# Preparare l'installazione del plug-in SnapCenter per Microsoft SQL Server

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-49/protect-scsql/task_install_snapcenter_plug_in_for_microsoft_sql_server_database.html on September 26, 2025. Always check docs.netapp.com for the latest.

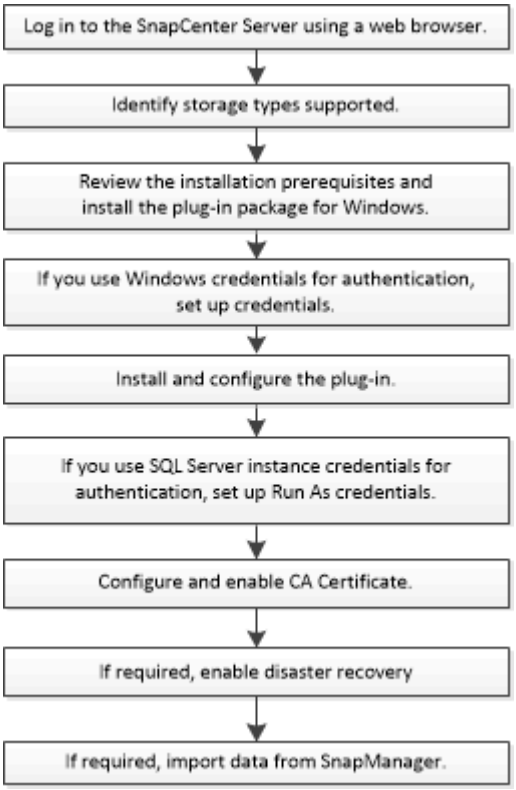
# Sommario


Preparare l'installazione del plug-in SnapCenter per Microsoft SQL Server . . . 1
- Workflow di installazione del plug-in SnapCenter per Microsoft SQL Server . . . 1
- Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft SQL Server . . . 1
- Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows . . . 2
- Impostare le credenziali per il pacchetto di plug-in SnapCenter per Windows . . . 3
- Configurare le credenziali per una singola risorsa SQL Server . . . 4
  - Fase 1: Aggiungere e configurare le credenziali . . . 5
  - Fase 2: Configurare le istanze . . . 6
- Configurare gMSA su Windows Server 2012 o versione successiva . . . 7
- Installare il plug-in SnapCenter per Microsoft SQL Server . . . 8
  - Aggiungere host e installare il pacchetto di plug-in SnapCenter per Windows . . . 8
  - Installare il plug-in SnapCenter per Microsoft SQL Server su più host remoti utilizzando i cmdlet . . . 12
  - Installare il plug-in SnapCenter per Microsoft SQL Server in modo invisibile dalla riga di comando . . . 12
  - Monitorare lo stato di installazione del plug-in per SQL Server . . . 13
- Configurare il certificato CA . . . 14
  - Generare il file CSR del certificato CA . . . 14
  - Importare i certificati CA . . . 15
  - Ottenere il thumbprint del certificato CA . . . 15
  - Configurare il certificato CA con i servizi plug-in dell'host Windows . . . 16
  - Abilitare i certificati CA per i plug-in . . . 17
- Configurare il disaster recovery . . . 17
  - Disaster recovery del plug-in SnapCenter per SQL Server . . . 17
  - Disaster recovery (DR) dello storage per il plug-in SnapCenter per SQL Server . . . 18
  - Failback dal plug-in SnapCenter per lo storage secondario SQL Server allo storage primario . . . 19

# Preparare l’installazione del plug-in SnapCenter per Microsoft SQL Server

## Workflow di installazione del plug-in SnapCenter per Microsoft SQL Server

Se si desidera proteggere i database di SnapCenter, è necessario installare e configurare il plug-in di SQL Server.




## Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft SQL Server

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario disporre di un utente 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.
- È necessario disporre di un utente con autorizzazioni sysadmin su SQL Server.

  Il plug-in SnapCenter per Microsoft SQL Server utilizza Microsoft VDI Framework, che richiede l’accesso sysadmin.

"Articolo di supporto Microsoft 2926557: Le operazioni di backup e ripristino VDI di SQL Server richiedono privilegi di amministratore di sistema"

- 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 SnapManager per Microsoft SQL Server è installato, è necessario aver arrestato o disattivato il servizio e le pianificazioni.

  Se si prevede di importare processi di backup o clonazione in SnapCenter, non disinstallare SnapManager per Microsoft SQL Server.

- L'host deve essere risolvibile con il nome di dominio completo (FQDN) dal server.

  Se il file hosts viene modificato in modo da renderlo risolvibile e se nel file hosts sono specificati sia il nome breve che l'FQDN, creare una voce nel file hosts di SnapCenter nel seguente formato: <ip_address> <host_fqdn> <host_name>

# 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<br><br>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<br><br>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. |

| Elemento | Requisiti |
| --- | --- |
| Pacchetti software richiesti | • Microsoft .NET Framework 4.7.2 o versione successiva<br>• Windows Management Framework (WMF) 4.0 o versione successiva<br>• PowerShell 4.0 o versione successiva<br><br>Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp".<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet." |

# Impostare le credenziali per il pacchetto di plug-in SnapCenter per Windows

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.

**Prima di iniziare**

- 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.
- Autenticazione SQL su host Windows

  È necessario impostare le credenziali SQL dopo l'installazione dei plug-in.

  Se si implementa il plug-in SnapCenter per Microsoft SQL Server, è necessario impostare le credenziali SQL dopo l'installazione dei plug-in. Impostare una credenziale per un utente con autorizzazioni sysadmin di SQL Server.

  Il metodo di autenticazione SQL esegue l'autenticazione con un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere rilevata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. È necessaria l'autenticazione di SQL Server per eseguire operazioni come la pianificazione o il rilevamento delle risorse.

**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… | Eseguire questa operazione… |
| --- | --- |
| Nome della credenziale | Immettere un nome per la credenziale. |
| Nome utente/Password | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio<br>Specificare l'amministratore di dominio sul sistema su cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono:<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>• Amministratore locale (solo per gruppi di lavoro)<br>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: `UserName`<br>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. |
| Modalità di autenticazione | Selezionare la modalità di autenticazione che si desidera utilizzare. Se si seleziona la modalità di autenticazione SQL, è necessario specificare anche l'istanza di SQL Server e l'host in cui si trova l'istanza SQL. |

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 le credenziali per una singola risorsa SQL Server

È possibile configurare le credenziali per eseguire processi di protezione dei dati su una

singola risorsa SQL Server per ciascun utente. Sebbene sia possibile configurare le credenziali a livello globale, è possibile eseguire questa operazione solo per una risorsa specifica.

**A proposito di questa attività**

- Se si utilizzano credenziali Windows per l'autenticazione, è necessario impostare le credenziali prima di installare i plug-in.

  Tuttavia, se si utilizza un'istanza di SQL Server per l'autenticazione, è necessario aggiungere la credenziale dopo l'installazione dei plug-in.

- Se è stata attivata l'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database rilevato viene visualizzato con un'icona a forma di lucchetto di colore rosso.

  Se viene visualizzata l'icona del lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.

- È necessario assegnare la credenziale a un utente RBAC (role-based access control) senza accesso sysadmin quando vengono soddisfatte le seguenti condizioni:
  - La credenziale viene assegnata a un'istanza SQL.
  - L'istanza o l'host SQL viene assegnato a un utente RBAC.

    L'utente deve disporre sia del gruppo di risorse che dei privilegi di backup.

## Fase 1: Aggiungere e configurare le credenziali

1. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni**.
2. Nella pagina Impostazioni, selezionare **credenziale**.
   a. Per aggiungere una nuova credenziale, selezionare **nuovo**.
   b. Nella pagina credenziale, configurare le credenziali:

| Per questo campo… | Eseguire questa operazione… |
| --- | --- |
| Nome della credenziale | Immettere un nome per le credenziali. |

| Per questo campo… | Eseguire questa operazione… |
| --- | --- |
| Nome utente | Immettere il nome utente utilizzato per l'autenticazione di SQL Server.<br>• 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:<br>◦ *NetBIOS/nome utente*<br>◦ *Dominio FQDN/nome utente*<br>• 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 l'utente La funzione di controllo degli accessi è disattivata sul sistema host. Il formato valido per il campo **Nome utente** è: *Nome utente* |
| Password | Inserire la password utilizzata per l'autenticazione. |
| Modalità di autenticazione | Selezionare la modalità di autenticazione di SQL Server. È inoltre possibile scegliere l'autenticazione di Windows se l'utente Windows dispone dei privilegi di amministratore di sistema sul server SQL. |
| Host | Selezionare l'host. |
| Istanza di SQL Server | Selezionare l'istanza di SQL Server. |

c. Selezionare **OK** per aggiungere la credenziale.

## Fase 2: Configurare le istanze

1. Nel riquadro di navigazione a sinistra, selezionare **risorse**.
2. Nella pagina Resources (risorse), selezionare **Instance** (istanza) dall'elenco **View** (Visualizza).
   a. Selezionare , quindi selezionare il nome host per filtrare le istanze.
   b. Selezionare per chiudere il riquadro del filtro.
3. Nella pagina protezione istanza, proteggere l'istanza e, se necessario, selezionare **Configura credenziali**.

   Se l'utente che ha effettuato l'accesso al server SnapCenter non ha accesso al plug-in SnapCenter per Microsoft SQL Server, l'utente deve configurare le credenziali.

   L'opzione credenziale non si applica ai database e ai gruppi di disponibilità.

4. Selezionare **Aggiorna risorse**.

# 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.

**Prima di iniziare**

- 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 il plug-in SnapCenter per Microsoft SQL Server

## Aggiungere host e installare il pacchetto di plug-in SnapCenter per Windows

Utilizzare la pagina SnapCenter **Aggiungi host** per aggiungere host e installare il pacchetto dei plug-in. I plug-in vengono installati automaticamente sugli host remoti.

**Prima di iniziare**

- 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, è necessario disattivare il controllo dell'account utente sull'host.
- 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 account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per SQL"

**A proposito di questa attività**

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

È possibile aggiungere un host e installare i pacchetti plug-in per un singolo host o per un cluster. Se si installano i plug-in su un cluster o su un cluster di failover di Windows Server (WSFC), i plug-in vengono installati su tutti i nodi del cluster.

Per informazioni sulla gestione degli host, vedere "Gestire gli host".

**Fasi**

1. Nel riquadro di navigazione a sinistra, selezionare **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Selezionare **Aggiungi**.
4. Nella pagina hosts:

| Per questo campo… | Eseguire questa operazione… |
|---|---|
| Tipo di host | Selezionare Windows come tipo di host. Il server SnapCenter aggiunge l'host, quindi installa il plug-in per Windows se il plug-in non è già installato sull'host.<br><br>Se si seleziona l'opzione Microsoft SQL Server nella pagina Plug-in, il server SnapCenter installa il plug-in per SQL Server. |
| Nome host | Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. L'indirizzo IP è supportato per gli host di dominio non attendibili solo se viene risolto nell'FQDN.<br><br>SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN.<br><br>È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi:<br><br>• Host standalone<br>• WSFC Se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN. |

| Per questo campo… | Eseguire questa operazione… |
| --- | --- |
| Credenziali | Selezionare il nome della credenziale creata o creare nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali.<br><br>È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

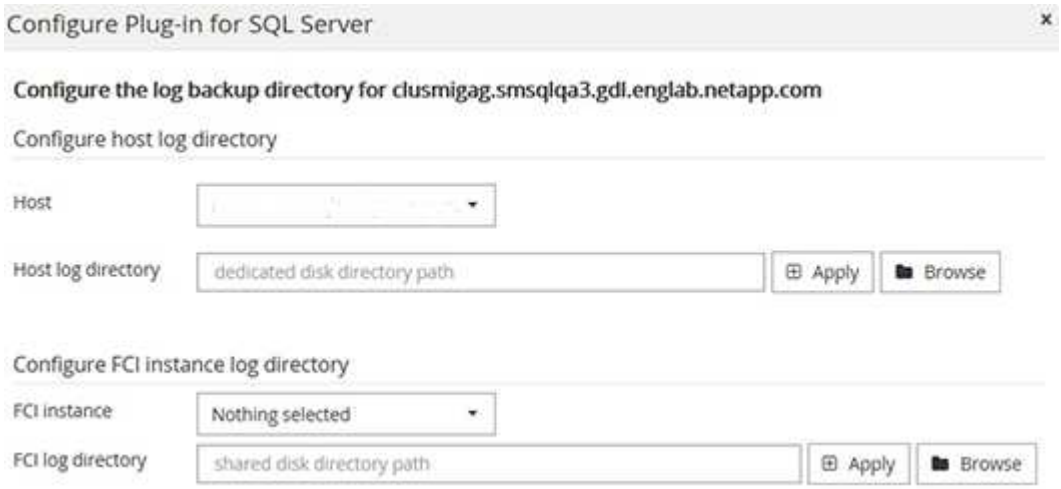
5. Nella sezione **Seleziona plug-in da installare**, selezionare i plug-in da installare.
6. Selezionare **altre opzioni**.

| 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.<br><br>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. |
| Aggiungere tutti gli host nel cluster | Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC o in un gruppo di disponibilità SQL. Per gestire e identificare più gruppi di disponibilità SQL disponibili all'interno di un cluster, è necessario aggiungere tutti i nodi del cluster selezionando la casella di controllo cluster appropriata nella GUI. |
| 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. |

| Per questo campo… | Eseguire questa operazione… |
| --- | --- |
| 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.<br><br>Fornire il nome gMSA nel seguente formato: Nome dominio/nome account.<br><br>Se l'host viene aggiunto con gMSA e gMSA dispone dei privilegi di login e di amministratore di sistema, gMSA verrà utilizzato per connettersi all'istanza SQL. |

7. Selezionare **Invia**.
8. Per il plug-in SQL, selezionare l'host per configurare la directory del registro.
   a. Selezionare **Configure log directory** e nella pagina Configure host log directory, selezionare **Browse** (Sfoglia) e completare la seguente procedura:

      Solo i LUN (dischi) NetApp sono elencati per la selezione. SnapCenter esegue il backup e replica della directory del registro host come parte dell'operazione di backup.




      i. Selezionare la lettera dell'unità o il punto di montaggio sull'host in cui verrà memorizzato il log dell'host.
      ii. Scegliere una sottodirectory, se necessario.
      iii. Selezionare **Salva**.
9. Selezionare **Invia**.

   Se non è stata selezionata la casella di controllo **Ignora 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, 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.

10. Monitorare l'avanzamento dell'installazione.

## Installare il plug-in SnapCenter per Microsoft SQL Server su più host remoti utilizzando i cmdlet

È possibile installare il plug-in SnapCenter per Microsoft SQL Server su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage PowerShell.

**Prima di iniziare**

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 il pacchetto del plug-in.

**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 SnapCenter per Microsoft SQL Server su più host remoti 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 anche a "Guida di riferimento al cmdlet del software SnapCenter".

   È possibile utilizzare l'opzione -skipprecheck quando 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.

4. Inserire le credenziali per l'installazione remota.

## Installare il plug-in SnapCenter per Microsoft SQL Server in modo invisibile dalla riga di comando

Installare il plug-in SnapCenter per Microsoft SQL Server dall'interfaccia utente di SnapCenter. Tuttavia, se per qualche motivo non è possibile eseguire il programma di installazione del plug-in per SQL Server in modalità automatica dalla riga di comando di Windows.

**Prima di iniziare**

- Prima di eseguire l'installazione, è necessario eliminare la versione precedente del plug-in SnapCenter per Microsoft SQL Server.

  Per ulteriori informazioni, vedere "Come installare un plug-in SnapCenter manualmente e direttamente dall'host del plug-in".

**Fasi**

1. Verificare se la cartella C:/temp esiste sull'host del plug-in e se l'utente connesso ha accesso completo a tale cartella.
2. Scaricare il plug-in per il software SQL Server da C: ProgramData/NetApp/SnapCenter/Package Repository.

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

3. Copiare il file di installazione nell'host su cui si desidera installare il plug-in.
4. Dal prompt dei comandi di Windows sull'host locale, accedere alla directory in cui sono stati salvati i file di installazione del plug-in.
5. Installare il plug-in per il software SQL Server:

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

   Sostituire i valori segnaposto con i dati

   - Debug_Log_Path è il nome e la posizione del file di log del programma di installazione della suite.
   - Log_Path è la posizione dei log di installazione dei componenti plug-in (SCW, SCSQL e SMCore).
   - Num è la porta su cui SnapCenter comunica con SMCore
   - Install_Directory_Path è la directory di installazione del pacchetto del plug-in host.
   - Dominio/amministratore è il plug-in SnapCenter per l'account del servizio Web Microsoft Windows.
   - Password è la password dell'account del servizio Web del plug-in SnapCenter per Microsoft Windows.
     ```
     "snapcenter_windows_host_plugin.exe"/silent
     /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
     SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
     BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
     ISFeatureInstall=SCW,SCSQL
     ```

   Tutti i parametri passati durante l'installazione del plug-in per SQL Server sono sensibili al maiuscolo/minuscolo.

6. Monitorare il Task Scheduler di Windows, il file di log dell'installazione principale C: Installdebug.log e i file di installazione aggiuntivi in C:
7. Monitorare la directory %temp% per verificare che i programmi di installazione msiexe.exe stiano installando il software senza errori.

   L'installazione del plug-in per SQL Server 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 plug-in per SQL Server

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 dei plug-in, procedere come segue:
   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 **Dettagli lavoro**, fare clic su **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.

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

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 e *.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”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$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.

**Prima di iniziare**

- 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 anche a "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.

# Configurare il disaster recovery

## Disaster recovery del plug-in SnapCenter per SQL Server

Quando il plug-in SnapCenter per SQL Server non è disponibile, attenersi alla seguente procedura per passare a un host SQL diverso e ripristinare i dati.

**Prima di iniziare**

- L'host secondario deve avere lo stesso sistema operativo, l'applicazione e il nome host dell'host primario.
- Trasferire il plug-in SnapCenter per SQL Server a un host alternativo utilizzando la pagina **Aggiungi host** o **Modifica host**. Vedere "Gestire gli host" per ulteriori informazioni.

**Fasi**

1. Selezionare l'host dalla pagina **hosts** per modificare e installare il plug-in SnapCenter per SQL Server.
2. (Facoltativo) sostituire il plug-in SnapCenter per i file di configurazione di SQL Server dal backup di disaster recovery (DR) al nuovo computer.
3. Importare pianificazioni Windows e SQL dalla cartella del plug-in SnapCenter per SQL Server dal backup DR.

**Informazioni correlate**

Vedere il "API di disaster recovery" video.

## Disaster recovery (DR) dello storage per il plug-in SnapCenter per SQL Server

È possibile ripristinare il plug-in SnapCenter per lo storage SQL Server attivando la modalità DR per lo storage nella pagina Impostazioni globali.

**Prima di iniziare**

- Assicurarsi che i plug-in siano in modalità di manutenzione.
- Interrompere la relazione SnapMirror/SnapVault. "Interrompere le relazioni con SnapMirror"
- Collegare il LUN da secondario al computer host con la stessa lettera di unità.
- Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.
- Riavviare il servizio del server MSSQL.
- Assicurarsi che le risorse SQL siano di nuovo in linea.

**A proposito di questa attività**

Il disaster recovery (DR) non è supportato nelle configurazioni VMDK e RDM.

**Fasi**

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **Disaster Recovery**.
2. Selezionare **Enable Disaster Recovery** (attiva Disaster Recovery).
3. Fare clic su **Apply** (Applica).
4. Verificare se il processo DR è attivato o meno facendo clic su **Monitor** > **Jobs**.

**Al termine**

- Se vengono creati nuovi database dopo il failover, i database saranno in modalità non DR.

  I nuovi database continueranno a funzionare come prima del failover.

- I nuovi backup creati in modalità DR saranno elencati in SnapMirror o SnapVault (secondario) nella pagina topologia.

  Accanto ai nuovi backup viene visualizzata l'icona "i" per indicare che questi backup sono stati creati

durante la modalità DR.

- È possibile eliminare il plug-in SnapCenter per i backup di SQL Server creati durante il failover utilizzando l'interfaccia utente o il seguente cmdlet: `Remove-SmBackup`
- Dopo il failover, se si desidera che alcune risorse siano in modalità non DR, utilizzare il seguente cmdlet: `Remove-SmResourceDRMode`

  Per ulteriori informazioni, fare riferimento alla "Guida di riferimento al cmdlet del software SnapCenter".

- Il server SnapCenter gestirà le singole risorse di storage (database SQL) in modalità DR o non DR, ma non il gruppo di risorse con risorse di storage in modalità DR o non DR.

## Failback dal plug-in SnapCenter per lo storage secondario SQL Server allo storage primario

Una volta che il plug-in SnapCenter per lo storage primario di SQL Server è tornato online, è necessario eseguire il failback allo storage primario.

**Prima di iniziare**

- Impostare il plug-in SnapCenter per SQL Server in modalità **manutenzione** dalla pagina host gestiti.
- Scollegare lo storage secondario dall'host e connettersi allo storage primario.
- Per eseguire il failback allo storage primario, assicurarsi che la direzione della relazione rimanga la stessa di prima del failover eseguendo l'operazione di risincronizzazione inversa.

  Per mantenere i ruoli dello storage primario e secondario dopo l'operazione di risincronizzazione inversa, eseguire nuovamente l'operazione di risincronizzazione inversa.

  Per ulteriori informazioni, vedere "Risincronizzazione inversa delle relazioni mirror"

- Riavviare il servizio del server MSSQL.
- Assicurarsi che le risorse SQL siano di nuovo in linea.

> Durante il failover o il failback del plug-in, lo stato generale del plug-in non viene aggiornato immediatamente. Lo stato generale dell'host e del plug-in viene aggiornato durante la successiva operazione di refresh dell'host.

**Fasi**

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **Disaster Recovery**.
2. Deselezionare **Enable Disaster Recovery**.
3. Fare clic su **Apply** (Applica).
4. Verificare se il processo DR è attivato o meno facendo clic su **Monitor** > **Jobs**.

**Al termine**

È possibile eliminare il plug-in SnapCenter per i backup di SQL Server creati durante il failover utilizzando l'interfaccia utente o il seguente cmdlet: `Remove-SmDRFailoverBackups`

## 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 COMMERCIABILITÀ 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.