



Preparare l'installazione dei plug-in personalizzati di SnapCenter

SnapCenter Software 4.6

NetApp
January 18, 2024

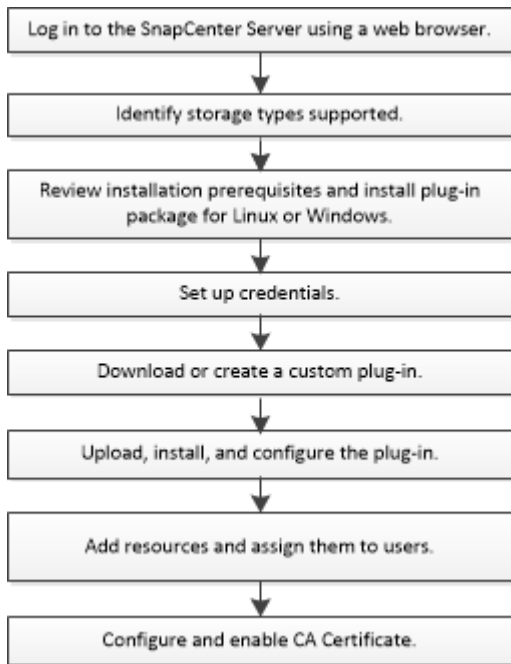
Sommario

- Preparare l'installazione dei plug-in personalizzati di SnapCenter 1
 - Workflow di installazione dei plug-in personalizzati di SnapCenter 1
 - Prerequisiti per l'aggiunta di host e l'installazione dei plug-in personalizzati di SnapCenter 1
 - Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows 2
 - Requisiti dell'host per l'installazione del pacchetto di plug-in SnapCenter per Linux 3
 - Impostare le credenziali per i plug-in personalizzati di SnapCenter 4
 - Configurare gMSA su Windows Server 2012 o versione successiva 6
 - Installare i plug-in personalizzati di SnapCenter 8
 - Configurare il certificato CA 15

Preparare l'installazione dei plug-in personalizzati di SnapCenter

Workflow di installazione dei plug-in personalizzati di SnapCenter

Se si desidera proteggere le risorse dei plug-in personalizzati, è necessario installare e configurare i plug-in personalizzati di SnapCenter.



["Sviluppare un plug-in per l'applicazione"](#)

Prerequisiti per l'aggiunta di host e l'installazione dei plug-in personalizzati di SnapCenter

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti. I plug-in personalizzati possono essere utilizzati in ambienti Windows e Linux.

- È necessario aver creato un plug-in personalizzato. Per ulteriori informazioni, consultare le informazioni per gli sviluppatori.

["Sviluppare un plug-in per l'applicazione"](#)

- Se si desidera gestire applicazioni MySQL o DB2, è necessario aver scaricato i plug-in personalizzati MySQL e DB2 forniti da NetApp.
- È necessario aver installato Java 1.8 a 64 bit sull'host Linux o Windows.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.

- I plug-in personalizzati devono essere disponibili sull'host client da cui viene eseguita l'operazione di aggiunta dell'host.

Generale

Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.

Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto.
- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.

Host Linux

- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java a 1.8 64 bit sull'host Linux.

Se si utilizza Windows 2019 o Windows 2016 per l'host del server SnapCenter, è necessario installare Java 1.8 a 64 bit. Lo strumento matrice di interoperabilità (IMT) contiene le informazioni più recenti sui requisiti.

["Download Java per tutti i sistemi operativi"](#)

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

- Per consentire l'accesso a diversi percorsi, è necessario configurare i privilegi sudo per l'utente non root. Aggiungere le seguenti righe al file /etc/sudoers usando l'utility visudo Linux. Ad esempio,


```
Cmnd_Alias SCCMD = /opt/NetApp/snapcenter/scc/bin/scc <non_root_user>
ALL=(ALL) NOPASSWD:SETENV: SCCMD
```

non_root_user è il nome dell'utente non root creato.

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp" .

Elemento	Requisiti
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB  È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.5.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva <p>Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp".</p>

Requisiti dell'host per l'installazione del pacchetto di plug-in SnapCenter per Linux

Assicurarsi che l'host soddisfi i requisiti prima di installare il pacchetto di plug-in SnapCenter per Linux.

Elemento	Requisiti
Sistemi operativi	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	1 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB  È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	Java 1.8 (64 bit) Oracle Java o OpenJDK Flavors Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in <code>/var/opt/snapcenter/spl/etc/spl.properties</code> sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, consultare ["Tool di matrice di interoperabilità NetApp"](#)

Impostare le credenziali per i plug-in personalizzati di SnapCenter

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati su database o file system Windows.

Cosa ti serve

- Host Linux

È necessario impostare le credenziali per l'installazione dei plug-in sugli host Linux.

Per installare e avviare il processo di plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root che dispone dei privilegi di sudo.

Best practice: sebbene sia consentito creare credenziali per Linux dopo l'implementazione degli host e l'installazione dei plug-in, la Best practice consiste nel creare credenziali dopo l'aggiunta di SVM, prima di distribuire host e installare plug-in.

- Host Windows

Prima di installare i plug-in, è necessario impostare le credenziali di Windows.

È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

- Applicazioni plug-in personalizzate

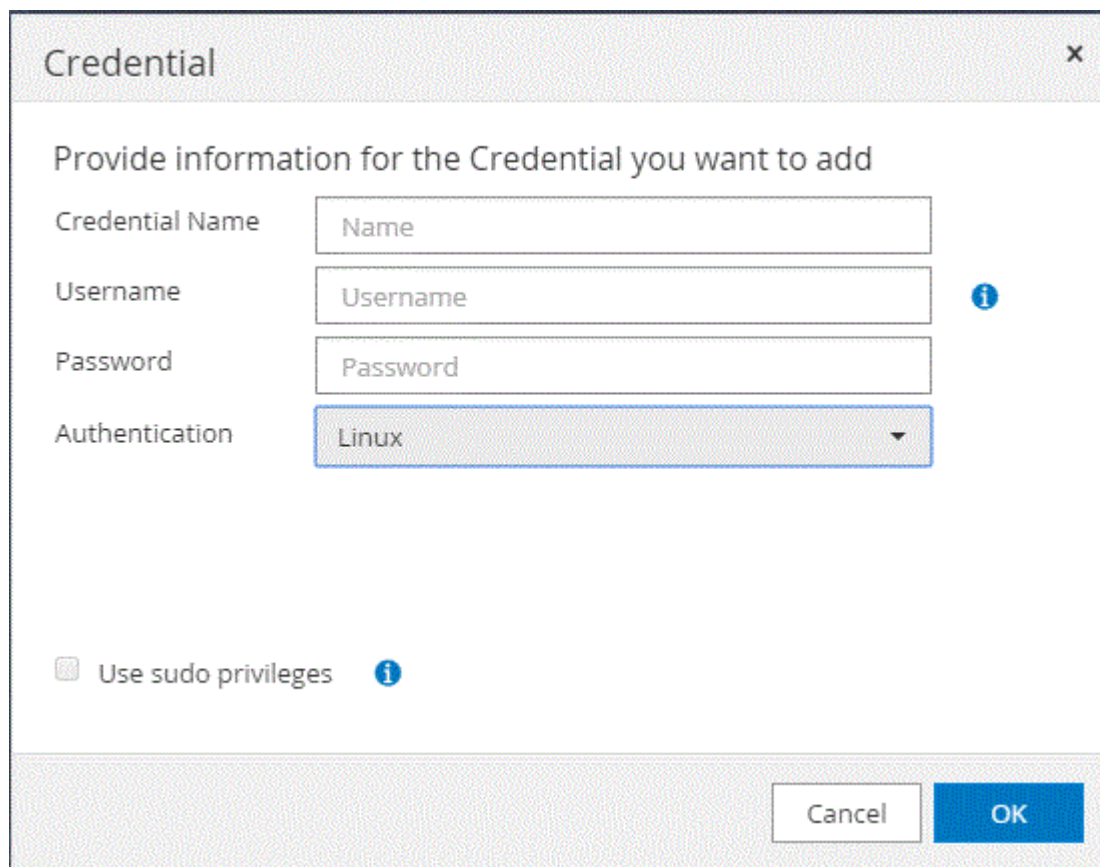
Il plug-in utilizza le credenziali selezionate o create durante l'aggiunta di una risorsa. Se una risorsa non richiede credenziali durante le operazioni di protezione dei dati, è possibile impostare le credenziali su **None**.

A proposito di questa attività

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.


Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.



4. Nella pagina credenziale, specificare le informazioni necessarie per la configurazione delle credenziali:

Per questo campo...	Eeguire questa operazione...
Nome della credenziale	Immettere un nome per le credenziali.

Per questo campo...	Eeguire questa operazione...
Nome utente	<p>Immettere il nome utente e la password da utilizzare per l'autenticazione.</p> <ul style="list-style-type: none"> • Amministratore di dominio o qualsiasi membro del gruppo di amministratori <p>Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori nel sistema in cui si installa il plug-in SnapCenter. I formati validi per il campo Nome utente sono:</p> <ul style="list-style-type: none"> ◦ <i>NetBIOS/nome utente</i> ◦ <i>Dominio FQDN/nome utente</i> • Amministratore locale (solo per gruppi di lavoro) <p>Per i sistemi appartenenti a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si installa il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locali se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata sul sistema host. Il formato valido per il campo Nome utente è: <i>Nome utente</i></p>
Password	Inserire la password utilizzata per l'autenticazione.
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare.
Utilizzare i privilegi sudo	<p>Selezionare la casella di controllo Usa privilegi sudo se si stanno creando credenziali per un utente non root.</p> <p> Applicabile solo agli utenti Linux.</p>

5. Fare clic su **OK**.

Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina User and Access (utenti e accesso).

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio

gestito.

Cosa ti serve

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Creare e configurare gMSA:
 - a. Creare un account di gruppo utenti nel seguente formato:

```
domainName\accountName$  
.. Aggiungere oggetti computer al gruppo.  
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

Ad esempio,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Eseguire `Get-ADServiceAccount` per verificare l'account del  
servizio.
```

4. Configurare gMSA sugli host:
 - a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

A tale scopo, eseguire il seguente comando da PowerShell:

```

PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                               Name                               Install State
-----
[ ] Active Directory Domain Services      AD-Domain-Services              Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
-----
True      No                Success      {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.

```

- a. Riavviare l'host.
- b. Installare gMSA sull'host eseguendo il seguente comando dal prompt dei comandi di PowerShell:
`Install-AdServiceAccount <gMSA>`
- c. Verificare l'account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`
5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Installare i plug-in personalizzati di SnapCenter

Aggiungere host e installare pacchetti plug-in su host remoti

Utilizzare la pagina SnapCenterAdd host per aggiungere host e installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare i pacchetti plug-in per un singolo host o per un cluster.

Cosa ti serve

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

["Configurare l'account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per le applicazioni personalizzate"](#)


A proposito di questa attività


Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.

Se si installano plug-in su un cluster (WSFC), i plug-in vengono installati su tutti i nodi del cluster.


Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:



Per questo campo...	Eseguire questa operazione...
Tipo di host	<p>Selezionare il tipo di host:</p> <ul style="list-style-type: none">• Windows• Linux <p> I plug-in personalizzati possono essere utilizzati in ambienti Windows e Linux.</p>
Nome host	<p>Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.</p> <p>SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN.</p> <p>Per gli ambienti Windows, l'indirizzo IP è supportato per gli host di dominio non attendibili solo se viene risolto nell'FQDN.</p> <p>È possibile inserire gli indirizzi IP o il nome FQDN di un host standalone.</p> <p>Se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.</p>

Per questo campo...	Eeguire questa operazione...
Credenziali	<p>Selezionare il nome della credenziale creata o creare nuove credenziali.</p> <p>Le credenziali devono disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali.</p> <p>È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.</p> </div>

5. Nella sezione **Seleziona plug-in da installare**, selezionare i plug-in da installare.
6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo...	Eeguire questa operazione...
Porta	<p>Mantenere il numero di porta predefinito oppure specificare il numero di porta.</p> <p>Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.</p> </div>

Per questo campo...	Eeguire questa operazione...
<p>Percorso di installazione</p>	<p>I plug-in personalizzati possono essere installati su un sistema Windows o Linux.</p> <ul style="list-style-type: none"> • Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: <p>In alternativa, è possibile personalizzare il percorso.</p> <ul style="list-style-type: none"> • Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/NetApp/snapcenter. <p>In alternativa, è possibile personalizzare il percorso.</p> <ul style="list-style-type: none"> • Per i plug-in personalizzati di SnapCenter: <ul style="list-style-type: none"> i. Nella sezione Custom Plug-in (Plug-in personalizzati), fare clic su Browse (Sfogliala) e selezionare la cartella dei plug-in personalizzati compressi. <p>La cartella zippata contiene il codice del plug-in personalizzato e il file .xml descrittore.</p> <p>Per Storage Plug-in, accedere a <i>C:/ProgramData/NetApp/SnapCenter/Package Repository</i> e selezionare <i>Storage.zip</i> cartella.</p> <ul style="list-style-type: none"> ii. Fare clic su carica. <p>Il file .xml descrittore nella cartella dei plug-in personalizzati compressi viene validato prima del caricamento del pacchetto.</p> <p>Vengono elencati i plug-in personalizzati caricati sul server SnapCenter.</p> <p>Se si desidera gestire applicazioni MySQL o DB2, è possibile utilizzare i plug-in personalizzati MySQL e DB2 forniti da NetApp. I plug-in personalizzati MySQL e DB2 sono disponibili sul sito "NetApp Automation Store"</p>
<p>Ignorare i controlli di preinstallazione</p>	<p>Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.</p>

Per questo campo...	Eeguire questa operazione...
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	<p>Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in.</p> <p> Fornire il nome gMSA nel seguente formato: Nome dominio/nome account.</p> <p> GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.</p>

7. Fare clic su **Invia**.

Se non è stata selezionata la casella di controllo **Salta precheck**, l'host viene validato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) sono validati in base ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in C: File di programma NetApp SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.



In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).



La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

I file di log specifici dell'installazione si trovano in /custom_location/snapcenter/logs.

Installare i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage PowerShell.

Cosa ti serve

L'utente che aggiunge un host deve disporre dei diritti amministrativi sull'host.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet `Open-SmConnection`, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet `Install-SmHostPackage` e i parametri richiesti.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, fare riferimento alla ["Guida di riferimento al cmdlet del software SnapCenter"](#).

È possibile utilizzare l'opzione `-skipprecheck` quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserire le credenziali per l'installazione remota.

Installare i plug-in personalizzati di SnapCenter sugli host Linux utilizzando l'interfaccia della riga di comando

Installare i plug-in personalizzati di SnapCenter utilizzando l'interfaccia utente di SnapCenter. Se l'ambiente in uso non consente l'installazione remota del plug-in dall'interfaccia utente di SnapCenter, è possibile installare i plug-in personalizzati in modalità console o in modalità silenziosa utilizzando l'interfaccia a riga di comando (CLI).

Fasi

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (`Snapcenter_linux_host_plugin.bin`) da `C: ProgramData/NetApp SnapCenter/Package Repository` all'host in cui si desidera installare i plug-in personalizzati.

È possibile accedere a questo percorso dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato copiato il file di installazione.
3. Installare il plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin`
`-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address`
`-DSERVER_HTTPS_PORT=port_number_for_server`
 - `-DPORT` specifica la porta di comunicazione HTTPS SMCORE.
 - `-DSERVER_IP` specifica l'indirizzo IP del server SnapCenter.
 - `-DSERVER_HTTPS_PORT` specifica la porta HTTPS del server SnapCenter.
 - `-DUSER_INSTALL_DIR` specifica la directory in cui si desidera installare il pacchetto di plug-in SnapCenter per Linux.
 - `DINSTALL_LOG_NAME` specifica il nome del file di log.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento alla "[Guida di riferimento al cmdlet del software SnapCenter](#)".

5. Accedere a SnapCenter e caricare il plug-in personalizzato dall'interfaccia utente o utilizzando i cmdlet PowerShell.

È possibile caricare il plug-in personalizzato dall'interfaccia utente facendo riferimento a. "[Aggiungere host e installare pacchetti plug-in su host remoti](#)" sezione.

La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell.






"[Guida di riferimento al cmdlet del software SnapCenter](#)".

Monitorare lo stato di installazione dei plug-in personalizzati

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

-  In corso
-  Completato correttamente
-  Non riuscito
-  Completato con avvisi o impossibile avviarlo a causa di avvisi
-  In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione del plug-in, attenersi alla seguente procedura:
 - a. Fare clic su **Filter** (filtro).

- b. Facoltativo: Specificare la data di inizio e di fine.
 - c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
 - d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
 - e. Fare clic su **Apply** (Applica).
4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
 5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

Per informazioni su come generare una CSR, vedere ["Come generare il file CSR del certificato CA"](#).



Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file > Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console > certificati – computer locale > autorità di certificazione root attendibili > certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks > Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata...	Effettuare le seguenti operazioni...
Importa chiave privata	Selezionare l'opzione Sì , importare la chiave privata, quindi fare clic su Avanti .
Formato del file di importazione	Non apportare modifiche; fare clic su Avanti .
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su Avanti .
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su fine per avviare l'importazione.



Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12, *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
 - a. Fare doppio clic sul certificato.
 - b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
 - c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
 - d. Copiare i caratteri esadecimali dalla casella.
 - e. Rimuovere gli spazi tra i numeri esadecimali.

Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
 - a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

```
Get-ChildItem -Path Certate: LocalMachine/My
```

- b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Ad esempio:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associare il certificato appena installato ai servizi plug-in
dell'host Windows eseguendo i seguenti comandi:
```

```
> $cert = "<certificate thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
```

Ad esempio:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Configurare il certificato CA per il servizio plug-in personalizzati di SnapCenter sull'host Linux

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file 'keystore.jks', che si trova in `/opt/NetApp/snapcenter/scc/etc` sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
keytool -storepasswd -keystore keystore.jks  
. Modificare la password per tutti gli alias delle chiavi private nel  
keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.



La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato: */Opt/NetApp/snapcenter/scc/ecc*.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere un certificato root o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Riavviare il servizio dopo aver configurato i certificati root o  
intermedi in un archivio di trust plug-in personalizzato.
```



Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato */opt/NetApp/snapcenter/scc/ecc*.

2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere il certificato CA con chiave pubblica e privata.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Elencare i certificati aggiunti nel keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks  
. Se il nome alias nel certificato CA è lungo e contiene spazi o  
caratteri speciali ("*", ",", "), modificare il nome alias con un nome  
semplice:
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks  
. Configurare il nome alias del certificato CA nel file  
agent.properties.
```

Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è 'opt/NetApp/snapcenter/scc/etc/crl'.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Configurare il certificato CA per il servizio plug-in personalizzati di SnapCenter sull'host Windows

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file *keystore.jks*, che si trova in `_C: File di programma NetApp, SnapCenter, Snapcenter Plug-in Creator, ecc.`, sia come archivio di fiducia che come archivio chiavi.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Modificare la password del keystore:

```
keytool -storepasswd -keystore keystore.jks
```



Se il comando "keytool" non viene riconosciuto dal prompt dei comandi di Windows, sostituire il comando keytool con il relativo percorso completo.

```
C: File di programma Java <jdk_version> keytool.exe" -storepasswd -keystore keystore.jks
```

3. Modificare la password per tutti gli alias delle chiavi private nel keystore con la stessa password utilizzata per il keystore:

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave *KEYSTORE_PASS* nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.



La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato `_C: File di`

programma/NetApp/SnapCenter/Snapcenter Plug-in Creator

2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere un certificato root o intermedio:

```
Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in un archivio di trust plug-in personalizzato.



Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file *keystore.jks*.
3. Elencare i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere il certificato CA con chiave pubblica e privata.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Elencare i certificati aggiunti nel keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file *agent.properties*.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

8. Configurare il nome alias del certificato CA nel file *agent.properties*.

Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- Per scaricare il file CRL più recente per il certificato CA correlato, vedere ["Come aggiornare il file dell'elenco di revoca dei certificati nel certificato CA di SnapCenter"](#).
- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è `_C:` File di programma, NetApp, SnapCenter, SnapCenter Plug-in Creator, ecc.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave `CRL_PATH`.
2. È possibile inserire più file CRL in questa directory.

I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Cosa ti serve

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.





Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento alla ["Guida di riferimento al cmdlet del software SnapCenter"](#).

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

-  Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
-  Indica che il certificato CA è stato validato correttamente.
-  Indica che non è stato possibile validare il certificato CA.
-  indica che non è stato possibile recuperare le informazioni di connessione.



Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

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

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

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

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

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

Informazioni sul marchio commerciale

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