



## Inizia subito

SnapCenter Plug-in for VMware vSphere 6.2

NetApp  
December 09, 2025

# Sommario

Inizia subito . . . . .	1
Panoramica sull'implementazione . . . . .	1
Workflow di implementazione per gli utenti esistenti . . . . .	1
Requisiti per l'implementazione del distributore idraulico . . . . .	2
Pianificazione e requisiti dell'implementazione . . . . .	2
Privilegi ONTAP richiesti . . . . .	7
Sono richiesti privilegi minimi per vCenter . . . . .	9
Scarica Open Virtual Appliance (OVA) . . . . .	9
Implementare il plug-in SnapCenter per VMware vSphere . . . . .	10
Operazioni e problemi richiesti dopo l'implementazione . . . . .	13
Operazioni richieste dopo l'implementazione . . . . .	14
Problemi di implementazione che potrebbero verificarsi . . . . .	14
Gestire gli errori di autenticazione . . . . .	14
Registrare il plug-in SnapCenter per VMware vSphere con il server SnapCenter . . . . .	14
Accedere al client VMware vSphere di SnapCenter . . . . .	16

# Inizia subito

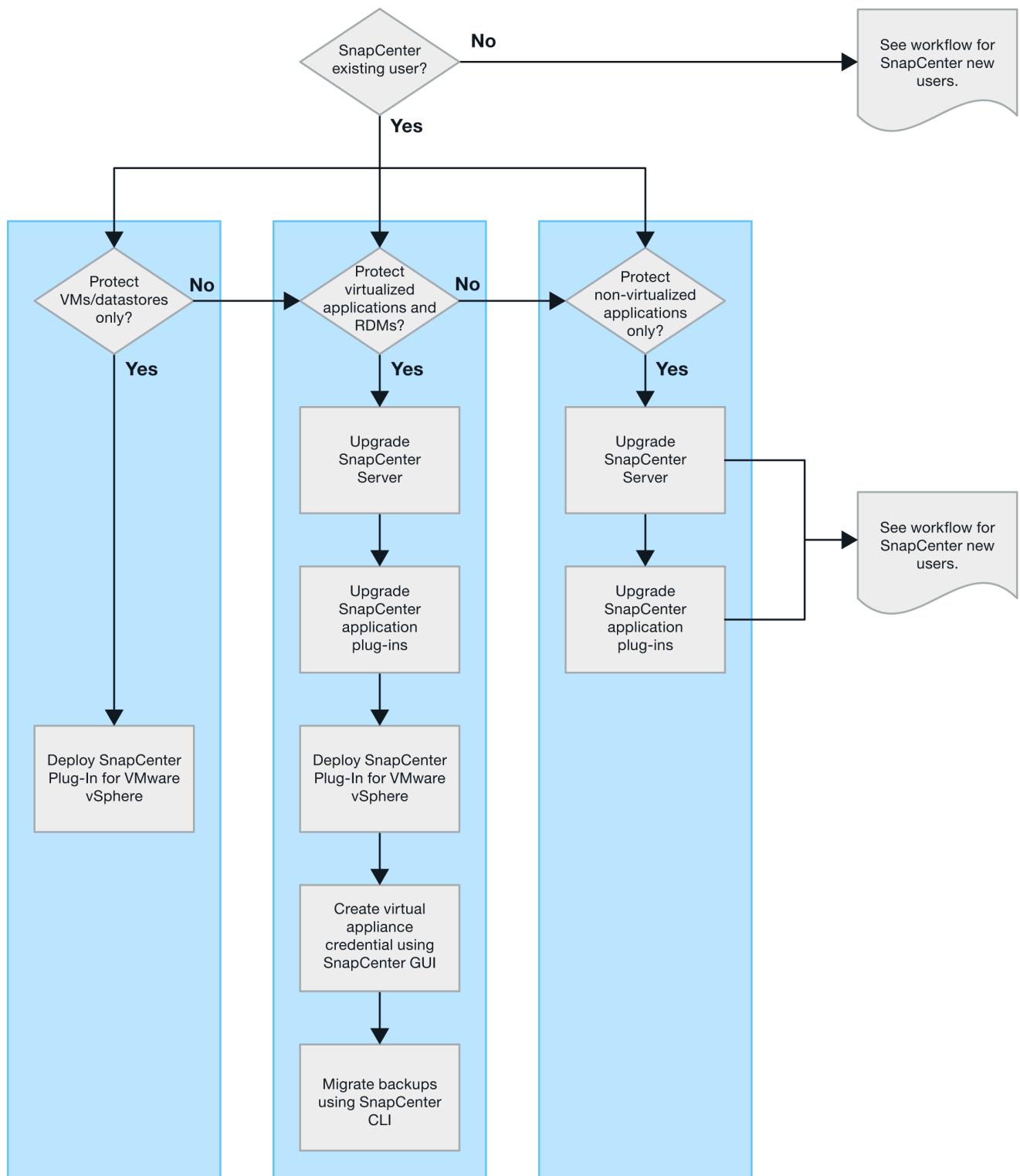
## Panoramica sull'implementazione

Per utilizzare le funzionalità di SnapCenter per proteggere macchine virtuali, datastore e database coerenti con le applicazioni su macchine virtualizzate, è necessario implementare il plug-in SnapCenter per VMware vSphere.

Gli utenti SnapCenter esistenti devono utilizzare un flusso di lavoro di implementazione diverso da quello dei nuovi utenti SnapCenter.

## Workflow di implementazione per gli utenti esistenti

Se si utilizza SnapCenter e si dispone di backup SnapCenter, utilizzare il seguente flusso di lavoro per iniziare.



## Requisiti per l'implementazione del distributore idraulico

### Pianificazione e requisiti dell'implementazione

Prima di iniziare a implementare il plug-in SnapCenter per VMware vSphere (SCV), è necessario conoscere i seguenti requisiti.

## Requisiti dell'host

Prima di iniziare l'implementazione del plug-in SnapCenter per VMware vSphere (SCV), è necessario conoscere i requisiti dell'host.

- Il plug-in SnapCenter per VMware vSphere viene implementato come macchina virtuale Linux indipendentemente dal fatto che venga utilizzato per proteggere i dati sui sistemi Windows o Linux.
- È necessario implementare il plug-in SnapCenter per VMware vSphere su vCenter Server.

Le pianificazioni di backup vengono eseguite nel fuso orario in cui viene implementato il plug-in SnapCenter per VMware vSphere e vCenter riporta i dati nel fuso orario in cui si trova. Pertanto, se il plug-in SnapCenter per VMware vSphere e vCenter si trova in fusi orari diversi, i dati del plug-in SnapCenter per la dashboard di VMware vSphere potrebbero non essere gli stessi dei dati dei report.

- Non è necessario distribuire il plug-in SnapCenter per VMware vSphere in una cartella con un nome che contiene caratteri speciali.

Il nome della cartella non deve contenere i seguenti caratteri speciali:@ n.%^&()\_+{}';, \*?"<>|

- Devi implementare e registrare un'istanza separata e univoca del plug-in SnapCenter per VMware vSphere per ogni vCenter Server.
  - Ogni vCenter Server, in modalità collegata o meno, deve essere abbinato a un'istanza separata del plug-in SnapCenter per VMware vSphere.
  - Ogni istanza del plug-in SnapCenter per VMware vSphere deve essere implementata come una VM Linux separata.

Ad esempio, si supponga di voler eseguire backup da sei istanze diverse di vCenter Server. In tal caso, è necessario implementare il plug-in SnapCenter per VMware vSphere su sei host e associare ciascun vCenter Server a un'istanza univoca del plug-in SnapCenter per VMware vSphere.

- Per proteggere le macchine virtuali vVol (macchine virtuali su datastore VMware vVol), è necessario prima implementare i tool ONTAP per VMware vSphere. I tool ONTAP consentono di eseguire il provisioning e la configurazione dello storage per vVol su ONTAP e sul client Web VMware.

Per ulteriori informazioni, fare riferimento alla documentazione degli ONTAP tools for VMware vSphere . Inoltre, fare riferimento a "[Tool di matrice di interoperabilità NetApp](#)" per informazioni aggiornate sulle versioni supportate dagli strumenti ONTAP .

- Il plug-in SnapCenter per VMware vSphere offre un supporto limitato di dispositivi PCI o PCIe condivisi (ad esempio, NVIDIA Grid GPU) a causa di un limite delle macchine virtuali che supportano Storage vMotion. Per ulteriori informazioni, consultare il documento del vendor Deployment Guide for VMware.

- Cosa è supportato:

Creazione di gruppi di risorse

Creazione di backup senza coerenza delle macchine virtuali

Ripristino di una macchina virtuale completa quando tutti i VMDK sono su un datastore NFS e il plug-in non richiede l'utilizzo di Storage vMotion

Collegamento e scollegamento dei VMDK

Montaggio e smontaggio di datastore

## Ripristino del file guest

- Cosa non è supportato:

Creazione di backup con coerenza delle macchine virtuali

Ripristino di una macchina virtuale completa quando uno o più VMDK si trovano su un datastore VMFS.

- Per un elenco dettagliato dei limiti del plug-in SnapCenter per VMware vSphere, fare riferimento a "[Note sulla versione del plug-in SnapCenter per VMware vSphere](#)".

## Requisiti di licenza

È necessario fornire le licenze per...	Requisito di licenza
ONTAP	Uno di questi: SnapMirror o SnapVault (per la protezione dei dati secondari indipendentemente dal tipo di relazione)
Prodotti aggiuntivi	vSphere Standard, Enterprise o Enterprise Plus per eseguire operazioni di ripristino con Storage vMotion è necessaria Una licenza vSphere. Le licenze vSphere Essentials o Essentials Plus non includono Storage vMotion.
Destinazioni principali	Standard SnapCenter: Necessario per eseguire la protezione basata sulle applicazioni su VMware SnapRestore: Necessario per eseguire operazioni di ripristino solo per macchine virtuali e datastore VMware: Utilizzato solo per operazioni di montaggio e collegamento su macchine virtuali e datastore VMware
Destinazioni secondarie	Standard SnapCenter: Utilizzato per le operazioni di failover per la protezione basata su applicazioni su VMware FlexClone: Utilizzato solo per le operazioni di montaggio e collegamento su macchine virtuali e datastore VMware

## Supporto software

Elemento	Versioni supportate
VCenter vSphere	7.0U1 e versioni successive.
Server ESXi	7.0U1 e versioni successive.
Indirizzi IP	IPv4, IPv6
VMware TLS	1.2, 1.3
TLS sul server SnapCenter	1.2 e 1.3 il server SnapCenter utilizza questo per comunicare con il plug-in SnapCenter per VMware vSphere per operazioni di protezione dei dati VMDK.

Elemento	Versioni supportate
Applicazione VMware vStorage API for Array Integration (VAAI)	Il plug-in SnapCenter per VMware vSphere utilizza questo metodo per migliorare le performance delle operazioni di ripristino. Inoltre, migliora le performance negli ambienti NFS.
Strumenti ONTAP per VMware	Il SnapCenter Plug-in for VMware vSphere lo utilizza per gestire i datastore vVol (volumi virtuali VMware). Per le versioni supportate, fare riferimento a <a href="#">"Tool di matrice di interoperabilità NetApp"</a> .
Amazon FSxN per l'archiviazione NetApp ONTAP	9.10 e oltre

Per le informazioni più recenti sulle versioni supportate, fare riferimento a ["Tool di matrice di interoperabilità NetApp"](#).

#### Requisiti per i protocolli NVMe su TCP e NVMe over FC

I requisiti software minimi per il supporto del protocollo NVMe over TCP e NVMe over FC sono:

- VCenter vSphere 7.0U3
- ESXi 7.0U3
- ONTAP 9.10.1

#### Requisiti di spazio, dimensionamento e scalabilità

Elemento	Requisiti
Conteggio CPU consigliato	8 core
RAM consigliata	24 GB
Spazio minimo su disco rigido per il plug-in SnapCenter per VMware vSphere, log e database MySQL	100 GB

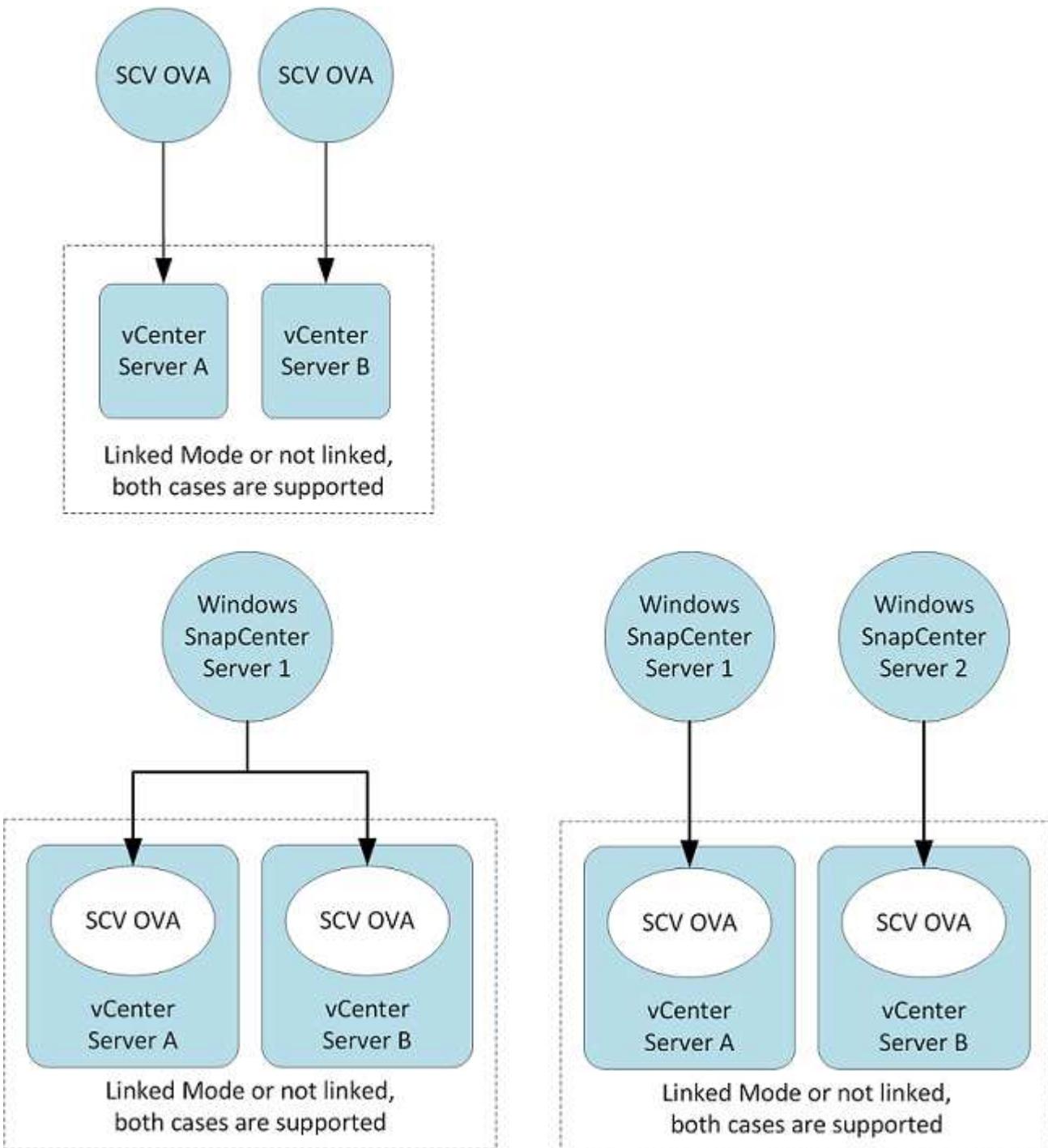
#### Requisiti di connessione e porta

Tipo di porta	Porta preconfigurata
Porta del server VMware ESXi	443 (HTTPS), bidirezionale questa porta viene utilizzata dalla funzione Ripristino file guest.
Plug-in SnapCenter per porta VMware vSphere	8144 (HTTPS), la porta bidirezionale viene utilizzata per le comunicazioni dal client VMware vSphere e dal server SnapCenter. 8080 bidirezionale questa porta viene utilizzata per gestire le appliance virtuali.  Nota: È supportata la porta personalizzata per l'aggiunta dell'host distributore idraulico a SnapCenter.
Porta di VMware vSphere vCenter Server	Se si proteggono le macchine virtuali vVol, è necessario utilizzare la porta 443.

Tipo di porta	Porta preconfigurata
Porta del cluster di storage o della VM di storage	443 (HTTPS), 80 bidirezionale (HTTP), la porta viene utilizzata per comunicare tra l'appliance virtuale e la macchina virtuale di storage o il cluster contenente la macchina virtuale di storage.

## Configurazioni supportate

Ogni istanza del plug-in supporta un solo vCenter Server, che è in modalità collegata. Tuttavia, più istanze plug-in possono supportare lo stesso server SnapCenter, come illustrato nella figura seguente.



## Privilegi RBAC richiesti

L'account amministratore di vCenter deve avere il vCenter Privileges richiesto elencato nella tabella seguente.

Per eseguire questa operazione...	È necessario disporre di questi privilegi vCenter...
Implementare e registrare il plug-in SnapCenter per VMware vSphere in vCenter	Interno: Registra interno
Aggiornare o rimuovere il plug-in SnapCenter per VMware vSphere	Interno <ul style="list-style-type: none"><li>• Aggiornare l'estensione</li><li>• Annullare la registrazione dell'interno</li></ul>
Consentire all'account utente vCenter Credential registrato in SnapCenter di convalidare l'accesso dell'utente al plug-in SnapCenter per VMware vSphere	sessions.validate.session
Consentire agli utenti di accedere al plug-in SnapCenter per VMware vSphere	SCV Administrator SCV Backup SCV Guest file Restore SCV Restore SCV View il privilegio deve essere assegnato alla radice vCenter.

## AutoSupport

Il plug-in SnapCenter per VMware vSphere fornisce un minimo di informazioni per il monitoraggio del suo utilizzo, incluso l'URL del plug-in. AutoSupport include una tabella dei plug-in installati che viene visualizzata dal visualizzatore AutoSupport.

## Privilegi ONTAP richiesti

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.



A partire dal plug-in SnapCenter per VMware (SCV) 5,0, è necessario aggiungere applicazioni di tipo HTTP e ONTAPI come metodi di accesso utente per qualsiasi utente ONTAP con accesso personalizzato basato sui ruoli al SCV. Senza l'accesso a queste applicazioni, i backup non avranno esito positivo. È necessario riavviare il servizio SCV per riconoscere le modifiche apportate ai metodi di accesso utente ONTAP.

### Sono richiesti privilegi minimi per ONTAP

Tutti i plug-in di SnapCenter richiedono i seguenti privilegi minimi.

Comandi per tutti gli accessi: ONTAP Privileges minimo.
event generate-autosupport-log
mostra la cronologia dei lavori
mostra lavoro
interruzione del lavoro

lun lun create lun delete lun igrup add lun igrup create lun igrup delete lun igrup rename lun igrup show  
lun mapping add-reporting-nodes lun mapping create lun mapping delete lun mapping remove-reporting-nodes lun mapping show lun modify lun move-in-volume lun offline lun online lun persistent-reservation clear  
lun resize serial lun lun show

elenco di destinazioni di snapmirror policy di snapmirror policy di aggiunta regola di snapmirror policy di modifica regola di snapmirror policy di rimozione regola di snapmirror policy di snapmirror di snapmirror di snapmirror show-history di snapmirror update-ls-set di snapmirror

#### Versione

Volume clone create volume clone show volume clone split start volume clone split status volume clone split volume clone split stop volume create volume delete volume distruggi volume clone create volume file show disk-use volume offline volume online volume gestito-Feature volume Modify volume qtree create volume volume create volume snapshot delete volume volume delete volume volume volume volume show volume volume show volume SnapLock-expiry-time snapshot volume snapshot restore volume snapshot restore volume show delta volume show

vserver vserver cifs share create vserver cifs share delete vserver cifs shadowcopy show vserver cifs share show vserver cifs show vserver cifs show vserver export-policy vserver export vserver policy export policy create vserver nvme

#### Comandi di sola lettura: ONTAP Privileges minimo

l'identità del cluster mostra l'interfaccia di rete mostra il vserver vserver peer vserver show

#### Comandi per tutti gli accessi: ONTAP Privileges minimo

presentazione delle unità di archiviazione del gruppo di coerenza

È possibile ignorare il comando *cluster Identity show* a livello di cluster quando si crea un ruolo da associare al Vserver dati.



È possibile ignorare i messaggi di avviso relativi ai comandi Vserver non supportati.

#### Ulteriori informazioni su ONTAP

- Per utilizzare la funzionalità di sincronizzazione attiva di SnapMirror sono necessarie ONTAP 9.12.1 o versioni successive.
- Per utilizzare la funzione di istantanea antimomanomissione (TPS):
  - È necessario ONTAP 9.13.1 e versioni successive per SAN
  - Per NFS sono necessarie ONTAP 9.12.1 e versioni successive
- Per i protocolli NVMe su TCP e NVMe over FC è necessario ONTAP 9.10.1 e versioni successive.



A partire dalla versione 9.11.1 ONTAP , la comunicazione con il cluster ONTAP avviene tramite API REST. L'utente ONTAP deve avere l'applicazione http abilitata. Tuttavia, se si riscontrano problemi con le API REST ONTAP , la chiave di configurazione 'FORCE\_ZAPI' facilita il passaggio al flusso di lavoro ZAPI tradizionale. Potrebbe essere necessario aggiungere o aggiornare questa chiave utilizzando le API di configurazione e impostarla su true. Fare riferimento all'articolo della Knowledge Base, "[Come utilizzare RestAPI per modificare i parametri di configurazione in SCV](#)" per maggiori informazioni.

## Sono richiesti privilegi minimi per vCenter

Prima di iniziare l'implementazione del plug-in SnapCenter per VMware vSphere, assicurarsi di disporre dei privilegi minimi richiesti per vCenter.

### Privilegi richiesti per il ruolo vCenter Admin

Datastore.AllocateSpace Datastore.Browse Datastore.Delete Datastore.FileManagement Datastore.Move Datastore.Rename Extension.Registrati Extension.Unregister Extension.Update host.Config.AdvancedConfig.Modify.VirtualMachine.Modif.Modif.Modif.Modif.ModificaConfig.ModificaConfig.ModificaConfig.ModificaModificaModaModaConfig.ModaModaConfig.ModaConfig.ModaConfig.ModificaConfig.ModificaModaConfig.MododaModaConfig.ModaConfig.ModaConfig.ModaConfig.ModificaConfig.ModificaConfig.ModificaConfig.ModificaModaModaModaModaConfig.ModificaModaModaModaConfig.ModalIndicalIndicaModaConfig.ModalIntermeModaModaConfig.ModificaModaModaIndicalIndicalIndicalIndicalIndicalIn

### Privilegi richiesti specifici del plug-in SnapCenter per VMware vCenter

Privilegi	Etichetta
NetappSCV.Guest.RestoreFile	Ripristino del file guest
NetappSCV.Recovery.MountUnmount	Montare/smontare
NetappSCV.Backup.DeleteBackupJob	Elimina gruppo di risorse/backup
NetappSCV.Configure.Configure.StorageSystems.Delete	Rimuovere i sistemi storage
NetappSCV.View	Visualizza
NetappSCV.Recovery.RecoverVM	Ripristinare la macchina virtuale
NetappSCV.Configure.Configure.StorageSystems.AddUpdate	Aggiungere/modificare i sistemi storage
NetappSCV.Backup.BackupNow	Esegui il backup ora
NetappSCV.Guest.Configure	Configurazione guest
NetappSCV.Configure.ConfigureSnapCenterServer	Configurare il server SnapCenter
NetappSCV.Backup.BackupScheduled	Crea gruppo di risorse

## Scarica Open Virtual Appliance (OVA)

Prima di installare Open Virtual Appliance (OVA), aggiungere il certificato a vCenter. Il file .tar contiene i certificati OVA e Entrust Root e Intermediate; i certificati si trovano nella cartella dei certificati. L'implementazione di OVA è supportata in VMware vCenter 7u1 e versioni successive.

Nelle versioni di VMware vCenter 7.0.3 e successive, l'OVA firmato dal certificato Entrust non è più attendibile. Per risolvere il problema, attenersi alla seguente procedura.

### Fasi

1. Per scaricare il plug-in SnapCenter per VMware:

- Accedere al NetApp Support Site ( "<https://mysupport.netapp.com/products/index.html>" ).
  - Dall'elenco dei prodotti, selezionare **Plug-in SnapCenter per VMware vSphere**, quindi selezionare il pulsante **Scarica ultima release**.
  - Scarica il plug-in SnapCenter per VMware vSphere .tar file in qualsiasi posizione.
2. Estrarre il contenuto del file tar. Il file tar contiene la cartella OVA e certs. La cartella certs contiene i certificati Entrust Root e Intermediate.
3. Accedere con il client vSphere al server vCenter.
4. Accedere a **Amministrazione > certificati > Gestione certificati**.
5. Accanto a **certificati principali attendibili**, selezionare **Aggiungi**
  - Accedere alla cartella *certs*.
  - Selezionare i certificati Entrust Root e Intermediate.
  - Installare ciascun certificato uno alla volta.
6. I certificati vengono aggiunti a un pannello in **certificati root attendibili**. Una volta installati i certificati, è possibile verificare e implementare OVA.



Se l'OVA scaricato non viene manomesso, nella colonna **Publisher** viene visualizzato **Trusted certificate**.

## Implementare il plug-in SnapCenter per VMware vSphere

Per utilizzare le funzionalità di SnapCenter per proteggere macchine virtuali, datastore e database coerenti con le applicazioni su macchine virtualizzate, è necessario implementare il plug-in SnapCenter per VMware vSphere.

### Prima di iniziare

Questa sezione elenca tutte le azioni necessarie da eseguire prima di iniziare la distribuzione.



L'implementazione di OVA è supportata in VMware vCenter 7u1 e versioni successive.

- Assicurati di aver esaminato i requisiti di distribuzione.
- Verificare di utilizzare una versione supportata di vCenter Server.
- Verificare che l'ambiente vCenter Server sia configurato e impostato.
- Preparare un host ESXi per il SnapCenter Plug-in for VMware vSphere VM.
- Scarica il file .tar SnapCenter Plug-in for VMware vSphere .
- Ottieni le credenziali di accesso per la tua istanza di vCenter Server.
- Ottieni un certificato con file di chiave pubblica e privata validi. Per i dettagli, vedere gli articoli nel "[Gestione dei certificati di storage](#)" sezione.
- Disconnettersi e chiudere tutte le sessioni del browser del client vSphere e cancellare la cache del browser per evitare problemi durante la distribuzione.
- Abilita Transport Layer Security (TLS) in vCenter. Fare riferimento alla documentazione VMware.
- Se si prevede di eseguire backup in vCenter diversi da quello in cui è distribuito il SnapCenter Plug-in for VMware vSphere , assicurarsi che il server ESXi, il SnapCenter Plug-in for VMware vSphere e ciascun vCenter siano sincronizzati con la stessa ora.

- Per proteggere le VM sui datastore vVol, distribuire prima gli ONTAP tools for VMware vSphere . Per le versioni degli strumenti ONTAP supportati, vedere "[Tool di matrice di interoperabilità NetApp](#)" . Gli strumenti ONTAP forniscono e configurano l'archiviazione su ONTAP e sul client Web VMware.

Implementa il plug-in SnapCenter per VMware vSphere nello stesso fuso orario di vCenter. Le pianificazioni di backup vengono eseguite nel fuso orario in cui viene implementato il plug-in SnapCenter per VMware vSphere. VCenter riporta i dati nel fuso orario in cui si trova vCenter. Pertanto, se il plug-in SnapCenter per VMware vSphere e vCenter si trova in fusi orari diversi, i dati del plug-in SnapCenter per la dashboard di VMware vSphere potrebbero non essere gli stessi dei dati dei report.

## Fasi

1. Per VMware vCenter 7.0.3 e versioni successive, seguire la procedura descritta in "[Scarica Open Virtual Appliance \(OVA\)](#)" Per importare i certificati in vCenter.
2. Nel browser, accedere a VMware vSphere vCenter.



Per i client Web HTML con indirizzo IPv6, è necessario utilizzare Chrome o Firefox.

3. Accedere alla pagina **VMware vCenter Single Sign-on**.
4. Nel riquadro del navigatore, fare clic con il pulsante destro del mouse su qualsiasi oggetto di inventario che sia un oggetto padre valido di una macchina virtuale, ad esempio un data center, un cluster o un host, e selezionare **Deploy OVF Template** per avviare la procedura guidata di distribuzione di VMware.
5. Estrarre il file .tar, che contiene il file .ova nel sistema locale. Nella pagina **Select an OVF template** (Seleziona un modello OVF), specificare la posizione di .ova file all'interno della cartella .tar estratta.
6. Selezionare **Avanti**.
7. Nella pagina **Select a name and folder** (Seleziona un nome e una cartella\*), immettere un nome univoco per la macchina virtuale o vApp, quindi selezionare un percorso di distribuzione, quindi **Next** (Avanti).

Questa operazione specifica dove importare .tar File in vCenter. Il nome predefinito per la macchina virtuale è lo stesso del nome della macchina selezionata .ova file. Se si modifica il nome predefinito, scegliere un nome univoco all'interno di ciascuna cartella VM di vCenter Server.

La posizione di implementazione predefinita per la macchina virtuale è l'oggetto di inventario in cui è stata avviata la procedura guidata.

8. Nella pagina **selezionare una risorsa**, selezionare la risorsa in cui si desidera eseguire il modello VM distribuito e selezionare **Avanti**.
9. Nella pagina **Dettagli revisione**, verificare i .tar dettagli del modello e selezionare **Avanti**.
10. Nella pagina **contratti di licenza**, selezionare la casella di controllo **Accetto tutti i contratti di licenza**.
11. Nella pagina **Select storage**, definire dove e come memorizzare i file per il modello OVF distribuito.
  - a. Selezionare il formato del disco per i VMDK.
  - b. Selezionare un criterio di storage della macchina virtuale.

Questa opzione è disponibile solo se i criteri di storage sono attivati sulla risorsa di destinazione.

- c. Selezionare un datastore per memorizzare il modello OVA implementato.

Il file di configurazione e i file dei dischi virtuali vengono memorizzati nell'archivio dati.

Selezionare un datastore di dimensioni tali da ospitare la macchina virtuale o la vApp e tutti i file dei dischi

virtuali associati.

12. Nella pagina **Select networks** (Seleziona reti), effettuare le seguenti operazioni:

- Selezionare una rete di origine e associarla a una rete di destinazione,

La colonna Source Network (rete di origine) elenca tutte le reti definite nel modello OVA.

- Nella sezione **Impostazioni allocazione IP**, selezionare il protocollo dell'indirizzo IP richiesto, quindi selezionare **Avanti**.

Il plug-in SnapCenter per VMware vSphere supporta un'unica interfaccia di rete. Se sono necessari più adattatori di rete, è necessario impostarli manualmente. Fare riferimento alla "[Articolo della Knowledge base: Come creare adattatori di rete aggiuntivi](#)".

13. Nella pagina **Personalizza modello**, effettuare le seguenti operazioni:

- Nella sezione **Register to existing vCenter** (Registra su vCenter esistente), immettere il nome vCenter e le credenziali vCenter dell'appliance virtuale.

Nel campo **vCenter username**, immettere il nome utente nel formato domain\username.

- Nella sezione **Crea credenziali SCV**, immettere le credenziali locali.

Nel campo **Nome utente**, immettere il nome utente locale; non includere i dettagli del dominio.



Annotare il nome utente e la password specificati. È necessario utilizzare queste credenziali se si desidera modificare in un secondo momento la configurazione del plug-in SnapCenter per VMware vSphere.

- Immettere le credenziali per l'utente principale.

- Nella sezione **impostazione delle proprietà di rete**, immettere il nome host.

- Nella sezione **Setup IPv4 Network Properties**, immettere le informazioni di rete quali indirizzo IPv4, maschera di rete IPv4, gateway IPv4, DNS primario IPv4, DNS secondario IPv4, e IPv4 Cerca domini.

- Nella sezione **Setup IPv6 Network Properties** (Proprietà rete \*), immettere le informazioni di rete quali l'indirizzo IPv6, la maschera di rete IPv6, il gateway IPv6, il DNS primario IPv6, il DNS secondario IPv6, e IPv6 Cerca domini.

Selezionare i campi indirizzo IPv4 o IPv6, o entrambi, se appropriato. Se si utilizzano entrambi gli indirizzi IPv4 e IPv6, specificare il DNS primario per uno solo di essi.



Se si desidera procedere con DHCP come configurazione di rete, è possibile ignorare questi passaggi e lasciare vuote le voci nella sezione **Setup Network Properties** (Impostazioni delle proprietà di rete).

- In **Setup Date and Time** (Data e ora di installazione), selezionare il fuso orario in cui si trova vCenter.

14. Nella pagina **Pronto per il completamento**, esaminare la pagina e selezionare **fine**.

Tutti gli host devono essere configurati con indirizzi IP (i nomi host FQDN non sono supportati). L'operazione di implementazione non convalida l'input prima dell'implementazione.

È possibile visualizzare lo stato di avanzamento della distribuzione dalla finestra Recent Tasks (attività

recenti) mentre si attende il completamento delle attività di importazione e distribuzione di OVF.

Quando il plug-in SnapCenter per VMware vSphere viene implementato con successo, viene implementato come macchina virtuale Linux, registrato con vCenter, e viene installato un client VMware vSphere.

15. Passare alla VM in cui è stato distribuito il plug-in SnapCenter per VMware vSphere, quindi selezionare la scheda **Riepilogo**, quindi selezionare la casella **accensione** per avviare l'appliance virtuale.
16. Durante l'accensione del plug-in SnapCenter per VMware vSphere, fare clic con il pulsante destro del mouse sul plug-in SnapCenter per VMware vSphere, selezionare **guest OS**, quindi selezionare **Install VMware Tools**.

I tool VMware sono installati sulla macchina virtuale in cui viene implementato il plug-in SnapCenter per VMware vSphere. Per ulteriori informazioni sull'installazione degli strumenti VMware, consultare la documentazione VMware.

Il completamento dell'implementazione potrebbe richiedere alcuni minuti. La distribuzione corretta è indicata quando il plug-in SnapCenter per VMware vSphere viene acceso, quando vengono installati gli strumenti VMware e la schermata richiede di accedere al plug-in SnapCenter per VMware vSphere. Durante il primo riavvio, è possibile impostare la configurazione di rete da DHCP a static. Tuttavia, il passaggio da statico a DHCP non è supportato.

Nella schermata viene visualizzato l'indirizzo IP in cui è distribuito il SnapCenter Plug-in for VMware vSphere . Prendi nota dell'indirizzo IP. Per apportare modifiche alla SnapCenter Plug-in for VMware vSphere SnapCenter Plug-in for VMware vSphere , è necessario accedere all'interfaccia utente di gestione.

17. Accedere all'interfaccia utente di gestione SnapCenter Plug-in for VMware vSphere utilizzando l'indirizzo IP visualizzato nella schermata di distribuzione e le credenziali fornite nella procedura guidata di distribuzione, quindi verificare nella Dashboard che il SnapCenter Plug-in for VMware vSphere sia connesso correttamente a vCenter e sia abilitato.

Utilizzare il formato `https://<appliance-IP-address>:8080` per accedere all'interfaccia utente di gestione.

Accedere con il nome utente e la password dell'amministratore impostati al momento dell'implementazione e il token MFA generato dalla console di manutenzione.

Se il plug-in SnapCenter per VMware vSphere non è abilitato, fare riferimento alla sezione "["Riavviare il servizio client VMware vSphere"](#)".

Se il nome host è "UnifiedVSC/SCV", riavviare l'appliance. Se il riavvio dell'appliance non modifica il nome host con il nome host specificato, è necessario reinstallare l'appliance.

#### Al termine

Completare la richiesta "["operazioni post-implementazione"](#)".

## Operazioni e problemi richiesti dopo l'implementazione

Dopo aver implementato il plug-in SnapCenter per VMware vSphere, è necessario completare l'installazione.

## Operazioni richieste dopo l'implementazione

Se sei un nuovo utente SnapCenter, devi aggiungere le VM di storage a SnapCenter prima di poter eseguire qualsiasi operazione di protezione dei dati. Quando si aggiungono VM di storage, specificare la LIF di gestione. È inoltre possibile aggiungere un cluster e specificare la LIF di gestione del cluster. Per informazioni sull'aggiunta di spazio di archiviazione, fare riferimento alla "[Aggiungere storage](#)".

## Problemi di implementazione che potrebbero verificarsi

- Dopo aver implementato l'appliance virtuale, la scheda **Backup Jobs** nella dashboard potrebbe non essere caricata nei seguenti scenari:
  - Si sta utilizzando l'indirizzo IPv4 e si dispone di due indirizzi IP per l'host VMware vSphere di SnapCenter. Di conseguenza, la richiesta di lavoro viene inviata a un indirizzo IP non riconosciuto dal server SnapCenter. Per evitare questo problema, aggiungere l'indirizzo IP che si desidera utilizzare, come indicato di seguito:
    - i. Accedere alla posizione in cui viene implementato il plug-in SnapCenter per VMware vSphere: /opt/netapp/scvservice/standalone\_aegis/etc
    - ii. Aprire la file network-interface.properties.
    - iii. In network.interface=10.10.10.10 Aggiungere l'indirizzo IP che si desidera utilizzare.
  - Hai due NIC.
- Dopo aver implementato il plug-in SnapCenter per VMware vSphere, la voce MOB del plug-in vCenter per SnapCenter per VMware vSphere potrebbe ancora mostrare il numero di versione precedente. Ciò può verificarsi quando altri job sono in esecuzione in vCenter. VCenter alla fine aggiornerà la voce.

Per correggere uno di questi problemi, procedere come segue:

1. Svuota la cache del browser e controlla se l'interfaccia utente funziona correttamente.

Se il problema persiste, riavviare il servizio client VMware vSphere

2. Accedi a vCenter, quindi seleziona **Menu** nella barra degli strumenti e seleziona **Plug-in SnapCenter per VMware vSphere**.

## Gestire gli errori di autenticazione

Se non si utilizzano le credenziali di amministratore, potrebbe essere visualizzato un errore di autenticazione dopo la distribuzione del plug-in SnapCenter per VMware vSphere o dopo la migrazione. Se si verifica un errore di autenticazione, è necessario riavviare il servizio.

### Fasi

1. Accedere all'interfaccia utente di gestione SnapCenter Plug-in for VMware vSphere utilizzando il formato `https://<appliance-IP-address>:8080`. Per effettuare l'accesso, utilizzare il nome utente amministratore, la password e i dettagli del token MFA. Il token MFA può essere generato dalla console di manutenzione.
2. Riavviare il servizio.

## Registrare il plug-in SnapCenter per VMware vSphere con il server SnapCenter

Se si desidera eseguire flussi di lavoro application-over-VMDK in SnapCenter (workflow di protezione basati su applicazioni per database e file system virtualizzati), è necessario registrare il plug-in SnapCenter per VMware

vSphere con il server SnapCenter.

## Prima di iniziare

- È necessario eseguire SnapCenter Server 4.2 o versione successiva.
- È necessario aver implementato e abilitato il plug-in SnapCenter per VMware vSphere.

## A proposito di questa attività

- È possibile registrare il SnapCenter Plug-in for VMware vSphere con SnapCenter Server utilizzando l’interfaccia utente SnapCenter per aggiungere un host di tipo "vsphere".

La porta 8144 è predefinita per la comunicazione all’interno del plug-in SnapCenter per VMware vSphere.

È possibile registrare più istanze del plug-in SnapCenter per VMware vSphere sullo stesso server SnapCenter per supportare le operazioni di protezione dei dati basate sull’applicazione sulle macchine virtuali. Non è possibile registrare lo stesso plug-in SnapCenter per VMware vSphere su più server SnapCenter.

- Per vCenter in modalità Linked, è necessario registrare il plug-in SnapCenter per VMware vSphere per ogni vCenter.

## Fasi

1. Nel riquadro di navigazione sinistro dell’interfaccia utente SnapCenter , selezionare **Host**.
2. Verificare che la scheda **host gestiti** sia selezionata nella parte superiore, quindi individuare il nome host dell’appliance virtuale e verificare che venga risolto dal server SnapCenter.
3. Selezionare **Aggiungi** per avviare la procedura guidata.
4. Nella finestra di dialogo **Aggiungi host**, specificare l’host che si desidera aggiungere al server SnapCenter come indicato nella seguente tabella:

Per questo campo...	Eseguire questa operazione...
Tipo di host	Selezionare <b>vsphere</b> come tipo di host.
Nome host	Verificare l’indirizzo IP dell’appliance virtuale.
Credenziale	Immettere il nome utente e la password per il plug-in SnapCenter per VMware vSphere fornito durante la distribuzione.

5. Selezionare **Invia**.

Una volta aggiunto correttamente l’host VM, questo viene visualizzato nella scheda Managed hosts (host gestiti).

6. Nel riquadro di spostamento di sinistra, selezionare **Impostazioni**, quindi selezionare la scheda **credenziale**, quindi selezionare **Aggiungi** per aggiungere le credenziali per il dispositivo virtuale.
7. Fornire le informazioni sulle credenziali specificate durante l’implementazione del plug-in SnapCenter per VMware vSphere.



Selezionare Linux per il campo Authentication (autenticazione).

## Al termine

Se le credenziali del plug-in SnapCenter per VMware vSphere vengono modificate, è necessario aggiornare la

registrazione nel server SnapCenter utilizzando la pagina host gestiti da SnapCenter.

## Accedere al client VMware vSphere di SnapCenter

Quando viene implementato il plug-in SnapCenter per VMware vSphere, viene installato un client VMware vSphere su vCenter, visualizzato sullo schermo di vCenter con altri client vSphere.

### Prima di iniziare

Transport Layer Security (TLS) deve essere attivato in vCenter. Consultare la documentazione VMware.

### Fasi

1. Nel browser, accedere a VMware vSphere vCenter.
2. Accedere alla pagina **VMware vCenter Single Sign-on**.



Selezionare il pulsante **accesso**. A causa di un problema VMware noto, non utilizzare il tasto INVIO per accedere. Per ulteriori informazioni, fare riferimento alla documentazione VMware relativa ai problemi del client host incorporato ESXi.

3. Nella pagina **VMware vSphere client**, selezionare Menu nella barra degli strumenti, quindi selezionare **plug-in SnapCenter per VMware vSphere**.

## **Informazioni sul copyright**

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ 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.