Sichern Sie Oracle-Datenbanken

SnapCenter software

NetApp
November 06, 2025

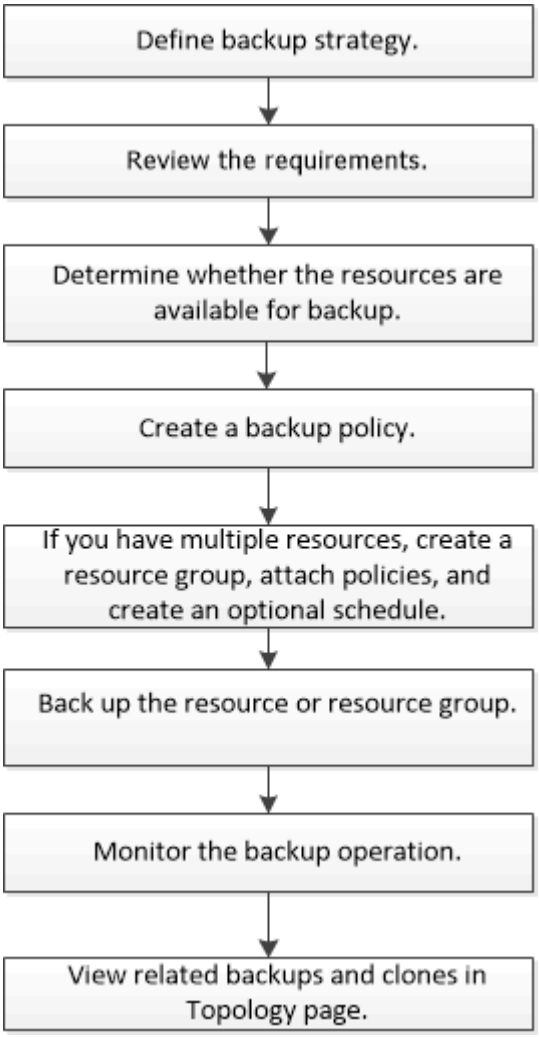
Inhalt

Sichern Sie Oracle-Datenbanken

Übersicht über das Backup-Verfahren

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Das Sicherungsverfahren umfasst die Planung, die Identifizierung der Ressourcen für die Sicherung, die Erstellung von Sicherungsrichtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Sicherungen und die Überwachung der Vorgänge.

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



Beim Erstellen einer Sicherung für Oracle-Datenbanken wird auf dem Oracle-Datenbankhost im Verzeichnis */var/opt/snapcenter/sco/lock* eine Betriebssperrdatei (*.sm_lock_dbsid*) erstellt, um zu vermeiden, dass mehrere Vorgänge auf der Datenbank ausgeführt werden. Nach der Sicherung der Datenbank wird die Betriebssperrdatei automatisch entfernt.

Wenn die vorherige Sicherung jedoch mit einer Warnung abgeschlossen wurde, wird die Betriebssperrdatei möglicherweise nicht gelöscht und der nächste Sicherungsvorgang wird in die Warteschlange gestellt. Es kann eventuell abgebrochen werden, wenn die Datei **.sm_lock_dbsid** nicht gelöscht wird. In einem solchen Szenario müssen Sie die Betriebssperrdatei manuell löschen, indem Sie die folgenden Schritte ausführen:

1. Navigieren Sie in der Eingabeaufforderung zu */var/opt/snapcenter/sco/lock*.
2. Löschen der Betriebssperre:`rm -rf .sm_lock_dbsid.`

Informationen zur Sicherungskonfiguration

Unterstützte Oracle-Datenbankkonfigurationen für Backups

SnapCenter unterstützt die Sicherung verschiedener Oracle-Datenbankkonfigurationen.

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

  Sie können nur Offline-Mount-Backups von Data Guard-Standbydatenbanken erstellen. Offline-Shutdown-Backup, reine Archivprotokoll-Backup und vollständige Backups werden nicht unterstützt.

- Oracle Active Data Guard-Standby

  Sie können nur Online-Backups von Active Data Guard-Standbydatenbanken erstellen. Nur Archivprotokollsicherungen und vollständige Sicherungen werden nicht unterstützt.

  Vor dem Erstellen einer Sicherung der Data Guard-Standby- oder Active Data Guard-Standby-Datenbank wird der verwaltete Wiederherstellungsprozess (MRP) gestoppt und nach der Erstellung der Sicherung wird MRP gestartet.

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

    Unter allen für Oracle-Datenbanken unterstützten Wiederherstellungsmethoden können Sie auf VMDK nur eine Connect-and-Copy-Wiederherstellung von ASM RAC-Datenbanken durchführen.

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

    PDB-Migrations- und PDB-Klonvorgänge werden nicht unterstützt.

  - Oracle Flex ASM

Die neuesten Informationen zu unterstützten Oracle-Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Unterstützte Sicherungstypen für Oracle-Datenbanken

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

Online-Backup

Eine Sicherung, die erstellt wird, wenn sich die Datenbank im Online-Zustand befindet, wird als Online-Sicherung bezeichnet. Mit einem Online-Backup, auch Hot-Backup genannt, können Sie eine Sicherung der Datenbank erstellen, ohne diese herunterzufahren.

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

- Nur Datendateien und Steuerdateien
- Nur Protokolldateien archivieren (die Datenbank wird in diesem Szenario nicht in den Sicherungsmodus versetzt)
- Vollständige Datenbank, die Datendateien, Steuerdateien und Archivprotokolldateien enthält

Offline-Backup

Eine Sicherung, die erstellt wird, während sich die Datenbank entweder im gemounteten oder heruntergefahrenen Zustand befindet, wird als Offline-Sicherung bezeichnet. Ein Offline-Backup wird auch als Cold Backup bezeichnet. Sie können in Offline-Backups nur Datendateien und Steuerdateien einschließen. Sie können entweder eine Offline-Mount- oder eine Offline-Shutdown-Sicherung erstellen.

- Beim Erstellen einer Offline-Mount-Sicherung müssen Sie sicherstellen, dass sich die Datenbank in einem gemounteten Zustand befindet.

  Wenn sich die Datenbank in einem anderen Zustand befindet, schlägt der Sicherungsvorgang fehl.

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

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

So erkennt SnapCenter Oracle-Datenbanken

Ressourcen sind Oracle-Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Sie können diese Datenbanken zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

In den folgenden Abschnitten wird der Prozess beschrieben, den SnapCenter zum Erkennen verschiedener Typen und Versionen von Oracle-Datenbanken verwendet.

Für Oracle-Versionen 11*g* bis 12*c*R1

RAC-Datenbank

Die RAC-Datenbanken werden nur auf der Grundlage von /etc/oratab`-Einträgen erkannt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Eigenständig

Die eigenständigen Datenbanken werden nur auf der Grundlage von /etc/oratab-Einträgen erkannt.

ASM

Der ASM-Instanzeintrag sollte in der Datei /etc/oratab verfügbar sein.

RAC Ein Knoten

Die RAC One Node-Datenbanken werden nur auf der Grundlage von /etc/oratab-Einträgen erkannt. Die Datenbanken sollten sich entweder im Status „nomount“, „mount“ oder „open“ befinden. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Der Datenbankstatus von RAC One Node wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt wurde und Sicherungen mit der Datenbank verknüpft sind.

Bei einer Datenbankverlagerung sollten Sie folgende Schritte durchführen:

1. Fügen Sie den verschobenen Datenbankeintrag manuell in die Datei /etc/oratab auf dem fehlgeschlagenen RAC-Knoten ein.
2. Aktualisieren Sie die Ressourcen manuell.
3. Wählen Sie auf der Ressourcenseite die RAC One Node-Datenbank aus und klicken Sie dann auf Datenbankeinstellungen.
4. Konfigurieren Sie die Datenbank, um die bevorzugten Clusterknoten auf den RAC-Knoten festzulegen, der derzeit die Datenbank hostet.
5. Führen Sie die SnapCenter -Vorgänge durch.
6. Wenn Sie eine Datenbank von einem Knoten auf einen anderen Knoten verschoben haben und der oratab-Eintrag im vorherigen Knoten nicht gelöscht wurde, löschen Sie den oratab-Eintrag manuell, um zu vermeiden, dass dieselbe Datenbank zweimal angezeigt wird.

Für Oracle-Versionen 12cR2 bis 18c, 19c oder 21c

RAC-Datenbank

Die RAC-Datenbanken werden mit dem Befehl „srvctl config“ erkannt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Eigenständig

Die eigenständigen Datenbanken werden anhand der Einträge in der Datei /etc/oratab und der Ausgabe des Befehls „srvctl config“ erkannt.

ASM

Der ASM-Instanzeintrag muss nicht in der Datei /etc/oratab enthalten sein.

RAC Ein Knoten

Die RAC One Node-Datenbanken werden nur mit dem Befehl „srvctl config“ erkannt. Die Datenbanken sollten sich entweder im Status „nomount“, „mount“ oder „open“ befinden. Der Datenbankstatus von RAC One Node wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt wurde und Sicherungen mit der Datenbank verknüpft sind.

Bei einer Verlagerung der Datenbank sollten Sie folgende Schritte durchführen: . Aktualisieren Sie die Ressourcen manuell. . Wählen Sie auf der Ressourcenseite die RAC One Node-Datenbank aus und klicken Sie dann auf Datenbankeinstellungen. . Konfigurieren Sie die Datenbank, um die bevorzugten Clusterknoten auf den RAC-Knoten festzulegen, der derzeit die Datenbank hostet. . Führen Sie die SnapCenter -Vorgänge durch.

Wenn in der Datei /etc/oratab Oracle 12*c*R2- und 18*c*-Datenbankeinträge vorhanden sind und dieselbe Datenbank mit dem Befehl srvctl config registriert ist, entfernt SnapCenter die doppelten Datenbankeinträge. Wenn veraltete Datenbankeinträge vorhanden sind, wird die Datenbank zwar erkannt, ist jedoch nicht erreichbar und hat den Status „Offline“.

Bevorzugte Knoten im RAC-Setup

Beim Einrichten von Oracle Real Application Clusters (RAC) können Sie die bevorzugten Knoten angeben, die SnapCenter zum Ausführen des Sicherungsvorgangs verwendet. Wenn Sie den bevorzugten Knoten nicht angeben, weist SnapCenter automatisch einen Knoten als bevorzugten Knoten zu und die Sicherung wird auf diesem Knoten erstellt.

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

Beispiel

Die RAC-Datenbank cdbrac hat drei Instanzen: cdbrac1 auf Knoten1, cdbrac2 auf Knoten2 und cdbrac3 auf Knoten3.

Die Instanzen node1 und node2 werden als bevorzugte Knoten konfiguriert, wobei node2 die erste Präferenz und node1 die zweite Präferenz ist. Wenn Sie einen Sicherungsvorgang durchführen, wird der Vorgang zuerst auf Knoten2 versucht, da dies der erste bevorzugte Knoten ist.

Wenn sich Knoten2 nicht im erforderlichen Status für die Sicherung befindet (was mehrere Gründe haben kann), z. B. dass der Plug-in-Agent auf dem Host nicht ausgeführt wird, die Datenbankinstanz auf dem Host sich nicht im erforderlichen Status für den angegebenen Sicherungstyp befindet oder die Datenbankinstanz auf Knoten2 in einer FlexASM-Konfiguration nicht von der lokalen ASM-Instanz bedient wird), wird der Vorgang auf Knoten1 versucht.

Der Knoten3 wird nicht für die Sicherung verwendet, da er nicht auf der Liste der bevorzugten Knoten steht.

Flex ASM-Setup

In einem Flex ASM-Setup werden Leaf-Knoten nicht als bevorzugte Knoten aufgeführt, wenn die Kardinalität geringer ist als die Anzahl der Knoten im RAC-Cluster. Wenn sich die Knotenrollen des Flex ASM-Clusters ändern, sollten Sie dies manuell feststellen, damit die bevorzugten Knoten aktualisiert werden.

Erforderlicher Datenbankstatus

Die RAC-Datenbankinstanzen auf den bevorzugten Knoten müssen sich im erforderlichen Zustand befinden, damit die Sicherung erfolgreich abgeschlossen werden kann:

- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im offenen Zustand befinden, um eine Onlinesicherung 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 eine Offline-Mount-Sicherung zu erstellen.
- RAC-Datenbankinstanzen können sich in jedem beliebigen Zustand befinden, Sie müssen jedoch die bevorzugten Knoten angeben, um eine Offline-Shutdown-Sicherung zu erstellen.

So katalogisieren Sie Backups mit Oracle Recovery Manager

Sie können die Sicherungen von Oracle-Datenbanken mit Oracle Recovery Manager (RMAN) katalogisieren, um die Sicherungsinformationen im Oracle RMAN-Repository zu speichern.

Die katalogisierten Sicherungen können später für die Wiederherstellung auf Blockebene oder für Point-in-Time-Wiederherstellungsvorgänge im Tablespace verwendet werden. Wenn Sie diese katalogisierten Sicherungen nicht benötigen, können Sie die Kataloginformationen entfernen.

Für die Katalogisierung muss die Datenbank im gemounteten oder höheren Zustand sein. Sie können Datensicherungen, Archivprotokollsicherungen und vollständige Sicherungen katalogisieren. Wenn die Katalogisierung für die Sicherung einer Ressourcengruppe mit mehreren Datenbanken aktiviert ist, wird die Katalogisierung für jede Datenbank durchgeführt. Bei Oracle RAC-Datenbanken wird die Katalogisierung auf dem bevorzugten Knoten durchgeführt, auf dem sich die Datenbank zumindest im gemounteten Zustand befindet.

Wenn Sie Sicherungen 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 Katalogisierungsvorgang fehl, anstatt in die Warteschlange gestellt zu werden.

Externe Katalogdatenbank

Standardmäßig wird die Steuerdatei der Zieldatenbank für die Katalogisierung verwendet. Wenn Sie eine externe Katalogdatenbank hinzufügen möchten, können Sie diese konfigurieren, indem Sie die Anmeldeinformationen und den Transparent Network Substrate (TNS)-Namen des externen Katalogs mithilfe des Datenbankeinstellungsassistenten der grafischen Benutzeroberfläche (GUI) von SnapCenter angeben. Sie können die externe Katalogdatenbank auch über die CLI konfigurieren, indem Sie den Befehl Configure-SmOracleDatabase mit den Optionen -OracleRmanCatalogCredentialName und -OracleRmanCatalogTnsName ausführen.

RMAN-Befehl

Wenn Sie die Katalogisierungsoption beim Erstellen einer Oracle-Sicherungsrichtlinie über die SnapCenter -GUI aktiviert haben, werden die Sicherungen im Rahmen des Sicherungsvorgangs mit Oracle RMAN katalogisiert. Sie können auch eine verzögerte Katalogisierung von Backups durchführen, indem Sie den `Catalog-SmBackupWithOracleRMAN` Befehl.

Nach der Katalogisierung der Backups können Sie die `Get-SmBackupDetails` Befehl zum Abrufen der katalogisierten Sicherungsinformationen, z. B. des Tags für katalogisierte Datendateien, des Katalogpfads der Steuerdatei und der Speicherorte der katalogisierten Archivprotokolle.

Benennungsformat

Wenn der Name der ASM-Datenträgergruppe größer oder gleich 16 Zeichen ist, lautet das für die Sicherung verwendete Namensformat ab SnapCenter 3.0 SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. Wenn der Name der Datenträgergruppe jedoch weniger als 16 Zeichen umfasst, lautet das für die Sicherung verwendete Namensformat DISKGROUPNAME_DBSID_BACKUPID. Dies ist dasselbe Format, das in SnapCenter 2.0 verwendet wird.

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

Crosscheck-Operationen

Sie können Gegenprüfungen durchführen, um veraltete RMAN-Repository-Informationen zu Sicherungen zu aktualisieren, deren Repository-Datensätze nicht mit ihrem physischen Status übereinstimmen. Wenn ein Benutzer beispielsweise archivierte Protokolle mit einem Betriebssystembefehl von der Festplatte entfernt, zeigt die Steuerdatei immer noch an, dass sich die Protokolle auf der Festplatte befinden, obwohl dies in Wirklichkeit nicht der Fall ist.

Durch die Gegenprüfung können Sie die Steuerdatei mit den Informationen aktualisieren. Sie können die Gegenprüfung aktivieren, indem Sie den Befehl „Set-SmConfigSettings“ ausführen und dem Parameter „ENABLE_CROSSCHECK“ den Wert „TRUE“ zuweisen. Der Standardwert ist auf FALSE gesetzt.

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

Kataloginformationen entfernen

Sie können die Kataloginformationen entfernen, indem Sie den Befehl Uncatalog-SmBackupWithOracleRMAN ausführen. Sie können die Kataloginformationen nicht über die SnapCenter -GUI entfernen. Allerdings werden Informationen zu einer katalogisierten Sicherung entfernt, wenn die Sicherung gelöscht wird oder wenn die mit dieser katalogisierten Sicherung verknüpfte Aufbewahrungs- und Ressourcengruppe gelöscht wird.

> Wenn Sie das Löschen des SnapCenter -Hosts erzwingen, werden die Informationen der mit diesem Host verknüpften katalogisierten Sicherungen nicht entfernt. Sie müssen Informationen aller katalogisierten Sicherungen für diesen Host entfernen, bevor Sie die Löschung des Hosts erzwingen.

Wenn das Katalogisieren und Entkatalogisieren fehlschlägt, weil die Vorgangszeit den für den Parameter ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT angegebenen Timeout-Wert 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 Dienst SnapCenter Plug-in Loader (SPL) neu, indem Sie den folgenden Befehl ausführen:

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

Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von Get-Help command_name. Alternativ können Sie sich an die "SnapCenter Software-Befehlsreferenzhandbuch" .

Vordefinierte Umgebungsvariablen für backupspezifisches Prescript und Postscript

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie beim Erstellen von Sicherungsrichtlinien das Prescript und Postscript ausführen. Diese Funktionalität wird für alle Oracle-Konfigurationen außer VMDK unterstützt.

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

Unterstützte vordefinierte Umgebungsvariablen zum Erstellen von Sicherungsrichtlinien

- **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 durch Pipe-Zeichen getrennte Datenbanknamen.

  Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

  Beispiel: NFSB32|NFSB31

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

  Bei RAC ist der Hostname der Name des Hosts, auf dem die Sicherung durchgeführt wird.

  Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

  Beispiel: scsmohost2.gdl.englabe.netapp.com

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

  Die Daten werden als <db1>@<osuser1>|<db2>@<osuser2> formatiert.

  Beispiel: NFSB31@oracle|NFSB32@oracle

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

  Die Daten werden als <db1>@<osgroup1>|<db2>@<osgroup2> formatiert.

  Beispiel: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE**" gibt den Sicherungstyp an (Online-Vollsicherung, Online-Daten, Online-Protokoll, Offline-Herunterfahren, Offline-Mount)

  Beispiele:

  - Für vollständige Sicherung: ONLINEFULL
  - Nur Datensicherung: ONLINEDATA
  - Für reine Protokollsicherung: ONLINELOG

- **SC_BACKUP_NAME** gibt den Namen der Sicherung an.

  Dieser Parameter wird für Anwendungsvolumes 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 Sicherungs-ID an.

  Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

  Beispiel: DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** gibt den Pfad des Oracle-Home-Verzeichnisses an.

  Beispiel: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|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: Stündlich|DATA@DAYS:3|LOG@COUNT:4
  - Für reine Datensicherung auf Abruf: Ondemand|DATA@COUNT:2
  - Für On-Demand-Protokollsicherung: Ondemand|LOG@COUNT:2
- **SC_RESOURCE_GROUP_NAME** gibt den Namen der Ressourcengruppe an.

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

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

  Beispiel: AV1|AV2
- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** gibt die Speicherzuordnung von SVM zum Volume für das Datendateiverzeichnis an. Dies ist der Name des übergeordneten Volumes für LUNs und Qtrees.

  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 zum Volume für das Protokolldateiverzeichnis an. Dies ist der Name des übergeordneten Volumes für LUNs und Qtrees.

  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 Datenträgers 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_07-21-2021_02.28.26.3973_1
  - Für mehrere Datenbankinstanzen: 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_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- **SC_PRIMARY_SNAPSHOT_NAMES** gibt die Namen der primären Snapshots an, die während der Sicherung 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 Konsistenzgruppen-Snapshots, 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 Mount-Point-Details an, die Teil der Sicherung sind.

  Die Details umfassen das Verzeichnis, in dem die Volumes bereitgestellt werden, und nicht das unmittelbar übergeordnete Verzeichnis der zu sichernden Datei. Bei einer ASM-Konfiguration ist dies der Name der Datenträgergruppe.

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

  Beispiele:

  - Für eine 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 Datenbankinstanz: 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
  - 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/nfsb32_log

- **SC_ARCHIVELOGS_LOCATIONS** gibt den Speicherort des Archivprotokollverzeichnisses an.

  Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Archivprotokolldateien. Wenn die Archivprotokolle an mehr als einem Ort abgelegt werden, werden alle Orte erfasst. Hierzu zählen

auch die FRA-Szenarien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

Beispiele:

- Für einzelne Datenbank auf NFS: /mnt/nfsdb2_log
- Für mehrere Datenbanken auf NFS und für die NFSB31-Datenbankarchivprotokolle, die an zwei verschiedenen Orten abgelegt werden: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
- Für ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** gibt den Speicherort des Redo-Log-Verzeichnisses an.

  Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Redo-Logdateien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

  Beispiele:

  - Für eine 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 Steuerdateiverzeichnisses an.

  Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Steuerdateien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

  Beispiele:

  - Für einzelne Datenbanken 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 Datendateiverzeichnisses an.

  Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Datendateien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

  Beispiele:

  - Für einzelne Datenbanken auf NFS: /mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
  - 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 Beschriftungen an.

  Beispiele: Stündlich, Täglich, Wöchentlich, Monatlich oder benutzerdefiniertes Etikett.

Unterstützte Trennzeichen

- **:** wird verwendet, um SVM-Name und Volume-Name zu trennen

  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_07-21-2021_02.28.26.3973_1

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

  Beispiele:

  - 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_07-21-2021_02.28.26.3973_1 |NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - NFSB31@oracle|NFSB32@oracle

- **|** wird verwendet, um die Daten zwischen zwei verschiedenen Datenbanken zu trennen und um die Daten zwischen zwei verschiedenen Entitäten für die Parameter SC_BACKUP_ID, SC_BACKUP_RETENTION und SC_BACKUP_NAME zu trennen.

  Beispiele:

  - DATEN@203|LOG@205
  - Stündlich|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

- **/** wird verwendet, um den Volumenamen von seinem Snapshot für die Parameter SC_PRIMARY_SNAPSHOT_NAMES und SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG zu trennen.

  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_07-21-2021_02.28.26.3973_1

- **,** wird verwendet, um Variablensätze für dieselbe Datenbank zu trennen.

  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_07-21-2021_02.28.26.3973_1 |NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie

aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.

Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

Sicherungszeitpläne

Die Sicherungshäufigkeit (Zeitplantyp) wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen. Beispielsweise können regelmäßige Sicherungen des Transaktionsprotokolls ausreichen, um sicherzustellen, dass Sie über die erforderlichen Sicherungen verfügen. Je häufiger Sie Ihre Datenbanken sichern, desto weniger Transaktionsprotokolle muss SnapCenter zum Zeitpunkt der Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

  Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können als Sicherungshäufigkeit für die Richtlinie stündlich, täglich, wöchentlich oder monatlich auswählen. Wenn Sie keine dieser Frequenzen auswählen, handelt es sich bei der erstellten Richtlinie um eine Nur-On-Demand-Richtlinie. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Sicherungszeitpläne

  Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer

Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Namenskonventionen für Backups

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
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 Bedeutung:

- *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 Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

Voraussetzungen für die Sicherung einer Oracle-Datenbank

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

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Sie sollten überprüft haben, dass alle zur Datenbank gehörenden Datenvolumes und Archivprotokollvolumes geschützt sind, wenn für diese Datenbank der sekundäre Schutz aktiviert ist.
- Sie sollten überprüft haben, dass sich die Datenbank mit Dateien auf den ASM-Datenträgergruppen entweder im Status „MOUNT“ oder „OPEN“ befindet, um ihre Sicherungen mit dem Oracle-Dienstprogramm DBVERIFY zu überprüfen.

- Sie sollten überprüft haben, dass die Länge des Volume-Mount-Punkts 240 Zeichen nicht überschreitet.
- Sie sollten den RESTTimeout-Wert in der Datei *C:\Program Files\ NetApp \SMCore\SMCoreServiceHost.exe.config* im SnapCenter Server-Host auf 86400000 ms erhöhen, wenn die zu sichernde Datenbank groß ist (Größe in TB).

  Stellen Sie beim Ändern der Werte sicher, dass keine Jobs ausgeführt werden, und starten Sie den SnapCenter SMCore-Dienst nach dem Erhöhen des Werts neu.

Entdecken Sie für die Sicherung verfügbare Oracle-Datenbanken

Ressourcen sind Oracle-Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Sie können diese Datenbanken zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

Bevor Sie beginnen

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

  Weitere Informationen finden Sie unter "Bereitstellen des SnapCenter Plug-in for VMware vSphere" .
- Wenn sich Datenbanken auf einem VMDK-Dateisystem befinden, müssen Sie sich bei vCenter angemeldet und zu **VM-Optionen** > **Erweitert** > **Konfiguration bearbeiten** navigiert haben, um den Wert von *disk.enableUUID* für die VM auf „true“ zu setzen.
- Sie müssen den Prozess überprüft haben, dem SnapCenter folgt, um verschiedene Typen und Versionen von Oracle-Datenbanken zu erkennen.

Schritt 1: Verhindern, dass SnapCenter Einträge erkennt, die nicht in der Datenbank enthalten sind

Sie können verhindern, dass SnapCenter in der oratab-Datei hinzugefügte Einträge erkennt, die nicht zur Datenbank gehören.

Schritte

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

   Erteilen Sie dem Oracle-Binärbesitzer und der Gruppe die Schreibberechtigung, damit die Datei in Zukunft verwaltet werden kann.

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

   Es wird empfohlen, dasselbe Format beizubehalten, das für die Nicht-Datenbankeinträge in der Datei */etc/oratab* definiert ist. Alternativ kann der Benutzer einfach die Nicht-Datenbank-Entitätszeichenfolge hinzufügen.

Bei der Zeichenfolge wird zwischen Groß- und Kleinschreibung unterschieden. 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 in **sc_oratab.config** hinzugefügten Nicht-Datenbankeinträge werden nicht auf der Ressourcenseite aufgeführt.

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

Schritt 2: Ressourcen entdecken

Nach der Installation des Plug-Ins werden alle Datenbanken auf diesem Host automatisch erkannt und auf der Ressourcenseite angezeigt.

Damit die Erkennung der Datenbanken erfolgreich ist, sollten sich die Datenbanken mindestens im gemounteten Zustand oder höher befinden. In einer Oracle Real Application Clusters (RAC)-Umgebung muss sich die RAC-Datenbankinstanz auf dem Host, auf dem die Erkennung durchgeführt wird, mindestens im gemounteten Zustand oder höher befinden, damit die Erkennung der Datenbankinstanz erfolgreich ist. Nur die erfolgreich erkannten Datenbanken können den Ressourcengruppen hinzugefügt werden.

Wenn Sie eine Oracle-Datenbank auf dem Host gelöscht haben, wird SnapCenter Server dies nicht bemerken und die gelöschte Datenbank auflisten. Sie sollten die Ressourcen manuell aktualisieren, um die SnapCenter Ressourcenliste 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 Filtersymbol] und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern. Sie können dann auf das Symbol imagfilter_icon.gif[Filtersymbol]_icon.png[] klicken, um den Filterbereich zu schließen.

3. Klicken Sie auf **Ressourcen aktualisieren**.

In einem RAC One Node-Szenario 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 Clustername, zugehörigen 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 Nicht- NetApp -Speichersystem befindet, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ die Meldung „Nicht für Sicherung verfügbar“ an.

  Sie können keine Datenschutzvorgänge für die Datenbank durchführen, die sich auf einem Nicht- NetApp -Speichersystem befindet.

- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und nicht geschützt ist, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ die Meldung „Nicht geschützt“ an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ die Meldung „Für Sicherung verfügbar“ an.

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

Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken

Bevor Sie SnapCenter zum Sichern von Oracle-Datenbankressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren. Sie können auch die Replikations-, Skript- und Sicherungstypeinstellungen angeben. Das Erstellen einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressource oder Ressourcengruppe wiederverwenden möchten.

Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.
- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erkennen von Datenbanken und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel- oder Tresor-Sekundärspeicher replizieren, muss der SnapCenter Administrator Ihnen die SVMs sowohl für das Quell- als auch für das Zielvolume zugewiesen haben.
- Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.
- Überprüfen Sie die spezifischen Voraussetzungen und Einschränkungen der SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektlimits für SnapMirror Active Sync" .

Informationen zu diesem Vorgang

Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.

+ Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.

+ Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie **Oracle-Datenbank** aus der Dropdown-Liste.
4. Klicken Sie auf **Neu**.
5. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
6. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:

    a. Wählen Sie Ihren Speichertyp aus.

    b. Wählen Sie den Richtlinienbereich aus:

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

          Sie müssen angeben, ob Sie alle Datendateien, Steuerdateien und Archivprotokolldateien, nur Datendateien und Steuerdateien oder nur Archivprotokolldateien sichern möchten.

        - Wenn Sie **eine Offline-Sicherung erstellen** möchten, wählen Sie **Offline-Sicherung** und dann eine der folgenden Optionen:

            - Wenn Sie eine Offlinesicherung erstellen möchten, während sich die Datenbank im gemounteten Zustand befindet, wählen Sie **Mount**.
            - Wenn Sie eine Offline-Shutdown-Sicherung erstellen möchten, indem Sie die Datenbank in den Shutdown-Status versetzen, wählen Sie **Shutdown**.

              Wenn Sie über Pluggable Databases (PDBs) verfügen und den Status der PDBs vor dem Erstellen der Sicherung speichern möchten, müssen Sie **Status der PDBs speichern** auswählen. Dadurch können Sie die PDBs nach der Erstellung des Backups in ihren ursprünglichen Zustand zurückversetzen.

    c. Wenn Sie die Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren**.

       Sie können die verzögerte Katalogisierung für jeweils eine Sicherung entweder über die GUI oder über den SnapCenter -CLI-Befehl Catalog-SmBackupWithOracleRMAN durchführen.

       Wenn Sie Sicherungen 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 Katalogisierungsvorgang fehl, anstatt in die Warteschlange gestellt zu werden.

d. Wenn Sie Archivprotokolle nach der Sicherung bereinigen möchten, wählen Sie **Archivprotokolle nach der Sicherung bereinigen**.

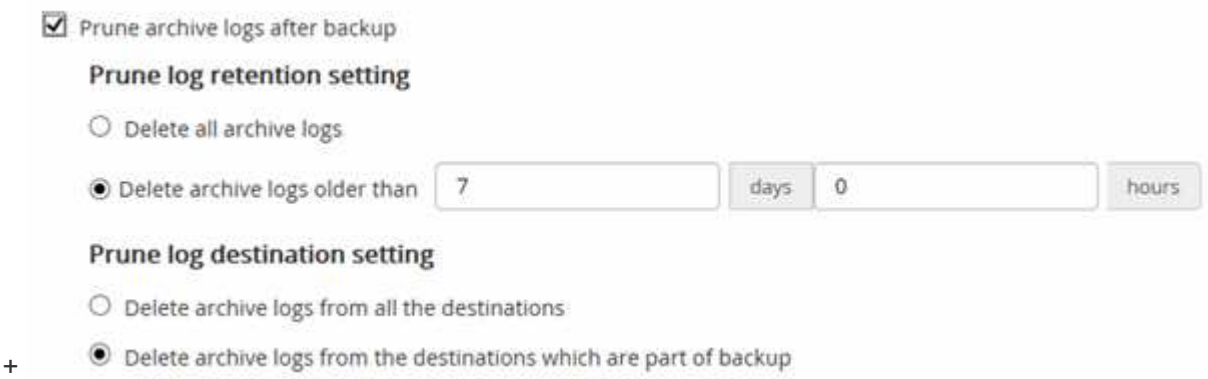
Das Bereinigen von Archivprotokollen aus dem Archivprotokollziel, das in der Datenbank nicht konfiguriert ist, wird übersprungen.

Wenn Sie Oracle Standard Edition verwenden, können Sie beim Durchführen einer Archivprotokollsicherung 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 Archivprotokollspeicherorte zugreifen können, damit der Löschvorgang erfolgreich ist.

Wenn Sie wollen…	**Dann…**
Alle Archivprotokolle löschen	Wählen Sie **Alle Archivprotokolle löschen**.
Löschen Sie ältere Archivprotokolle	Wählen Sie **Archivprotokolle löschen, die älter sind als** und geben Sie dann das Alter der zu löschenden Archivprotokolle in Tagen und Stunden an.
Archivprotokolle von allen Zielen löschen	Wählen Sie **Archivprotokolle von allen Zielen löschen**.
Löschen Sie die Archivprotokolle aus den Protokollzielen, die Teil der Sicherung sind	Wählen Sie **Archivprotokolle aus den Zielen löschen, die Teil der Sicherung sind**.



+

7. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:

a. Geben Sie die Zeitplanhäufigkeit an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.

Sie können den Zeitplan (Startdatum und Enddatum) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.

Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

a. Geben Sie im Abschnitt „Einstellungen für die Aufbewahrung von Daten-Snapshots“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

Wenn Sie wollen…	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots	Wählen Sie **Zu behaltende Kopien** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden. Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden ONTAP Version unterstützt wird. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Kopien aufbewahren für** und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.

Sperrzeitraum für Snapshot-Kopien	Wählen Sie den **Sperrzeitraum für die Snapshot-Kopie** und geben Sie die Dauer in Tagen, Monaten oder Jahren an. Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.

b. Geben Sie im Abschnitt „Aufbewahrungseinstellungen für Archivprotokoll-Snapshots“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

Wenn Sie wollen…	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots	Wählen Sie **Zu behaltende Kopien** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden. Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden ONTAP Version unterstützt wird. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Kopien aufbewahren für** und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.

Sperrzeitraum für Snapshot-Kopien	Wählen Sie den **Sperrzeitraum für die Snapshot-Kopie** und geben Sie die Dauer in Tagen, Monaten oder Jahren an. Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.

c. Wählen Sie die Richtlinienbezeichnung aus.

> Sie können primären Snapshots SnapMirror Labels für die Remote-Replikation zuweisen, sodass die primären Snapshots den Snapshot-Replikationsvorgang von SnapCenter auf sekundäre ONTAP -Systeme auslagern können. Dies kann erfolgen, ohne die Option SnapMirror oder SnapVault auf der Richtlinienseite zu aktivieren.

8. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

> Sie müssen die sekundären Replikationsoptionen für den **Sperrzeitraum für sekundäre Snapshot-Kopien** auswählen, damit diese wirksam werden.

Für dieses Feld…	**Machen Sie Folgendes…**
Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots	Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation). Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden. Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.

Für dieses Feld…	Machen Sie Folgendes…
Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups). Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird. Weitere Informationen zu SnapLock Vault finden Sie unter "Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel" Sehen "Anzeigen von Oracle-Datenbanksicherungen und -klonen auf der Seite „Topologie“" .
Fehleranzahl der Wiederholungsversuche	Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

9. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das Sie vor bzw. nach dem Sicherungsvorgang ausführen möchten.

   Sie müssen die Prescripts und Postscripts entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

   Sie können auch den Timeout-Wert des Skripts angeben. Der Standardwert beträgt 60 Sekunden.

   SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen."Mehr erfahren"

10. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

    a. Wählen Sie den Sicherungszeitplan aus, für den Sie den Überprüfungsvorgang durchführen möchten.
    b. Geben Sie im Abschnitt „Befehle des Überprüfungsskripts“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das Sie vor bzw. nach dem Überprüfungsvorgang ausführen möchten.

       Sie müssen die Prescripts und Postscripts entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

Sie können auch den Timeout-Wert des Skripts angeben. Der Standardwert beträgt 60 Sekunden.

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

Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Oracle-Datenbanken hinzu

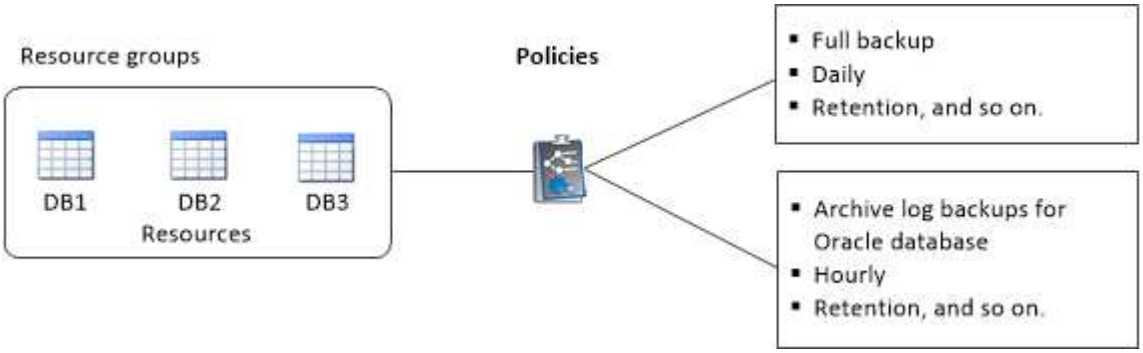
Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern.

Informationen zu diesem Vorgang

- Eine Datenbank mit Dateien in ASM-Datenträgergruppen muss sich im Status „MOUNT“ oder „OPEN“ befinden, um ihre Sicherungen mit dem Oracle-Dienstprogramm DBVERIFY zu überprüfen.

  Fügen Sie der Ressourcengruppe eine oder mehrere Richtlinien hinzu, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

  Die folgende Abbildung veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



- Wenn Sie für SnapLock -fähige Richtlinien für ONTAP 9.12.1 und niedrigere Versionen eine Snapshot-Sperrdauer angeben, erben die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellten Klone die SnapLock Ablaufzeit. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.
- Das Hinzufügen neuer Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Zustand Ressourcen hinzufügen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und 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 aus:
   a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

   Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

   Sie sollten genau dasselbe Ziel verwenden, das in Oracle festgelegt wurde, einschließlich Präfix, falls erforderlich.

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

   Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die Ressourcen aus dem Abschnitt „Verfügbare 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. Wählen Sie auf der Seite „Anwendungseinstellungen“ die Sicherungsoption aus.
7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

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

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

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
   a. Klicken Sie auf **Locators laden**, um die SnapMirror oder SnapVault -Volumes zu laden und die Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
   c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

   d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.
   e. Klicken Sie auf **OK**.

      Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

   ⓘ Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Oracle-Ressourcen auf ASA R2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA R2-Systemen befinden. Sie können den sekundären Schutz auch beim Erstellen der Ressourcengruppe bereitstellen.

Bevor Sie beginnen

- Sie sollten sicherstellen, dass Sie nicht sowohl ONTAP 9.x-Ressourcen als auch ASA r2-Ressourcen zur

gleichen Ressourcengruppe hinzufügen.

- Sie sollten sicherstellen, dass Sie keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen haben.

Informationen zu diesem Vorgang

- Der sekundäre Schutz ist nur verfügbar, wenn dem angemeldeten Benutzer die Rolle zugewiesen ist, für die die Funktion **SecondaryProtection** aktiviert ist.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nachdem die primäre und sekundäre Konsistenzgruppe erstellt wurden, wird der Wartungsmodus der Ressourcengruppe beendet.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und 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 aus:
   a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

   b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

      Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

   c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

      Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

   d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

      Sie sollten genau dasselbe Ziel verwenden, das in der Anwendung festgelegt wurde, gegebenenfalls einschließlich Präfix.

4. Wählen Sie auf der Seite „Ressourcen“ den Datenbank-Hostnamen aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die ASA r2-Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.
6. Wählen Sie auf der Seite „Anwendungseinstellungen“ die Sicherungsoption aus.
7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

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

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

b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Wenn der sekundäre Schutz für die von Ihnen ausgewählte Richtlinie aktiviert ist, wird die Seite „Sekundärer Schutz“ angezeigt und Sie müssen die folgenden Schritte ausführen:

a. Wählen Sie den Typ der Replikationsrichtlinie aus.

Die synchrone Replikationsrichtlinie wird nicht unterstützt.

b. Geben Sie das Konsistenzgruppensuffix an, das Sie verwenden möchten.

c. Wählen Sie aus den Dropdown-Menüs „Zielcluster“ und „Ziel-SVM“ den Peering-Cluster und die SVM aus, die Sie verwenden möchten.

Das Cluster- und SVM-Peering wird von SnapCenter nicht unterstützt. Sie sollten System Manager oder ONTAP CLIs verwenden, um Cluster- und SVM-Peering durchzuführen.

Wenn die Ressourcen bereits außerhalb von SnapCenter geschützt sind, werden diese Ressourcen im Abschnitt „Sekundär geschützte Ressourcen“ angezeigt.

1. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

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

b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.

c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.

e. Klicken Sie auf **OK**.

Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

3. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Sichern von Oracle-Ressourcen

Wenn eine Ressource nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

Schritte

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

Sie können dann auf , um den Filterbereich zu schließen.

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

Die Seite „Datenbank schützen“ wird angezeigt.

5. Führen Sie auf der Seite „Ressourcen“ die folgenden Schritte aus:

a. Aktivieren Sie das Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Zum Beispiel, `customtext_policy_hostname` oder `resource_hostname` . Dem Snapshot-Namen wird standardmäßig ein Zeitstempel angehängt.

b. 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 Dropdownliste aus.

      Sie können eine Richtlinie erstellen, indem Sie auf + .

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

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um einen Zeitplan für die gewünschte Richtlinie zu konfigurieren.

   c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und wählen Sie dann `OK` .

      policy_name ist der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

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

   a. Klicken Sie auf **Locators laden**, um die SnapMirror oder SnapVault -Volumes zu laden und den sekundären Speicher zu überprüfen.

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren. + Im Dialogfeld „Verifizierungszeitpläne hinzufügen *Richtlinienname*“ können Sie die folgenden Schritte ausführen:

   c. Wählen Sie **Überprüfung nach Sicherung ausführen**.

   d. Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie den Zeitplantyp aus der Dropdownliste aus.

      In einem Flex ASM-Setup können Sie keine Überprüfungsvorgänge an Blattknoten durchführen, wenn die Kardinalität kleiner ist als die Anzahl der Knoten im RAC-Cluster.

   e. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Backups auf dem sekundären Speicher zu überprüfen.

   f. Klicken Sie auf **OK**.

      Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

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

   Sie müssen die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den für die Ressource durchgeführten Sicherungsvorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

   Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl angegeben haben. `Set-SmSmtpServer` .

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

   Die Seite „Datenbanktopologie“ wird angezeigt.

10. Klicken Sie auf **Jetzt sichern**.
11. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdownliste „Richtlinie“ die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

       Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

    b. Klicken Sie auf **Sichern**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Nach Abschluss

- Im AIX-Setup können Sie die `lkdev` Befehl zum Sperren und die `rendev` Befehl zum Umbenennen der Datenträger, auf denen sich die gesicherte Datenbank befand.

  Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mithilfe dieser Sicherung durchführen.

- Wenn der Sicherungsvorgang 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 den `Set-SmConfigSettings` Cmdlet:

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

- Wenn während des Überprüfungsprozesses nicht auf die Datei zugegriffen werden kann und der Einhängepunkt nicht verfügbar ist, schlägt der Vorgang möglicherweise mit dem Fehlercode DBV-00100 für die angegebene Datei fehl. 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 (SPL)-Dienst neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

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

  Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei */opt/netapp/init_scripts/scvservice*. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M .`

Weitere Informationen

- "SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"

- "Die Oracle RAC One Node-Datenbank wird für die Durchführung von SnapCenter -Vorgängen übersprungen"
- "Der Status einer Oracle 12c ASM-Datenbank konnte nicht geändert werden"
- "Anpassbare Parameter für Sicherungs-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"(Anmeldung erforderlich)

Sichern von Oracle-Datenbankressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Der Sicherungsvorgang wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden Sicherungen gemäß dem Zeitplan erstellt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Geben Sie den Namen der Ressourcengruppe in das Suchfeld ein oder klicken Sie auf und wählen Sie das Tag aus.

   Klicken , um den Filterbereich zu schließen.
4. Wählen Sie auf der Seite „Ressourcengruppe“ die zu sichernde Ressourcengruppe aus.

   Wenn Sie über eine föderierte Ressourcengruppe mit zwei Datenbanken verfügen und eine davon Daten auf einem Nicht- NetApp -Speicher enthält, wird der Sicherungsvorgang abgebrochen, obwohl sich die andere Datenbank auf einem NetApp -Speicher befindet.
5. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
   a. Wenn der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die gewünschte Sicherungsrichtlinie aus.

      Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

   b. Wählen Sie **Backup**.
6. Überwachen Sie den Fortschritt, indem Sie **Überwachen > Jobs** auswählen.

Nach Abschluss

- Im AIX-Setup können Sie die `lkdev` Befehl zum Sperren und die `rendev` Befehl zum Umbenennen der Datenträger, auf denen sich die gesicherte Datenbank befand.

  Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mithilfe dieser Sicherung durchführen.
- Wenn der Sicherungsvorgang 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 den `Set-SmConfigSettings` Cmdlet:

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

- Wenn während des Überprüfungsprozesses nicht auf die Datei zugegriffen werden kann und der Einhängepunkt nicht verfügbar ist, schlägt der Vorgang möglicherweise mit dem Fehlercode DBV-00100 für die angegebene Datei fehl. 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 (SPL)-Dienst neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

Überwachen der Oracle-Datenbanksicherung

Erfahren Sie, wie Sie den Fortschritt von Sicherungs- und Datenschutzvorgängen überwachen.

Überwachen von Oracle-Datenbanksicherungsvorgängen

Sie können den Fortschritt verschiedener Sicherungsvorgänge mithilfe der SnapCenterJobs-Seite überwachen. Möglicherweise möchten Sie den Fortschritt überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

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

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

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 um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.

e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.

4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.

> Obwohl der Status des Sicherungsauftrags angezeigt wird ✔ Wenn Sie auf die Auftragsdetails klicken, sehen Sie möglicherweise, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt werden oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

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

Überwachen von Datenschutzvorgängen im Aktivitätsbereich

Im Aktivitätsbereich werden die fünf zuletzt ausgeführten Vorgänge angezeigt. Im Aktivitätsbereich wird auch angezeigt, wann der Vorgang gestartet wurde und welchen Status er hat.

Im Aktivitätsbereich werden Informationen zu Sicherungs-, Wiederherstellungs-, Klon- und geplanten Sicherungsvorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Auftragsdetails** aufgelistet.

Andere Sicherungsvorgänge

Sichern Sie Oracle-Datenbanken mit UNIX-Befehlen

Der Sicherungsworkflow umfasst die Planung, die Identifizierung der Ressourcen für die Sicherung, die Erstellung von Sicherungsrichtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Sicherungen und die Überwachung der Vorgänge.

Was Sie brauchen

- Sie sollten die Speichersystemverbindungen hinzugefügt und die Anmeldeinformationen mit den Befehlen *Add-SmStorageConnection* und *Add-SmCredential* erstellt haben.
- Sie sollten die Verbindungssitzung mit dem SnapCenter -Server mit dem Befehl *Open-SmConnection* hergestellt haben.

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

Die Verbindungssitzung ist nur 24 Stunden gültig. Sie können jedoch mit der Option „TokenNeverExpires“ ein Token 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, eine Sicherung durchzuführen und die Sicherung zu überprüfen.

Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von Get-Help *command_name*. Alternativ können Sie auch auf die "SnapCenter Software-Befehlsreferenzhandbuch" .

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer: *Open-SmConnection*
2. Führen Sie den Vorgang zur Erkennung von Hostressourcen durch: *Get-SmResources*
3. Konfigurieren Sie die Anmeldeinformationen und bevorzugten Knoten der Oracle-Datenbank für den Sicherungsvorgang einer Real Application Cluster (RAC)-Datenbank: *Configure-SmOracleDatabase*
4. Erstellen Sie eine Sicherungsrichtlinie: *Add-SmPolicy*
5. Rufen Sie die Informationen zum sekundären Speicherort (SnapVault oder SnapMirror) ab: *Get-SmSecondaryDetails*

   Dieser Befehl ruft die Zuordnungsdetails zwischen Primär- und Sekundärspeicher einer angegebenen Ressource ab. Sie können die Zuordnungsdetails verwenden, um die sekundären Überprüfungseinstellungen beim Erstellen einer Sicherungsressourcengruppe zu konfigurieren.
6. Fügen Sie SnapCenter eine Ressourcengruppe hinzu: *Add-SmResourceGroup*
7. Erstellen Sie ein Backup: *New-SmBackup*

   Sie können den Job mit der Option „WaitForCompletion“ abfragen. Wenn diese Option angegeben ist, fragt der Befehl den Server weiterhin ab, bis der Sicherungsauftrag abgeschlossen ist.
8. Rufen Sie die Protokolle von SnapCenter ab: *Get-SmLogs*

Abbrechen von Sicherungsvorgängen von Oracle-Datenbanken

Sie können Sicherungsvorgänge abbrechen, die entweder ausgeführt werden, in der Warteschlange stehen oder nicht reagieren.

Sie müssen als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Sicherungsvorgänge abzubrechen.

Über diese Aufgabe

Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter Server den Vorgang und entfernt alle Snapshots aus dem Speicher, wenn die erstellte Sicherung nicht beim SnapCenter -Server registriert ist. Wenn die Sicherung bereits beim SnapCenter Server registriert ist, wird der bereits erstellte Snapshot auch nach dem Auslösen des Abbruchs nicht zurückgesetzt.

- Sie können nur Protokoll- oder vollständige Sicherungsvorgänge abbrechen, die sich in der Warteschlange befinden oder ausgeführt werden.
- Sie können den Vorgang nicht mehr abbrechen, nachdem die Überprüfung begonnen hat.

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

- Sie können den Sicherungsvorgang nicht abbrechen, nachdem die Katalogvorgänge gestartet wurden.
- Sie können einen Sicherungsvorgang entweder auf der Seite „Überwachen“ oder im Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter -GUI können Sie CLI-Befehle verwenden, um Vorgänge abzubrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitorseite	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 Sicherungsauftrags auf im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite „Auftragsdetails“ auf **Auftrag abbrechen**.

Ergebnisse

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

Wenn der von Ihnen abgebrochene Vorgang im Status „Abbrechen“ oder „Ausführen“ nicht reagiert, sollten Sie „Cancel-SmJob -JobID <int> -Force“ ausführen, um den Sicherungsvorgang zwangsweise zu beenden.

Anzeigen von Oracle-Datenbanksicherungen und -klonen auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzuzeigen.

Über diese Aufgabe

Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

Sie können die folgenden Symbole in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die Sicherungen und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).

-  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 Speicher gespiegelt werden.
-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.

  Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups. Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.

Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

Wenn Sie eine sekundäre Beziehung als SnapMirror Active Sync haben (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), können Sie die folgenden zusätzlichen Symbole sehen:

-  Die Replikationssite ist aktiv.
-  Die Replikationssite ist ausgefallen.
-  Die sekundäre Spiegel- oder Tresorbeziehung wurde nicht wiederhergestellt.

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 die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Ressourcendetailansicht oder aus der Ressourcengruppendetailansicht aus.

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

4. Überprüfen Sie die Karte „Zusammenfassung“, um eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen und Klone anzuzeigen.

   Im Abschnitt „Zusammenfassungskarte“ wird die Gesamtzahl der Sicherungen und Klone sowie die Gesamtzahl der Protokollsicherungen angezeigt.

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

   Wenn eine SnapLock -fähige Sicherung durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock aktualisiert. Ein wöchentlicher Zeitplan aktualisiert auch die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock .

   Wenn die Anwendungsressource auf mehrere Volumes verteilt ist, entspricht die SnapLock -Ablaufzeit für die Sicherung der längsten SnapLock -Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock -Ablaufzeit wird von ONTAP abgerufen.

   Bei der aktiven Synchronisierung von SnapMirror wird durch Klicken auf die Schaltfläche **Aktualisieren** das SnapCenter -Sicherungsinventar aktualisiert, indem ONTAP sowohl nach primären als auch nach Replikationsstandorten abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken aus, die eine aktive Synchronisierungsbeziehung mit SnapMirror enthalten.

   - Für SnapMirror Active Sync und nur für ONTAP 9.14.1 sollten Async Mirror- oder Async MirrorVault-Beziehungen zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault automatisch auf das neue primäre Ziel konfiguriert.
   - Nach dem Failover sollte ein Backup für SnapCenter erstellt werden, um über das Failover informiert zu sein. Sie können erst auf **Aktualisieren** klicken, nachdem eine Sicherung erstellt wurde.

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

   Die Details der Backups und Klone werden in einem Tabellenformat angezeigt.

6. Wählen Sie die Sicherung aus der Tabelle aus und klicken Sie dann auf die Datenschutzsymbole, um Vorgänge wie Wiederherstellen, Klonen, Mounten, Unmounten, Umbenennen, Katalogisieren, Dekatalogisieren und Löschen durchzuführen.

   Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch löschen.

   - Wenn Sie eine Protokollsicherung ausgewählt haben, können Sie nur die Vorgänge Umbenennen, Einbinden, Aufheben der Einbindung, Katalogisieren, Auskatalogisieren und Löschen durchführen.
   - Wenn Sie die Sicherung mit Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Sicherungen nicht umbenennen.

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

Wenn der SnapmirrorStatusUpdateWaitTime zugewiesene Wert kleiner ist, werden die Mirror- und Vault-Sicherungskopien nicht auf der Topologieseite aufgeführt, selbst wenn Daten- und Protokollvolumes erfolgreich geschützt wurden. Sie sollten den SnapmirrorStatusUpdateWaitTime zugewiesenen Wert mithilfe des PowerShell-Cmdlets *Set-SmConfigSettings* erhöhen.

Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie

durch Ausführen von Get-Help *command_name*.

Alternativ können Sie auch auf die "SnapCenter Software-Befehlsreferenzhandbuch" oder "Referenzhandbuch für SnapCenter -Software-Cmdlets" .