Installare il plug-in SnapCenter per Microsoft Windows

SnapCenter Software 4.6

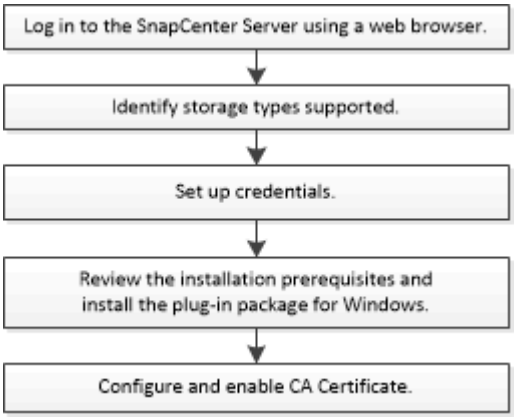
NetApp
January 18, 2024

Sommario

Installare il plug-in SnapCenter per Microsoft Windows

Workflow di installazione del plug-in SnapCenter per Microsoft Windows

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



Requisiti di installazione del 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 di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività dei prerequisiti.

- Per installare il plug-in per Windows, è necessario disporre dei privilegi di amministratore di SnapCenter.

  Il ruolo di amministratore di SnapCenter deve disporre dei privilegi di amministratore.

- È necessario aver installato e configurato il server 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 disattivare il controllo dell'account utente sull'host.
- Se si desidera eseguire la replica di backup, è necessario configurare SnapMirror e SnapVault.

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".
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	• Microsoft .NET Framework 4.5.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp".

Impostare le credenziali per il plug-in per Windows

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

Cosa ti serve

- 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 le credenziali per singoli gruppi di risorse e l'utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup all'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 Credential, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.
Nome utente/Password	Immettere il nome utente e la password utilizzati per l'autenticazione. • Amministratore di dominio o qualsiasi membro del gruppo di amministratori 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 i seguenti: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Amministratore locale (solo per gruppi di lavoro) 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 il seguente: `UserName` Non utilizzare virgolette doppie (") o backtick (`) nelle password. Non utilizzare il valore inferiore a (<) e il punto esclamativo (!) simboli insieme nelle password. Ad esempio, meno di<!10, meno di 10<!, backtick`12.
Password	Inserire la password utilizzata per l'autenticazione.

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.

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.

Aggiungere host e installare 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.

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.
- 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.
- L'utente SnapCenter deve essere aggiunto al ruolo "accesso come servizio" del server Windows.
- 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 il file system di Windows"

A proposito di questa attività

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

- Storage e-Series

  Non è possibile installare il plug-in per Windows su un host Windows connesso allo storage e-series.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Assicurarsi che nella parte superiore sia selezionato **Managed hosts**.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare il tipo di host **Windows**. Il server SnapCenter aggiunge l'host e installa il plug-in per Windows, se non è già installato sull'host.
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire il nome di dominio completo (FQDN). È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi: • Host standalone • Clustering di failover di Windows Server (WSFC) Se si aggiunge un host utilizzando SnapCenter e fa parte di un sottodominio, è necessario fornire l'FQDN.
Credenziali	Selezionare il nome della credenziale creata o creare le nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere la sezione relativa alla creazione di una credenziale. I dettagli relativi alle credenziali, inclusi nome utente, dominio e tipo di host, vengono visualizzati posizionando il cursore sul nome della credenziale fornito. La modalità di autenticazione è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.

   Per le nuove implementazioni, non sono elencati pacchetti plug-in.

6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. 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. 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.
Percorso di installazione	Il percorso predefinito è C:/Program Files/NetApp/SnapCenter. È possibile personalizzare il percorso. Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: File di programma. Tuttavia, se lo si desidera, è possibile personalizzare il percorso predefinito.
Aggiungere tutti gli host nel cluster	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC.
Ignorare i controlli di preinstallazione	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 di gruppo (gMSA) per eseguire i servizi plug-in	Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: *Domainname/accountName*. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo **Salta precheck**, l'host viene validato 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 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 all'indirizzo `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 PowerShell

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

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando `Open-SmConnection` cmdlet, quindi immettere le credenziali.
3. Aggiungere l'host standalone 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, fare riferimento alla "Guida di riferimento al cmdlet del software SnapCenter".

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

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

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

È possibile installare il plug-in SnapCenter per Microsoft Windows localmente su un host Windows se non si riesce a installare il plug-in in remoto dall'interfaccia grafica di SnapCenter. È possibile eseguire il plug-in SnapCenter per il programma di installazione

di Microsoft Windows senza supervisione, in modalità silenziosa, dalla riga di comando di Windows.

Cosa ti serve

- È necessario aver installato Microsoft .Net 4.5.2 o versione successiva.
- PowerShell 4.0 o versione successiva deve essere installato.
- È necessario aver attivato la funzione di accodamento dei messaggi di Windows.
- È necessario essere un amministratore locale dell'host.

Fasi

1. Scaricare 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 il server SnapCenter.

2. Copiare il file di installazione nell'host su cui si desidera installare il plug-in.
3. Dal prompt dei comandi, accedere alla directory in cui è stato scaricato il file di installazione.
4. Immettere il seguente comando, sostituendo le variabili con i dati:

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

   Ad 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 al maiuscolo/minuscolo.

   Inserire i valori per le seguenti variabili:

Variabile	Valore
/debuglog"<Debug_Log_Path>	Specificare il nome e la posizione del file di log del programma di installazione della suite, come nell'esempio seguente: setup.exe /debuglog"C: PathToLog setupexe.log".

Variabile	Valore
PORTA_BI_SNAPCENTER	Specificare la porta su cui SnapCenter comunica con SMCore.
SUITE_INSTALLDIR	Specificare la directory di installazione del pacchetto del plug-in host.
BI_SERVICEACCOUNT	Specificare il plug-in SnapCenter per l'account del servizio Web Microsoft Windows.
BI_SERVICEPWD	Specificare la password per l'account del servizio Web di SnapCenter per il plug-in Microsoft Windows.
ISFeatureInstall	Specificare la soluzione da implementare da SnapCenter sull'host remoto.

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

Se necessario, è possibile trovare ulteriori informazioni per la risoluzione dei problemi nel file di registro del pacchetto SnapCenter per Windows. I file di log per il pacchetto sono elencati (per primi quelli meno recenti) nella cartella *%Temp%*, ad esempio _C:.

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 utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Una volta aggiunto l'host, il plug-in viene rilevato automaticamente.

Monitorare lo stato di installazione del pacchetto plug-in SnapCenter

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"
   ```

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

Informazioni sul marchio commerciale