



# **Tool ONTAP per la documentazione di VMware vSphere**

ONTAP tools for VMware vSphere 10.1

NetApp  
June 21, 2024

# Sommario

Tool ONTAP per la documentazione di VMware vSphere	1
Note di rilascio	2
Concetti	3
Panoramica sui tool ONTAP per VMware vSphere	3
Concetti e termini chiave	3
Controllo degli accessi in base al ruolo	5
Configura l'alta disponibilità per i tool ONTAP per VMware vSphere	10
AutoSupport	11
Implementa i tool ONTAP per VMware vSphere	12
Prerequisiti per la distribuzione degli strumenti ONTAP per VMware vSphere	12
Scarica i tool ONTAP per VMware vSphere	13
Preparazione all'implementazione dei tool ONTAP per VMware vSphere	14
Implementa una configurazione non ha a nodo singolo	15
Implementazione della configurazione ha	18
Ripristina i tool ONTAP per la configurazione di VMware vSphere	23
Codici di errore di distribuzione	24
Configurare gli strumenti ONTAP	29
Interfaccia utente di ONTAP tools Manager	29
Aggiungere e gestire le istanze di vCenter Server	29
Registrare il provider VASA con un'istanza di vCenter Server	30
Verificare il provider VASA registrato	31
Installare il plug-in NFS VAAI	31
Aggiornare i dati dell'host	32
Configurare le impostazioni dell'host ESXi	33
Rilevamento di host e sistemi storage	35
Aggiunta del backend dello storage	36
Associare il backend dello storage a un'istanza di vCenter Server	37
Configurare l'accesso alla rete	37
Configurare i ruoli e i privilegi degli utenti ONTAP	38
Panoramica dei tool NetApp ONTAP per la dashboard dei plug-in VMware vSphere	41
Crea archivio dati	44
Protezione di datastore e macchine virtuali	47
Abilitare SRA per proteggere i datastore	47
Configurare il sistema storage per il disaster recovery	47
Configurare SRA sull'appliance SRM	49
Aggiornare le credenziali SRA	50
Configurare siti protetti e di ripristino	51
Gestire gli strumenti ONTAP	57
Gestire i datastore	57
Gestire la soglia di archiviazione	61
Gestire i back-end dello storage	61
Gestire l'istanza di vCenter Server	63
Gestire i certificati	64

Gestire i criteri di igroup ed export . . . . .	65
Accedi ai tool ONTAP per la console di manutenzione di VMware vSphere . . . . .	65
Report sui tool ONTAP . . . . .	68
Raccogliere i file di log . . . . .	68
Gestire le macchine virtuali . . . . .	69
Modificare le impostazioni degli host ESXi utilizzando gli strumenti ONTAP . . . . .	71
Gestire le password . . . . .	72
Pulire i volumi . . . . .	74
Aggiornare i tool ONTAP . . . . .	76
Effettua l'aggiornamento alla versione piÙ recente dei tool ONTAP . . . . .	76
Aggiornare i codici di errore . . . . .	78
Strumenti ONTAP per la migrazione . . . . .	80
Eseguire la migrazione alla versione piÙ recente dei tool ONTAP . . . . .	80
Automatizzare utilizzando le API REST . . . . .	86
Panoramica delle API REST . . . . .	86
Come accedere ai tool ONTAP per l'API REST di VMware vSphere . . . . .	86
Variabili di input che controllano una richiesta API . . . . .	87
Accedi ai tool ONTAP per la documentazione di riferimento dell'API VMware vSphere tramite l'interfaccia utente Swagger . . . . .	90
Inizia con L'API REST . . . . .	91
Flussi di lavoro . . . . .	91
Note legali . . . . .	102
Copyright . . . . .	102
Marchi . . . . .	102
Brevetti . . . . .	102
Direttiva sulla privacy . . . . .	102
Open source . . . . .	102

# **Tool ONTAP per la documentazione di VMware vSphere**

# Note di rilascio

Fornisce importanti informazioni su questa release di strumenti ONTAP per VMware vSphere, inclusi problemi risolti, problemi noti, precauzioni e limitazioni.

Per ulteriori informazioni, consultare ["Note sulla versione dei tool ONTAP per VMware vSphere 10,1"](#).

# 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. I tool ONTAP per VMware vSphere si integrano con l'ecosistema VMware per consentire il provisioning dei datastore e fornire una protezione di base alle macchine virtuali.

Gli strumenti ONTAP per VMware vSphere 10,1 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).

### **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.

### **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 consente di gestire istanze di vCenter Server, backend di storage, certificati, password e download di pacchetti di registro.

### **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.

## **Storage Replication Adapter (SRA)**

SRA è il software specifico del vendor di soluzioni storage installato all'interno dell'appliance SRM. 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.

## **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.

## **SRM (Site Recovery Manager) di VMware**

SRM fornisce funzionalità di business continuity, disaster recovery, migrazione dei siti e test senza interruzioni per gli ambienti virtuali VMware.

## **API VMware vSphere per Storage Awareness (VASA)**

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

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

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

## **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 offre RBAC (role-based access control) che consente di controllare l'accesso agli oggetti vSphere. VCenter Server fornisce servizi di autenticazione e autorizzazione centralizzati a diversi livelli all'interno del proprio inventario, utilizzando i diritti degli utenti e dei gruppi con ruoli e privilegi. VCenter Server è dotato di 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 dei propri utenti e gruppi locali che è possibile utilizzare.
Permessi	Le autorizzazioni consentono di assegnare privilegi 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:

<b>Ruolo</b>	<b>Descrizione</b>
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: <ul style="list-style-type: none"><li>• Creare nuovi datastore</li><li>• Gestire i datastore</li></ul>

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 si dispone dei privilegi ONTAP corretti, è possibile accedere a.

Lo storage termina ed esegue tool ONTAP per i task 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

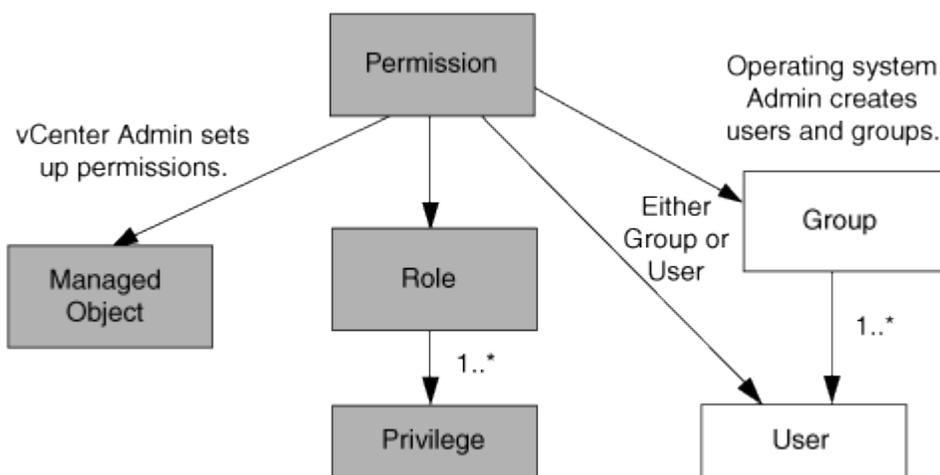
vCenter Server riconosce le autorizzazioni e non i privilegi. Ogni autorizzazione vCenter Server è composta da tre componenti.

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.
Distuggere 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".

## Configura l'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.

# Implementa i tool ONTAP per VMware vSphere

## Prerequisiti per la distribuzione degli strumenti ONTAP per 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 spazio per il pacchetto di installazione per nodo**

- 10 GB per le installazioni con thin provisioning
- 248 GB per installazioni con thick provisioning

- **Requisiti di dimensionamento del sistema host per nodo**

La memoria consigliata, in base alle dimensioni dell'implementazione e per nodo, è illustrata nella tabella seguente:

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

### Requisiti minimi di storage e applicazioni:

Storage, host e applicazioni	Requisiti minimi di versione
ONTAP	Ultima versione della patch di ONTAP 9.12.1, 9.13.1 o 9.14.1
Host ESXi	ESXi 7.0.3
Server vCenter	vCenter 7.0U3
Provider VASA	3,0
Applicazione OVA	10,1

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"](#)

### Ulteriori considerazioni sull'implementazione

È necessario considerare alcuni requisiti durante la personalizzazione dell'installazione degli strumenti ONTAP.

## Password dell'utente dell'applicazione

Questa è la password assegnata all'account amministratore. Per motivi di sicurezza, si consiglia di utilizzare una lunghezza della password compresa tra otto e trenta caratteri e di inserire almeno un carattere superiore, uno inferiore, uno speciale e un carattere speciale.

## Credenziali della console di manutenzione dell'appliance

Si dovrebbe accedere alla console di manutenzione usando il nome utente "maint". È possibile impostare la password per l'utente "maint" durante l'implementazione. Per modificare la password, è possibile utilizzare l'opzione Restart guest OS (Riavvia sistema operativo guest) disponibile durante il riavvio della VM in vCenter Server.

## Proprietà di rete dell'appliance

Specificare un nome host DNS valido (non qualificato) nonché l'indirizzo IP statico per gli strumenti ONTAP per VMware vSphere e gli altri parametri di rete. Gli indirizzi IP forniti devono essere accessibili dalla rete VLAN selezionata durante la distribuzione. DHCP non è supportato per gli strumenti ONTAP per VMware vSphere 10,1. Tutti questi parametri sono necessari per un'installazione e un funzionamento corretti.

# Scarica i tool ONTAP per VMware vSphere

È possibile scaricare .zip File contenente file binari (.ova) e certificati firmati per gli strumenti ONTAP per VMware vSphere da "[Sito di supporto NetApp](#)".

Una volta completata l'implementazione, nel tuo ambiente vengono installati i tool ONTAP per i prodotti VMware vSphere e VASA. Per impostazione predefinita, i tool di ONTAP per VMware vSphere iniziano a funzionare non appena decidi il successivo modello di implementazione e scegli se abilitare il provider VASA in base ai tuoi requisiti. Vedere "[Registrazione il provider VASA con un'istanza di vCenter Server](#)" per ulteriori informazioni.

## Archivio di contenuti

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.

Creare la libreria di contenuti utilizzando i seguenti passaggi:

### Fasi

1. Accedere al client vSphere utilizzando `https://vcenterip/ui`
2. Selezionare i puntini di sospensione orizzontali accanto al client vSphere e selezionare **Libreria di contenuti**.
3. Selezionare **Crea** sul lato destro della pagina.
4. Fornire un nome per la libreria e creare la libreria di contenuti.

5. Accedere alla libreria di contenuti creata.
6. Selezionare **azioni** sul lato destro della pagina, quindi selezionare **Importa elemento** e importare il file OVA.

## Preparazione all'implementazione dei tool ONTAP per VMware vSphere

Prima di iniziare la distribuzione dei tool ONTAP per VMware vSphere, devi conoscere i requisiti di base del backend dello storage, le esigenze applicative e le licenze. Pianifica in anticipo la tua implementazione e decidi come configurare i tool ONTAP per VMware vSphere nel tuo ambiente.

### Preparazione per l'implementazione

Di seguito sono elencati i tool ONTAP per i requisiti di VMware vSphere prima di procedere con l'implementazione:

1. Configurare e configurare l'ambiente vCenter Server.
2. Scaricare il file `.ova`.
3. (Facoltativo) usato per l'utente dell'automazione - raccogliere il file JSON delle collezioni Postman fornito da NetApp.
4. Credenziali vCenter Server padre per distribuire l'OVA. La password di vCenter Server padre non deve contenere questi caratteri speciali (`$`, `'`, `"`)
5. Assicurarsi che l'host o il pool di risorse in cui viene distribuito l'OVA disponga delle risorse minime menzionate nella "[Prerequisiti per la distribuzione degli strumenti ONTAP per VMware vSphere](#)" sezione.
6. Le credenziali di accesso per l'istanza di vCenter Server a cui si conatteranno gli strumenti ONTAP per VMware vSphere per la post-implementazione per la registrazione.
7. Eliminare la cache del browser.
8. Per l'implementazione non ha, hai bisogno di tre indirizzi IP gratuiti - un indirizzo IP gratuito per il bilanciamento del carico e un indirizzo IP gratuito per il pannello di controllo di 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 dell'assegnazione. Tutti e cinque gli indirizzi IP devono trovarsi sulla stessa VLAN selezionata per la distribuzione.
9. Il modello della libreria di contenuti una volta caricato non deve essere eliminato dopo la distribuzione poiché verrà utilizzato durante i riavvii.
10. In un'implementazione multi-vCenter in cui i certificati CA personalizzati sono obbligatori, mappare il nome di dominio su cui il certificato viene rilasciato all'indirizzo IP virtuale. Eseguire un controllo `nslookup` sul nome di dominio per verificare se il dominio viene risolto all'indirizzo IP desiderato. I certificati devono essere creati con il nome di dominio e l'indirizzo IP dell'indirizzo IP del bilanciatore del carico.
11. VLAN supportata IPv4/IPv6 - pure IPv6 non è supportato. La modalità mista è supportata con VLAN con indirizzi IPv6 e IPv4.
12. Server NTP fornito a vCenter Server per Time Sync.
13. Indirizzo IP statico Dettagli di configurazione per il nodo o la VM in cui viene distribuito l'OVA (obbligatorio) e altri dettagli.

- a. Nome host vCenter Server (vCenter dove viene distribuito OVA)
- b. Nome utente vCenter Server (vCenter dove viene distribuito OVA)
- c. Password vCenter Server (vCenter dove viene distribuito OVA)
- d. Pool di risorse
- e. Data LIF (IPv4/IPv6)
  - f. LIF di gestione
- g. Nome utente ONTAP
- h. Password ONTAP
- i. Nome SVM
- j. Protocollo
- k. Indirizzi IP virtuali per il piano di controllo di Kubernetes.
  - l. Menu a discesa HA/NON ha
- m. Elenco dei nomi host
- n. Indirizzi IP (stringa)
- o. Nome della libreria di contenuti
- p. Nome modello OVF
- q. Gateway IPv6 (opzionale)

## Implementa una configurazione non ha a nodo singolo

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 VM.

Esempio: C1\_sti67-vsimsim-ucs154k\_1679633108::> route di rete create -vserver <SVM> -destination 0,0.0.0/0 -gateway <gateway\_ip>

### Fasi

1. Accedere al server vSphere.
2. Accedere al pool di risorse, al cluster 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...).



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

4. È possibile immettere l'URL del file .ova o navigare alla cartella in cui è stato salvato il file .ova, quindi

selezionare **Avanti**.

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 la configurazione **distribuzione semplice(S)**, **distribuzione facile(M)** o **distribuzione avanzata(S)** o **distribuzione avanzata(M)**.

L'opzione di implementazione avanzata usa Trident come provisioner di storage dinamico per ONTAP per creare volumi e l'implementazione semplice usa lo storage locale per creare volumi.

10. Selezionare il datastore in cui è necessario implementare l'OVA e selezionare **Avanti**.
11. Selezionare la rete di origine e di destinazione e selezionare **Avanti**.
12. Selezionare la finestra **Personalizza modello > Configurazione di sistema**.

System Configuration		8 settings
Application username(*)	Username to assign to the Application	
Application password(*)	Password to assign to the Application	
	Password	<input type="password"/>
	Confirm Password	<input type="password"/>
Enable ASUP	Select this checkbox to enable ASUP	
	<input checked="" type="checkbox"/>	
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.	
	<input type="text"/>	
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '.', '-', '_', '!' special characters are supported	
	<input type="text"/>	
Administrator password(*)	Password to assign to the Administrator	
	Password	<input type="password"/>
	Confirm Password	<input type="password"/>
NTP servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used	
	<input type="text"/>	
Maintenance user password(*)	Password to assign to maint user account	
	Password	<input type="password"/>
	Confirm Password	<input type="password"/>

Inserire i seguenti dati:

- .. Nome utente e password dell'applicazione: Questo nome utente e password vengono utilizzati per registrare sia il provider VASA che SRA in vCenter Server.
- .. La casella di controllo **Abilita ASUP** è selezionata per impostazione predefinita.

AutoSupport può essere attivato o disattivato solo durante l'implementazione.

.. Nel campo **ASUP Proxy URL**, fornire questo URL per evitare il blocco del firewall per la trasmissione dei dati AutoSupport.

.. Administrator Username (Nome utente amministratore) e Administrator Password (Password amministratore): Password utilizzata per accedere a Gestione strumenti ONTAP.

.. Immettere le informazioni sul server NTP nel campo **Server NTP**.

- .. Password utente di manutenzione: Consente di accedere a 'Opzioni console manutenzione'.
- . Nella finestra **Personalizza modello > Configurazione distribuzione**, immettere i seguenti dettagli:

+

Load balancer IP(*)	Load balancer IP (*) eg: 10.0.0.1
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane eg: 10.0.0.1
Enable SVM scoping	Ignore when cluster scoping is required <input type="checkbox"/>
Protocol	Internet Small Computer Systems Interface (iSCSI)/Network File System (NFS) NFS
ONTAP/SVM management LIF(*)	Specify the management LIF for trident eg: 172.17.0
ONTAP/SVM data LIF(*)	Specify the data LIF for trident. IPv6gateway field is mandatory if you provide IPv6 address here. Ignored when SVM scoping
ONTAP/SVM username(*)	Specify the ONTAP cluster username eg: username
ONTAP/SVM password(*)	Specify the ONTAP cluster password Password: ..... Confirm Password: .....
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. <input checked="" type="checkbox"/>

1. Inserisci un indirizzo IP disponibile nell'indirizzo IP virtuale per il piano di controllo di Kubernetes. Tutto ciò è necessario per Kubernetes API Server.
2. Selezionare l'opzione **attiva ambito SVM** quando si intende utilizzare l'account utente SVM aggiunto direttamente. Per usare ONTAP cluster, non selezionare la casella di controllo.



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

3. Selezionare NFS o iSCSI nel campo **protocollo**.
4. Inserisci il cluster ONTAP o l'indirizzo IP di gestione SVM nel campo **LIF di gestione ONTAP/SVM**.
5. Entra nel cluster ONTAP o nella SVM ONTAP/SVM Data LIF. La LIF dati deve appartenere al protocollo selezionato. Ad esempio, se si seleziona il protocollo iSCSI, deve essere fornita una LIF dati iSCSI.
6. Per Storage VM, puoi scegliere di fornire i dettagli relativi alla Storage VM predefinita di ONTAP o creare una nuova Storage VM. Non immettere il valore nel campo **Storage VM** quando è selezionata l'opzione Enable SVM scoping (attiva ambito SVM), poiché questo campo viene ignorato.
7. Inserisci il nome utente di ONTAP/SVM. Trident richiede username e password di ONTAP/SVM per creare volumi per memorizzare i dati dei servizi in caso di implementazione avanzata o ha e per recuperare i dati dai volumi durante il guasto dei nodi.
8. Inserisci la password ONTAP/SVM. La password di login di ONTAP/SVM per questa Storage VM non deve contenere questi caratteri speciali (\$, ', ").
9. La macchina virtuale primaria è abilitata per impostazione predefinita. Non modificare questa scelta.
  - a. Nella finestra **Personalizza modello > Configurazione nodo** immettere le proprietà di rete dell'OVA.



Le informazioni qui fornite verranno convalidate per i modelli corretti durante il processo di installazione. In caso di discrepanza, sulla console Web viene visualizzato un messaggio di errore e viene richiesto di correggere eventuali informazioni errate fornite.

10. Immettere il nome host nel campo host name. Sono supportati solo i nomi host composti da lettere maiuscole (A-Z), lettere minuscole (a-z), cifre (0-9) e il trattino (-). Se si desidera configurare lo stack doppio, specificare il nome host mappato all'indirizzo IPv6.
11. Immettere l'indirizzo IP (IPv4) mappato al nome host. In caso di doppio stack, fornire qualsiasi indirizzo IP IPv4 disponibile che si trovi nella stessa VLAN dell'indirizzo IPv6.
12. Immettere l'indirizzo IPv6 sulla rete distribuita solo quando è necessario utilizzare la doppia leva.
13. Specificare la lunghezza del prefisso solo per IPv6.
14. Specificare la subnet da utilizzare nella rete distribuita nel campo maschera di rete (solo per IPv4).
15. Specificare il gateway sulla rete distribuita.
16. Specificare l'indirizzo IP del server DNS principale.
17. Specificare l'indirizzo IP del server DNS secondario.
18. Specificare il nome del dominio di ricerca da utilizzare quando si risolve il nome host.
19. Specificare il gateway IPv6 sulla rete distribuita solo quando è necessario disporre di uno stack doppio.
  - a. 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.

- b. 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 vengono convalidate. 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.

- c. Apportare le modifiche necessarie nella finestra di dialogo. Utilizzare il pulsante Tab per spostarsi all'interno del pannello per immettere i valori, **OK** o **Annulla**.
    - d. Selezionando **OK**, i valori forniti verranno nuovamente convalidati. È possibile correggere i valori fino a tre volte. Se non si riesce a correggere entro i 3 tentativi, l'installazione del prodotto si interrompe e si consiglia di provare a eseguire l'installazione su una nuova macchina virtuale.
    - e. Una volta completata l'installazione, la console Web mostra lo stato degli strumenti ONTAP per VMware vSphere.

## Implementazione della 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 passaggio obbligatorio per la distribuzione della configurazione ha a tre nodi. Vedere "[Scarica gli strumenti di ONTAP](#)" per ulteriori informazioni. Scopri di più "[Creazione e utilizzo della libreria di contenuti](#)".

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. Per eseguire la distribuzione dal server vSphere:
  - a. Accedere al server vSphere.
  - b. Accedere al pool di risorse o all'host in cui si desidera distribuire l'OVA e fare clic con il pulsante destro del mouse sulla posizione in cui si desidera distribuire la VM, quindi selezionare **Deploy OVF template...**



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

- c. È possibile immettere l'URL del file `.ova` o navigare alla cartella in cui è stato salvato il file `.ova`, quindi selezionare **Avanti**
2. Per eseguire la distribuzione dalla libreria 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**
  3. Selezionare un nome e una cartella per la macchina virtuale e selezionare **Avanti**.
  4. Selezionare l'host e selezionare **Avanti**
  5. Rivedere il riepilogo del modello e selezionare **Avanti**.
  6. Leggere e accettare il contratto di licenza e selezionare **Avanti**.
  7. Nella finestra **Configurazione**, selezionare la configurazione **High-Availability Deployment(S)**, **High-Availability Deployment(M)** o **High-Availability Deployment(L)**, a seconda delle proprie esigenze.
  8. Selezionare lo spazio di archiviazione per i file di configurazione e del disco, quindi selezionare **Avanti**.
  9. Selezionare la rete di destinazione per ciascuna rete di origine, quindi selezionare **Avanti**.
  10. Selezionare la finestra **Personalizza modello > Configurazione di sistema**.

System Configuration		8 settings	
Application username(*)	Username to assign to the Application	<input type="text"/>	
Application password(*)	Password to assign to the Application	Password <input type="password"/> ⓘ ⓘ Enter a password to enable authentication.	Confirm Password <input type="password"/> ⓘ
Enable ASUP	Select this checkbox to enable ASUP	<input checked="" type="checkbox"/>	
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.	<input type="text"/>	
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '.', '-', '_', ':' special characters are supported	<input type="text"/>	
Administrator password(*)	Password to assign to the Administrator	Password <input type="password"/> ⓘ ⓘ Enter a password to enable authentication.	Confirm Password <input type="password"/> ⓘ
NTP servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used	<input type="text"/>	
Maintenance user password(*)	Password to assign to maint user account	Password <input type="password"/> ⓘ ⓘ Enter a password to enable authentication.	Confirm Password <input type="password"/> ⓘ

Inserire i seguenti dati:

- a. Nome utente e password dell'applicazione: Questo nome utente e password vengono utilizzati per registrare sia il provider VASA che SRA in vCenter Server.
  - b. La casella di controllo **Abilita AutoSupport** è selezionata per impostazione predefinita. AutoSupport può essere attivato o disattivato solo durante l'implementazione.
  - c. Nel campo **ASUP Proxy URL**, fornire questo URL per evitare il blocco del firewall per la trasmissione dei dati AutoSupport.
  - d. Administrator Username (Nome utente amministratore) e Administrator Password (Password amministratore): Password utilizzata per accedere a ONTAP Tools Manager (Gestione strumenti di gestione).
  - e. Immettere le informazioni sul server NTP nel campo **Server NTP**.
  - f. Password utente di manutenzione: Consente di accedere a 'Opzioni console manutenzione'.
11. Nella finestra **Personalizza modello > Configurazione distribuzione**, immettere i seguenti dettagli:

Load balancer IP(*)	Load balancer IP (*) eg: 10.0.0.1
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane eg: 10.0.0.1
Enable SVM scoping	Ignore when cluster scoping is required <input type="checkbox"/>
Protocol	Internet Small Computer Systems Interface (iSCSI)/Network File System (NFS) NFS
ONTAP/SVM management LIF(*)	Specify the management LIF for trident eg: 172.17.0
ONTAP/SVM data LIF(*)	Specify the data LIF for trident. IPv6gateway field is mandatory if you provide IPv6 address here. Ignored when SVM scoping is enabled
ONTAP/SVM username(*)	Specify the ONTAP cluster username eg: username
ONTAP/SVM password(*)	Specify the ONTAP cluster password Password: ..... Confirm Password: .....
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. <input checked="" type="checkbox"/>

- a. Inserisci un indirizzo IP disponibile nell'indirizzo IP virtuale per il piano di controllo di Kubernetes. Tutto ciò è necessario per Kubernetes API Server.
- b. Nell'opzione di implementazione avanzata, selezionare l'opzione **Enable SVM scoping** (Abilita ambito SVM) quando si intende utilizzare l'account utente SVM aggiunto direttamente. Per usare ONTAP cluster, non selezionare la casella di controllo.



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

- c. Selezionare NFS o iSCSI nel campo **protocollo**.
  - d. Inserisci il cluster ONTAP o l'indirizzo IP di gestione SVM nel campo **LIF di gestione ONTAP/SVM**.
  - e. Entra nel cluster ONTAP o nella SVM ONTAP/SVM Data LIF. La LIF dati deve appartenere al protocollo selezionato. Ad esempio, se si seleziona il protocollo iSCSI, deve essere fornita una LIF dati iSCSI.
  - f. Per Storage VM, puoi scegliere di fornire i dettagli relativi alla Storage VM predefinita di ONTAP o creare una nuova Storage VM. Non immettere il valore nel campo **Storage VM** quando è selezionata l'opzione Enable SVM scoping (attiva ambito SVM), poiché questo campo viene ignorato.
  - g. Inserisci il nome utente di ONTAP/SVM. Trident richiede username e password di ONTAP/SVM per creare volumi per memorizzare i dati dei servizi in caso di implementazione avanzata o ha e per recuperare i dati dai volumi durante il guasto dei nodi.
  - h. Inserisci la password ONTAP/SVM. La password di login di ONTAP/SVM per questa Storage VM non deve contenere questi caratteri speciali (\$, ', ").
  - i. La macchina virtuale primaria è abilitata per impostazione predefinita. Non modificare questa scelta.
12. Nella finestra **Personalizza modello > Dettagli libreria contenuti**, immettere il **Nome libreria contenuti** e il **Nome modello OVF**.
  13. Nella finestra **Personalizza modello > Configurazione vCenter**, fornire i dettagli di vCenter Server in cui è ospitata la libreria di contenuti.
  14. Nella finestra **Personalizza modello > Configurazione nodo**, immettere le proprietà di rete dell'OVA per

tutti e tre i nodi.



Le informazioni qui fornite verranno 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.

- a. Immettere il nome host. Sono supportati solo i nomi host composti da lettere maiuscole (A-Z), lettere minuscole (a-z), cifre (0-9) e il trattino (-). Se si desidera configurare lo stack doppio, specificare il nome host mappato all'indirizzo IPv6.
  - b. Immettere l'indirizzo IP (IPv4) mappato al nome host. In caso di doppio stack, fornire qualsiasi indirizzo IP IPv4 disponibile che si trovi nella stessa VLAN dell'indirizzo IPv6.
  - c. Immettere l'indirizzo IPv6 sulla rete distribuita solo quando è necessario disporre di uno stack doppio.
  - d. Specificare la lunghezza del prefisso solo per IPv6.
  - e. Specificare la subnet da utilizzare nella rete distribuita nel campo maschera di rete (solo per IPv4).
  - f. Specificare il gateway sulla rete distribuita.
  - g. Specificare l'indirizzo IP del server DNS principale.
  - h. Specificare l'indirizzo IP del server DNS secondario.
  - i. Specificare il nome del dominio di ricerca da utilizzare quando si risolve il nome host.
  - j. Specificare il gateway IPv6 sulla rete distribuita solo quando è necessario disporre di uno stack doppio.
15. Nella finestra **Personalizza modello > Configurazione nodo 2 e Configurazione nodo 3**, immettere i seguenti dettagli:
- a. Nome host 2 e 3 - sono supportati solo i nomi host costituiti da lettere maiuscole (A-Z), lettere minuscole (a-z), cifre (0-9) e il carattere speciale trattino (-). Se si desidera configurare lo stack doppio, specificare il nome host mappato all'indirizzo IPv6.
  - b. Indirizzo IP
  - c. Indirizzo IPv6
16. 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.

17. 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 vengono convalidate. 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.

18. Apportare le modifiche necessarie nella finestra di dialogo. Utilizzare il pulsante Tab per spostarsi all'interno del pannello per immettere i valori, **OK** o **Annulla**.
19. Selezionando **OK**, i valori forniti verranno nuovamente convalidati. È possibile correggere i valori fino a 3 volte. Se non si riesce a correggere entro i 3 tentativi, l'installazione del prodotto si interrompe e si consiglia di provare a eseguire l'installazione su una nuova macchina virtuale.
20. Una volta completata l'installazione, la console Web mostra lo stato degli strumenti ONTAP per VMware vSphere.

# 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.

Puoi ripristinare sia l'implementazione a nodo singolo che le configurazioni ha a tre nodi.



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. Accedere al pool di risorse, 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. È possibile immettere l'URL del file .ova o navigare alla cartella in cui è stato salvato il file .ova, quindi selezionare **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. Selezionare la finestra **Personalizza modello > Configurazione di sistema**. Inserire i seguenti dati:
  - a. Nome utente e password dell'applicazione: Questo nome utente e password vengono utilizzati per registrare sia il provider VASA che SRA in vCenter Server. Questo può essere diverso dal nome utente e dalla password forniti durante la distribuzione iniziale.
  - b. La casella di controllo **Abilita ASUP** è selezionata per impostazione predefinita.

AutoSupport può essere attivato o disattivato solo durante l'implementazione.

.. Nel campo **ASUP Proxy URL**, fornire questo URL per evitare il blocco del firewall per la trasmissione dei dati AutoSupport.

.. Administrator Username (Nome utente amministratore) e Administrator Password (Password)

amministratore): Password utilizzata per accedere a Gestione strumenti ONTAP. Questo può essere diverso dal nome utente e dalla password forniti durante la distribuzione iniziale.

.. Immettere le informazioni sul server NTP nel campo **Server NTP**.

.. Maintenance user password (Password utente di manutenzione): Questa opzione consente di accedere alle opzioni della console di manutenzione.

. Nella finestra **Personalizza modello > Configurazione distribuzione**, immettere i dettagli forniti durante la distribuzione. Tutti i valori di questa sezione devono essere uguali a quelli forniti durante l'implementazione iniziale, ad eccezione del valore di LIF dei dati.



Non modificare il nome della SVM storage, in quanto su cui sono archiviati i dati di recovery. Ciò si applica anche all'account utente SVM aggiunto direttamente.

. Nel caso di recovery ha-deployment, fornisci i seguenti dettagli:

.. Dettagli della libreria di contenuti.

.. Dettagli di configurazione di vCenter.

. Nella finestra **Customize template > Node Configuration** (Personalizza modello\* > **Configurazione nodo**) immettere i dettagli come da impostazione che si sta tentando di ripristinare, non ha o ha.

. 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.

. 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 vengono convalidate. 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.

. Apportare le modifiche necessarie nella finestra di dialogo. Utilizzare il pulsante Tab per spostarsi all'interno del pannello per immettere i valori, **OK** o **Annulla**.

. Selezionando **OK** o **Annulla**, i valori forniti verranno nuovamente convalidati. È possibile correggere i valori per 3 volte. Se non si riesce a correggere entro i 3 tentativi, l'installazione del prodotto si interrompe e si consiglia di provare a eseguire l'installazione su una nuova macchina virtuale.

. 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.

## 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	<p>* 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.</p> <p>* 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.</p> <p>* Ridistribuire.</p>
052	Copia chiavi SSH non riuscita	Riavviare la macchina virtuale principale.

053	Installazione RKE2 non riuscita	Eseguire quanto segue e riavviare la macchina virtuale primaria o ridistribuire: Sudo rke2-killall.sh (tutte le VM) Sudo rke2-uninstall.sh (tutte le VM).
054	Impostazione kubeconfig non riuscita	Ridistribuzione
055	Distribuzione del registro non riuscita	Se il pod del Registro di sistema è presente, attendere che il pod sia pronto, quindi riavviare la macchina virtuale primaria oppure ridistribuirlo.
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	<p>*Assicurarsi che gli indirizzi IP della LIF di gestione e della LIF dati siano raggiungibili dalla VM.</p> <p>*Assicurarsi che il protocollo NFS o iSCSI sia abilitato e configurato correttamente su ONTAP.</p> <p>*Verificare che l'indirizzo IP NFS/iSCSI Data LIF fornito sia corretto e online.</p> <p>*Assicurarsi che il nome utente e la password forniti siano corretti e che l'utente disponga di privilegi sufficienti per creare un volume.</p> <p>* Riavviare se tutti i punti precedenti sono corretti. Altrimenti, ridistribuzione.</p>
058	Importazione Trident non riuscita	<p>*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.</p> <p>*Assicurarsi di utilizzare la stessa configurazione di ONTAP per ripristinare l'installazione e riprovare il ripristino.</p>

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, redistribuzione.
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.	<p>* Assicurati di utilizzare la stessa SVM e che sia presente il volume di recovery nella SVM. (Il nome del volume di ripristino inizia con otvng_trident_recovery)</p> <p>* Assicurati che gli indirizzi IP della LIF di gestione e della LIF dati siano raggiungibili dalla VM.</p> <p>* Assicurarsi che il protocollo NFS/iSCSI sia abilitato e configurato correttamente su ONTAP.</p> <p>* Assicuratevi che l'indirizzo IP NFS/iSCSI DAT LIF fornito sia corretto e online.</p> <p>* 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.</p> <p>* Riprovare il ripristino</p>

# Configurare gli strumenti ONTAP

## Interfaccia utente di ONTAP tools Manager

I tool ONTAP per VMware vSphere sono un sistema multi-tenant che gestisce diverse 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 rinnovarlo o aggiornare tutti i certificati.
- Gestione password - Reimposta la password dell'applicazione OVA per l'utente.

Per accedere a Gestione strumenti ONTAP, avviare

<https://loadBalanceIP:8443/virtualization/ui/> Dal browser e accedi con gli strumenti ONTAP per le credenziali di amministratore di VMware vSphere fornite durante la distribuzione.

## Aggiungere e gestire le istanze di vCenter Server

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

### Aggiungere un'istanza di vCenter Server

#### 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.

## Registra i tool ONTAP per il plug-in VMware vSphere con l'istanza di vCenter Server

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.

## Annulla la registrazione dei tool ONTAP per il plug-in VMware vSphere

Puoi annullare la registrazione degli strumenti ONTAP per il plug-in VMware vSphere da un'istanza di vCenter Server seguendo la procedura riportata di seguito.

### 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. Fare clic sulle ellissi verticali sul vCenter che si desidera rimuovere e selezionare l'opzione **Rimuovi**.



Non è possibile rimuovere un'istanza di vCenter Server se è collegata una mappatura dello storage. È necessario rimuovere la mappatura prima di rimuovere l'istanza di vCenter Server.

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.

## 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**.

## Verificare il provider VASA registrato

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 vStorage di VMware per l'integrazione degli array (VAAI) utilizzando i tool ONTAP per VMware vSphere.

## Cosa ti serve

- Dovresti aver scaricato il pacchetto di installazione per il plug-in NFS per VAAI (.vib) Dal NetApp Support Site. "[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.
- È necessario impostare i valori di `DataMover.HardwareAcceleratedMove`, `DataMover.HardwareAcceleratedInit`, e `VMFS3.HardwareAcceleratedLocking` impostazioni host su "1".

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

- L'opzione vstorage dovrebbe essere stata attivata sulla macchina virtuale di storage (SVM) utilizzando `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. Individuare e selezionare .vib Quindi fare clic su **carica** per caricare il file sugli strumenti ONTAP.
5. Fare clic su **Install on EXSI 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. Non è necessario eseguire ulteriori operazioni per attivare il plug-in.

## Aggiornare i dati dell'host

È possibile eseguire un rilevamento on-demand sull'host ESXi per ottenere gli ultimi aggiornamenti dei dati storage.

### 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, quindi selezionare **NetApp ONTAP tools > Aggiorna dati host**.

3. Nella finestra a comparsa **Aggiorna dati host**, selezionare **Sì** per riavviare il rilevamento di tutti i sistemi di archiviazione connessi.

## 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, quindi 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

Configura 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.

In ambienti dalle performance elevate o quando si testano le performance con un singolo datastore LUN, si consiglia di modificare l'impostazione del bilanciamento del carico del criterio di selezione del percorso (PSP) round-robin (VMW\_PSP\_RR) dall'impostazione IOPS predefinita di 1000 a un valore di 1.

## Impostazioni NFS

- **Net.TcpipHeapSize**

Impostare questo valore su 32.

- **Net.TcpipHeapMax**

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.

## 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, quindi selezionare **NetApp ONTAP tools > Update host Data** (Strumenti **aggiornamento 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 **Si**.
4. Selezionare i controller di storage rilevati con lo stato `Authentication Failure`, Quindi 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 storage con `Authentication Failure` stato.

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

- Utilizzare gli strumenti ONTAP per VMware vSphere per configurare le impostazioni dell'host ESXi per gli host che visualizzano l'icona Avviso nella colonna Impostazioni adattatore, Impostazioni MPIO o Impostazioni NFS.

- Fornire le credenziali del sistema storage.

## Aggiunta del backend dello storage

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

### 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 abilitare l'utente SVM per il provisioning del datastore vVol.



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

## Aggiungi il backend dello storage con 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 in 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. Specificare l'indirizzo IP del server o i dettagli FQDN, Nome utente e 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.

## Aggiungere il backend dello storage utilizzando l'interfaccia utente client vSphere:

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 i dettagli relativi a indirizzo IP del server, nome utente, password e porta e fare clic su **Aggiungi**



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

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

## Associare il 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 degli 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 ai criteri 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 nel passaggio 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 la virgola (,) per separare gli indirizzi IP. È possibile specificare un indirizzo IP specifico, un intervallo di indirizzi IP o IPv6.

4. Fare clic su **SALVA**.

## 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](https://<loadbalancerIP>:8443/Virtualization/user-Privileges/users_roles.zip).
- Il file dei privilegi di ONTAP dovrebbe essere stato scaricato da ONTAP Tools utilizzando [https://<loadbalancerIP>:8443/virtualization/user-privileges/users\\_roles.zip](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.



Puoi creare utenti a livello di cluster o a livello di 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.

### Fasi

1. Estrarre il file scaricato [https://<loadbalancerIP>:8443/Virtualization/user-privileges/users\\_roles.zip](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. Effettua l'accesso come cluster o utente SVM.
4. Selezionare **Cluster > Impostazioni > pannello utenti e ruoli**.
5. Selezionare **Aggiungi** in utenti.
6. Nella finestra di dialogo **Aggiungi utente**, selezionare **prodotti di virtualizzazione**.
7. **Sfoglia** per selezionare e caricare il file JSON con privilegi ONTAP.

Il campo prodotto viene compilato automaticamente.

8. Selezionare la funzionalità desiderata dal menu a discesa funzionalità prodotto.

Il campo **ruolo** viene compilato automaticamente in base alla capacità del prodotto selezionata.

9. Immettere il nome utente e la password richiesti.

10. 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 i privilegi specifici dello strumento ONTAP e aggiunge il prefisso `XXX missing privilege` a loro. 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:

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

## Creare manualmente un utente e un ruolo ONTAP

Seguire le istruzioni in questa sezione per creare manualmente l'utente e i ruoli senza utilizzare il file JSON.

1. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster del cluster.
2. Effettua l'accesso come cluster o utente SVM.
3. Selezionare **Cluster > Impostazioni > pannello utenti e ruoli**.
4. 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.
5. 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 il 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".

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

Quando si selezionano gli strumenti NetApp ONTAP per l'icona del 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 visualizzazioni del plugin.

La selezione di vCenter Server effettuata in una pagina persiste nelle schede del plug-in.

vmw vSphere Client    Menu    Search in all environments

NetApp ONTAP Tools    INSTANCE 10.224.132.8444

Overview    vCenter server: 172.21.104.101

6  
Storage backends

**Unhealthy**

VASA provider    **Online**

[other vasa provider states](#)

Storage backends - capacity

197.3 GB USED AND RESERVED    481.69 GB PHYSICAL AVAILABLE

VIEW ALL STORAGE BACKENDS (6)

Virtual machines

Name	vCenter VM latency	vCenter VM committed capacity	Max datastore latency	Total datastore IOPS	Avg datastore throughput
AE-WEB-APSG-P01	176 ms	33 GB	176 ms	33 k	62 MB/s
AE-WEB-AUD-P01	168 ms	10 GB	168 ms	10 k	96 MB/s
ib-sne-vnx-p01	162 ms	6 GB	162 ms	6 k	180 MB/s
AE-VESTA3	151 ms	11 GB	151 ms	11 k	354 MB/s
AE-VMware1-Network-AAEF0038	75 ms	19 GB	75 ms	19 k	106 MB/s
AE-WEB-APSG-P03	73 ms	40 GB	73 ms	40 k	62 MB/s
AE-WEB-AUD-P07	68 ms	8 GB	68 ms	8 k	96 MB/s
ib-sne-vnx-p04	66 ms	16 GB	66 ms	16 k	180 MB/s
AE-VESTA9	65 ms	24 GB	65 ms	24 k	354 MB/s
AE-VMware1-Network-AAEF0038	63 ms	12 GB	63 ms	12 k	106 MB/s

VIEW ALL VIRTUAL MACHINES (318)

Datstores    Datastore type: All

Name	Space utilized (Top 10↓)	IOPS	Latency	Throughput	Storage VM	Type
datastore01	98%	33 k	176 ms	200	storage_vm_01	NFS
datastore02_long_name	83%	10 k	168 ms	300	svm_02	NFS
datastore03	72%	6 k	162 ms	200	storage_vm_03_long_name	VVols
datastore04	68%	11 k	151 ms	300	storage_vm_04	VMFS
datastore05_long_name	61%	19 k	75 ms	500	storage_vm_05	NFS
datastore06	55%	40 k	73 ms	200	storage_vm_06_long_name	VVols
datastore07	45%	8 k	68 ms	200	storage_vm_07	VMFS
datastore08	36%	16 k	66 ms	500	storage_vm_08	NFS
datastore09	27%	24 k	65 ms	300	storage_vm_09	VMFS
datastore10_very_long_name	12%	12 k	63 ms	500	storage_vm_10_long_name	NFS

VIEW ALL DATASTORES (54)

ESXi host compliance

NFS    **Issues (15)**    **Unknown (7)**    **Compliant (27)**

MPIO    **Issues (15)**    **Unknown (7)**    **Compliant (27)**

APPLY RECOMMENDED SETTINGS    VIEW ALL HOSTS (49)

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	<p>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.</p> <p>Lo stato dei backend di archiviazione viene visualizzato come "integro" quando tutti i backend di archiviazione sono normali.</p> <p>Lo stato dei backend di archiviazione viene visualizzato come "non integro" se uno dei backend di archiviazione presenta un problema (stato sconosciuto/irraggiungibile/danneggiato).</p> <p>Quando si fa clic sullo stato "non integro", viene visualizzata una descrizione comandi con lo stato dei backend di archiviazione. I nomi dei cluster sono dotati di collegamento ipertestuale, è possibile fare clic sul link per aprire la pagina di riepilogo del backend dello storage e ottenere ulteriori dettagli.</p> <p>Il collegamento altri stati del provider VASA (VP) mostra lo stato corrente del VP registrato in vCenter Server.</p>
Backend di archiviazione - capacità	<p>Questa scheda mostra la capacità aggregata utilizzata e disponibile di tutti i backend storage per l'istanza di vCenter Server selezionata.</p>
Macchine virtuali	<p>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.</p>
Datastore	<p>Questa scheda mostra i primi 10 datastore ordinati in base a una metrica di prestazioni.</p> <p>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.</p>

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 <b>Applica impostazioni consigliate</b> per applicare le impostazioni consigliate. È possibile fare clic su <b>Issues/Unknown</b> per visualizzare l'elenco degli host.
--------------------------------	---

## Crea archivio dati

A seconda della destinazione scelta per l'azione, 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. L'interfaccia utente è autoesplicativa, utilizzare questi passaggi come linee guida.

### Creare il datastore vVol

Puoi creare un datastore vVol con nuovi volumi o con volumi esistenti. Non puoi creare un datastore vVol con la combinazione di volumi esistenti e nuovi volumi.



Controllare che gli aggregati root non siano mappati alla SVM.

#### 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, quindi selezionare **NetApp ONTAP Tools > Create Datastore**
3. Nel riquadro **tipo**, selezionare vVol in **tipo datastore**.



Si ottiene l'opzione vVol solo se il provider VASA è registrato con il vCenter selezionato.

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**, a seconda della scelta, selezionare criterio di esportazione personalizzato (per il protocollo NFS) o nome gruppo iniziatore personalizzato (per il protocollo iSCSI).
  - 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.
  - Asymmetric è vero per la piattaforma AFF e falso 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 viene creato e montato su tutti gli host.

## Creare un datastore NFS

Datastore NFS (VMware Network file System) è un tipo di storage che utilizza il protocollo NFS per connettere gli host ESXi a un dispositivo storage condiviso attraverso 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, quindi selezionare **NetApp ONTAP Tools > Create Datastore**
3. Nel riquadro **Type**, selezionare NFS in **Datastore Type**.
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 si seleziona 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 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:

- Controllare se tutti gli host di destinazione sono integri e controllare se l'host supporta il protocollo.
- Creare un nuovo volume (dimensione minima 2GB)
- Impostare le opzioni del volume con QOS
- Creare LUN di tipo VMware
- Ottenere gli iniziatori per tutti gli host di destinazione
- Crea/riutilizza igroup in base agli iniziatori corrispondenti
- Mappare il LUN a igroup
- Aggiunta di destinazioni iSCSI agli host ESXi

- Eseguire nuovamente la scansione degli HBA (host Bus Adapter) su tutti gli host
- Montare il volume come datastore VMFS6 (per oltre 6,5 host)
- Eseguire nuovamente la scansione dello storage VMFS sugli host ESXi
- Sposta il datastore nel cluster di datastore
- Ribilanciamento dei percorsi iSCSI

## 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, quindi 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 archiviazione. 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 il datastore o creare un nuovo igroup con un nome personalizzato.

Se si sceglie **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.

6. Nel riquadro degli 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.
7. Rivedere i dettagli del datastore nel riquadro **Riepilogo** e fare clic su **fine**. Il datastore viene creato e montato su tutti gli host.

# Protezione di datastore e macchine virtuali

## Abilitare SRA per proteggere i datastore

I tool ONTAP per VMware vSphere consentono di utilizzare la funzionalità SRA con i tool ONTAP per VMware vSphere per configurare il 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.
- L'adattatore SRA dovrebbe essere stato scaricato `.tar.gz` dal "[Sito di supporto NetApp](#)".

### Fasi

1. Accedere all'interfaccia di gestione delle appliance SRM utilizzando l'URL: `https://:<srm_ip>:5480`, Quindi passare a Storage Replication Adapter nell'interfaccia di gestione degli appliance di VMware SRM.
2. Selezionare **Nuova scheda**.
3. Caricare il programma di installazione di `.tar.gz` per il plug-in SRA su SRM.
4. Eseguire nuovamente la scansione delle schede per verificare che i dettagli siano aggiornati sulle schede di replica dello storage SRM pagina.

## Configurare il sistema storage per il disaster recovery

### Configurare SRA per gli ambienti SAN e NAS

È necessario configurare i sistemi di archiviazione prima di eseguire Storage Replication Adapter (SRA) per Site Recovery Manager (SRM).

### Configurare SRA per l'ambiente SAN

#### Cosa ti serve

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

- SRM

La documentazione sull'installazione di SRM è disponibile sul sito VMware.

["Documentazione di VMware Site Recovery Manager"](#)

- SRA

L'adattatore viene installato su SRM.

### Fasi

1. Verificare che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario sul sito

protetto.

2. Verificare che i LUN si trovino in igroups che dispongono di `ostype` Opzione impostata su *VMware* sul sistema di storage primario.
3. Verificare che gli host ESXi nel sito di 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, analogamente gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

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

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

## Configurare SRA per l'ambiente NAS

### Cosa ti serve

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

- SRM

La documentazione sull'installazione di SRM è disponibile sul sito VMware.

["Documentazione di VMware Site Recovery Manager"](#)

- SRA

L'adattatore viene installato su SRM 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 come l'indirizzo IP, il nome host o l'FQDN su cui sono presenti le esportazioni NFS siano specificati nel campo **NFS Addresses** (indirizzi NFS) quando si utilizza la procedura guidata Array Manager per aggiungere array a SRM.
4. Utilizzare `ping` Su ciascun host ESXi nel sito di ripristino per verificare che l'host disponga di una porta VMkernel in grado di accedere agli indirizzi IP utilizzati per le esportazioni NFS dalla SVM.

## Configurare SRA per ambienti ad elevata 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

Impostare i seguenti valori di timeout su SRM per l'ambiente in scala:

Impostazioni avanzate	Valori di timeout
-----------------------	-------------------

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

Attivare anche il `StorageProvider.autoResignatureMode` opzione.

Per ulteriori informazioni sulla modifica delle impostazioni dello Storage Provider, 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` ad un valore più alto.



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.

La documentazione VMware sulla modifica delle impostazioni DEL provider SAN contiene ulteriori informazioni.

["Documentazione di VMware Site Recovery Manager: Modifica delle impostazioni di storage"](#)

## Configurare SRA sull'appliance SRM

Dopo aver installato l'appliance SRM, è necessario configurare SRA sull'appliance SRM. La corretta configurazione di SRA consente a SRM Appliance di comunicare con SRA per la gestione del disaster recovery. È necessario archiviare gli strumenti ONTAP per le credenziali VMware vSphere (indirizzo IP) nell'appliance SRM per consentire la comunicazione tra appliance SRM 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 su appliance SRM memorizza le credenziali SRA nell'appliance SRM.

### Fasi

1. Nella schermata dell'appliance SRM, fare clic su **Storage Replication Adapter > New Adapter** (nuovo

adattatore\*).

2. Caricare il file `.tar.gz` su SRM.
3. Effettuare l'accesso utilizzando l'account amministratore al dispositivo SRM 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 log, immettere il comando per ottenere l'ID del 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 SRM con i tool 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.

9. Eseguire nuovamente la scansione delle schede per verificare che i dettagli siano aggiornati nella pagina schede di replica dello storage SRM.

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 SRM comunichi con SRA, è necessario aggiornare le credenziali SRA sul server SRM se sono state modificate.

### Cosa ti serve

Dovresti aver eseguito i passaggi descritti nell'argomento "[Configurazione di SRA sull'appliance SRM](#)"

### Fasi

1. Eseguire i seguenti comandi per eliminare la cartella macchina SRM memorizzata nella cache ONTAP Tools username password:
  - a. `sudo su <enter root password>`
  - b. `docker ps`
  - c. `docker exec -it <container_id> sh`
  - d. `cd /conf`
  - e. `rm -rf *`
2. Eseguire il comando perl per configurare SRA con le nuove credenziali:
  - a. `cd ..`
  - b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid`

<VCENTER\_GUID> È necessario disporre di un'unica citazione relativa al valore della password.

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

## Configurare siti protetti e di ripristino

### 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:

- Stessa versione di SRM installata
- 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, quindi 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 SRM deve ripristinare la macchina virtuale dalla sua destinazione.

### Cosa ti serve

- Site Recovery Manager (SRM) deve essere installato nei 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, quindi 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 **Avanti**.
4. Nella sezione Select vCenter Server (Seleziona server vCenter), procedere come segue:
  - a. Verificare che vCenter Server del sito protetto venga visualizzato come candidato corrispondente per l'associazione.
  - b. Immettere le credenziali amministrative SSO, quindi 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, quindi 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 mapping**.
  - 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, quindi 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 mapping**.
  - 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 Site Recovery Manager (SRM), 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, quindi 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 i mapping per la risorsa con i 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 mapping**.
  - 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, quindi 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, quindi 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 datastore 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 Site Recovery Manager (SRM) per abilitare le interazioni tra SRM e le macchine virtuali di storage (SVM).

### Cosa ti serve

- È necessario aver abbinato i siti protetti e i siti di ripristino in SRM.
- 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 SRM, fare clic su **Array Manager**, quindi su **Add Array Manager**.
2. Immettere le seguenti informazioni per descrivere l'array in SRM:
  - 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 array SRM.
- 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 l'ArrayPair richiesto 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

## Gestire i datastore

### 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.

#### 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 un cluster host o host, fare clic con il pulsante destro del mouse su di esso, quindi selezionare **NetApp ONTAP tools > Mount Datastores**.
5. Selezionare gli archivi dati che si desidera montare, quindi fare clic su **Mount**.

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

### Montare il datastore vVol

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.

### Ridimensionamento di 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, quindi fare clic su **OK**.

### Espandere i datastore vVol

Quando si fa clic con il pulsante destro del mouse sull'oggetto del datastore nella vista oggetto vCenter, gli strumenti ONTAP per le azioni supportate da VMware vSphere 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.

### Ridurre i 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 Remove (Rimuovi) 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, un cluster host o un datastore, quindi selezionare **NetApp ONTAP tools > Delete datastore**.



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.

- 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**.

## 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.

## Soluzioni di storage ONTAP per datastore NFS

### Fasi

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

## 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 a 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 riportate in "[Espandere i datastore vVol](#)" Sezione per aggiungere il datastore vVol e. "[Ridurre i datastore vVol](#)" per eliminare l'archivio dati.

## 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 a 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 la soglia di archiviazione

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 il 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.

### Modifica del backend dello storage

Per modificare il backend di archiviazione esistente, 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.

## Rimozione del backend dello storage

Prima di rimuovere il backend dello storage, occorre eliminare tutti gli archivi dati collegati al back-end dello storage.

Per rimuovere il 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 l'istanza di vCenter Server

I vCenter Server sono piattaforme di gestione centralizzata che consentono di controllare host, macchine virtuali e backend dello storage.

### Associare o dissociare il backend dello 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 di 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 istanze di vCenter Server 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 l'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 istanze di vCenter Server 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 l'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 istanze di vCenter Server 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, l'applicazione non le manterrà più.

## 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 a 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 **Aggiorna**



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

## Gestire i criteri di igroup ed export

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.

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 in formato tridente-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 ed esporta periodicamente i criteri.
- Se il provisioning del datastore viene eseguito a livello di cluster host, viene creato igroup con tutti gli initiator dell'host nel cluster host 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. Si consiglia di utilizzare `maint` Nome utente e password configurati durante la distribuzione per accedere alla console di manutenzione degli strumenti ONTAP. Si consiglia di utilizzare `nano` per modificare i file in manutenzione o nella console di login principale.



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

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

Menu console	Opzioni
--------------	---------

Configurazione dell'applicazione	<ol style="list-style-type: none"> <li>1. Visualizza il riepilogo dello stato del server</li> <li>2. Modificare il livello di REGISTRAZIONE per servizi provider VASA e servizi SRA</li> <li>3. Disattiva AutoSupport</li> </ol>
Configurazione del sistema	<ol style="list-style-type: none"> <li>1. Riavviare la macchina virtuale</li> <li>2. Arrestare la macchina virtuale</li> <li>3. Genera token per reimpostare la password dell'interfaccia utente del gestore</li> <li>4. Modificare il fuso orario</li> <li>5. Aggiungere un nuovo server NTP</li> <li>6. Aumentare la dimensione del disco jail (/jail)</li> <li>7. Eseguire l'upgrade</li> <li>8. Installare VMware Tools</li> </ol>
Configurazione di rete	<ol style="list-style-type: none"> <li>1. Visualizzare le impostazioni dell'indirizzo IP</li> <li>2. Visualizzare le impostazioni di ricerca dei nomi di dominio</li> <li>3. Modificare le impostazioni di ricerca dei nomi di dominio</li> <li>4. Visualizza percorsi statici</li> <li>5. Modificare i percorsi statici</li> <li>6. Eseguire il commit delle modifiche</li> <li>7. Eseguire il ping di un host</li> <li>8. Ripristinare le impostazioni predefinite</li> </ol>
Supporto e diagnostica	<ol style="list-style-type: none"> <li>1. Accedere alla shell di diagnostica</li> <li>2. Abilitare l'accesso remoto alla diagnostica</li> </ol>

## 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. Invio 4 Per selezionare Support and Diagnostics (supporto e diagnostica).
4. Invio 3 Per selezionare Enable remote Diagnostics access (attiva accesso di diagnostica remota).
5. Invio y Nella finestra di dialogo Confirmation (Conferma) per abilitare l'accesso remoto alla diagnostica.
6. Inserire una password per l'accesso remoto alla diagnostica.

## Avviare SSH su altri nodi

È necessario avviare SSH su altri nodi prima di eseguire l'aggiornamento.

### 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. Invio 4 Per selezionare Support and Diagnostics (supporto e diagnostica).
4. Invio 1 Per selezionare Accedi alla shell diagnostica.
5. Invio y per procedere.
6. Eseguire il comando `sudo systemctl restart ssh`.

## 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. Invio 4 Per selezionare Support and Diagnostics (supporto e diagnostica).
4. Invio 1 Per selezionare Accedi alla shell diagnostica.
5. Invio y per procedere.
6. Aggiornare le credenziali come richiesto:

- a. Per aggiornare le credenziali ONTAP, eseguire il comando:

```
otv-update --ontapUsername <new username> --ontapPassword <new password>
```

- b. Per aggiornare le credenziali vCenter, eseguire il comando:

```
otv-update --vcenterUsername <new username> --vcenterPassword <new password>
```

- c. Per aggiornare la LIF dati esegui il comando:

```
otv-update --dataLif <new Datalif IP>
```

## Report sui tool ONTAP

I tool ONTAP per il plug-in VMware vSphere forniscono report su macchine virtuali e datastore.

Quando si selezionano gli strumenti NetApp ONTAP per l'icona del 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 (dovrebbe 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 di vVol consentono di soddisfare i requisiti di carico di lavoro più elevati.

#### **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, quindi fare clic su **Migrate**.
2. Selezionare **Cambia solo storage**, quindi fare clic su **Avanti**.
3. Seleziona un formato di disco virtuale, una policy storage delle macchine virtuali e un datastore vVol corrispondente alle funzionalità del datastore da migrare, quindi fai clic su **Avanti**.
4. Rivedere le impostazioni, quindi 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](https://OTV_IP:8143/Register.html)
2. Verificare che il plug-in non sia più disponibile su vCenter Server.
3. Shutdown dei tool ONTAP per VMware vSphere VM
4. Elimina i tool ONTAP per VMware vSphere VM

## 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

È necessario configurare un sistema host ESXi per l'istanza di vCenter Server.

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 generare il token per reimpostare la password del gestore
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

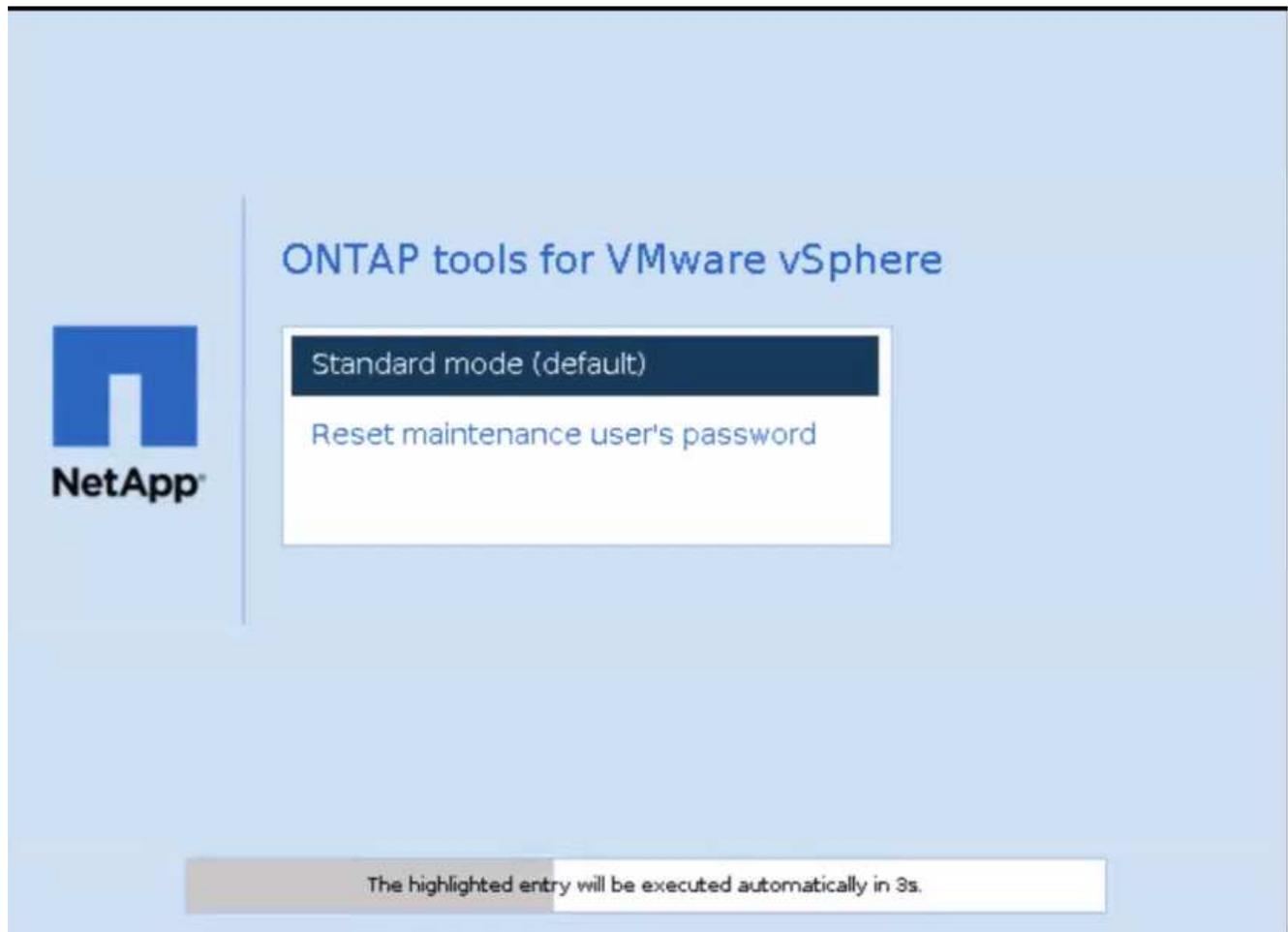
1. Avviare Gestione strumenti ONTAP da un browser Web:  
`https://loadBalanceIP:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Fare clic su **Impostazioni** dalla barra laterale.
4. Nella schermata **credenziali utente applicazione**, selezionare **Reimposta password**.
5. Fornire il nome utente, la 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 operativo guest**  
Durante il riavvio del sistema, viene visualizzata la seguente schermata:



Hai 5 secondi per scegliere la tua opzione. Premere un tasto qualsiasi per interrompere l'avanzamento e bloccare il menu 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 GRUB si apre anche durante l'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. Eliminazione di volumi da ONTAP System Manager, 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.

Esegui il seguente comando per trovare il primo nome igroup:

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

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

# Aggiornare i tool ONTAP

## Effettua l'aggiornamento alla versione più recente dei tool ONTAP

Eseguendo l'upgrade dai tool di ONTAP per VMware vSphere 10,0 a 10,1, viene creato un volume di recovery e verranno inserite tutte le informazioni necessarie nel volume di recovery. Se è necessario ripristinare la configurazione, il volume di ripristino può essere utilizzato per ripristinare i tool ONTAP per la configurazione di VMware vSphere. Se stai eseguendo un aggiornamento a livello di patch dei tool ONTAP per VMware vSphere 10,1, viene utilizzato lo stesso volume di recovery e i dettagli vengono aggiornati. L'aggiornamento è supportato per le implementazioni ha e non ha.

### Prima di iniziare

Prima di procedere con l'aggiornamento, è necessario completare i seguenti passaggi:

### 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.

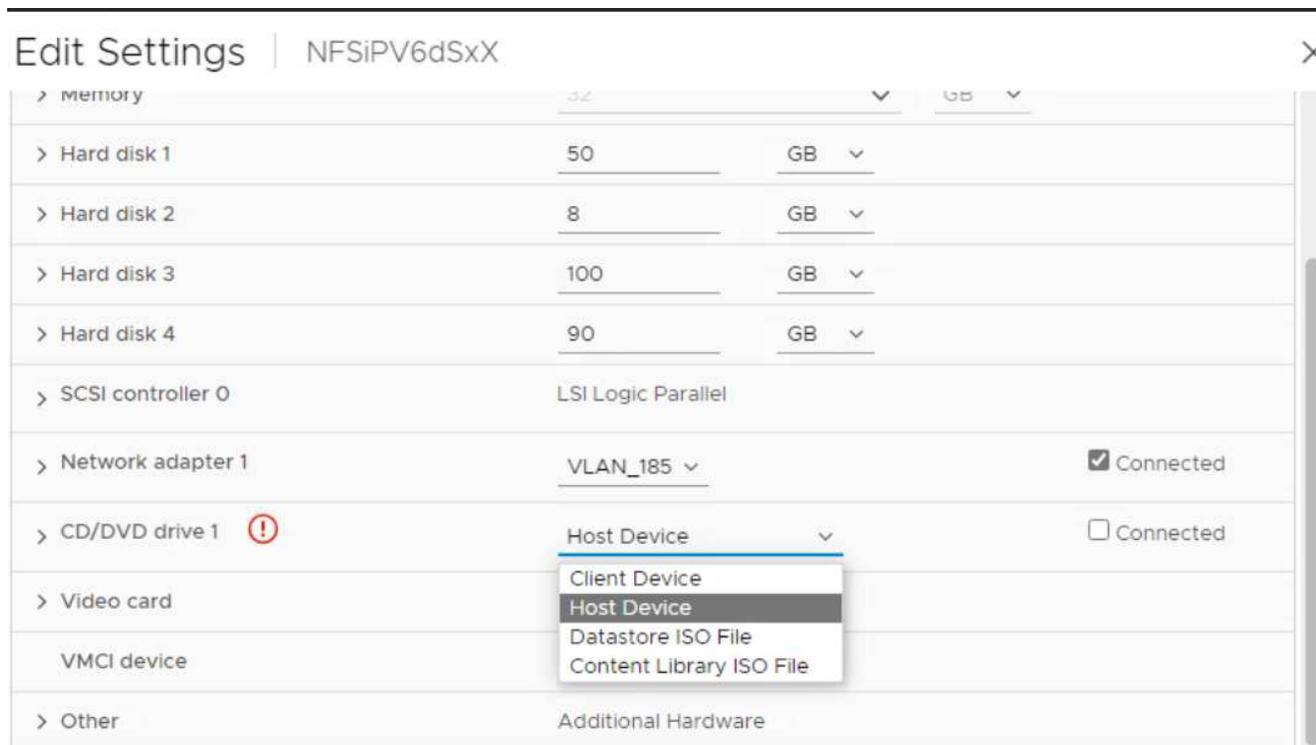
### Istantanea degli strumenti ONTAP per le VM VMware vSphere in vCenter (3VMs in caso di implementazione ha, 1 VM in caso di implementazione non ha)

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

## 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	Non riuscito. per completare i passaggi di aggiornamento da 10,0 a 10,1	Procedura di post-aggiornamento non riuscita.
088	La configurazione della rotazione del registro per il giornale non è riuscita	Riprovare a eseguire l'aggiornamento.

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

# Strumenti ONTAP per la migrazione

## Eseguire la migrazione alla versione più recente dei tool ONTAP

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.xx solo se il setup utilizza solo la funzione del provider VASA. Se disponi di datastore NVMe e di replica vVol, non è consigliato migrare ai tool ONTAP per VMware vSphere 10,1.

### A proposito di questa attività

La migrazione è supportata dai tool ONTAP per le release VMware vSphere 9.10D2, 9.11D4, 9,12 e 9,13 alla release 10,1.



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 10,1.
2. Aggiungere l'istanza di vCenter Server che si desidera migrare agli strumenti ONTAP per VMware vSphere 10,1. Vedere ["Aggiungere e gestire le istanze di vCenter Server"](#)
3. Back-end dello storage integrato a livello locale dai tool ONTAP per le API 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 10,1 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 sospenso. 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 dell'adattatore SRA nell'interfaccia utente SRM, attenersi alla seguente procedura:
  - a. Andare alla pagina di gestione della configurazione SRM

- 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 10,1 sui siti di protezione e ripristino seguendo i passaggi descritti in "[Configurare SRA sull'appliance SRM](#)"
3. Nella pagina dell'interfaccia utente SRM, 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 10,1.
3. Aggiungere l'istanza di vCenter Server che si desidera migrare agli strumenti ONTAP per VMware vSphere 10,1. Vedere "[Aggiungere un'istanza di vCenter Server](#)".
4. Back-end dello storage integrato locale dalle API 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 della richiesta per la migrazione da 9,12 e 9,13:

```
{
  "otv_ip": "10.12.13.45",
  "credenziali_provider_vasa": {
    "nome utente": "vasauser",
    "password": " "
  }
  "database_password": " "
}
```

Corpo della richiesta per un'altra migrazione delle release:

```
{
  "otv_ip": "10.12.13.45",
  "credenziali_provider_vasa": {
    "nome utente": "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",
  "stato": "in esecuzione"
}
```

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 il provider di storage VMware vSphere 10,1 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 10,1. Tutti i datastore e le macchine virtuali sono accessibili e vengono serviti dai tool ONTAP per VMware vSphere 10,1.

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",  
  "stato": "in esecuzione"  
}
```

## 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",  
  "stato": "in esecuzione"  
}
```

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 10,1 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'
```

## 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
≤	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 altre proprietà dell'oggetto utilizzando `fields` eseguire la query del parametro 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 `order_by` parametro di 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 kibble
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 bytes) o pebibyte

## 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 di documentazione dell'API ONTAP con le chiamate API organizzate in una delle principali risorse categorie in basso.

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'intero `username:password` stringa tra virgolette 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"
```

## Flussi di lavoro

### Rilevamento dello storage

L'intervallo di ricerca può essere configurato come parte della mappa di configurazione. Il rilevamento pianificato viene eseguito ogni 60 minuti. Le API fornite qui consentono di

eseguire il rilevamento on-demand per un backend dello storage specificato, aggiunto nell'ambito locale.

Utilizzare la seguente API per eseguire il rilevamento:

```
POST
/virtualization/api/v1/vcenters/{vcguid}/storage-backends/{id}/discovery-jobs
```



Vedi il workflow di back-end dello storage integrato (SVM o Cluster) e ottieni l'ID dalla risposta dell'API di back-end post-storage.

Il rilevamento da questo endpoint API è supportato solo per backend di storage con ambito locale e non per backend di storage con ambito globale.

Se il tipo di backend dello storage è cluster, il rilevamento viene eseguito implicitamente per le SVM figlio.

Se il tipo di backend dello storage è SVM, il rilevamento viene eseguito solo per la SVM selezionata.

Esempio:

Per eseguire il rilevamento su un backend di storage specificato dall'ID

```
POST
/api/v1/vcenters/3fa85f64-5717-4562-b3fc-2c963f66afa6/storage-backends/74e85f64-5717-4562-b3fc-2c963f669dde/discovery-jobs
```

È necessario passare x-auth per l'API. È possibile generare questo x-auth dalla nuova API aggiunta in Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

## Requisiti di mappatura degli aggregati delle SVM

Per utilizzare le credenziali utente delle SVM per il provisioning dei datastore, i tool ONTAP per VMware vSphere creano volumi nell'aggregato specificato nei datastore SUCCESSIVI ALLE API. ONTAP non consente la creazione di volumi su aggregati non mappati in una SVM utilizzando le credenziali utente della SVM. Per risolvere questo problema, associare le SVM agli aggregati utilizzando l'API REST o l'interfaccia CLI di ONTAP come descritto qui.

API REST ONTAP:

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

CLI ONTAP:

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

## Backend di storage integrato (SVM o Cluster) con un'istanza vCenter Server

Utilizza la seguente API per integrare i backend storage e mappare la SVM a vCenter localmente. Vedere "[Configurare i ruoli e i privilegi degli utenti ONTAP](#)" Per i privilegi utente della SVM ONTAP.

```
POST /virtualization/api/v1/vcenters/<vcguid>/storage-backends

{
  "hostname_or_ip": "172.21.103.107",
  "username": "svm11",
  "password": "xxxxxx"
}
```



L'ID della risposta API di cui sopra viene utilizzato nel rilevamento.

È necessario passare x-auth per l'API. È possibile generare questo x-auth dalla nuova API aggiunta in Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

## Creare il datastore vVol

Puoi creare un datastore vVol con nuovi volumi o con volumi esistenti. Puoi anche creare un datastore vVol con la combinazione di volumi esistenti e nuovi volumi.



Controllare che gli aggregati root non siano mappati alla SVM.

Generare un token JWT prima di creare datastore o aumentare la scadenza del token SAML impostando "durata massima token portante" su 60m su vCenter.

È necessario passare x-auth per l'API. È possibile generare questo x-auth dalla nuova API aggiunta in Auth in Swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

1. Crea un datastore vVol con un nuovo volume.

Otteni l'id aggregato, storage\_id (uuid SVM) utilizzando l'API REST di ONTAP.  
POST /Virtualization/api/v1/vcenter/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvol/datastore

Utilizzare il seguente URI per controllare lo stato:

+

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

+

Corpo della richiesta per datastore NFS

```
{  
  "nome": "nfsds1",  
  "protocollo": "nfs",  
  "platform_type": "aff",  
  "moref": "dominio-c8",  
  "volumi": [  
    {  
      "is_existing": false,  
      "name": "vol_nfs_pvt",  
      "size_in_mb": 2048000,  
      "efficienza_spazio": "sottile",  
      "aggregato": {  
        "id": "d7078b3c-3827-4ac9-9273-0a3290945c2"  
      },  
      "qos": {  
        "min_iops": 200,  
        "max_iops": 5000  
      }  
    }  
  ],  
  "storage_backend": {  
    "storage_id": "654c67bc-0f75-11ee-8a8c-00a09860a3ff"  
  }  
}
```

Corpo della richiesta per datastore iSCSI:

```
{  
  "nome": "iscsi_custom",  
  "protocollo": "iscsi",  
  "platform_type": "AFF",  
  "moref": "dominio-c8",  
  "volumi": [  
    {  
      "is_existing": falso,  
      "nome": "iscsi_custom",  
      "dimensione_in_mb": 8034,  
      "efficienza_spazio": "sottile",  
      "aggregate": {  
        "id": "54fe5d4-e461-49c8-bb2d-6d62c5d75af2"  
      }  
    }  
  ]  
}
```

```

}
}
],
"nome_igroup_personalizzato": "igroup1",
"storage_backend": {
"storage_id": "eb9d33ab-1960-11ee-9506-00a0985c6d9b" }
}

```

. Crea un datastore vVol con volumi esistenti.

Otteni `aggregate_id` e `volume_id` utilizzando l'API REST di ONTAP.

```

POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datstores
Corpo della richiesta

```

```

{
"name" : "nfsds2",
"protocol" : "nfs",
"platform_type": "aff",
"moref" : "domain-c8",
"volumes" : [
  {
    "is_existing": true,
    "id": "e632a632-1412-11ee-8a8c-00a09860a3ff"
  }
],
"storage_backend": {
  "storage_id": "33a8b6b3-10cd-11ee-8a8c-00a09860a3ff"
}

```

```

}

```

## Montare e smontare il datastore vVol

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 utilizzando le API.

Utilizzare la seguente API per montare o smontare un datastore vVol.

È necessario passare `x-auth` per l'API. È possibile generare questo `x-auth` dalla nuova API aggiunta in Auth in Swagger.

```

/virtualization/api/v1/auth/vcenter-login

```

PATCH

```
/virtualization/api/v1/vcenters/{vcguid}/vvolts/datastores/{moref}/hosts
```

Ottieni moref del datastore vVol da vCenter.

Corpo della richiesta

```
{
  "operation": "mount",
  "morefs": [
    "host-7044"
  ],
}
```

Esempi:

\* Montare su un host aggiuntivo

Utilizzare la seguente API per il montaggio su host aggiuntivo:

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvolts/datastores/datastore-24/hosts
```

Request Body

```
{
  "operation": "mount",
  "morefs": ["host-13"],
}
```

- Smontare su un host aggiuntivo

Utilizzare la seguente API per smontare l'host aggiuntivo:

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvolts/datastores/datastore-24/hosts
```

Request Body

```
{
  "operation": "unmount",
  "morefs": ["host-13"],
}
```

## Espandere o ridurre lo storage di vVol datastore

Sono previste API per aumentare o diminuire lo storage disponibile.

### Fasi

Utilizzare la seguente API per espandere o ridurre il datastore vVol:

```
PATCH
/virtualization/api/v1/vcenters/{vcguid}/v vols/datastores/{moref}/volumes
```

### Esempi

- Modificare il datastore vVol per aggiungere un nuovo volume

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/v vols/datastores/datastore-24/volumes
```

Request Body

```
{
  "operation": "grow",
  "volumes": [{
    "is_existing": false,
    "name": "exp3",
    "size_in_mb": 51200,
    "space_efficiency": "thin",
    "aggregate": {
      "id": "1466e4bf-c6d6-411a-91d5-c4f56210e1ab"
    },
    "storage_backend": {
      "storage_id": "13d86e4f-1fb1-11ee-9509-005056a75778"
    },
    "qos": {
      "max_iops": 5000
    }
  }]
}
```

- Modificare il datastore vVol per aggiungere un volume esistente

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/volumes
```

Request Body

```
{
  "operation": "grow",
  "volumes": [{
    "is_existing": true,
    "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
  }]
}
```

- Modifica il datastore vVol per rimuovere il volume ed eliminare il volume dallo storage

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=true
```

Request Body

```
{
  "operation": "shrink",
  "volumes": [{
    "is_existing": true,
    "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
  }]
}
```

- Modifica il datastore vVol per rimuovere il volume e non eliminare il volume dallo storage

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=false
```

Request Body

```
{
  "operation": "shrink",
  "volumes": [{
    "is_existing": true,
    "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
  }]
}
```

## Eliminare il datastore vVol

Esiste un datastore vVols purché almeno un volume FlexVol sia disponibile nell'archivio

dati. Se si desidera eliminare un datastore vVol in un cluster ha, è necessario prima smontare il datastore da tutti gli host all'interno del cluster ha, quindi eliminare manualmente la cartella *.vsphere-ha* residente utilizzando l'interfaccia utente del server vCenter.

## Fasi

Utilizzare la seguente API per eliminare il datastore vVol.

```
DELETE
/virtualization/api/v1/vcenters/{vcguid}/v vols/datastores/{moref}
```

## Esempi

- Elimina il datastore vVol ed elimina i volumi dallo storage

```
DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/v vols/datastores/datastore-28?delete_volumes=true
```



Delete vVol il flusso di lavoro del datastore elimina i volumi del datastore se il flag `delete_volume` è stato superato come `true`, indipendentemente dal fatto che il volume del datastore sia gestito o non gestito.

- Elimina il datastore vVol e non rimuovi volumi dallo storage

```
DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/v vols/datastores/datastore-28?delete_volumes=false
```

Risposta:

```
{
  "id": "1889"
}
```

## Gestire la soglia di archiviazione

Utilizzare l'API Get Threshold riportata di seguito per recuperare i limiti di soglia dello storage configurati per volume e aggregato.

```
GET/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

Esempi:

Otteni le soglie di storage per ogni istanza di vCenter Server di vCenter guid

```
GET "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-
thresholds"
```

Utilizzare il seguente allarme di configurazione PATCH per volume e aggregazione per generare notifica quando vengono raggiunti i limiti di soglia configurati.

```
PATCH/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

Esempi:

Update delle soglie di storage per vCenter di vCenter guid. I limiti predefiniti sono 80% per quasi pieno e 90% per pieno.

Modifica di tutte le impostazioni di soglia

```
{{{}}PATCH "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-
thresholds"
Request Body
{
"volume":

{ "nearly_full_percent": 80, "full_percent": 90 }
,
"aggregate": {
"nearly_full_percent": 80,
"full_percent": 90
}
}{}{}{}}
```

## Gestire l'accesso alla rete

Utilizzare la seguente API per aggiungere indirizzi IP per la whitelist:

```
patch /api/v1/vcenters/{vcguid}/settings/ip-whitelist
```

```
{  
  value: string  
}
```

```
GET /api/v1/vcenters/{vcguid}/settings/ip-whitelist
```

```
{  
  value: string  
}
```

# Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

## Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Direttiva sulla privacy

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

["Avviso relativo ai tool ONTAP per VMware vSphere 10,1"](#)

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

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

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

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

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

## Informazioni sul marchio commerciale

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