



Installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from <https://docs.netapp.com/de-de/snapcenter-61/protect-sco/install-snapcenter-plug-in-for-oracle-workflow.html> on November 06, 2025. Always check docs.netapp.com for the latest.

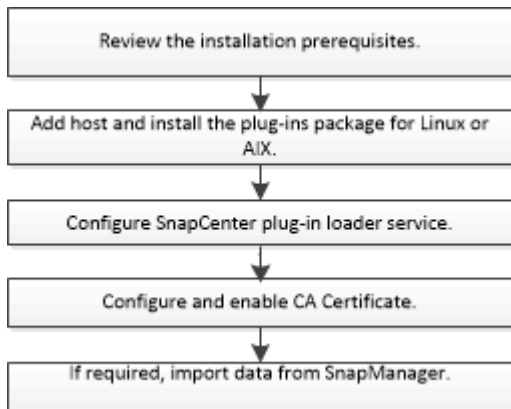
Inhalt

Installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank	1
Installationsworkflow des SnapCenter Plug-ins für Oracle-Datenbanken	1
Voraussetzungen für das Hinzufügen von Hosts und die Installation des Plug-In-Pakets für Linux oder AIX	1
Linux-Hostanforderungen	2
AIX-Hostanforderungen	5
Einrichten von Anmeldeinformationen	8
Konfigurieren der Anmeldeinformationen für eine Oracle-Datenbank	9
Fügen Sie Hosts hinzu und installieren Sie das Plug-In-Paket für Linux oder AIX über die GUI	11
Überwachen des Installationsstatus	14
Alternative Möglichkeiten zur Installation des Plug-In-Pakets für Linux oder AIX	15
Installieren Sie mithilfe von Cmdlets auf mehreren Remotehosts	15
Auf Clusterhost installieren	16
Installieren Sie das Plug-In-Paket für Linux im unbeaufsichtigten Modus	16
Installieren Sie das Plug-In-Paket für AIX im unbeaufsichtigten Modus	17
Konfigurieren des SnapCenter Plug-in Loader -Dienstes	18
Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Dienst auf dem Linux-Host	21
Verwalten Sie das Kennwort für den SPL-Schlüsselspeicher und den Alias des verwendeten CA-signierten Schlüsselpaars	22
Konfigurieren Sie Stamm- oder Zwischenzertifikate für den SPL-Truststore	22
Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Vertrauensspeicher	23
Konfigurieren der Zertifikatsperrliste (CRL) für SPL	24
CA-Zertifikate für Plug-Ins aktivieren	24
Importieren Sie Daten aus SnapManager für Oracle und SnapManager für SAP in SnapCenter	25
Unterstützte Konfigurationen für den Datenimport	26
Was wird in SnapCenter importiert?	26
Was nicht in SnapCenter importiert wird	28
Vorbereiten des Datenimports	29
Daten importieren	30

Installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank

Installationsworkflow des SnapCenter Plug-ins für Oracle-Datenbanken

Sie sollten das SnapCenter -Plug-in für Oracle Database installieren und einrichten, wenn Sie Oracle-Datenbanken schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und die Installation des Plug-In-Pakets für Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-In-Pakete installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.

Das SnapCenter Plug-in für Oracle Database kann von einem Nicht-Root-Benutzer installiert werden. Sie sollten jedoch die Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um den Plug-In-Prozess zu installieren und zu starten. Nach der Installation des Plug-Ins werden die Prozesse effektiv als Nicht-Root-Benutzer ausgeführt.

- Wenn Sie das SnapCenter Plug-ins-Paket für AIX auf einem AIX-Host installieren, sollten Sie die symbolischen Links auf Verzeichnisebene manuell aufgelöst haben.

Das SnapCenter Plug-ins-Paket für AIX löst automatisch den symbolischen Link auf Dateiebene auf, nicht jedoch die symbolischen Links auf Verzeichnisebene, um den absoluten Pfad JAVA_HOME zu erhalten.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus „Linux“ oder „AIX“ für den Installationsbenutzer.
- Sie müssen Java 11 auf Ihrem Linux- oder AIX-Host installiert haben.
 - Java von Oracle und OpenJDK wird für Linux unterstützt
 - IBM Java für AIX. Sie können von herunterladen ["IBM Semeru Runtimes-Downloads"](#)



Stellen Sie sicher, dass Sie nur die zertifizierte Edition von JAVA 11 auf dem Linux-Host installiert haben.

- Für Oracle-Datenbanken, die auf einem Linux- oder AIX-Host ausgeführt werden, sollten Sie sowohl das SnapCenter -Plug-in für Oracle-Datenbanken als auch das SnapCenter -Plug-in für UNIX installieren.



Mit dem Plug-in für Oracle-Datenbanken können Sie auch Oracle-Datenbanken für SAP verwalten. Die SAP BR*Tools-Integration wird jedoch nicht unterstützt.

- Wenn Sie die Oracle-Datenbank 11.2.0.3 oder höher verwenden, müssen Sie den Oracle-Patch 13366202 installieren.



Die UUID-Zuordnung in der Datei /etc/fstab wird von SnapCenter nicht unterstützt.

- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

Linux-Hostanforderungen

Sie sollten sicherstellen, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren.

Artikel	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux  Wenn Sie eine Oracle-Datenbank auf LVM in den Betriebssystemen Oracle Linux oder Red Hat Enterprise Linux 6.6 oder 7.0 verwenden, müssen Sie die neueste Version von Logical Volume Manager (LVM) installieren. • SUSE Linux Enterprise Server (SLES)
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	2 GB

Artikel	Anforderungen
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	2 GB  Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle und OpenJDK  Stellen Sie sicher, dass Sie nur die zertifizierte Edition von JAVA 11 auf dem Linux-Host installiert haben. Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option <code>JAVA_HOME</code> unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#) .

Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host

SnapCenter 2.0 und spätere Versionen ermöglichen es einem Nicht-Root-Benutzer, das SnapCenter -Plug-In -Paket für Linux zu installieren und den Plug-In-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#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
```

Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

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

Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.

```

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 SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „/`<crs_home>`/bin/olsnodes“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`LINUX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den Prüfsummenwert aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

AIX-Hostanforderungen

Sie sollten sicherstellen, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter Plug-Ins-Paket für AIX installieren.



Das SnapCenter -Plug-in für UNIX, das Teil des SnapCenter Plug-in-Pakets für AIX ist, unterstützt keine gleichzeitigen Volume-Gruppen.

Artikel	Anforderungen
Betriebssysteme	AIX 7.1 oder höher
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	4 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	2 GB  Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 IBM Java Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option <code>JAVA_HOME</code> unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#).

Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host

SnapCenter 4.4 und höher ermöglicht es einem Nicht-Root-Benutzer, das SnapCenter Plug-ins-Paket für AIX zu installieren und den Plug-in-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:


```
#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
```

Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/bin/spl

Schritte

1. Melden Sie sich beim AIX-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für AIX installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.

```
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_Precchecks.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
```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „`/<crs_home>/bin/olsnodes`“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`AIX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

Einrichten von Anmeldeinformationen

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation des Plug-In-Pakets auf Linux- oder AIX-Hosts erstellen.

Über diese Aufgabe

Die Anmeldeinformationen werden entweder für den Root-Benutzer oder für einen Nicht-Root-Benutzer erstellt, der über Sudo-Berechtigungen zum Installieren und Starten des Plug-In-Prozesses verfügt.

Weitere Informationen finden Sie unter: [Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host](#) oder [Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host](#)

Best Practice: Obwohl Sie Anmeldeinformationen nach der Bereitstellung von Hosts und der Installation von Plug-Ins erstellen dürfen, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die Anmeldeinformationen ein:

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.

Für dieses Feld...	Machen Sie Folgendes...
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind: ◦ <i>NetBIOS\Benutzername</i> ◦ <i>Domänen-FQDN\Benutzername</i> • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i>
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten. Wählen Sie je nach Betriebssystem des Plug-in-Hosts entweder Linux oder AIX aus.
Verwenden Sie Sudo-Berechtigungen	Aktivieren Sie das Kontrollkästchen Sudo-Berechtigungen verwenden, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite **Benutzer und Zugriff** zuweisen.

Konfigurieren der Anmeldeinformationen für eine Oracle-Datenbank

Sie müssen Anmeldeinformationen konfigurieren, die zum Ausführen von Datenschutzvorgängen in Oracle-Datenbanken verwendet werden.

Über diese Aufgabe

Sie sollten die verschiedenen für die Oracle-Datenbank unterstützten Authentifizierungsmethoden überprüfen. Weitere Informationen finden Sie unter "[Authentifizierungsmethoden für Ihre Anmeldeinformationen](#)".

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, muss der Benutzername mindestens über Ressourcengruppen- und Sicherungsrechte verfügen.

Wenn Sie die Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ressourcenansicht ein rotes Vorhängeschlosssymbol angezeigt. Sie müssen Datenbankanmeldeinformationen konfigurieren, um die Datenbank schützen zu können, oder sie der Ressourcengruppe hinzufügen, um Datenschutzvorgänge durchzuführen.



Wenn Sie beim Erstellen eines Berechtigungsnachweises falsche Angaben machen, wird eine Fehlermeldung angezeigt. Sie müssen auf **Abbrechen** klicken und es dann erneut versuchen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Ansicht“ die Option „Datenbank“ aus.
3. Klicken  und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern.

Sie können dann auf , um den Filterbereich zu schließen.

4. Wählen Sie die Datenbank aus und klicken Sie dann auf **Datenbankeinstellungen > Datenbank konfigurieren**.
5. Wählen Sie im Abschnitt „Datenbankeinstellungen konfigurieren“ aus der Dropdownliste **Vorhandene Anmeldeinformationen verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datenschutzjobs in der Oracle-Datenbank verwendet werden sollen.



Der Oracle-Benutzer sollte über Sysdba-Berechtigungen verfügen.

Sie können auch Anmeldeinformationen erstellen, indem Sie auf .

6. Wählen Sie im Abschnitt „ASM-Einstellungen konfigurieren“ aus der Dropdownliste **Vorhandene Anmeldeinformationen verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datenschutzjobs auf der ASM-Instanz verwendet werden sollen.



Der ASM-Benutzer sollte über Sysasm-Berechtigungen verfügen.

Sie können auch Anmeldeinformationen erstellen, indem Sie auf .

7. Wählen Sie im Abschnitt „RMAN-Katalogeinstellungen konfigurieren“ aus der Dropdownliste **Vorhandene Anmeldeinformationen verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datenschutzjobs in der Oracle Recovery Manager (RMAN)-Katalogdatenbank verwendet werden sollen.

Sie können auch Anmeldeinformationen erstellen, indem Sie auf .

Geben Sie im Feld **TNSName** den Dateinamen des Transparent Network Substrate (TNS) ein, der vom SnapCenter -Server zur Kommunikation mit der Datenbank verwendet wird.

8. Geben Sie im Feld **Bevorzugte RAC-Knoten** die für die Sicherung bevorzugten Real Application Cluster

(RAC)-Knoten an.

Bei den bevorzugten Knoten kann es sich um einen oder alle Clusterknoten handeln, auf denen die RAC-Datenbankinstanzen vorhanden sind. Der Sicherungsvorgang wird nur auf diesen bevorzugten Knoten in der Reihenfolge der Präferenz ausgelöst.

In RAC One Node ist nur ein Knoten in den bevorzugten Knoten aufgeführt, und dieser bevorzugte Knoten ist der Knoten, auf dem die Datenbank derzeit gehostet wird.

Nach einem Failover oder einer Verlagerung der RAC One Node-Datenbank wird durch die Aktualisierung der Ressourcen auf der SnapCenter Ressourcenseite der Host aus der Liste **Bevorzugte RAC-Knoten** entfernt, auf dem die Datenbank zuvor gehostet wurde. Der RAC-Knoten, auf den die Datenbank verschoben wird, wird in **RAC-Knoten** aufgeführt und muss manuell als bevorzugter RAC-Knoten konfiguriert werden.

Weitere Informationen finden Sie unter ["Bevorzugte Knoten im RAC-Setup"](#) .

9. Klicken Sie auf **OK**.

Fügen Sie Hosts hinzu und installieren Sie das Plug-In-Paket für Linux oder AIX über die GUI

Sie können auf der Seite „Host hinzufügen“ Hosts hinzufügen und dann das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

Über diese Aufgabe

Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie das Plug-in auf einem Cluster (Oracle RAC) installieren, wird das Plug-in auf allen Knoten des Clusters installiert. Für Oracle RAC One Node sollten Sie das Plug-in sowohl auf aktiven als auch auf passiven Knoten installieren.



Wenn Sie das Plug-In auf einem Oracle RAC installieren, wird nur die kennwortbasierte Authentifizierung unterstützt. Die auf SSH-Schlüsseln basierende Authentifizierung wird nicht unterstützt.

Ihnen sollte eine Rolle zugewiesen werden, die über die Berechtigung zum Installieren und Deinstallieren des Plug-Ins verfügt, beispielsweise die SnapCenter Administratorrolle.



Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Hosttyp	Wählen Sie Linux oder AIX als Hosttyp. Der SnapCenter -Server fügt den Host hinzu und installiert dann das Plug-in für Oracle Database und das Plug-in für UNIX, falls die Plug-ins nicht bereits auf dem Host installiert sind.
Hostname	Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben. Sie können die IP-Adressen oder den FQDN eines der folgenden Elemente eingeben: • Eigenständiger Host • Jeder Knoten in der Oracle Real Application Clusters (RAC)-Umgebung  Knoten-VIP oder Scan-IP wird nicht unterstützt Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.
Anmeldeinformationen	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.  Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

6. (Optional) Klicken Sie auf **Weitere Optionen**.

Für dieses Feld...	Machen Sie Folgendes...
Hafen	Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an. Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.  Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist <code>/opt/NetApp/snapcenter</code>. Optional können Sie den Pfad anpassen.
Alle Hosts im Oracle RAC hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem Oracle RAC hinzuzufügen. In einem Flex ASM-Setup werden alle Knoten hinzugefügt, unabhängig davon, ob es sich um einen Hub- oder Leaf-Knoten handelt.
Überspringen optionaler Vorinstallationsprüfungen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen „Vorabprüfungen überspringen“ nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob er die Anforderungen für die Installation des Plug-Ins erfüllt.



Das Vorabprüfungsskript validiert den Firewall-Status des Plug-In-Ports nicht, wenn dieser in den Ablehnungsregeln der Firewall angegeben ist.

Sollten die Mindestanforderungen nicht erfüllt sein, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt. Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei `web.config` unter `C:\Programme\NetApp\ SnapCenter WebApp` aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, sollten Sie das Problem beheben.



Wenn Sie in einem HA-Setup die Datei web.config aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

- Überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



SnapCenter unterstützt den ECDSA-Algorithmus nicht.



Die Überprüfung des Fingerabdrucks ist obligatorisch, auch wenn derselbe Host zuvor zu SnapCenter hinzugefügt und der Fingerabdruck bestätigt wurde.

- Überwachen Sie den Installationsfortschritt.

Die installationsspezifischen Protokolldateien befinden sich unter `/custom_location/snapcenter/logs`.

Ergebnis

Alle Datenbanken auf dem Host werden automatisch erkannt und auf der Ressourcenseite angezeigt. Wenn nichts angezeigt wird, klicken Sie auf **Ressourcen aktualisieren**.

Überwachen des Installationsstatus

Sie können den Fortschritt der Installation des SnapCenter -Plug-In-Pakets auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Installationsfortschritt überprüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange

Schritte

- Klicken Sie im linken Navigationsbereich auf **Monitor**.
- Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
- Um auf der Seite **Jobs** die Liste so zu filtern, dass nur Plug-In-Installationsvorgänge aufgeführt werden, gehen Sie wie folgt vor:
 - Klicken Sie auf **Filter**.
 - Optional: Geben Sie das Start- und Enddatum an.
 - Wählen Sie im Dropdown-Menü „Typ“ die Option „Plug-in-Installation“ aus.
 - Wählen Sie im Dropdown-Menü „Status“ den Installationsstatus aus.

- e. Klicken Sie auf **Übernehmen**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

Alternative Möglichkeiten zur Installation des Plug-In-Pakets für Linux oder AIX

Sie können das Plug-In-Paket für Linux oder AIX auch manuell installieren, indem Sie entweder die Cmdlets oder CLIs verwenden.

Bevor Sie das Plug-in manuell installieren, sollten Sie die Signatur des Binärpakets mithilfe der Schlüssel **snapcenter_public_key.pub** und **snapcenter_linux_host_plugin.bin.sig** unter *C:\ProgramData\NetApp\SnapCenter\Package Repository* validieren.



Stellen Sie sicher, dass **OpenSSL 1.0.2g** auf dem Host installiert ist, auf dem Sie das Plug-in installieren möchten.

Validieren Sie die Signatur des Binärpakets, indem Sie den folgenden Befehl ausführen:

- Für Linux-Host: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Für AIX-Host: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

Installieren Sie mithilfe von Cmdlets auf mehreren Remotehosts

Sie sollten das PowerShell-Cmdlet *Install-SmHostPackage* verwenden, um das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX auf mehreren Hosts zu installieren.

Was Sie brauchen

Sie sollten auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet sein.

Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX mit dem Cmdlet *Install-SmHostPackage* und den erforderlichen Parametern.

Sie können die Option *-skippercheck* verwenden, wenn Sie die Plug-Ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.



Das Vorabprüfungsskript validiert den Firewall-Status des Plug-In-Ports nicht, wenn dieser in den Ablehnungsregeln der Firewall angegeben ist.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Auf Clusterhost installieren

Sie sollten das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX auf beiden Knoten des Clusterhosts installieren.

Jeder Knoten des Cluster-Hosts hat zwei IPs. Eine der IPs ist die öffentliche IP der jeweiligen Knoten und die zweite IP ist die Cluster-IP, die von beiden Knoten gemeinsam genutzt wird.

Schritte

1. Installieren Sie das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX auf beiden Knoten des Clusterhosts.
2. Überprüfen Sie, ob die richtigen Werte für die Parameter `SNAPCENTER_SERVER_HOST`, `SPL_PORT`, `SNAPCENTER_SERVER_PORT` und `SPL_ENABLED_PLUGINS` in der Datei `spl.properties` unter `/var/opt/snapcenter/spl/etc/` angegeben sind.

Wenn `SPL_ENABLED_PLUGINS` in `spl.properties` nicht angegeben ist, können Sie es hinzufügen und den Wert `SCO,SCU` zuweisen.

3. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
4. Legen Sie in jedem Knoten die bevorzugten IPs des Knotens mit dem `sccli`-Befehl *Set-PreferredHostIPsInStorageExportPolicy* und den erforderlichen Parametern fest.
5. Fügen Sie im SnapCenter Server-Host einen Eintrag für die Cluster-IP und den entsprechenden DNS-Namen in `C:\Windows\System32\drivers\etc\hosts` hinzu.
6. Fügen Sie den Knoten mit dem Cmdlet *Add-SmHost* zum SnapCenter -Server hinzu, indem Sie die Cluster-IP für den Hostnamen angeben.

Ermitteln Sie die Oracle-Datenbank auf Knoten 1 (vorausgesetzt, die Cluster-IP wird auf Knoten 1 gehostet) und erstellen Sie eine Sicherungskopie der Datenbank. Wenn ein Failover auftritt, können Sie die auf Knoten 1 erstellte Sicherung verwenden, um die Datenbank auf Knoten 2 wiederherzustellen. Sie können das auf Knoten 1 erstellte Backup auch verwenden, um einen Klon auf Knoten 2 zu erstellen.



Wenn das Failover erfolgt, während andere SnapCenter -Vorgänge ausgeführt werden, bleiben veraltete Volumes, Verzeichnisse und Sperrdateien übrig.

Installieren Sie das Plug-In-Paket für Linux im unbeaufsichtigten Modus

Sie können das SnapCenter Plug-Ins-Paket für Linux im unbeaufsichtigten Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-In-Pakets überprüfen.
- Sie sollten sicherstellen, dass die Umgebungsvariable `DISPLAY` nicht festgelegt ist.

Wenn die Umgebungsvariable `DISPLAY` festgelegt ist, sollten Sie `unset DISPLAY` ausführen und dann versuchen, das Plug-In manuell zu installieren.

Über diese Aufgabe

Bei der Installation im Konsolenmodus müssen Sie die erforderlichen Installationsinformationen angeben, bei der Installation im unbeaufsichtigten Modus hingegen müssen Sie keine Installationsinformationen angeben.

Schritte

1. Laden Sie das SnapCenter Plug-Ins-Paket für Linux vom Installationsort des SnapCenter Servers herunter.

Der Standardinstallationspfad ist *C:\ProgramData\NetApp\ SnapCenter\PackageRepository*. Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.

3. Laufen

```
./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. Bearbeiten Sie die Datei *spl.properties* unter */var/opt/snapcenter/spl/etc/*, um *SPL_ENABLED_PLUGINS=SCO,SCU* hinzuzufügen, und starten Sie dann den Dienst SnapCenter Plug-in Loader neu.



Durch die Installation des Plug-In-Pakets werden die Plug-Ins auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie sollten die Plug-Ins auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter -GUI oder des PowerShell-Cmdlets hinzufügen. Wählen Sie beim Hinzufügen des Hosts „Keine“ als Anmeldeinformationen aus. Nachdem der Host hinzugefügt wurde, werden die installierten Plug-Ins automatisch erkannt.

Installieren Sie das Plug-In-Paket für AIX im unbeaufsichtigten Modus

Sie können das SnapCenter Plug-ins-Paket für AIX im unbeaufsichtigten Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-In-Pakets überprüfen.
- Sie sollten sicherstellen, dass die Umgebungsvariable *DISPLAY* nicht festgelegt ist.

Wenn die Umgebungsvariable *DISPLAY* festgelegt ist, sollten Sie *unset DISPLAY* ausführen und dann versuchen, das Plug-In manuell zu installieren.

Schritte

1. Laden Sie das SnapCenter Plug-ins-Paket für AIX vom Installationsort des SnapCenter Servers herunter.

Der Standardinstallationspfad ist *C:\ProgramData\NetApp\ SnapCenter\PackageRepository*. Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.

3. Laufen

```
./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. Bearbeiten Sie die Datei `spl.properties` unter `/var/opt/snapcenter/spl/etc/`, um `SPL_ENABLED_PLUGINS=SCO,SCU` hinzuzufügen, und starten Sie dann den Dienst SnapCenter Plug-in Loader neu.



Durch die Installation des Plug-In-Pakets werden die Plug-Ins auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie sollten die Plug-Ins auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter -GUI oder des PowerShell-Cmdlets hinzufügen. Wählen Sie beim Hinzufügen des Hosts „Keine“ als Anmeldeinformationen aus. Nachdem der Host hinzugefügt wurde, werden die installierten Plug-Ins automatisch erkannt.

Konfigurieren des SnapCenter Plug-in Loader -Dienstes

Der SnapCenter Plug-in Loader -Dienst lädt das Plug-in-Paket für Linux oder AIX, um mit dem SnapCenter Server zu interagieren. Der SnapCenter Plug-in Loader -Dienst wird installiert, wenn Sie das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX installieren.

Über diese Aufgabe

Nach der Installation des SnapCenter Plug-ins-Pakets für Linux oder des SnapCenter Plug-ins-Pakets für AIX wird der SnapCenter Plug-in Loader -Dienst automatisch gestartet. Wenn der SnapCenter Plug-in Loader -Dienst nicht automatisch gestartet wird, sollten Sie:

- Stellen Sie sicher, dass das Verzeichnis, in dem das Plug-In ausgeführt wird, nicht gelöscht wird
- Erhöhen Sie den der Java Virtual Machine zugewiesenen Speicherplatz

Die Datei `spl.properties`, die sich unter `/custom_location/ NetApp/snapcenter/spl/etc/` befindet, enthält die folgenden Parameter. Diesen Parametern sind Standardwerte zugewiesen.

Parametername	Beschreibung
LOG_LEVEL	Zeigt die unterstützten Protokollebenen an. Die möglichen Werte sind TRACE, DEBUG, INFO, WARN, ERROR und FATAL.
SPL_PROTOCOL	Zeigt das vom SnapCenter Plug-in Loader unterstützte Protokoll an. Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.

Parametername	Beschreibung
SNAPCENTER_SERVER_PROTOKOLL	Zeigt das vom SnapCenter Server unterstützte Protokoll an. Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SKIP_JAVAHOME_UPDATE	Standardmäßig erkennt der SPL-Dienst den Java-Pfad und aktualisiert den JAVA_HOME-Parameter. Daher ist der Standardwert auf FALSE gesetzt. Sie können es auf TRUE setzen, wenn Sie das Standardverhalten deaktivieren und den Java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Passwort der Keystore-Datei an. Sie können diesen Wert nur ändern, wenn Sie das Kennwort ändern oder eine neue Keystore-Datei erstellen.
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter Plug-in Loader -Dienst ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.  Sie sollten den Wert nach der Installation der Plug-Ins nicht mehr ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter -Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Keystore-Datei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter -Server ausgeführt wird.

Parametername	Beschreibung
LOGS_MAX_COUNT	Zeigt die Anzahl der Protokolldateien des SnapCenter Plug-in Loader an, die im Ordner <code>/custom_location/snapcenter/spl/logs</code> gespeichert sind. Der Standardwert ist auf 5000 eingestellt. Wenn die Anzahl größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Überprüfung der Anzahl der Dateien erfolgt automatisch alle 24 Stunden ab dem Start des SnapCenter Plug-in Loader -Dienstes.  Wenn Sie die Datei „spl.properties“ manuell löschen, wird die Anzahl der beizubehaltenden Dateien auf 9999 festgelegt.
JAVA_HOME	Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird. Dieser Pfad wird während der Installation und beim Starten von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Protokolldatei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei komprimiert und die Protokolle in die neue Datei dieses Auftrags geschrieben.
Protokolle der letzten Tage aufbewahren	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
Zertifikatsvalidierung aktivieren	Zeigt „true“ an, wenn die CA-Zertifikatsvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder durch Bearbeiten der spl.properties oder mithilfe der SnapCenter -GUI oder des Cmdlets aktivieren oder deaktivieren.

Wenn einem dieser Parameter nicht der Standardwert zugewiesen ist oder Sie den Wert zuweisen oder ändern möchten, können Sie die Datei spl.properties ändern. Sie können auch die Datei „spl.properties“ überprüfen und bearbeiten, um alle Probleme im Zusammenhang mit den den Parametern zugewiesenen Werten zu beheben. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter Plug-in Loader -Dienst neu starten.

Schritte

1. Führen Sie je nach Bedarf eine der folgenden Aktionen aus:

- Starten Sie den SnapCenter Plug-in Loader -Dienst:
 - Führen Sie als Root-Benutzer Folgendes aus:
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
 - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
- Stoppen Sie den SnapCenter Plug-in Loader -Dienst:
 - Führen Sie als Root-Benutzer Folgendes aus:
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`



Sie können die Option `-force` mit dem Stoppbefehl verwenden, um den SnapCenter Plug-in Loader -Dienst zwangsweise zu stoppen. Allerdings sollten Sie dabei vorsichtig sein, da dadurch auch die bestehenden Vorgänge beendet werden.

- Starten Sie den SnapCenter Plug-in Loader -Dienst neu:
 - Führen Sie als Root-Benutzer Folgendes aus:
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Ermitteln Sie den Status des SnapCenter Plug-in Loader Dienstes:
 - Führen Sie als Root-Benutzer Folgendes aus:
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Suchen Sie die Änderung im SnapCenter Plug-in Loader -Dienst:
 - Führen Sie als Root-Benutzer Folgendes aus:
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl change`

Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Dienst auf dem Linux-Host

Sie sollten das Kennwort des SPL-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den SPL-Truststore konfigurieren und das von der CA signierte Schlüsselpaar für den SPL-Truststore mit dem SnapCenter Plug-in Loader -Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.



SPL verwendet die Datei „`keystore.jks`“, die sich unter „`/var/opt/snapcenter/spl/etc`“ befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den SPL-Schlüsselspeicher und den Alias des verwendeten CA-signierten Schlüsselpaars

Schritte

1. Sie können das Standardkennwort für den SPL-Schlüsselspeicher aus der SPL-Eigenschaftendatei abrufen.

Dies ist der Wert, der dem Schlüssel „SPL_KEYSTORE_PASS“ entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks  
. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge  
im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher  
verwendet wird:
```

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

Aktualisieren Sie dasselbe für den Schlüssel SPL_KEYSTORE_PASS in der Datei spl.properties.

3. Starten Sie den Dienst nach der Änderung des Kennworts neu.



Das Kennwort für den SPL-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den SPL-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den SPL-Truststore konfigurieren.

Schritte

1. Navigieren Sie zum Ordner, der den SPL-Schlüsselspeicher enthält: */var/opt/snapcenter/spl/etc*.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks  
. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:
```



```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks  
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder  
Zwischenzertifikate für den SPL-Truststore konfiguriert haben.
```



Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Vertrauensspeicher

Sie sollten das von der CA signierte Schlüsselpaar für den SPL-Truststore konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher /var/opt/snapcenter/spl/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks  
. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel  
hinzu.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS  
. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.
```

```
keytool -list -v -keystore keystore.jks  
. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem  
neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt  
wurde.  
. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-  
Zertifikat in das Schlüsselspeicherkenwort.
```

Das Standardkennwort für den SPL-Schlüsselspeicher ist der Wert des Schlüssels
SPL_KEYSTORE_PASS in der Datei spl.properties.

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

. Wenn der Aliasname im CA-Zertifikat lang ist und Leerzeichen oder Sonderzeichen („*“, „“,“) enthält, ändern Sie den Aliasnamen in einen einfachen Namen:

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
```

. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher in der Datei `spl.properties`.

Aktualisieren Sie diesen Wert anhand des Schlüssels `SPL_CERTIFICATE_ALIAS`.

4. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

- SPL sucht in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SPL ist `/var/opt/snapcenter/spl/etc/crl`.

Schritte

1. Sie können das Standardverzeichnis in der Datei `spl.properties` anhand des Schlüssels `SPL_CRL_PATH` ändern und aktualisieren.
2. Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen.

Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

CA-Zertifikate für Plug-Ins aktivieren

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter -Server und den entsprechenden Plug-In-Hosts bereitstellen. Sie sollten die CA-Zertifikatvalidierung für die Plug-Ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „*Set-SmCertificateSettings*“ aktivieren oder deaktivieren.
- Den Zertifikatsstatus der Plug-Ins können Sie sich mit *Get-SmCertificateSettings* anzeigen lassen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die [Referenzhandbuch für SnapCenter -Software-Cmdlets](#) .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie einzelne oder mehrere Plug-In-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung aktivieren**.

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss angezeigt und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- *  * zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-In-Host zugewiesen ist.
- *  * zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- *  * zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- *  * zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.



Wenn der Status gelb oder grün ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.

Importieren Sie Daten aus SnapManager für Oracle und SnapManager für SAP in SnapCenter

Durch das Importieren von Daten aus SnapManager für Oracle und SnapManager für SAP in SnapCenter können Sie Ihre Daten aus früheren Versionen weiterhin verwenden.

Sie können Daten von SnapManager für Oracle und SnapManager für SAP in SnapCenter importieren, indem Sie das Importtool über die Befehlszeilenschnittstelle (Linux-Host-CLI) ausführen.

Das Importtool erstellt Richtlinien und Ressourcengruppen in SnapCenter. Die in SnapCenter erstellten Richtlinien und Ressourcengruppen entsprechen den Profilen und Vorgängen, die mit diesen Profilen in SnapManager für Oracle und SnapManager für SAP ausgeführt werden. Das SnapCenter Importtool interagiert mit den Repository-Datenbanken SnapManager für Oracle und SnapManager für SAP und der Datenbank, die Sie importieren möchten.

- Ruft alle Profile, Zeitpläne und Vorgänge ab, die mit den Profilen ausgeführt wurden.
- Erstellt eine SnapCenter -Sicherungsrichtlinie für jeden einzelnen Vorgang und jeden Zeitplan, der einem Profil zugeordnet ist.
- Erstellt eine Ressourcengruppe für jede Zieldatenbank.

Sie können das Importtool ausführen, indem Sie das Skript `sc-migrate` unter `/opt/NetApp/snapcenter/spl/bin` ausführen. Wenn Sie das SnapCenter Plug-ins-Paket für Linux auf dem Datenbankhost installieren, den Sie importieren möchten, wird das Skript `sc-migrate` nach `/opt/NetApp/snapcenter/spl/bin` kopiert.



Das Importieren von Daten wird von der grafischen Benutzeroberfläche (GUI) von SnapCenter nicht unterstützt.

SnapCenter unterstützt Data ONTAP im 7-Modus nicht. Mit dem 7-Mode Transition Tool können Sie Daten und

Konfigurationen, die auf einem System mit Data ONTAP im 7-Mode gespeichert sind, auf ein ONTAP -System migrieren.

Unterstützte Konfigurationen für den Datenimport

Bevor Sie Daten von SnapManager 3.4.x für Oracle und SnapManager 3.4.x für SAP in SnapCenter importieren, sollten Sie sich über die Konfigurationen im Klaren sein, die mit dem SnapCenter -Plug-in für Oracle-Datenbanken unterstützt werden.

Die Konfigurationen, die mit dem SnapCenter Plug-in für Oracle Database unterstützt werden, sind in der ["NetApp Interoperabilitätsmatrix-Tool"](#) .

Was wird in SnapCenter importiert?

Sie können Profile, Zeitpläne und mithilfe der Profile durchgeführte Vorgänge importieren.

Von SnapManager für Oracle und SnapManager für SAP	Zu SnapCenter
Profile ohne Operationen und Zeitpläne	Es wird eine Richtlinie mit dem Standardsicherungstyp „Online“ und dem Sicherungsumfang „Vollständig“ erstellt.
Profile mit einer oder mehreren Operationen	Mehrere Richtlinien werden basierend auf einer einzigartigen Kombination aus einem Profil und den mit diesem Profil ausgeführten Vorgängen erstellt. Die in SnapCenter erstellten Richtlinien enthalten die aus dem Profil und den entsprechenden Vorgängen abgerufenen Details zum Bereinigen und Aufbewahren des Archivprotokolls.
Profile mit Oracle Recovery Manager (RMAN)-Konfiguration	Richtlinien werden mit aktivierter Option Katalogsicherung mit Oracle Recovery Manager erstellt. Wenn in SnapManager eine externe RMAN-Katalogisierung verwendet wurde, müssen Sie die RMAN-Katalogeinstellungen in SnapCenter konfigurieren. Sie können entweder die vorhandenen Anmeldeinformationen auswählen oder neue Anmeldeinformationen erstellen. Wenn RMAN über die Steuerdatei in SnapManager konfiguriert wurde, müssen Sie RMAN nicht in SnapCenter konfigurieren.
An ein Profil angehängter Zeitplan	Es wird eine Richtlinie nur für den Zeitplan erstellt.

Von SnapManager für Oracle und SnapManager für SAP	Zu SnapCenter
Datenbank	Für jede importierte Datenbank wird eine Ressourcengruppe erstellt. In einem Real Application Clusters (RAC)-Setup wird der Knoten, auf dem Sie das Importtool ausführen, nach dem Import zum bevorzugten Knoten und die Ressourcengruppe wird für diesen Knoten erstellt.



Beim Importieren eines Profils wird zusammen mit der Sicherungsrichtlinie eine Überprüfungsrichtlinie erstellt.

Wenn SnapManager für Oracle und SnapManager für SAP-Profilen, Zeitpläne und alle mit den Profilen ausgeführten Vorgänge in SnapCenter importiert werden, werden auch die verschiedenen Parameterwerte importiert.

SnapManager für Oracle und SnapManager für SAP-Parameter und -Werte	SnapCenter -Parameter und -Werte	Hinweise
Sicherungsumfang • Voll • Daten • Protokoll	Sicherungsumfang • Voll • Daten • Protokoll	
Backup-Modus • Automatisch • Online • Offline	Sicherungstyp • Online • Offline-Herunterfahren	Wenn der Sicherungsmodus „Auto“ ist, überprüft das Importtool den Datenbankstatus zum Zeitpunkt der Ausführung des Vorgangs und legt den Sicherungstyp entsprechend auf „Online-Herunterfahren“ oder „Offline-Herunterfahren“ fest.
Zurückbehaltung • Tage • Zählt	Zurückbehaltung • Tage • Zählt	SnapManager für Oracle und SnapManager für SAP verwenden sowohl Tage als auch Zählwerte, um die Aufbewahrung festzulegen. In SnapCenter gibt es entweder Tage ODER Zählungen. Daher wird die Aufbewahrung in Tagen festgelegt, da die Tage Vorrang vor der Zählung in SnapManager für Oracle und SnapManager für SAP haben.

SnapManager für Oracle und SnapManager für SAP-Parameter und -Werte	SnapCenter -Parameter und -Werte	Hinweise
Beschneiden für Zeitpläne • Alle • Systemänderungsnummer (SCN) • Datum • Protokolle, die vor den angegebenen Stunden, Tagen, Wochen und Monaten erstellt wurden	Beschneiden für Zeitpläne • Alle • Protokolle, die vor den angegebenen Stunden und Tagen erstellt wurden	SnapCenter unterstützt kein Beschneiden basierend auf SCN, Datum, Wochen und Monaten.
Benachrichtigung • E-Mails werden nur bei erfolgreichen Vorgängen gesendet • E-Mails werden nur bei fehlgeschlagenen Vorgängen gesendet • E-Mails werden sowohl bei erfolgreichen als auch bei fehlgeschlagenen Vorgängen gesendet	Benachrichtigung • Stets • Bei einem Fehler • Warnung • Fehler	Die E-Mail-Benachrichtigungen werden importiert. Sie müssen den SMTP-Server jedoch manuell über die SnapCenter -GUI aktualisieren. Der Betreff der E-Mail bleibt leer, damit Sie ihn konfigurieren können.

Was nicht in SnapCenter importiert wird

Das Importtool importiert nicht alles in SnapCenter.

Folgendes können Sie nicht in SnapCenter importieren:

- Metadaten sichern
- Teilsicherungen
- Raw Device Mapping (RDM) und Virtual Storage Console (VSC) bezogene Backups
- Rollen oder alle im SnapManager für Oracle und SnapManager für SAP-Repository verfügbaren Anmeldeinformationen
- Daten im Zusammenhang mit Überprüfungs-, Wiederherstellungs- und Klonvorgängen
- Beschneiden für den Betrieb
- Im SnapManager für Oracle- und SnapManager für SAP-Profil angegebene Replikationsdetails

Nach dem Importieren müssen Sie die entsprechende in SnapCenter erstellte Richtlinie manuell bearbeiten, um die Replikationsdetails einzuschließen.

- Katalogisierte Sicherungsinformationen

Vorbereiten des Datenimports

Bevor Sie Daten in SnapCenter importieren, müssen Sie bestimmte Aufgaben ausführen, um den Importvorgang erfolgreich auszuführen.

Schritte

1. Identifizieren Sie die Datenbank, die Sie importieren möchten.
2. Fügen Sie mithilfe von SnapCenter den Datenbankhost hinzu und installieren Sie das SnapCenter Plug-ins-Paket für Linux.
3. Richten Sie mithilfe von SnapCenter die Verbindungen für die von den Datenbanken auf dem Host verwendeten Storage Virtual Machines (SVMs) ein.
4. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
5. Stellen Sie auf der Seite „Ressourcen“ sicher, dass die zu importierende Datenbank erkannt und angezeigt wird.

Wenn Sie das Importtool ausführen möchten, muss auf die Datenbank zugegriffen werden können, sonst schlägt die Erstellung der Ressourcengruppe fehl.

Wenn für die Datenbank Anmeldeinformationen konfiguriert sind, müssen Sie in SnapCenter entsprechende Anmeldeinformationen erstellen, die Anmeldeinformationen der Datenbank zuweisen und dann die Erkennung der Datenbank erneut ausführen. Wenn sich die Datenbank auf Automatic Storage Management (ASM) befindet, müssen Sie Anmeldeinformationen für die ASM-Instanz erstellen und die Anmeldeinformationen der Datenbank zuweisen.

6. Stellen Sie sicher, dass der Benutzer, der das Importtool ausführt, über ausreichende Berechtigungen verfügt, um SnapManager für Oracle- oder SnapManager für SAP-CLI-Befehle (wie den Befehl zum Anhalten von Zeitplänen) vom SnapManager für Oracle- oder SnapManager für SAP-Host aus auszuführen.
7. Führen Sie die folgenden Befehle auf dem SnapManager für Oracle- oder SnapManager für SAP-Host aus, um die Zeitpläne auszusetzen:
 - a. Wenn Sie die Zeitpläne auf dem SnapManager für Oracle-Host aussetzen möchten, führen Sie Folgendes aus:

- `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`



Sie müssen den Befehl „smo credential set“ für jedes Profil auf dem Host ausführen.

- b. Wenn Sie die Zeitpläne auf dem SnapManager für SAP-Host aussetzen möchten, führen Sie Folgendes aus:

- `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`



Sie müssen den Befehl „Smsap Credential Set“ für jedes Profil auf dem Host ausführen.

8. Stellen Sie sicher, dass der vollqualifizierte Domänenname (FQDN) des Datenbankhosts angezeigt wird, wenn Sie `hostname -f` ausführen.

Wenn der FQDN nicht angezeigt wird, müssen Sie `/etc/hosts` ändern, um den FQDN des Hosts anzugeben.

Daten importieren

Sie können Daten importieren, indem Sie das Importtool vom Datenbankhost ausführen.

Über diese Aufgabe

Die nach dem Import erstellten SnapCenter -Sicherungsrichtlinien haben unterschiedliche Namensformate:

- Für Profile ohne Vorgänge und Zeitpläne erstellte Richtlinien haben das Format `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED`.

Wenn kein Vorgang mithilfe eines Profils ausgeführt wird, wird die entsprechende Richtlinie mit dem Standardsicherungstyp „Online“ und dem Sicherungsumfang „Vollständig“ erstellt.

- Für die Profile mit einem oder mehreren Vorgängen erstellte Richtlinien haben das Format `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.
- Für die an die Profile angehängten Zeitpläne erstellte Richtlinien haben das Format `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.

Schritte

1. Melden Sie sich beim Datenbankhost an, den Sie importieren möchten.
2. Führen Sie das Importtool aus, indem Sie das Skript `sc-migrate` unter `/opt/NetApp/snapcenter/spl/bin` ausführen.
3. Geben Sie den Benutzernamen und das Kennwort des SnapCenter -Servers ein.

Nach der Validierung der Anmeldeinformationen wird eine Verbindung mit SnapCenter hergestellt.

4. Geben Sie die Repository-Datenbankdetails von SnapManager für Oracle oder SnapManager für SAP ein.

Die Repository-Datenbank listet die Datenbanken auf, die auf dem Host verfügbar sind.

5. Geben Sie die Details der Zieldatenbank ein.

Wenn Sie alle Datenbanken auf dem Host importieren möchten, geben Sie „all“ ein.

6. Wenn Sie ein Systemprotokoll erstellen oder ASUP-Nachrichten für fehlgeschlagene Vorgänge senden möchten, müssen Sie diese entweder durch Ausführen des Befehls `Add-SmStorageConnection` oder `Set-`

SmStorageConnection aktivieren.



Wenn Sie einen Importvorgang abbrechen möchten, entweder während der Ausführung des Importtools oder nach dem Importieren, müssen Sie die SnapCenter -Richtlinien, Anmeldeinformationen und Ressourcengruppen, die im Rahmen des Importvorgangs erstellt wurden, manuell löschen.

Ergebnisse

Die SnapCenter -Sicherungsrichtlinien werden für Profile, Zeitpläne und Vorgänge erstellt, die mithilfe der Profile ausgeführt werden. Für jede Zieldatenbank werden außerdem Ressourcengruppen erstellt.

Nach dem erfolgreichen Importieren der Daten werden die mit der importierten Datenbank verknüpften Zeitpläne in SnapManager für Oracle und SnapManager für SAP angehalten.



Nach dem Importieren müssen Sie die importierte Datenbank oder das Dateisystem mit SnapCenter verwalten.

Die Protokolle für jede Ausführung des Importtools werden im Verzeichnis */var/opt/snapcenter/spl/logs* unter dem Namen *spl_migration_timestamp.log* gespeichert. Sie können dieses Protokoll verwenden, um Importfehler zu überprüfen und zu beheben.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.