Installare il plug-in SnapCenter per database Oracle

SnapCenter Software 5.0

NetApp
July 18, 2024

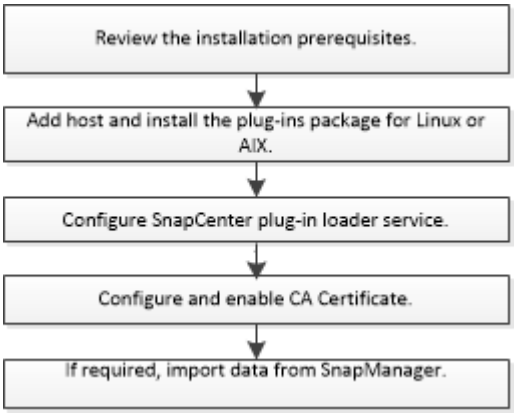
Sommario

Installare il plug-in SnapCenter per database Oracle . . . 1
Workflow di installazione del plug-in SnapCenter per database Oracle . . . 1
Prerequisiti per l'aggiunta di host e l'installazione di Plug-ins Package per Linux o AIX . . . 1
Aggiungere host e installare Plug-ins Package per Linux o AIX utilizzando la GUI . . . 10
Metodi alternativi per installare Plug-ins Package per Linux o AIX . . . 14
Configurare il servizio caricatore plug-in di SnapCenter . . . 17
Configurare il certificato CA con il servizio caricatore plug-in (SPL) di SnapCenter sull'host Linux . . . 20
Abilitare i certificati CA per i plug-in . . . 23
Importa i dati da SnapManager per Oracle e SnapManager per SAP a SnapCenter . . . 23

Installare il plug-in SnapCenter per database Oracle

Workflow di installazione del plug-in SnapCenter per database Oracle

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



Prerequisiti per l'aggiunta di host e l'installazione di Plug-ins Package per Linux o AIX

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 aver attivato la connessione SSH basata su password per l'utente root o non root.

  Il plug-in SnapCenter per database Oracle 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 di plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utenti non root.

- Se si installa il pacchetto di plug-in SnapCenter per AIX su host AIX, i collegamenti simbolici a livello di directory dovrebbero essere stati risolti manualmente.

  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 le credenziali con la modalità di autenticazione come Linux o AIX per l'utente di installazione.
- È necessario aver installato Java 1.8.x o Java 11 a 64 bit sull'host Linux o AIX.

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

  Per informazioni su come scaricare JAVA, consulta:

- "Download Java per tutti i sistemi operativi"
- "IBM Java per AIX"

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

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

- Se si utilizza Oracle database 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.

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

Requisiti degli host Linux

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

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux Se si utilizza un 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). • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	2 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.

Elemento	Requisiti
Pacchetti software richiesti	• Java 1,8.x (64 bit) Oracle Java e OpenJDK • Java 11 (64 bit) Oracle Java e OpenJDK Assicurarsi di aver installato solo L'edizione certificata DI JAVA 11 sull'host Linux. Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

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

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

Cosa ti serve

- Sudo versione 1.8.7 o successiva.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione del messaggio: 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
```

A proposito di questa attività

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

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Fasi

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

```
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 !visiblepw
Defaults: LINUX_USER !requiretty
```

> Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, 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 creato.

È possibile ottenere il *checksum_value* dal file **oracle_checksum.txt**, che si trova in *C:/ProgramData/NetApp/SnapCenter/Package Repository*.

Se è stata specificata una posizione personalizzata, la posizione sarà *custom_path/NetApp/SnapCenter/Package Repository*.

> L'esempio deve essere utilizzato solo come riferimento per la creazione di dati personali.

Requisiti dell'host AIX

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

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

Elemento	Requisiti
Sistemi operativi	AIX 7,1 o versione successiva
RAM minima per il plug-in SnapCenter sull'host	4 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Java 1.8.x (64 bit) IBM Java • Java 11 (64 bit) IBM Java Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di 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 di plug-in verranno eseguiti come utenti non root. È necessario configurare i privilegi sudo per l'utente non root per fornire l'accesso a diversi percorsi.

Cosa ti serve

- Sudo versione 1.8.7 o successiva.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione del messaggio: 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
```

A proposito di questa attività

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

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Fasi

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 usando l'utility visudo Linux.

```
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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, 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 creato.

È possibile ottenere il *checksum_value* dal file **oracle_checksum.txt**, che si trova in *C:/ProgramData/NetApp/SnapCenter/Package Repository*.

Se è stata specificata una posizione personalizzata, la posizione sarà *custom_path/NetApp/SnapCenter/Package Repository*.

L'esempio deve essere utilizzato solo come riferimento per la creazione di dati personali.

Impostare le credenziali

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. Creare le credenziali per l'installazione del pacchetto plug-in su host Linux o AIX.

A proposito di questa attività

Le credenziali vengono create per l'utente root o per un utente non root che dispone dei privilegi di sudo per installare e avviare il processo di 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

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

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, immettere le informazioni sulle credenziali:

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

Per questo campo…	Eseguire questa operazione…
Nome utente/Password	Immettere il nome utente e la password da utilizzare per l'autenticazione. • Amministratore di dominio Specificare l'amministratore di dominio sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ *NetBIOS/nome utente* ◦ *Dominio FQDN/nome utente* • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è: *Nome utente*
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare. A seconda del sistema operativo dell'host plug-in, selezionare Linux o AIX.
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**.

Al termine dell'impostazione delle credenziali, è possibile 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.

A proposito di questa attività

È necessario esaminare i diversi metodi di autenticazione supportati per il database Oracle. Per informazioni, vedere "Metodi di autenticazione per le credenziali".

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

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

Se si specificano dettagli errati durante la creazione di una credenziale, viene visualizzato un messaggio di errore. Fare clic su **Annulla**, quindi riprovare.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).
3. Fare clic su , quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   È quindi possibile fare clic su per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Impostazioni database** > **Configura database**.
5. Nella sezione Configure database settings (Configura impostazioni database), dall'elenco a discesa **Use Existing Credential** (Usa credenziale esistente), selezionare la credenziale da utilizzare per eseguire i processi di protezione dei dati nel database Oracle.

   L'utente Oracle deve disporre dei privilegi sysdba.

   È anche possibile creare una credenziale facendo clic su .
6. Nella sezione Configure ASM settings (Configura impostazioni ASM), dall'elenco a discesa **Use Existing Credential** (Usa credenziale esistente), selezionare la credenziale da utilizzare per eseguire i processi di protezione dei dati sull'istanza di ASM.

   L'utente ASM deve disporre del privilegio sysasm.

   È anche possibile creare una credenziale facendo clic su .
7. Nella sezione Configure RMAN catalog settings (Configura impostazioni catalogo RMAN), dall'elenco a discesa **Use existing credential** (Usa credenziale esistente), selezionare la credenziale da utilizzare per eseguire i processi di protezione dei dati nel database del catalogo di Oracle Recovery Manager (RMAN).

   È anche possibile creare una credenziale facendo clic su .

   Nel campo **TNSName**, immettere il nome del file TNS (transparent Network substrate) che verrà utilizzato dal server SnapCenter per comunicare con il database.
8. Nel campo **Preferred RAC Nodes** (nodi RAC preferiti), specificare i nodi RAC (Real Application Cluster) preferiti per il backup.

   I nodi preferiti possono 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 in ordine di preferenza.

   In RAC One Node, nei nodi preferiti è elencato solo un nodo, che è il nodo in cui è attualmente ospitato il

database.

Dopo il failover o il trasferimento del database RAC a un nodo, l'aggiornamento delle risorse nella pagina risorse SnapCenter rimuoverà l'host dall'elenco **Preferred RAC Node** (nodi RAC preferiti) in cui il database era stato ospitato in precedenza. Il nodo RAC in cui viene ricollocato il database viene elencato in **nodi RAC** e deve essere configurato manualmente come nodo RAC preferito.

Per ulteriori informazioni, vedere "Nodi preferiti nella configurazione RAC".

9. Fare clic su **OK**.

Aggiungere host e installare Plug-ins Package per Linux o AIX utilizzando la GUI

È possibile utilizzare la pagina Aggiungi host per aggiungere host, 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.

A proposito di questa attività

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 su entrambi i nodi attivi e passivi.

È necessario assegnare un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.

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

Fasi

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

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare **Linux** o **AIX** come tipo di host. Il server SnapCenter aggiunge l'host, quindi installa il plug-in per il database Oracle e il plug-in per UNIX se i plug-in non sono già installati sull'host.

Per questo campo…	Eseguire questa operazione…
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi: • Host standalone • Qualsiasi nodo nell'ambiente Oracle Real Application Clusters (RAC) Il nodo VIP o l'IP di scansione non sono supportati Se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.
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. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

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

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il percorso predefinito è */OPT/NetApp/Snapcenter*. È possibile personalizzare il percorso.
Aggiungere tutti gli host in Oracle RAC	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un RAC Oracle. In una configurazione di Flex ASM, verranno aggiunti tutti i nodi indipendentemente dal fatto che si tratti di un nodo Hub o Leaf.
Ignorare i controlli opzionali 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.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo Ignora precheck, l'host viene validato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

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

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

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

8. Verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   In una configurazione del cluster, verificare l'impronta digitale di ciascuno dei nodi 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 log specifici dell'installazione si trovano in */custom_location/snapcenter/logs*.

Risultato

Tutti i database dell'host vengono automaticamente rilevati e visualizzati nella pagina risorse. Se non viene visualizzato alcun messaggio, fare clic su **Refresh Resources** (Aggiorna risorse).

Monitorare lo stato dell'installazione

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 avvertenze o impossibile avviarsi a causa di avvertenze
- 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**.

Metodi alternativi per installare Plug-ins Package per Linux o AIX

È inoltre possibile installare manualmente il pacchetto di plug-in per Linux o AIX utilizzando i cmdlet o le CLI.

Prima di installare il plug-in manualmente, è necessario convalidare la firma del pacchetto binario utilizzando le chiavi **snapcenter_public_key.pub** e **snapcenter_linux_host_plugin.bin.sig** situate 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 snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Per l'host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

Installazione su più host remoti utilizzando cmdlet

Utilizzare il cmdlet *Install-SmHostPackage* PowerShell per installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su più host.

Cosa ti serve

È necessario accedere a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto di 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 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 precheck non convalida lo stato del firewall della porta plug-in se specificato nelle regole di rifiuto del firewall.

4. Inserire le 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, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Installare sull'host del cluster

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 dispone di 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.

Fasi

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:
6. Aggiungere il nodo al server SnapCenter utilizzando il cmdlet *Add-SmHost* specificando l'IP del cluster per il nome host.

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

Installare 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 a riga di comando (CLI).

Cosa ti serve

- Esaminare i prerequisiti per l'installazione del pacchetto di plug-in.
- Assicurarsi che la variabile di ambiente DI VISUALIZZAZIONE non sia impostata.

  Se la variabile di ambiente DI VISUALIZZAZIONE è impostata, eseguire unset DISPLAY, quindi provare a installare manualmente il plug-in.

A proposito di questa attività

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

installazione.

Fasi

1. Scaricare il pacchetto di plug-in SnapCenter per Linux dal percorso di installazione del server SnapCenter.

   Il percorso di installazione predefinito è *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato scaricato il file di installazione.
3. Eseguire

   ```
   ./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
   ```

4. Modificare il file spl.properties che si trova in */var/opt/snapcenter/spl/etc/* per aggiungere SPL_ENABLED_PLUGINS=SCO,SCU, quindi riavviare il servizio caricatore plug-in di SnapCenter.

> L'installazione del pacchetto di 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 utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, selezionare "Nessuno" come credenziale. Una volta 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 plug-in SnapCenter per AIX in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

Cosa ti serve

- Esaminare i prerequisiti per l'installazione del pacchetto di plug-in.
- Assicurarsi che la variabile di ambiente DI VISUALIZZAZIONE non sia impostata.

  Se la variabile di ambiente DI VISUALIZZAZIONE è impostata, eseguire unset DISPLAY, quindi provare a installare manualmente il plug-in.

Fasi

1. Scaricare il pacchetto di plug-in SnapCenter per AIX dal percorso di installazione del server SnapCenter.

   Il percorso di installazione predefinito è *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato scaricato il file di installazione.
3. Eseguire

   ```
   ./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 che si trova in */var/opt/snapcenter/spl/etc/* per aggiungere SPL_ENABLED_PLUGINS=SCO,SCU, quindi riavviare il servizio caricatore plug-in di SnapCenter.

> L'installazione del pacchetto di 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 utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, selezionare "Nessuno" come credenziale. Una volta aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

Configurare il servizio caricatore plug-in di SnapCenter

Il servizio caricatore plug-in SnapCenter carica il pacchetto plug-in per Linux o AIX per interagire con il server SnapCenter. Il servizio caricatore plug-in SnapCenter viene installato quando si installa il pacchetto plug-in SnapCenter per Linux o il pacchetto plug-in SnapCenter per AIX.

A proposito di questa attività

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

- Assicurarsi che la directory in cui opera 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
LOG_LEVEL	Visualizza i livelli di registro supportati. I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR, E FATALE.
PROTOCOLLO_SPL	Visualizza il protocollo supportato dal caricatore plug-in SnapCenter. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
PROTOCOLLO_SERVER_SNAPCENTER	Visualizza il protocollo supportato dal server SnapCenter. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.

Nome del parametro	Descrizione
SKIP_JAVAHOME_UPDATE	Per impostazione predefinita, il servizio SPL rileva il percorso java e aggiorna IL parametro JAVA_HOME. Pertanto, il valore predefinito è IMPOSTATO SU FALSE. È possibile impostare SU TRUE se si desidera disattivare il comportamento predefinito e correggere manualmente il percorso java.
SPL_KEYSTORE_PASS	Visualizza la password del file keystore. È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore.
SPL_PORT	Visualizza il numero di porta su cui è in esecuzione il servizio caricatore plug-in di SnapCenter. È possibile aggiungere il valore se manca il valore predefinito. Non modificare il valore dopo l'installazione dei plug-in.
SNAPCENTER_SERVER_HOST	Visualizza l'indirizzo IP o il nome host del server SnapCenter.
SPL_KEYSTORE_PATH	Visualizza il percorso assoluto del file keystore.
PORTA_SERVER_SNAPCENTER	Visualizza il numero di porta su cui è in esecuzione il server SnapCenter.
LOG_MAX_COUNT	Visualizza il numero di file di log del caricatore plug-in SnapCenter conservati nella cartella */custom_location/snapcenter/spl/logs*. Il valore predefinito è 5000. Se il conteggio supera il 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 caricatore plug-in di SnapCenter. Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999.

Nome del parametro	Descrizione
JAVA_HOME	Visualizza il percorso assoluto della directory DI JAVA_HOME che viene utilizzato per avviare il servizio SPL. Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL.
LOG_MAX_SIZE	Visualizza la dimensione massima del file di log del lavoro. Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file del lavoro.
RETAIN_LOGS_OF_LAST_DAYS	Visualizza il numero di giorni in cui i registri vengono conservati.
ENABLE_CERTIFICATE_VALIDATION	Viene visualizzato true quando la convalida del certificato CA è attivata per l'host. È possibile attivare o disattivare questo parametro modificando il file spl.properties o utilizzando l'interfaccia grafica o il cmdlet di SnapCenter.

Se uno 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, riavviare il servizio caricatore plug-in di SnapCenter.

Fasi

1. Eseguire una delle seguenti operazioni, secondo necessità:
   - Avviare il servizio caricatore plug-in SnapCenter:
     - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Arrestare il servizio caricatore plug-in di SnapCenter:
     - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     È possibile utilizzare l'opzione -force con il comando stop per arrestare con forza il servizio caricatore plug-in di SnapCenter. Tuttavia, prima di eseguire questa operazione, è necessario prestare attenzione, in quanto termina anche le operazioni esistenti.

- Riavviare il servizio caricatore plug-in di SnapCenter:
  - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
  - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Individuare lo stato del servizio caricatore plug-in di SnapCenter:
  - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
  - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Individuare la modifica nel servizio caricatore plug-in di SnapCenter:
  - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurare il certificato CA con il servizio caricatore plug-in (SPL) di SnapCenter sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio di trust SPL e configurare la coppia di chiavi firmate CA per l'archivio di trust SPL con il servizio caricatore plug-in SnapCenter per attivare il certificato digitale installato.

SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmate CA in uso

Fasi

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

   È il valore corrispondente alla chiave 'SOL_KEYSTORE_PASS'.

2. Modificare la password del keystore:

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

```
keytool -keypasswd -alias "<alias_name>" -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 l'archivio chiavi SPL e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust SPL

È necessario configurare i certificati root o intermedi senza la chiave privata in SPL trust-store.

Fasi

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

```
 keytool -list -v -keystore keystore.jks
. Aggiungere un certificato root o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in SPL trust-store.
```

> Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi con firma CA nell'archivio di trust SPL

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di fiducia SPL.

Fasi

1. Accedere alla cartella contenente il keystore /var/opt/snapcenter/spl/ecc. della SPL
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

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

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elencare 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 in password archivio chiavi.
```

Default SPL keystore password 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 con un nome
semplice:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurare il nome alias dal keystore che si trova nel file
spl.properties.
```

Aggiornare questo valore con la chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA in SPL trust-store.

Configurare l'elenco CRL (Certificate Revocation List) per SPL

Configurare il CRL per SPL

A proposito di questa attività

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

Fasi

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 file CRL in questa directory.

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

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

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 convalidato correttamente.
- * * Indica che il certificato CA non può essere 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 vengono completate correttamente.

Importa i dati da SnapManager per Oracle e SnapManager per SAP a SnapCenter

L'importazione dei dati da SnapManager per Oracle e SnapManager per SAP a SnapCenter consente di continuare a utilizzare i dati delle versioni precedenti.

È possibile importare i dati da SnapManager per Oracle e SnapManager per SAP a 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. I criteri 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 dei 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 allegata a un profilo.
- Crea un gruppo di risorse per ogni database di destinazione.

È possibile eseguire lo strumento di importazione eseguendo lo script sc-migra situato in */opt/NetApp/snapcenter/spl/bin*. Quando si installa il pacchetto di plug-in SnapCenter per Linux sull'host di database che si desidera importare, lo script di migrazione sc viene copiato in */opt/NetApp/snapcenter/spl/bin*.

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

SnapCenter non supporta Data ONTAP in 7-Mode. È possibile utilizzare lo strumento di transizione 7-Mode per migrare i dati e le configurazioni memorizzati in un sistema che esegue Data ONTAP in 7-Mode a un sistema ONTAP.

Configurazioni supportate per l'importazione dei dati

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

Le configurazioni supportate dal plug-in SnapCenter per database Oracle sono elencate nella "Tool di 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	A SnapCenter
Profili senza operazioni e pianificazioni	Viene creato un criterio con il tipo di backup predefinito online e l'ambito di backup completo.
Profili con una o più operazioni	Vengono create più policy in base a una combinazione univoca di un profilo e delle operazioni eseguite utilizzando tale profilo. I criteri creati in SnapCenter contengono l'eliminazione del log di archiviazione e i dettagli di conservazione recuperati dal profilo e dalle operazioni corrispondenti.

Da SnapManager per Oracle e SnapManager per SAP	A SnapCenter
Profili con configurazione di Oracle Recovery Manager (RMAN)	Le policy vengono create con l'opzione **Catalog backup with Oracle Recovery Manager** attivata. Se è stata utilizzata la catalogazione RMAN esterna in SnapManager, è necessario configurare le impostazioni del catalogo RMAN in SnapCenter. È possibile selezionare la credenziale esistente o crearne una nuova. 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 solo per la pianificazione.
Database	Viene creato un gruppo di risorse per ogni database importato. In un'installazione di Real Application Clusters (RAC), il nodo su cui viene eseguito lo strumento di importazione diventa il nodo preferito dopo l'importazione e il gruppo di risorse viene creato per quel nodo.

Quando viene importato un profilo, viene creato un criterio di verifica insieme al criterio di backup.

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

Parametri e valori di SnapManager per Oracle e SnapManager per SAP	Parametri e valori SnapCenter	Note
Ambito del backup • Completo • Dati • Log (Registro)	Ambito del backup • Completo • Dati • Log (Registro)	
Modalità di backup • Automatico • Online • Offline	Tipo di backup • Online • Spegnimento 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 correttamente il tipo di backup come Online o Offline Shutdown.

Parametri e valori di SnapManager per Oracle e SnapManager per SAP	Parametri e valori SnapCenter	Note
Conservazione • Giorni • Conta	Conservazione • Giorni • Conta	SnapManager per Oracle e SnapManager per SAP utilizzano giorni e conteggi per impostare la conservazione. In SnapCenter, sono disponibili i conteggi dei giorni o dei giorni. Pertanto, la conservazione viene stabilita rispetto ai giorni in cui i giorni ottengono la preferenza rispetto ai conteggi in SnapManager per Oracle e SnapManager per SAP.
Eliminazione delle pianificazioni • Tutto • Numero di cambio di sistema (SCN) • Data • Registri creati prima di ore, giorni, settimane e mesi specificati	Eliminazione delle pianificazioni • Tutto • Registri creati prima di ore e giorni specificati	SnapCenter non supporta la potatura in base a SCN, Data, settimane e mesi.
Notifica • E-mail inviate solo per operazioni riuscite • E-mail inviate solo per operazioni non riuscite • E-mail inviate per operazioni riuscite e non riuscite	Notifica • Sempre • In caso di guasto • Attenzione • Errore	Le notifiche e-mail vengono importate. Tuttavia, è necessario aggiornare manualmente il server SMTP utilizzando l'interfaccia grafica di SnapCenter. L'oggetto del messaggio di posta elettronica viene lasciato vuoto per la configurazione.

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 RDM (Raw Device mapping) e VSC (Virtual Storage Console) correlati
- Ruoli o credenziali disponibili nel repository SnapManager per Oracle e SnapManager per SAP

- Dati relativi alle operazioni di verifica, ripristino e clonazione
- Eliminazione delle operazioni
- Dettagli di replica 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 della replica.

- Informazioni di backup catalogate

Prepararsi all'importazione dei dati

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

Fasi

1. Identificare il database che si desidera importare.
2. Utilizzando SnapCenter, aggiungere l'host del database e installare il pacchetto di plug-in SnapCenter per Linux.
3. Utilizzando SnapCenter, impostare le connessioni per le macchine virtuali di storage (SVM) utilizzate dai database sull'host.
4. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
5. Nella pagina Resources (risorse), verificare che il database da importare venga rilevato e visualizzato.

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

   Se nel database sono configurate le credenziali, è necessario creare una credenziale corrispondente in SnapCenter, assegnarla al database ed eseguire di nuovo il rilevamento del database. Se il database risiede in 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 CLI di SnapManager per Oracle o SnapManager per SAP (ad esempio il comando per sospendere le pianificazioni) da SnapManager per Oracle o SnapManager per host 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 sspap credential set per ogni profilo sull'host.

8. Assicurarsi che FQDN (Fully Qualified Domain Name) dell'host di database sia visualizzato quando si esegue hostname -F.

   Se FQDN non viene visualizzato, è necessario modificare /etc/hosts per specificare l'FQDN dell'host.

Importare i dati

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

A proposito di questa attività

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

- Le policy create per i profili senza operazioni e pianificazioni hanno il formato SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED.

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

Fasi

1. Accedere all'host di database che si desidera importare.
2. Eseguire lo strumento di importazione eseguendo lo script sc-migra situato in */opt/NetApp/Snapcenter/spl/bin*.
3. Immettere il nome utente e la password del server SnapCenter.

   Una volta convalidate 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. Inserire i dettagli del database di destinazione.

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

6. Se si desidera generare un log di sistema o inviare messaggi ASUP per operazioni non riuscite, è necessario attivarli 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 di SnapCenter creati durante l'operazione di importazione.

Risultati

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

Una volta importati 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 per ogni esecuzione del tool di importazione sono memorizzati 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

Informazioni sul marchio commerciale