Backup von Oracle Datenbanken

SnapCenter Software 4.7

NetApp
September 26, 2025

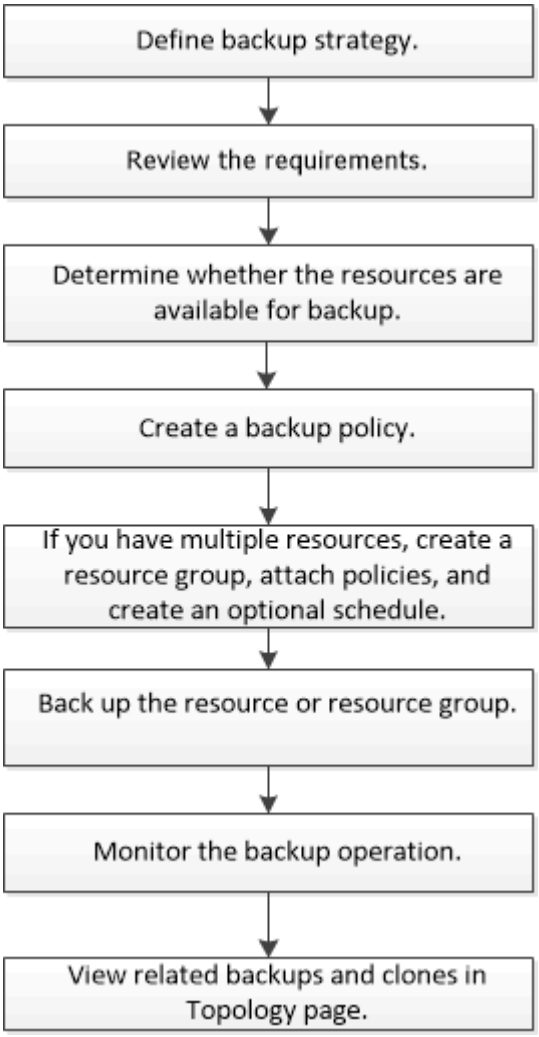
Inhalt

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.

Vordefinierte Umgebungsvariablen für Backup-spezifische Prescript und Postscript

Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie während der Erstellung von Backup-Richtlinien das Prescript und das Postscript ausführen. Diese Funktion wird mit Ausnahme von VMDK für alle Oracle-Konfigurationen unterstützt.

SnapCenter definiert die Werte der Parameter, auf die in der Umgebung, in der die Shell-Skripte ausgeführt werden, direkt zugegriffen werden kann. Bei der Ausführung der Skripte müssen Sie die Werte dieser Parameter nicht manuell angeben.

Unterstützte vordefinierte Umgebungsvariablen für das Erstellen von Backup-Richtlinien

- **SC_JOB_ID** gibt die Job-ID des Vorgangs an.

  Beispiel: 256

- **SC_ORACLE_SID** gibt die Systemkennung der Datenbank an.

  Wenn der Vorgang mehrere Datenbanken umfasst, enthält der Parameter Datenbanknamen, die per Pipe getrennt sind.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: NFSB32 NFSB31

- **SC_HOST** gibt den Hostnamen der Datenbank an.

  Bei RAC ist der Hostname der Name des Hosts, auf dem das Backup durchgeführt wird.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** gibt den Betriebssystembesitzer der Datenbank an.

  Die Daten werden als <db1>@<osser1><db2>@<osser2> formatiert.

  Beispiel: NFSB31@oracle NFSB32@oracle

- **SC_OS_GROUP** gibt die Betriebssystemgruppe der Datenbank an.

  Die Daten werden als <db1>@<osgroup1><db2>@<osgroerp2> formatiert.

  Beispiel: NFSB31@Installation von NFSB32@oinstall

- **SC_BACKUP_TYPE**" gibt den Sicherungstyp an (online voll, online Daten, Online log, offline Shutdown, offline Mount)

  Beispiele:

    - Für vollständige Backups: ONLINEFULL
    - Backup nur Daten: OnLINEDATA
    - Für nur-Protokoll-Sicherung: ONLINELOG
- **SC_BACKUP_NAME** gibt den Namen des Backups an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1 AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267
- **SC_BACKUP_ID** gibt die Backup-ID an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  BEISPIEL: DATEN@203 LOG@@205 V/207
- **SC_ORACLE_HOME** gibt den Pfad des Oracle Home-Verzeichnisses an.

  Beispiel: NFSB32@/ora01/App/oracle/Produkt/18.1.0/db_1 natürlich NFSB31@/ora01/App/oracle/Product/18.1.0/db_1
- **SC_BACKUP_RETENTION** gibt den in der Richtlinie definierten Aufbewahrungszeitraum an.

  Beispiele:

    - Für vollständige Sicherung: Stündliche DATEN@TAGE:3 natürlich LOG@ANZAHL:4
    - Nur für On-Demand-Datensicherung: OnDemand Daten@COUNT:2
    - Nur für On-Demand-Log-Backup: OnDemand-LOG@COUNT:2
- **SC_RESOURCE_GROUP_NAME** gibt den Namen der Ressourcengruppe an.

  Beispiel: RG1
- **SC_BACKUP_POLICY_NAME** gibt den Namen der Backup Policy an.

  Beispiel: Backup_Policy
- **SC_AV_NAME** gibt die Namen der Anwendungsvolumes an.

  Beispiel: AV1 natürlich AV2
- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** gibt die Speicherzuordnung von SVM zu Volume für das Verzeichnis der Datendateien an. Er wird der Name des übergeordneten Volume für luns und qtrees sein.

  Die Daten werden als <db1>@<SVM1:Volume1><db2>@<SVM2:Volume2> formatiert.

  Beispiele:

    - Für 2 Datenbanken in derselben Ressourcengruppe: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA NFSB31@Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
    - Für eine einzelne Datenbank mit Datendateien, die über mehrere Volumes verteilt sind:

Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** gibt die Speicherzuordnung von SVM zu Volume für das Log-Dateiverzeichnis an. Er wird der Name des übergeordneten Volume für luns und qtrees sein.

  Beispiele:

  - Für einzelne Datenbankinstanz: Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
  - Für mehrere Datenbankinstanzen: NFSB31@Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO NFSB32@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** gibt die Liste der Snapshots an, die den Namen des Speichersystems und den Namen des Volumes enthalten.

  Beispiele:

  - Für einzelne Datenbankinstanz: Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07 02.28.26.3973-21-2021_1_1
  - Für mehrere Datenbankinstanzen: NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_CDB_2021_07 02.28.26.3973 2021 21_SB1-17002_SB002_SB71_21_SB71BG_07 02.28.26.3973 2021_21_SB002_SB71B2B2BG_07 02.28.26.3973_SB002_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB002_SB1.01_SB002_SB71.01_SB71.01_SB1.01_SB002_SB002_SB1.01_SB1.01_
- **SC_PRIMARY_SNAPSHOT_NAMES** gibt die Namen der primären Snapshots an, die während des Backups erstellt wurden.

  Beispiele:

  - Für einzelne Datenbankinstanz: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Für mehrere Datenbankinstanzen: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1_NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Für Snapshots der Konsistenzgruppe, die 2 Volumes umfassen: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350
- **SC_PRIMARY_MOUNT_POINTS** gibt die Details des Mount-Punkts an, die Teil des Backups sind.

  Zu den Details gehört das Verzeichnis, auf dem Volumes angehängt sind und nicht das unmittelbare übergeordnete Objekt der zu sicherenden Datei. Bei einer ASM-Konfiguration ist dies der Name der Laufwerksgruppe.

  Die Daten werden als <db1>@<mountpoint1,mountpoint2><db2>@<mountpoint1,mountpoint2> formatiert.

  Beispiele:

  - Für einzelne Datenbankinstanz: /Mnt/nfsdb3_Data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
  - Für mehrere Datenbankinstanzen: NFSB31@/mnt/nfsdb31_Data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1

NFSB32@/mnt/nfsdb32_Data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1

- FÜR ASM: +DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** gibt die Namen der Snapshots an, die während der Sicherung der einzelnen Mount-Punkte erstellt wurden.

  Beispiele:

  - Für einzelne Datenbank-Instanz: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfb32_Data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
  - Für mehrere Datenbankinstanzen: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_Data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_Data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/b32_nfslog

- **SC_ARCHIVELOGS_LOCATIONS** gibt den Speicherort des Archiv-Log-Verzeichnisses an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Archivprotokolldateien. Wenn die Archivprotokolle an mehreren Orten abgelegt werden, werden alle Speicherorte erfasst. Dazu gehören auch die FRA-Szenarien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_log
  - Für mehrere Datenbanken auf NFS und für die NFSB31 Datenbank-Archiv-Logs, die in zwei verschiedenen Speicherorten platziert sind: NFSB31@/mnt/nsdb31_log1,/mnt/nfsdb31_log2 natürlich NFSB32@/mnt/nfsdb32_log
  - FÜR ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** gibt den Speicherort des Verzeichnisses der Wiederherstellungsprotokolle an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Redo-Log-Dateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_Data/newdb1
  - Für mehrere Datenbanken auf NFS: NFSB31@/mnt/nfsdb31_Data/newdb31 NFSB32@/mnt/nfsdb32_Data/newdb32
  - FÜR ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** gibt den Speicherort des Steuerdateien-Verzeichnisses an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Steuerdateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_Data/Fra/newdb1,/mnt/nfsdb2_Data/newdb1
  - Für mehrere Datenbanken auf NFS:

NFSB31@/mnt/nfsdb31_Data/Fra/newdb31,/mnt/nfsdb31_Data/newdb31
NFSB32@/mnt/nfsdb32_Data/Fra/newdb32,/mnt/nfsdb32_Data/newdb32

- FÜR ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS**" gibt den Speicherort des Verzeichnisses der Datendateien an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Datendateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank auf NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_Data/NEWDB3/Datendatei
  - Für mehrere Datenbanken auf NFS:
    NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_Data/NEWDB31/Datafile
    NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_Data/NEWDB32/Datafile
  - FÜR ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE

- **SC_SNAPSHOT_LABEL** gibt den Namen der sekundären Labels an.

  Beispiele: Stündliche, tägliche, wöchentliche, monatliche oder benutzerdefinierte Bezeichnung.

Unterstützte Trennzeichen

- **:** wird zur Trennung von SVM-Name und Volume-Name verwendet

  Beispiel: Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07 02.28.26.3973-21-2021_1

- **@** wird verwendet, um Daten von ihrem Datenbanknamen zu trennen und den Wert von seinem Schlüssel zu trennen.

  Beispiele:

  - NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21 07 02.28.26.3973 2021 21-2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_SB32_SB00G2_spsprod2417819002_SB1_21_SB1-1271_2021 21 07 02.28.26.3973_SB00DB_SB002_SB71_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB002_SB002_SB00BG_07 02.28.26.3973 2021_SB1.01_SB1.0
  - NFSB31@oracle NFSB32@oracle

- * * Wird verwendet, um die Daten zwischen zwei unterschiedlichen Datenbanken zu trennen und die Daten zwischen zwei verschiedenen Einheiten für SC_BACKUP_ID, SC_BACKUP_RETENTION und SC_BACKUP_NAME Parameter zu trennen.

  Beispiele:

  - DATEN@203 PROTOKOLL@205
  - STÜNDLICHE DATEN@TAGE:3 LOG@ANZAHL:4
  - DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** dient zur Trennung des Volume-Namens von seinem Snapshot für SC_PRIMARY_SNAPSHOT_NAMES und SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG-Parameter.

  Beispiel: NFSB32@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07 02.28.26.3973-21-2021_1_1

- **,** wird verwendet, um einen Satz von Variablen für dieselbe DB zu trennen.

  Beispiel: NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21 07 02.28.26.3973 2021 21-2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_CDB_NF32_REDO_2021 21 07 02.28.26.3973_21_SB001.01_SB1-172_SB002_SB1.01_SB002_SB1.02_SB1.02_SB1.01_SB002_SB1.02_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB002_SB002_SB002_SB00BG_SB002_07 02.28.26.3973 2021_SB1.01_SB1.01

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. Sie können dann auf das Symbol klicken , um das Filterfenster zu schließen.
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.

Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

- 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.

So verhindern Sie, dass SnapCenter nicht aus Datenbanken stammende Einträge ermittelt

Sie können verhindern, dass SnapCenter nicht-Datenbank-Einträge entdeckt, die in der oratab-Datei hinzugefügt wurden.

Schritte

1. Nach der Installation des Plug-ins für Oracle sollte der Root-Benutzer die Datei **sc_oratab.config** unter dem Verzeichnis */var/opt/snapcenter/sco/etc/* erstellen.

   Gewähren Sie dem Oracle Binäreigentümer und der Gruppe die Schreibberechtigung, damit die Datei zukünftig beibehalten werden kann.

2. Der Datenbankadministrator sollte die nicht-Datenbankeinträge in die Datei **sc_oratab.config** hinzufügen.

   Es wird empfohlen, dasselbe Format beizubehalten, das für die nicht aus Datenbanken stammenden Einträge in der */etc/oratab*-Datei definiert ist, oder der Benutzer kann einfach die Entity-Zeichenfolge hinzufügen, die nicht aus der Datenbank stammt.

   Die Groß-/Kleinschreibung des Strings wird beachtet. Jeder Text mit # am Anfang wird als Kommentar behandelt. Der Kommentar kann nach dem nicht-Datenbanknamen angehängt werden.

   ```
   For example:
   ----------------------------------------------
   # Sample entries
   # Each line can have only one non-database name
   # These are non-database name
   oratar  # Added by the admin group -1
   #Added by the script team
   NEWSPT
   DBAGNT:/ora01/app/oracle/product/agent:N
   ----------------------------------------------
   ```

3. Entdecken Sie die Ressourcen.

   Die Einträge, die nicht aus Datenbanken in der Seite **sc_oratab.config** hinzugefügt wurden, werden auf der Seite Ressourcen nicht aufgeführt.

Es wird immer empfohlen, vor dem Upgrade des SnapCenter-Plug-ins eine Sicherung der sc_oratab.config-Datei zu erstellen.

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.

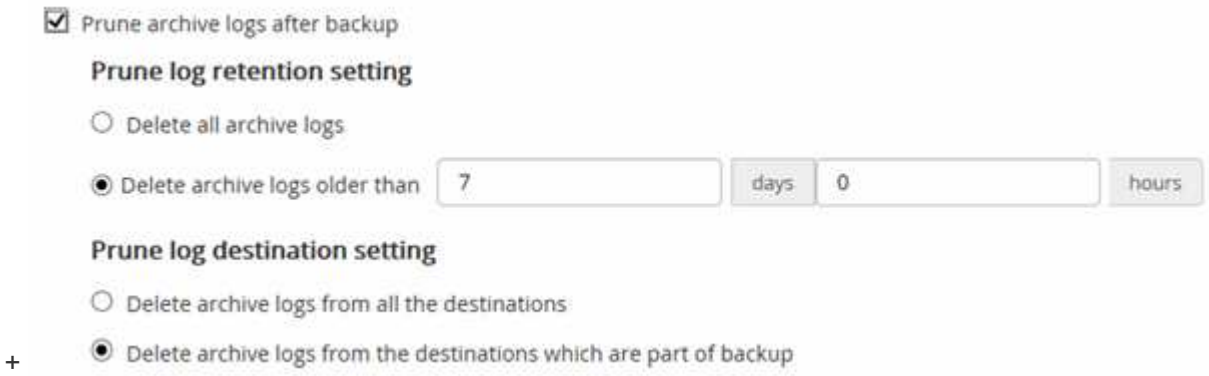
  Das Beschneiden von Archivprotokollen aus dem Archiv-Protokollziel, das in der Datenbank nicht konfiguriert ist, wird übersprungen.

  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).
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.

   Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Preskript und das Postscript ausführen. "Weitere Informationen ."

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

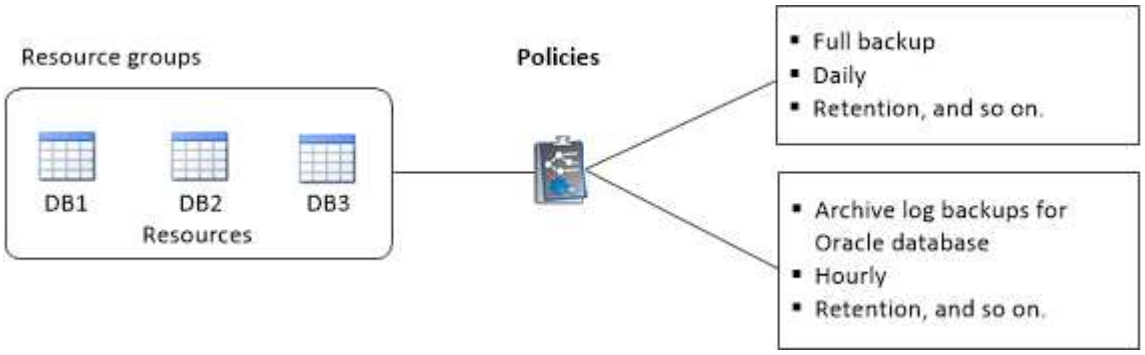
Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind.

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.
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 aus:

   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 in der Spalte Zeitpläne konfigurieren auf * * 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 in der Spalte Configure Schedules auf * * , 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.
- Der Wert von RESTTimeout sollte auf 86400000 ms erhöht werden in *C:\Programme\NetApp \SMCore\SMCoreServiceHost.exe.config* Datei auf dem SnapCenter-Server-Host, 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 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, 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 aus:

   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 in der Spalte Zeitpläne konfigurieren auf 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**.

      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 in der Spalte Zeitpläne konfigurieren auf , 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**.

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 durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf * * klicken und dann das Tag auswählen. Sie können dann auf * * klicken, um den Filterbereich zu schließen.

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 hier , um die Liste so zu filtern, dass 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 den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   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 Initiieren des Backupjobs auf  das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 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 dann 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 oder verweisen "SnapCenter Software Command Reference Guide" "SnapCenter Software Cmdlet Referenzhandbuch".