Schutz von Oracle Datenbanken

SnapCenter Software 4.5

NetApp
September 29, 2025

Inhalt

Schutz von Oracle Datenbanken

Überblick über das SnapCenter Plug-in für Oracle Database

Welche Möglichkeiten bietet das Plug-in für Oracle Database

Das SnapCenter Plug-in für Oracle Database ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das applikationsspezifische Datensicherungsmanagement von Oracle Datenbanken ermöglicht.

Das Plug-in für Oracle Database automatisiert das Backup, die Katalogisierung und die Katalogisierung mit Oracle Recovery Manager (RMAN), Überprüfung, Mounten, Unmounten, Restore, Recovery und Klonen von Oracle Datenbanken in Ihrer SnapCenter Umgebung. Das Plug-in für Oracle Database installiert das SnapCenter Plug-in für UNIX, um alle Datensicherungsvorgänge auszuführen.

Sie können mit dem Plug-in für Oracle Database Backups von Oracle Datenbanken, auf denen SAP Applikationen ausgeführt werden, verwalten. Die Integration von SAP BR*Tools wird jedoch nicht unterstützt.

- Sichern Sie Datendateien, Kontrolldateien und Archivprotokolldateien.

  Backup wird nur auf CDB-Ebene (Container-Datenbank) unterstützt.

- Wiederherstellung und Recovery von Datenbanken, Datenbanken und Plug-in-Datenbanken (PDBs).

  Unvollständige Wiederherstellung von PDBs wird nicht unterstützt.

- Erstellung von Klonen von Produktionsdatenbanken bis zu einem bestimmten Zeitpunkt

  Das Klonen wird nur auf CDB-Ebene unterstützt.

- Sofortige Überprüfung der Backups.
- Mounten und Aufheben von Daten und Protokollierung von Backups für den Wiederherstellungsvorgang.
- Planung von Backup- und Verifizierungsvorgängen
- Monitoring aller Vorgänge
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

Funktionen von Plug-in für Oracle Database

Das Plug-in für Oracle Database ist in die Oracle Datenbank auf dem Linux oder AIX Host und in NetApp Technologien auf dem Storage-System integriert.

- Einheitliche grafische Benutzeroberfläche

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore-, Recovery- und Klonvorgänge über alle Plug-ins hinweg, zentralisierte Berichterstellung, Dashboard-Ansichten auf einen Blick, rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Aufgaben über alle Plug-ins hinweg.

- Automatisierte, zentrale Administration

Sie können Backup- und Klonvorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- Unterbrechungsfreie Technologie zur NetApp Snapshot Kopie

  SnapCenter nutzt die NetApp Snapshot-Kopiertechnologie mit dem Plug-in für Oracle Database und Plug-in für UNIX, um Datenbanken zu sichern. Snapshot Kopien belegen nur minimalen Speicherplatz.

Das Plug-in für Oracle Database bietet darüber hinaus folgende Vorteile:

- Unterstützung für Backup, Restore, Klonen, Mounten, Unmounten, Und Verifizierungs-Workflows
- Automatische Erkennung von auf dem Host konfigurierten Oracle-Datenbanken
- Unterstützung von Katalogisierung und Katalogisierung mit Oracle Recovery Manager (RMAN)
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktgenauer Kopien von Produktionsdatenbanken für Test- oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Die Unterstützung der Konsistenzgruppendaten (CG) von ONTAP im Rahmen der Erstellung von Backups in SAN- und ASM-Umgebungen
- Unterbrechungsfreie und automatisierte Backup-Verifizierung
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Datenbank-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshot Kopien konsolidiert, wenn Datenbanken in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Unterstützung physischer und virtualisierter Infrastrukturen
- Unterstützung von NFS, iSCSI, Fibre Channel (FC), RDM, VMDK über NFS und VMFS sowie ASM over NFS, SAN, RDM und VMDK
- Unterstützung für die Selective LUN Map (SLM)-Funktion von ONTAP

  Standardmäßig erkennt die SLM-Funktion regelmäßig die LUNs, die keine optimierten Pfade haben, und behebt sie. Sie können SLM konfigurieren, indem Sie die Parameter in der Datei scu.properties unter /var/opt/snapcenter/scu/etc. Ändern

  - Sie können dies deaktivieren, indem Sie DEN Wert ENABLE_LUNPATH_MONITORING auf false setzen.
  - Sie können die Häufigkeit angeben, in der die LUN-Pfade automatisch korrigiert werden, indem Sie den Wert (in Stunden) LUNPATH_MONITORING_INTERVAL zuweisen. Informationen zu SLM finden Sie im "ONTAP 9 – Systemadministrationshandbuch".

Von Plug-in für Oracle Database unterstützte Storage-Typen

SnapCenter unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf

Virtual Machines. Sie müssen die Unterstützung Ihres Speichertyps überprüfen, bevor Sie das SnapCenter Plug-ins Paket für Linux oder SnapCenter Plug-ins Package für AIX installieren.

SnapCenter unterstützt Storage-Bereitstellung für Linux und AIX nicht.

Storage-Typen unterstützt auf Linux

In der folgenden Tabelle sind die unter Linux unterstützten Speichertypen aufgeführt.

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf VMFS oder NFS-Datastores • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden

Storage Types supported auf AIX

In der folgenden Tabelle sind die auf AIX unterstützten Storage-Typen aufgeführt.

Maschine	Storage-Typ
Physischer Server	• FC-connected und iSCSI-Connected LUNs. In einer SAN-Umgebung werden ASM, LVM und SAN-Dateisysteme unterstützt. NFS auf AIX und Dateisystem wird nicht unterstützt. • Erweitertes Journaled File System (JFS2) Unterstützt die Inline-Protokollierung auf SAN-Dateisystemen und LVM-Layout.

Der "NetApp Interoperabilitäts-Matrix-Tool" Enthält die neuesten Informationen zu den gewünschten Versionen.

Minimale ONTAP-Berechtigungen, die für das Plug-in für Oracle erforderlich sind

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
• Event Generate-AutoSupport-log
• Job-Verlauf wird angezeigt • Job beenden

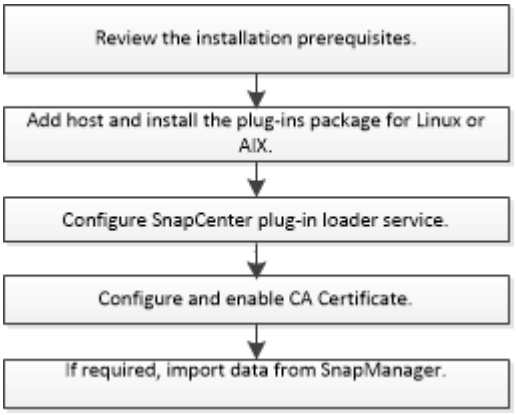
All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
• lun • lun-Attribut anzeigen • lun erstellen • lun löschen • lun-Geometrie • lun Initiatorgruppe hinzufügen • lun-Initiatorgruppe wird erstellt • lun-Initiatorgruppe löschen • lun igroup umbenennen • lun-Initiatorgruppe wird angezeigt • lun Mapping Add-Reporting-Nodes • lun-Zuordnung erstellen • lun-Zuordnung löschen • lun Mapping remove-Reporting-Nodes • lun-Zuordnung wird angezeigt • lun ändern • lun-Verschiebung in Volume • lun ist offline • lun ist online • lun Persistent-Reservierung löschen • die lun-Größe wird geändert • lun seriell • lun anzeigen
• SnapMirror Richtlinie Add-Rule • änderungsregel für snapmirror • Remove-Rule für snapmirror-Richtlinie • snapmirror-Richtlinie anzeigen • snapmirror Wiederherstellung • snapmirror zeigen • snapmirror Vorgeschichte • snapmirror Update • snapmirror Update-ls-Set • snapmirror Listenziele
• Version

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
• Erstellung von Volume-Klonen • Klon von Volume anzeigen • Split-Start des Volume-Klons • Split-Stopp für Volume-Klon • Volume erstellen • Volume destroy • Erstellen eines Volume-Dateiklonen • Show-Disk-Nutzung für Volume-Dateien • Volume ist offline • Das Volume ist online • Volume-Änderung • Erstellen von Volume-qtree • Volume qtree löschen • Änderung des Volume-qtree • Volume-qtree anzeigen • Volume-Einschränkung • Volumen anzeigen • Erstellen von Volume-Snapshots • Volume Snapshot löschen • Ändern des Volume-Snapshots • Umbenennung von Volume-Snapshots • Wiederherstellung von Volume Snapshots • Restore-Datei für Volume Snapshots • Volume-Snapshot werden angezeigt • Volume-Aufhängung nicht verfügbar
• vserver • cifs von vserver • vserver cifs shadowcopy anzeigen • vserver zeigen
• Netzwerkschnittstelle • Netzwerkschnittstelle wird angezeigt
• MetroCluster zeigen

Installieren Sie das SnapCenter Plug-in für Oracle Database

Installations-Workflow des SnapCenter Plug-ins für Oracle Database

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 von Plug-ins Package für Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-ins-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 Benutzer ohne Root 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 als effektiver Root-Benutzer ausgeführt.

- Wenn Sie das SnapCenter Plug-ins Paket für AIX auf 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, nicht aber die symbolischen Links auf Verzeichnisebene, um den ABSOLUTEN Pfad JAVA_HOME zu erhalten.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus als Linux oder AIX für den Installationsbenutzer.
- Sie müssen Java 1.8.x, 64-bit, auf Ihrem Linux oder AIX Host installiert haben.

  Informationen zum Herunterladen VON JAVA finden Sie unter:

  - "Java-Downloads für alle Betriebssysteme"
  - "IBM Java für AIX"

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

Sie können das Plug-in für Oracle Database auch zur Verwaltung von Oracle Datenbanken für SAP verwenden. Die Integration von SAP BR*Tools wird jedoch nicht unterstützt.

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

Linux Host-Anforderungen

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

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux Wenn Sie die Oracle-Datenbank auf LVM unter 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)
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	Java 1.8.x (64-Bit)Oracle Java und OpenJDK Varianten Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter 2.0 und höheren Versionen kann ein nicht-Root-Benutzer das SnapCenter Plug-ins-Paket für Linux installieren und das Plug-in-Verfahren starten. Sie sollten sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

Was Sie brauchen

- Sudo 1.8.7 oder höher.
- Stellen Sie sicher, dass der nicht-Root-Benutzer Teil der Oracle-Installationsgruppe ist.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*SUDO_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin

- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux hinzu.

```
Cmnd_Alias SCCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/Linux_Prechecks.sh
SUDO_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: SUDO_USER env_keep=JAVA_HOME
Defaults: SUDO_USER !visiblepw
Defaults: SUDO_USER !requiretty
```

SUDO_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können den Prüfsummenwert aus der Datei **oracle_cham.txt** abrufen, die sich unter *C:\ProgramData\NetApp\SnapCenter\Package Repository* befindet.

Wenn Sie einen benutzerdefinierten Speicherort angegeben haben, befindet sich der Speicherort *Custom_Path\NetApp\SnapCenter\Package Repository*.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Best Practice: aus Sicherheitsgründen sollten Sie den sudo-Eintrag nach Abschluss jeder Installation oder Aktualisierung entfernen.

AIX Host-Anforderungen

Bevor Sie das SnapCenter Plug-ins Package für AIX installieren, sollten Sie sicherstellen, dass der Host die Anforderungen erfüllt.

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

Element	Anforderungen
Betriebssysteme	AIX 6.1 oder höher
MindestRAM für das SnapCenter Plug-in auf dem Host	4 GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	1 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 1.8.x (64-Bit)IBM Java Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Konfigurieren Sie sudo-Berechtigungen für Benutzer, die nicht root sind, für 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. Sie sollten sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

Was Sie brauchen

- Sudo 1.8.7 oder höher.
- Stellen Sie sicher, dass der nicht-Root-Benutzer Teil der Oracle-Installationsgruppe ist.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_Host_Plugin.bsx
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux hinzu.

```
Cmnd_Alias SCCMD = 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
AIX_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

AIX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können den Prüfsummenwert aus der Datei **oracle_cham.txt** abrufen, die sich unter *C:\ProgramData\NetApp\SnapCenter\Package Repository* befindet.

Wenn Sie einen benutzerdefinierten Speicherort angegeben haben, befindet sich der Speicherort *Custom_Path\NetApp\SnapCenter\Package Repository*.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Best Practice: aus Sicherheitsgründen sollten Sie den sudo-Eintrag nach Abschluss jeder Installation oder Aktualisierung entfernen.

Anmeldedaten einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten 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 Benutzer ohne Root-Benutzer erstellt, der über sudo-Berechtigungen zum Installieren und Starten des Plug-in-Prozesses verfügt.

Weitere Informationen finden Sie unter: Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts Oder die nicht root sind, für AIX-Host

Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten erstellen dürfen, empfiehlt es sich, erst nach dem Hinzufügen von SVMs Anmeldeinformationen zu erstellen, bevor Sie Hosts implementieren und Plug-ins installieren.

Schritte

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

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domain-Administrator Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username*
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten. Wählen Sie je nach Betriebssystem des Plug-in-Hosts entweder Linux oder AIX aus.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite **Benutzer und Zugriff** die Pflege von Anmeldeinformationen zuweisen.

Konfigurieren von Anmeldeinformationen für eine Oracle-Datenbank

Sie müssen Anmeldedaten konfigurieren, die für Datensicherungsvorgänge 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 Anmeldedaten".

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername keine vollständigen Administratorrechte hat, muss der Benutzername mindestens über Ressourcengruppen- und Sicherungsrechte verfügen.

Wenn Sie die Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ansicht Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Sie müssen Datenbankanmeldeinformationen konfigurieren, um die Datenbank schützen oder zur Ressourcengruppe hinzufügen zu können, um Datensicherungsvorgänge durchzuführen.

Wenn Sie beim Erstellen einer Anmeldedaten falsche Details angeben, wird eine Fehlermeldung angezeigt. Klicken Sie auf **Abbrechen** und versuchen Sie es dann erneut.

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 Sie Auf Und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern.

   Sie können dann auf klicken 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 in der Dropdown-Liste **vorhandene Anmeldedaten verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datensicherungsjobs in der Oracle-Datenbank verwendet werden sollen.

   Der Oracle-Benutzer sollte über sysdba-Berechtigungen verfügen.

   Sie können auch Anmeldedaten erstellen, indem Sie auf klicken .
6. Wählen Sie im Abschnitt ASM-Einstellungen konfigurieren in der Dropdown-Liste **vorhandene Anmeldedaten verwenden** die Anmeldeinformationen aus, die für die Ausführung von Datensicherungsjobs auf der ASM-Instanz verwendet werden sollen.

   Der ASM-Benutzer sollte über syssm-Berechtigung verfügen.

   Sie können auch Anmeldedaten erstellen, indem Sie auf klicken .
7. Wählen Sie im Abschnitt Configure RMAN Catalog Settings aus der Dropdown-Liste **Use Existing Credentials** die Anmeldeinformationen aus, die für die Ausführung von Datenschutzaufträgen in der Oracle Recovery Manager (RMAN)-Katalogdatenbank verwendet werden sollen.

   Sie können auch Anmeldedaten erstellen, indem Sie auf klicken .

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

8. Geben Sie im Feld **bevorzugte RAC-Knoten** die RAC-Knoten (Real Application Cluster) an, die für das Backup bevorzugt sind.

   Die bevorzugten Knoten sind möglicherweise ein oder alle Cluster-Knoten, wo die RAC-Datenbankinstanzen vorhanden sind. Der Backup-Vorgang wird nur auf den bevorzugten Knoten in der bevorzugten Reihenfolge ausgelöst.

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

   Nach dem Failover oder der Verschiebung der RAC One Node-Datenbank wird durch die Aktualisierung von Ressourcen auf der Seite SnapCenter-Ressourcen der Host aus der Liste **bevorzugte RAC-Knoten** entfernt, in der die Datenbank zuvor gehostet wurde. Der RAC-Knoten, in dem die Datenbank verschoben wird, wird in **RAC-Knoten** aufgelistet 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 mithilfe der GUI das Plug-ins Package für Linux oder AIX

Auf der Seite „Host hinzufügen“ können Sie Hosts hinzufügen, und dann das SnapCenter Plug-ins Paket für Linux oder SnapCenter Plug-ins Package 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 für einen einzelnen Host oder für ein Cluster installieren. Wenn Sie das Plug-in auf einem Cluster installieren (Oracle RAC), 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.

Sie sollten einer Rolle zugewiesen werden, die über die Berechtigungen zum Installieren und Deinstallieren des Plug-ins verfügt, z. B. über die Rolle „SnapCenter Admin“.

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. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie als Hosttyp * Linux* oder **AIX** aus. 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.
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Jeder Node 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 Unterdomäne ist, müssen Sie den FQDN angeben.

Für dieses Feld…	Tun Sie das…
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer 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 */opt/NetApp/snapcenter*. Optional können Sie den Pfad anpassen.

Für dieses Feld…	Tun Sie das…
Fügen Sie alle Hosts im Oracle RAC hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem Oracle RAC hinzuzufügen. In einem Flex ASM-Setup werden alle Knoten, unabhängig davon, ob es sich um einen Hub- oder Leaf-Knoten handelt, hinzugefügt.
Überspringen Sie die Prüfungen vor der Installation	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 **Absenden**.

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

   Das Precheck-Skript überprüft den Firewall-Status des Plug-in-Ports nicht, wenn er in den Regeln für die Ablehnung der Firewall angegeben ist.

   Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt. Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter *C:\Program Files\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.

8. Überprüfen Sie den Fingerabdruck, und klicken Sie dann auf **Bestätigen und Senden**.

   In einer Cluster-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

   SnapCenter unterstützt keinen ECDSA-Algorithmus.

   Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Log-Dateien befinden sich unter */Custom_Location/snapcenter/logs*.

Nach Ihrer Beendigung

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

Installieren Sie sie mithilfe von Cmdlets auf mehreren Remote Hosts

Sie sollten das Cmdlet *Install-SmHostPackage* PowerShell 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 bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet sein.

Schritte

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

   Sie können die Option *-skipprecheck* 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 Precheck-Skript überprüft den Firewall-Status des Plug-in-Ports nicht, wenn er in den Regeln für die Ablehnung der Firewall angegeben ist.

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

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Installieren Sie das Plug-ins-Paket für Linux interaktiv

Sie können das SnapCenter-Plug-ins-Paket für Linux interaktiv auf einem Linux-Host installieren.

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-ins-Pakets überprüfen.
- Sie sollten die UMGEBUNGSVARIABLE DISPLAY so einstellen, dass die IP-Adresse und die Portnummer des Linux-Hosts angegeben werden, auf dem Sie den Assistenten starten möchten.

Schritte

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

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

2. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-in installieren möchten.
3. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben, und führen Sie Folgendes aus: `./SnapCenter_linux_host_plugin.bin –i swing`
4. Befolgen Sie die Anweisungen auf dem Bildschirm im Assistenten, um das Plug-ins-Paket zu installieren.

5. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

Installation auf Cluster-Host

Sie sollten SnapCenter Plug-ins Package für Linux oder SnapCenter Plug-ins Package für AIX auf beiden Knoten des Cluster-Hosts installieren.

Jeder der Nodes des Cluster-Hosts verfügt über 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 Package für Linux oder das SnapCenter Plug-ins Package für AIX auf beiden Knoten des Cluster-Hosts.
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 nicht in spl.properties angegeben ist, können Sie es hinzufügen und den Wert SCO,SCU zuordnen.

3. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, und geben Sie dann Ihre Anmeldeinformationen ein.
4. Legen Sie in jedem Knoten die bevorzugten IPs des Knotens mithilfe des Befehls *set-PreferredHostIPsInStorageExportPolicy* scli und der erforderlichen Parameter fest.
5. Fügen Sie im SnapCenter-Serverhost einen Eintrag für die Cluster-IP und den entsprechenden DNS-Namen in *C:\Windows\System32\drivers\etc\Hosts* hinzu.
6. Fügen Sie den Knoten mithilfe des 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 ein Backup der Datenbank. Wenn ein Failover auftritt, können Sie das auf Node 1 erstellte Backup verwenden, um die Datenbank auf Node 2 wiederherzustellen. Sie können auch das auf Node 1 erstellte Backup verwenden, um einen Klon auf Node 2 zu erstellen.

Es gibt veraltete Volumes, Verzeichnisse und Sperrdateien, wenn das Failover während der Ausführung anderer SnapCenter Vorgänge durchgeführt wird.

Installieren Sie das Plug-ins-Paket für Linux im Silent-Modus oder im Konsolenmodus

Sie können das SnapCenter-Plug-ins-Paket für Linux entweder im Konsolenmodus oder im Silent-Modus installieren, indem Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-ins-Pakets überprüfen.
- Sie sollten sicherstellen, dass die UMGEBUNGSVARIABLE DISPLAY nicht eingestellt ist.

  Wenn die UMGEBUNGSVARIABLE DISPLAY eingestellt ist, sollten Sie die Anzeige Unset ausführen und anschließend versuchen, das Plug-in manuell zu installieren.

Über diese Aufgabe

Bei der Installation im Konsolenmodus müssen Sie die erforderlichen Installationsinformationen bereitstellen, während Sie bei der Installation im Silent Mode keine Installationsinformationen angeben müssen.

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 von dem Host zugegriffen werden, auf dem der SnapCenter-Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben.
3. Führen Sie je nach gewünschter Installationsart einen der folgenden Schritte aus.

Installationsmodus	Schritte
Konsolenmodus	a. Ausführen: `./SnapCenter_linux_host_plugin.bin -i console` b. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation abzuschließen.
Silent-Modus	Ausführen: `./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 SnapCenter Plug-in Loader Service neu.

> Die Installation des Plug-ins-Pakets registriert die Plug-ins auf dem Host und nicht auf dem SnapCenter-Server. Sie sollten die Plug-ins auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Wählen Sie beim Hinzufügen des Hosts als Anmeldeinformationen „Keine“ aus. Nach dem Hinzufügen des Hosts werden die installierten Plug-ins automatisch erkannt.

Installieren Sie Plug-ins Package für AIX im Silent-Modus

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

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-ins-Pakets überprüfen.

- Sie sollten sicherstellen, dass die UMGEBUNGSVARIABLE DISPLAY nicht eingestellt ist.

  Wenn die UMGEBUNGSVARIABLE DISPLAY eingestellt ist, sollten Sie die Anzeige Unset ausführen und anschließend 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 von dem Host zugegriffen werden, auf dem der SnapCenter-Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 SnapCenter Plug-in Loader Service neu.

> Die Installation des Plug-ins-Pakets registriert die Plug-ins auf dem Host und nicht auf dem SnapCenter-Server. Sie sollten die Plug-ins auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Wählen Sie beim Hinzufügen des Hosts als Anmeldeinformationen „Keine“ aus. Nach dem Hinzufügen des Hosts werden die installierten Plug-ins automatisch erkannt.

Überwachung des Installationsstatus

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Gehen Sie auf der Seite **Jobs** folgendermaßen vor, um die Liste so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden:
   a. Klicken Sie Auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst

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 SnapCenter Plug-ins-Paket für AIX installieren.

Über diese Aufgabe

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

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

Die Datei spl.properties befindet sich unter */Custom_Location/NetApp/snapcenter/spl/etc/* und enthält die folgenden Parameter: Diesen Parametern werden Standardwerte zugewiesen.

Parametername	Beschreibung
PROTOKOLL_LEVEL	Zeigt die unterstützten Protokollebenen an. Die möglichen Werte sind INFO, DEBUG, TRACE, ERROR, FATAL, Und WARNEN.
SPL_PROTOKOLL	Zeigt das von SnapCenter Plug-in Loader unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.

Parametername	Beschreibung
SNAPCENTER_SERVER_PROTOCOL	Zeigt das von SnapCenter-Server unterstützte Protokoll an. Nur das HTTPS-Protokoll wird 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 auf „TRUE“ setzen, wenn Sie das Standardverhalten deaktivieren und den java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Kennwort der Schlüsselspeicherdatei an. Sie können diesen Wert nur ändern, wenn Sie das Passwort ändern oder eine neue Schlüsselspeicherdatei erstellen.
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Plug-in-Loader ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt. Nach der Installation der Plug-ins sollten Sie den Wert nicht ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter-Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Schlüsselspeicherdatei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.

Parametername	Beschreibung
„LOGS_MAX_COUNT“	Zeigt die Anzahl der SnapCenter-Plug-in-Loader-Protokolldateien an, die im Ordner */Custom_location/snapcenter/spl/logs* aufbewahrt werden. Der Standardwert ist 5000. Wenn der Zähler größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Prüfung auf die 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 zu behaltenden 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 im Rahmen des Startens von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Log-Datei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei gezippt und die Protokolle werden in die neue Datei dieses Jobs geschrieben.
BEIBEHALTEN_LOGS_OF_LAST_DAYS	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
ENABLE_CERTIFICATE_VALIDATION	Zeigt true an, wenn die Zertifikatvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder aktivieren oder deaktivieren, indem Sie den spl.properties bearbeiten oder den SnapCenter GUI oder Cmdlet verwenden.

Wenn einer dieser Parameter dem Standardwert nicht 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 die Datei bearbeiten, um Probleme zu beheben, die mit den Werten, die den Parametern zugeordnet sind, zusammenhängen. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter-Plug-in-Loader-Dienst neu starten.

Schritte

1. Führen Sie bei Bedarf eine der folgenden Aktionen aus:
   - Starten Sie den SnapCenter Plug-in Loader-Dienst als Root-Benutzer:

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl start`
** Stoppen Sie den SnapCenter-Plug-in-Loader-Dienst:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```

> Sie können die Option -Force mit dem Befehl STOP verwenden, um den SnapCenter Plug-in Loader Dienst nachdrücklich zu stoppen. Vor diesem Verfahren sollten Sie jedoch Vorsicht walten lassen, da auch die bestehenden Vorgänge beendet werden.

   - Starten Sie den SnapCenter-Plug-in-Loader-Dienst neu:

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
** Suchen Sie den Status des SnapCenter-Plug-in-Loader-Dienstes:
```

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl status`
** Finden Sie die Änderung im SnapCenter-Plug-in-Loader-Dienst:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

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

Sie sollten das Passwort von SPL Keystore und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für SPL Trust-Store konfigurieren und das CA-signierte Schlüsselpaar für SPL Trust-Store mit dem SnapCenter Plug-in Loader Service konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

> SPL verwendet die Datei 'keystore.jks', die sich bei ‘/var/opt/snapcenter/spl/etc’ sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für SPL-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen.

   Dieser Wert entspricht dem Schlüssel 'SPL_KEYSTORE_PASS'.

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

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

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

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

Passwort für SPL-Schlüsselspeicher und für alle zugeordneten Alias-Passwort des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel in den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher: */var/opt/snapcenter/spl/etc*.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

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

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder
Zwischenzertifikate in den SPL Trust-Store konfiguriert haben.
```

Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar für SPL Trust-Store

Sie sollten das CA-signierte Schlüsselpaar für den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Schlüsselspeicher /var/opt/snapcenter/spl/etc. Enthält
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen
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
. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält,
der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher
hinzugefügt wurde.
. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für
das CA-Zertifikat in das Schlüsselspeicher-Passwort.
```

Das Standard-SPL-Schlüsselspeicherkennwort ist der Wert des Schlüssels SPL_KEYSTORE_PASS in der Datei spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Wenn der Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen enthält („*","), ändern Sie den Alias-Namen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Konfigurieren Sie den Alias-Namen aus dem Schlüsselspeicher, der sich
in der Datei spl.properties befindet.
```

Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.

4. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

- SPL wird nach den CRL-Dateien in einem vorkonfigurierten Verzeichnis suchen.
- Das Standardverzeichnis für die CRL-Dateien für SPL lautet */var/opt/snapcenter/spl/etc/crl*.

Schritte

1. Sie können das Standardverzeichnis in der Datei spl.properties mit dem Schlüssel SPL_CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Was Sie brauchen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nach Ihrer Beendigung

Auf dem Reiter Managed Hosts wird ein Schloss 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 lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Import der Daten von SnapManager für Oracle und SnapManager für SAP zu 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 Importwerkzeug über die Befehlszeilenschnittstelle (Linux Host CLI) ausführen.

Das Importprogramm erstellt Richtlinien und Ressourcengruppen in SnapCenter. Die in SnapCenter erstellten Richtlinien und Ressourcengruppen entsprechen den Profilen und Vorgängen, die mithilfe dieser Profile in SnapManager für Oracle und SnapManager für SAP durchgeführt wurden. Das Importtool von SnapCenter arbeitet mit den Datenbanken SnapManager für Oracle und SnapManager für SAP sowie mit der zu importierenden Datenbank zusammen.

- Ruft alle Profile, Zeitpläne und Vorgänge ab, die mithilfe der Profile durchgeführt werden.
- Erstellt für jeden eindeutigen Vorgang und jeden mit einem Profil verbundenen Zeitplan eine SnapCenter-Backup-Richtlinie.
- Erstellt für jede Zieldatenbank eine Ressourcengruppe.

Sie können das Import-Tool ausführen, indem Sie das sc-Migrationsskript unter */opt/NetApp/snapcenter/spl/bin* ausführen. Wenn Sie das SnapCenter Plug-ins-Paket für Linux auf dem Datenbank-Host installieren, den Sie importieren möchten, wird das sc-Migration-Skript in */opt/NetApp/snapcenter/spl/bin* kopiert.

> Der Datenimport wird von der grafischen SnapCenter-Benutzeroberfläche (GUI) nicht unterstützt.

SnapCenter unterstützt Data ONTAP in 7-Mode nicht. Mit dem 7-Mode Transition Tool können Sie Daten und Konfigurationen, die auf einem System mit Data ONTAP 7-Mode gespeichert sind, auf einem ONTAP System migrieren.

Konfigurationen für den Datenimport unterstützt

Bevor Sie Daten von SnapManager 3.4.x für Oracle und SnapManager 3.4.x für SAP zu SnapCenter importieren, sollten Sie die Konfigurationen kennen, die vom SnapCenter Plug-in für Oracle Database unterstützt werden.

Die mit dem SnapCenter Plug-in für Oracle Database unterstützten Konfigurationen sind im aufgeführt "NetApp Interoperabilitäts-Matrix-Tool".

Was wird nach SnapCenter importiert

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

Von SnapManager für Oracle und SnapManager für SAP	Für SnapCenter
Profile ohne Vorgänge und Zeitpläne	Eine Richtlinie wird mit dem Standardsicherungstyp „Online“ und dem Backup-Umfang als „voll“ erstellt.
Profile mit einem oder mehreren Operationen	Mehrere Richtlinien werden auf der Grundlage einer einzigartigen Kombination eines Profils und der Operationen erstellt, die mit diesem Profil durchgeführt werden. Die in SnapCenter erstellten Richtlinien enthalten die Details zum Archivprotokoll und zur Aufbewahrung, die vom Profil und den entsprechenden Vorgängen abgerufen werden.
Profile mit der Konfiguration von Oracle Recovery Manager (RMAN	Richtlinien werden mit der Option **Katalog Backup mit Oracle Recovery Manager** erstellt. Wenn die externe RMAN Katalogisierung in SnapManager verwendet wurde, müssen Sie die RMAN-Katalogeinstellungen in SnapCenter konfigurieren. Sie können entweder die vorhandenen Anmeldedaten auswählen oder neue Anmeldedaten erstellen. Wenn RMAN über die Steuerdatei in SnapManager konfiguriert wurde, müssen Sie RMAN nicht in SnapCenter konfigurieren.
Mit einem Profil angehängte Planung	Eine Richtlinie wird nur für den Zeitplan erstellt.
Datenbank	Für jede importierte Datenbank wird eine Ressourcengruppe erstellt. In einem RAC-Setup (Real Application Clusters) wird der Knoten, auf dem Sie das Importwerkzeug ausführen, nach dem Import der bevorzugte Knoten und die Ressourcengruppe für diesen Knoten erstellt.

Wenn ein Profil importiert wird, wird zusammen mit der Backup-Richtlinie eine Verifizierungsrichtlinie erstellt.

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

Parameter und Werte von SnapManager für Oracle und SnapManager für SAP	SnapCenter-Parameter und -Werte	Hinweise
Umfang Des Backups • Voll • Daten • Protokoll	Umfang Des Backups • Voll • Daten • Protokoll	
Backup-Modus • Automatisch • Online • Offline	Backup-Typ • Online • Offline Herunterfahren	Wenn der Backup-Modus automatisch ist, überprüft das Importwerkzeug den Datenbankstatus bei Durchführung des Vorgangs und setzt den Backup-Typ entsprechend entweder als Online- oder Offline-Herunterfahren.
Aufbewahrung • Tage • Zählt	Aufbewahrung • Tage • Zählt	SnapManager für Oracle und SnapManager für SAP benötigt zur Festlegung der Datenhaltung sowohl Tage als auch Zählung. In SnapCenter gibt es entweder Days *ODER* Counts. Die Aufbewahrung wird also in Bezug auf Tage festgelegt, an denen in SnapManager für Oracle und SnapManager für SAP die Präferenz für Tage erhalten wird.
Beschneidung für Schichtpläne • Alle • Systemänderungsnummer (SCN) • Datum • Protokolle, die vor den angegebenen Stunden, Tagen, Wochen und Monaten erstellt wurden	Beschneidung für Schichtpläne • Alle • Protokolle, die vor den angegebenen Stunden und Tagen erstellt wurden	SnapCenter unterstützt keine Hochgau auf Basis von SCN, Datum, Wochen und Monaten.

Parameter und Werte von SnapManager für Oracle und SnapManager für SAP	SnapCenter-Parameter und -Werte	Hinweise
Benachrichtigung • E-Mails werden nur für erfolgreiche Vorgänge gesendet • E-Mails werden nur für fehlgeschlagene Vorgänge gesendet • Sowohl für erfolgreiche als auch für fehlgeschlagene Vorgänge gesendete E-Mails	Benachrichtigung • Immer • Bei Ausfall • Warnung • Fehler	Die E-Mail-Benachrichtigungen werden importiert. Sie müssen den SMTP-Server jedoch manuell über die SnapCenter-Benutzeroberfläche aktualisieren. Der Betreff der E-Mail bleibt leer, damit Sie sie konfigurieren können.

Was wird nicht in SnapCenter importiert

Das Importwerkzeug importiert nicht alles nach SnapCenter.

Folgendes kann nicht in SnapCenter importiert werden:

- Backup von Metadaten
- Teilweise Backups
- RDM (Raw Device Mapping) und Virtual Storage Console (VSC)-bezogene Backups
- Rollen oder Zugangsdaten, die im Repository von SnapManager für Oracle und SnapManager für SAP verfügbar sind
- Daten zu Verifizierungs-, Restore- und Klonvorgängen
- Beschnitt für den Betrieb
- Replikationsdetails, die im Profil SnapManager für Oracle und SnapManager für SAP angegeben sind

  Nach dem Import müssen Sie die entsprechende Richtlinie, die in SnapCenter erstellt wurde, manuell bearbeiten, um die Replikationsdetails einzuschließen.

- Katalogisierte Backup-Informationen

Vorbereitung für den Import von Daten

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

Schritte

1. Geben Sie die Datenbank an, die Sie importieren möchten.
2. Fügen Sie mithilfe von SnapCenter den Datenbank-Host hinzu und installieren Sie das SnapCenter Plug-ins Paket für Linux.
3. Richten Sie mithilfe von SnapCenter die Verbindungen zu den Storage Virtual Machines (SVMs) ein, die von den Datenbanken auf dem Host verwendet werden.

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 Importwerkzeug ausführen möchten, muss die Datenbank zugänglich sein, sonst schlägt die Erstellung der Ressourcengruppe fehl.

   Wenn die Datenbank Anmeldeinformationen konfiguriert ist, müssen Sie in SnapCenter eine entsprechende Berechtigung erstellen, die Anmeldeinformationen der Datenbank zuweisen und dann die Ermittlung der Datenbank erneut ausführen. Wenn sich die Datenbank auf Automatic Storage Management (ASM) befindet, müssen Sie Anmeldedaten für die ASM-Instanz erstellen und die Anmeldeinformationen der Datenbank zuweisen.
6. Stellen Sie sicher, dass der Benutzer, der das Importwerkzeug ausführt, über ausreichende Berechtigungen verfügt, um SnapManager für Oracle oder SnapManager für SAP CLI-Befehle (z. B. den Befehl zum Unterbrechen von Zeitplänen) von SnapManager für Oracle oder SnapManager für SAP-Host auszuführen.
7. Führen Sie die folgenden Befehle auf dem SnapManager für Oracle oder SnapManager für SAP Host aus, um die Zeitpläne zu unterbrechen:
   a. Wenn Sie die Zeitpläne auf dem SnapManager für Oracle Host unterbrechen möchten, führen Sie folgende Schritte 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 folgende Schritte 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 für jedes Profil auf dem Host den Befehl smsap Credential Set ausführen.
8. Stellen Sie sicher, dass der vollständig qualifizierte Domänenname (FQDN) des Datenbankhosts angezeigt wird, wenn Sie den Hostnamen -f ausführen.

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

Daten importieren

Sie können Daten importieren, indem Sie das Importwerkzeug vom Datenbank-Host ausführen.

Über diese Aufgabe

Die nach dem Importieren erstellten SnapCenter Backup-Richtlinien haben unterschiedliche Benennungsformate:

- Richtlinien, die für die Profile ohne Operationen und Zeitpläne erstellt wurden, haben das SM_PROFILNAME_ONLINE_FULL_DEFAULT_MIGRIERTE Format.

  Wenn mit einem Profil kein Vorgang durchgeführt wird, wird die entsprechende Richtlinie mit dem Standard-Backup-Typ als online und im Backup-Umfang vollständig erstellt.

- Richtlinien, die für die Profile mit einem oder mehreren Operationen erstellt wurden, haben das SM_PROFILNAME_BACKUPMODE_BACKUPSCOPE_MIGRIERTE Format.
- Richtlinien, die für die an die Profile angeschlossenen Zeitpläne erstellt wurden, weisen das SM_PROFILNAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRIERTE Format auf.

Schritte

1. Melden Sie sich beim Datenbank-Host an, den Sie importieren möchten.
2. Führen Sie das Import-Tool aus, indem Sie das sc-Migrationsskript unter */opt/NetApp/snapcenter/spl/bin* ausführen.
3. Geben Sie den Benutzernamen und das Kennwort des SnapCenter-Servers ein.

   Nach dem Validieren der Zugangsdaten wird eine Verbindung mit SnapCenter hergestellt.

4. Geben Sie die Datenbankdetails zu SnapManager für Oracle oder SnapManager für SAP ein.

   In der Repository-Datenbank werden die auf dem Host verfügbaren Datenbanken aufgelistet.

5. Geben Sie die Details der Zieldatenbank ein.

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

6. Wenn Sie ein Systemprotokoll generieren oder ASUP-Nachrichten für fehlgeschlagene Vorgänge senden möchten, müssen Sie diese entweder aktivieren, indem Sie den Befehl *Add-SmStorageConnection* oder *set-SmStorageConnection* ausführen.

> Wenn Sie einen Importvorgang abbrechen möchten, entweder während des Imports oder nach dem Import, müssen Sie die SnapCenter-Richtlinien, Anmeldedaten und Ressourcengruppen, die im Rahmen des Importvorgangs erstellt wurden, manuell löschen.

Ergebnisse

Die SnapCenter Backup-Richtlinien werden für Profile, Zeitpläne und Vorgänge erstellt, die mithilfe der Profile durchgeführt werden. Ressourcengruppen werden auch für jede Zieldatenbank erstellt.

Nach dem erfolgreichen Import der Daten werden die mit der importierten Datenbank verknüpften Zeitpläne in

SnapManager für Oracle und SnapManager für SAP ausgesetzt.

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

Die Protokolle für jede Ausführung des Importwerkzeugs werden im Verzeichnis */var/opt/snapcenter/spl/logs* mit dem Namen spl_Migration_timestamp.log gespeichert. In diesem Protokoll können Sie Importfehler überprüfen und beheben.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

Wenn Ihre Datenbanken auf Virtual Machines (VMs) gespeichert sind oder VMs und Datastores geschützt werden sollen, müssen Sie das SnapCenter Plug-in für die virtuelle Appliance VMware vSphere implementieren.

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

Informationen zur Konfiguration des CA-Zertifikats mit dem SnapCenter-Plug-in für VMware vSphere finden Sie unter "Erstellen oder importieren Sie ein SSL-Zertifikat".

Konfigurieren Sie die CRL-Datei

Das SnapCenter Plug-in für VMware vSphere sucht die CRL-Dateien in einem vorkonfigurierten Verzeichnis. Das Standardverzeichnis der CRL-Dateien für das SnapCenter Plug-in für VMware vSphere ist */opt/netapp/config/crl*.

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Bereiten Sie sich auf den Schutz von Oracle Datenbanken vor

Bevor Sie Datensicherungsvorgänge wie Backup-, Klon- oder Restore-Vorgänge durchführen, müssen Sie Ihre Strategie definieren und die Umgebung festlegen. Sie können den SnapCenter Server auch zur Verwendung von SnapMirror und SnapVault Technologie einrichten.

Um von der SnapVault und SnapMirror Technologie zu profitieren, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes auf dem Storage-Gerät konfigurieren und initialisieren. Sie können entweder NetApp System Manager verwenden oder die Storage-Konsole verwenden, um diese Aufgaben auszuführen.

Bevor Sie das Plug-in für Oracle Database verwenden, muss der SnapCenter-Administrator den SnapCenter-Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installation und Konfiguration von SnapCenter Server "Weitere Informationen ."
- Konfigurieren Sie die SnapCenter Umgebung durch Hinzufügen von Storage-Systemverbindungen. "Weitere Informationen ."

SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede für SnapCenter registrierte SVM, die eine SVM-Registrierung oder eine Cluster-Registrierung verwendet, muss eindeutig sein.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus als Linux oder AIX für den Installationsbenutzer. "Weitere Informationen ."
- Fügen Sie Hosts hinzu, installieren Sie die Plug-ins und ermitteln Sie die Ressourcen.
- Wenn Sie SnapCenter Server zum Schutz von Oracle Datenbanken nutzen, die sich auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.
- Installieren Sie Java auf Ihrem Linux oder AIX Host.

  Siehe "Anforderungen an Linux-Hosts" Oder "AIX-Host-Anforderungen" Finden Sie weitere Informationen.
- Sie sollten den Zeitwert der Anwendungs-Firewall auf 3 Stunden oder mehr einstellen.
- Wenn Sie Oracle Datenbanken in NFS-Umgebungen haben, müssen Sie mindestens eine NFS Daten-LIF für primären oder sekundären Storage konfiguriert haben, um Mount-, Klon-, Verifizierungs- und Restore-Vorgänge durchzuführen.
- Wenn Sie mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration haben, können Sie Folgendes mithilfe der SnapCenter-CLI auf dem Datenbank-Host durchführen:
  - Standardmäßig werden alle IP-Adressen des Datenbank-Hosts der Richtlinie für den NFS-Storage-Export in der Storage Virtual Machine (SVM) für die geklonten Volumes hinzugefügt. Wenn Sie eine bestimmte IP-Adresse haben oder auf eine Teilmenge der IP-Adressen beschränken möchten, führen Sie die CLI Set-PreferredHostIPsInStorageExportPolicy aus.
  - Wenn in einer SVM mehrere Datenpfade (LIFs) vorhanden sind, wählt SnapCenter den entsprechenden Datenpfad (LIF) zur Mounten des geklonten NFS-Volumes. Wenn Sie jedoch einen bestimmten Datenpfad (LIF) angeben möchten, müssen Sie die CLI Set-SvmPreferredDataPath ausführen. Das Command Reference Guide enthält weitere Informationen.
- Wenn Sie Oracle-Datenbanken in SAN-Umgebungen nutzen, stellen Sie sicher, dass die SAN-Umgebung gemäß der in den folgenden Leitfäden genannten Empfehlung konfiguriert ist:
  - "Empfohlene Host-Einstellungen für Linux Unified Host Utilities"
  - "Verwendung von Linux Hosts mit ONTAP Storage"
  - "Host-Einstellungen, die von AIX Host Utilities betroffen sind"
- Wenn Sie Oracle-Datenbanken auf LVM in Oracle Linux- oder RHEL-Betriebssystemen haben, installieren Sie die neueste Version von Logical Volume Management (LVM).
- Wenn Sie SnapManager für Oracle verwenden und zu SnapCenter Plug-in für Oracle Database migrieren möchten, können Sie die Profile mithilfe des scli-Befehls sc-migrate zu Richtlinien und Ressourcengruppen von SnapCenter migrieren.
- Konfigurieren Sie SnapMirror und SnapVault auf ONTAP, falls Sie eine Backup-Replizierung möchten

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für SnapCenter 4.3.x-Anwender enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Filesysteme mithilfe des Linux-basierten SnapCenter Plug-ins für VMware vSphere Virtual Appliance (Open Virtual Appliance Format).

Weitere Informationen

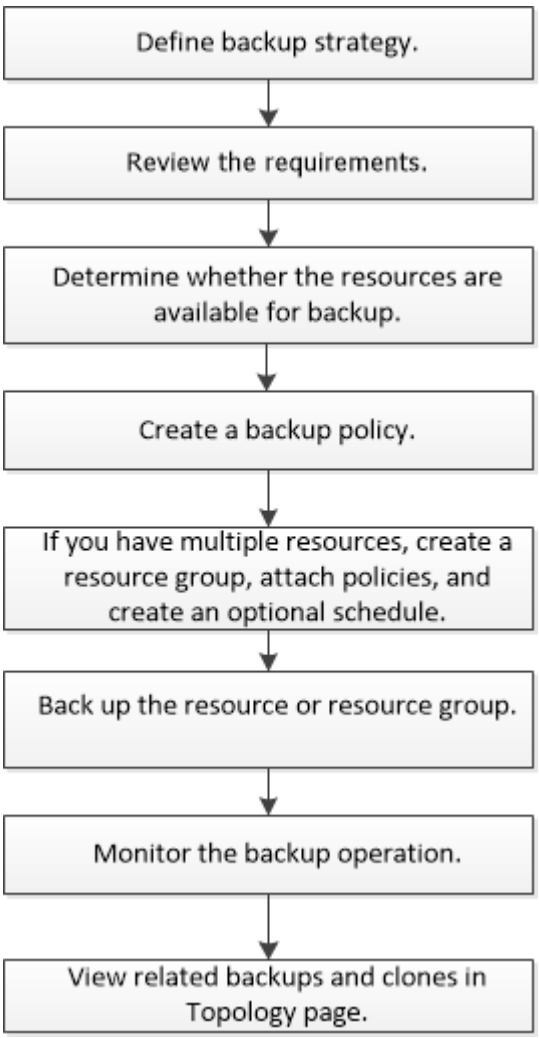
- "Interoperabilitäts-Matrix-Tool"
- "Dokumentation zum SnapCenter Plug-in für VMware vSphere"
- "Die Datensicherung schlägt in einer Umgebung ohne Multipath in RHEL 7 und höher fehl"

Backup von Oracle Datenbanken

Backup-Workflow

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, die Ermittlung der Backup-Ressourcen, die Erstellung von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Während der Erstellung eines Backups für Oracle-Datenbanken wird auf dem Oracle-Datenbank-Host im Verzeichnis _ € ORACLE_HOME/dbs_ eine operative Sperrdatei (.sm_Lock_dbsid) erstellt, um zu vermeiden, dass mehrere Operationen auf der Datenbank ausgeführt werden. Nach dem Sichern der Datenbank wird die

operative Sperrdatei automatisch entfernt.

Wenn jedoch das vorherige Backup mit einer Warnung abgeschlossen wurde, wird die betriebliche Sperrdatei möglicherweise nicht gelöscht und der nächste Backup-Vorgang in die Warteschleife gelangt. Es kann schließlich abgebrochen werden, wenn die **.SM_Lock_dbsid**-Datei nicht gelöscht wird. In diesem Szenario müssen Sie die operative Sperrdatei manuell löschen, indem Sie die folgenden Schritte durchführen:

1. Navigieren Sie in der Eingabeaufforderung zu €Oracle_HOME/dbs.
2. Löschen Sie die Betriebssperre:`rm -rf .sm_lock_dbsid.`

Backup-Strategie für Oracle Datenbanken definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, stellen Sie sicher, dass Sie über die Backups verfügen, die Sie benötigen, um Ihre Datenbanken erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Unterstützte Oracle Database Konfigurationen für Backups

SnapCenter unterstützt das Backup verschiedener Oracle Database Konfigurationen.

- Oracle Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container-Datenbank (CDB)
- Oracle Data Guard Standby

  Sie können nur Offline-Mount-Backups von Data Guard Standby-Datenbanken erstellen. Offline-Shutdown-Backup, Backup nur für Archivprotokolle und vollständiges Backup werden nicht unterstützt.

- Oracle Active Data Guard Standby

  Sie können nur Online-Backups von Active Data Guard Standby-Datenbanken erstellen. Backup nur für Archivprotokolle und vollständige Backups werden nicht unterstützt.

  > Vor dem Erstellen eines Backups von Data Guard Standby oder der Active Data Guard Standby Datenbank wird der Managed Recovery-Prozess (MRP) angehalten und nach dem Erstellen des Backups wird MRP gestartet.

- Automatisches Storage-Management (ASM)
  - ASM Standalone und ASM RAC auf Virtual Machine Disk (VMDK)

Unter allen für Oracle-Datenbanken unterstützten Wiederherstellungsmethoden können Sie nur eine Verbindung-und-Kopie-Wiederherstellung von ASM RAC-Datenbanken auf VMDK durchführen.

- ASM Standalone und ASM RAC auf Raw Device Mapping (RDM) Sie können Backup-, Restore- und Klonvorgänge auf Oracle Datenbanken auf ASM mit oder ohne ASMLib durchführen.
- Oracle ASM Filtertreiber (ASMFD)

  PDB-Migration und PDB-Klonvorgänge werden nicht unterstützt.

- Oracle Flex ASM

Aktuelle Informationen zu unterstützten Oracle-Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Arten von Backups, die für Oracle-Datenbanken unterstützt werden

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt Online- und Offline-Backups für Oracle Datenbanken.

Online-Backup

Ein Backup, das erstellt wird, wenn sich die Datenbank im Online-Status befindet, wird als Online-Backup bezeichnet. Auch als Hot Backup bezeichnet, ermöglicht ein Online-Backup die Erstellung eines Backups der Datenbank, ohne dass es heruntergefahren werden muss.

Im Rahmen des Online-Backups können Sie eine Sicherung der folgenden Dateien erstellen:

- Nur Datendateien und Kontrolldateien
- Nur Archivprotokolldateien (in diesem Szenario wird die Datenbank nicht in den Backup-Modus versetzt)
- Vollständige Datenbank, die Datendateien, Kontrolldateien und Archivprotokolldateien umfasst

Offline-Backup

Ein Backup, das erstellt wird, wenn sich die Datenbank entweder im gemounteten oder Herunterfahrzustand befindet, wird als Offline-Backup bezeichnet. Ein Offline-Backup wird auch als Cold Backup bezeichnet. Sie können nur Datendateien und Kontrolldateien in Offline-Backups einbeziehen. Sie können entweder einen Offline-Mount- oder Offline-Shutdown-Backup erstellen.

- Wenn Sie ein Offline-Mount-Backup erstellen, müssen Sie sicherstellen, dass sich die Datenbank in einem gemounteten Zustand befindet.

  Wenn sich die Datenbank in einem anderen Zustand befindet, schlägt der Backup-Vorgang fehl.

- Beim Erstellen einer Offline-Shutdown-Sicherung kann sich die Datenbank in einem beliebigen Zustand befinden.

  Der Datenbankstatus wird in den erforderlichen Zustand geändert, um ein Backup zu erstellen. Nach dem Erstellen des Backups wird der Datenbankzustand in den ursprünglichen Zustand zurückgesetzt.

Wie SnapCenter Oracle Datenbanken erkennt

„Ressourcen“ sind Oracle Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Diese Datenbanken können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben. Sie sollten den Prozess kennen, den SnapCenter befolgt, um verschiedene Typen und Versionen von Oracle Datenbanken zu ermitteln.

Für Oracle-Versionen 11*g*_ *bis 12*c__R1	**Für Oracle-Versionen 12*c*R2 bis 18*c***
RAC-Datenbank: Die RAC-Datenbanken werden nur auf Basis von /etc/oratab-Einträgen entdeckt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.	**RAC-Datenbank**: Die RAC-Datenbanken werden mit dem Befehl srvctl config ermittelt.
Standalone: Die Standalone-Datenbanken werden nur auf Basis von /etc/oratab-Einträgen entdeckt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.	**Standalone**: Die Standalone-Datenbanken werden anhand der Einträge in der Datei /etc/oratab und der Ausgabe des Befehls srvctl config ermittelt.
ASM: Der ASM-Instanzeintrag sollte in der Datei /etc/oratab verfügbar sein.	**ASM**: Der ASM-Instanzeintrag muss nicht in der Datei /etc/oratab enthalten sein.

Für Oracle-Versionen 11*g*_ bis 12**c**__R1	Für Oracle-Versionen 12*c*R2 bis 18*c*
RAC One Node: Die RAC One Node-Datenbanken werden nur auf der Grundlage von /etc/oratab-Einträgen entdeckt. Die Datenbanken sollten sich entweder im Status *nomount*, *Mount* oder *open* befinden. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben. Der RAC One Node Datenbankstatus wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt und Backups mit der Datenbank verknüpft sind. Wenn die Datenbank verschoben wird, sollten Sie die folgenden Schritte ausführen: 1. Fügen Sie den umgelagerten Datenbankeintrag manuell in der Datei /etc/oratab auf dem Knoten Failed-over RAC hinzu. 2. Aktualisieren Sie die Ressourcen manuell. 3. Wählen Sie auf der Seite Ressource die RAC One Node-Datenbank aus, und klicken Sie dann auf **Datenbankeinstellungen**. 4. Konfigurieren Sie die Datenbank so, dass die bevorzugten Cluster-Knoten auf den RAC-Knoten eingestellt werden, der derzeit die Datenbank hostet. 5. Führen Sie die SnapCenter Vorgänge aus. Wenn Sie eine Datenbank von einem Node auf einen anderen Node verschoben haben und der Oratab-Eintrag im früheren Node nicht gelöscht wird, sollten Sie den Oratab-Eintrag manuell löschen, um zu vermeiden, dass dieselbe Datenbank zweimal angezeigt wird.	**RAC One Node**: Die RAC One Node-Datenbanken werden nur mit dem Befehl srvctl config ermittelt. Die Datenbanken sollten sich entweder im Status *nomount*, *Mount* oder *open* befinden. Der RAC One Node Datenbankstatus wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt und Backups mit der Datenbank verknüpft sind. Wenn die Datenbank verschoben wird, sollten Sie die folgenden Schritte ausführen: 1. Aktualisieren Sie die Ressourcen manuell. 2. Wählen Sie die RAC One Node-Datenbank auf der Ressourcen-Seite aus, und klicken Sie dann auf **Datenbank-Einstellungen**. 3. Konfigurieren Sie die Datenbank so, dass die bevorzugten Cluster-Knoten auf den RAC-Knoten eingestellt werden, der derzeit die Datenbank hostet. 4. Führen Sie die SnapCenter Vorgänge aus.

Wenn in der Datei /etc/oratab Oracle 12*c*R2 und 18*c*-Datenbankeinträge vorhanden sind und dieselbe Datenbank beim Befehl srvctl config registriert ist, beseitigt SnapCenter die doppelten Datenbankeinträge. Wenn veraltete Datenbankeinträge vorhanden sind, wird die Datenbank erkannt, die Datenbank ist jedoch nicht erreichbar und der Status ist offline.

Bevorzugte Knoten im RAC-Setup

Im Oracle Real Application Clusters (RAC)-Setup können Sie die bevorzugten Knoten angeben, auf denen der Backup-Vorgang ausgeführt wird. Wenn Sie den bevorzugten Node nicht angeben, weist SnapCenter automatisch einen Node als bevorzugten Node zu und auf diesem Node wird das Backup erstellt.

Die bevorzugten Knoten können einer oder alle Cluster-Knoten sein, wo die RAC-Datenbankinstanzen vorhanden sind. Der Backup-Vorgang wird nur auf den bevorzugten Knoten in der Reihenfolge der Präferenz ausgelöst.

Beispiel: Die RAC-Datenbank cdbrac hat drei Instanzen: Cdbrac1 auf node1, cdbrac2 auf node2 und cdbrac3 auf node3. Die Instanzen node1 und node2 werden als bevorzugte Nodes konfiguriert, wobei node2 die erste Präferenz und node1 als zweite Präferenz. Wenn Sie einen Sicherungsvorgang ausführen, wird in node2 der erste Vorgang versucht, da er der erste bevorzugte Node ist. Wenn node2 nicht in dem Status zum Sichern ist, was aus mehreren Gründen, wie z. B. dem Plug-in-Agent, auf dem Host nicht ausgeführt werden kann, ist die Datenbankinstanz auf dem Host nicht im erforderlichen Zustand für den angegebenen Backup-Typ, Oder die Datenbankinstanz auf node2 in einer FlexASM-Konfiguration wird nicht von der lokalen ASM-Instanz bereitgestellt; dann wird der Vorgang auf node1 versucht. Das node3 wird nicht für das Backup verwendet, da es sich nicht auf der Liste der bevorzugten Nodes befindet.

In einem Flex ASM-Setup werden Leaf-Knoten nicht als bevorzugte Knoten aufgeführt, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist. Wenn sich Änderungen an den Flex ASM-Cluster-Knotenrollen ergeben, sollten Sie manuell ermitteln, damit die bevorzugten Nodes aktualisiert werden.

Erforderlicher Datenbankstatus

Die RAC-Datenbankinstanzen auf den bevorzugten Nodes müssen den erforderlichen Status aufweisen, damit das Backup erfolgreich abgeschlossen werden kann:

- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im offenen Zustand befinden, um ein Online-Backup zu erstellen.
- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im Mount-Status befinden, und alle anderen Instanzen, einschließlich anderer bevorzugter Knoten, müssen sich im Mount-Status oder niedriger befinden, um ein Offline-Mount-Backup zu erstellen.
- Instanzen von RAC Datenbanken können in jedem Zustand sein. Sie müssen jedoch die bevorzugten Nodes angeben, um ein Offline-Herunterfahren-Backup zu erstellen.

So katalogisieren Sie Backups mit Oracle Recovery Manager

Die Backups von Oracle-Datenbanken können mit Oracle Recovery Manager (RMAN) katalogisiert werden, um die Backup-Informationen im Oracle RMAN-Repository zu speichern.

Die katalogisierten Backups können später für Wiederherstellungen auf Blockebene oder für zeitpunktgenaue Recovery-Vorgänge in Tablespaces verwendet werden. Wenn Sie diese katalogisierten Backups nicht benötigen, können Sie die Kataloginformationen entfernen.

Die Datenbank muss im gemounteten oder höheren Zustand für die Katalogisierung enthalten sein. Sie können Katalogisierung von Daten-Backups, Archivierungs-Log-Backups und vollständigen Backups durchführen. Wenn die Katalogisierung für ein Backup einer Ressourcengruppe mit mehreren Datenbanken aktiviert ist, wird für jede Datenbank eine Katalogisierung durchgeführt. Bei Oracle RAC-Datenbanken wird die Katalogisierung auf dem bevorzugten Knoten durchgeführt, auf dem die Datenbank mindestens gemounted ist.

> Wenn Sie Backups einer RAC-Datenbank katalogisieren möchten, stellen Sie sicher, dass für diese Datenbank kein anderer Job ausgeführt wird. Wenn ein anderer Job ausgeführt wird, schlägt der Katalogisierung fehl, anstatt sich in die Warteschlange zu stellen.

Standardmäßig wird die Kontrolldatei der Zieldatenbank zur Katalogisierung verwendet. Wenn Sie eine externe Katalogdatenbank hinzufügen möchten, können Sie diese konfigurieren, indem Sie die Anmeldeinformationen und den TNS-Namen (Transparent Network Substrat) des externen Katalogs mithilfe des Datenbankeinstellungs-Assistenten von der grafischen Benutzeroberfläche von SnapCenter (GUI) angeben.

Sie können die externe Katalogdatenbank auch über die CLI konfigurieren, indem Sie den Befehl Configure-SmOracleDatabase mit den Optionen -OracleRmanCatalogCredentialName und -OracleRmanCatalogTnsName ausführen.

Wenn Sie die Katalogisierung-Option aktiviert haben und gleichzeitig eine Oracle-Backup-Richtlinie über die SnapCenter-GUI erstellen, werden die Backups über Oracle RMAN als Teil des Backup-Vorgangs katalogisiert. Sie können auch die verzögerten Katalogisierung von Backups mithilfe des Befehls Catalog-SmBackupWithOracleRMAN durchführen. Nach dem Katalogisierung der Backups können Sie den Befehl Get-SmBackupDetails ausführen, um die katalogisierten Backup-Informationen wie das Tag für katalogisierte Datendateien, den Kontroll-Dateikatalog-Pfad und die katalogisierten Archiv-Log-Speicherorte zu erhalten.

Wenn der Name der ASM-Festplattengruppe größer oder gleich 16 Zeichen ist, ab SnapCenter 3.0, lautet das für die Datensicherung verwendete Namensformat SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. Wenn der Name der Laufwerksgruppe jedoch weniger als 16 Zeichen beträgt, ist das für das Backup verwendete Namensformat DISKGROUPNAME_DBSID_BACKUPID, das gleiche Format wie in SnapCenter 2.0.

Die HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Stellen), die für jede ASM-Laufwerksgruppe eindeutig ist.

Sie können crosschecks durchführen, um veraltete RMAN Repository-Informationen über Backups zu aktualisieren, deren Repository-Datensätze nicht ihrem physischen Status entsprechen. Wenn ein Benutzer zum Beispiel archivierte Protokolle mit einem Betriebssystembefehl von der Festplatte entfernt, zeigt die Steuerdatei immer noch an, dass sich die Protokolle auf der Festplatte befinden, wenn sie sich tatsächlich nicht befinden. Mit der crosscheck-Operation können Sie die Steuerdatei mit den Informationen aktualisieren. Sie können crosscheck aktivieren, indem Sie den Befehl set-SmConfigSettings ausführen und den Wert TRUE dem PARAMETER ENABLE_CROSSCHECK zuweisen. Der Standardwert ist FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Sie können die Kataloginformationen entfernen, indem Sie den Befehl Uncatalog-SmBackupWithOracleRMAN ausführen. Sie können die Kataloginformationen nicht mithilfe der SnapCenter-GUI entfernen. Die Informationen eines katalogisierten Backups werden jedoch beim Löschen des Backups oder beim Löschen der mit diesem katalogisierten Backup verknüpften Aufbewahrungs- und Ressourcengruppe entfernt.

Wenn Sie eine Löschung des SnapCenter-Hosts erzwingen, werden die Informationen der mit diesem Host verbundenen katalogisierten Backups nicht entfernt. Sie müssen die Informationen aller katalogisierten Backups für diesen Host entfernen, bevor Sie die Löschung des Hosts erzwingen.

Wenn die Katalogisierung und Entkatalogisieren fehlschlägt, weil die Betriebsdauer den für DEN PARAMETER ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT angegebenen Zeitwert überschritten hat, sollten Sie den Wert des Parameters ändern, indem Sie den folgenden Befehl ausführen:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Nachdem Sie den Wert des Parameters geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help Command_Name abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide".

Backup-Pläne

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen. So könnten beispielsweise regelmäßige Transaktions-Log-Backups ausreichen, um sicherzustellen, dass Sie die Backups haben, die Sie benötigen. Je öfter Sie Ihre Datenbanken sichern, desto weniger Transaktions-Logs benötigt SnapCenter zum Zeitpunkt der Wiederherstellung, was zu schnelleren Restore-Vorgängen führen kann.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Konventionen bei Backup-Namen

Sie können entweder die standardmäßige Namenskonvention für Snapshot Kopien verwenden oder eine individuelle Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt einen Zeitstempel zu den Namen von Snapshot Kopien hinzu, der Ihnen hilft, zu identifizieren, wann die Kopien erstellt wurden.

Die Snapshot Kopie verwendet die folgende standardmäßige Namenskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutungen:

- *Dts1* ist der Name der Ressourcengruppe.
- *Mach1x88* ist der Hostname.
- *03-12-2015_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Namensformat für die Snapshot-Kopie angeben und Ressourcen oder Ressourcengruppen schützen, indem Sie **Verwenden Sie benutzerdefiniertes Namensformat für die Snapshot-Kopie** wählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Namen der Snapshot Kopie das Suffix mit dem Zeitstempel hinzugefügt.

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Überprüfen Sie die Backup-Kopie mithilfe des primären oder sekundären Storage Volumes

Sie können Backup-Kopien auf dem primären Storage Volume oder auf dem sekundären SnapMirror oder SnapVault Storage Volume überprüfen. Bei der Überprüfung und Verwendung eines sekundären Storage-Volumes wird die Last für das primäre Storage Volume verringert.

Wenn Sie ein Backup auf dem primären oder sekundären Storage Volume überprüfen, werden alle primären und sekundären Snapshot Kopien als überprüft markiert.

Zur Überprüfung von Backup-Kopien auf dem sekundären SnapVault Storage Volume ist eine SnapRestore Lizenz erforderlich.

Ermitteln Sie, ob Oracle-Datenbanken für Backups verfügbar sind

Ressourcen sind Oracle Datenbanken auf dem Host, die von SnapCenter gemanagt werden. Diese Datenbanken können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren Datenbanken

ermittelt haben.

Was Sie brauchen

- Sie müssen Aufgaben wie das Installieren des SnapCenter-Servers, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Wenn die Datenbanken auf einer Virtual Machine Disk (VMDK) oder RDM (Raw Device Mapping) befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Implementieren Sie das SnapCenter Plug-in für VMware vSphere".
- Wenn sich Datenbanken auf einem VMDK-Dateisystem befinden, müssen Sie sich bei vCenter angemeldet und in **VM-Optionen** > **Erweitert** > **Konfiguration bearbeiten** navigiert haben, um den Wert von *Disk.enableUUID* auf true für die VM festzulegen.
- Sie müssen den Prozess überprüft haben, den SnapCenter befolgt, um verschiedene Typen und Versionen von Oracle Datenbanken zu ermitteln.

Über diese Aufgabe

Nach der Installation des Plug-ins werden alle Datenbanken auf diesem Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Die Datenbanken sollten sich mindestens im angehängten Zustand oder oben befinden, damit die Datenbanken erfolgreich erkannt werden können. In einer Oracle Real Application Clusters (RAC)-Umgebung sollte sich die RAC-Datenbankinstanz auf dem Host, auf dem die Ermittlung ausgeführt wird, mindestens im gemounteten Zustand oder oben befinden, damit die Datenbankinstanz erfolgreich ermittelt werden kann. Nur die erfolgreich erkannten Datenbanken können den Ressourcengruppen hinzugefügt werden.

Wenn Sie eine Oracle-Datenbank auf dem Host gelöscht haben, ist SnapCenter-Server nicht bekannt und führt die gelöschte Datenbank auf. Sie sollten die Ressourcen manuell aktualisieren, um die Liste der SnapCenter-Ressourcen zu aktualisieren.

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.

   Klicken Sie Auf  Und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern. Anschließend können Sie auf die klicken  Symbol zum Schließen des Filterfensters.
3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   In einem RAC-Szenario mit einem Knoten wird die Datenbank als RAC-Datenbank auf dem Knoten erkannt, auf dem sie derzeit gehostet wird.

Ergebnisse

Die Datenbanken werden zusammen mit Informationen wie Datenbanktyp, Host- oder Cluster-Name, zugeordnete Ressourcengruppen und -Richtlinien sowie Status angezeigt.

- Wenn sich die Datenbank auf einem Storage-System außerhalb von NetApp befindet, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ einen für die Backup-Meldung nicht verfügbaren Status an.

  Sie können keine Datensicherungsvorgänge für die Datenbank ausführen, die sich auf einem Storage-System anderer Anbieter befindet.

- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und nicht geschützt ist, wird auf der Benutzeroberfläche in der Spalte Gesamtstatus eine nicht geschützte Meldung angezeigt.
- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ eine für die Datensicherung verfügbare Meldung an.

Wenn Sie eine Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ansicht Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Sie müssen Datenbankanmeldeinformationen konfigurieren, um die Datenbank schützen oder zur Ressourcengruppe hinzufügen zu können, um Datensicherungsvorgänge durchzuführen.

Erstellung von Backup-Richtlinien für Oracle Datenbanken

Bevor Sie SnapCenter zum Backup von Oracle-Datenbankressourcen verwenden, müssen Sie eine Backup-Richtlinie für die Ressource oder die Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln. Sie können auch die Einstellungen für Replikation, Skript und Backup-Typ festlegen. Das Erstellen einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressource oder Ressourcengruppe wiederverwenden möchten.

Was Sie brauchen

- Sie müssen Ihre Backup-Strategie definiert haben.
- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erkennen von Datenbanken und das Erstellen von Speichersystemverbindungen ausführen.
- Wenn Sie Snapshot Kopien in einen gespiegelten oder sekundären Vault-Storage replizieren, muss der SnapCenter Administrator Ihnen die SVMs sowohl für die Quell- als auch die Ziel-Volumes zugewiesen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Wählen Sie in der Dropdown-Liste * Oracle Database* aus.
4. Klicken Sie Auf **Neu**.
5. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
6. Führen Sie auf der Seite Sicherungstyp die folgenden Schritte durch:

   ◦ Wenn Sie **ein Online-Backup erstellen** möchten, wählen Sie **Online-Backup**.

   Sie müssen angeben, ob Sie alle Datendateien, Kontrolldateien und Archivprotokolldateien, nur

Datendateien und Kontrolldateien oder nur Archivprotokolldateien sichern möchten.

- Wenn Sie **ein Offline-Backup** erstellen möchten, wählen Sie **Offline-Backup** aus, und wählen Sie dann eine der folgenden Optionen aus:
  - Wenn Sie eine Offline-Sicherung erstellen möchten, wenn sich die Datenbank im Bereitstellungszustand befindet, wählen Sie **Mount**.
  - Wenn Sie eine Offline-Shutdown-Sicherung erstellen möchten, indem Sie die Datenbank in den Shutdown-Status ändern, wählen Sie **Shutdown** aus.

    Wenn Sie über steckbare Datenbanken (PDBs), und möchten den Zustand der PDBs vor der Erstellung des Backups speichern, müssen Sie **Save State of PDBs** wählen. Dies ermöglicht Ihnen, die PDBs in den ursprünglichen Zustand zu bringen, nachdem das Backup erstellt wurde.
- Geben Sie die Zeitplanhäufigkeit an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

  Sie können den Zeitplan (Startdatum und Enddatum) für den Backup-Vorgang festlegen, während Sie eine Ressourcengruppe erstellen. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

  Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.
- Wenn Sie das Backup mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Katalog-Backup mit Oracle Recovery Manager (RMAN)** aus.

  Sie können die Katalogisierung für ein Backup auf einmal entweder über die Benutzeroberfläche oder über den SnapCenter-CLI-Befehl Catalog-SmBackupWithOracleRMAN aufgeschobenen.

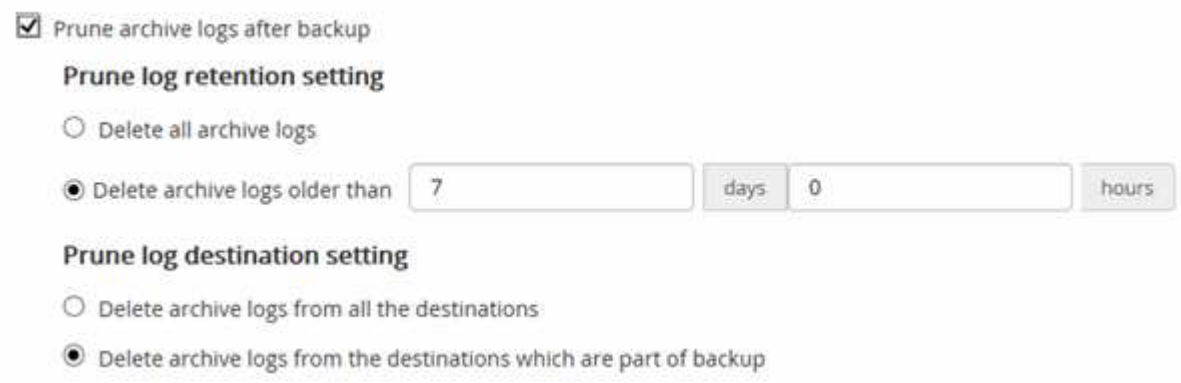
  Wenn Sie Backups einer RAC-Datenbank katalogisieren möchten, stellen Sie sicher, dass für diese Datenbank kein anderer Job ausgeführt wird. Wenn ein anderer Job ausgeführt wird, schlägt der Katalogisierung fehl, anstatt sich in die Warteschlange zu stellen.
- Wenn Sie Archivprotokolle nach Backup beschneiden möchten, wählen Sie **Prune Archivprotokolle nach Backup** aus.

  Das Beschneiden von Archivprotokollen aus dem Archiv-Protokollziel, das in der Datenbank nicht konfiguriert ist, wird übersprungen.

  Wenn Sie Oracle Standard Edition verwenden, können Sie WÄHREND der Sicherung des Archivprotokolls DIE Parameter LOG_ARCHIVE_DEST und LOG_ARCHIVE_DUPLEX_DEST verwenden.
- Sie können Archivprotokolle nur löschen, wenn Sie die Archivprotokolldateien als Teil Ihrer Sicherung ausgewählt haben.

  Sie müssen sicherstellen, dass alle Knoten in einer RAC-Umgebung auf alle Archivprotokolle zugreifen können, damit der Löschvorgang erfolgreich ist.

Ihr Ziel ist	Dann…
Löschen Sie alle Archivprotokolle	Wählen Sie **Alle Archivprotokolle löschen**.
Löschen alter Archivprotokolle	Wählen Sie **Archivprotokolle löschen, die älter als** sind, und geben Sie dann das Alter der Archivprotokolle an, die in Tagen und Stunden gelöscht werden sollen.
Löschen Sie Archivprotokolle von allen Zielen	Wählen Sie **Archivprotokolle von allen Zielen löschen**.
Löschen Sie die Archivprotokolle von den Protokollzielen, die Teil des Backups sind	Wählen Sie **Archivprotokolle aus den Zielen löschen, die Teil der Datensicherung sind**.



+

7. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…

Aufbewahrung einer bestimmten Anzahl von Snapshot Kopien	Wählen Sie **Gesamtanzahl der zu behenden Snapshot-Kopien** aus, und geben Sie dann die Anzahl der Snapshot-Kopien an, die beibehalten werden sollen. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 festlegen, kann der Aufbewahrungsvorgang möglicherweise fehlschlagen, da die erste Snapshot Kopie die Referenzkopie für die SnapVault-Beziehung ist, bis eine neuere Snapshot Kopie auf das Ziel repliziert wird.
Behalten Sie die Snapshot Kopien für eine bestimmte Anzahl von Tagen bei	Wählen Sie **Snapshot Kopien behalten für** aus, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshot Kopien behalten möchten, bevor Sie sie löschen.

Sie können Archiv-Protokoll-Backups nur dann aufbewahren, wenn Sie die Archiv-Log-Dateien als Teil Ihrer Sicherung ausgewählt haben.

8. Geben Sie auf der Seite Replikation die Replikationseinstellungen an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation).

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen.
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Abhängig von dem ausgewählten Etikett der Snapshot Kopie wendet ONTAP die Aufbewahrungsrichtlinie für sekundäre Snapshot Kopien an, die mit dem Etikett übereinstimmt. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um zu vermeiden, dass die maximale Anzahl an Snapshot Kopien auf dem sekundären Storage erreicht wird.

9. Geben Sie auf der Seite Skript den Pfad und die Argumente des Prescript oder Postscript ein, das Sie vor oder nach dem Backup ausführen möchten.

   Die Voreinstellungen und Postskripte müssen entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

   Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.

10. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

    a. Wählen Sie den Backup-Zeitplan aus, für den Sie den Verifizierungsvorgang durchführen möchten.

    b. Geben Sie im Abschnitt Skriptbefehle überprüfen den Pfad und die Argumente des Preskript oder Postscript ein, die vor bzw. nach der Verifikation ausgeführt werden sollen.

       Die Voreinstellungen und Postskripte müssen entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Oracle-Datenbanken

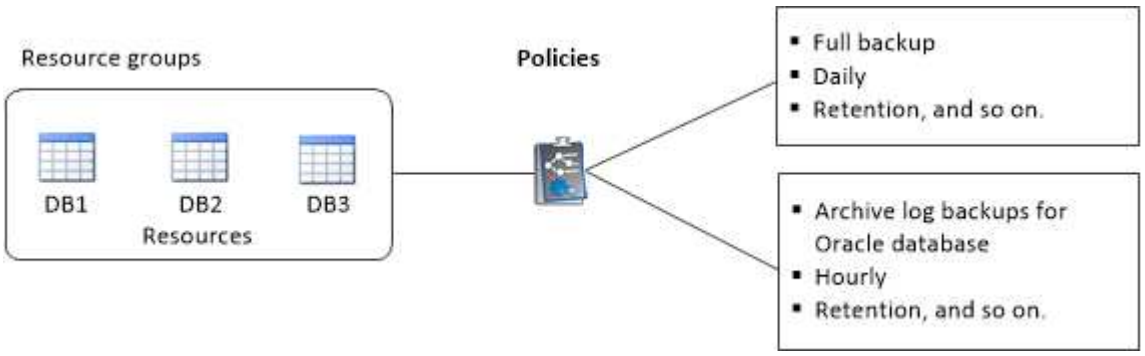
Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind.

Über diese Aufgabe

Sie sollten sicherstellen, dass die Datenbank mit Dateien auf den ASM-Laufwerksgruppen entweder im „MOUNT“- oder „OPEN“-Zustand sein sollte, um die Backups mit dem Oracle DBVERIFY-Dienstprogramm zu überprüfen.

Sie sollten eine oder mehrere Richtlinien an die Ressourcengruppe anhängen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf der Seite Ressourcen auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

Für dieses Feld…	Tun Sie das…
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot Kopie verwenden möchten. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.
Ausschließen von Zielen für Archivprotokolle von der Sicherung	Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

4. Wählen Sie auf der Seite Ressourcen einen Oracle-Datenbank-Hostnamen aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden im Abschnitt Verfügbare Ressourcen nur dann aufgelistet, wenn die Ressource erfolgreich ermittelt wurde. Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

5. Wählen Sie im Abschnitt Verfügbare Ressourcen die Ressourcen aus, und verschieben Sie sie in den Abschnitt Ausgewählte Ressourcen.

   Sie können Datenbanken von Linux- und AIX-Hosts in einer einzigen Ressourcengruppe hinzufügen.

6. Führen Sie auf der Seite Richtlinien die folgenden Schritte durch:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf klicken + .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken Sie Auf + In der Spalte Zeitplan konfigurieren für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Fenster Add Schedules for Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

   Dabei ist *Policy_Name* der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror oder SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Klicken Sie Auf + In der Spalte Zeitplan konfigurieren, um den Überprüfungsplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
   c. Führen Sie im Dialogfeld Add Verification Schedules_Policy_Name_ die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen** und wählen Sie dann den Terminplantyp aus der Dropdown-Liste aus.

   d. Wählen Sie **am sekundären Standort überprüfen**, um Ihre Backups auf dem sekundären Speichersystem zu überprüfen.
   e. Klicken Sie auf **OK**.

      Die konfigurierten Überprüfungszeitpläne sind in der Spalte „angewendete Zeitpläne“ aufgeführt.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Anforderungen für das Backup einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank sichern, sollten Sie sicherstellen, dass die Voraussetzungen abgeschlossen sind.

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Sie müssen das Aggregat, das vom Backup-Vorgang verwendet wird, der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Sie sollten überprüft haben, ob alle zu der Datenbank gehörenden Daten-Volumes und Archivprotokoll-Volumes geschützt sind, wenn für diese Datenbank ein sekundärer Schutz aktiviert ist.
- Sie sollten überprüfen, dass die Datenbank, die Dateien auf den ASM-Laufwerksgruppen enthält, entweder im Status „`MOUNT`“ oder „`OPEN`“ liegt, um die Backups mit dem Dienstprogramm Oracle DBVERIFY zu überprüfen.
- Sie sollten überprüfen, ob die Länge des Mount-Punkts für das Volumen 240 Zeichen nicht überschreitet.
- Den Wert von RESTTimeout sollten Sie in *C:\Programme\NetApp \SMCore\SMCoreServiceHost.exe.config* der Datei SnapCenter Server auf 86400000 Sekunden erhöhen, wenn die zu sichernde Datenbank groß ist (Größe in TB).

  Während Sie die Werte ändern, stellen Sie sicher, dass keine laufenden Jobs vorhanden sind, und starten Sie den SnapCenter SMCore-Dienst nach Erhöhung des Werts neu.

Oracle-Ressourcen sichern

Wenn eine Ressource nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

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 Sie Auf , und wählen Sie dann den Host-Namen und den Datenbanktyp, um die Ressourcen zu filtern.

   Sie können dann auf * klicken * Zum Schließen des Filterfensters.

4. Wählen Sie die Datenbank aus, die Sie sichern möchten.

   Die Seite Datenbankschutz wird angezeigt.

5. Führen Sie auf der Seite „Ressource“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie anschließend ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot Kopie verwenden möchten. Beispiel: Custtext__Policy_hostname oder Resource_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.
Ausschließen von Zielen für Archivprotokolle von der Sicherung	Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

6. Führen Sie auf der Seite Richtlinien die folgenden Schritte durch:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf * klicken *.

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken Sie Auf In der Spalte Zeitplan konfigurieren für die Richtlinie konfigurieren, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Fenster Add Schedules for Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

   a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror oder SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.

   b. Klicken Sie Auf In der Spalte „Zeitpläne konfigurieren“ können Sie den Überprüfungsplan für alle Zeitplantypen der Richtlinie konfigurieren.

   c. Führen Sie im Dialogfeld Add Verification Schedules_Policy_Name_ die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.

Ihr Ziel ist	Tun Sie das…
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen** aus, und wählen Sie dann den Terminplantyp aus der Dropdown-Liste aus. In einem Flex ASM-Setup können Sie auf Leaf-Knoten keine Verifizierungsvorgang durchführen, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist.

d. Wählen Sie **am sekundären Standort überprüfen**, um Ihre Backups auf dem sekundären Speicher zu überprüfen.

e. Klicken Sie auf **OK**.

Die konfigurierten Überprüfungszeitpläne sind in der Spalte „angewendete Zeitpläne“ aufgeführt.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den Backup-Vorgang anhängen möchten, der an der Ressource durchgeführt wird, und dann wählen Sie **Job-Bericht anhängen**.

Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Die Seite der Datenbanktopologie wird angezeigt.

10. Klicken Sie auf **Jetzt sichern**.
11. Führen Sie auf der Seite Backup die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

    Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

    b. Klicken Sie Auf **Backup**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Nach Ihrer Beendigung

- In AIX Setup können Sie den Befehl lkdev zum Sperren und den Befehl rendev verwenden, um die Festplatten umzubenennen, auf denen sich die gesicherte Datenbank befand.

Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang,

wenn Sie die Wiederherstellung mit diesem Backup durchführen.

- Wenn der Backup-Vorgang fehlschlägt, weil die Ausführungszeit der Datenbankabfrage den Timeout-Wert überschritten hat, sollten Sie den Wert der PARAMETER ORACLE_SQL_QUERY_TIMEOUT und ORACLE_PLUGIN_SQL_QUERY_TIMEOUT ändern, indem Sie das Cmdlet Set-SmConfigSettings ausführen:

  Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Wenn die Datei nicht zugänglich ist und der Mount-Punkt während des Verifizierungsvorgangs nicht verfügbar ist, kann der Vorgang mit dem Fehlercode DBV-00100 der angegebenen Datei fehlschlagen. Sie sollten die Werte der Parameter VERIFICATION_DELAY und VERIFICATION_RETRY_COUNT in sco.properties ändern.

  Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

- In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung erkennen.
- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java Heap-Größe für das SnapCenter-Plug-in für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

  Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei */opt/netapp/init_scripts/scvservice*. In diesem Skript, das `do_start method` Befehl startet den SnapCenter-VMware-Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Weitere Informationen

- "SnapMirror oder SnapVault-Beziehung kann nach MetroCluster Failover nicht erkannt werden"
- "Oracle RAC One-Knoten-Datenbank wird zur Durchführung von SnapCenter-Operationen übersprungen"
- "Fehler beim Ändern des Status einer Oracle 12c ASM-Datenbank"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Sichern Sie Oracle Database Resource Groups

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

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 **Ressourcengruppe** aus.

Sie können die Ressourcengruppe entweder durch Eingabe des Ressourcengruppennamens in das Suchfeld oder durch Klicken auf * durchsuchen* Und dann das Tag auswählen. Sie können dann auf * klicken* Zum Schließen des Filterfensters.

3. Wählen Sie auf der Seite Ressourcengruppen die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.

   Wenn Sie eine föderierte Ressourcengruppe mit zwei Datenbanken haben und eine der Datenbanken Datendatei auf nicht-NetApp-Storage hat, wird der Backup-Vorgang abgebrochen, obwohl sich die andere Datenbank auf NetApp Storage befindet.

4. Führen Sie auf der Seite Backup die folgenden Schritte aus:

   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Klicken Sie Auf **Backup**.

5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Nach Ihrer Beendigung

- In AIX Setup können Sie den Befehl lkdev zum Sperren und den Befehl rendev verwenden, um die Festplatten umzubenennen, auf denen sich die gesicherte Datenbank befand.

  Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mit diesem Backup durchführen.

- Wenn der Backup-Vorgang fehlschlägt, weil die Ausführungszeit der Datenbankabfrage den Timeout-Wert überschritten hat, sollten Sie den Wert der PARAMETER ORACLE_SQL_QUERY_TIMEOUT und ORACLE_PLUGIN_SQL_QUERY_TIMEOUT ändern, indem Sie das Cmdlet Set-SmConfigSettings ausführen:

  Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Wenn die Datei nicht zugänglich ist und der Mount-Punkt während des Verifizierungsvorgangs nicht verfügbar ist, kann der Vorgang mit dem Fehlercode DBV-00100 der angegebenen Datei fehlschlagen. Sie sollten die Werte der Parameter VERIFICATION_DELAY und VERIFICATION_RETRY_COUNT in sco.properties ändern.

  Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

Sichern Sie Oracle Datenbanken mit UNIX Befehlen

Der Backup-Workflow umfasst die Planung, die Ermittlung der Backup-Ressourcen, die Erstellung von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das

Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Was Sie brauchen

- Sie sollten die Verbindungen zum Speichersystem hinzugefügt und die Anmeldedaten mit den Befehlen *Add-SmStorageConnection* und *Add-SmCredential* erstellt haben.
- Sie sollten die Verbindungssitzung mit dem SnapCenter-Server mit dem Befehl *Open-SmConnection* eingerichtet haben.

  Sie können nur eine SnapCenter-Konto-Anmeldesitzung haben und das Token wird im Home-Verzeichnis des Benutzers gespeichert.

> Die Verbindungssitzung ist nur 24 Stunden lang gültig. Sie können jedoch ein Token mit der Option TokenNeverExpires erstellen, um ein Token zu erstellen, das nie abläuft und die Sitzung immer gültig ist.

Über diese Aufgabe

Sie sollten die folgenden Befehle ausführen, um die Verbindung mit dem SnapCenter Server herzustellen, die Oracle-Datenbankinstanzen zu ermitteln, Richtlinien und Ressourcengruppen hinzuzufügen, die Sicherung und Überprüfung des Backups durchzuführen.

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide".

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer: *Open-SmConnection*
2. Führen Sie Host-Ressourcen Discovery-Vorgang durch: *Get-SmResources*
3. Konfigurieren Sie die Anmeldeinformationen für Oracle-Datenbanken und bevorzugte Knoten für den Backup-Betrieb einer RAC-Datenbank (Real Application Cluster): *Configure-SmOracleDatabase*
4. Backup-Richtlinie erstellen: *Add-SmPolicy*
5. Abrufen der Informationen zum sekundären Speicherort (SnapVault oder SnapMirror) : *get-SmSecondaryDetails*

   Dieser Befehl ruft Details zur Zuordnung von primärem zu sekundärem Speicher einer bestimmten Ressource ab. Sie können die Zuordnungsdetails verwenden, um die sekundären Verifizierungseinstellungen beim Erstellen einer Backup-Ressourcengruppe zu konfigurieren.

6. Eine Ressourcengruppe zu SnapCenter hinzufügen: *Add-SmResourceGroup*
7. Backup erstellen: *New-SmBackup*

   Sie können den Job mit der Option WaitForCompletion abfragen. Wenn diese Option angegeben ist, fragt der Befehl den Server bis zum Abschluss des Backup-Jobs ab.

8. Abrufen der Protokolle von SnapCenter: *Get-SmLogs*

Überwachen Sie die Backup-Vorgänge für die Oracle Datenbank

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie Auf Filtern der Liste, sodass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Der Status des Backupjobs wird zwar angezeigt Wenn Sie auf die Jobdetails klicken, wird möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Backup-Vorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite **Jobdetails** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen Sie Datensicherungsvorgänge im Teilfenster „Vorgang“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten

Backup-Vorgängen angezeigt. Wenn Sie Plug-in für SQL Server oder Plug-in für Exchange Server verwenden, werden im Aktivitätsbereich auch Informationen über den erneuten Seeding angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie Auf  Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt.

   Wenn Sie auf einen der Vorgänge klicken, werden die Arbeitsdetails auf der Seite Jobdetails aufgeführt.

Backup-Vorgänge von Oracle-Datenbanken abbrechen

Sie können Backup-Vorgänge, die ausgeführt werden, in die Warteschlange gestellt oder nicht ansprechbar sind, abbrechen.

Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Backup-Vorgänge abzubrechen.

Über diese Aufgabe

Wenn Sie einen Backup-Vorgang abbrechen, stoppt der SnapCenter-Server den Vorgang und entfernt alle Snapshot-Kopien aus dem Storage, falls das erstellte Backup nicht beim SnapCenter Server registriert ist. Wenn das Backup bereits beim SnapCenter Server registriert ist, wird die bereits erstellte Snapshot-Kopie nicht wieder zurückgeführt, auch wenn der Vorgang ausgelöst wird.

- Sie können nur den Protokoll- oder Vollbackup-Vorgang abbrechen, der in die Warteschlange oder in Betrieb ist.
- Sie können den Vorgang nicht abbrechen, nachdem die Überprüfung gestartet wurde.

  Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Verifizierungsvorgang wird nicht durchgeführt.

- Sie können den Sicherungsvorgang nicht abbrechen, nachdem der Katalogvorgang gestartet wurde.
- Sie können einen Sicherungsvorgang entweder über die Seite Überwachen oder über den Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter GUI können Sie CLI-Befehle verwenden, um Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Vorgang aus und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Backup-Jobs auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Ergebnisse

Der Vorgang wird abgebrochen und die Ressource wird in den ursprünglichen Zustand zurückgesetzt.

Wenn der Vorgang, den Sie abgebrochen haben, im Status Abbrechen oder Ausführen nicht reagiert, sollten Sie Cancel-SmJob -JobID <int> -Force ausführen, um den Backup-Vorgang eindringlich zu beenden.

Sehen Sie sich Backups und Klone von Oracle Datenbanken auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

- Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapMirror Technologie auf dem sekundären Storage gespiegelt werden.
- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault Technologie auf dem sekundären Storage repliziert werden.

Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

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 entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone sowie die Gesamtanzahl der Backup-Protokolle angezeigt.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um die Wiederherstellung, den Clone, Mount, unmounten, umbenennen, Katalogisieren, Entkatalogisieren und Löschen von Vorgängen

   Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

   - Wenn Sie eine Protokollsicherung ausgewählt haben, können Sie nur umbenennen, mounten, unmounten, Katalog, Katalog aufheben, Katalog aufheben, Und -Lösch.
   - Wenn Sie das Backup mit dem Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Backups nicht umbenennen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie anschließend auf .

Wenn der für SnapmirrorStatusUpdateWaitTime zugewiesene Wert kleiner ist, werden die Backup-Kopien von Mirror und Vault nicht auf der Topologieseite aufgeführt, auch wenn Daten- und Protokoll-Volumes erfolgreich geschützt sind. Sie sollten den Wert erhöhen, der SnapmirrorStatusUpdateWaitTime mit dem Cmdlet *Set-SmConfigSettings* PowerShell zugewiesen wurde.

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden.

Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide" Oder "SnapCenter Software Cmdlet Referenzhandbuch".

Binden Sie Datenbank-Backups ein und heben Sie sie ab

Sie können einzelne oder mehrere Daten mounten und Backups protokollieren, wenn Sie auf die Dateien im Backup zugreifen möchten. Sie können das Backup entweder auf demselben Host, auf dem das Backup erstellt wurde, oder auf einem Remote-Host mit denselben Oracle- und Host-Konfigurationen mounten. Wenn Sie die Backups manuell gemountet haben, sollten Sie die Bereitstellung der Backups nach Abschluss des Vorgangs manuell aufheben. Bei jeder beliebigen Instanz kann ein Backup einer Datenbank auf einen beliebigen Host eingebunden werden. Während eines Vorgangs können Sie nur ein einzelnes Backup mounten.

In einem Flex ASM-Setup können Sie den Mount-Vorgang auf Leaf-Knoten nicht ausführen, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist.

Mounten Sie ein Datenbank-Backup

Sie sollten eine Datenbanksicherung manuell mounten, wenn Sie auf die Dateien im Backup zugreifen möchten.

Was Sie brauchen

- Wenn Sie in einer NFS-Umgebung über eine Instanz für Automatic Storage Management (ASM)-Datenbank verfügen und die ASM-Backups mounten möchten, sollten Sie den ASM-Festplattenpfad */var/opt/snapcenter/sco/Backup*/*/*/*/*/_*/* in den im parameter asm_diskstring festgelegten Pfad eingefügt haben.
- Wenn Sie über eine ASM-Datenbankinstanz in einer NFS-Umgebung verfügen und die ASM-Protokollsicherungen im Rahmen eines Wiederherstellungsvorgangs mounten möchten, sollten Sie den ASM-Festplattenpfad */var/opt/snapcenter/scu/Clones/*/** zu dem im parameter asm_diskstring definierten Pfad hinzugefügt haben.
- Im parameter asm_diskstring sollten Sie *AFD:** konfigurieren, wenn Sie ASMFD verwenden oder *ORCL:** konfigurieren, wenn Sie ASMLIB verwenden.

Informationen zum Bearbeiten des Parameters asm_diskstring finden Sie unter "So fügen Sie Datenträgerpfade zu asm_diskstring hinzu".

- Sie sollten die ASM-Anmeldedaten und den ASM-Port konfigurieren, wenn er sich von der des Quelldatenbank-Hosts während des Mounten des Backups unterscheidet.
- Wenn Sie ein Mount an einen alternativen Host mounten möchten, müssen Sie überprüfen, dass der alternative Host die folgenden Anforderungen erfüllt:
  - Dieselbe UID und dieselbe GID wie beim ursprünglichen Host
  - Dieselbe Oracle Version wie die des ursprünglichen Hosts
  - Betriebssystemverteilung und -Version wie beim ursprünglichen Host

- Sie sollten sicherstellen, dass die LUN nicht dem AIX-Host mit iGroup zugeordnet ist, die aus gemischten Protokollen iSCSI und FC besteht. Weitere Informationen finden Sie unter "Der Vorgang schlägt fehl, da der Fehler nicht in der Lage ist, das Gerät für die LUN zu ermitteln".

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf  .
6. Wählen Sie auf der Seite Mount Backups den Host aus, auf dem Sie das Backup mounten möchten, aus der Dropdown-Liste **Wählen Sie den Host aus, um die Backup**-Sicherung zu mounten.

   Der Mount-Pfad */var/opt/snapcenter/sco/Backup_Mount/Backup_Name/Database_Name* wird angezeigt.

   Wenn Sie das Backup einer ASM-Datenbank mounten, wird der Mount Path +diskgroupname_SID_Backup angezeigt.

7. Klicken Sie Auf **Mount**.

Nach Ihrer Beendigung

- Sie können den folgenden Befehl ausführen, um die Informationen bezüglich des gemounteten Backups abzurufen:

  ```
  ./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
  ```

- Wenn Sie eine ASM-Datenbank angehängt haben, können Sie den folgenden Befehl ausführen, um die Informationen zu dem gemounteten Backup abzurufen:

  ```
  ./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
  ```

- Führen Sie zum Abrufen der Backup-ID den folgenden Befehl aus:

  ```
  ./sccli Get-Smbackup-BackupNamebackup_name
  ```

  Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide".

Heben Sie die Bereitstellung eines Datenbank-Backups auf

Sie können die Bereitstellung einer gemounteten Datenbanksicherung manuell aufheben, wenn Sie nicht mehr

auf Dateien im Backup zugreifen möchten.

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.

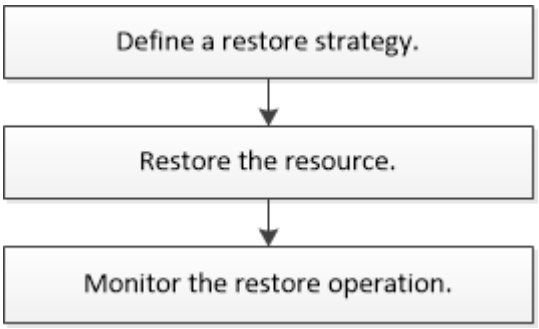
4. Wählen Sie das bereitgestellte Backup aus, und klicken Sie dann auf  .
5. Klicken Sie auf **OK**.

Stellen Sie Oracle Datenbanken wieder her

Wiederherstellung des Workflows

Der Restore-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Definition einer Restore- und Recovery-Strategie für Oracle Datenbanken

Sie müssen eine Strategie definieren, bevor Sie Ihre Datenbank wiederherstellen und wiederherstellen, damit Restore- und Recovery-Vorgänge erfolgreich durchgeführt werden können.

Arten von Backups, die für Wiederherstellungs- und Recovery-Vorgänge unterstützt werden

SnapCenter unterstützt die Wiederherstellung und Wiederherstellung unterschiedlicher Arten von Oracle Datenbank-Backups.

- Online Daten-Backup
- Offline Herunterfahren Datensicherung
- Datensicherung für Offline-Mounten

- Vollständiges Backup
- Offline-Mount-Backups von Data Guard Standby-Datenbanken
- Reine Online-Backups von Active Data Guard Standby-Datenbanken

> Sie können keine Wiederherstellung von Active Data Guard Standby-Datenbanken durchführen.

- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer RAC-Konfiguration (Real Application Clusters)
- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer ASM-Konfiguration (Automatic Storage Management)

Arten von Wiederherstellungsmethoden, die für Oracle-Datenbanken unterstützt werden

SnapCenter unterstützt Connect-and-Copy oder in-Place-Restore für Oracle Datenbanken. Während eines Wiederherstellungsvorgangs bestimmt SnapCenter die Wiederherstellungsmethode, die für die Wiederherstellung des Dateisystems ohne Datenverlust geeignet ist.

> SnapCenter bietet keine Unterstützung für Volume-basierte SnapRestore.

Wiederherstellung von Verbindungen und Kopien

Unterscheidet sich das Datenbanklayout von dem Backup, oder gibt es nach dem Backup neue Dateien, so wird die Wiederherstellung der Connect-and-Copy durchgeführt. In der Methode zum Wiederherstellen von Connect-and-Copy werden die folgenden Aufgaben ausgeführt:

Schritte

1. Das Volume ist aus der Snapshot Kopie geklont und der Filesystem-Stack basiert auf dem Host, der die geklonten LUNs oder Volumes verwendet.
2. Die Dateien werden von den geklonten Dateisystemen in die ursprünglichen Dateisysteme kopiert.
3. Die geklonten Filesysteme werden dann vom Host abgehängt und die geklonten Volumes werden aus den ONTAP gelöscht.

> Bei einem Flex ASM-Setup (bei dem die Kardinalität kleiner ist als die Anzahl Nodes im RAC-Cluster) oder ASM RAC-Datenbanken auf VMDK oder RDM wird nur die Connect-and-Copy-Wiederherstellungsmethode unterstützt.

Auch wenn Sie die Wiederherstellung vor Ort mit Nachdruck aktiviert haben, führt SnapCenter die Wiederherstellung von Connect und Copy in den folgenden Szenarien durch:

- Wiederherstellung aus einem sekundären Storage-System und bei Data ONTAP vor 8.3
- Wiederherstellen von ASM-Laufwerksgruppen auf Knoten eines Oracle RAC-Setups, auf denen die Datenbankinstanz nicht konfiguriert ist
- Wenn in Oracle RAC-Setup auf einem der Peer-Nodes nicht die ASM-Instanz oder die Cluster-Instanz ausgeführt wird oder wenn der Peer-Node nicht verfügbar ist
- Restore von Kontrolldateien
- Stellen Sie einen Teil der Tabellen aus, die sich in einer ASM-Festplattengruppe befinden, wieder her

- Die Laufwerksgruppe wird zwischen Datendateien, sp-Datei und Kennwortdatei freigegeben
- Der SnapCenter-Plug-in-Loader-Service (SPL) ist nicht auf dem Remote-Knoten in einer RAC-Umgebung installiert oder wird nicht ausgeführt
- Dem Oracle RAC werden neue Knoten hinzugefügt, und der SnapCenter-Server kennt die neu hinzugefügten Knoten nicht

In-Place-Wiederherstellung

Wenn das Datenbank-Layout dem Backup ähnelt und keine Konfigurationsänderungen am Storage- und Datenbank-Stack durchgeführt wurden, erfolgt die Wiederherstellung direkt, wobei die Wiederherstellung von Datei oder LUN auf ONTAP durchgeführt wird. SnapCenter unterstützt als Teil der in-Place-Wiederherstellungsmethode nur Single File SnapRestore (SFSR).

Data ONTAP 8.3 oder höher unterstützt in-Place-Restores vom sekundären Standort.

Wenn Sie die Datenbank wiederherstellen möchten, stellen Sie sicher, dass nur Datendateien auf der ASM-Festplattengruppe vorhanden sind. Sie müssen ein Backup erstellen, nachdem Änderungen an der ASM-Laufwerksgruppe oder in der physischen Struktur der Datenbank vorgenommen wurden. Nach der Durchführung der in-Place-Wiederherstellung enthält die Festplattengruppe die gleiche Anzahl von Datendateien wie zum Zeitpunkt des Backups.

Die in-Place-Wiederherstellung wird automatisch angewendet, wenn die Laufwerksgruppe oder der Mount-Punkt den folgenden Kriterien entspricht:

- Nach dem Backup werden keine neuen Datendateien hinzugefügt (Prüfung für fremde Dateien)
- Kein Zusatz, Löschen oder Freizeit von ASM-Festplatte oder LUN nach Backup (ASM-Festplattengruppenstrukturüberprüfung)
- Keine Ergänzung, Löschung oder Wiederherstellung von LUNs zu LVM Disk Group (LVM Disk Group Strukturänderprüfung)

Sie können auch die Wiederherstellung an Ort und Stelle mit GUI, SnapCenter CLI oder PowerShell Cmdlet aktivieren, um die Prüfung der ausländischen Datei und die Strukturänderprüfung der LVM-Laufwerksgruppe zu überschreiben.

Durchführung einer in-Place-Wiederherstellung auf ASM RAC

In SnapCenter wird der Knoten, auf dem Sie wiederherstellen, als primärer Knoten und alle anderen Knoten des RAC bezeichnet, auf dem sich die ASM-Festplattengruppe befindet, als Peer-Nodes. SnapCenter ändert den Status der ASM-Laufwerksgruppe auf alle Nodes, in denen sich die ASM-Laufwerksgruppe im Mount-Zustand befindet, bevor sie die Speicherwiederherstellung durchführt. Nachdem die Speicherwiederherstellung abgeschlossen ist, ändert SnapCenter den Status der ASM-Laufwerksgruppe wie vor der Wiederherstellung.

In SAN-Umgebungen entfernt SnapCenter Geräte aus allen Peer-Nodes und führt LUN-Aufheben der Zuordnung durch, bevor der Storage wiederhergestellt wird. Nach der Storage-Wiederherstellung führt die SnapCenter die LUN-Zuordnung durch und stellt Geräte auf allen Peer-Knoten wieder her. Wenn sich das Oracle RAC ASM-Layout in einer SAN-Umgebung auf LUNs befindet, führt die Wiederherstellung von SnapCenter LUN-Aufheben, LUN-Wiederherstellung und LUN-Map-Operationen auf allen Nodes des RAC-Clusters, in dem sich die ASM-Festplattengruppe befindet. Vor der Wiederherstellung auch dann, wenn alle Initiatoren der RAC-Nodes nicht für die LUNs verwendet wurden, erstellt nach dem Wiederherstellen von SnapCenter eine neue iGroup mit allen Initiatoren aller RAC-Nodes.

- Falls während der Vorratsspeicher-Aktivität auf Peer-Nodes ein Fehler auftritt, gibt SnapCenter den Status

der ASM-Laufwerksgruppe automatisch wieder, so wie es zuvor war, bevor die Wiederherstellung auf Peer-Nodes durchgeführt wurde, auf denen der Vorspeichervorgang erfolgreich war. Rollback wird für den primären und den Peer-Knoten, auf dem der Vorgang fehlgeschlagen ist, nicht unterstützt. Bevor Sie eine andere Wiederherstellung versuchen, müssen Sie das Problem auf dem Peer-Node manuell beheben und die ASM-Laufwerksgruppe auf dem primären Node wieder in den Mount-Status versetzen.

- Falls während der Wiederherstellungsaktivität ein Fehler auftritt, schlägt der Wiederherstellungsvorgang fehl und es wird kein Rollback durchgeführt. Bevor Sie eine weitere Wiederherstellung versuchen, müssen Sie das Problem mit der Speicherwiederherstellung manuell beheben und die ASM-Laufwerksgruppe auf dem primären Knoten wieder in den Bereitstellungsstatus versetzen.
- Falls während der Speicherung auf einem der Peer-Nodes ein Fehler auftritt, wird SnapCenter mit dem Wiederherstellungsvorgang auf den anderen Peer-Nodes fortgesetzt. Sie müssen das Problem nach der Wiederherstellung manuell auf dem Peer-Node beheben.

Arten von Wiederherstellungsvorgängen, die für Oracle-Datenbanken unterstützt werden

SnapCenter ermöglicht Ihnen die Durchführung verschiedener Arten von Restore-Vorgängen für Oracle Datenbanken.

Vor dem Wiederherstellen der Datenbank werden Backups validiert, um festzustellen, ob Dateien im Vergleich zu den tatsächlichen Datenbankdateien fehlen.

Vollständige Wiederherstellung

- Stellt nur die Datendateien wieder her
- Stellt nur die Kontrolldateien wieder her
- Stellt die Datendateien und Kontrolldateien wieder her
- Stellt Datendateien, Kontrolldateien und Wiederherstellungsprotokolle in Data Guard Standby und Active Data Guard Standby-Datenbanken wieder her

Teilwiederherstellung

- Stellt nur die ausgewählten Tabellen wieder her
- Stellt nur die ausgewählten pluggable Datenbanken (PDBs) wieder her
- Stellt nur die ausgewählten Tabellen einer PDB wieder her

Arten von für Oracle-Datenbanken unterstützten Recovery-Vorgängen

SnapCenter ermöglicht Ihnen die Durchführung verschiedener Arten von Recovery-Vorgängen für Oracle Datenbanken.

- Die Datenbank bis zur letzten Transaktion (alle Logs)
- Die Datenbank bis zu einer bestimmten Systemänderungsnummer (SCN)
- Die Datenbank auf einem bestimmten Datum und einer bestimmten Uhrzeit aktualisiert

  Sie müssen Datum und Uhrzeit für die Recovery auf der Grundlage der Zeitzone des Datenbankhosts angeben.

  SnapCenter bietet auch die Option „kein Recovery“ für Oracle Datenbanken.

Das Plug-in für Oracle-Datenbank unterstützt kein Recovery, wenn Sie mithilfe eines Backups wiederhergestellt haben, das mit der Datenbankrolle als Standby erstellt wurde. Sie müssen für physische Standby-Datenbanken immer ein manuelles Recovery durchführen.

Einschränkungen im Zusammenhang mit dem Restore und Recovery von Oracle Datenbanken

Bevor Sie Restore- und Recovery-Vorgänge durchführen, müssen Sie die Einschränkungen beachten.

Wenn Sie eine beliebige Oracle-Version von 11.2.0.4 bis 12.1 verwenden, 0.1 befindet sich der Wiederherstellungsvorgang im Status „Hung“, wenn Sie den Befehl „*renamedg*“ ausführen. Sie können den Oracle Patch 19544733 anwenden, um dieses Problem zu beheben.

Die folgenden Wiederherstellungs- und Recovery-Vorgänge werden nicht unterstützt:

- Restore und Recovery von Tabellen der Root-Container-Datenbank (CDB)
- Wiederherstellung temporärer Tabellen und temporärer Tablespaces im Zusammenhang mit PDBs
- Wiederherstellung und Wiederherstellung von Tabellen aus mehreren PDBs gleichzeitig
- Wiederherstellung von Log-Backups
- Wiederherstellung von Backups an einem anderen Speicherort
- Wiederherstellung von Wiederherstellungsprotokolldateien in einer anderen Konfiguration als Data Guard Standby oder Active Data Guard Standby-Datenbanken
- SPFILE und Password wiederherstellen
- Wenn Sie einen Wiederherstellungsvorgang für eine Datenbank durchführen, die mit dem bestehenden Datenbanknamen auf demselben Host neu erstellt wurde, von SnapCenter verwaltet wurde und über gültige Backups verfügte, überschreibt der Wiederherstellungsvorgang die neu erstellten Datenbankdateien, obwohl die DBIDs unterschiedlich sind.

  Dies kann durch die Durchführung einer der folgenden Maßnahmen vermieden werden:

  - Ermitteln Sie die SnapCenter Ressourcen, nachdem die Datenbank neu erstellt wurde
  - Erstellen Sie ein Backup der neu erstellten Datenbank

Einschränkungen im Zusammenhang mit der zeitpunktgenauen Recovery von Tablespaces

- Point-in-Time Recovery (PITR) von SYSTEM, SYSAUX und UNDO Tablespaces wird nicht unterstützt
- PITR der Tabellen können nicht zusammen mit anderen Arten von Restores ausgeführt werden
- Wenn ein Tablespace umbenannt wird und Sie ihn bis zu einem Punkt wiederherstellen möchten, bevor er umbenannt wurde, müssen Sie den früheren Namen des Tablespaces angeben
- Wenn die Tabellenbedingungen in einem Tablespace in einem anderen Tablespace enthalten sind, sollten Sie beide Tabellen wiederherstellen
- Wenn eine Tabelle und ihre Indizes in verschiedenen Tabellen gespeichert werden, sollten die Indizes vor der Durchführung von PITR gelöscht werden
- PITR kann nicht verwendet werden, um den aktuellen Standardtablespaces wiederherzustellen
- PITR kann nicht verwendet werden, um Tabellen mit einem der folgenden Objekte wiederherzustellen:
  - Objekte mit zugrunde liegenden Objekten (z. B. materialisierte Ansichten) oder enthaltenen Objekten (z. B. partitionierte Tabellen), sofern sich nicht alle zugrunde liegenden oder enthaltenen Objekte im Wiederherstellungssatz befinden

Wenn außerdem die Partitionen einer partitionierten Tabelle in verschiedenen Tabellen gespeichert werden, sollten Sie die Tabelle entweder vor der Durchführung von PITR ablegen oder alle Partitionen in denselben Tablespace verschieben, bevor Sie PITR ausführen.

- Segmente rückgängig machen oder zurücksetzen
- Oracle 8 kompatible erweiterte Warteschlangen mit mehreren Empfängern
- Objekte, die dem SYS-Benutzer gehören

  Beispiele für diese Objekttypen sind PL/SQL, Java-Klassen, Ausrufprogramme, Ansichten, Synonyme, Benutzer, Berechtigungen, Abmessungen, Verzeichnisse und Sequenzen.

Quellen und Ziele für die Wiederherstellung von Oracle-Datenbanken

Sie können eine Oracle Datenbank aus einer Backup-Kopie auf dem Primär- oder Sekundärspeicher wiederherstellen. Sie können Datenbanken nur an demselben Speicherort auf derselben Datenbankinstanz wiederherstellen. Im Real Application Cluster (RAC) Setup können Sie jedoch Datenbanken auf anderen Knoten wiederherstellen.

Quellen für Wiederherstellungsvorgänge

Sie können Datenbanken aus einem Backup auf dem primären oder sekundären Storage wiederherstellen. Wenn Sie in einer Konfiguration mit mehreren Spiegelungen ein Backup auf dem sekundären Storage wiederherstellen möchten, können Sie die sekundäre Storage-Spiegelung als Quelle auswählen.

Ziele für Wiederherstellungen

Sie können Datenbanken nur an demselben Speicherort auf derselben Datenbankinstanz wiederherstellen.

In einem RAC Setup können Sie RAC-Datenbanken von jedem Knoten im Cluster wiederherstellen.

Anforderungen für die Wiederherstellung einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank wiederherstellen, sollten Sie sicherstellen, dass die Voraussetzungen abgeschlossen sind.

- Sie sollten Ihre Restore- und Recovery-Strategie definiert haben.
- Der SnapCenter Administrator sollte Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch die Ziel-Volumes zugewiesen haben, wenn Sie Snapshot Kopien zu einer Spiegelung oder einem Vault replizieren.
- Wenn Archivprotokolle im Rahmen der Datensicherung beschnitten werden, sollten Sie die erforderlichen Archiv-Log-Backups manuell gemountet haben.
- Wenn Sie Oracle Datenbanken wiederherstellen möchten, die sich auf einer Virtual Machine Disk (VMDK) befinden, sollten Sie sicherstellen, dass der Gastrechner die erforderliche Anzahl an freien Steckplätzen für die Zuweisung der geklonten VMDKs bietet.
- Sie sollten sicherstellen, dass alle Daten-Volumes und Archivprotokollvolumes der Datenbank geschützt sind, wenn für diese Datenbank ein sekundärer Schutz aktiviert ist.
- Sie sollten sicherstellen, dass sich die RAC One Node-Datenbank im Status „Nomount“ befindet, um die Steuerdatei oder die vollständige Datenbankwiederherstellung durchzuführen.
- Wenn Sie eine ASM-Datenbankinstanz in einer NFS-Umgebung haben, sollten Sie den ASM-Festplattenpfad */var/opt/snapcenter/scu/Clones/*/** in den im parameter asm_diskstring festgelegten Pfad

hinzufügen, um die ASM-Protokoll-Backups erfolgreich im Rahmen des Wiederherstellungsvorgangs zu mounten.

- Im parameter asm_diskstring sollten Sie *AFD:** konfigurieren, wenn Sie ASMFD verwenden oder *ORCL:** konfigurieren, wenn Sie ASMLIB verwenden.

  Informationen zum Bearbeiten des Parameters asm_diskstring finden Sie unter "So fügen Sie Datenträgerpfade zu asm_diskstring hinzu"

- Sie sollten den statischen Listener in der Datei **Listener.ora** konfigurieren, die bei _ € ORACLE_HOME/Network/admin_ für nicht-ASM-Datenbanken verfügbar ist, und _ € GRID_HOME/Network/admin_ für ASM-Datenbanken, wenn Sie die Betriebssystemauthentifizierung deaktiviert und die Oracle-Datenbankauthentifizierung für eine Oracle-Datenbank aktiviert haben, und die Datendateien und Kontrolldateien dieser Datenbank wiederherstellen möchten.
- Sie sollten den Wert des SCORestoreTimeout-Parameters erhöhen, indem Sie den Befehl Set-SmConfigSettings ausführen, wenn sich die Datenbankgröße in Terabyte (TB) befindet.
- Sie sollten sicherstellen, dass alle für vCenter erforderlichen Lizenzen installiert sind und auf dem neuesten Stand sind.

  Wenn die Lizenzen nicht installiert oder auf dem neuesten Stand sind, wird eine Warnmeldung angezeigt. Wenn Sie die Warnung ignorieren und fortfahren, schlägt die Wiederherstellung aus RDM fehl.

- Sie sollten sicherstellen, dass die LUN nicht dem AIX-Host mit iGroup zugeordnet ist, die aus gemischten Protokollen iSCSI und FC besteht. Weitere Informationen finden Sie unter "Der Vorgang schlägt fehl, da der Fehler nicht in der Lage ist, das Gerät für die LUN zu ermitteln".

Oracle Datenbank wiederherstellen

Bei einem Datenverlust können Sie mit SnapCenter Daten von einem oder mehreren Backups auf Ihrem aktiven Dateisystem wiederherstellen und dann die Datenbank wiederherstellen.

Über diese Aufgabe

Die Recovery wird anhand der Archivprotokolle durchgeführt, die am konfigurierten Speicherort für das Archivprotokoll verfügbar sind. Wenn die für die Recovery erforderlichen Archivprotokolle nicht am konfigurierten Speicherort verfügbar sind, sollten Sie die Snapshot Kopie mit den Protokollen mounten und den Pfad als externe Archivprotokolle angeben.

Wenn Sie ASM-Datenbank von ASMLIB zu ASMFD migrieren, können die mit ASMLIB erstellten Backups nicht zur Wiederherstellung der Datenbank verwendet werden. Sie sollten Backups in der ASMFD-Konfiguration erstellen und diese Backups für die Wiederherstellung verwenden. Wenn die ASM-Datenbank von ASMFD zu ASMLIB migriert wird, sollten Sie zur Wiederherstellung auch Backups in der ASMLIB-Konfiguration erstellen.

Wenn Sie eine Datenbank wiederherstellen, wird eine operative Sperrdatei (.SM_Lock_dbsid) auf dem Oracle-Datenbank-Host im Verzeichnis Dollar ORACLE_HOME/dbs erstellt, um zu vermeiden, dass mehrere Operationen auf der Datenbank ausgeführt werden. Nach dem Wiederherstellen der Datenbank wird die operative Sperrdatei automatisch entfernt.

Die Wiederherstellung der SPFILE- und Password-Datei wird nicht unterstützt.

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.
4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:

   a. Wenn Sie in einer RAC-Umgebung (Real Application Clusters) eine Sicherung einer Datenbank ausgewählt haben, wählen Sie den RAC-Knoten aus.

   b. Wenn Sie eine gespiegelte oder Vault-Daten auswählen:

      - Wenn keine Protokollsicherung bei Spiegel oder Tresor vorhanden ist, wird nichts ausgewählt und die Lokatoren leer sind.
      - Wenn Protokollsicherungen in Mirror oder Vault vorhanden sind, wird die neueste Protokollsicherung ausgewählt und der entsprechende Locator angezeigt.

      Wenn die ausgewählte Protokollsicherung sowohl im Spiegelungs- als auch im Tresorverzeichnis vorhanden ist, werden beide Lokatoren angezeigt.

   c. Führen Sie folgende Aktionen durch:

Sie möchten wiederherstellen…	**Tun Sie das…**
Alle Datendateien der Datenbank	Wählen Sie **Alle Datendateien**. Nur die Datendateien der Datenbank werden wiederhergestellt. Die Kontrolldateien, Archivprotokolle oder Wiederherstellungsprotokolle werden nicht wiederhergestellt.
Tablespaces	Wählen Sie **Tablespaces**. Sie können die Tabellen angeben, die Sie wiederherstellen möchten.

Sie möchten wiederherstellen…	Tun Sie das…
Kontrolldateien	Wählen Sie **Kontrolldateien** aus. Stellen Sie beim Wiederherstellen von Kontrolldateien sicher, dass die Verzeichnisstruktur entweder vorhanden ist oder mit dem korrekten Benutzer- und Gruppeneigentum erstellt werden soll, falls vorhanden, damit die Dateien durch den Wiederherstellungsvorgang an den Zielspeicherort kopiert werden können. Wenn das Verzeichnis nicht vorhanden ist, schlägt der Wiederherstellungsauftrag fehl.
Wiederholen Sie die Protokolldateien	Wählen Sie **Redo-Log-Dateien** aus. Diese Option ist nur für Data Guard Standby- oder Active Data Guard-Standby-Datenbanken verfügbar. Redo-Log-Dateien werden nicht für Datenbanken gesichert, die nicht von Data Guard stammen. Für Datenbanken, die nicht von Data Guard stammen, wird die Recovery mit Archivprotokollen durchgeführt.
Steckbare Datenbanken (PDBs)	Wählen Sie **Pluggable Databases** aus, und geben Sie dann die PDBs an, die Sie wiederherstellen möchten.
Steckbare Datenbank-Tabellen (PDB)	Wählen Sie **Pluggable Database (PDB) Tablespaces** aus, und geben Sie dann die PDB und die Tablespaces dieser PDB an, die Sie wiederherstellen möchten. Diese Option ist nur verfügbar, wenn Sie eine PDB für die Wiederherstellung ausgewählt haben.

d. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.

   Die verschiedenen Status einer Datenbank von höher bis niedriger sind offen, montiert, gestartet und heruntergefahren. Sie müssen dieses Kontrollkästchen aktivieren, wenn sich die Datenbank in einem höheren Zustand befindet, der Status jedoch in einen niedrigeren Zustand geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen. Wenn sich die Datenbank in einem niedrigeren

Zustand befindet, aber der Status in einen höheren Zustand geändert werden muss, um den Wiederherstellungsvorgang auszuführen, wird der Datenbankstatus automatisch geändert, auch wenn Sie das Kontrollkästchen nicht aktivieren.

Wenn sich eine Datenbank im Status „offen“ befindet und die Datenbank für die Wiederherstellung im Status „angehängt“ befinden muss, wird der Datenbankzustand nur geändert, wenn Sie dieses Kontrollkästchen aktivieren.

a. Wählen Sie **erzwingen in place Restore** aus, wenn Sie in den Szenarien, in denen neue Datendateien nach dem Backup hinzugefügt werden, oder wenn LUNs zu einer LVM-Laufwerksgruppe hinzugefügt, gelöscht oder neu erstellt werden sollen, in-place-Wiederherstellung durchführen möchten.

7. Führen Sie auf der Seite „Recovery Scope“ die folgenden Schritte aus:

Sie suchen…	**Tun Sie das…**
Möchten Sie die letzte Transaktion wiederherstellen	Wählen Sie **Alle Protokolle**.
Wiederherstellen einer bestimmten Systemänderungsnummer (SCN)	Wählen Sie **bis SCN (Systemänderungsnummer)**.
Möchten Sie Daten zu einer bestimmten Zeit wiederherstellen	Wählen Sie **Datum und Uhrzeit**. Sie müssen Datum und Uhrzeit der Zeitzone des Datenbank-Hosts angeben.
Möchten Sie nicht wiederherstellen	Wählen Sie **Keine Wiederherstellung**.
Soll beliebige externe Archiv-Log-Speicherorte angeben	Wählen Sie **Externe Archiv-Log-Speicherorte angeben** und geben Sie dann den Speicherort der externen Archiv-Log-Dateien an. Wenn Archivprotokolle im Rahmen der Sicherung beschnitten werden und Sie die erforderlichen Archiv-Log-Backups manuell gemountet haben, müssen Sie den gemounteten Backup-Pfad als externen Archiv-Log-Speicherort für die Wiederherstellung angeben. • "Oracle Datensicherung mit ONTAP" • "Der Vorgang schlägt mit ORA-00308-Fehler fehl"

Eine Wiederherstellung mit einer Recovery von sekundären Backups ist nicht möglich, wenn Archiv-Protokoll-Volumes nicht geschützt sind, aber Daten-Volumes gesichert sind. Sie können nur wiederherstellen, indem Sie **Keine Wiederherstellung**.

Wenn Sie eine RAC-Datenbank wiederherstellen, bei der die Option Open Database ausgewählt ist, wird nur die RAC-Instanz, in der der Wiederherstellungsvorgang initiiert wurde, wieder in den Status Open zurückgebracht.

Die Recovery wird nicht für Data Guard Standby- und Active Data Guard-Standby-Datenbanken unterstützt.

8. Geben Sie auf der Seite PreOps den Pfad und die Argumente des Vorschrifts ein, das Sie vor der Wiederherstellung ausführen möchten.

   Sie müssen die Voreinstellungen entweder im Pfad */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

   Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.

9. Führen Sie auf der Seite PostOps die folgenden Schritte aus:

   a. Geben Sie den Pfad und die Argumente des Postscript ein, das Sie nach der Wiederherstellung ausführen möchten.

      Sie müssen die Postskripte entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

   b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

      Nach dem Wiederherstellen einer Container-Datenbank (CDB) mit oder ohne Kontrolldateien oder nach dem Wiederherstellen nur CDB-Kontrolldateien, wenn Sie angeben, die Datenbank nach der Wiederherstellung zu öffnen, dann wird nur die CDB geöffnet und nicht die steckbaren Datenbanken (PDB) in dieser CDB.

      In einem RAC-Setup wird nach der Wiederherstellung nur die RAC-Instanz geöffnet, die für die Wiederherstellung verwendet wird.

      Nach dem Wiederherstellen eines Benutzertablespaces mit Steuerdateien, eines Systemtablespaces mit oder ohne Steuerdateien oder einer PDB mit oder ohne Steuerdateien wird nur der Status der PDB, die mit dem Wiederherstellungsvorgang in Verbindung steht, in den ursprünglichen Zustand geändert. Der Zustand der anderen PDBs, die nicht für die Wiederherstellung verwendet wurden, wird nicht in den ursprünglichen Zustand geändert, weil der Zustand dieser PDBs nicht gespeichert wurden. Sie müssen manuell den Status der PDBs ändern, die nicht für die Wiederherstellung verwendet wurden.

10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.

    Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den ausgeführten Wiederherstellungsvorgang anhängen möchten, müssen Sie **Job-Bericht anhängen** auswählen.

    Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Für weitere Informationen

- "Oracle RAC One-Knoten-Datenbank wird zur Durchführung von SnapCenter-Operationen übersprungen"
- "Fehler beim Wiederherstellen von einem sekundären SnapMirror- oder SnapVault-Standort"
- "Wiederherstellung aus einem Backup einer verwaisten Inkarnation fehlgeschlagen"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Wiederherstellen von Tabellen mit Point-in-Time Recovery

Sie können einen bestimmten Satz von Tablespaces wiederherstellen, die beschädigt oder verworfen wurden, ohne dass die anderen Tabellen der Datenbank beeinträchtigt werden. SnapCenter verwendet RMAN für die Durchführung des Point-in-Time Recovery (PITR) der Tabellen.

Was Sie brauchen

Die Backups, die zur Durchführung von PITR von Tabellen erforderlich sind, sollten katalogisiert und gemountet werden.

Über diese Aufgabe

Während des PITR-Betriebs erstellt RMAN eine Zusatzinstanz am angegebenen Hilfsziel. Das Hilfeziel kann ein Bereitstellungspunkt oder eine ASM-Laufwerksgruppe sein. Wenn genügend Speicherplatz am Einbauort vorhanden ist, können Sie eine der montierten Positionen anstelle eines dedizierten Mount-Punkts wiederverwenden.

Geben Sie Datum und Uhrzeit oder SCN an, und der Tablespace wird in der Quelldatenbank wiederhergestellt.

Sie können mehrere Tabellen mit ASM, NFS und SAN-Umgebungen auswählen und wiederherstellen. Wenn sich beispielsweise Tablespaces TS2 und TS3 auf NFS und TS4 im SAN befinden, können Sie alle Tabellen wiederherstellen.

In einem RAC-Setup können Sie PITR von Tablespaces von jedem Knoten des RAC ausführen.

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank des Typs Single Instance (mandantenfähig) aus der Detailansicht der Datenbank oder in der Detailansicht der Ressourcengruppen aus.

   Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.

   Wenn die Sicherung nicht katalogisiert ist, sollten Sie die Sicherung auswählen und auf **Katalog** klicken.

5. Wählen Sie die katalogisierte Sicherung aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wenn Sie in einer RAC-Umgebung (Real Application Clusters) eine Sicherung einer Datenbank ausgewählt haben, wählen Sie den RAC-Knoten aus.
   b. Wählen Sie **Tablespaces** aus, und legen Sie dann die Tablespaces fest, die Sie wiederherstellen möchten.

      PITR kann auf SYSAUX, SYSTEM und TABLESPACES nicht ausgeführt werden.

   c. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.
7. Führen Sie auf der Seite „Wiederherstellungsumfang“ eine der folgenden Aktionen durch:
   - Wenn Sie eine bestimmte Systemänderungsnummer (SCN) wiederherstellen möchten, wählen Sie **bis SCN** und geben Sie das SCN und das Hilfeziel an.
   - Wenn Sie ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten, wählen Sie **Datum und Uhrzeit** und geben Sie Datum und Uhrzeit sowie das Hilfsziel an. Wenn Sie SCN oder Datum und Uhrzeit angeben, listet SnapCenter die Backups auf, die für die Durchführung von PITR erforderlich sind, aber nicht katalogisiert und gemountet sind.
8. Geben Sie auf der Seite PreOps den Pfad und die Argumente des Vorschrifts ein, das Sie vor der Wiederherstellung ausführen möchten.

   Sie sollten die Voreinstellungen entweder im Pfad /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig wird der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

   Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.
9. Führen Sie auf der Seite PostOps die folgenden Schritte aus:
   a. Geben Sie den Pfad und die Argumente des Postscript ein, das Sie nach der Wiederherstellung ausführen möchten.
   b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.
10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Wiederherstellen steckbarer Datenbanken über zeitpunktgenaues Recovery

Sie können eine steckbare Datenbank (PDB) wiederherstellen, die beschädigt oder verworfen wurde, ohne die andere DBs in der Container-Datenbank (CDB) zu belasten. SnapCenter nutzt RMAN für die Durchführung von Point-in-Time Recoverys (PITR) der PDB.

Was Sie brauchen

Die Backups, die für die PITR einer PDB benötigt werden, sollten katalogisiert und gemountet werden.

In einem RAC-Setup sollten Sie die PDB manuell schließen (ändern des Status in „MOUNT“) auf allen Knoten des RAC-Setups.

Über diese Aufgabe

Während des PITR-Betriebs erstellt RMAN eine Zusatzinstanz am angegebenen Hilfsziel. Das Hilfeziel kann ein Bereitstellungspunkt oder eine ASM-Laufwerksgruppe sein. Wenn genügend Speicherplatz am Einbauort vorhanden ist, können Sie eine der montierten Positionen anstelle eines dedizierten Mount-Punkts wiederverwenden.

Sie sollten das Datum und die Uhrzeit oder das SCN angeben, um PITR der PDB durchzuführen. RMAN kann LESE-, SCHREIBSCHUTZ- ODER abfallende PDBs einschließlich Datendateien wiederherstellen.

Sie können nur Folgendes wiederherstellen:

- Jeweils eine PDB
- Ein Tablespace in einer PDB
- Mehrere Tabellen derselben PDB

In einem RAC-Setup können Sie PITR von Tablespaces von jedem Knoten des RAC ausführen.

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank des Typs Single Instance (mandantenfähig) aus der Detailansicht der Datenbank oder in der Detailansicht der Ressourcengruppen aus.

   Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.

   Wenn die Sicherung nicht katalogisiert ist, sollten Sie die Sicherung auswählen und auf **Katalog** klicken.

5. Wählen Sie die katalogisierte Sicherung aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wenn Sie in einer RAC-Umgebung (Real Application Clusters) eine Sicherung einer Datenbank ausgewählt haben, wählen Sie den RAC-Knoten aus.
   b. Je nachdem, ob Sie die PDB oder Tablespaces in einer PDB wiederherstellen möchten, führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Schritte…

PDB wiederherstellen	i. Wählen Sie **Pluggable Databases (PDBs)** aus. ii. Geben Sie die PDB an, die wiederhergestellt werden soll. Sie können PITR nicht in der PDB-Datenbank mit Wert für „PITR“ ausführen.
Tablespaces in einer PDB wiederherstellen	i. Wählen Sie die Tabellen * Pluggable Database (PDB)* aus. ii. Geben Sie die PDB an. iii. Geben Sie entweder einen einzelnen Tablespace oder mehrere Tablespaces an, die Sie wiederherstellen möchten. PITR kann auf SYSAUX, SYSTEM und TABLESPACES nicht ausgeführt werden.

c. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.

7. Führen Sie auf der Seite „Wiederherstellungsumfang“ eine der folgenden Aktionen durch:
   - Wenn Sie eine bestimmte Systemänderungsnummer (SCN) wiederherstellen möchten, wählen Sie **bis SCN** und geben Sie das SCN und das Hilfeziel an.
   - Wenn Sie ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten, wählen Sie **Datum und Uhrzeit** und geben Sie Datum und Uhrzeit sowie das Hilfsziel an. Wenn Sie SCN oder Datum und Uhrzeit angeben, listet SnapCenter die Backups auf, die für die Durchführung von PITR erforderlich sind, aber nicht katalogisiert und gemountet sind.
8. Geben Sie auf der Seite PreOps den Pfad und die Argumente des Vorschrifts ein, das Sie vor der Wiederherstellung ausführen möchten.

   Sie sollten die Voreinstellungen entweder im Pfad /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig wird der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

   Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.
9. Führen Sie auf der Seite PostOps die folgenden Schritte aus:
   a. Geben Sie den Pfad und die Argumente des Postscript ein, das Sie nach der Wiederherstellung ausführen möchten.
   b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

      In einem RAC-Setup wird die PDB nur auf dem Knoten geöffnet, auf dem die Datenbank

wiederhergestellt wurde. Sie sollten die wiederhergestellte PDB manuell auf allen anderen Knoten des RAC-Setups öffnen.

10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Stellen Sie Oracle Datenbanken mithilfe von UNIX-Befehlen wieder her

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore- und Recovery-Vorgängen und Monitoring der betrieblichen Vorgänge.

Über diese Aufgabe

Sie sollten die folgenden Befehle ausführen, um die Verbindung zum SnapCenter-Server herzustellen, die Backups aufzulisten, seine Informationen abzurufen und die Sicherung wiederherzustellen.

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide".

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer: *Open-SmConnection*
2. Rufen Sie die Informationen über die Backups ab, die Sie wiederherstellen möchten: *Get-SmBackup*
3. Rufen Sie die detaillierten Informationen zum angegebenen Backup ab: *Get-SmBackupDetails*

   Dieser Befehl ruft die detaillierten Informationen zum Backup einer bestimmten Ressource mit einer bestimmten Backup-ID ab. Die Informationen umfassen Datenbanknamen, Version, Home, SCN starten und beenden, Tabellen, steckbare Datenbanken und deren Tabellen.

4. Stellen Sie Daten aus dem Backup wieder her: *Restore-SmBackup*

Überwachen Sie die Restore-Vorgänge für Oracle Datenbanken

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen

- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie Auf So filtern Sie die Liste, damit nur Wiederherstellungsvorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Jobdetails** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Nach der Volume-basierten Wiederherstellung werden die Backup-Metadaten aus dem SnapCenter-Repository gelöscht, die Backup-Katalogeinträge bleiben aber im SAP HANA-Katalog. Der Status des Wiederherstellungsjobs wird angezeigt , Sie sollten auf Jobdetails klicken, um das Warnzeichen einiger der untergeordneten Aufgaben anzuzeigen. Klicken Sie auf das Warnschild und löschen Sie die angezeigten Backup-Katalog-Einträge.

Wiederherstellungsvorgänge für Oracle-Datenbank abbrechen

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite Überwachen oder über den Aktivitätsbereich abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite

Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Oracle Datenbank klonen

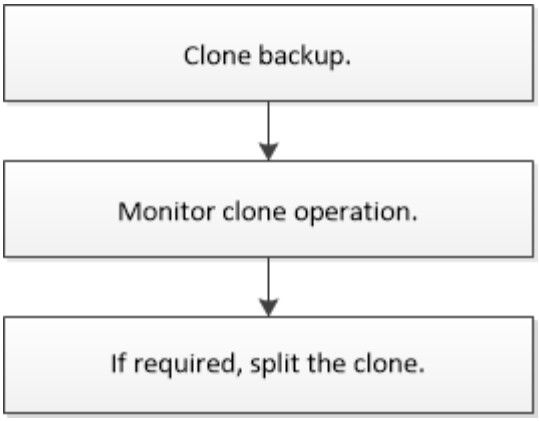
Klon-Workflow

Der Klon-Workflow umfasst die Planung, die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Sie können Datenbanken aus den folgenden Gründen klonen:

- Funktionen zu testen, die während der Applikationsentwicklungszyklen mit der aktuellen Datenbankstruktur und Inhalten implementiert werden müssen.
- Um Data Warehouses mit Tools zur Datenextraktion und -Bearbeitung zu befüllen.
- Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden.

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Klonstrategie für Oracle Datenbanken definieren

Eine Strategie vor dem Klonen Ihrer Datenbank definieren, um sicherzustellen, dass der Klonvorgang erfolgreich ist.

Arten von Backups, die zum Klonen unterstützt werden

SnapCenter unterstützt das Klonen verschiedener Backup-Typen von Oracle Datenbanken.

- Online Daten-Backup
- Online-Vollbackup
- Backup für Offline-Mounten
- Offline-Herunterfahren-Backup
- Backups von Data Guard Standby-Datenbanken und Active Data Guard Standby-Datenbanken
- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer RAC-Konfiguration (Real Application Clusters)
- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer ASM-Konfiguration (Automatic Storage Management)

Oracle ASM-Konfiguration wird nicht unterstützt, wenn die Option User_friendly_Names in der Multipath-Konfigurationsdatei auf „yes“ gesetzt ist und Aliase oder symbolische Links für die Oracle-ASM-Laufwerke mit der udev-Regeldatei definiert werden.

Das Klonen von Backups für Archivprotokolle wird nicht unterstützt.

Arten von unterstützten Klonen für Oracle-Datenbanken

In einer Oracle Datenbankumgebung unterstützt SnapCenter das Klonen eines Datenbank-Backups. Sie können das Backup aus primären und sekundären Storage-Systemen klonen.

Der SnapCenter Server klont mit NetApp FlexClone Technologie Backups.

Sie können einen Klon aktualisieren, indem Sie den Befehl „Refresh-SmClone“ ausführen. Mit diesem Befehl wird ein Backup der Datenbank erstellt, der vorhandene Klon gelöscht und ein Klon mit demselben Namen erstellt.

Die Klonaktualisierung kann nur mit den UNIX Befehlen ausgeführt werden.

Namenskonventionen für Klone für Oracle Datenbanken

Von SnapCenter 3.0 unterscheidet sich die Namenskonvention für Klone von Dateisystemen von den Klonen von ASM-Festplattengruppen.

- Die Namenskonvention für SAN oder NFS-File-Systeme ist FileSystemNamesourceDatabase_CLONESID.
- Die Namenskonvention für ASM-Festplattengruppen ist SC_HASHCODEofDISKGROUP_CLONESID.

  HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Laufwerksgruppe eindeutig ist.

Einschränkungen beim Klonen von Oracle Datenbanken

Die Einschränkungen von Klonvorgängen sollten Sie beachten, bevor Sie die Datenbanken klonen.

- Wenn Sie eine Oracle-Version von 11.2.0.4 bis 12.1.0.1 verwenden, befindet sich der Klonvorgang im Status „Hung“, wenn Sie den Befehl „*renamedg*“ ausführen. Sie können den Oracle Patch 19544733 anwenden, um dieses Problem zu beheben.
- Das Klonen von Datenbanken aus einem LUN, die direkt an einen Host angebunden ist (z. B. durch die Verwendung von Microsoft iSCSI Initiator auf einem Windows Host), wird auf demselben Windows Host oder einem anderen Windows Host oder umgekehrt nicht unterstützt.
- Das Stammverzeichnis des Volume-Bereitstellungspunkts kann kein freigegebenes Verzeichnis sein.
- Wenn Sie eine LUN verschieben, die einen Klon in ein neues Volume enthält, kann der Klon nicht gelöscht werden.

Anforderungen für das Klonen einer Oracle Datenbank

Bevor Sie eine Oracle-Datenbank klonen, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie sollten eine Sicherung der Datenbank mit SnapCenter erstellt haben.

  Sie sollten erfolgreich Online-Daten erstellen und Backups oder Offline-Backups (Mounten oder Herunterfahren) protokollieren, damit der Klonvorgang erfolgreich abgeschlossen wurde.

- Wenn Sie die Steuerdatei oder die Pfade für die Wiederherstellungsprotokolle anpassen möchten, sollten Sie die erforderliche Dateisystemgruppe oder die automatische Speicherverwaltung (ASM) vorbereitgestellt haben.

  Standardmäßig werden Wiederherstellungsprotokolle und Kontrolldateien der geklonten Datenbank auf der ASM-Festplattengruppe oder auf dem von SnapCenter bereitgestellten Dateisystem für die Datendateien der Klondatenbank erstellt.

- Wenn Sie ASM über NFS verwenden, sollten Sie */var/opt/snapcenter/scu/Clones/*/** zum vorhandenen Pfad hinzufügen, der im Parameter asm_diskstring definiert ist.
- Im parameter asm_diskstring sollten Sie *AFD:** konfigurieren, wenn Sie ASMFD verwenden oder *ORCL:** konfigurieren, wenn Sie ASMLIB verwenden.

  Informationen zum Bearbeiten des Parameters asm_diskstring finden Sie unter "So fügen Sie

Datenträgerpfade zu asm_diskstring hinzu".

- Wenn Sie den Klon auf einem alternativen Host erstellen, sollte der alternative Host folgende Anforderungen erfüllen:
  - Das SnapCenter Plug-in für Oracle Database sollte auf dem alternativen Host installiert sein.
  - Der Klon-Host sollte LUNs vom primären oder sekundären Storage erkennen können.
    - Wenn Sie vom primären Storage oder sekundären Storage (Vault oder Mirror) in einem alternativen Host klonen, stellen Sie sicher, dass eine iSCSI-Sitzung zwischen dem sekundären Storage und dem alternativen Host aufgebaut ist oder richtig für FC abgegrenzt wird.
    - Wenn Sie von Vault oder Mirror Storage auf demselben Host klonen, stellen Sie sicher, dass eine iSCSI-Sitzung zwischen dem Vault- oder Mirror-Storage und dem Host eingerichtet oder richtig für FC abgegrenzt wird.
    - Wenn Sie in einer virtualisierten Umgebung klonen, stellen Sie sicher, dass entweder eine iSCSI-Sitzung zwischen dem primären oder sekundären Storage und dem ESX-Server, der den alternativen Host hostet, eingerichtet oder ordnungsgemäß für FC.
      Weitere Informationen finden Sie unter "Dokumentation zu Host Utilities".
  - Wenn die Quelldatenbank eine ASM-Datenbank ist:
    - Die ASM-Instanz sollte auf dem Host ausgeführt werden, auf dem der Klon ausgeführt wird.
    - Die ASM-Laufwerksgruppe sollte vor dem Klonvorgang bereitgestellt werden, wenn Sie Archivprotokolldateien der geklonten Datenbank in eine dedizierte ASM-Laufwerksgruppe platzieren möchten.
    - Der Name der Datendisk-Gruppe kann konfiguriert werden, aber stellen Sie sicher, dass der Name nicht von einer anderen ASM-Laufwerksgruppe auf dem Host verwendet wird, auf dem der Klon ausgeführt wird.

      Datendateien auf der ASM-Festplattengruppe werden als Teil des SnapCenter-Klon-Workflows bereitgestellt.
- Der Schutztyp für die Daten-LUN und die Protokoll-LUN, wie Spiegel, Vault oder Mirror-Vault, sollte der gleiche sein, um beim Klonen zu einem alternativen Host mithilfe von Protokoll-Backups sekundäre Lokatoren zu erkennen.
- Sie sollten den Wert exclude_Seed_cdb_view in der Parameterdatei der Quelldatenbank auf FALSE setzen, um Informationen zum Klonen einer Sicherung von 12*c*__-Datenbank abzurufen.

  Die SEED-PDB ist eine vom System bereitgestellte Vorlage, mit der die CDB PDBs erstellen kann. Die Samen-PDB wird PDB als Samen bezeichnet. Informationen zu PDB-Dollar finden Sie im Oracle Doc ID 1940806.1.

  Sie sollten den Wert festlegen, bevor Sie die Datenbank 12*c*_ sichern.
- SnapCenter unterstützt die Sicherung von Dateisystemen, die vom Autofs-Subsystem verwaltet werden. Wenn Sie die Datenbank klonen, stellen Sie sicher, dass die Mount-Punkte der Daten nicht unter der Wurzel des Mount-Punkts von Autofs liegen, da der Root-Benutzer des Plug-in-Hosts keine Berechtigung hat, Verzeichnisse unter dem Stammverzeichnis des Autofs Mount-Punkts zu erstellen.

  Wenn sich Kontroll- und Wiederherstellungsprotokolle unter dem Dateneinhängungspunkt befinden, sollten Sie den Pfad der Kontrolldatei ändern und anschließend den Dateipfad wiederholen.

Sie können die neuen geklonten Mount-Punkte manuell mit dem Autofs-Subsystem registrieren. Die neuen geklonten Mount-Punkte werden nicht automatisch registriert.

- Wenn Sie ein TDE (Auto Login) haben und die Datenbank auf demselben oder einem anderen Host klonen möchten, sollten Sie Wallet (Schlüsseldateien) unter */etc/ORACLE/WALLET/ €ORACLE_SID* von der Quelldatenbank in die geklonte Datenbank kopieren.
- Sie sollten den Wert von use_lvmetad = 0 in _/etc/lvm/lvm.conf setzen und den lvm2-lvmetad-Service beenden, um erfolgreich ein Klonen in SAN-Umgebungen (Storage Area Network) unter Oracle Linux 7 oder höher oder Red hat Enterprise Linux (RHEL) 7 oder höher durchzuführen.
- Sie sollten den Oracle-Patch 13366202 installieren, wenn Sie die Oracle-Datenbank 11.2.0.3 oder höher verwenden und die Datenbank-ID für die Hilfsinstanz mit einem NID-Skript geändert wird.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Sie sollten sicherstellen, dass die LUN nicht dem AIX-Host mit iGroup zugeordnet ist, die aus gemischten Protokollen iSCSI und FC besteht. Weitere Informationen finden Sie unter "Der Vorgang schlägt fehl, da der Fehler nicht in der Lage ist, das Gerät für die LUN zu ermitteln".

Klonen eines Backups einer Oracle Datenbank

Sie können SnapCenter verwenden, um eine Oracle Datenbank mithilfe des Backups der Datenbank zu klonen.

Über diese Aufgabe

Der Klonvorgang erstellt eine Kopie der Datenbankdatendateien und erstellt neue Online-Protokolldateien für die Wiederherstellung sowie Kontrolldateien. Die Datenbank kann auf Basis der angegebenen Wiederherstellungsoptionen optional bis zu einem bestimmten Zeitpunkt wiederhergestellt werden.

Das Klonen schlägt fehl, wenn Sie versuchen, ein Backup zu klonen, das auf einem Linux Host auf einem AIX Host erstellt wurde, oder umgekehrt.

SnapCenter erstellt eine Standalone-Datenbank, wenn sie aus einem Backup einer Oracle RAC Datenbank geklont wird. SnapCenter unterstützt die Erstellung von Klonen aus der Backup von Data Guard Standby und Active Data Guard Standby Datenbanken.

Während des Klonens mountet SnapCenter das Protokoll-Backup für Recovery-Vorgänge. Nach der Wiederherstellung wird die Protokollsicherung abgehängt. Alle diese Klone sind unter */var/opt/snapcenter/scu/Clones/* eingebunden. Wenn Sie ASM über NFS verwenden, sollten Sie */var/opt/snapcenter/scu/Clones/*/** zum vorhandenen Pfad hinzufügen, der im Parameter asm_diskstring definiert ist.

Beim Klonen eines Backups einer ASM-Datenbank in einer SAN-Umgebung werden udev-Regeln für die geklonten Host-Geräte unter */etc/udev/rules.d/999-scu-netapp.rules* erstellt. Diese udev-Regeln, die den geklonten Host-Geräten zugeordnet sind, werden beim Löschen des Klons gelöscht.

In einem Flex ASM-Setup können Sie keinen Klonvorgang auf Leaf-Knoten ausführen, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist.

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.
4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (sekundär) aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Name eine der folgenden Aktionen durch:

Ihr Ziel ist	Schritte…
Klonen einer Datenbank (CDB oder nicht-CDB)	a. Geben Sie die SID des Klons an. Der Clone SID ist standardmäßig nicht verfügbar, und die maximale Länge der SID beträgt 8 Zeichen. Sie sollten sicherstellen, dass auf dem Host, auf dem der Klon erstellt wird, keine Datenbank mit derselben SID vorhanden ist.
Klonen einer Plug-in-Datenbank (PDB)	a. Wählen Sie **PDB Clone**. b. Geben Sie die PDB an, die Sie klonen möchten. c. Geben Sie den Namen der geklonten PDB an. Detaillierte Schritte zum Klonen einer PDB finden Sie unter "Klonen einer sofort anschließbaren Datenbank".

   Wenn Sie eine gespiegelte oder Vault-Daten auswählen:

   - Wenn keine Protokollsicherung bei Spiegel oder Tresor vorhanden ist, wird nichts ausgewählt und die Lokatoren leer sind.
   - Wenn Protokollsicherungen in Mirror oder Vault vorhanden sind, wird die neueste Protokollsicherung ausgewählt und der entsprechende Locator angezeigt.

   Wenn die ausgewählte Protokollsicherung sowohl im Spiegelungs- als auch im Tresorverzeichnis vorhanden ist, werden beide Lokatoren angezeigt.
7. Führen Sie auf der Seite Standorte die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonhost	Standardmäßig wird der Quell-Datenbank-Host befüllt. Wenn Sie den Klon auf einem anderen Host erstellen möchten, wählen Sie den Host aus, der dieselbe Version von Oracle und dasselbe Betriebssystem wie der des Quelldatenbankhosts hat.
Datendateiorte	Standardmäßig wird der Speicherort der Datendatei gefüllt. Die standardmäßige Namenskonvention von SnapCenter für SAN- oder NFS-File-Systeme ist FileSystemNamesourceDatabase_CLONESID. Die standardmäßige SnapCenter-Namenskonvention für ASM-Festplattengruppen ist SC_HASHCODEofDISKGROUP_CLONESID. Die HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Laufwerksgruppe eindeutig ist. Wenn Sie den Namen der ASM-Laufwerksgruppe anpassen, stellen Sie sicher, dass die Namenslänge die von Oracle unterstützte maximale Länge erfüllt. Wenn Sie einen anderen Pfad angeben möchten, müssen Sie die Mount-Punkte für Datendatei oder die Namen der ASM-Festplattengruppen für die Klondatenbank eingeben. Wenn Sie den Datenpfad anpassen, müssen Sie auch die Steuerdatei und die Redo-Log-Datei ASM-Festplattengruppennamen oder Dateisystem entweder auf den gleichen Namen für Datendateien oder auf ein vorhandenes ASM-Laufwerksgruppen oder Dateisystem ändern.

Für dieses Feld…	Tun Sie das…
Kontrolldateien	Standardmäßig wird der Pfad der Kontrolldatei ausgefüllt. Die Steuerdateien werden in derselben ASM-Laufwerksgruppe oder in demselben Dateisystem wie die der Datendateien abgelegt. Wenn Sie den Pfad der Steuerdatei überschreiben möchten, können Sie einen anderen Pfad für die Steuerdatei angeben. ⓘ Das Dateisystem oder die ASM-Laufwerksgruppe sollte auf dem Host vorhanden sein. Standardmäßig ist die Anzahl der Kontrolldateien mit der der Quelldatenbank identisch. Sie können die Anzahl der Kontrolldateien ändern, aber zum Klonen der Datenbank ist mindestens eine Kontrolldatei erforderlich. Sie können den Pfad der Steuerdatei an ein anderes Dateisystem (vorhanden) anpassen als den der Quelldatenbank.

Für dieses Feld…	Tun Sie das…
Wiederherstellungsprotokolle	Standardmäßig werden die Gruppe, der Pfad und ihre Größe der Wiederherstellungsprotokolle ausgefüllt. Die Wiederherstellungsprotokolle werden in derselben ASM-Festplattengruppe oder demselben Filesystem wie die Datendateien der geklonten Datenbank platziert. Wenn Sie den Pfad für die Wiederherstellungsprotokoll-Datei überschreiben möchten, können Sie den Pfad für die Wiederherstellungsprotokolle auf ein anderes Dateisystem als den der Quelldatenbank anpassen. Auf dem Host sollte das neue Dateisystem oder die ASM-Laufwerksgruppe vorhanden sein. Standardmäßig ist die Anzahl der Wiederherstellungsprotokolle, der Wiederherstellungsprotokolle und ihrer Größe mit der Quelldatenbank identisch. Sie können die folgenden Parameter ändern: • Anzahl der Wiederherstellungsprotokolle Zum Klonen der Datenbank sind mindestens zwei Wiederherstellungsprotokolle erforderlich. • Wiederholen Sie die Protokolldateien in jeder Gruppe und ihrem Pfad Sie können den Pfad der Redo-Log-Datei an ein anderes (vorhandenes) Dateisystem anpassen als den der Quelldatenbank. In der Gruppe für Wiederherstellungsprotokolle ist mindestens eine Wiederherstellungsprotokoll-Datei erforderlich, um die Datenbank zu klonen. • Größe der Wiederherstellungsprotokolldatei

8. Führen Sie auf der Seite Anmeldeinformationen die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Anmeldeinformationsname für sys-Benutzer	Wählen Sie das Credential aus, das zum Definieren des sys-Benutzerpassworts der Clone-Datenbank verwendet werden soll. Wenn SQLNET.AUTHENTICATION_SERVICES in sqlnet.ora-Datei auf dem Ziel-Host auf KEINE gesetzt ist, sollten Sie in der SnapCenter-GUI nicht **kein** als Credential auswählen.
Benutzername für die ASM-Instanz	Wählen Sie **Keine** aus, wenn die OS-Authentifizierung für die Verbindung zur ASM-Instanz auf dem Clone-Host aktiviert ist. Wählen Sie andernfalls die Oracle ASM-Berechtigung aus, die entweder mit „`sys`“-Benutzer oder mit einem Benutzer mit der Berechtigung `sysasm`“ für den Klon-Host konfiguriert ist.

Die Oracle-Startseite, der Benutzername und die Gruppendetails werden automatisch aus der Quelldatenbank ausgefüllt. Sie können die Werte basierend auf der Oracle-Umgebung des Hosts ändern, auf dem der Klon erstellt wird.

9. Führen Sie auf der Seite PreOps die folgenden Schritte aus:

   a. Geben Sie den Pfad und die Argumente für das Prescript ein, das Sie vor dem Klonvorgang ausführen möchten.

      Sie müssen das Prescript entweder in */var/opt/snapcenter/spl/scripts* oder in einem Ordner in diesem Pfad speichern. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird.

   b. Ändern Sie im Abschnitt Datenbankparameter-Einstellungen die Werte vorausgefüllter Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.

      Sie können weitere Parameter hinzufügen, indem Sie auf * klicken + *.

      Wenn Sie Oracle Standard Edition verwenden und die Datenbank im Archiv-Log-Modus ausgeführt wird oder Sie eine Datenbank aus dem Wiederherstellungsprotokoll wiederherstellen möchten, fügen Sie die Parameter hinzu und geben den Pfad an.

      - LOG_ARCHIVE_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

      > ⓘ Der fast Recovery Area (FRA) ist in den vorausgefüllten Datenbankparametern nicht definiert. Sie können FRA konfigurieren, indem Sie die zugehörigen Parameter hinzufügen.

Der Standardwert von log_Archive_dest_1 liegt bei „€ORACLE_HOME/Clone_sid“ und an diesem Ort werden die Archivprotokolle der geklonten Datenbank erstellt. Wenn Sie den Parameter log_Archive_dest_1 gelöscht haben, wird der Speicherort des Archivprotokolls von Oracle bestimmt. Sie können einen neuen Speicherort für das Archivprotokoll definieren, indem Sie log_Archive_dest_1 bearbeiten. Stellen Sie jedoch sicher, dass das Dateisystem oder die Laufwerksgruppe vorhanden sein und auf dem Host verfügbar gemacht werden soll.

a. Klicken Sie auf **Zurücksetzen**, um die Standardeinstellungen für die Datenbankparameter anzuzeigen.

10. Auf der PostOps Seite werden **Recover Database** und **Until Cancel** standardmäßig ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

    SnapCenter führt eine Recovery durch, indem das letzte Protokoll-Backup montiert wird, bei dem die nicht unterbrochene Sequenz von Archivprotokollen nach dem Daten-Backup zum Klonen ausgewählt wurde. Das Protokoll und das Daten-Backup sollten sich auf dem Primärspeicher befinden, um den Klon im Primärspeicher durchzuführen und Protokoll- und Daten-Backups auf dem Sekundärspeicher zu erstellen, um den Klon im Sekundärspeicher durchzuführen.

    Die Optionen **Recover Database** und **bis Abbrechen** sind nicht ausgewählt, wenn SnapCenter die entsprechenden Log-Backups nicht findet. Sie können den externen Archiv-Log-Speicherort angeben, wenn die Protokollsicherung in **externen Archiv-Log-Speicherorten angeben** nicht verfügbar ist. Sie können mehrere Protokollpositionen angeben.

    Wenn Sie eine Quelldatenbank klonen möchten, die für die Unterstützung von Flash Recovery Area (FRA) und Oracle Managed Files (OMF) konfiguriert ist, muss das Protokollziel für die Wiederherstellung auch der OMF-Verzeichnisstruktur entsprechen.

    Die Seite PostOps wird nicht angezeigt, wenn die Quelldatenbank Data Guard Standby oder eine Active Data Guard Standby-Datenbank ist. Für Data Guard Standby oder eine Active Data Guard Standby-Datenbank bietet SnapCenter keine Option, um den Typ der Wiederherstellung in der SnapCenter GUI auszuwählen, aber die Datenbank wird mit bis Abbrechen Recovery-Typ wiederhergestellt, ohne Protokolle anzuwenden.

Feldname	Beschreibung
Bis Abbrechen	SnapCenter führt eine Recovery durch, indem das neueste Protokoll-Backup mit der nicht unterbrochenen Sequenz von Archivprotokollen nach dem Daten-Backup, das zum Klonen ausgewählt wurde, mounten. Die geklonte Datenbank wird wiederhergestellt, bis die fehlende oder beschädigte Protokolldatei vorliegt.
Datum und Uhrzeit	SnapCenter stellt die Datenbank bis zu einem festgelegten Datum und einer bestimmten Uhrzeit wieder her. Das akzeptierte Format lautet mm/TT/JJJJ hh:mm:ss Die Zeit kann im 24-Stunden-Format angegeben werden.

Feldname	Beschreibung
Bis SCN (Systemänderungsnummer)	SnapCenter stellt die Datenbank bis zu einer angegebenen Systemänderungsnummer (SCN) wieder her.
Geben Sie externe Archivprotokolle an	Geben Sie den Speicherort des externen Archivprotokolls an.
Neue DBID erstellen	Standardmäßig ist das Kontrollkästchen Neue DBID* erstellen aktiviert, um eine eindeutige Nummer (DBID) für die geklonte Datenbank zu generieren, die sie von der Quelldatenbank unterscheidet. Deaktivieren Sie das Kontrollkästchen, wenn Sie der geklonten Datenbank die DBID der Quelldatenbank zuweisen möchten. Wenn Sie in diesem Szenario die geklonte Datenbank im externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.
Erstellen Sie eine tempfile für temporäre Tablespaces	Aktivieren Sie das Kontrollkästchen, wenn Sie eine tempfile für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten. Wenn das Kontrollkästchen nicht aktiviert ist, wird der Datenbankklon ohne die tempfile erstellt.
Geben Sie beim Erstellen eines Klons sql-Einträge ein, die angewendet werden sollen	Fügen Sie die sql-Einträge hinzu, die Sie beim Erstellen des Klons anwenden möchten.
Geben Sie Skripte ein, die nach dem Klonvorgang ausgeführt werden sollen	Geben Sie den Pfad und die Argumente des Postskripts an, die Sie nach dem Klonvorgang ausführen möchten. Das Postscript sollte entweder in */var/opt/snapcenter/spl/scripts* oder in einem Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird.

11. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den ausgeführten Klonvorgang anhängen möchten, wählen Sie **Job-Bericht anhängen** aus.

> Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

12. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

> Während des Recovery im Rahmen des Klonens wird der Klon mit einer Warnung erstellt, auch wenn das Recovery fehlschlägt. Sie können für diesen Klon ein manuelles Recovery durchführen, um die Klondatenbank konsistent zu machen.

13. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Ergebnis

Nach dem Klonen der Datenbank können Sie die Seite „Ressourcen“ aktualisieren, um die geklonte Datenbank als eine der für Backups verfügbaren Ressourcen aufzulisten. Die geklonte Datenbank kann mithilfe des Standard-Backup-Workflows wie jede andere Datenbank gesichert oder in eine Ressourcengruppe (entweder neu erstellt oder bereits vorhanden) aufgenommen werden. Die geklonte Datenbank kann weiter geklont werden (Klon von Klonen).

Nach dem Klonen sollten Sie die geklonte Datenbank niemals umbenennen.

> Falls Sie das Recovery während des Klonens nicht durchgeführt haben, kann das Backup der geklonten Datenbank fehlschlagen, da ein unsachgemäßes Recovery erforderlich ist und Sie möglicherweise manuelles Recovery durchführen müssen. Das Protokoll-Backup kann auch fehlschlagen, wenn der Standardspeicherort, der für Archivprotokolle erfasst wurde, auf einem Storage anderer Anbieter liegt oder wenn das Storage-System nicht mit SnapCenter konfiguriert ist.

In AIX Setup können Sie den Befehl lkdev zum Sperren und den Befehl rendev verwenden, um die Festplatten umzubenennen, auf denen sich die geklonte Datenbank residierte.

Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Löschvorgang. Bei AIX LVM-Layouts, die auf SAN-Geräten aufgebaut sind, werden die Umbenennung von Geräten für die geklonten SAN-Geräte nicht unterstützt.

Weitere Informationen

- "Die Wiederherstellung oder das Klonen schlägt mit der ORA-00308-Fehlermeldung fehl"
- "Fehler beim Wiederherstellen einer geklonten Datenbank"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Klonen einer sofort anschließbaren Datenbank

Sie können eine steckbare Datenbank (PDB) auf einem anderen oder demselben Ziel-CDB auf demselben Host oder einem anderen Host klonen. Sie können die geklonte PDB auch auf einem gewünschten SCN oder Datum und Uhrzeit wiederherstellen.

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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank des Typs Single Instance (mandantenfähig) aus der Detailansicht der Datenbank oder in der Detailansicht der Ressourcengruppen aus.

   Die Seite der Datenbanktopologie wird angezeigt.
4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (sekundär) aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   a. Wählen Sie **PDB Clone**.
   b. Geben Sie die PDB an, die Sie klonen möchten.

      Sie können jeweils nur eine PDB klonen.

   c. Geben Sie den Namen der Klon-PDB an.
7. Führen Sie auf der Seite Standorte die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonhost	Standardmäßig wird der Quell-Datenbank-Host befüllt. Wenn Sie den Klon auf einem anderen Host erstellen möchten, wählen Sie den Host aus, der dieselbe Version von Oracle und dasselbe Betriebssystem wie der des Quelldatenbankhosts hat.
Ziel-CDB	Wählen Sie die CDB aus, in die die geklonte PDB einbezogen werden soll. Sie sollten sicherstellen, dass die Ziel-CDB ausgeführt wird.
Datenbankstatus	Aktivieren Sie das Kontrollkästchen **Öffnen Sie die geklonte PDB im LESE-SCHREIBMODUS**, wenn Sie die PDB im LESE-SCHREIB-Modus öffnen möchten.

Datendateiorte	Standardmäßig wird der Speicherort der Datendatei gefüllt. Die standardmäßige Namenskonvention von SnapCenter für SAN- oder NFS-Dateisysteme ist FileSystemNamesourceDatabase_SCJOBID. Die standardmäßige SnapCenter-Namenskonvention für ASM-Festplattengruppen ist SC_HASHCODEofDISKGROUP_SCJOBID. Die HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Laufwerksgruppe eindeutig ist. Wenn Sie den Namen der ASM-Laufwerksgruppe anpassen, stellen Sie sicher, dass die Namenslänge die von Oracle unterstützte maximale Länge erfüllt. Wenn Sie einen anderen Pfad angeben möchten, müssen Sie die Mount-Punkte für Datendatei oder die Namen der ASM-Festplattengruppen für die Klondatenbank eingeben.

Die Oracle-Startseite, der Benutzername und die Gruppendetails werden automatisch aus der Quelldatenbank ausgefüllt. Sie können die Werte basierend auf der Oracle-Umgebung des Hosts ändern, auf dem der Klon erstellt wird.

8. Führen Sie auf der Seite PreOps die folgenden Schritte aus:
   a. Geben Sie den Pfad und die Argumente für das Prescript ein, das Sie vor dem Klonvorgang ausführen möchten.

      Sie sollten das Prescript entweder in /var/opt/snapcenter/spl/scripts oder in einem Ordner in diesem Pfad speichern. Standardmäßig wird der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird.

   b. Ändern Sie im Abschnitt Parametereinstellungen der Zusatzdatenbank CDB Clone die Werte vorbefüllter Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
9. Klicken Sie auf **Zurücksetzen**, um die Standardeinstellungen für die Datenbankparameter anzuzeigen.
10. Auf der PostOps-Seite ist **bis Abbrechen** standardmäßig ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

    Die Option **bis Abbrechen** wird nicht ausgewählt, wenn SnapCenter die entsprechenden Log-Backups nicht findet. Sie können den externen Archiv-Log-Speicherort angeben, wenn die Protokollsicherung in **externen Archiv-Log-Speicherorten angeben** nicht verfügbar ist. Sie können mehrere Protokollpositionen angeben.

Wenn Sie eine Quelldatenbank klonen möchten, die für die Unterstützung von Flash Recovery Area (FRA) und Oracle Managed Files (OMF) konfiguriert ist, muss das Protokollziel für die Wiederherstellung auch der OMF-Verzeichnisstruktur entsprechen.

Feldname	Beschreibung
Bis Abbrechen	SnapCenter führt eine Recovery durch, indem das neueste Protokoll-Backup mit der nicht unterbrochenen Sequenz von Archivprotokollen nach dem Daten-Backup, das zum Klonen ausgewählt wurde, mounten. Das Protokoll und das Daten-Backup sollten sich auf dem Primärspeicher befinden, um den Klon im Primärspeicher durchzuführen und Protokoll- und Daten-Backups auf dem Sekundärspeicher zu erstellen, um den Klon im Sekundärspeicher durchzuführen. Die geklonte Datenbank wird wiederhergestellt, bis die fehlende oder beschädigte Protokolldatei vorliegt.
Datum und Uhrzeit	SnapCenter stellt die Datenbank bis zu einem festgelegten Datum und einer bestimmten Uhrzeit wieder her. Die Zeit kann im 24-Stunden-Format angegeben werden.
Bis SCN (Systemänderungsnummer)	SnapCenter stellt die Datenbank bis zu einer angegebenen Systemänderungsnummer (SCN) wieder her.
Geben Sie externe Archivprotokolle an	Geben Sie den Speicherort des externen Archivprotokolls an.
Neue DBID erstellen	Standardmäßig ist das Kontrollkästchen Neue DBID* erstellen nicht für die Zusatzklondatenbank ausgewählt. Aktivieren Sie das Kontrollkästchen, wenn Sie eine eindeutige Nummer (DBID) für die zusätzliche geklonte Datenbank generieren möchten, die sie von der Quelldatenbank unterscheidet.

Feldname	Beschreibung
Erstellen Sie eine tempfile für temporäre Tablespaces	Aktivieren Sie das Kontrollkästchen, wenn Sie eine tempfile für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten. Wenn das Kontrollkästchen nicht aktiviert ist, wird der Datenbankklon ohne die tempfile erstellt.
Geben Sie beim Erstellen eines Klons sql-Einträge ein, die angewendet werden sollen	Fügen Sie die sql-Einträge hinzu, die Sie beim Erstellen des Klons anwenden möchten.
Geben Sie Skripte ein, die nach dem Klonvorgang ausgeführt werden sollen	Geben Sie den Pfad und die Argumente des Postskripts an, die Sie nach dem Klonvorgang ausführen möchten. Das Postscript sollte entweder in */var/opt/snapcenter/spl/scripts* oder in einem Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird.

11. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

    Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den ausgeführten Klonvorgang anhängen möchten, wählen Sie **Job-Bericht anhängen** aus.

    Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

12. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
13. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Nach Ihrer Beendigung

Wenn Sie eine Sicherung der geklonten PDB erstellen möchten, sollten Sie die Ziel-CDB dort sichern, wo die PDB geklont wird, da eine Sicherung nur der geklonten PDB nicht möglich ist. Sie sollten eine sekundäre Beziehung für das Ziel-CDB erstellen, wenn Sie die Sicherung mit einer sekundären Beziehung erstellen möchten.

In einem RAC-Setup ist der Speicher für geklonte PDB nur mit dem Knoten verbunden, auf dem der PDB-Klon ausgeführt wurde. Die PDBs auf den anderen Knoten des RAC befinden sich im MOUNT-Status. Wenn Sie möchten, dass die geklonte PDB von den anderen Nodes aus zugänglich ist, sollten Sie den Storage manuell den anderen Nodes zuweisen.

Weitere Informationen

- "Die Wiederherstellung oder das Klonen schlägt mit der ORA-00308-Fehlermeldung fehl"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Backups der Oracle Datenbank mit UNIX Befehlen klonen

Der Klon-Workflow umfasst die Planung, die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

Sie sollten die folgenden Befehle ausführen, um die Oracle Database Clone Specification File zu erstellen und den Klonvorgang zu starten.

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide".

Schritte

1. Erstellen Sie eine Oracle-Datenbankklonspezifikation aus einem angegebenen Backup: *New-SmOracleCloneSpecification*

   Wenn die sekundäre Datenschutzrichtlinie ein einheitliches Mirror-Vault ist, geben Sie nur -IncludeSecond Details an. Sie müssen nicht -SecondaryStorageType angeben.

   Mit diesem Befehl wird automatisch eine Oracle-Datenbankklonspezifikationsdatei für die angegebene Quelldatenbank und ihr Backup erstellt. Außerdem müssen Sie eine Klon-Datenbank-SID angeben, damit die erstellte Spezifikationsdatei die automatisch generierten Werte für die von Ihnen erstellte Klondatenbank enthält.

   Die Klon-Spezifikations-Datei wird unter */var/opt/snapcenter/sco/Clone_specs* erstellt.

2. Initiieren einer Klonoperation aus einer Clone Resource Group oder einem vorhandenen Backup: *New-SmClone*

   Dieser Befehl initiiert einen Klonvorgang. Für den Klonvorgang müssen Sie außerdem einen Pfad für die Oracle-Klonspezifikation angeben. Zudem können Sie die Recovery-Optionen festlegen, auf denen der Klonvorgang ausgeführt werden soll, sowie Vorskripte, Postskripte und andere Details.

   Standardmäßig wird die Zieldatei des Archivprotokolls für die Klondatenbank automatisch mit einer Zieldatei von _ € ORACLE_HOME/CLONE_SIDs_ gefüllt.

Oracle Database klonen

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon ist unabhängig von der übergeordneten Ressource.

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien des Klons gelöscht.
- Informationen zu den Einschränkungen für den Klon-Split-Vorgang finden Sie im "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

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. Wählen Sie die geklonte Ressource aus (z. B. die Datenbank oder die LUN), und klicken Sie dann auf  .
4. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Klonabteilvorgang reagiert nicht mehr, wenn der SMCore-Service neu gestartet wird und die Datenbanken, auf denen der Klonabteilvorgang ausgeführt wurde, als Klone auf der Seite Ressourcen aufgeführt werden. Sie sollten das Cmdlet *Stop-SmJob* ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragezeit oder kürzere Abfragezeit benötigen, um zu prüfen, ob der Klon aufgeteilt ist oder nicht, können Sie den Wert von CloneSplitStatusCheckPollTime in der Datei SMCoreServiceHost.exe.config ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Klonabteilvorgangs abgefragt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klontrennung schlägt fehl, wenn derzeit eine Sicherung, Wiederherstellung oder eine andere Klonverteilung durchgeführt wird. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Split-Klon einer steckbaren Datenbank

Sie können eine geklonte Plug-in-Datenbank (PDB) mit SnapCenter teilen.

Über diese Aufgabe

Wenn Sie eine Sicherung der Ziel-CDB erstellt haben, in der die PDB geklont wird, wird die geklonte PDB bei der Aufteilung des PDB-Klons auch aus allen Backups der Ziel-CDB entfernt, die die geklonte PDB enthalten.

Die PDB-Klone werden in der Ansicht „Inventar“ oder „Ressourcen“ nicht angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie die Quellcontainer-Datenbank (CDB) aus der Ressourcen- oder Ressourcengruppenansicht aus.
3. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
4. Wählen Sie den PDB-Klon (targetCDB:PDBClone) aus, und klicken Sie dann auf  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Überwachen Sie die Klonvorgänge von Oracle Datenbanken

Sie können den Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie Auf Filtern der Liste, sodass nur Klonvorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.

d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.

e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.

4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Aktualisieren Sie einen Klon

Sie können den Klon aktualisieren, indem Sie den Befehl *Refresh-SmClone* ausführen. Mit diesem Befehl wird ein Backup der Datenbank erstellt, der vorhandene Klon gelöscht und ein Klon mit demselben Namen erstellt.

Ein PDB-Klon kann nicht aktualisiert werden.

Was Sie brauchen

- Erstellen Sie ein komplettes Online-Backup oder eine Offline Daten-Backup-Richtlinie, ohne dass geplante Backups aktiviert sind.
- Konfigurieren Sie die E-Mail-Benachrichtigung in der Richtlinie nur für Backup-Fehler.
- Definieren Sie die Aufbewahrungszahl für die On-Demand-Backups entsprechend, um sicherzustellen, dass keine unerwünschten Backups vorhanden sind.
- Stellen Sie sicher, dass nur ein vollständiges Online-Backup oder eine Richtlinie für Offline-Daten-Backups der Ressourcengruppe zugeordnet ist, die für den Klon-Aktualisierungsvorgang ermittelt wird.
- Erstellen Sie eine Ressourcengruppe mit nur einer Datenbank.
- Wenn ein Cron-Job für den Befehl „Clone Refresh“ erstellt wird, stellen Sie sicher, dass sich die SnapCenter-Zeitpläne und cron-Zeitpläne nicht mit der Datenbankressourcengruppe überschneiden.

  Stellen Sie für einen Cron-Job, der für den Befehl „Clone refresh“ erstellt wurde, sicher, dass Sie Open-SmConnection nach allen 24 Stunden ausführen.

- Stellen Sie sicher, dass die Klon-SID für einen Host eindeutig ist.

  Wenn mehrere Aktualisierungsklonvorgänge dieselbe Klon-Spezifikationsdatei verwenden oder die Klon-Spezifikationsdatei mit derselben Clone-SID verwenden, wird der vorhandene Klon mit der SID auf dem Host gelöscht und dann der Klon erstellt.

- Stellen Sie sicher, dass die Backup-Richtlinie mit sekundärem Schutz aktiviert ist und dass die Klon-Spezifikations-Datei mit „`-IncludeSecondaryDetails`“ erstellt wird, um die Klone mit sekundären Backups zu erstellen.
  - Wenn die Spezifikationsdatei für den primären Klon angegeben ist, die Richtlinie jedoch die Option für das sekundäre Update ausgewählt hat, wird das Backup erstellt und das Update wird auf den sekundären Server übertragen. Der Klon wird jedoch aus dem primären Backup erstellt.
  - Wenn die Spezifikations-Datei für den primären Klon angegeben ist und für die Richtlinie keine Option für das sekundäre Update ausgewählt ist, wird das Backup auf dem primären erstellt und der Klon aus dem primären erstellt.

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer: *Open-SmConnection*

2. Erstellen Sie eine Oracle-Datenbankklonspezifikation aus einem angegebenen Backup: *New-SmOracleCloneSpecification*

   Wenn die sekundäre Datenschutzrichtlinie ein einheitliches Mirror-Vault ist, geben Sie nur -IncludeSecond Details an. Sie müssen nicht -SecondaryStorageType angeben.

   Mit diesem Befehl wird automatisch eine Oracle-Datenbankklonspezifikationsdatei für die angegebene Quelldatenbank und ihr Backup erstellt. Außerdem müssen Sie eine Klon-Datenbank-SID angeben, damit die erstellte Spezifikationsdatei die automatisch generierten Werte für die von Ihnen erstellte Klondatenbank enthält.

   Die Klon-Spezifikations-Datei wird unter */var/opt/snapcenter/sco/Clone_specs* erstellt.

3. Führen Sie *Refresh-SmClone* aus.

   Falls der Vorgang mit der Fehlermeldung „PL-SCO-20032: CanExecute fehlgeschlagen mit Fehler: PL-SCO-30031: Redo Log file +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists“, geben Sie einen höheren Wert für die Fehlermeldungen *-WaitToTriggerClone* an.

   Ausführliche Informationen zu UNIX-Befehlen finden Sie im "SnapCenter Software Command Reference Guide".

Löschen des Klons einer steckbaren Datenbank

Sie können den Klon einer steckbaren Datenbank (PDB) löschen, wenn Sie nicht mehr benötigen.

Wenn Sie eine Sicherung der Ziel-CDB erstellt haben, wo die PDB geklont wird, wird beim Löschen des PDB-Klons auch die geklonte PDB aus der Sicherung der Ziel-CDB entfernt.

Die PDB-Klone werden in der Ansicht „Inventar“ oder „Ressourcen“ nicht angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie die Quellcontainer-Datenbank (CDB) aus der Ressourcen- oder Ressourcengruppenansicht aus.
3. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
4. Wählen Sie den PDB-Klon (targetCDB:PDBClone) aus, und klicken Sie dann auf .
5. Klicken Sie auf **OK**.