



# Install il plug-in SnapCenter per Microsoft Windows

## SnapCenter software

NetApp  
November 06, 2025

This PDF was generated from [https://docs.netapp.com/it-it/snapcenter-61/protect-scw/concept\\_install\\_snapcenter\\_plug\\_in\\_for\\_microsoft\\_windows.html](https://docs.netapp.com/it-it/snapcenter-61/protect-scw/concept_install_snapcenter_plug_in_for_microsoft_windows.html) on November 06, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

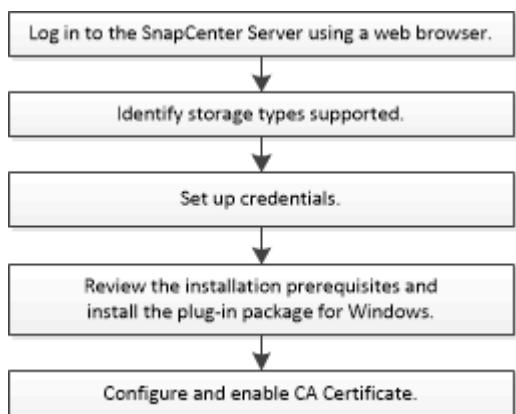
# Sommario

Installa il plug-in SnapCenter per Microsoft Windows .....	1
Flusso di lavoro di installazione del plug-in SnapCenter per Microsoft Windows .....	1
Requisiti di installazione per il plug-in SnapCenter per Microsoft Windows .....	1
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows .....	1
Imposta le tue credenziali per il plug-in per Windows .....	2
Configurare gMSA su Windows Server 2016 o versioni successive .....	4
Aggiungi host e installa il plug-in SnapCenter per Microsoft Windows .....	5
Installa il plug-in SnapCenter per Microsoft Windows su più host remoti utilizzando i cmdlet di PowerShell .....	9
Installare il plug-in SnapCenter per Microsoft Windows in modo silenzioso dalla riga di comando .....	9
Monitorare lo stato di installazione del pacchetto plug-in SnapCenter .....	11
Configurare il certificato CA .....	12
Genera file CSR del certificato CA .....	12
Importa certificati CA .....	12
Ottieni l'impronta digitale del certificato CA .....	13
Configurare il certificato CA con i servizi plug-in host di Windows .....	13
Abilita i certificati CA per i plug-in .....	14

# Installare il plug-in SnapCenter per Microsoft Windows

## Flusso di lavoro di installazione del plug-in SnapCenter per Microsoft Windows

Se si desidera proteggere i file di Windows che non sono file di database, è necessario installare e configurare il plug-in SnapCenter per Microsoft Windows.



## Requisiti di installazione per il plug-in SnapCenter per Microsoft Windows

Prima di installare il plug-in per Windows, è necessario conoscere alcuni requisiti di installazione.

Prima di iniziare a utilizzare il plug-in per Windows, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Per installare il plug-in per Windows è necessario disporre dei privilegi di amministratore SnapCenter . Il ruolo di amministratore SnapCenter deve disporre di privilegi di amministratore.
- È necessario aver installato e configurato SnapCenter Server.
- 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 disabilitare UAC sull'host.
- Se si desidera la replica del backup, è necessario configurare SnapMirror e SnapVault .

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

Articolo	Requisiti
Sistemi operativi	<p>Microsoft Windows</p> <p>Per le informazioni più recenti sulle versioni supportate, vedere "<a href="#">Strumento matrice di interoperabilità NetApp</a>".</p> <p>Se si utilizza un cluster Windows, è necessario installare e configurare anche Windows Remote Management (WinRM).</p>
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host	<p>5 GB</p> <p></p> <p>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati.</p>
Pacchetti software richiesti	<ul style="list-style-type: none"> <li>• Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Per le informazioni più recenti sulle versioni supportate, vedere "<a href="#">Strumento matrice di interoperabilità NetApp</a>".</p> <p>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "<a href="#">L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet</a>".</p>

## Imposta le tue credenziali per il plug-in per Windows

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

### Cosa ti servirà

- 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.

- Se si impostano credenziali per singoli gruppi di risorse e l'utente non dispone di privilegi di amministratore completi, è necessario assegnare all'utente almeno i privilegi di gruppo di risorse e di backup.

## Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, procedi come segue:

Per questo campo...	Fai questo...
Nome della credenziale	Inserisci un nome per le credenziali.
Nome utente/Password	<p>Inserisci il nome utente e la password utilizzati per l'autenticazione.</p> <ul style="list-style-type: none"><li>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori</li></ul> <p>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono i seguenti:</p> <ul style="list-style-type: none"><li>◦ NetBIOS\UserName</li><li>◦ Domain FQDN\UserName</li><li>◦ UserName@upn</li></ul> <ul style="list-style-type: none"><li>• Amministratore locale (solo per gruppi di lavoro)</li></ul> <p>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è il seguente: UserName</p> <p>Non utilizzare virgolette doppie ("") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (&lt;) e punto esclamativo (!) nelle password. Ad esempio, lessthan&lt;!10, lessthan10&lt;!, backtick`12.</p>

Per questo campo...	Fai questo...
Password	Inserisci la password utilizzata per l'autenticazione.

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

### Prima di iniziare

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

### Passi

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -Effectivelmmediately
3. Crea e configura il tuo gMSA:
  - a. Crea un account di gruppo utenti nel seguente formato:

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

Per esempio,

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

4. Configurare gMSA sui tuoi host:

- a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

Per fare ciò, 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. Riavvia il tuo host.
  - b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell:  
`Install-AdServiceAccount <gMSA>`
  - c. Verifica il tuo 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 .

SnapCenter Server 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.

## Aggiungi host e installa il plug-in SnapCenter per Microsoft Windows

È possibile utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host Windows. Il plug-in SnapCenter per Microsoft Windows viene installato automaticamente sull'host specificato. Questo è il metodo consigliato per installare i plug-in. È possibile aggiungere un host e installare un plug-in per un singolo host o per un cluster.

### Prima di iniziare

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disininstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- 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 disabilitare UAC sull'host.
- L'utente SnapCenter dovrebbe essere aggiunto al ruolo "Accedi come servizio" di Windows Server.
  - È necessario 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 del servizio gestito del gruppo su Windows Server 2016 o versioni successive per Windows File System"](#)

### Informazioni su questo compito

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.
- Plug-in di Windows
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installazione di plug-in su un cluster

Se si installano plug-in su un cluster (WSFC, Oracle RAC o Exchange DAG), questi vengono installati su tutti i nodi del cluster.

- Archiviazione serie E

Non è possibile installare il plug-in per Windows su un host Windows connesso all'archiviazione serie E.



SnapCenter non supporta l'aggiunta dello stesso host (host plug-in) a SnapCenter se l'host fa già parte di un gruppo di lavoro ed è stato modificato in un altro dominio o viceversa. Se si desidera aggiungere lo stesso host, è necessario rimuoverlo da SnapCenter e aggiungerlo nuovamente.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Assicurarsi che in alto sia selezionato **Host gestiti**.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, procedi come segue:

Per questo campo...	Fai questo...
Tipo di host	<p>Selezionare il tipo di host <b>Windows</b>.</p> <p>SnapCenter Server aggiunge l'host e quindi installa il plug-in per Windows se non è già installato sull'host.</p>

Per questo campo...	Fai questo...
Nome host	<p>Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.</p> <p>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).</p> <p>È possibile immettere gli indirizzi IP o il nome di dominio completo di uno dei seguenti:</p> <ul style="list-style-type: none"> <li>• Host autonomo</li> <li>• Clustering di failover di Windows Server (WSFC)</li> </ul> <p>Se si aggiunge un host tramite SnapCenter e fa parte di un sottodominio, è necessario fornire l'FQDN.</p>
Credenziali	<p>Seleziona il nome delle credenziali che hai creato oppure creane di nuove.</p> <p>La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, vedere le informazioni sulla creazione di una credenziale.</p> <p>I dettagli sulle credenziali, tra cui nome utente, dominio e tipo di host, vengono visualizzati posizionando il cursore sul nome della credenziale fornito.</p> <div style="display: flex; align-items: center;"> <span data-bbox="878 1275 931 1332"></span> <div data-bbox="985 1233 1432 1364"> <p>La modalità di autenticazione è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.</p> </div> </div>

5. Nella sezione Selezione plug-in da installare, seleziona i plug-in da installare.

Per le nuove distribuzioni non sono elencati pacchetti plug-in.

6. (Facoltativo) Fare clic su **Altre opzioni**.

Per questo campo...	Fai questo...
Porta	<p>Mantenere il numero di porta predefinito oppure specificare il numero di porta.</p> <p>Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.</p> <p> Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce.</p>
Percorso di installazione	<p>Il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter.</p> <p>Facoltativamente, è possibile personalizzare il percorso. Per il pacchetto plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Tuttavia, se lo desideri, puoi personalizzare il percorso predefinito.</p>
Aggiungi tutti gli host nel cluster	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC.
Salta i controlli pre-installazione	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.
Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in	<p>Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.</p> <p>Fornire il nome gMSA nel seguente formato: <i>nomedominio\nameaccount\$</i>.</p> <p> gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in in SnapCenter per il servizio Windows.</p>

## 7. Fare clic su **Invia**.

Se non hai selezionato la casella di controllo **Salta controlli preliminari**, l'host verrà convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET e la posizione vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Program Files\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. Monitorare l'avanzamento dell'installazione.

# Installare il plug-in SnapCenter per Microsoft Windows su più host remoti utilizzando i cmdlet di PowerShell

Se si desidera installare il plug-in SnapCenter per Microsoft Windows su più host contemporaneamente, è possibile farlo utilizzando `Install-SmHostPackage` Cmdlet di PowerShell.

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare i plug-in.

### Passi

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando `Open-SmConnection` cmdlet, quindi immettere le credenziali.
3. Aggiungere l'host autonomo o il cluster a SnapCenter utilizzando `Add-SmHost` cmdlet 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, puoi anche fare riferimento a "[Guida di riferimento ai cmdlet del software SnapCenter](#)".

4. Installare il plug-in su più host utilizzando `Install-SmHostPackage` cmdlet e i parametri richiesti.

Puoi usare il `-skipprecheck` opzione quando hai installato i plug-in manualmente e non vuoi verificare se l'host soddisfa i requisiti per installare il plug-in.

# Installare il plug-in SnapCenter per Microsoft Windows in modo silenzioso dalla riga di comando

Se non è possibile installare il plug-in in remoto dall'interfaccia utente grafica SnapCenter SnapCenter , è possibile installarlo localmente su un host Windows. È possibile eseguire il programma di installazione del plug-in SnapCenter per Microsoft Windows senza intervento dell'utente, in modalità silenziosa, dalla riga di comando di Windows.

### Prima di iniziare

- È necessario aver installato ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) Hosting Bundle.
- È necessario aver installato PowerShell 7.4.2 o versione successiva.

- Devi essere un amministratore locale sull'host.

## Passi

1. Scarica il plug-in SnapCenter per Microsoft Windows dal percorso di installazione.

Ad esempio, il percorso di installazione predefinito è C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.

2. Copiare il file di installazione sull'host su cui si desidera installare il plug-in.
3. Dal prompt dei comandi, accedi alla directory in cui hai scaricato il file di installazione.
4. Inserisci il seguente comando, sostituendo le variabili con i tuoi dati:

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log"""
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
ISFeatureInstall=SCW
```

Per esempio:

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent / debuglog"C:
\HPPW_SCW_Install.log" /log"C:\\" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW`
```



Tutti i parametri passati durante l'installazione del plug-in per Windows sono sensibili alle maiuscole e alle minuscole.

Inserisci i valori per le seguenti variabili:

Variabile	Valore
/debuglog"<Percorso_registro_debug>	Specificare il nome e il percorso del file di registro del programma di installazione della suite, come nell'esempio seguente: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Specificare la porta su cui SnapCenter comunica con SMCore.
SUITE_INSTALLDIR	Specificare la directory di installazione del pacchetto plug-in host.
BI_SERVICEACCOUNT	Specificare il plug-in SnapCenter per l'account del servizio Web di Microsoft Windows.

Variabile	Valore
BI_SERVICEPWD	Specificare la password per l'account del servizio Web SnapCenter Plug-in per Microsoft Windows.
ISFeatureInstall	Specificare la soluzione da distribuire tramite SnapCenter sull'host remoto.

Il parametro *debuglog* include il percorso del file di registro per SnapCenter. La scrittura in questo file di registro è il metodo preferito per ottenere informazioni sulla risoluzione dei problemi, poiché il file contiene i risultati dei controlli eseguiti dall'installazione per i prerequisiti del plug-in.

Se necessario, è possibile trovare ulteriori informazioni sulla risoluzione dei problemi nel file di registro del pacchetto SnapCenter per Windows. I file di registro per il pacchetto sono elencati (dal più vecchio) nella cartella %Temp%, ad esempio, C:\temp\.



L'installazione del plug-in per Windows registra il plug-in sull'host e non sul server SnapCenter. È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Dopo aver aggiunto l'host, il plug-in viene rilevato automaticamente.

## Monitorare lo stato di installazione del pacchetto plug-in SnapCenter

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

### Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
  - a. Fare clic su **Filtro**.
  - b. Facoltativo: specificare la data di inizio e di fine.

- c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
  - d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
  - e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
  5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera 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 sarà associata una chiave privata.

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



La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

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



Se possiedi il certificato CA per il tuo dominio (\*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (\*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

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

#### Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File > Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root > Certificati – Computer locale > Autorità di certificazione radice attendibili > Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività > Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata...	Procedi come segue...
Importa chiave privata	Selezionare l'opzione <b>Sì</b> , importare la chiave privata, quindi fare clic su <b>Avanti</b> .
Formato file di importazione	Non apportare modifiche; fare clic su <b>Avanti</b> .
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su <b>Avanti</b> .
Completamento della procedura guidata di importazione del certificato	Rivedi il riepilogo, quindi fai clic su <b>Fine</b> per avviare l'importazione.



Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: \*.pfx, \*.p12 e \*.p7b).

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

## Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

### Passi

1. Eseguire le seguenti operazioni sulla GUI:
  - Fare doppio clic sul certificato.
  - Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
  - Scorri l'elenco dei campi e clicca su **Impronta digitale**.
  - Copia i caratteri esadecimali dalla casella.
  - Rimuovere gli spazi tra i numeri esadecimali.

Ad esempio, se l'impronta digitale 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: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
  - Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

```
Get-ChildItem -Percorso Cert:\LocalMachine\My
```

- Copia l'impronta digitale.

## Configurare il certificato CA con i servizi plug-in host di Windows

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

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

#### Passi

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>
```

Per esempio:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associare il certificato appena installato ai servizi plug-in host di
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"
```

Per esempio:

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

## Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

#### Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *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, puoi anche fare riferimento a "[Guida di riferimento ai cmdlet del software SnapCenter](#)".

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.

4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

#### Dopo aver finito

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

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



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

## **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.