornite sono convalidate per i modelli corretti durante il processo di installazione. In caso di discrepanza, viene visualizzato un messaggio di errore sulla console Web e viene richiesto di correggere eventuali informazioni errate fornite.
    - I nomi host devono essere costituiti da lettere maiuscole (A-Z), lettere minuscole (a-z), cifre (0-9) o dal trattino (-). Se si desidera configurare lo stack doppio, specificare il nome host mappato all'indirizzo IPv6.

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

14. 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.

15. 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 nei valori immessi nel modulo OVF, viene visualizzata una finestra di dialogo che richiede di intraprendere un'azione correttiva. Apportare le modifiche necessarie all'interno della finestra di dialogo, utilizzando il pulsante Tab per navigare e selezionare "OK". Hai tre tentativi per risolvere eventuali problemi. Se i problemi persistono dopo tre tentativi, il processo di installazione verrà interrotto e si consiglia di riprovare l'installazione su una nuova VM.

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 tb, 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

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).
051	Distribuzione delle macchine virtuali secondarie non riuscita	* Se vengono create la seconda e la terza macchina virtuale, accertarsi che siano disponibili risorse di CPU/memoria sufficienti prima di accendere le macchine virtuali secondarie e riavviare la macchina virtuale principale. * Se la seconda e la terza macchina virtuale si trovano negli strumenti di distribuzione ONTAP per l'attività modello VMware vSphere, attendere il completamento dell'attività, accendere le macchine virtuali e riavviare la macchina virtuale principale. * Ridistribuire.
052	Copia chiavi SSH non riuscita	Riavviare la macchina virtuale principale.
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 ridistribuirla.
056	Accesso a ISCSI non riuscito	Accertarsi che il protocollo iSCSI sia attivato e configurato correttamente su ONTAP. Verificare che l'indirizzo IP della LIF dati iSCSI fornito sia corretto e online. Riavviare la VM se i punti precedenti sono corretti. Altrimenti, ridistribuzione.

057	Implementazione Trident non riuscita	*Assicurati che gli indirizzi IP della LIF di gestione e della LIF dati siano raggiungibili dalla VM. *Assicurarsi che il protocollo NFS o iSCSI sia abilitato e configurato correttamente su ONTAP. *Verificare che l'indirizzo IP NFS/iSCSI Data LIF fornito sia corretto e online. *Assicurarsi che il nome utente e la password forniti siano corretti e che l'utente disponga di privilegi sufficienti per creare un volume. * Riavviare se tutti i punti precedenti sono corretti. Altrimenti, ridistribuzione.
058	Importazione Trident non riuscita	*Assicurarsi che il nome utente e la password forniti siano corretti e che l'utente disponga di privilegi sufficienti per creare, montare, clonare ed eliminare volumi. *Assicurarsi di utilizzare la stessa configurazione di ONTAP per ripristinare l'installazione e riprovare il ripristino.
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 ridistribuisci.
062	Distribuzione del provider VASA e SRA non riuscita	Fare riferimento ai log degli errori in /var/log/ansible-perl-errors.log per ulteriori dettagli e ridistribuire.
064	verifica version.xml non riuscita	Ridistribuzione
065	L'URL della pagina Swagger non è raggiungibile	Ridistribuzione

066	Procedura di post-implementazione non riuscita	-
088	La configurazione della rotazione del registro per il giornale non è riuscita	Riavviare la macchina virtuale principale.
089	La modifica della proprietà del file di configurazione rotazione del registro di riepilogo non è riuscita	Riavviare la macchina virtuale principale.

Riavviare il codice di errore	Flusso di lavoro
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

Codice errore di ripristino	Flusso di lavoro	Risoluzione
104	I passaggi successivi al ripristino non sono riusciti.	-
105	La copia dei contenuti nel volume di ripristino non è riuscita.	-
106	Impossibile montare il volume di ripristino.	* Assicurati di utilizzare la stessa SVM e che sia presente il volume di recovery nella SVM. (Il nome del volume di recovery inizia con otvng_Trident_recovery) * assicurati che gli indirizzi IP della LIF di gestione e della LIF dati siano raggiungibili dalla VM. * Assicurarsi che il protocollo NFS/iSCSI sia abilitato e configurato correttamente su ONTAP. * Assicuratevi che l'indirizzo IP NFS/iSCSI DAT LIF fornito sia corretto e online. * Assicurarsi che il nome utente, la password e il protocollo forniti siano corretti e che l'utente disponga di privilegi sufficienti per creare, montare, clonare ed eliminare. * Riprovare il ripristino

Configurare gli strumenti ONTAP

Aggiungere istanze di vCenter Server

VCenter Server offre la piattaforma di gestione centrale che consente di controllare host, macchine virtuali (VM) e backend dello storage.

A proposito di questa attività

Puoi aggiungere e gestire più istanze di vCenter Server con una sola istanza dei tool ONTAP per VMware vSphere.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web: `https://loadBalanceIP: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** dalla barra laterale.
4. Selezionare **Aggiungi** per le istanze di vCenter Server integrate e fornire l'indirizzo IP/nome host vCenter, il nome utente, la password e i dettagli della porta.

Quando si aggiunge un'istanza di vCenter Server agli strumenti ONTAP, vengono eseguite automaticamente le seguenti azioni:

- Il plug-in del client vCenter è registrato
- I privilegi personalizzati per i plug-in e le API vengono inviati all'istanza di vCenter Server
- Per gestire gli utenti vengono creati ruoli personalizzati.

Quando si aggiunge un'istanza di vCenter Server, gli strumenti ONTAP per il plug-in VMware vSphere vengono registrati automaticamente in vCenter Server come plug-in remoto. Il plug-in è visibile nei collegamenti dell'interfaccia utente di vSphere.

Il plug-in viene registrato con la chiave *com.netapp.otv* dell'istanza di vCenter Server ed è visibile in ExtensionManager dell'istanza di vCenter Server.

Registrare il provider VASA con un'istanza di vCenter Server

È possibile registrare e annullare la registrazione del provider VASA con un'istanza di vCenter Server utilizzando gli strumenti ONTAP per l'interfaccia di plug-in remoto di VMware vSphere. La sezione Impostazioni provider VASA mostra lo stato di registrazione provider VASA per vCenter Server selezionato.

Fasi

1. Accedere al client vSphere utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **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. Fare clic sul 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, quindi fare clic su **REGISTRA**.
6. Una volta completata la registrazione e l'aggiornamento della pagina, l'interfaccia utente mostra lo stato, il nome e la versione del provider VASA registrato. L'azione di annullamento della registrazione è attivata.
7. Se si desidera annullare la registrazione del provider VASA, attenersi alla seguente procedura:
   a. Per annullare la registrazione del provider VASA, selezionare l'opzione **Annulla registrazione** nella parte inferiore della schermata.
   b. Nella pagina **Unregister VASA provider**, è possibile vedere il nome del provider VASA. In questa pagina, fornire le credenziali utente dell'applicazione e fare clic su **Annulla registrazione**.

Al termine

Verificare che il provider VASA integrato sia elencato sotto VASA Provider dall'interfaccia utente del client vCenter e dall'interfaccia utente del plug-in remoto.

Fasi

1. Per verificare VASA Provider dall'interfaccia utente del client vCenter, attenersi alla seguente procedura:
   a. Accedere a vCenter Server.
   b. Accedere con le credenziali di amministratore.
   c. Selezionare **fornitori di archiviazione**.
   d. Selezionare **Configura**.
   e. Nella sezione relativa ai backend storage/provider di storage, verificare che il provider VASA integrato sia elencato correttamente.
2. Per verificare il provider VASA dall'interfaccia utente del plug-in remoto, attenersi alla seguente procedura:
   a. Accedere al client vSphere utilizzando `https://vcenterip/ui`
   b. Nella pagina dei collegamenti, fare clic su **NetApp ONTAP tools** nella sezione dei plug-in.
   c. È possibile visualizzare il provider VASA registrato nella pagina panoramica e nella pagina **Impostazioni** > **Impostazioni provider VASA**.

Installare il plug-in NFS VAAI

Puoi installare il plug-in NFS NetApp per le API vSphere per l'integrazione degli array (VAAI) utilizzando i tool ONTAP per VMware vSphere.

Cosa ti serve

- Si dovrebbe aver scaricato il pacchetto di installazione per il plug-in NFS per VAAI (`.vib`) dal sito di supporto NetApp. "Plug-in NetApp NFS per VMware VAAI"
- Si dovrebbe avere installato ESXi host 7.0U3 ultima patch come versione minima e ONTAP 9.12.1Px (ultima versione P) 9.13.1Px, 9.14.1Px, o successiva.
- L'host ESXi dovrebbe essere stato alimentato e montato un datastore NFS.

- I valori delle `DataMover.HardwareAcceleratedMove` `DataMover.HardwareAcceleratedInit` `VMFS3.HardwareAcceleratedLocking` impostazioni , e host dovrebbero essere impostati su "`1'".

  Questi valori vengono impostati automaticamente sull'host ESXi quando viene aggiornata la finestra di dialogo Recommended Settings (Impostazioni consigliate).

- Dovresti aver attivato l'opzione vstorage sulla storage Virtual Machine (SVM) usando il `vserver nfs modify -vserver vserver_name -vstorage enabled` comando.
- Se si utilizza il plug-in NetApp NFS VAAI 2,0, si dovrebbe avere ESXi 7.0U3 o versione successiva.
- È necessario disporre delle ultime release di patch di vSphere 7.0U3 poiché vSphere 6,5 è stato obsoleto.
- VSphere 8.x è supportato con il plug-in NetApp NFS VAAI 2,0.1 (build 16).

Fasi

1. Fare clic su **Impostazioni** nella home page degli strumenti di ONTAP per VMware vSphere.
2. Fare clic sulla scheda **NFS VAAI Tools** (Strumenti VAAI NFS).
3. 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**.
4. Sfogliare e selezionare il `.vib` file e fare clic su **carica** per caricare il file negli strumenti ONTAP.
5. Fare clic su **Install on ESXI host**, selezionare l'host ESXi su cui si desidera installare il plug-in NFS VAAI, quindi fare clic su **Install**.

   Vengono visualizzati solo gli host ESXi idonei per l'installazione del plug-in. Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo. È possibile monitorare l'avanzamento dell'installazione nella sezione Recent Tasks (attività recenti) di vSphere Web Client.

6. Al termine dell'installazione, riavviare manualmente l'host ESXi.

   Quando l'amministratore VMware riavvia l'host ESXi, i tool ONTAP per VMware vSphere rilevano automaticamente il plug-in NFS VAAI e non occorre eseguire passaggi aggiuntivi per abilitare il plug-in.

Configura le policy di esportazione NFS corrette per l'offload delle copie VAAI

Quando si configura VAAI in un ambiente NFS, le regole delle policy di esportazione devono essere configurate tenendo presente i seguenti requisiti:

- Il volume corrispondente deve consentire le chiamate NFSv4.
- 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.

Configurare le impostazioni dell'host ESXi

Configurare le impostazioni di multipath e timeout del server ESXi

I tool ONTAP per VMware vSphere controllano e impostano le impostazioni di multipath

host ESXi e le impostazioni di timeout HBA che funzionano meglio con i sistemi storage NetApp.

A proposito di questa attività

Questo processo potrebbe richiedere molto tempo, a seconda della configurazione e del carico di sistema. L'avanzamento dell'attività viene visualizzato nel pannello Recent Tasks (attività recenti). Una volta completate le attività, l'icona Avviso di stato dell'host viene sostituita dall'icona normale o dall'icona di riavvio in sospeso.

Fasi

1. Nella home page del client Web VMware vSphere, fare clic su **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, fare clic su **NetApp ONTAP tools** nella sezione dei plug-in.
4. Accedere alla scheda di conformità host ESXi nella Panoramica (dashboard) dei tool 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 rispettare con le impostazioni dell'host consigliate da NetApp e fare clic su **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 riquadro di riepilogo, controllare i valori e fare clic su **fine**. È possibile tenere traccia dell'avanzamento nel riquadro attività recenti.

Impostare i valori dell'host ESXi

È possibile impostare timeout e altri valori sugli host ESXi utilizzando gli strumenti ONTAP per VMware vSphere per garantire le migliori performance e il failover corretto. 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

Consente di impostare le impostazioni di timeout dell'HBA consigliate per i sistemi di archiviazione NetApp.

- **Disk.QFullSampleSize**

  Impostare questo valore su 32 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.

- **Disk.QFullThreshold**

  Impostare questo valore su 8 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.

- **Timeout HBA FC Emulex**

  Utilizzare il valore predefinito.

- **Timeout HBA FC QLogic**

  Utilizzare il valore predefinito.

Impostazioni MPIO

Le impostazioni MPIO definiscono i percorsi preferiti per i sistemi storage NetApp. Le impostazioni MPIO determinano quali percorsi disponibili sono ottimizzati (rispetto ai percorsi non ottimizzati che attraversano il cavo di interconnessione) e impostano il percorso preferito verso 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.

Impostazioni NFS

- **Net.TcpipelHeapSize**

  Impostare questo valore su 32.

- **Net.TcpipelHeapMax**

  Impostare questo valore su 1024 MB.

- **NFS.MaxVolumes**

  Impostare questo valore su 256.

- **NFS41.MaxVolumes**

  Impostare questo valore su 256.

- **NFS.MaxQueueDepth**

  Impostare questo valore su 128 o superiore per evitare colli di bottiglia in coda.

- **NFS.HeartbeatMaxFailures**

  Impostare questo valore su 10 per tutte le configurazioni NFS.

- **NFS.HeartbeatFrequency**

  Impostare questo valore su 12 per tutte le configurazioni NFS.

- **NFS.HeartbeatTimeout**

  Impostare questo valore su 5 per tutte le configurazioni NFS.

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.

Cosa ti serve

- 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. Accedi 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. **Sfoglia** 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 i privilegi (rilevamento, Crea archivio, Modifica archivio, archiviazione distrutta, ruolo NAS/SAN) richiesti per l'utente, quindi fare clic su **Aggiungi**.

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

L'operazione di disinstallazione non rimuove i ruoli dello strumento ONTAP, ma rimuove i nomi localizzati per Privileges specifico dello strumento ONTAP e aggiunge il prefisso `XXX missing privilege`. Quando si reinstallano gli strumenti ONTAP per VMware vSphere o si esegue l'aggiornamento a una versione più recente, vengono ripristinati tutti gli strumenti ONTAP standard per i ruoli VMware vSphere e i privilegi specifici degli strumenti ONTAP.

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:

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

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. Accedi 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.

   c. Aggiungere tutte le API necessarie e salvare le modifiche.
4. Crea utenti:

a. Selezionare **Aggiungi** nella tabella **utenti**.
b. Nella finestra di dialogo **Aggiungi utente**, selezionare **System Manager**.
c. Immettere il **Nome utente**.
d. Selezionare **ruolo** dalle opzioni create nel passaggio **Crea ruoli** riportato sopra.
e. Immettere le applicazioni a cui assegnare l'accesso e il metodo di autenticazione. ONTAPI e HTTP sono le applicazioni richieste e il tipo di autenticazione è **Password**.
f. Impostare **Password per l'utente** e **Salva** l'utente.

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

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/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
/api	Sola lettura	Gli utenti del cluster devono avere questo privilegio per ottenere il corretto stato di backend dello storage. In caso contrario, Gestione strumenti di ONTAP mostra lo stato di backend dello storage "sconosciuto".

Aggiorna i tool ONTAP per VMware vSphere 10,1 a un utente 10,2

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 10,2.

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 10,2.

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

I backend dello storage sono sistemi utilizzati dagli host ESXi per lo storage dei dati. Puoi aggiungere un backend dello storage usando il gestore degli strumenti di ONTAP o l'interfaccia utente del client vSphere.

A proposito di questa attività

Questo task ti aiuta a integrare un cluster ONTAP. Quando Aggiungi il backend dello storage utilizzando ONTAP Tools Manager, il back-end dello storage viene aggiunto al cluster globale. Associare il cluster globale a un'istanza di vCenter Server per consentire a un utente SVM il provisioning del datastore vVol.

Utilizzo di ONTAP Tools Manager

Un backend dello storage è globale quando aggiunto da ONTAP Tools Manager o dalle API degli strumenti ONTAP. Un backend dello storage è locale quando aggiunto dalle API di vCenter Server. Ad esempio, in un setup multi-tenant, puoi aggiungere un back-end dello storage (cluster) a livello globale e una SVM a livello locale per utilizzare le credenziali utente della SVM.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web: `https://loadBalanceIP: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 **Aggiungi**.
5. Fornire l'indirizzo IP del server o i dettagli relativi all'FQDN, al nome utente e alla password e selezionare **Aggiungi**.

Sono supportate le LIF di gestione IPv4 e IPv6. Sono supportate anche le credenziali basate sugli utenti SVM con LIF di gestione.

Utilizzo dell'interfaccia utente del client vSphere

Quando si aggiunge un backend storage utilizzando l'interfaccia utente del client vSphere, il datastore vVol non supporta l'aggiunta diretta di un utente SVM.

1. Accedere al client vSphere utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti di ONTAP, accedere a **backend di archiviazione** e selezionare **Aggiungi**.
4. Nella finestra **Aggiungi backend archiviazione**, specificare l'indirizzo IP del server, il nome utente, la password e i dettagli della porta e fare clic su **Aggiungi**.

Puoi aggiungere credenziali basate sul cluster e LIF DI gestione IPv4 e IPv6 o credenziali basate su SVM con una LIF di gestione SVM per aggiungere direttamente un utente SVM.

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

La pagina dell'elenco di vCenter Server mostra il numero associato di backend storage. Ogni istanza di vCenter Server può associare un backend dello storage.

A proposito di questa attività

Questo task ti aiuta a creare la mappatura tra il back-end dello storage e l'istanza vCenter Server integrata a livello globale.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web: `https://loadBalanceIP: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. Fare clic sulle ellissi verticali sul vCenter che si desidera associare ai backend di storage.
5. Selezionare il backend di archiviazione dal menu a discesa nella finestra a comparsa.
6. Selezionare l'opzione **Associa backend archiviazione** per associare l'istanza di vCenter Server al backend di archiviazione richiesto.

Configurare l'accesso alla rete

Se si dispone di più indirizzi IP dell'host ESXi, tutti gli indirizzi IP rilevati dall'host vengono aggiunti a un criterio di esportazione per impostazione predefinita. Se non si desidera aggiungere tutti gli indirizzi IP a un criterio di esportazione, fornire un'impostazione per consentire specifici indirizzi IP in un elenco o intervallo separati da virgola o CIDR o una combinazione di tutti e tre per ogni vCenter.

È possibile scegliere di consentire alcuni indirizzi host ESXi specifici per l'operazione di montaggio del datastore. Se l'impostazione non viene fornita, il criterio di esportazione aggiunge tutti gli indirizzi IP rilevati nella fase di pre-montaggio. Se viene fornita l'impostazione, gli strumenti ONTAP per VMware vSphere aggiungono solo quelli che rientrano nell'intervallo o negli indirizzi IP elencati. Se nessuno degli indirizzi IP di un host appartiene agli indirizzi IP elencati, il montaggio su tale host non riesce.

Fasi

1. Accedere al client vSphere utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti di ONTAP, selezionare **Impostazioni** > **Gestisci accesso alla rete** > **Modifica**.

   Utilizzare una virgola (,) per separare gli indirizzi IP. È possibile specificare un indirizzo IP specifico, un intervallo di indirizzi IP o IPv6.

4. Fare clic su **Save** (Salva).

Protezione di datastore e macchine virtuali

Proteggere utilizzando la protezione del cluster host

Creazione della protezione dei cluster di 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.

Prerequisiti

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. Gli archivi dati 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 utilizzando `https://vcenterip/ui`
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 una relazione SnapMirror come policy di tipo AutomatedFailOverDuplex, è obbligatorio aggiungere la VM di 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 è presente una configurazione host uniforme e non uniforme. 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 a. "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**, durante l'operazione di creazione, è supportata solo l'azione di eliminazione. È possibile eliminare e aggiungere nuovamente la protezione. Durante l'operazione di modifica della protezione del cluster host, è disponibile l'opzione di modifica. È possibile modificare o eliminare le relazioni utilizzando le opzioni del menu kebab.
10. Selezionare il pulsante **Proteggi**.

    Viene creata un'attività vCenter con i dettagli dell'ID lavoro e l'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.

Cosa ti serve

- È necessario aver configurato l'istanza di vCenter Server e l'host ESXi configurato.
- Dovresti aver distribuito gli strumenti ONTAP.
- Il `.tar.gz` file dell'adattatore SRA dovrebbe essere stato scaricato dal "Sito di supporto NetApp" .

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

Cosa ti serve

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

Cosa ti serve

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
`StorageProvider.resignatureTimeout`	Aumentare il valore dell'impostazione da 900 secondi a 12000 secondi.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	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 storage, consultare la documentazione di VMware.

"Documentazione VMware vSphere: Modifica delle impostazioni dello Storage Provider"

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 ulteriori informazioni, consultare la documentazione VMware sulla modifica delle impostazioni del provider SAN.

"Documentazione di VMware Site Recovery Manager: Modifica delle impostazioni di storage"

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.

Cosa ti serve

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, fare clic su **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 del provider VASA/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.

Cosa ti serve

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 i gruppi di protezione

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

Cosa ti serve

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 fare clic su **Site Recovery** > **gruppi di protezione**.
2. Nel riquadro **Protection Groups** (gruppi di protezione), fare clic su **New** (nuovo).
3. Specificare un nome e una descrizione per il gruppo protezione, direzione e fare clic su **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 fare clic su **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 facendo clic su **Aggiungi al nuovo piano di ripristino**.
7. Nella scheda Pronto per il completamento, esaminare i dettagli del gruppo di protezione creato, quindi fare clic su **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).

> Storage Replication Adapter (SRA) non supporta le configurazioni di SnapMirror fan-out. Le configurazioni fan-out di SnapMirror sono quelle in cui un volume di origine viene replicato in due diverse destinazioni. Questi creano un problema durante il ripristino quando VMware Live Site Recovery deve ripristinare la macchina virtuale dalla sua destinazione.

Cosa ti serve

- 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 fare clic su **Sites**.
2. Fare clic su **oggetti** > **azioni** > **Associa siti**.
3. Nella finestra di dialogo **Pair Site Recovery Manager Servers**, immettere l'indirizzo del Platform Services Controller del sito protetto, quindi fare clic su **Next**.
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 fare clic su **fine**.
5. Se richiesto, fare clic su **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

Cosa ti serve

È necessario aver collegato i siti protetti e di ripristino.

Fasi

1. Accedere a vCenter Server e fare clic su **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e fare clic su **Gestisci**.
3. Nella scheda Manage (Gestisci), selezionare **Network Mappings** (Mapping di rete).
4. Fare clic su **nuovo** per creare una nuova mappatura di rete.

   Viene visualizzata la procedura guidata Create Network Mapping.

5. Nella procedura guidata Create Network Mapping (Crea mappatura di rete), eseguire le seguenti operazioni:
   a. Selezionare **prepara automaticamente mappature per reti con nomi corrispondenti** e fare clic su **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e fare clic su **Aggiungi mappature**.
   c. Fare clic su **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi fare clic su **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.

Cosa ti serve

È necessario aver collegato i siti protetti e di ripristino.

Fasi

1. Accedere a vCenter Server e fare clic su **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e fare clic su **Gestisci**.
3. Nella scheda Gestisci, selezionare **Mapping cartelle**.
4. Selezionare l'icona **cartella** per creare una nuova mappatura di cartelle.

   Viene visualizzata la procedura guidata Create Folder Mapping.

5. Nella procedura guidata Create Folder Mapping (Crea mappatura cartelle), eseguire le seguenti operazioni:
   a. Selezionare **prepara automaticamente mappature per cartelle con nomi corrispondenti** e fare clic su **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e fare clic su **Aggiungi mappature**.
   c. Fare clic su **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi fare clic su **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.

Cosa ti serve

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 fare clic su **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e fare clic su **Gestisci**.
3. Nella scheda Manage (Gestisci), selezionare **Resource Mapping**.
4. Fare clic su **nuovo** per creare una nuova mappatura delle risorse.

   Viene visualizzata la procedura guidata Create Resource Mapping.

5. Nella procedura guidata Create Resource Mapping (Crea mappatura risorse), eseguire le seguenti operazioni:
   a. Selezionare **prepara automaticamente mappature per risorsa con nomi corrispondenti** e fare clic su **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e fare clic su **Aggiungi mappature**.
   c. Fare clic su **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi fare clic su **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.

Cosa ti serve

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

Fasi

1. Accedere a vCenter Server e fare clic su **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e fare clic su **Gestisci**.
3. Nella scheda Manage (Gestisci), selezionare **Placeholder Datastore**.
4. Fare clic su **nuovo** per creare un nuovo archivio dati segnaposto.
5. Selezionare l'archivio dati appropriato e fare clic su **OK**.

   Gli archivi dati segnaposto possono essere locali o remoti e non devono essere replicati.

6. 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).

Cosa ti serve

- 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, fare clic su **Array Managers**, quindi su **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 di storage utilizzato per integrare il sistema storage con gli strumenti di ONTAP. 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. Fare clic su **Avanti**.
4. Verificare che l'array sia rilevato e visualizzato nella parte inferiore della finestra Add Array Manager (Aggiungi array) e fare clic su **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.

Cosa ti serve

- 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.

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.

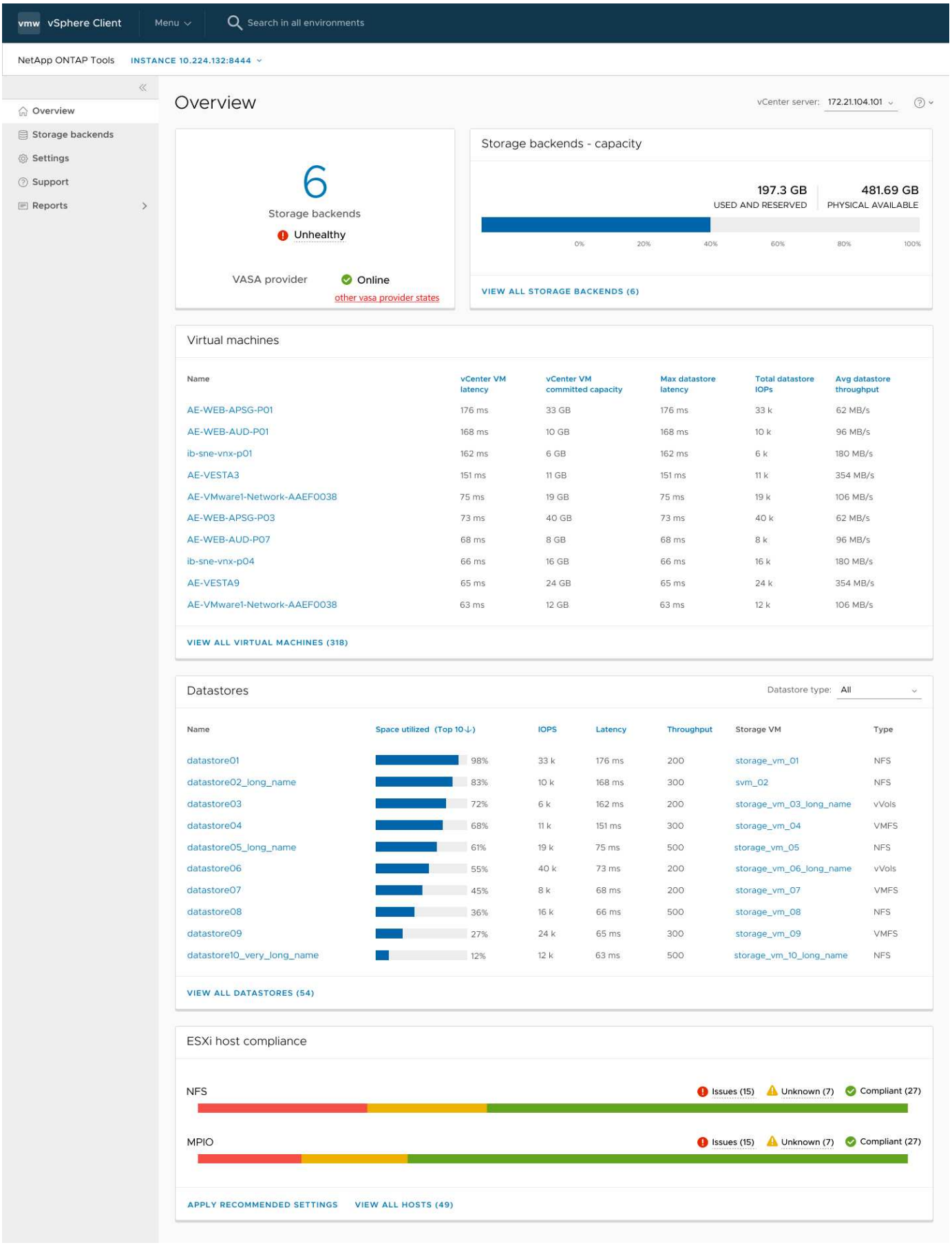
   I sistemi di archiviazione devono essere rilevati nel sito protetto e nel sito di ripristino con lo stato "`abilitato"'.

Gestire gli strumenti ONTAP

Panoramica dei tool NetApp ONTAP per la dashboard dei plug-in VMware vSphere

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 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.



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

diverse schede e ciò che esse rappresentano.

Nome carta	Descrizione
Stato	La scheda Stato mostra il numero di backend storage aggiunti, lo stato di salute generale dei backend storage e lo stato del provider VASA di un vCenter. Lo stato dei backend di archiviazione viene visualizzato come "integro" quando tutti i backend di archiviazione sono normali. Lo stato dei backend di archiviazione viene visualizzato come "non integro" se uno dei backend di archiviazione presenta un problema (stato sconosciuto/irraggiungibile/danneggiato). Quando si fa clic sullo stato "non integro", viene visualizzata una descrizione comandi con lo stato dei backend di archiviazione. Per ulteriori dettagli, è possibile fare clic su qualsiasi backend di storage. Il collegamento altri stati del provider VASA (VP) mostra lo stato corrente del VP 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.
Macchine virtuali	Questa scheda mostra le 10 macchine virtuali principali ordinate in base alla metrica delle prestazioni. È possibile fare clic sull'intestazione per visualizzare 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 primi 10 datastore ordinati in base a una metrica di prestazioni. È possibile fare clic sull'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 fare clic sul collegamento Applica impostazioni consigliate per applicare le impostazioni consigliate. È possibile fare clic su Issues/Unknown per visualizzare l'elenco degli host.

Gestire i datastore

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.

La procedura guidata di creazione dell'archivio dati supporta la creazione di datastore NFS, VMFS e vVols.

- È possibile creare solo datastore VMFS su un cluster protetto. 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 se il cluster host principale è protetto con una relazione del tipo di criterio Automated failover Duplex (Uniform/non-Uniform config).
- È possibile creare un datastore VMFS su un host, solo quando ha una relazione asincrona.

Creare un datastore vVol

Puoi creare un datastore vVol con nuovi volumi o volumi esistenti. Non è possibile creare un datastore vVol con un mix di volumi esistenti e nuovi.

Controllare che gli aggregati root non siano mappati alla SVM.

Prima di iniziare

Assicurarsi che il provider VASA sia registrato con il vCenter selezionato.

Fasi

1. Accedere al client vSphere utilizzando `https://vcenterip/ui`
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 **NetApp ONTAP Tools** > **Create Datastore**.
3. Nel riquadro **tipo**, selezionare vVol in **tipo datastore**.
4. Nel riquadro **Nome e protocollo**, fornire le informazioni **Nome archivio dati** e **protocollo**.
5. Nel riquadro **Storage**, selezionare **Platform** e **Storage VM**. Nella sezione **Opzioni avanzate**, selezionare criterio di esportazione personalizzato (per il protocollo NFS) o nome gruppo iniziatore personalizzato (per il protocollo iSCSI amd FC), a seconda dei casi.
   - Le opzioni relative alla piattaforma e all'asimmetria consentono di filtrare le opzioni a discesa SVM. Devi selezionare la SVM per creare o utilizzare i volumi per la creazione del datastore.
   - Il pulsante di commutazione **asimmetrico** è visibile solo se iSCSI è stato selezionato nella fase precedente e prestazioni o capacità è selezionato nell'elenco a discesa della piattaforma.
   - Selezionare il pulsante di commutazione **asimmetrico** per la piattaforma AFF e disattivarlo per la piattaforma ASA.
6. Nel riquadro **attributi archiviazione** è possibile creare nuovi volumi o utilizzare i volumi esistenti. Durante la creazione di un nuovo volume, puoi abilitare la QoS nel datastore.
7. Controllare la selezione nel riquadro **Riepilogo** e fare clic su **fine**. Il datastore vVols viene creato e montato su tutti gli host.

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 utilizzando `https://vcenterip/ui`
2. Fare clic con il pulsante destro del mouse su un sistema host o un cluster host o un data center e selezionare **NetApp ONTAP tools** > **Create Datastore**.
3. Nel riquadro **tipo**, selezionare NFS in **tipo datastore**.
4. Nel riquadro **Nome e protocollo**, immettere il nome del datastore, le dimensioni e le informazioni sul protocollo. Nelle opzioni avanzate, selezionare **Datastore cluster** e **autenticazione Kerberos**.

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

5. Nel riquadro **Storage**, selezionare **Platform** e **Storage VM**. È possibile selezionare **criterio di esportazione personalizzato** nella sezione **opzione avanzata**.
   - Il pulsante di commutazione **asimmetrico** è visibile solo se nel menu a discesa della piattaforma sono selezionate le prestazioni o la capacità.
   - **Any** (qualsiasi opzione) nel menu a discesa delle piattaforme consente di visualizzare tutte le SVM che fanno parte di vCenter, indipendentemente dalla piattaforma o dal flag asimmetrico.
6. Nel riquadro **attributi archiviazione**, selezionare l'aggregato per la creazione del volume. Nelle opzioni avanzate scegliere **Riserva spazio** e **attiva QoS** come richiesto.
7. Rivedere le selezioni nel riquadro **Riepilogo** e fare clic su **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 appositamente progettato per l'archiviazione dei file delle macchine virtuali negli ambienti VMware vSphere. Consente a più host ESXi di accedere contemporaneamente ai file della stessa macchina virtuale, abilitando funzionalità come vMotion e High Availability.

Prima di iniziare

Prima di procedere, controllare quanto segue:

- Per ogni protocollo dallo storage ONTAP, è necessario abilitare i rispettivi servizi e LIF.
- Se si utilizza il protocollo NVMe/TCP, attenersi alla seguente procedura per configurare l'host ESXi:
  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 sul sito VMware "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 utilizzando `https://vcenterip/ui`
2. Fare clic con il pulsante destro del mouse su un sistema host o un cluster host o un datastore e selezionare **NetApp ONTAP Tools** > **Create Datastore**.
3. Nel riquadro **tipo**, selezionare VMFS in **tipo datastore**.
4. Nel riquadro **Nome e protocollo**, immettere il nome del datastore, le dimensioni e le informazioni sul protocollo. Nella sezione **Opzioni avanzate** del riquadro, selezionare il cluster di datastore a cui si desidera aggiungere il datastore.
5. Selezionare piattaforma e VM di archiviazione nel riquadro **Storage**. Selezionare il pulsante di commutazione asimmetrico. Specificare il nome del gruppo **personalizzato iniziatore** nella sezione **Opzioni avanzate** del riquadro (facoltativo). È possibile scegliere un igroup esistente per l'archivio dati o creare un nuovo igroup con un nome personalizzato.

   Se si sceglie l'opzione **any** nel menu a discesa delle piattaforme, è possibile visualizzare tutte le SVM che fanno parte di vCenter, indipendentemente dalla piattaforma o dal flag asimmetrico. Quando si seleziona il protocollo come NVMe/FC o NVMe/TCP, viene creato un nuovo sottosistema di namespace e utilizzato per la mappatura dei namespace. Per impostazione predefinita, 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** nelle opzioni avanzate del riquadro **Storage**.

6. Nel riquadro **attributi di archiviazione**, selezionare **aggregate** dal menu a discesa. Selezionare le opzioni **riserva di spazio**, **Usa volume esistente** e **attiva QoS** come richiesto nella sezione **Opzioni avanzate** e fornire i dettagli come richiesto.

   Per la creazione di datastore VMFS con i protocolli 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 fare clic su **fine**.

   Se si crea il datastore su un cluster protetto, viene visualizzato un messaggio di sola lettura che informa che il datastore è stato montato su un cluster protetto. Il datastore VMFS viene creato e montato su tutti gli host.

Montare datastore NFS e VMFS

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

- Alcune azioni del pulsante destro del mouse sono disattivate o non disponibili a seconda delle versioni 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 le opzioni sono visualizzate, l'azione sarà disattivata.
- Il datastore mount è disattivato quando il cluster di host è protetto con configurazioni uniformi.

Fasi

1. Dalla home page del client vSphere, fare clic su **host e cluster**.
2. Nel riquadro di navigazione, selezionare il data center che contiene l'host.
3. Ripetere il passaggio 2 per tutti gli host aggiuntivi.
4. Per montare i datastore NFS/VMFS su host o cluster host, fate clic con il pulsante destro del mouse su di esso e selezionate **NetApp ONTAP tools** > **Mount Datastores**.
5. Selezionare gli archivi dati che si desidera montare e fare clic su **Mount**.

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

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 utilizzando `https://vcenterip/ui`
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.

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

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 del client vSphere, fare clic su **host e cluster**.
2. Nel riquadro di navigazione, selezionare il data center che contiene il datastore.
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 fare clic su **Mount**.

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

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 del client vSphere, fare clic su **host e cluster**.
2. Nel riquadro di navigazione, selezionare il data center che contiene il datastore.
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 fare clic su **OK**.

Espandere vVol Datastore

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 sono visualizzati nella sezione del plug-in. Le azioni specifiche vengono attivate in base al tipo di datastore e ai privilegi dell'utente corrente.

Fasi

1. Dalla home page del client vSphere, fare clic su **host e cluster**.
2. Nel riquadro di navigazione, selezionare il data center che contiene il datastore.

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 fare clic su **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.

Fasi

1. Dalla home page del client vSphere, fare clic su **host e cluster**.
2. Nel riquadro di navigazione, selezionare il data center che contiene il datastore.
3. Fare clic con il pulsante destro del mouse sul datastore vVol e selezionare **NetApp ONTAP tools** > **Rimuovi archiviazione dal datastore**.
4. Selezionare i volumi che non dispongono di vVol e fare clic su **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 fai clic su **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 utilizzando `https://vcenterip/ui`
2. Fare clic con il pulsante destro del mouse su un sistema host o su un cluster host o su un datastore e selezionare **NetApp ONTAP tools** > **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. 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.

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

La vista dello storage ONTAP nella scheda Configure dei tool ONTAP per VMware vSphere offre dati relativi ai datastore e al loro volume. Questa vista fornisce la vista laterale dello storage del datastore.

Viste dello storage ONTAP per datastore NFS

Fasi

1. Dal client vSphere, accedere al datastore NFS.
2. Fare clic sulla scheda **Configura** nel riquadro di destra.
3. Selezionare **NetApp ONTAP tools** > **archiviazione ONTAP**. Nel riquadro destro vengono visualizzati i dettagli **Storage details** e **NFS details**.
   - Questa pagina contiene informazioni sui backend, gli aggregati e i volumi di storage.
   - La pagina dei dettagli di NFS contiene dati correlati al datastore NFS.

Viste dello storage ONTAP per datastore VMFS

Fasi

1. Dal client vSphere, accedere al datastore VMFS.
2. Fare clic sulla scheda **Configura** nel riquadro di destra.
3. Selezionare **NetApp ONTAP tools** > **archiviazione ONTAP**. Nel riquadro destro vengono visualizzati i dettagli **Storage details** e **LUN details** o **namespace details** in caso di protocollo NVMe/TCP o NVMe/FC.
   - Questa pagina contiene informazioni sui backend, gli aggregati e i volumi di storage.
   - La pagina dei dettagli LUN contiene i dati correlati al LUN.
   - Quando si utilizza il protocollo NVMe/TCP o NVMe/FC per il datastore VMFS, la pagina dei dettagli del namespace contiene dati correlati al namespace.

Viste dello storage ONTAP per i datastore vVol

Fasi

1. Dal client vSphere, accedere al datastore vVols.
2. Fare clic sulla scheda **Configura** nel riquadro di destra.
3. Selezionare **NetApp ONTAP tools** > **archiviazione ONTAP**.
4. La vista dello storage ONTAP elenca tutti i volumi. È possibile espandere o rimuovere lo spazio di archiviazione dal riquadro di archiviazione di ONTAP.

   Seguire le istruzioni nella "Espandere vVol Datastore" sezione per aggiungere il datastore vVol e "Restringere il datastore vVol" la sezione per eliminare il datastore.

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. Fare clic sulla 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 utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **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 fare clic su 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 utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **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. Fare clic sul menu ellissi verticali e selezionare **Ricerca 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 utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **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. Fare clic sul 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://loadBalanceIP: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. Fare clic sul 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 utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **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. Fare clic sul 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://loadBalanceIP: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. Fare clic sul menu ellissi verticali e selezionare **Rimuovi**.

Drill-down del backend dello storage

La pagina del backend di archiviazione elenca tutti i backend di archiviazione. È possibile eseguire operazioni di rilevamento dello storage, modifica e rimozione sui backend dello storage aggiunti, non su un singolo figlio sotto il cluster.

Facendo clic sul cluster padre o su quello figlio nel back-end dello storage è possibile visualizzare il riepilogo generale del componente. Facendo clic sul cluster padre, è disponibile il menu a discesa delle azioni da cui è possibile eseguire le operazioni di rilevamento, modifica e rimozione. Questa opzione non è disponibile quando si fa clic su SVM figlio.

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 scheda Interface (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.

Associare o 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 ha la possibilità di associare o disassociare un backend dello storage. Questo task ti aiuta a creare la mappatura tra il back-end dello storage e l'istanza vCenter Server integrata a livello globale.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
   `https://loadBalanceIP: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. Fare clic sulle ellissi verticali su vCenter Server che si desidera associare o dissociare dai backend di storage.
5. Selezionare **Associa o dissocia backend archiviazione** a seconda dell'azione che si desidera eseguire.

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://loadBalanceIP: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. Fare clic sulle ellissi verticali su 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://loadBalanceIP: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. Fare clic sulle ellissi verticali su 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

Una singola istanza dei tool ONTAP per VMware vSphere può gestire più istanze di vCenter Server. 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 abilitare la funzionalità vVol su più istanze di vCenter Server, è necessario modificare il certificato autofirmato in certificato CA personalizzato utilizzando l'interfaccia di ONTAP Tools Manager. È possibile utilizzare la stessa interfaccia per rinnovare o aggiornare tutti i certificati.

Un diverso indirizzo IP del sistema di bilanciamento del carico mappato a domini diversi non è supportato quando si esegue l'aggiornamento della CA autofirmata alla CA personalizzata.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
   `https://loadBalanceIP: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** > **provider VASA** > **Rinnova** per rinnovare i certificati.

   Il sistema non sarà in linea fino a quando il certificato non sarà rinnovato.

4. Per aggiornare il certificato autofirmato al certificato CA personalizzato, selezionare l'opzione **certificati** > **provider VASA** > **Aggiorna a CA**.
   a. Nella finestra a comparsa **Aggiorna certificato alla CA** personalizzata, caricare il certificato del server, la chiave privata del certificato del server, il certificato della CA principale e i file di certificato intermedio. La descrizione dei certificati viene fornita nella descrizione.
   b. Immettere il nome di dominio per il quale è stato generato il certificato.
   c. Fare clic su **Upgrade** (Aggiorna).

      Il sistema non sarà in linea fino al completamento dell'aggiornamento.

Gestire gli igroup e i criteri di esportazione

In ONTAP, le policy di esportazione vengono utilizzate per fornire l'accesso al percorso dei dati del volume agli host, mentre gli igroup (Initiator group) vengono utilizzati per fornire l'accesso al percorso dei dati LUN (Logical Unit Number) agli host ESXi. Gli strumenti ONTAP per VMware vSphere rendono semplice e intuitiva la creazione di igroup e offrono flussi di lavoro end-to-end completi. Per garantire la coerenza, la creazione diretta di iGroup sulle piattaforme di storage non è supportata.

Quando i datastore di volumi virtuali vengono creati o montati sugli host in vCenter Server, gli host devono poter accedere ai volumi (NFS) o alle LUN (iSCSI), a seconda del tipo di protocollo del datastore.

Il criterio di esportazione è dinamico e il nuovo criterio di esportazione viene creato con il formato di denominazione trident-uid. In Gestione sistema di ONTAP, accedere a **archiviazione** > **VM di archiviazione** > **[nome VM di archiviazione]** > **Impostazioni** > **Criteri di esportazione** per visualizzare i criteri di esportazione.

Gli igroup e le policy di esportazione degli strumenti ONTAP per VMware vSphere sono gestiti in modo efficiente e offrono i seguenti vantaggi:

- Supporta i criteri di esportazione migrati e gli igroup.
- Nessuna interruzione delle operazioni di input e output della macchina virtuale.
- Supporta il montaggio su host aggiuntivi senza intervento manuale.
- Riduce al minimo la necessità di gestire il numero di igroup e le policy di esportazione.
- Un Garbage Collector elimina automaticamente tutti gli igroup gestiti non utilizzati e i criteri di esportazione periodicamente.
- Se il provisioning di un datastore a livello del cluster host viene eseguito, igroup viene creato con tutti gli initiator dell'host nel cluster host che vengono aggiunti all'igroup.

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 fa clic su  , viene avviata la console di manutenzione.

Menu console	Opzioni

Configurazione dell'applicazione	1. Visualizza il riepilogo dello stato del server 2. Modificare il livello di REGISTRAZIONE per servizi provider VASA e servizi SRA 3. Disattiva AutoSupport
Configurazione del sistema	1. Riavviare la macchina virtuale 2. Arrestare la macchina virtuale 3. Modificare la password utente "maint" 4. Modificare il fuso orario 5. Aggiungere un nuovo server NTP 6. Aumentare la dimensione del disco jail (/jail) 7. Eseguire l'upgrade 8. Installare VMware Tools
Configurazione di rete	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	1. Accedere alla shell di diagnostica 2. Abilitare l'accesso remoto alla diagnostica

Configurare l'accesso remoto alla diagnostica

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

Cosa ti serve

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. Da vCenter Server, aprire una console al 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.

Cosa ti serve

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. Da vCenter Server, aprire una console al 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.

Cosa ti serve

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. Da vCenter Server, aprire una console al 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://loadBalanceIP: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 utilizzando `https://vcenterip/ui`
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 necessario tenere presenti alcune considerazioni durante la 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.

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.

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.

Cosa ti serve

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 che si desidera migrare e fare clic su **Migra**.
2. Selezionare **Cambia solo memoria**, quindi fare clic su **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. Fare clic su **Avanti**.
4. Controllare le impostazioni e fare clic su **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.

Cosa ti serve

- 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 data center desiderato e selezionare **NetApp ONTAP tools** > **Update host Data** (Strumenti * > Aggiorna dati host).

   Gli strumenti ONTAP per VMware vSphere visualizzano una finestra di dialogo **Conferma** con il seguente messaggio:

   "Questa azione riavvierà il rilevamento di tutti i sistemi di archiviazione connessi e potrebbe richiedere alcuni minuti. Vuoi continuare?"

3. Fare clic su **Sì**.
4. Selezionare i controller di archiviazione rilevati che hanno lo stato `Authentication Failure` e fare clic su **azioni** > **Modifica**.
5. Inserire le informazioni richieste nella finestra di dialogo **Modify Storage System** (Modifica sistema di storage).
6. 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 Avviso nella colonna Impostazioni adattatore, Impostazioni MPIO o 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.

Cosa ti serve

Se si verifica un problema con le impostazioni dell'host ESXi, il problema viene visualizzato nel portlet dei sistemi host ESXi della dashboard. Fare clic sul problema per visualizzare il nome host o l'indirizzo IP dell'host ESXi che ha il problema.

Fasi

1. Accedere al client vSphere utilizzando `https://vcenterip/ui`
2. Nella pagina dei collegamenti, fare clic su **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 fare clic su **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 riquadro di riepilogo, controllare i valori e fare clic su **fine**. È possibile tenere traccia dell'avanzamento nel riquadro attività recenti.

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://loadBalanceIP:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Fare clic sull'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 UI.

5. Fare clic su **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://loadBalanceIP: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. .. Da vCenter Server, aprire la console di manutenzione .. Immettere '2' per selezionare l'opzione Configurazione di sistema .. 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. Fare clic su **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 dei provider SRA e VASA con vCenter Server.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web: `https://loadBalanceIP:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Fare clic su **Impostazioni** dalla barra laterale.
4. Nella schermata **credenziali utente applicazione**, selezionare **Reimposta password**.
5. Fornire nome utente, nuova password e confermare l'immissione della nuova password.
6. Fare clic su **Reimposta** per implementare le modifiche.

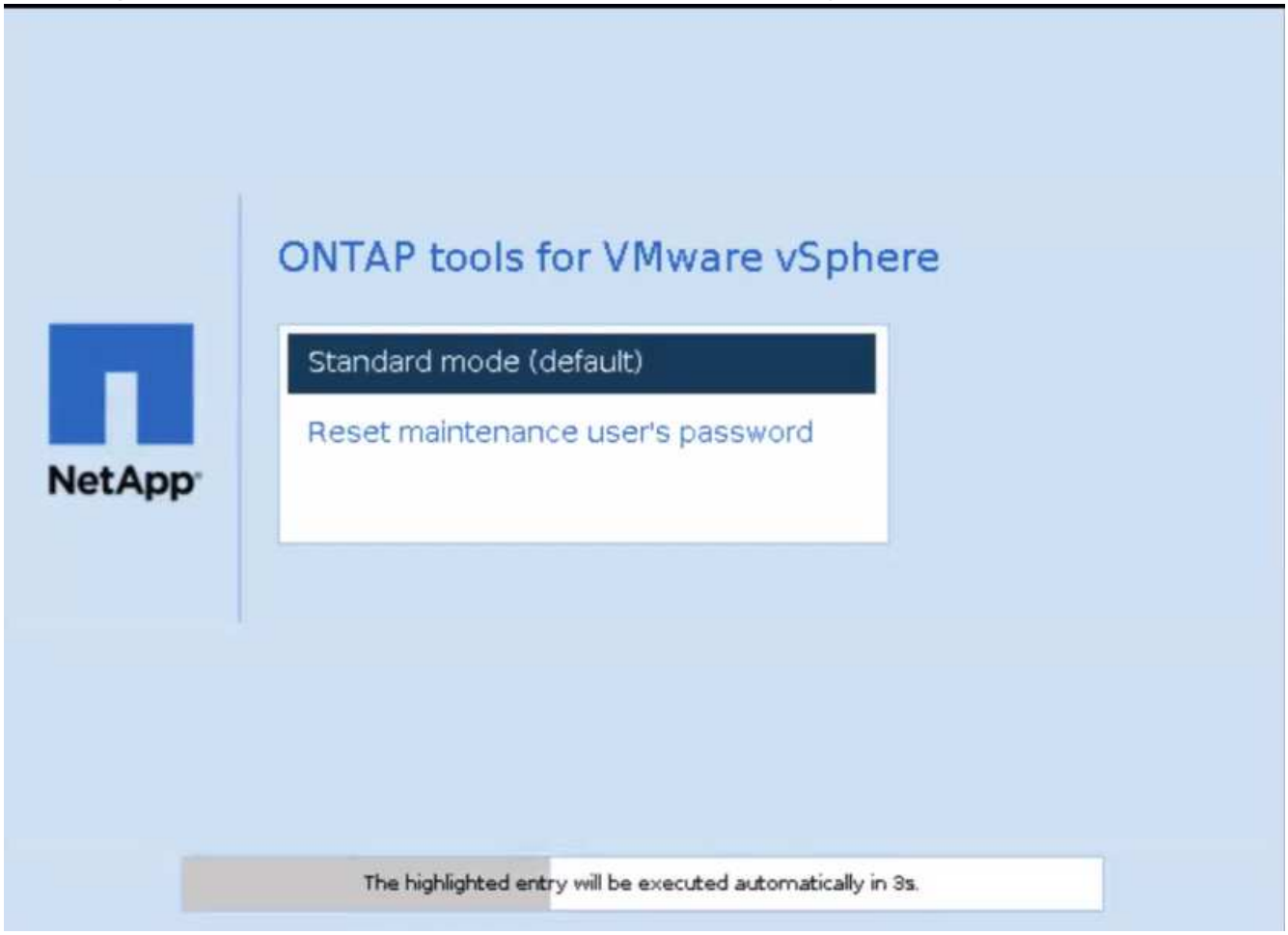
Reimpostare la password utente della console di manutenzione

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.

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**.

Pulire i volumi

Dopo aver eliminato gli strumenti ONTAP per la distribuzione di VMware vSphere, è necessario ripulire i volumi flessibili creati durante la distribuzione. Se hai utilizzato un cluster ONTAP dedicato per le implementazioni, dovresti pulire quei volumi perché l'implementazione crea molti volumi complessi, che non sono utilizzati, con un conseguente calo delle performance.

Utilizzare le seguenti linee guida per ripulire i dispositivi FlexVolumes dopo la rimozione degli strumenti ONTAP per la distribuzione di VMware vSphere.

Fasi

1. Dalla macchina virtuale del nodo principale dei tool ONTAP per VMware vSphere, esegui il seguente comando per identificare il tipo di implementazione.

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

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

2. Recuperare l'elenco di FlexVolumes creati in ONTAP durante la distribuzione utilizzando il seguente comando.

   Kubectl describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'

3. Eliminazione di macchine virtuali da vCenter Server, vedere "Rimozione di macchine virtuali o modelli di macchine virtuali da vCenter Server o dal datastore"
4. Eliminare volumi da Gestione di sistema ONTAP, vedere "Eliminare un volume FlexVol". Fornire il nome esatto di FlexVolume nel comando cli per eliminare il volume.
5. In caso di distribuzione iSCSI, eliminare gli igroup SAN da ONTAP, vedere "Visualizza e gestisci GLI iniziatori SAN e igroups".

   Nell'implementazione ha, vengono creati quattro igroup e, nell'implementazione non ha, vengono creati due igroup. Eseguire il seguente comando per trovare il primo nome igroup:

   Kubectl -n tridente get tbc tridente-backend -o yaml| grep igroupName: | awk -F':' '{print $2}'

   Gli altri nomi igroup iniziano con il nome host della VM.

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.

- Aggiungi nuovi datastore o host al cluster protetto.
- Aggiungere nuove relazioni SnapMirror alle impostazioni di protezione.
- Elimina le relazioni SnapMirror esistenti dalle impostazioni di protezione.
- Modificare una relazione SnapMirror esistente.

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 utilizzando `https://vcenterip/ui`
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 utilizzando `https://vcenterip/ui`
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**, fare clic sul menu kebab 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 kebab 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. Fare clic su **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 utilizzando `https://vcenterip/ui`
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**, fare clic sul menu kebab 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. Fare clic su **Protect** (protezione).
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**.

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 utilizzando `https://vcenterip/ui`
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**, fare clic sul menu kebab 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 kebab 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 utilizzando `https://vcenterip/ui`
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**, fare clic sul menu kebab 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 **host cluster Protection**, fare clic sul menu kebab sul cluster, quindi selezionare **Rimuovi protezione**.

Aggiornare i tool ONTAP

Aggiornamento dai tool ONTAP per VMware vSphere 10.x alla 10,2

L'aggiornamento è supportato per le implementazioni ha e non ha.

> Per eseguire l'upgrade dai tool ONTAP per VMware vSphere 10,0 alla release 10,2, è necessario prima eseguire l'upgrade ai tool ONTAP per VMware vSphere 10,1, quindi alla release 10,2.

Prima di iniziare

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, aprite 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 di diagnostica remota.
5. Immettere **y** per impostare la password desiderata.
6. Accedere all'indirizzo IP della VM dal terminale/putty con l'utente come 'diag' e la password impostata nel passaggio precedente.

Esegui il 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.
- Env | grep MONGODB_ROOT_PASSWORD - esegui questo comando all'interno del pod.
- 'esci' - eseguire questa operazione per uscire dal pod.
- KN exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip - esegui questo comando per sostituire MONGO_ROOT_PASSWORD set dal comando precedente.
- kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz - eseguire questo comando per copiare il backup mongodb creato utilizzando il comando sopra riportato da pod all'host.

Acquisire l'istantanea 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 aprire il volume facendo clic sul nome. Andare allo snapshot e aggiungere lo snapshot di

quel volume.

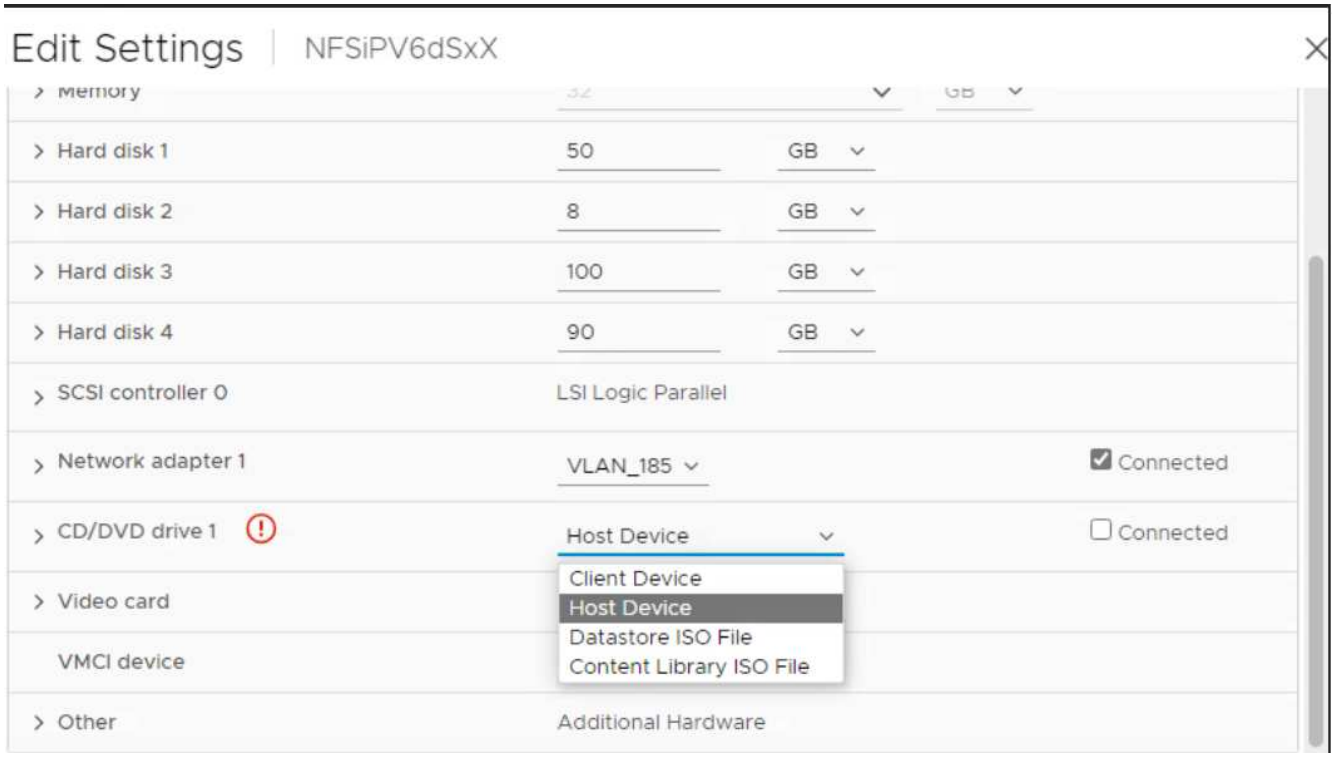
Istantanea degli strumenti ONTAP per le VM VMware vSphere in vCenter (3VMs in caso di implementazione ha, 1 VM in caso di distribuzione non ha)

- Nell'interfaccia utente del client vSphere, selezionare la VM.
- Andare alla scheda istantanee e fare clic sul pulsante **scatta istantanea**.

Prima di eseguire l'aggiornamento, eliminare i pod completati 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.

Fasi

1. Carica gli strumenti ONTAP per l'aggiornamento ISO di VMware vSphere nella libreria di contenuti.
2. Nella pagina principale della macchina virtuale, selezionare **azioni** > **Modifica impostazioni**
3. Nella finestra di modifica delle impostazioni sotto il campo **unità CD/DVD**, selezionare file ISO della libreria di contenuti.
4. Selezionare il file ISO e fare clic su **OK**. Selezionare la casella di controllo connesso nel campo **unità CD/DVD**.



5. Da vCenter Server, aprite 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

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 tb, 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

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
063	La copia dei contenuti nel volume di ripristino non è riuscita	Eseguire un ripristino basato su snapshot.
068	Il rollback dei pacchetti Debian non è riuscito	Eseguire un ripristino basato su snapshot.
069	Ripristino dei file non riuscito	Eseguire un ripristino basato su snapshot.
070	Impossibile eliminare il backup	Eseguire un ripristino basato su snapshot.
071	Il cluster Kubernetes non era integro	Eseguire un ripristino basato su snapshot.
072	Il file CR non esiste nel disco jail	Eseguire un ripristino basato su snapshot.

073	Applicazione CR non riuscita durante l'impostazione del flag di riconciliazione forzata su false	Eseguire un ripristino basato su snapshot.
074	Montaggio ISO non riuscito	Riprovare a eseguire l'aggiornamento.
075	I controlli preliminari dell'aggiornamento non sono riusciti	Riprovare a eseguire l'aggiornamento.
076	Aggiornamento del Registro di sistema non riuscito	Eseguire un ripristino basato su snapshot.
077	Ripristino del Registro di sistema non riuscito	Eseguire un ripristino basato su snapshot.
078	Aggiornamento dell'operatore non riuscito	Eseguire un ripristino basato su snapshot.
079	Il richiamo dell'operatore non è riuscito	Eseguire un ripristino basato su snapshot.
080	Aggiornamento servizi non riuscito	Eseguire un ripristino basato su snapshot.
081	Ripristino servizi non riuscito	Eseguire un ripristino basato su snapshot.
082	Eliminazione delle vecchie immagini dal contenitore non riuscita	Eseguire un ripristino basato su snapshot.
083	Eliminazione backup non riuscita	Eseguire un ripristino basato su snapshot.
084	La modifica di JobManager in produzione non è riuscita	Eseguire un ripristino basato su snapshot.
085	Impossibile creare i segreti del certificato CA	Eseguire un ripristino basato su snapshot.
086	impossibile creare i segreti del certificato server/chiave privata	Eseguire un ripristino basato su snapshot.
087	Impossibile completare i passaggi di aggiornamento da 10,0 a 10,1 post	Procedura di post-aggiornamento non riuscita.
088	La configurazione della rotazione del registro per il giornale non è riuscita	Riprovare a eseguire l'aggiornamento.
089	La modifica della proprietà del file di configurazione rotazione del registro di riepilogo non è riuscita	Riprovare a eseguire l'aggiornamento.
091	Aggiornamento iSCSI non riuscito	Riprovare a eseguire l'aggiornamento.

092	Rollback iSCSI non riuscito	Riprovare a eseguire l'aggiornamento.
093	aggiornamento Trident non riuscito	Riprovare a eseguire l'aggiornamento.
094	ripristino Trident non riuscito	Riprovare a eseguire l'aggiornamento.
095	Aggiornamento Debian non riuscito	Nessun recupero per l'aggiornamento debian. I servizi vengono aggiornati e saranno in esecuzione nuovi pod

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

Ripristino degli strumenti ONTAP

Ripristina i tool ONTAP per la configurazione di VMware vSphere

In caso di perdita dei tool ONTAP per la configurazione di VMware vSphere, sarà possibile ripristinare i tool ONTAP per la configurazione di VMware vSphere utilizzando i dati disponibili nel volume ONTAP. Quando si perde la configurazione, abbassare la configurazione senza problemi.

Non puoi ripristinare i tool ONTAP per la configurazione di VMware vSphere in caso di problemi con vCenter Server o il software di gestione dei dati ONTAP.

Fasi

1. Accedere al server vSphere.
2. Passare al pool di risorse creato o al cluster di nodi o all'host in cui si desidera distribuire l'OVA.
3. Fare clic con il pulsante destro del mouse sulla posizione desiderata e selezionare **Deploy OVF template** (distribuire modello OVF*).
4. Selezionare il file OVA tramite l'URL per il file *.ova* o navigare alla cartella in cui è stato salvato il file *.ova*, quindi fare clic su **Avanti**.

   È necessario utilizzare la stessa build OVA utilizzata per l'installazione della configurazione di ripristino.

5. Selezionare un nome e una cartella per la macchina virtuale e selezionare **Avanti**.
6. Selezionare l'host e selezionare **Avanti**.
7. Rivedere il riepilogo del modello e selezionare **Avanti**.
8. Leggere e accettare il contratto di licenza e selezionare **Avanti**.
9. Nella finestra **Configurazione**, selezionare l'opzione **Ripristino**.
10. Nella finestra **Seleziona archiviazione**, selezionare lo spazio di archiviazione per le configurazioni e i file del disco.
11. Nella finestra **Seleziona reti**, selezionare una rete di destinazione per ciascuna rete di origine.

    Devi mantenere l'indirizzo IP del bilanciatore del carico e l'indirizzo IP del Kubernetes API Server. È possibile modificare l'indirizzo IP del nodo oppure mantenere lo stesso indirizzo IP.

12. Nella finestra **Personalizza modello**, immettere i dettagli richiesti e fare clic su **Avanti**

    Una volta abilitato l'ambito SVM, dovresti aver già abilitato il supporto SVM con l'indirizzo IP di gestione.

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.

    L'installazione viene avviata. È possibile tenere traccia dell'avanzamento dell'installazione nella console Web della VM. Come parte dell'installazione, le configurazioni dei nodi sono validate. Gli input forniti nelle diverse sezioni del modello Personalizza nel modulo OVF vengono convalidati. In caso di discrepanze, viene visualizzata una finestra di dialogo che richiede di intraprendere un'azione correttiva.

15. Apportare le modifiche necessarie nella finestra di dialogo. Utilizzare il pulsante Tab per spostarsi all'interno del pannello e selezionare **OK**.

    I valori forniti vengono nuovamente convalidati. Gli strumenti ONTAP per VMware vSphere consentono di correggere tre tentativi di valori non validi. Se dopo tre tentativi non è possibile risolvere i problemi, l'installazione del prodotto si interrompe e si consiglia di provare a eseguire l'installazione su una nuova VM.

Una volta completata l'installazione, la console Web mostra lo stato degli strumenti ONTAP per VMware vSphere.

Una volta completata l'installazione, è necessario modificare manualmente i requisiti hardware in base alle linee guida riportate nella "Prerequisiti per la distribuzione degli strumenti ONTAP per VMware vSphere" pagina.

Strumenti ONTAP per la migrazione

Migrazione dai tool ONTAP per VMware vSphere 9.x a 10,2

Durante la migrazione dei dati di storage, i backend di storage vengono inseriti manualmente utilizzando le API REST. Durante la migrazione dei dati dei provider VASA, i dati vengono esportati dal database Derby esistente e importati nel database MongoDB.

Si consiglia di eseguire la migrazione dei tool ONTAP per il setup di VMware vSphere 9.x solo se il setup utilizza solo la funzione del provider VASA.

Dopo la migrazione da tool ONTAP per VMware vSphere 9.x a 10,2, i datastore vVol con protocollo NVMe/FC non funzionano perché gli strumenti ONTAP 10,2 supportano solo NVMe-of con datastore VMFS.

A proposito di questa attività

La migrazione è supportata dai tool ONTAP per le versioni VMware vSphere 9.10D2, 9.11D4, 9.12D1 e 9.13D2 alla versione 10,2.

Se si utilizzano strumenti ONTAP per VMware vSphere 9.13P1, è necessario eseguire l'aggiornamento a 9.13D2 prima della migrazione alla versione 10,2.

Come utente esistente, è necessario eseguire il backup OVA dalla versione corrente prima di eseguire l'aggiornamento alle versioni delle patch.

Passaggi comuni di migrazione

1. Distribuzione di OVA per strumenti ONTAP per VMware vSphere 10,2.
2. Aggiungere l'istanza di vCenter Server che si desidera migrare agli strumenti ONTAP per VMware vSphere 10,2. Vedere "Aggiungere istanze di vCenter Server"
3. Back-end dello storage integrato a livello locale dai tool ONTAP per le API del server vCenter del plug-in VMware vSphere. Aggiungere storage come storage per la migrazione a livello locale.
4. I datastore NFS e VMFS migrati dai tool ONTAP per VMware vSphere 9.xx sono visibili nei tool ONTAP per VMware vSphere 10,2 solo dopo l'attivazione del processo di rilevamento del datastore, che potrebbe richiedere fino a 30 minuti per l'attivazione. Verificare se gli archivi dati sono visibili nella pagina Panoramica della pagina dell'interfaccia utente degli strumenti di ONTAP per VMware vSphere Plugin.

Fasi di migrazione SRA

Prima di iniziare

Prima di eseguire la migrazione, assicurarsi che uno dei siti sia in uno stato protetto e l'altro sia in uno stato di recupero.

Non eseguire la migrazione se il failover è stato appena completato e la funzione di protezione è in sospeso. Completare la protezione e quindi eseguire la migrazione. Lo stesso vale per la verifica del piano di ripristino. Una volta completato il test del piano di ripristino, ripulire il ripristino di prova e avviare la migrazione.

1. Per eliminare gli strumenti ONTAP per VMware vSphere 9.xx release SRA adapter in VMware Live Site Recovery UI, attenersi alla seguente procedura:
   a. Accedere alla pagina di gestione della configurazione di VMware Live Site Recovery
   b. Consultare la sezione Storage Replication Adapter
   c. Fare clic sul menu Kebab, quindi su **Reimposta configurazione**
   d. Fare clic sul menu Kebab e selezionare **Elimina**

   Eseguire queste operazioni sui siti di protezione e ripristino.
2. Installare i tool ONTAP per l'adattatore SRA VMware vSphere 10,2 sui siti di protezione e ripristino seguendo i passaggi descritti in "Configurare SRA sull'appliance VMware Live Site Recovery"
3. Nella pagina dell'interfaccia utente di VMware Live Site Recovery, eseguire le operazioni **Discover Arrays** e **Discover Devices** e verificare che i dispositivi siano visualizzati come prima della migrazione.

Fasi di migrazione del provider VASA

1. Abilitare la PORTA Derby 1527 sugli strumenti ONTAP esistenti per VMware vSphere. Per attivare la porta, accedere alla CLI con l'utente root ed eseguire il seguente comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Distribuzione di OVA per strumenti ONTAP per VMware vSphere 10,2.
3. Aggiungere l'istanza di vCenter Server che si desidera migrare agli strumenti ONTAP per VMware vSphere 10,2. Vedere "Aggiungere un'istanza di vCenter Server".
4. Back-end dello storage integrato in locale dalle API del server vCenter del plug-in remoto. Aggiungi storage come ambito locale per la migrazione.
5. Eseguire la seguente chiamata API per la migrazione:

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

/api/v1/vcenter/{vcguid}/migration-jobs

Esempio di input JSON corpo di richiesta per la migrazione da 9,12 e 9,13:

{ "otv_ip": "10.12.13.45", "vasa_provider_credits": { "username": "vasauser", "password": **"" } "database_password": ""** }

Corpo della richiesta per un'altra migrazione delle release:

{ "otv_ip": "10.12.13.45", "vasa_provider_credits": { "username": "vasauser", "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 per controllare lo stato:

```
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true
```

   Una volta completato il processo, convalidare il rapporto di migrazione. È possibile visualizzare il rapporto dalla risposta al lavoro come parte di JobData.

7. Aggiungi i tool ONTAP per lo storage provider di VMware vSphere a vCenter Server e "Registrare il provider VASA su vCenter Server".
8. Stop ONTAP tools for VMware vSphere storage provider 9,10/9,11/9,12/9,13 VASA Provider service 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.

9. Eseguire la migrazione delle patch utilizzando la seguente API:

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 "/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/Migration-jobs/84dr73bd-9173-65r7-w345-8ufdb87d43

Esempio di input JSON

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

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 nella risposta dell'API post-migrazione.

Una volta completata con successo l'API di migrazione delle patch, tutte le VM saranno conformi alla policy di storage.

10. L'API di eliminazione per la migrazione è:

Metodo HTTP	Percorso
ELIMINARE	/api/v1

Tipo di lavorazione

Asincrono

Esempio Curl

/api/v1/vcenter/{vcguid}/migration-jobs/{migration_id}

Questa API elimina la migrazione tramite ID migrazione ed elimina la migrazione su vCenter Server specificato.

Dopo aver eseguito correttamente la migrazione e aver registrato gli strumenti ONTAP 10,2 in vCenter Server, procedere come segue:

- Aggiornare il certificato su tutti gli host.
- Attendere qualche istante prima di eseguire le operazioni di DataStore (DS) e Virtual Machine (VM). Il tempo di attesa dipende dal numero di host, DS e VM presenti nell'installazione. Quando non si attende, le operazioni potrebbero non riuscire in modo intermittente.

Automatizzare utilizzando le API REST

Panoramica delle API REST

Le API REST possono essere utilizzate per eseguire diversi tool ONTAP per le operazioni di gestione di VMware vSphere. Le API REST sono esposte attraverso la pagina web di Swagger.

È possibile accedere alla pagina Web Swagger disponibile su *https://loadbalancerIP:8443/* per visualizzare la documentazione dell'API REST e per eseguire manualmente una chiamata API.

Tutte le API hanno un corpo di richiesta ed esempi menzionati nella pagina swagger. I flussi di lavoro e gli esempi forniti in questa sezione sono solo a scopo di riferimento.

Come accedere ai tool ONTAP per l'API REST di VMware vSphere

È possibile accedere all'API REST di ONTAP in diversi modi.

Considerazioni sulla rete

È possibile connettersi all'API REST tramite le seguenti interfacce:

- LIF gestione cluster
- LIF di gestione dei nodi
- LIF gestione SVM

La LIF che scegli di utilizzare deve essere configurata in modo da supportare il protocollo di gestione HTTPS. Inoltre, la configurazione del firewall nella rete dovrebbe consentire il traffico HTTPS.

Si consiglia di utilizzare sempre una LIF di gestione del cluster. In questo modo, le richieste API vengono bilanciate in tutti i nodi ed è possibile evitare i nodi offline o che presentano problemi di connettività. Se sono configurate più LIF di gestione del cluster, sono tutte equivalenti per quanto riguarda l'accesso all'API REST.

Pagina della documentazione online dei tool ONTAP per l'API VMware vSphere

È possibile accedere a Swagger dal collegamento ipertestuale nella pagina di supporto dei tool NetApp ONTAP per il plug-in VMware vSphere.

Il formato dell'URL utilizzato per accedere alla pagina della documentazione relativa alla versione più recente dell'API è:

`https://<loadbalancer_ip_address>/docs/api'

Software e tool personalizzati

Puoi accedere ai tool ONTAP per le API VMware vSphere utilizzando diversi linguaggi e tool di programmazione. Le scelte più popolari includono Python, Java, Curl e PowerShell. Un programma, uno script o uno strumento che utilizza l'API agisce come un client di servizi Web REST. L'utilizzo di un linguaggio di programmazione consente una conoscenza più approfondita dell'API e offre l'opportunità di automatizzare gli

strumenti ONTAP per l'amministrazione di VMware vSphere.

Il formato dell'URL di base utilizzato per accedere direttamente alla versione più recente dell'API è:

`https://<loadbalancer_ip_address>/api'

Per accedere a una versione API specifica in cui sono supportate più versioni, il formato dell'URL è:

`https://<loadbalancer_ip_address>/api/v1'

Accedi ai tool ONTAP per la documentazione di riferimento dell'API VMware vSphere tramite l'interfaccia utente Swagger

È possibile accedere alla documentazione dell'API REST ONTAP tramite l'interfaccia utente Swagger nel sistema ONTAP locale.

Prima di iniziare

Dovresti disporre di quanto segue:

- Indirizzo IP o nome host della LIF di gestione del cluster ONTAP
- Nome utente e password per un account con autorizzazione ad accedere all'API REST ONTAP

Fasi

1. Digitare l'URL nel browser e premere **Invio**: *https://<ip_address>/docs/api*
2. Accedi utilizzando l'account ONTAP

   Viene visualizzata la pagina della documentazione API ONTAP con le chiamate API organizzate in base alle principali categorie di risorse.

3. Come esempio di una singola chiamata API, scorrere verso il basso fino alla categoria **cluster** e fare clic su **GET /cluster**.

Inizia con L'API REST

Puoi iniziare rapidamente a utilizzare i tool ONTAP per le API REST di VMware vSphere. L'accesso all'API offre una prospettiva prima di iniziare a utilizzarla con i processi di workflow più complessi in un setup live.

Ciao mondo

Puoi eseguire un semplice comando sul tuo sistema per iniziare a utilizzare i tool di ONTAP per l'API REST di VMware vSphere e verificarne la disponibilità.

Prima di iniziare

- Assicurarsi che l'utility Curl sia disponibile sul sistema.
- Indirizzo IP o nome host degli strumenti ONTAP per il server VMware vSphere
- Nome utente e password per un account con autorizzazione ad accedere agli strumenti ONTAP per l'API REST VMware vSphere.

Se le credenziali includono caratteri speciali, è necessario formattarle in modo accettabile per Curl in base alla shell in uso. Ad esempio, è possibile inserire una barra rovesciata prima di ogni carattere speciale o racchiudere l'intera stringa tra virgolette `username:password` singole.

Fase

Nell'interfaccia della riga di comando, eseguire quanto segue per recuperare le informazioni del plug-in:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Esempio:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

Come accedere ai tool ONTAP per l'API REST di VMware vSphere

È possibile accedere all'API REST di ONTAP in diversi modi.

Considerazioni sulla rete

È possibile connettersi all'API REST tramite le seguenti interfacce:

- LIF gestione cluster
- LIF di gestione dei nodi
- LIF gestione SVM

La LIF che scegli di utilizzare deve essere configurata in modo da supportare il protocollo di gestione HTTPS. Inoltre, la configurazione del firewall nella rete dovrebbe consentire il traffico HTTPS.

Si consiglia di utilizzare sempre una LIF di gestione del cluster. In questo modo, le richieste API vengono bilanciate in tutti i nodi ed è possibile evitare i nodi offline o che presentano problemi di connettività. Se sono configurate più LIF di gestione del cluster, sono tutte equivalenti per quanto riguarda l'accesso all'API REST.

Variabili di input che controllano una richiesta API

È possibile controllare la modalità di elaborazione di una chiamata API attraverso parametri e variabili impostati nella richiesta HTTP.

Metodi HTTP

I metodi HTTP supportati dai tool ONTAP per l'API REST VMware vSphere sono illustrati nella tabella seguente.

Non tutti i metodi HTTP sono disponibili in ogni endpoint REST.

Metodo HTTP	Descrizione
OTTIENI	Recupera le proprietà dell'oggetto su un'istanza o una raccolta di risorse.
POST	Crea una nuova istanza di risorsa in base all'input fornito.
ELIMINARE	Elimina un'istanza di risorsa esistente.
IN PRIMO PIANO	Modifica un'istanza di risorsa esistente.

Intestazioni delle richieste

È necessario includere diverse intestazioni nella richiesta HTTP.

Tipo di contenuto

Se il corpo della richiesta include JSON, questa intestazione deve essere impostata su *application/json*.

Accettare

Questa intestazione deve essere impostata su *application/json*.

Autorizzazione

L'autenticazione di base deve essere impostata con il nome utente e la password codificati come una stringa base64.

Corpo della richiesta

Il contenuto del corpo della richiesta varia in base alla chiamata specifica. Il corpo della richiesta HTTP è costituito da uno dei seguenti elementi:

- Oggetto JSON con variabili di input
- Vuoto

Filtraggio degli oggetti

Quando si esegue una chiamata API che utilizza GET, è possibile limitare o filtrare gli oggetti restituiti in base a qualsiasi attributo. Ad esempio, è possibile specificare un valore esatto da associare:

```
<field>=<query value>
```

Oltre a una corrispondenza esatta, sono disponibili altri operatori per restituire un set di oggetti su un intervallo di valori. Gli strumenti ONTAP per l'API REST di VMware vSphere supportano gli operatori di filtraggio illustrati nella tabella seguente.

Operatore	Descrizione
=	Uguale a.
<	Inferiore a.
>	Maggiore di

Operatore	Descrizione
⇐	Minore o uguale a.
>=	Maggiore o uguale a.
AGGIORNARE	Oppure
!	Non uguale a.
*	Goloso carattere jolly

È inoltre possibile restituire un insieme di oggetti in base all'impostazione o meno di un campo specifico utilizzando la parola chiave **null** o la relativa negazione **!null** come parte della query.

Tutti i campi non impostati sono generalmente esclusi dalle query corrispondenti.

Richiesta di campi oggetto specifici

Per impostazione predefinita, l'emissione di una chiamata API utilizzando GET restituisce solo gli attributi che identificano in modo univoco lo o gli oggetti. Questo insieme minimo di campi funge da chiave per ciascun oggetto e varia in base al tipo di oggetto. È possibile selezionare ulteriori proprietà dell'oggetto utilizzando il `fields` parametro di query nei seguenti modi:

Campi comuni o standard

Specificare **fields=*** per recuperare i campi oggetto più comunemente utilizzati. Questi campi vengono generalmente mantenuti nella memoria del server locale o richiedono un'elaborazione ridotta per l'accesso. Si tratta delle stesse proprietà restituite per un oggetto dopo l'utilizzo DI GET con una chiave UUID (URL PATH Key).

Tutti i campi

Specificare **fields=**** per recuperare tutti i campi oggetto, inclusi quelli che richiedono un'ulteriore elaborazione del server per l'accesso.

Selezione di campi personalizzati

Utilizzare **fields=<field_name>** per specificare il campo desiderato. Quando si richiedono più campi, i valori devono essere separati utilizzando virgole senza spazi.

Come Best practice, devi sempre identificare i campi specifici che desideri. Recuperare solo il set di campi comuni o tutti i campi quando necessario. I campi classificati come comuni e restituiti utilizzando *fields=**, vengono determinati da NetApp in base all'analisi interna delle performance. La classificazione di un campo potrebbe cambiare nelle release future.

Ordinamento degli oggetti nel set di output

I record di una raccolta di risorse vengono restituiti nell'ordine predefinito definito dall'oggetto. È possibile modificare l'ordine utilizzando il `order_by` parametro query con il nome del campo e la direzione di ordinamento come segue:

```
order_by=<field name> asc|desc
```

Ad esempio, è possibile ordinare il campo tipo in ordine decrescente seguito da id in ordine crescente:

```
order_by=type desc, id asc
```

- Se si specifica un campo di ordinamento ma non si fornisce una direzione, i valori vengono ordinati in ordine crescente.
- Quando si includono più parametri, separare i campi con una virgola.

Impaginazione durante il recupero di oggetti in una raccolta

Quando si esegue una chiamata API utilizzando GET per accedere a un insieme di oggetti dello stesso tipo, gli strumenti ONTAP per VMware vSphere tentano di restituire il maggior numero possibile di oggetti in base a due vincoli. È possibile controllare ciascuno di questi vincoli utilizzando parametri di query aggiuntivi sulla richiesta. Il primo vincolo raggiunto per una richiesta GET specifica termina la richiesta e limita quindi il numero di record restituiti.

Se una richiesta termina prima di scorrere tutti gli oggetti, la risposta contiene il collegamento necessario per recuperare il batch successivo di record.

Limitazione del numero di oggetti

Per impostazione predefinita, i tool di ONTAP per VMware vSphere restituiscono un massimo di 10.000 oggetti per una richiesta GET. È possibile modificare questo limite utilizzando il parametro di query *max_records*. Ad esempio:

```
max_records=20
```

Il numero di oggetti restituiti può essere inferiore al numero massimo effettivo, in base al vincolo temporale correlato e al numero totale di oggetti nel sistema.

Limitare il tempo impiegato per recuperare gli oggetti

Per impostazione predefinita, i tool di ONTAP per VMware vSphere restituiscono il maggior numero possibile di oggetti entro il tempo consentito per la richiesta GET. Il timeout predefinito è 15 secondi. È possibile modificare questo limite utilizzando il parametro di query *return_timeout*. Ad esempio:

```
return_timeout=5
```

Il numero di oggetti restituiti può essere inferiore al numero massimo effettivo, in base al vincolo correlato sul numero di oggetti e sul numero totale di oggetti nel sistema.

Restringimento del set di risultati

Se necessario, è possibile combinare questi due parametri con altri parametri di query per restringere il set di risultati. Ad esempio, quanto segue restituisce fino a 10 eventi EMS generati dopo il tempo specificato:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

È possibile inviare più richieste per scorrere gli oggetti. Ogni successiva chiamata API deve utilizzare un nuovo valore temporale basato sull'ultimo evento dell'ultimo set di risultati.

Proprietà delle dimensioni

I valori di input utilizzati con alcune chiamate API e alcuni parametri di query sono numerici. Invece di fornire un numero intero in byte, è possibile utilizzare un suffisso come mostrato nella tabella seguente.

Suffisso	Descrizione
KB	KB kilobyte (1024 byte) o kibyte
MB	MB Megabyte (KB x 1024 byte) o megibyte
GB	GB Gigabyte (MB x 1024 byte) o gibibyte
TB	TB terabyte (GB x 1024 byte) o tebibyte
PB	PB petabyte (TB x 1024 byes) o pebibyte

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/"

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/"

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/"

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 10,2"