



Installare il plug-in SnapCenter per Oracle Database

SnapCenter software

NetApp
November 06, 2025

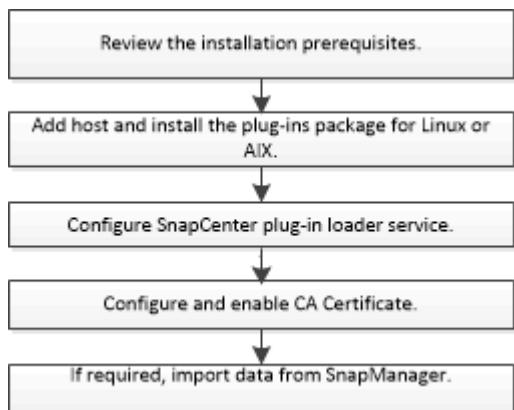
Sommario

Installa il plug-in SnapCenter per Oracle Database	1
Flusso di lavoro di installazione del plug-in SnapCenter per Oracle Database	1
Prerequisiti per l'aggiunta di host e l'installazione del pacchetto plug-in per Linux o AIX	1
Requisiti dell'host Linux	2
Requisiti dell'host AIX	5
Imposta le credenziali	7
Configurare le credenziali per un database Oracle	9
Aggiungi host e installa il pacchetto plug-in per Linux o AIX utilizzando l'interfaccia grafica	10
Monitorare lo stato dell'installazione	13
Metodi alternativi per installare il pacchetto Plug-in per Linux o AIX	14
Installa su più host remoti utilizzando cmdlet	14
Installa sull'host del cluster	15
Installa il pacchetto Plug-in per Linux in modalità silenziosa	15
Installa il pacchetto Plug-in per AIX in modalità silenziosa	16
Configurare il servizio SnapCenter Plug-in Loader	17
Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux	20
Gestisci la password per il keystore SPL e l'alias della coppia di chiavi firmata dalla CA in uso	20
Configurare i certificati radice o intermedi per l'archivio attendibile SPL	21
Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL	21
Configurare l'elenco di revoche dei certificati (CRL) per SPL	22
Abilita i certificati CA per i plug-in	22
Importa dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter	23
Configurazioni supportate per l'importazione dei dati	24
Cosa viene importato in SnapCenter	24
Cosa non viene importato in SnapCenter	26
Prepararsi all'importazione dei dati	26
Importa dati	28

Installa il plug-in SnapCenter per Oracle Database

Flusso di lavoro di installazione del plug-in SnapCenter per Oracle Database

Se si desidera proteggere i database Oracle, è necessario installare e configurare il plug-in SnapCenter per Oracle Database.



Prerequisiti per l'aggiunta di host e l'installazione del pacchetto plug-in per Linux o AIX

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

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.

Il plug-in SnapCenter per Oracle Database può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo del plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utente non root.

- Se si installa il pacchetto di plug-in SnapCenter per AIX su un host AIX, è necessario aver risolto manualmente i collegamenti simbolici a livello di directory.

Il pacchetto di plug-in SnapCenter per AIX risolve automaticamente il collegamento simbolico a livello di file, ma non i collegamenti simbolici a livello di directory, per ottenere il percorso assoluto JAVA_HOME.

- Creare credenziali con modalità di autenticazione Linux o AIX per l'utente installatore.
- È necessario aver installato Java 11 sul proprio host Linux o AIX.
 - Java di Oracle e OpenJDK è supportato per Linux
 - IBM Java per AIX. Puoi scaricare da "[Download di IBM Semeru Runtimes](#)"



Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.

- Per i database Oracle in esecuzione su un host Linux o AIX, è necessario installare sia SnapCenter Plug-in per Oracle Database sia SnapCenter Plug-in per UNIX.



È possibile utilizzare il plug-in per Oracle Database anche per gestire i database Oracle per SAP. Tuttavia, l'integrazione con SAP BR*Tools non è supportata.

- Se si utilizza il database Oracle 11.2.0.3 o versione successiva, è necessario installare la patch Oracle 13366202.



La mappatura UUID nel file /etc/fstab non è supportata da SnapCenter.

- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

Requisiti dell'host Linux

Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario assicurarsi che l'host soddisfi i requisiti.

Articolo	Requisiti
Sistemi operativi	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux <p> Se si utilizza il database Oracle su LVM nei sistemi operativi Oracle Linux o Red Hat Enterprise Linux 6.6 o 7.0, è necessario installare la versione più recente di Logical Volume Manager (LVM).</p> <ul style="list-style-type: none"> • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	2 GB
Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host	<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>

Articolo	Requisiti
Pacchetti software richiesti	<p>Java 11 Oracle e OpenJDK</p> <p> Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.</p> <p>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.</p>

Per le informazioni più recenti sulle versioni supportate, vedere "[Strumento matrice di interoperabilità NetApp](#)" .

Configurare i privilegi sudo per gli utenti non root per l'host Linux

SnapCenter 2.0 e le versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

Cosa ti servirà

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file `/etc/ssh/sshd_config` per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

Esempio:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress :::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Informazioni su questo compito

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

Passi

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```



Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file /etc/oracle/olr.loc.

LINUX_USER è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt se SnapCenter Server è installato sull'host Windows.
- /opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt se SnapCenter Server è installato sull'host Linux.



L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

Requisiti dell'host AIX

Prima di installare il pacchetto di plug-in SnapCenter per AIX, è necessario assicurarsi che l'host soddisfi i requisiti.



Il plug-in SnapCenter per UNIX, che fa parte del pacchetto di plug-in SnapCenter per AIX, non supporta gruppi di volumi simultanei.

Articolo	Requisiti
Sistemi operativi	AIX 7.1 o successivo
RAM minima per il plug-in SnapCenter sull'host	4 GB
Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host	2 GB 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.
Pacchetti software richiesti	Java 11 IBM Java Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per le informazioni più recenti sulle versioni supportate, vedere "[Strumento matrice di interoperabilità NetApp](#)" .

Configurare i privilegi sudo per gli utenti non root per l'host AIX

SnapCenter 4.4 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per AIX e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

Cosa ti servirà

- Sudo versione 1.8.7 o successiva.

- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Modificare il file `/etc/ssh/sshd_config` per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

Esempio:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress :::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Informazioni su questo compito

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl`

Passi

1. Accedere all'host AIX su cui si desidera installare il pacchetto plug-in SnapCenter per AIX.
2. Aggiungere le seguenti righe al file `/etc/sudoers` utilizzando l'utilità Linux visudo.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/  
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
AIX_USER/.sc_netapp/AIX_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: AIX_USER !visiblepw  
Defaults: AIX_USER !requiretty
```



Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file /etc/oracle/olr.loc.

AIX_USER è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt se SnapCenter Server è installato sull'host Windows.
- /opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt se SnapCenter Server è installato sull'host Linux.



L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

Imposta le credenziali

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare le credenziali per installare il pacchetto plug-in su host Linux o AIX.

Informazioni su questo compito

Le credenziali vengono create per l'utente root o per un utente non root che dispone dei privilegi sudo per installare e avviare il processo del plug-in.

Per informazioni, vedere:[Configurare i privilegi sudo per gli utenti non root per l'host Linux](#) O[Configurare i privilegi sudo per gli utenti non root per l'host AIX](#)

Procedura consigliata: Sebbene sia consentito creare credenziali dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

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, inserisci le informazioni sulle credenziali:

Per questo campo...	Fai questo...
Nome della credenziale	Inserisci un nome per le credenziali.
Nome utente/Password	<p>Immettere il nome utente e la password da utilizzare per l'autenticazione.</p> <ul style="list-style-type: none"> • Amministratore di dominio <p>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:</p> <ul style="list-style-type: none"> ◦ <i>NetB/OS\NomeUtente</i> ◦ <i>FQDN dominio\Nome utente</i> <ul style="list-style-type: none"> • Amministratore locale (solo per gruppi di lavoro) <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: <i>UserName</i></p>
Modalità di autenticazione	<p>Seleziona la modalità di autenticazione che desideri utilizzare.</p> <p>A seconda del sistema operativo dell'host del plug-in, selezionare Linux o AIX.</p>
Utilizzare i privilegi sudo	Selezionare la casella di controllo Usa privilegi sudo se si stanno creando credenziali per un utente non root.

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 le credenziali per un database Oracle

È necessario configurare le credenziali utilizzate per eseguire operazioni di protezione dei dati sui database Oracle.

Informazioni su questo compito

Dovresti esaminare i diversi metodi di autenticazione supportati per il database Oracle. Per informazioni, vedere "[Metodi di autenticazione per le tue credenziali](#)".

Se si impostano credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, il nome utente deve disporre almeno dei privilegi di gruppo di risorse e di backup.

Se hai abilitato l'autenticazione del database Oracle, nella vista delle risorse verrà visualizzata un'icona a forma di lucchetto rosso. È necessario configurare le credenziali del database per poter proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.



Se durante la creazione di una credenziale si specificano dati errati, verrà visualizzato un messaggio di errore. È necessario fare clic su **Annulla** e riprovare.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.
3. Clic , quindi selezionare il nome host e il tipo di database per filtrare le risorse.
Puoi quindi fare clic per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Impostazioni database > Configura database**.
5. Nella sezione Configura impostazioni database, dall'elenco a discesa **Usa credenziali esistenti**, seleziona le credenziali da utilizzare per eseguire processi di protezione dei dati sul database Oracle.



L'utente Oracle deve disporre dei privilegi sysdba.

Puoi anche creare una credenziale cliccando .

6. Nella sezione Configura impostazioni ASM, dall'elenco a discesa **Usa credenziali esistenti**, seleziona le credenziali da utilizzare per eseguire processi di protezione dei dati sull'istanza ASM.



L'utente ASM deve avere il privilegio sysasm.

Puoi anche creare una credenziale cliccando .

7. Nella sezione Configura impostazioni catalogo RMAN, dall'elenco a discesa **Usa credenziale esistente**, selezionare la credenziale da utilizzare per eseguire processi di protezione dei dati sul database del catalogo Oracle Recovery Manager (RMAN).

Puoi anche creare una credenziale cliccando  .

Nel campo **TNSName**, immettere il nome del file Transparent Network Substrate (TNS) che verrà utilizzato da SnapCenter Server per comunicare con il database.

8. Nel campo **Nodi RAC preferiti**, specificare i nodi RAC (Real Application Cluster) preferiti per il backup.

I nodi preferiti potrebbero essere uno o tutti i nodi del cluster in cui sono presenti le istanze del database RAC. L'operazione di backup viene attivata solo su questi nodi preferiti, nell'ordine di preferenza.

In RAC One Node, solo un nodo è elencato tra i nodi preferiti e questo nodo preferito è il nodo in cui è attualmente ospitato il database.

Dopo il failover o la rilocazione del database RAC One Node, l'aggiornamento delle risorse nella pagina Risorse SnapCenter rimuoverà l'host dall'elenco **Nodi RAC preferiti** in cui era precedentemente ospitato il database. Il nodo RAC in cui viene trasferito il database verrà elencato in **Nodi RAC** e dovrà essere configurato manualmente come nodo RAC preferito.

Per ulteriori informazioni, consultare "[Nodi preferiti nella configurazione RAC](#)" .

9. Fare clic su **OK**.

Aggiungi host e installa il pacchetto plug-in per Linux o AIX utilizzando l'interfaccia grafica

È possibile utilizzare la pagina Aggiungi host per aggiungere host e quindi installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX. I plug-in vengono installati automaticamente sugli host remoti.

Informazioni su questo compito

È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster. Se si installa il plug-in su un cluster (Oracle RAC), il plug-in viene installato su tutti i nodi del cluster. Per Oracle RAC One Node, è necessario installare il plug-in sia sui nodi attivi che su quelli passivi.



Quando si installa il plug-in su un Oracle RAC, è supportata solo l'autenticazione basata su password. L'autenticazione basata sulla chiave SSH non è supportata.

Dovresti essere assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .



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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

Per questo campo...	Fai questo...
Tipo di host	<p>Selezionare Linux o AIX come tipo di host.</p> <p>SnapCenter Server aggiunge l'host e quindi installa il plug-in per Oracle Database e il plug-in per UNIX se i plug-in non sono già installati sull'host.</p>
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"> • Host autonomo • Qualsiasi nodo nell'ambiente Oracle Real Application Clusters (RAC) <p> Il nodo VIP o l'IP di scansione non sono supportati</p> <p>Se si aggiunge un host tramite SnapCenter e l'host 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, consultare le informazioni sulla creazione delle credenziali.</p> <p>È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato.</p> <p> La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.</p>

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

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 <code>/opt/NetApp/snapcenter</code>.</p> <p>Facoltativamente, è possibile personalizzare il percorso.</p>
Aggiungere tutti gli host in Oracle RAC	<p>Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un Oracle RAC.</p> <p>In una configurazione Flex ASM, verranno aggiunti tutti i nodi, indipendentemente dal fatto che si tratti di un nodo Hub o Leaf.</p>
Salta i controlli di preinstallazione facoltativi	<p>Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.</p>

7. Fare clic su **Invia**.

Se non hai selezionato la casella di controllo Salta controlli preliminari, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in.



Lo script di pre-controllo non convalida lo stato del firewall della porta del plug-in se è specificato nelle regole di rifiuto del firewall.

Se i requisiti minimi non vengono soddisfatti, vengono visualizzati 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 situato in `C:\Programmi\NetApp\SnapCenter WebApp` per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, dovresti risolvere il problema.



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

8. Verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.



SnapCenter non supporta l'algoritmo ECDSA.



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

9. Monitorare l'avanzamento dell'installazione.

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

Risultato

Tutti i database sull'host vengono rilevati automaticamente e visualizzati nella pagina Risorse. Se non viene visualizzato nulla, fare clic su **Aggiorna risorse**.

Monitorare lo stato dell'installazione

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**.

Metodi alternativi per installare il pacchetto Plug-in per Linux o AIX

È anche possibile installare manualmente il pacchetto Plug-in per Linux o AIX utilizzando i cmdlet o le CLI.

Prima di installare manualmente il plug-in, è necessario convalidare la firma del pacchetto binario utilizzando la chiave **snapshot_public_key.pub** e **snapshot_linux_host_plugin.bin.sig** che si trovano in C:\ProgramData\NetApp\SnapCenter\Package Repository.



Assicurarsi che **OpenSSL 1.0.2g** sia installato sull'host in cui si desidera installare il plug-in.

Convalidare la firma del pacchetto binario eseguendo il comando:

- Per host Linux: `openssl dgst -sha256 -verify snapshot_public_key.pub -signature snapshot_linux_host_plugin.bin.sig snapshot_linux_host_plugin.bin`
- Per host AIX: `openssl dgst -sha256 -verify snapshot_public_key.pub -signature snapshot_aix_host_plugin.bsx.sig snapshot_aix_host_plugin.bsx`

Installa su più host remoti utilizzando cmdlet

Per installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su più host, è necessario utilizzare il cmdlet PowerShell *Install-SmHostPackage*.

Cosa ti servirà

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

Passi

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
3. Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX utilizzando il cmdlet *Install-SmHostPackage* e i parametri richiesti.

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.



Lo script di pre-controllo non convalida lo stato del firewall della porta del plug-in se è specificato nelle regole di rifiuto del firewall.

4. Inserisci le tue credenziali per l'installazione remota.

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" .

Installa sull'host del cluster

È necessario installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su entrambi i nodi dell'host del cluster.

Ciascuno dei nodi dell'host del cluster ha due IP. Uno degli IP sarà l'IP pubblico dei rispettivi nodi e il secondo IP sarà l'IP del cluster condiviso tra entrambi i nodi.

Passi

1. Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su entrambi i nodi dell'host del cluster.
2. Verificare che i valori corretti per i parametri SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT e SPL_ENABLED_PLUGINS siano specificati nel file spl.properties situato in /var/opt/snapcenter/spl/etc/.

Se SPL_ENABLED_PLUGINS non è specificato in spl.properties, è possibile aggiungerlo e assegnare il valore SCO,SCU.

3. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
4. In ciascuno dei nodi, impostare gli IP preferiti del nodo utilizzando il comando *Set-PreferredHostIPsInStorageExportPolicy* sccli e i parametri richiesti.
5. Nell'host del server SnapCenter , aggiungere una voce per l'IP del cluster e il nome DNS corrispondente in C:\Windows\System32\drivers\etc\hosts.
6. Aggiungere il nodo al server SnapCenter utilizzando il cmdlet *Add-SmHost* specificando l'IP del cluster per il nome host.

Individuare il database Oracle sul nodo 1 (supponendo che l'IP del cluster sia ospitato sul nodo 1) e creare un backup del database. In caso di failover, è possibile utilizzare il backup creato sul nodo 1 per ripristinare il database sul nodo 2. È anche possibile utilizzare il backup creato sul nodo 1 per creare un clone sul nodo 2.



Se il failover avviene mentre sono in esecuzione altre operazioni SnapCenter , saranno presenti volumi, directory e file di blocco obsoleti.

Installa il pacchetto Plug-in per Linux in modalità silenziosa

È possibile installare il pacchetto di plug-in SnapCenter per Linux in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

Cosa ti servirà

- Dovresti rivedere i prerequisiti per l'installazione del pacchetto plug-in.
- È necessario assicurarsi che la variabile d'ambiente DISPLAY non sia impostata.

Se la variabile d'ambiente DISPLAY è impostata, dovresti eseguire unset DISPLAY e quindi provare a installare manualmente il plug-in.

Informazioni su questo compito

Durante l'installazione in modalità console è necessario fornire le informazioni di installazione necessarie, mentre nell'installazione in modalità silenziosa non è necessario fornire alcuna informazione di installazione.

Passi

- Scaricare il pacchetto di plug-in SnapCenter per Linux dal percorso di installazione di SnapCenter Server.

Il percorso di installazione predefinito è `C:\ProgramData\NetApp\ SnapCenter\PackageRepository`. Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.

- Dal prompt dei comandi, accedi alla directory in cui hai scaricato il file di installazione.

- Correre

```
./SnapCenter_linux_host_plugin.bin -i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR=/opt/custom_path
```

- Modificare il file `spl.properties` situato in `/var/opt/snapcenter/spl/etc/` per aggiungere `SPL_ENABLED_PLUGINS=SCO,SCU`, quindi riavviare il servizio SnapCenter Plug-in Loader .

 L'installazione del pacchetto plug-in registra i plug-in sull'host e non sul server SnapCenter . È necessario registrare i plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, seleziona "Nessuno" come credenziale. Dopo aver aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

Installare il pacchetto Plug-in per AIX in modalità silenziosa

È possibile installare il pacchetto di plug-in SnapCenter per AIX in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

Cosa ti servirà

- Dovresti rivedere i prerequisiti per l'installazione del pacchetto plug-in.
- È necessario assicurarsi che la variabile d'ambiente DISPLAY non sia impostata.

Se la variabile d'ambiente DISPLAY è impostata, dovresti eseguire `unset DISPLAY` e quindi provare a installare manualmente il plug-in.

Passi

- Scaricare il pacchetto di plug-in SnapCenter per AIX dal percorso di installazione di SnapCenter Server.

Il percorso di installazione predefinito è `C:\ProgramData\NetApp\ SnapCenter\PackageRepository`. Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.

- Dal prompt dei comandi, accedi alla directory in cui hai scaricato il file di installazione.

- Correre

```
./snapcenter_aix_host_plugin.bsx -i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR=/opt/custom_path-
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. Modificare il file spl.properties situato in `/var/opt/snapcenter/spl/etc/` per aggiungere
`SPL_ENABLED_PLUGINS=SCO,SCU`, quindi riavviare il servizio SnapCenter Plug-in Loader .



L'installazione del pacchetto plug-in registra i plug-in sull'host e non sul server SnapCenter . È necessario registrare i plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, seleziona "Nessuno" come credenziale. Dopo aver aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

Configurare il servizio SnapCenter Plug-in Loader

Il servizio SnapCenter Plug-in Loader carica il pacchetto plug-in per Linux o AIX per interagire con SnapCenter Server. Il servizio SnapCenter Plug-in Loader viene installato quando si installa il pacchetto SnapCenter Plug-ins per Linux o il pacchetto SnapCenter Plug-ins per AIX.

Informazioni su questo compito

Dopo aver installato il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX, il servizio SnapCenter Plug-in Loader si avvia automaticamente. Se il servizio SnapCenter Plug-in Loader non si avvia automaticamente, è necessario:

- Assicurarsi che la directory in cui è in esecuzione il plug-in non venga eliminata
- Aumentare lo spazio di memoria assegnato alla Java Virtual Machine

Il file `spl.properties`, che si trova in `/custom_location/NetApp/snapcenter/spl/etc/`, contiene i seguenti parametri. A questi parametri vengono assegnati valori predefiniti.

Nome del parametro	Descrizione
<code>LOG_LEVEL</code>	Visualizza i livelli di registro supportati. I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
<code>SPL_PROTOCOL</code>	Visualizza il protocollo supportato da SnapCenter Plug-in Loader. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
<code>PROTOCOLLO_SERVER_SNAPCENTER</code>	Visualizza il protocollo supportato da SnapCenter Server. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.

Nome del parametro	Descrizione
SKIP_JAVAHOME_UPDATE	<p>Per impostazione predefinita, il servizio SPL rileva il percorso Java e aggiorna il parametro JAVA_HOME.</p> <p>Pertanto il valore predefinito è impostato su FALSE. È possibile impostare su TRUE se si desidera disabilitare il comportamento predefinito e correggere manualmente il percorso Java.</p>
SPL_KEYSTORE_PASS	<p>Visualizza la password del file keystore.</p> <p>È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore.</p>
SPL_PORT	<p>Visualizza il numero di porta su cui è in esecuzione il servizio SnapCenter Plug-in Loader .</p> <p>È possibile aggiungere il valore se manca il valore predefinito.</p> <div data-bbox="850 846 910 910" style="border: 1px solid #ccc; border-radius: 50%; width: 35px; height: 35px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">  </div> <p>Non modificare il valore dopo aver installato i plug-in.</p>
SNAPCENTER_SERVER_HOST	Visualizza l'indirizzo IP o il nome host del server SnapCenter .
SPL_KEYSTORE_PATH	Visualizza il percorso assoluto del file keystore.
SNAPCENTER_SERVER_PORT	Visualizza il numero di porta su cui è in esecuzione SnapCenter Server.
LOGS_MAX_COUNT	<p>Visualizza il numero di file di registro di SnapCenter Plug-in Loader conservati nella cartella /custom_location/snapcenter/spl/logs.</p> <p>Il valore predefinito è impostato su 5000. Se il conteggio è superiore al valore specificato, vengono conservati gli ultimi 5000 file modificati. Il controllo del numero di file viene eseguito automaticamente ogni 24 ore dall'avvio del servizio SnapCenter Plug-in Loader .</p> <div data-bbox="850 1691 910 1755" style="border: 1px solid #ccc; border-radius: 50%; width: 35px; height: 35px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">  </div> <p>Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999.</p>

Nome del parametro	Descrizione
JAVA_HOME	<p>Visualizza il percorso assoluto della directory JAVA_HOME utilizzata per avviare il servizio SPL.</p> <p>Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL.</p>
LOG_MAX_SIZE	<p>Visualizza la dimensione massima del file di registro dei lavori.</p> <p>Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file di quel processo.</p>
CONSERVA_I_LOG_DEGLI_ULTIMI_GIORNI	Visualizza il numero di giorni per i quali vengono conservati i registri.
ABILITA_VALIDAZIONE_CERTIFICATO	<p>Visualizza true quando la convalida del certificato CA è abilitata per l'host.</p> <p>È possibile abilitare o disabilitare questo parametro modificando spl.properties oppure utilizzando l'interfaccia utente grafica o il cmdlet SnapCenter .</p>

Se uno qualsiasi di questi parametri non è assegnato al valore predefinito o se si desidera assegnare o modificare il valore, è possibile modificare il file spl.properties. È inoltre possibile verificare il file spl.properties e modificarlo per risolvere eventuali problemi relativi ai valori assegnati ai parametri. Dopo aver modificato il file spl.properties, è necessario riavviare il servizio SnapCenter Plug-in Loader .

Passi

1. Eseguire una delle seguenti azioni, a seconda delle necessità:

- Avviare il servizio SnapCenter Plug-in Loader :
 - Come utente root, esegui: /custom_location/NetApp/snapcenter/spl/bin/spl start
 - Come utente non root, esegui: sudo /custom_location/NetApp/snapcenter/spl/bin/spl start
- Arrestare il servizio SnapCenter Plug-in Loader :
 - Come utente root, esegui: /custom_location/NetApp/snapcenter/spl/bin/spl stop
 - Come utente non root, esegui: sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop



È possibile utilizzare l'opzione -force con il comando stop per arrestare forzatamente il servizio SnapCenter Plug-in Loader . Tuttavia, è necessario procedere con cautela prima di procedere, poiché ciò interrompe anche le operazioni in corso.

◦ Riavviare il servizio SnapCenter Plug-in Loader :

- Come utente root, esegui: /custom_location/NetApp/snapcenter/spl/bin/spl

- restart
- Come utente non root, esegui: sudo
/custom_location/NetApp/snapcenter/spl/bin/spl restart
- Trova lo stato del servizio SnapCenter Plug-in Loader :
 - Come utente root, esegui: /custom_location/NetApp/snapcenter/spl/bin/spl status
 - Come utente non root, esegui: sudo
/custom_location/NetApp/snapcenter/spl/bin/spl status
- Trova la modifica nel servizio SnapCenter Plug-in Loader :
 - Come utente root, esegui: /custom_location/NetApp/snapcenter/spl/bin/spl change
 - Come utente non root, esegui: sudo
/custom_location/NetApp/snapcenter/spl/bin/spl change

Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per l'archivio attendibile SPL e configurare la coppia di chiavi firmata dalla CA per l'archivio attendibile SPL con il servizio SnapCenter Plug-in Loader per attivare il certificato digitale installato.



SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come archivio attendibile che come archivio chiavi.

Gestisci la password per il keystore SPL e l'alias della coppia di chiavi firmata dalla CA in uso

Passi

1. È possibile recuperare la password predefinita del keystore SPL dal file delle proprietà SPL.

È il valore corrispondente alla chiave 'SPL_KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel file spl.properties.

3. Riavviare il servizio dopo aver modificato la password.



La password per il keystore SPL e per tutte le password alias associate della chiave privata devono essere le stesse.

Configurare i certificati radice o intermedi per l'archivio attendibile SPL

È necessario configurare i certificati radice o intermedi senza la chiave privata nell'archivio attendibile SPL.

Passi

1. Passare alla cartella contenente il keystore SPL: `/var/opt/snapcenter/spl/etc`.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
. Aggiungi un certificato radice o intermedio:
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riarriare il servizio dopo aver configurato i certificati radice o
intermedi su SPL trust-store.
```



Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL

È necessario configurare la coppia di chiavi firmata dalla CA nell'archivio attendibile SPL.

Passi

1. Passare alla cartella contenente il keystore dell'SPL `/var/opt/snapcenter/spl/etc`.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
. Aggiungere il certificato CA con chiave sia privata che pubblica.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srckeystoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elenca i certificati aggiunti nel keystore.
```

```
keytool -list -v -keystore keystore.jks
.
. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.
```

La password predefinita del keystore SPL è il valore della chiave SPL_KEYSTORE_PASS nel file spl.properties.

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

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
.
. Configurare il nome alias dal keystore situato nel file spl.properties.
```

Aggiornare questo valore in base alla chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL.

Configurare l'elenco di revoche dei certificati (CRL) per SPL

Dovresti configurare il CRL per SPL

Informazioni su questo compito

- SPL cercherà i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per SPL è /var/opt/snapcenter/spl/etc/crl.

Passi

1. È possibile modificare e aggiornare la directory predefinita nel file spl.properties in base alla chiave SPL_CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

I certificati in arrivo saranno verificati rispetto a ciascun CRL.

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.

Importa dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter

Importando i dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter è possibile continuare a utilizzare i dati delle versioni precedenti.

È possibile importare dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter eseguendo lo strumento di importazione dall'interfaccia della riga di comando (CLI host Linux).

Lo strumento di importazione crea policy e gruppi di risorse in SnapCenter. Le policy e i gruppi di risorse creati in SnapCenter corrispondono ai profili e alle operazioni eseguite utilizzando tali profili in SnapManager per Oracle e SnapManager per SAP. Lo strumento di importazione SnapCenter interagisce con i database del repository SnapManager per Oracle e SnapManager per SAP e con il database che si desidera importare.

- Recupera tutti i profili, le pianificazioni e le operazioni eseguite utilizzando i profili.
- Crea una policy di backup SnapCenter per ogni operazione univoca e ogni pianificazione associata a un profilo.
- Crea un gruppo di risorse per ciascun database di destinazione.

È possibile eseguire lo strumento di importazione eseguendo lo script sc-migrate che si trova in `/opt/`

`/NetApp/snapcenter/spl/bin`. Quando si installa il pacchetto di plug-in SnapCenter per Linux sull'host del database che si desidera importare, lo script sc-migrate viene copiato in `/opt/NetApp/snapcenter/spl/bin`.



L'importazione dei dati non è supportata dall'interfaccia utente grafica (GUI) SnapCenter .

SnapCenter non supporta Data ONTAP funzionante in modalità 7. È possibile utilizzare lo strumento di transizione a 7 modalità per migrare dati e configurazioni archiviati su un sistema che esegue Data ONTAP in modalità 7 modalità verso un sistema ONTAP .

Configurazioni supportate per l'importazione dei dati

Prima di importare dati da SnapManager 3.4.x per Oracle e SnapManager 3.4.x per SAP in SnapCenter, è necessario conoscere le configurazioni supportate dal plug-in SnapCenter per Oracle Database.

Le configurazioni supportate con il plug-in SnapCenter per Oracle Database sono elencate in "[Strumento matrice di interoperabilità NetApp](#)" .

Cosa viene importato in SnapCenter

È possibile importare profili, pianificazioni e operazioni eseguite utilizzando i profili.

Da SnapManager per Oracle e SnapManager per SAP	Per SnapCenter
Profili senza alcuna operazione e programmazione	Viene creato un criterio con tipo di backup predefinito come Online e ambito di backup come Completo.
Profili con una o più operazioni	Vengono create più policy in base a una combinazione univoca di un profilo e di operazioni eseguite utilizzando tale profilo. I criteri creati in SnapCenter contengono i dettagli di conservazione e potatura del registro di archivio recuperati dal profilo e dalle operazioni corrispondenti.
Profili con configurazione Oracle Recovery Manager (RMAN)	Le policy vengono create con l'opzione Backup del catalogo con Oracle Recovery Manager abilitata. Se in SnapManager è stata utilizzata la catalogazione RMAN esterna, è necessario configurare le impostazioni del catalogo RMAN in SnapCenter. È possibile selezionare le credenziali esistenti oppure crearne di nuove. Se RMAN è stato configurato tramite il file di controllo in SnapManager, non è necessario configurare RMAN in SnapCenter.
Programma allegato a un profilo	Viene creata una policy specifica per la pianificazione.

Da SnapManager per Oracle e SnapManager per SAP	Per SnapCenter
Banca dati	<p>Per ogni database importato viene creato un gruppo di risorse.</p> <p>In una configurazione RAC (Real Application Clusters), il nodo su cui si esegue lo strumento di importazione diventa il nodo preferito dopo l'importazione e per tale nodo viene creato il gruppo di risorse.</p>



Quando si importa un profilo, viene creata una policy di verifica insieme alla policy di backup.

Quando i profili, le pianificazioni e tutte le operazioni eseguite tramite i profili SnapManager per Oracle e SnapManager per SAP vengono importati in SnapCenter, vengono importati anche i diversi valori dei parametri.

Parametri e valori SnapManager per Oracle e SnapManager per SAP	Parametro e valori SnapCenter	Note
Ambito di backup <ul style="list-style-type: none"> • Pieno • Dati • Tronco d'albero 	Ambito di backup <ul style="list-style-type: none"> • Pieno • Dati • Tronco d'albero 	
Modalità di backup <ul style="list-style-type: none"> • Auto • In linea • Fuori linea 	Tipo di backup <ul style="list-style-type: none"> • In linea • Arresto offline 	Se la modalità di backup è Auto, lo strumento di importazione controlla lo stato del database al momento dell'esecuzione dell'operazione e imposta opportunamente il tipo di backup su Arresto online o Arresto offline.
Conservazione <ul style="list-style-type: none"> • Giorni • Conti 	Conservazione <ul style="list-style-type: none"> • Giorni • Conti 	<p>SnapManager per Oracle e SnapManager per SAP utilizzano sia Giorni che Conteggi per impostare la conservazione.</p> <p>In SnapCenter, ci sono Giorni O Conteggi. Pertanto, la conservazione è impostata in base ai giorni, poiché in SnapManager per Oracle e SnapManager per SAP i giorni hanno la precedenza sui conteggi.</p>

Parametri e valori SnapManager per Oracle e SnapManager per SAP	Parametro e valori SnapCenter	Note
Potatura per programmi <ul style="list-style-type: none"> • Tutto • numero di modifica del sistema (SCN) • Data • Registri creati prima di ore, giorni, settimane e mesi specificati 	Potatura per programmi <ul style="list-style-type: none"> • Tutto • Registri creati prima delle ore e dei giorni specificati 	SnapCenter non supporta la potatura basata su SCN, data, settimane e mesi.
Notifica <ul style="list-style-type: none"> • Email inviate solo per operazioni riuscite • Email inviate solo per operazioni non riuscite • Email inviate sia per operazioni riuscite che non riuscite 	Notifica <ul style="list-style-type: none"> • Sempre • In caso di fallimento • Avvertimento • Errore 	Le notifiche e-mail vengono importate. Tuttavia, è necessario aggiornare manualmente il server SMTP tramite l'interfaccia grafica utente SnapCenter . L'oggetto dell'e-mail viene lasciato vuoto per consentirti di configurerlo.

Cosa non viene importato in SnapCenter

Lo strumento di importazione non importa tutto in SnapCenter.

Non è possibile importare quanto segue in SnapCenter:

- Metadati di backup
- Backup parziali
- Backup relativi a Raw Device Mapping (RDM) e Virtual Storage Console (VSC)
- Ruoli o credenziali disponibili nel repository SnapManager per Oracle e SnapManager per SAP
- Dati relativi alle operazioni di verifica, ripristino e clonazione
- Potatura per operazioni
- Dettagli di replicazione specificati nel profilo SnapManager per Oracle e SnapManager per SAP

Dopo l'importazione, è necessario modificare manualmente il criterio corrispondente creato in SnapCenter per includere i dettagli di replica.

- Informazioni di backup catalogate

Prepararsi all'importazione dei dati

Prima di importare i dati in SnapCenter, è necessario eseguire determinate attività per eseguire correttamente l'operazione di importazione.

Passi

1. Identifica il database che vuoi importare.
2. Utilizzando SnapCenter, aggiungere l'host del database e installare il pacchetto plug-in SnapCenter per Linux.
3. Utilizzando SnapCenter, impostare le connessioni per le macchine virtuali di archiviazione (SVM) utilizzate dai database sull'host.
4. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
5. Nella pagina Risorse, assicurati che il database da importare sia stato individuato e visualizzato.

Quando si desidera eseguire lo strumento di importazione, il database deve essere accessibile, altrimenti la creazione del gruppo di risorse non riesce.

Se il database ha credenziali configurate, è necessario creare una credenziale corrispondente in SnapCenter, assegnare la credenziale al database e quindi eseguire nuovamente l'individuazione del database. Se il database risiede su Automatic Storage Management (ASM), è necessario creare le credenziali per l'istanza ASM e assegnarle al database.

6. Assicurarsi che l'utente che esegue lo strumento di importazione disponga di privilegi sufficienti per eseguire i comandi SnapManager per Oracle o SnapManager per SAP CLI (ad esempio il comando per sospendere le pianificazioni) dall'host SnapManager per Oracle o SnapManager per SAP.
7. Eseguire i seguenti comandi sull'host SnapManager per Oracle o SnapManager per SAP per sospendere le pianificazioni:
 - a. Se si desidera sospendere le pianificazioni sull'host SnapManager per Oracle, eseguire:
 - smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database
 - smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database
 - smo credential set -profile -name profile_name



È necessario eseguire il comando smo credential set per ciascun profilo sull'host.

- b. Se si desidera sospendere le pianificazioni sull'host SnapManager per SAP, eseguire:
 - smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database
 - smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database
 - smsap credential set -profile -name profile_name



È necessario eseguire il comando smsap credential set per ciascun profilo sull'host.

8. Assicurarsi che il nome di dominio completo (FQDN) dell'host del database venga visualizzato quando si esegue hostname -f.

Se il nome di dominio completo (FQDN) non viene visualizzato, è necessario modificare /etc/hosts per specificare il nome di dominio completo (FQDN) dell'host.

Importa dati

È possibile importare i dati eseguendo lo strumento di importazione dall'host del database.

Informazioni su questo compito

I criteri di backup SnapCenter creati dopo l'importazione hanno formati di denominazione diversi:

- I criteri creati per i profili senza alcuna operazione e pianificazione hanno il formato `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED`.

Quando non viene eseguita alcuna operazione utilizzando un profilo, viene creato il criterio corrispondente con il tipo di backup predefinito online e l'ambito del backup completo.

- I criteri creati per i profili con una o più operazioni hanno il formato `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.
- I criteri creati per le pianificazioni associate ai profili hanno il formato `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.

Passi

1. Accedi all'host del database che desideri importare.
2. Eseguire lo strumento di importazione eseguendo lo script `sc-migrate` che si trova in `/opt/NetApp/snapcenter/spl/bin`.
3. Immettere il nome utente e la password di SnapCenter Server.

Dopo aver convalidato le credenziali, viene stabilita una connessione con SnapCenter.

4. Immettere i dettagli del database del repository SnapManager per Oracle o SnapManager per SAP.

Il database del repository elenca i database disponibili sull'host.

5. Inserisci i dettagli del database di destinazione.

Se si desidera importare tutti i database sull'host, immettere all.

6. Se si desidera generare un registro di sistema o inviare messaggi ASUP per operazioni non riuscite, è necessario abilitarli eseguendo il comando `Add-SmStorageConnection` o `Set-SmStorageConnection`.



Se si desidera annullare un'operazione di importazione, durante l'esecuzione dello strumento di importazione o dopo l'importazione, è necessario eliminare manualmente i criteri, le credenziali e i gruppi di risorse SnapCenter creati come parte dell'operazione di importazione.

Risultati

I criteri di backup SnapCenter vengono creati per profili, pianificazioni e operazioni eseguite utilizzando i profili. Vengono creati anche gruppi di risorse per ogni database di destinazione.

Dopo aver importato correttamente i dati, le pianificazioni associate al database importato vengono sospese in

SnapManager per Oracle e SnapManager per SAP.



Dopo l'importazione, è necessario gestire il database o il file system importato utilizzando SnapCenter.

I log di ogni esecuzione dello strumento di importazione vengono archiviati nella directory `/var/opt/snapcenter/spl/logs` con il nome `spl_migration_timestamp.log`. È possibile fare riferimento a questo registro per esaminare gli errori di importazione e risolverli.

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.