



Installation und Einrichtung von UNIX für Clustered Data ONTAP

SnapManager for SAP

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/de-de/snapmanager-sap/unix-installation-cmode/reference-smsap-isg-snapmanager-architecture.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

- Installation und Einrichtung von UNIX für Clustered Data ONTAP 1
 - Produktübersicht 1
 - Implementierungs-Workflow 3
 - Vorbereitungen für die Implementierung 4
 - Konfigurieren von Datenbanken 7
 - Installation von SnapManager 10
 - SnapManager einrichten 13
 - Vorbereiten der Speichersysteme für die SnapMirror- und SnapVault-Replizierung 16
 - Sichern und Überprüfen Ihrer Datenbanken 20
 - Deinstallieren Sie die Software von einem UNIX-Host 30
 - Upgrade von SnapManager 30
 - Weitere Schritte 43

Installation und Einrichtung von UNIX für Clustered Data ONTAP

Produktübersicht

SnapManager für SAP automatisiert und vereinfacht komplexe, manuelle und zeitintensive Prozesse, die im Zusammenhang mit Backup, Recovery und dem Klonen von Datenbanken anfallen. Mithilfe von SnapManager mit ONTAP SnapMirror Technologie können Sie Backup-Kopien auf einem anderen Volume erstellen. Mit der ONTAP SnapVault Technologie werden Backups effizient auf Festplatten archiviert.

SnapManager bietet die erforderlichen Tools wie OnCommand Unified Manager und die Integration mit den SAP BR* Tools für richtlinienbasiertes Datenmanagement, die Planung und Erstellung regelmäßiger Datenbank-Backups und die Wiederherstellung von Daten aus diesen Backups im Falle eines Datenverlusts oder Notfalls.

SnapManager lässt sich auch mit nativen Oracle Technologien wie Oracle Real Application Clusters (Oracle RAC) und Oracle Recovery Manager (RMAN) integrieren, um Backup-Informationen zu erhalten. Diese Backups können zu einem späteren Zeitpunkt in Restores auf Blockebene oder in Tablespace zu zeitpunktgenauen Recovery-Vorgängen verwendet werden.

SnapManager Highlights

SnapManager ermöglicht die nahtlose Integration mit Datenbanken auf dem UNIX Host sowie mit den Technologien Snapshot, SnapRestore und FlexClone am Backend. Es bietet eine benutzerfreundliche Oberfläche (UI) und eine Befehlszeilenschnittstelle (CLI) für Administrationsfunktionen.

Mit SnapManager können Sie folgende Datenbankvorgänge ausführen und Daten effizient managen:

- Erstellung platzsparender Backups auf primärem oder sekundärem Storage

SnapManager ermöglicht Ihnen ein separates Backup der Datendateien und die Archivierung von Protokolldateien.

- Planen von Backups
- Wiederherstellung vollständiger oder partieller Datenbanken unter Verwendung eines dateibasierten oder Volume-basierten Restore-Vorgangs
- Wiederherstellung von Datenbanken durch Erkennung, Mounten und Anwendung von Archivprotokolldateien aus Backups
- Beschneiden von Archiv-Log-Dateien von Archiv-Protokollzielen bei der Erstellung von Backups nur der Archivprotokolle
- Automatische Aufbewahrung einer minimalen Anzahl von Archiv-Log-Backups, da nur die Backups gespeichert werden, die eindeutige Archivprotokolldateien enthalten
- Verfolgung von Betriebsdetails und Erstellung von Berichten
- Backup wird überprüft, um sicherzustellen, dass sich Backups in einem gültigen Blockformat befinden und dass keine der gesicherten Dateien beschädigt sind
- Pflegen eines Verlaufs von Vorgängen, die im Datenbankprofil durchgeführt werden

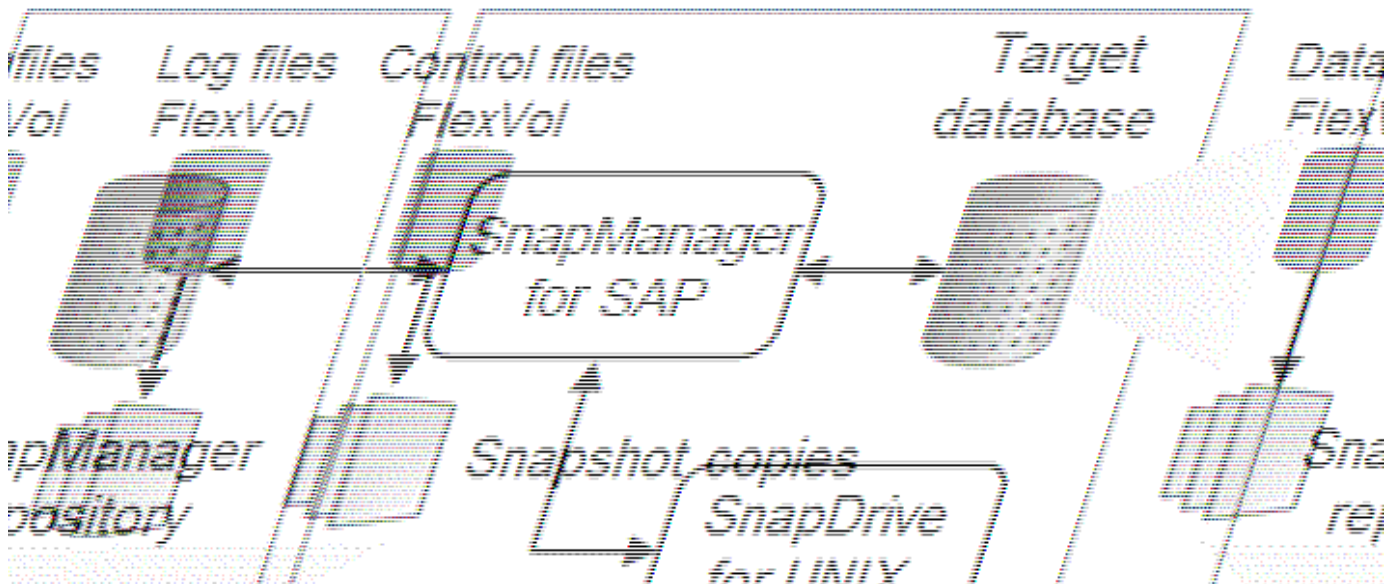
Ein Profil enthält Informationen über die Datenbank, die von SnapManager gemanagt werden soll.

- Sicherung von Backups auf sekundären Storage-Systemen.
- Erstellung platzsparender Backup-Klone auf primärem oder sekundärem Storage

SnapManager ermöglicht Ihnen die Aufteilung eines Datenbankklonen.

Architektur von SnapManager

SnapManager für SAP enthält Komponenten, die gemeinsam eine umfassende und leistungsstarke Backup-, Restore-, Recovery- und Klonlösung für Oracle Datenbanken bereitstellen.



SnapDrive für UNIX

SnapManager benötigt SnapDrive, um die Verbindung zum Storage-System herzustellen. Sie müssen SnapDrive for UNIX auf jedem Ziel-Datenbank-Host installieren, bevor Sie SnapManager installieren.

SnapManager für SAP

Sie müssen SnapManager für SAP auf jedem Ziel-Datenbank-Host installieren.

Sie können entweder die Befehlszeilenschnittstelle (CLI) oder die Benutzeroberfläche vom Datenbank-Host verwenden, auf dem SnapManager für SAP installiert ist. Sie können die SnapManager-Benutzeroberfläche auch Remote verwenden, indem Sie einen Webbrowser von jedem System verwenden, das auf einem von SnapManager unterstützten Betriebssystem ausgeführt wird.



Die unterstützte JRE-Version ist 1.8.

Zieldatenbank

Die Zieldatenbank ist eine Oracle Datenbank, die Sie mit SnapManager managen möchten, indem Sie Backup-, Restore-, Recovery- und Klonvorgänge durchführen.

Die Zieldatenbank kann eine eigenständige Real Application Clusters (RAC) sein oder auf Oracle Automatic Storage Management (ASM)-Volumes residieren. Weitere Informationen zu den unterstützten Oracle Datenbankversionen, Konfigurationen, Betriebssystemen und Protokollen finden Sie im NetApp Interoperabilitäts-Matrix-Tool.

SnapManager Repository

Das SnapManager Repository befindet sich in einer Oracle Datenbank und speichert Metadaten zu Profilen, Backups, Restores, Recoverys und Klonen. Ein einziges Repository kann Informationen über Vorgänge enthalten, die an mehreren Datenbankprofilen durchgeführt werden.

Das SnapManager-Repository kann sich nicht in der Zieldatenbank befinden. Die SnapManager-Repository-Datenbank und die Zieldatenbank müssen online sein, bevor SnapManager Vorgänge durchgeführt werden können.

Primärspeicher

SnapManager sichert die Zieldatenbanken auf dem primären NetApp Storage-System.

Sekundäres Storage-System

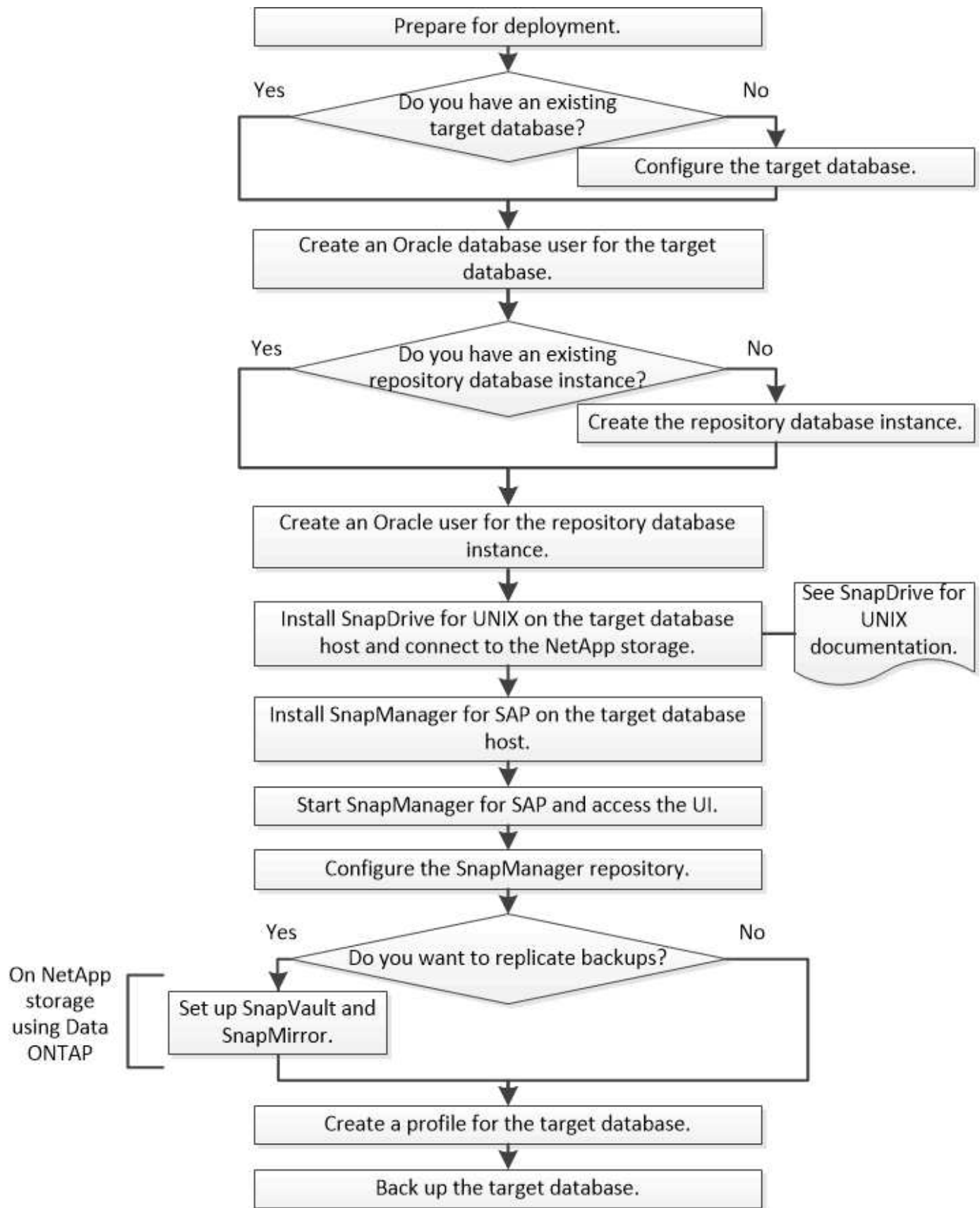
Wenn Sie die Datensicherung in einem Datenbankprofil ermöglichen, werden die Backups, die von SnapManager auf dem primären Storage-System erstellt wurden, mithilfe von SnapVault und SnapMirror Technologien auf ein sekundäres NetApp Storage-System repliziert.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Implementierungs-Workflow

Bevor Sie Backups mit SnapManager erstellen können, müssen Sie zuerst SnapDrive für UNIX installieren und dann SnapManager für SAP installieren.



Vorbereitungen für die Implementierung

Bevor Sie SnapManager bereitstellen, müssen Sie sicherstellen, dass Ihr

Speichersystem und UNIX-Hosts die Mindestanforderungen für die Ressourcen erfüllen.

Schritte

1. Stellen Sie sicher, dass Sie über die erforderlichen Lizenzen verfügen.
2. Überprüfen Sie die unterstützten Konfigurationen.
3. Überprüfen Sie die unterstützten Speichertypen.
4. Vergewissern Sie sich, dass Ihre UNIX Hosts die SnapManager-Anforderungen erfüllen.

SnapManager Lizenzierung

Zur Aktivierung des SnapManager Betriebs sind eine SnapManager Lizenz und mehrere Storage-System-Lizenzen erforderlich. Die SnapManager Lizenz ist in zwei Lizenzmodellen verfügbar: *Lizenzierung pro Server*, bei denen sich die SnapManager Lizenz auf jedem Datenbank-Host befindet, und *pro-Storage-System-Lizenzierung*, bei dem sich die SnapManager Lizenz im Storage-System befindet.

Die SnapManager Lizenzanforderungen lauten wie folgt:

Lizenz	Beschreibung	Bei Bedarf
SnapManager pro Server	Eine Host-seitige Lizenz für einen bestimmten Datenbank-Host. Lizenzen sind nur für Datenbank-Hosts erforderlich, auf denen SnapManager installiert ist. Für das Storage-System ist keine SnapManager Lizenz erforderlich.	Auf dem SnapManager-Host. Auf primären und sekundären Storage-Systemen ist keine SnapManager-Lizenz erforderlich, wenn die Lizenzierung pro Server verwendet wird.
SnapManager pro Storage-System	Eine Storage-seitige Lizenz, die eine beliebige Anzahl von Datenbank-Hosts unterstützt. Nur erforderlich, wenn Sie keine Serverlizenz auf dem Datenbank-Host verwenden.	Auf primären und sekundären Storage-Systemen.
SnapRestore	Eine erforderliche Lizenz zum Wiederherstellen von Datenbanken durch SnapManager.	Auf primären und sekundären Storage-Systemen. erforderlich auf SnapMirror Zielsystemen zur Remote-Verifizierung Erforderlich auf SnapVault Zielsystemen, um eine Remote-Verifizierung und die Wiederherstellung aus einem Backup durchzuführen.

Lizenz	Beschreibung	Bei Bedarf
FlexClone	Eine optionale Lizenz zum Klonen von Datenbanken.	Auf primären und sekundären Storage-Systemen. erforderlich auf SnapVault Zielsystemen beim Erstellen von Klonen aus einem Backup.
SnapMirror	Eine optionale Lizenz zum Spiegeln von Backups auf ein Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
SnapVault	Eine optionale Lizenz zur Archivierung von Backups auf einem Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
Protokolle	NFS-, iSCSI- oder FC-Lizenzen sind abhängig vom verwendeten Protokoll erforderlich.	Auf primären und sekundären Storage-Systemen. Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.

Unterstützte Konfigurationen

Die Hosts, auf denen Sie SnapManager installieren, müssen die angegebenen Software-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Vor der Installation oder dem Upgrade von SnapManager müssen Sie die Unterstützung Ihrer Konfiguration überprüfen.

Informationen zu unterstützten Konfigurationen finden Sie im Interoperabilitäts-Matrix-Tool.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Unterstützte Speichertypen

SnapManager unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf Virtual Machines. Sie müssen die Unterstützung Ihres Storage-Typs überprüfen, bevor Sie SnapManager installieren oder aktualisieren.

Maschine	Storage-Typ
Physischer Server	<ul style="list-style-type: none"> • Volumes mit NFS-Anbindung • FC-verbundene LUNs • iSCSI-verbundene LUNs

Maschine	Storage-Typ
VMware ESX	<ul style="list-style-type: none"> • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • RDM-LUNs auf dem Gastbetriebssystem

UNIX Host-Anforderungen

Sie müssen SnapManager für SAP auf jedem Host installieren, auf dem die Datenbank, die Sie sichern möchten, gehostet wird. Sie müssen sicherstellen, dass Ihre Hosts die Mindestanforderungen für die SnapManager-Konfiguration erfüllen.

- Sie müssen SnapDrive auf dem Datenbank-Host installieren, bevor Sie SnapManager installieren.
- Sie können SnapManager entweder auf physischen oder virtuellen Maschinen installieren.
- Sie müssen dieselbe SnapManager-Version auf allen Hosts installieren, die sich dasselbe Repository teilen.
- Sie müssen Oracle Patch installieren 13366202 Wenn Sie Oracle Datenbanken 11.2.0.2 oder 11.2.0.3 verwenden.

Wenn Sie DNFS verwenden, müssen Sie außerdem die Patches installieren, die im Bericht My Oracle Support (MOS) aufgeführt sind 1495104.1 Für maximale Leistung und Stabilität.

Um die SnapManager Graphical User Interface (GUI) zu verwenden, müssen Sie einen Host auf einer der folgenden Plattformen ausführen. Die GUI erfordert außerdem, dass Java Runtime Environment (JRE) 1.8 auf dem Host installiert ist.

- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- SUSE Enterprise Linux
- Solaris SPARC, x86 und x86_64
- IBM AIX



SnapManager arbeitet auch in der virtualisierten VMware ESX Umgebung.

Konfigurieren von Datenbanken

Sie müssen mindestens zwei Datenbanken konfigurieren: Eine Zieldatenbank, die Sie mit SnapManager sichern möchten, und eine Repository-Datenbank zum Speichern der Zieldatenbank-Metadaten. Die Zieldatenbank und die SnapManager Repository-Datenbank müssen konfiguriert und online sein, bevor SnapManager Vorgänge durchgeführt werden können.

Konfigurieren Sie die Zieldatenbank

Die Zieldatenbank ist eine Oracle-Datenbank, die entweder als Standalone, Real

Application Clusters (RAC), Automatic Storage Management (ASM) oder als andere unterstützte Kombinationen konfiguriert werden kann.

Schritt

1. Konfiguration der Zieldatenbank unter Verweis auf *NetApp Technical Report 3633: Best Practices für Oracle Datenbanken auf NetApp Storage*.

Verwandte Informationen

["NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage"](#)

Erstellen Sie einen Oracle-Datenbankbenutzer für die Zieldatenbank

Ein Benutzer der Oracle-Datenbank muss sich bei der Datenbank anmelden und SnapManager Vorgänge durchführen. Sie müssen diesen Benutzer mit der Berechtigung *sysdba* erstellen, wenn für die Zieldatenbank kein Benutzer mit der Berechtigung *sysdba* vorhanden ist.

Über diese Aufgabe

SnapManager kann jeden Oracle-Benutzer mit der Berechtigung *sysdba* verwenden, die für die Zieldatenbank vorhanden ist. Beispielsweise kann SnapManager den standardmäßigen Benutzer *sys* verwenden. Selbst wenn der Benutzer vorhanden ist, können Sie jedoch einen neuen Benutzer für die Zieldatenbank erstellen und die Berechtigung *sysdba* zuweisen.

Sie können auch die OS-Authentifizierungsmethode verwenden, bei der das Betriebssystem (OS) es der Oracle-Datenbank ermöglicht, die vom Betriebssystem gepflegten Anmeldeinformationen zu verwenden, um Benutzer zur Anmeldung in der Datenbank und zur Durchführung von SnapManager-Vorgängen zu authentifizieren. Wenn Sie über das Betriebssystem authentifiziert sind, können Sie eine Verbindung zur Oracle-Datenbank herstellen, ohne einen Benutzernamen oder ein Kennwort anzugeben.

Schritte

1. Melden Sie sich bei SQL an `*Plus: sqlplus '/ as sysdba'`
2. Erstellen Sie einen neuen Benutzer mit einem Administratorkennwort: **`create user user_name identified by admin_password;`**

`user_name` ist der Name des Benutzers, den Sie erstellen, und `admin_password` ist das Passwort, das Sie dem Benutzer zuweisen möchten.

3. Weisen Sie dem neuen Oracle-Benutzer die *sysdba*-Berechtigung zu: **`grant sysdba to user_name;`**

Erstellen Sie die Repository-Datenbankinstanz

Die Repository-Datenbankinstanz ist eine Oracle-Datenbank, in der Sie das SnapManager-Repository erstellen. Die Repository-Datenbankinstanz muss eine eigenständige Datenbank sein und kann nicht die Zieldatenbank sein.

Was Sie benötigen

Sie benötigen eine Oracle-Datenbank und ein Benutzerkonto, um auf die Datenbank zugreifen zu können.

Schritte

1. Melden Sie sich bei SQL an *Plus: `sqlplus '/ as sysdba'`
2. Erstellen Sie einen neuen Tablespace für das SnapManager-Repository: **create tablespace** `tablespace_name datafile` `'/u01/app/oracle/oradata/datafile/tablespace_name.dbf'` **size 100M autoextend on;**

`tablespace_name` ist der Name des Tablespaces.

3. Überprüfen Sie die Blockgröße des Tablespaces: **select** `tablespace_name, block_size` **from** `dba_tablespaces;`

SnapManager erfordert für den Tablespaces eine Blockgröße von mindestens 4 KB.

Verwandte Informationen

["Technischer Bericht 3761: SnapManager für Oracle: Best Practices"](#)

Erstellen Sie einen Oracle-Benutzer für die Repository-Datenbankinstanz

Ein Oracle-Benutzer ist erforderlich, um sich bei der Repository-Datenbankinstanz anzumelden und auf diese zuzugreifen. Sie müssen diesen Benutzer mit den Berechtigungen `connect` und `_Resource_` erstellen.

Schritte

1. Melden Sie sich bei SQL an *Plus: `sqlplus '/ as sysdba'`
2. Erstellen Sie einen neuen Benutzer, und weisen Sie diesem Benutzer ein Administratorkennwort zu: **create user** `user_name` **identified by** `admin_password` **default tablespace** `tablespace_name` **quota unlimited on** `tablespace_name;`
 - `user_name` ist der Name des Benutzers, den Sie für die Repository-Datenbank erstellen.
 - `admin_password` ist das Passwort, das Sie dem Benutzer zuweisen möchten.
 - `tablespace_name` ist der Name des Tablespaces, der für die Repository-Datenbank erstellt wurde.
3. Dem neuen Oracle-Benutzer `connect` und `_Resource_` Berechtigungen zuweisen: **grant** `connect, resource` **to** `user_name;`

Überprüfen Sie die Oracle Listener-Konfiguration

Der Listener ist ein Prozess, der Client-Verbindungsanforderungen abhört. Es empfängt eingehende Client-Verbindungsanfragen und verwaltet den Datenverkehr dieser Anfragen an die Datenbank. Bevor Sie eine Verbindung zu einer Zieldatenbank oder einer Repository-Datenbankinstanz herstellen, können Sie das verwenden `STATUS` Befehl zum Überprüfen der Listener-Konfiguration.

Über diese Aufgabe

Der `STATUS` Befehl zeigt grundlegende Statusinformationen zu einem bestimmten Listener an, einschließlich einer Zusammenfassung der Listener-Konfigurationseinstellungen, Listener-Protokolladressen und einer Zusammenfassung der bei diesem Listener registrierten Dienste.

Schritt

1. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: **lsnrctl STATUS**

Der dem Listener-Port zugewiesene Standardwert ist 1521.

Installation von SnapManager

Sie müssen SnapManager auf jedem Host installieren, auf dem die Datenbank, die Sie sichern möchten, ausgeführt wird.

Was Sie benötigen

Sie müssen SnapDrive für UNIX auf dem Datenbank-Host installiert und eine Verbindung zum Speichersystem hergestellt haben.

Informationen zum Installieren SnapDrive und Herstellen einer Verbindung zum Storage-System finden Sie in der Dokumentation von SnapDrive für UNIX.

Über diese Aufgabe

Sie müssen eine SnapManager-Instanz pro Datenbank-Host installieren. Wenn Sie eine RAC-Datenbank (Real Application Cluster) verwenden und die RAC-Datenbank sichern möchten, müssen Sie SnapManager auf allen Hosts der RAC-Datenbank installieren.

Schritte

1. Laden Sie das SnapManager für SAP Installationspaket für UNIX von der NetApp Support Site herunter und kopieren Sie es auf das Host-System.

["NetApp Downloads: Software"](#)

2. Melden Sie sich beim Datenbank-Host als Root-Benutzer an.
3. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie das Installationspaket kopiert haben.
4. Machen Sie das Installationspaket ausführbar: `chmod 755install_package.bin`
5. Install-SnapManager: `./install_package.bin`
6. Drücken Sie `Enter` Um fortzufahren.
7. Führen Sie folgende Schritte aus:

- a. Ändern Sie den Standardwert des Betriebssystembenutzers in **ora** `sid`, Wo `sid` ist die Systemkennung der Datenbank.
- b. Drücken Sie `Enter` Um den Standardwert für die Betriebssystemgruppe anzunehmen.

Der Standardwert für die Gruppe ist `dba`.

- c. Drücken Sie `Enter` Um den Standardwert für den Starttyp zu akzeptieren.

Die Konfigurationsübersicht wird angezeigt.

8. Überprüfen Sie die Konfigurationsübersicht, und drücken Sie `Enter` Um fortzufahren.

SnapManager für SAP und die erforderliche Java Runtime Environment (JRE) sind installiert und die `smsap_setup` Skript wird automatisch ausgeführt.

SnapManager für SAP ist installiert unter `/opt/NetApp/smsap`.

Nachdem Sie fertig sind

Sie können überprüfen, ob die Installation erfolgreich war, indem Sie die folgenden Schritte durchführen:

1. Starten Sie den Server für SnapManager, indem Sie folgenden Befehl ausführen: `smsap_server start`

Es wird eine Meldung angezeigt, die angibt, dass das für den SnapManager-Server ausgeführt wird.

2. Überprüfen Sie, ob das SnapManager für SAP für das System ordnungsgemäß ausgeführt wird, indem Sie den folgenden Befehl eingeben: `smsap system verify`

Die folgende Meldung wird angezeigt: `Operation Id number succeeded`.

`number` ist die Vorgangs-ID-Nummer.

Verwandte Informationen

["NetApp Dokumentation: SnapDrive für UNIX"](#)

["Dokumentation auf der NetApp Support Site: `mysupport.netapp.com`"](#)

Integration in SAP BR* Tools

Die SAP BR* Tools, die SAP-Tools für die Oracle-Datenbankadministration enthalten, z. B. BRARCHIVE, BRBACKUP, BRCONNECT, BRRECOVER, BRRESTORE, BRSCACE und BRTOOLS verwenden die BACKINT-Schnittstelle von SnapManager für SAP. Um SAP BR* Tools zu integrieren, müssen Sie einen Link aus dem BR* Tools Verzeichnis erstellen `/opt/NetApp/smsap/bin/`, wo die BACKINT-Datei installiert ist.

Was Sie benötigen

- Sie müssen sicherstellen, dass Sie SAP BR* Tools installiert haben.

Schritte

1. Erstellen Sie einen Link aus dem BR*Tools-Verzeichnis zum `/opt/NetApp/smsap/bin/backint` Datei für jede SAP-Instanz.



Sie müssen den Link verwenden, anstatt die Datei so zu kopieren, dass bei der Installation einer neuen Version von SnapManager der Link auf die neue BACKINT-Schnittstellenversion verweisen wird.

2. Legen Sie die Anmeldeinformationen für den Benutzer fest, der die Befehle BR*Tools ausführt.

Der Betriebssystembenutzer benötigt zur Unterstützung der Sicherung und Wiederherstellung der SAP Instanz die Zugangsdaten für das SnapManager für SAP-Repository, -Profil und -Server.

3. Geben Sie einen anderen Profilnamen an.

Standardmäßig verwendet SnapManager bei der Verarbeitung von Befehlen aus BR*Tools das Profil mit dem gleichen Namen wie die SAP-Systemkennung. Wenn diese Systemkennung in Ihrer Umgebung nicht eindeutig ist, ändern Sie den `initSID.utl` SAP-Initialisierungsdatei, und erstellen Sie einen Parameter, um das richtige Profil anzugeben. Der `initSID.utl` Datei befindet sich unter

`%ORACLE_HOME%\database.`

Beispiel

Ein Muster `initSID.utl` Die Datei ist wie folgt:

```
# Backup Retention policy.
# Specifies the retention / lifecycle of backups on the filer.
#
-----
# Default Value: daily
# Valid Values: unlimited/hourly/daily/weekly/monthly
# retain = daily
# Enabling Fast Restore.
#
-----
# Default Value: fallback
# Valid Values: require/fallback/off
#
# fast = fallback
# Data Protection.
#
-----
# Default Value: empty
# Valid Values: empty/yes/no
# protect =
# profile_name = SID_BRTOOLS
```



Der Parameternamen ist immer in Kleinbuchstaben und die Kommentare müssen ein Zahlenzeichen (#) haben.

4. Bearbeiten Sie das `initSID.sap` BR*Tools-Konfigurationsdatei durch folgende Schritte:

- Öffnen Sie das `initSID.sap` Datei:
- Suchen Sie den Abschnitt mit den Dateinformationen des Backup Utility-Parameters.

Beispiel

```
# backup utility parameter file
# default: no parameter file
# util_par_file =
```

c. Bearbeiten Sie die letzte Zeile, um die einzuschließen `initSID.utl` Datei:

Beispiel

```
# backup utility parameter file
# default: no parameter file
# util_par_file = initSID.utl
```

Nachdem Sie fertig sind

Registrieren Sie die BACKINT-Schnittstelle im Systemlandschaftsverzeichnis (SLD), indem Sie den ausführen `backint register-sld` Befehl.

SnapManager einrichten

Sie können SnapManager starten und entweder über die Benutzeroberfläche (UI) oder die Befehlszeilenschnittstelle (CLI) darauf zugreifen. Nach dem Zugriff auf SnapManager müssen Sie das SnapManager-Repository erstellen, bevor Sie SnapManager-Vorgänge durchführen.

Starten Sie den SnapManager-Server

Sie müssen den SnapManager-Server vom Ziel-Datenbank-Host starten.

Schritt

1. Melden Sie sich beim Ziel-Datenbank-Host an und starten Sie den SnapManager-Server:

`smsap_server start`

Die folgende Meldung wird angezeigt: SnapManager Server started on secure port `port_number` with PID `PID_number`.



Der Standardport ist 27214.

Sie können überprüfen, ob SnapManager ordnungsgemäß ausgeführt wird:

`smsap_server verify`

Die folgende Meldung wird angezeigt: Operation Id `operation_ID_number` succeeded.

Greifen Sie auf die Benutzeroberfläche von SnapManager zu

Sie können die SnapManager-Benutzeroberfläche (UI) Remote über einen Webbrowser von jedem System aus aufrufen, das auf einem von SnapManager unterstützten Betriebssystem ausgeführt wird. Sie können auch auf die SnapManager-Benutzeroberfläche vom Ziel-Datenbank-Host zugreifen, indem Sie das ausführen `smsapgui` Befehl.

Was Sie benötigen

- Sie müssen sicherstellen, dass SnapManager ausgeführt wird.
- Sie müssen sicherstellen, dass das unterstützte Betriebssystem und Java auf dem System installiert sind, auf dem Sie auf die SnapManager-Benutzeroberfläche zugreifen möchten.

Informationen zum unterstützten Betriebssystem und Java finden Sie im Interoperabilitäts-Matrix-Tool.

Schritte

1. Geben Sie im Webbrowser-Fenster Folgendes

ein: **`https://server_name.domain.com:port_number`**

◦ *server_name* Ist der Name des Ziel-Datenbank-Hosts, auf dem SnapManager installiert ist.

Sie können auch die IP-Adresse des Ziel-Datenbank-Hosts eingeben.

◦ *port_number* Ist der Port, auf dem SnapManager ausgeführt wird.

Der Standardwert ist 27214.

2. Klicken Sie auf den Link **SnapManager für SAP** starten.

Die Benutzeroberfläche von SnapManager für SAP wird angezeigt.

Konfigurieren Sie das SnapManager-Repository

Sie müssen das SnapManager-Repository in der Repository-Datenbankinstanz konfigurieren. Die Repository-Datenbank speichert Metadaten für Datenbanken, die von SnapManager gemanagt werden.

Was Sie benötigen

- Sie müssen die Repository-Datenbankinstanz erstellt haben.
- Sie müssen den Oracle-Benutzer für die Repository-Datenbankinstanz mit den erforderlichen Berechtigungen erstellt haben.
- Sie müssen die Details der Repository-Datenbankinstanz in das enthalten haben `tnsnames.ora` Datei:

Über diese Aufgabe

Sie können das SnapManager-Repository entweder über die SnapManager-Benutzeroberfläche (UI) oder über die Befehlszeilenschnittstelle (CLI) konfigurieren. Mit diesen Schritten wird das Erstellen eines Repositorys mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es

bevorzugen.

Informationen zum Erstellen des Repositorys mithilfe von CLI finden Sie im Handbuch *SnapManager for SAP Administration for UNIX*.

Schritte

1. Klicken Sie im linken Bereich der SnapManager-Benutzeroberfläche mit der rechten Maustaste auf **Repositories**.
2. Wählen Sie **Neues Repository erstellen** und klicken Sie auf **Weiter**.
3. Geben Sie im Fenster **Repository Database Configuration Information** die folgenden Informationen ein:

In diesem Feld...	Tun Sie das...
Benutzername	Geben Sie den Namen des Benutzers ein, den Sie für die Repository-Datenbankinstanz erstellt haben.
Passwort	Geben Sie das Passwort ein.
Gastgeber	Geben Sie die IP-Adresse des Hosts ein, auf dem die Repository-Datenbankinstanz erstellt wird.
Port	Geben Sie den Port ein, der für die Verbindung zur Repository-Datenbankinstanz verwendet wird. Der Standardport ist 1521.
Dienstname	Geben Sie den Namen ein, den SnapManager für die Verbindung zur Repository-Datenbankinstanz verwendet. Abhängig von den im enthaltenen Details <code>tnsnames.ora</code> Datei: Es kann sich um den kurzen Servicennamen oder den vollqualifizierten Servicennamen handeln.

4. Überprüfen Sie im Fenster * Repository hinzufügen Operation Window die Konfigurationszusammenfassung und klicken Sie auf **Add**.

Wenn der Vorgang fehlschlägt, klicken Sie auf die Registerkarte **Operationsinformationen**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat. Die Fehlerdetails werden auch im Betriebsprotokoll unter erfasst `/var/log/smsap`.

5. Klicken Sie Auf **Fertig Stellen**.

Das Repository wird im linken Fensterbereich unter dem Baum **Repositories** aufgelistet. Wenn das Repository nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf **Repositories** und klicken Sie auf **Aktualisieren**.

Verwandte Informationen

["SnapManager 3.4.1 für SAP – Administratorhandbuch für UNIX"](#)

Vorbereiten der Speichersysteme für die SnapMirror- und SnapVault-Replizierung

Mithilfe von SnapManager mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie können Disk-to-Disk-Backup-Replizierungen zwecks Standards und zu anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Beziehung „*Data-Protection Relationship* zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung_initialisieren_.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

Verständnis der Unterschiede zwischen SnapMirror und SnapVault

SnapMirror ist eine Disaster-Recovery-Technologie für den Failover von primärem Storage zu sekundärem Storage an einem geografisch verteilten Standort. SnapVault ist eine Disk-to-Disk Backup-Replizierungstechnologie, die für Compliance-Standards und andere Governance-bezogene Zwecke entwickelt wurde.

Diese Ziele berücksichtigen das unterschiedliche Gleichgewicht, das jede Technologie zwischen den Zielen der Backup-Währung und der Backup-Aufbewahrung findet:

- SnapMirror speichert _nur die Snapshot Kopien, die sich im Primär-Storage befinden, da bei einem Ausfall ein Failover zur neuesten Version der Primärdaten erforderlich sein muss, von der Sie wissen, dass sie gut sind.

Beispielsweise könnte Ihr Unternehmen stündliche Kopien von Produktionsdaten über einen Zeitraum von zehn Tagen spiegeln. Wie der Anwendungsfall des Failovers schon andeutet, müssen die Geräte auf dem Sekundärsystem äquivalent oder nahezu identisch mit der Ausrüstung auf dem Primärsystem sein, um Daten effizient aus dem gespiegelten Storage bereitzustellen.

- Im Gegensatz dazu speichert SnapVault Snapshot Kopien _unabhängig davon, ob sie sich derzeit im Primärspeicher befinden, da im Rahmen eines Audits wahrscheinlich der Zugriff auf historische Daten so wichtig sein wird wie der Zugriff auf aktuelle Daten.

Möglicherweise möchten Sie monatlich Snapshot Kopien Ihrer Daten über einen Zeitraum von 20 Jahren aufbewahren, um beispielsweise gesetzliche Buchhaltungsvorschriften für Ihr Unternehmen einzuhalten. Da keine Daten aus dem sekundären Storage bereitgestellt werden müssen, können Sie langsamere und kostengünstigere Festplatten auf dem Vault-System verwenden.

Die verschiedenen Gewichte, die SnapMirror und SnapVault der Backup-Währung und der Backup-Aufbewahrung geben, entstammen letztendlich vom Limit von 255 Snapshot Kopien für jedes Volume. Bei SnapMirror werden die letzten Kopien aufbewahrt. SnapVault behält die Kopien, die über den längsten Zeitraum erstellt wurden, bei.

Storage-Systeme für die SnapMirror Replizierung vorbereiten

Bevor Sie SnapManager zur Spiegelung von Snapshot Kopien verwenden können,

müssen Sie eine *Datensicherungsbeziehung* zwischen den Quell- und Ziel-Volumes konfigurieren und dann die Beziehung initialisieren. Bei der Initialisierung erstellt SnapMirror eine Snapshot Kopie des Quell-Volume, dann überträgt die Kopie und alle Datenblöcke, auf die sie Bezug nimmt auf das Ziel-Volume. Es überträgt außerdem alle anderen, weniger neuesten Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein.
- Für die Überprüfung von Snapshot Kopien auf dem Ziel-Volume müssen die Storage Virtual Machines (SVMs) aus Quell- und Ziel-Storage über eine Management-LIF und eine Daten-LIF verfügen.

Die Management-LIF muss den gleichen DNS-Namen wie die SVM aufweisen. Legen Sie die Management-LIF-Rolle auf Daten, das Protokoll ohne und die Firewall-Richtlinie auf **Management** fest.

Über diese Aufgabe

Sie können eine SnapMirror Beziehung mit der ONTAP Befehlszeilenschnittstelle (CLI) oder OnCommand System Manager erstellen. Das folgende Verfahren dokumentiert die Verwendung der CLI.



Wenn Sie Datenbankdateien und Transaktions-Logs auf verschiedenen Laufwerken speichern, müssen Sie für die Transaktions-Logs Beziehungen zwischen den Quell- und Ziel-Volumes für die Datenbankdateien sowie zwischen den Quell- und Ziel-Volumes erstellen.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapMirror Beziehung:

Schritte

1. Ermitteln des Ziel-Clusters
2. Verwenden Sie auf dem Ziel-Cluster die `volume create` Befehl mit dem `-type DP`-Option zum Erstellen eines SnapMirror Ziel-Volume, das entweder gleich oder größer ist als das Quell-Volume.



Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

Beispiel

Mit dem folgenden Befehl wird ein 2 GB großes Ziel-Volume namens `dstvolB` in SVM2 auf dem Aggregat `node01_aggr` erstellt:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -type DP  
-size 2GB
```

3. Verwenden Sie auf der Ziel-SVM den `snapmirror create` Befehl mit dem `-type DP` Parameter zum Erstellen einer SnapMirror Beziehung.

Der DP-Typ definiert die Beziehung als SnapMirror-Beziehung.

Beispiel

Mit dem folgenden Befehl wird eine SnapMirror Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2 erstellt und diesem wird die Standard-SnapMirror-Richtlinie DDPStandard zugewiesen:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path  
SVM2:dstvolB  
-type DP
```



Definieren Sie keinen Spiegelungsplan für die SnapMirror Beziehung. Das gilt für Sie, wenn Sie einen Backup-Zeitplan erstellen.

Wenn Sie die standardmäßige SnapMirror Richtlinie nicht verwenden möchten, können Sie den aufrufen `snapmirror policy create` Befehl zum Definieren einer SnapMirror-Richtlinie

4. Verwenden Sie die `snapmirror initialize` Befehl zum Initialisieren der Beziehung.

Der Initialisierungsvorgang führt einen *Baseline Transfer* zum Ziel-Volume durch. SnapMirror erstellt eine Snapshot-Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die er auf das Ziel-Volume verweist. Sie überträgt zudem alle anderen Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume.

Beispiel

Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2 initialisiert:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Verwandte Informationen

["ONTAP 9 Cluster Peering Express Guide"](#)

["ONTAP 9 Express-Anleitung zur Vorbereitung der Wiederherstellung von Volumes"](#)

Storage-Systeme für die SnapVault-Replizierung vorbereiten

Bevor Sie SnapManager zur Durchführung der Disk-to-Disk-Backup-Replizierung verwenden können, müssen Sie eine *Datensicherungsbeziehung* zwischen den Quell- und Ziel-Volumes konfigurieren und anschließend die Beziehung initialisieren. Bei der Initialisierung erstellt SnapVault eine Snapshot Kopie des Quell-Volume, überträgt dann die Kopie und alle Datenblöcke, auf die sie auf das Ziel-Volume verweist.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein.

Über diese Aufgabe

Sie können SnapVault Beziehungen mit der ONTAP Befehlszeilenschnittstelle (CLI) oder mit OnCommand System Manager erstellen. Das folgende Verfahren dokumentiert die Verwendung der CLI.



Wenn Sie Datenbankdateien und Transaktions-Logs auf verschiedenen Laufwerken speichern, müssen Sie für die Transaktions-Logs Beziehungen zwischen den Quell- und Ziel-Volumes für die Datenbankdateien sowie zwischen den Quell- und Ziel-Volumes erstellen.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapVault Beziehung:

Schritte

1. Ermitteln des Ziel-Clusters
2. Verwenden Sie auf dem Ziel-Cluster die `volume create` Befehl mit dem `-type DP`-Option zum Erstellen eines SnapVault Ziel-Volume, das mit dem Quell-Volume größer oder gleich ist.



Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

Beispiel

Mit dem folgenden Befehl wird ein 2 GB großes Ziel-Volume namens `dstvolB` in SVM2 auf dem Aggregat `node01_aggr` erstellt:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -type DP  
-size 2GB
```

3. Verwenden Sie auf der Ziel-SVM den `snapmirror policy create` Befehl zum Erstellen einer SnapVault-Richtlinie

Beispiel

Mit dem folgenden Befehl wird die SVM-weite Richtlinie `SVM1-Vault` erstellt:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-vault
```



Für die SnapVault-Beziehung dürfen keine Cron-Zeitpläne oder Snapshot-Kopierrichtlinien definiert werden. Das gilt für Sie, wenn Sie einen Backup-Zeitplan erstellen.

4. Verwenden Sie die `snapmirror create` Befehl mit dem `-type XDP` Und das `-policy` Parameter, um eine SnapVault-Beziehung zu erstellen und eine Vault-Richtlinie zuzuweisen.

Der XDP-Typ definiert die Beziehung als eine SnapVault-Beziehung.

Beispiel

Mit dem folgenden Befehl wird eine SnapVault-Beziehung zwischen dem Quell-Volume `srcvolA` auf SVM1

und dem Ziel-Volume dstvolB auf SVM2 erstellt und der Richtlinie SVM1-Vault zugewiesen:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path  
SVM2:dstvolB  
-type XDP -policy SVM1-vault
```

5. Verwenden Sie die `snapmirror initialize` Befehl zum Initialisieren der Beziehung.

Der Initialisierungsvorgang führt einen *Baseline Transfer* zum Ziel-Volume durch. SnapMirror erstellt eine Snapshot-Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die er auf das Ziel-Volume verweist.

Beispiel

Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2 initialisiert:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Verwandte Informationen

["ONTAP 9 Cluster Peering Express Guide"](#)

["ONTAP 9 Volume Backup mit SnapVault Express Guide"](#)

Sichern und Überprüfen Ihrer Datenbanken

Nach der Installation von SnapManager können Sie ein Basis-Backup Ihrer Datenbank erstellen und überprüfen, ob das Backup keine beschädigten Dateien enthält.

SnapManager Backup – Überblick

SnapManager erstellt mithilfe von NetApp Snapshot Technologie die Backups von Datenbanken. Sie können das DBVERIFY-Dienstprogramm verwenden oder SnapManager verwenden, um die Integrität der Backups zu überprüfen.

SnapManager sichert eine Datenbank, indem Snapshot Kopien der Volumes erstellt werden, die Datendateien, Kontrolldateien und Archivprotokolldateien enthalten. Diese Snapshot Kopien bestehen zusammen aus einem Backup-Set, mit dem SnapManager eine Datenbank wiederherstellen kann.

Backup-Strategie definieren

Wenn Sie eine Backup-Strategie vor der Erstellung Ihrer Backups definieren, stellen Sie sicher, dass Ihnen Backups zur erfolgreichen Wiederherstellung Ihrer Datenbanken zur Verfügung stehen. SnapManager bietet einen flexiblen, granularen Backup-Zeitplan, der Ihr Service Level Agreement (SLA) erfüllt.



Welcher Modus für SnapManager Backups benötigen Sie?

SnapManager unterstützt zwei Backup-Modi:

Backup-Modus	Beschreibung
Online-Backup	Erstellt ein Backup der Datenbank, wenn sich die Datenbank im Online-Status befindet. Dieser Backup-Modus wird auch als Hot Backup bezeichnet.
Offline-Backup	Erstellt eine Sicherung der Datenbank, wenn sich die Datenbank entweder im angehängten oder abschaltenden Zustand befindet. Dieser Backup-Modus wird auch als Cold Backup bezeichnet.

Welche Art von SnapManager-Backup benötigen Sie?

SnapManager unterstützt drei Arten von Backups:

Backup-Typ	Beschreibung
Vollständiges Backup	Erstellt ein Backup der gesamten Datenbank, die alle Datendateien, Kontrolldateien und Archivprotokolldateien umfasst.
Teilweise Sicherung	Erstellt ein Backup ausgewählter Datendateien, Kontrolldateien, Tablespaces und Archivprotokolldateien
Backup nur für Archivierung	Erstellt eine Sicherung nur der Archivprotokolldateien. Sie müssen beim Erstellen des Profils Archivprotokolle separat auswählen.

Was für ein Datenbankprofil benötigen Sie?

SnapManager erstellt Backups basierend darauf, ob das Datenbankprofil die Archiv-Log-Backups von den Datendatei-Backups trennt.

Profiltyp	Beschreibung
Ein einzelnes Datenbankprofil für eine kombinierte Sicherung von Datendateien und Archivprotokollen	<p>Ermöglicht Ihnen das Erstellen von:</p> <ul style="list-style-type: none">• Vollständige Sicherung mit allen Datendateien, Archivprotokolldateien und Kontrolldateien• Partielles Backup mit ausgewählten Datendateien, Tablespaces, Archivprotokolldateien und Kontrolldateien

Profiltyp	Beschreibung
Separate Datenbankprofile für Backups von Archivierungsprotokolldaten und Datendatei-Backups	<p>Ermöglicht Ihnen das Erstellen von:</p> <ul style="list-style-type: none"> • Kombiniertes Backup mit unterschiedlichen Kennungen für Backup von Datendateien und Backup von Archivierungsprotokolldaten • Datendatei-only-Backup aller Datendateien zusammen mit den Kontrolldateien • Partielles, datenonly Backup von ausgewählten Datendateien oder Tablespace zusammen mit den Control Files • Backup nur bei Archivierung und Protokollen

Welche Namenskonventionen sollten für Snapshot Kopien verwendet werden?

Von Backups erstellte Snapshot Kopien können einer benutzerdefinierten Namenskonvention folgen. Benutzerdefinierte Text oder integrierte Variablen wie der Profilname, der Datenbankname und die von SnapManager bereitgestellte Datenbank-SID können zur Erstellung der Namenskonvention verwendet werden. Sie können die Namenskonvention erstellen, während Sie die Richtlinie erstellen.



Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

Die Namenskonventionen für Snapshot Kopien können während oder nach der Erstellung eines Profils geändert werden. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Vorhandene Snapshot Kopien behalten das vorherige Muster bei.

Wie lange möchten Sie Backup-Kopien auf dem primären Storage-System und dem sekundären Storage-System aufbewahren?

In einer Backup-Aufbewahrungsrichtlinie wird die Anzahl der erfolgreichen Sicherungskopien festgelegt, die aufbewahrt werden sollen. Sie können die Aufbewahrungsrichtlinie angeben, während Sie die Richtlinie erstellen.

Sie können stündlich, täglich, wöchentlich, monatlich oder unbegrenzt als Aufbewahrungsklasse auswählen. Sie können für jede Aufbewahrungsklasse den Aufbewahrungszähler und die Aufbewahrungsdauer entweder gemeinsam oder einzeln festlegen.

- Die Anzahl der Aufbewahrung bestimmt die Mindestanzahl der Backups einer bestimmten Aufbewahrungsklasse, die beibehalten werden soll.

Wenn beispielsweise der Backup-Zeitplan *Daily* lautet und die Anzahl der Aufbewahrung 10 ist, werden 10 tägliche Backups aufbewahrt.



Die maximale Anzahl von Snapshot Kopien, die Sie mit Data ONTAP aufbewahren können, ist 255. Nach Erreichen des maximalen Limits schlägt die Erstellung neuer Snapshot Kopien standardmäßig fehl. Sie können jedoch die Rotationsrichtlinie in Data ONTAP konfigurieren, um ältere Snapshot-Kopien zu löschen.

- Die Aufbewahrungsdauer legt die Mindestanzahl an Tagen fest, für die das Backup aufbewahrt werden

soll.

Wenn beispielsweise der Backup-Zeitplan *täglich* lautet und die Aufbewahrungsdauer *10* beträgt, werden täglich 10 Tage Backups aufbewahrt.

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



Zur langfristigen Aufbewahrung von Backup-Kopien sollten Sie SnapVault verwenden.

Möchten Sie Backup-Kopien mithilfe des Quell-Volume oder eines Ziel-Volume überprüfen?

Wenn Sie SnapMirror oder SnapVault einsetzen, können Sie Backup-Kopien mithilfe der Snapshot-Kopie auf dem SnapMirror oder SnapVault Ziel-Volume überprüfen anstelle der Snapshot-Kopie auf dem primären Storage-System. Die Verwendung eines Ziel-Volumes zur Verifizierung reduziert die Last auf dem primären Storage-System.

Verwandte Informationen

["Technischer Bericht 3761: SnapManager für Oracle: Best Practices"](#)

Erstellen Sie ein Profil für Ihre Datenbank

Sie müssen ein Profil erstellen, damit Ihre Datenbank alle Vorgänge in dieser Datenbank ausführen kann. Das Profil enthält Informationen über die Datenbank und kann nur auf eine Datenbank verweisen. Eine Datenbank kann jedoch durch mehrere Profile referenziert werden. Ein Backup, das mit einem Profil erstellt wird, kann nicht von einem anderen Profil aus aufgerufen werden, auch wenn beide Profile mit derselben Datenbank verknüpft sind.

Was Sie benötigen

Sie müssen sicherstellen, dass die Details der Zieldatenbank in enthalten sind `/etc/oratab` Datei:

Über diese Aufgabe

Mit diesen Schritten wird die Erstellung eines Profils für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es bevorzugen.

Informationen zum Erstellen von Profilen mithilfe der CLI finden Sie im Handbuch *SnapManager for SAP Administration for UNIX*.

Schritte

1. Klicken Sie in der Repository-Struktur mit der rechten Maustaste auf das Repository oder den Host und wählen Sie **Profil erstellen** aus.
2. Geben Sie auf der Seite **Profile Configuration Information** den benutzerdefinierten Namen und das Kennwort für das Profil ein.
3. Geben Sie auf der Seite **Datenbankkonfigurationsinformationen** die folgenden Informationen ein:

In diesem Feld...	Tun Sie das...
Datenbankname	Geben Sie den Namen der Datenbank ein, die Sie sichern möchten.
• Datenbank-SID*	Geben Sie die sichere ID (SID) der Datenbank ein. Der Datenbankname und die Datenbank-SID können identisch sein.
Gastgeber	Geben Sie die IP-Adresse des Hosts ein, auf dem sich die Zieldatenbank befindet. Sie können auch den Hostnamen angeben, wenn der Hostname im Domain Name System (DNS) angegeben ist.
Host-Konto	Geben Sie den Oracle-Benutzernamen der Zieldatenbank ein. der Standardwert für den Benutzer ist oracle.
Host-Gruppe	Geben Sie den Namen der Oracle-Benutzergruppe ein. Der Standardwert ist dba.

4. Wählen Sie auf der Seite **Datenbankverbindungsinformationen** eine der folgenden Optionen aus:

Wählen Sie diese Option...	Ihr Ziel ist
O/S-Authentifizierung verwenden	Verwenden Sie die vom Betriebssystem gepflegten Anmeldeinformationen, um Benutzer zu authentifizieren, die auf die Datenbank zugreifen.
Datenbankauthentifizierung Verwenden	<p>Erlauben Sie Oracle, einen administrativen Benutzer mithilfe der Authentifizierung von Kennwortdateien zu authentifizieren. Geben Sie die entsprechenden Informationen zur Datenbankverbindung ein.</p> <ul style="list-style-type: none"> • Geben Sie im Feld SYSDBA Privileged User Name den Namen des Datenbankadministrators mit Administratorrechten ein. • Geben Sie im Feld Passwort das Passwort des Datenbankadministrators ein. • Geben Sie im Feld Port die Portnummer ein, die für die Verbindung mit dem Host verwendet wird, auf dem sich die Datenbank befindet. <p>Der Standardwert ist 1527.</p>

Wählen Sie diese Option...	Ihr Ziel ist
Verwendung der ASM-Instanz-Authentifizierung	<p>Zulassen, dass die ASM-Datenbankinstanz einen administrativen Benutzer authentifiziert. Geben Sie die entsprechenden Authentifizierungsdaten für die ASM-Instanz ein.</p> <ul style="list-style-type: none"> • Geben Sie im Feld SYSDBA/SYSASM Privileged User Name den Benutzernamen des ASM-Instanzadministrators mit Administratorrechten ein. • Geben Sie im Feld Passwort das Passwort des Administrators ein.



Sie können den ASM-Authentifizierungsmodus nur auswählen, wenn Sie eine ASM-Instanz auf dem Datenbank-Host haben.

5. Wählen Sie auf der Seite **RMAN-Konfigurationsinformationen** eine der folgenden Optionen aus:

Wählen Sie diese Option...	Wenn...
Verwenden Sie nicht RMAN	Sie verwenden RMAN nicht für das Management von Backup- und Restore-Vorgängen.
Verwenden Sie RMAN über die Steuerdatei	Sie verwalten das RMAN-Repository mit Steuerdateien.
Verwenden Sie RMAN über den Wiederherstellungskatalog	Sie verwalten das RMAN-Repository mithilfe der Recovery-Katalogdatenbank. Geben Sie den Benutzernamen ein, der Zugriff auf die Datenbank des Wiederherstellungspatalogs, das Kennwort und den Oracle-Nettodiensnamen der Datenbank hat, die die TNS-Verbindung (Transparent Network Substrat) verwaltet.

6. Wählen Sie auf der Seite **Snapshot Naming Information** die Variablen aus, um ein Benennungsformat für die Snapshot Kopie anzugeben.

Sie müssen die *smid*-Variable in das Benennungsformat aufnehmen. Die Variable *smid* erstellt eine eindeutige Snapshot-Kennung.

7. Führen Sie auf der Seite **Richtlinieneinstellungen** folgende Schritte aus:

- Geben Sie Anzahl und Dauer der Aufbewahrung für jede Aufbewahrungsklasse ein.
- Wählen Sie aus der Dropdown-Liste **Schutzrichtlinie** die Schutzrichtlinie aus.

Je nachdem, ob SnapMirror oder SnapVault Beziehung aufgebaut ist, müssen Sie entweder *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* Richtlinien auswählen.

- Wenn Sie Archivprotokolle separat sichern möchten, aktivieren Sie das Kontrollkästchen **Archivprotokolle separat sichern**, legen Sie die Aufbewahrung fest und wählen Sie die

Schutzrichtlinie aus.

Sie können eine Richtlinie auswählen, die sich von der für Datendateien verknüpften Richtlinie unterscheidet. Wenn Sie beispielsweise *SnapManager_cDOT_Mirror* für Datendateien ausgewählt haben, können Sie *SnapManager_cDOT_Vault* für Archivprotokolle auswählen.

8. Geben Sie auf der Seite **Benachrichtigungseinstellungen konfigurieren** die Einstellungen für E-Mail-Benachrichtigungen an.
9. Wählen Sie auf der Seite **Verlauf Konfigurationsdaten** eine der Optionen aus, um den Verlauf der SnapManager-Vorgänge beizubehalten.
10. Überprüfen Sie auf der Seite **Vorgang erstellen** die Informationen und klicken Sie auf **Erstellen**.
11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

["SnapManager 3.4.1 für SAP – Administratorhandbuch für UNIX"](#)

Sichern Sie Ihre Datenbank

Nachdem Sie ein Profil erstellt haben, müssen Sie Ihre Datenbank sichern. Sie können wiederkehrende Backups nach der erstmaligen Sicherung und Überprüfung planen.

Über diese Aufgabe

In diesen Schritten wird gezeigt, wie Sie mithilfe der SnapManager-Benutzeroberfläche ein Backup Ihrer Datenbank erstellen. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden.

Informationen zum Erstellen von Backups mithilfe der CLI- oder SAP BR*-Tools finden Sie im *SnapManager for SAP Administration Guide for UNIX*.

Schritte

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die zu sichernde Datenbank enthält, und wählen Sie **Backup** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die bearbeiten `override.default.backup.pattern` und `new.default.backup.pattern` Konfigurationsvariablen zum Erstellen Ihres eigenen Standard-Backup-Label-Musters.

3. Optional: In **SnapVault-Label** müssen Sie beim Einrichten der SnapVault-Beziehung das SnapMirror-Label eingeben, das Sie in den Regeln der SnapMirror-Richtlinie angegeben haben.



Das Feld **SnapVault Label** wird nur angezeigt, wenn Sie beim Erstellen des Profils *SnapManager_cDOT_Vault* als Schutzrichtlinie ausgewählt haben.

4. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

5. Auf der **Datenbank, Tablespaces** oder **Datafiles** bis **Backup** Führen Sie folgende Schritte aus:
 - a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
 - b. Wählen Sie **Backup Archivelogs** aus, um die Archiv-Log-Dateien separat zu sichern.
 - c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.



Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

- d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

- e. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

Wenn Sie *Auto* auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

- f. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.

- g. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.

6. Geben Sie auf der Seite **Task Enabling** an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.

7. Überprüfen Sie auf der Seite *** Backup-Vorgang durchführen*** die Informationen und klicken Sie auf **Backup**.

8. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

["SnapManager 3.4.1 für SAP – Administratorhandbuch für UNIX"](#)

Datenbank-Backups prüfen

Sie können die Sicherung Ihrer Datenbank überprüfen, um sicherzustellen, dass die gesicherten Dateien nicht beschädigt sind.

Über diese Aufgabe

Wenn Sie beim Erstellen eines Backups nicht das Kontrollkästchen **Backup überprüfen mit dem Dienstprogramm Oracle DBVERIFY** aktiviert haben, müssen Sie diese Schritte manuell durchführen, um die Sicherung zu überprüfen. Wenn Sie das Kontrollkästchen aktiviert haben, überprüft SnapManager das Backup automatisch.

Schritte

1. Wählen Sie aus der Struktur **Repositories** das Profil aus.
2. Klicken Sie mit der rechten Maustaste auf das Backup, das Sie überprüfen möchten, und wählen Sie **Überprüfen**.
3. Klicken Sie Auf **Fertig Stellen**.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Klicken Sie im Baum **Repository** mit der rechten Maustaste auf das Backup und klicken Sie dann auf **Eigenschaften**, um die Ergebnisse des Verifizierungsvorgangs anzuzeigen.

Nachdem Sie fertig sind

Sie können gesicherte Dateien verwenden, um Wiederherstellungsvorgänge durchzuführen. Informationen zur Durchführung von Wiederherstellungsvorgängen über die SnapManager-Benutzeroberfläche (UI) finden Sie in der *Online-Hilfe*. Wenn Sie mithilfe der Befehlszeilenschnittstelle (CLI) Wiederherstellungsvorgänge ausführen möchten, finden Sie im Handbuch „*SnapManager for SAP Administration Guide for UNIX*“.

Verwandte Informationen

["SnapManager 3.4.1 für SAP – Administratorhandbuch für UNIX"](#)

Planen Sie regelmäßige Backups

Sie können Backup-Vorgänge so planen, dass die Backups automatisch in regelmäßigen Abständen initiiert werden. SnapManager ermöglicht die Planung von Backups auf Stundenbasis, täglich, wöchentlich, monatlich oder einmalig.

Über diese Aufgabe

Sie können mehrere Backup-Zeitpläne für eine einzige Datenbank zuweisen. Wenn Sie jedoch mehrere Backups für dieselbe Datenbank planen, müssen Sie sicherstellen, dass die Backups nicht gleichzeitig geplant sind.

Mit diesen Schritten wird das Erstellen eines Backup-Zeitplans für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche (UI) erläutert. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden. Informationen zum Planen von Backups mithilfe der CLI finden Sie im *SnapManager for SAP Administration Guide for UNIX*.

Schritte

1. Klicken Sie in der Verzeichnisstruktur **Repositories** mit der rechten Maustaste auf das Profil, das die Datenbank enthält, für die Sie einen Backup-Zeitplan erstellen möchten, und wählen Sie **Backup planen** aus.

2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die bearbeiten `override.default.backup.pattern` Und `new.default.backup.pattern` Konfigurationsvariablen zum Erstellen Ihres eigenen Standard-Backup-Label-Musters.

3. Optional: In **SnapVault-Label** müssen Sie beim Einrichten der SnapVault-Beziehung das SnapMirror-Label eingeben, das Sie in den Regeln der SnapMirror-Richtlinie angegeben haben.



Das Feld **SnapVault Label** wird nur angezeigt, wenn Sie beim Erstellen des Profils *SnapManager_cDOT_Vault* als Schutzrichtlinie ausgewählt haben.

4. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

5. Führen Sie auf der Seite **Database, Tablespaces** oder **Datafiles** auf **Backup** folgende Schritte durch:

- Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
- Wählen Sie **Backup Archivlogs** aus, um die Archiv-Log-Dateien separat zu sichern.
- Wählen Sie **Prune Archivlogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.



Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

- Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

- Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

Wenn Sie *Auto* auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

- Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
- Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.

6. Geben Sie im Feld **Terminplanname** einen benutzerdefinierten Namen des Zeitplans ein.

Sie dürfen keine Leerzeichen in den Namen einfügen.

7. Führen Sie auf der Seite *** Backup Schedule konfigurieren*** folgende Schritte durch:

- Wählen Sie aus der Dropdown-Liste **Durchführung dieser Operation** die Häufigkeit des Backup-

Zeitplans aus.

- b. Geben Sie im Feld **Startdatum** das Datum an, an dem Sie den Backup-Zeitplan starten möchten.
- c. Geben Sie im Feld **Startzeit** den Zeitpunkt an, zu dem der Backup-Zeitplan gestartet werden soll.
- d. Geben Sie das Intervall an, in dem Backups erstellt werden sollen.

Wenn Sie beispielsweise die Frequenz als stündlich ausgewählt haben und das Intervall als 2 angeben, werden die Backups alle 2 Stunden geplant.

8. Geben Sie auf der Seite **Task Enabling** an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.
9. Überprüfen Sie die Informationen auf der Seite * Backup Schedule Operation* durchführen und klicken Sie auf **Schedule**.
10. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

["SnapManager 3.4.1 für SAP – Administratorhandbuch für UNIX"](#)

Deinstallieren Sie die Software von einem UNIX-Host

Wenn Sie die SnapManager-Software nicht mehr benötigen, können Sie sie auf dem Hostserver deinstallieren.

Schritte

1. Melden Sie sich als Root an.
2. Geben Sie zum Beenden des Servers den folgenden Befehl ein: `smsap_server stop`
3. Geben Sie zum Entfernen der SnapManager Software den folgenden Befehl ein: **UninstallSmsap**
4. Drücken Sie nach dem Einführungstext **Enter**, um fortzufahren.

Die Deinstallation ist abgeschlossen.

Upgrade von SnapManager

Sie können von einer der früheren Versionen auf die neueste Version von SnapManager für SAP aktualisieren. Sie können entweder alle SnapManager Hosts gleichzeitig aktualisieren oder ein Rolling Upgrade durchführen, wodurch Sie die Hosts auf gestaffelte, Host-für-Host-Art aktualisieren können.

SnapManager wird vorbereitet

Die Umgebung, in der Sie ein SnapManager-Upgrade durchführen möchten, muss die spezifischen Software-, Hardware-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Aktuelle Informationen zu den Anforderungen

finden Sie im ["Interoperabilitätsmatrix"](#).

Sie müssen vor dem Upgrade sicherstellen, dass Sie die folgenden Aufgaben ausführen:

- Führen Sie die erforderlichen Vorinstallationsaufgaben aus.
- Laden Sie das neueste Installationspaket von SnapManager für SAP herunter.
- Installieren und konfigurieren Sie die entsprechende Version von SnapDrive für UNIX auf allen Ziel-Hosts.
- Erstellen eines Backups der vorhandenen Repository-Datenbank SnapManager für SAP

Verwandte Informationen

["Interoperabilitätsmatrix"](#)

Aktualisieren Sie die SnapManager-Hosts

Sie können alle vorhandenen Hosts auf die neueste Version von SnapManager aktualisieren. Alle Hosts werden gleichzeitig aktualisiert. Dies kann jedoch zu einer Ausfallzeit aller SnapManager-Hosts und der geplanten Operationen während dieser Zeit führen.

Schritte

1. Melden Sie sich beim Hostsystem als Root-Benutzer an.
2. Navigieren Sie von der Befehlszeilenschnittstelle (CLI) zu dem Speicherort, an dem Sie die Installationsdatei heruntergeladen haben.
3. Optional: Wenn die Datei nicht ausführbar ist, ändern Sie die Berechtigungen: `chmod 544 netapp.smsap*`
4. Stoppen Sie den SnapManager Server: `smsap_server stop`
5. Je nach UNIX Host, installieren Sie SnapManager:

Wenn das Betriebssystem...	Starten Sie dann...
Solaris (SPARC64)	<code>\# ./netapp.smsap.sunos-sparc64-version_number.bin</code>
Solaris (x86_64)	<code>\# ./netapp.smsap.sunos-x64-version_number.bin</code>
AIX (PPC64)	<code>\# ./netapp.smsap.aix-ppc64-version_number.bin</code>
• Linux x86*	<code>\# ./netapp.smsap.linux-x86-version_number.bin</code>
• Linux x64*	<code>\# ./netapp.smsap.linux-x64-version_number.bin</code>

6. Drücken Sie auf der Seite **Einführung** die Eingabetaste*, um fortzufahren.

Die folgende Meldung wird angezeigt: Existing SnapManager For SAP Detected.

7. Drücken Sie **Enter**.

8. Führen Sie an der Eingabeaufforderung Folgendes aus:

- a. Ändern Sie den Standardwert des Betriebssystembenutzers in **ora** *sid*.

sid ist die Systemkennung der SAP-Datenbank.

- b. Geben Sie den richtigen Wert für die Betriebssystemgruppe ein, oder drücken Sie **Enter**, um den Standardwert zu akzeptieren.
- c. Geben Sie den richtigen Wert für den Starttyp des Servers ein, oder drücken Sie **Enter**, um den Standardwert zu akzeptieren.

Die Konfigurationsübersicht wird angezeigt.

9. Drücken Sie **Enter**, um fortzufahren.

Die folgende Meldung wird angezeigt: Uninstall of Existing SnapManager For SAP has started.

Die Deinstallation ist abgeschlossen und die aktuelle Version von SnapManager ist installiert.

Aufgaben nach dem Upgrade

Nach dem Upgrade auf eine neuere Version von SnapManager müssen Sie das vorhandene Repository aktualisieren. Möglicherweise möchten Sie auch die Backup-Aufbewahrungsklasse, die dem bestehenden Backup zugewiesen ist, ändern. Ermitteln Sie dann, welchen Restore-Prozess Sie verwenden können.



Nach dem Upgrade auf SnapManager 3.3 oder höher müssen Sie einstellen `sqlnet.authentication_services` An **NONE**, wenn Sie Datenbank (DB) Authentifizierung als einzige Authentifizierungsmethode verwenden möchten. Diese Funktion wird für RAC-Datenbanken nicht unterstützt.

Aktualisieren Sie das vorhandene Repository

Sie müssen das vorhandene Repository nicht aktualisieren, wenn Sie ein Upgrade von SnapManager 3.3.x auf SnapManager 3.4 oder höher durchführen. Für alle anderen Upgrade-Pfade müssen Sie jedoch das vorhandene Repository aktualisieren, damit Sie nach dem Upgrade darauf zugreifen können.

Was Sie benötigen

- Der aktualisierte SnapManager-Server muss gestartet und verifiziert worden sein.
- Ein Backup des vorhandenen Repositories muss vorhanden sein.

Über diese Aufgabe

- Wenn Sie ein Upgrade von einer älteren Version als SnapManager 3.1 auf SnapManager 3.3 oder höher durchführen, müssen Sie zuerst auf SnapManager 3.2 aktualisieren.

Nach dem Upgrade auf SnapManager 3.2 können Sie dann ein Upgrade auf SnapManager 3.3 oder höher durchführen.

- Nach dem Aktualisieren des Repositorys können Sie das Repository nicht mit einer früheren SnapManager-Version verwenden.

Schritt

1. Aktualisieren des vorhandenen Repositorys: `smsap repository update -repository -dbname repository_service_name -host repository_host_name -login -username repository_user_name -port repository_port`
 - Der Repository-Benutzername, der Repository-Dienstname und der Repository-Hostname können aus alphanumerischen Zeichen, einem Minuszeichen, einem Unterstrich und einem Zeitraum bestehen.
 - Der Repository-Port kann eine beliebige gültige Portnummer sein. Die anderen Optionen, die beim Aktualisieren des vorhandenen Repositorys verwendet werden, sind wie folgt:
 - Der `force` Option
 - Der `noprompt` Option
 - Der `quiet` Option
 - Der `verbose` Option

Beispiel

```
smsap repository update -repository -dbname HR1  
-host server1 -login -username admin -port 1521
```

Nachdem Sie fertig sind

Starten Sie den SnapManager-Server neu, um die zugehörigen Zeitpläne neu zu starten.

Ändern Sie die Backup-Aufbewahrungsklasse

Nach dem Upgrade weist SnapManager den vorhandenen Backups die standardmäßige Backup-Aufbewahrungsklasse zu. Sie können die Standardwerte für die Aufbewahrungsklassen entsprechend Ihren Backup-Anforderungen ändern.

Über diese Aufgabe

Die standardmäßige Backup-Aufbewahrungsklasse, die den vorhandenen Backups zugewiesen ist, lautet wie folgt:

Backup-Typ	Zuweisung von Aufbewahrungsklassen nach Upgrade
Backups werden für immer aufbewahrt	Unbegrenzt
Andere Backups	Täglich



Sie können die Backups löschen, die für immer aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Wenn Sie ein Upgrade auf SnapManager 3.0 oder höher durchführen, werden den vorhandenen Profilen der größere der folgenden beiden Werte zugewiesen:

- Vorherige Aufbewahrungsanzahl für das Profil
- Standardwerte für die Aufbewahrungsanzahl und die Dauer der täglichen Backups, wie im festgelegt `smsap.config` Datei

Schritt

1. Ändern Sie die zugewiesenen Werte `retain.hourly.count` Und `retain.hourly.duration` Im `smsap.config` Datei:

Der `smsap.config` Datei befindet sich unter `default installation location/properties/smsap.config`.

Beispiel

Sie können die folgenden Werte eingeben:

- ° `retain.hourly.count = 12`
- ° `retain.hourly.duration = 2`

Prozessarten wiederherstellen

Alle Wiederherstellungsprozesse werden in allen SnapManager für SAP-Versionen nicht unterstützt. Nach dem Upgrade von SnapManager müssen Sie auf den Wiederherstellungsprozess achten, den Sie zum Wiederherstellen eines Backups verwenden können.

Die mit SnapManager 3.0 oder höher erstellten Backups können sowohl mit schnellen Restore- als auch mit dateibasierten Restore-Prozessen wiederhergestellt werden. Die Backups, die mit einer älteren Version als SnapManager 3.0 erstellt wurden, können jedoch nur mit dem dateibasierten Wiederherstellungsprozess wiederhergestellt werden.

Sie können die SnapManager-Version bestimmen, die zum Erstellen des Backups verwendet wird, indem Sie das ausführen `-backup show` Befehl.

Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade

Der Rolling Upgrade-Ansatz, mit dem Sie Hosts auf gestaffelte, Host-für-Host-Art

aktualisieren können, wird von SnapManager 3.1 unterstützt.

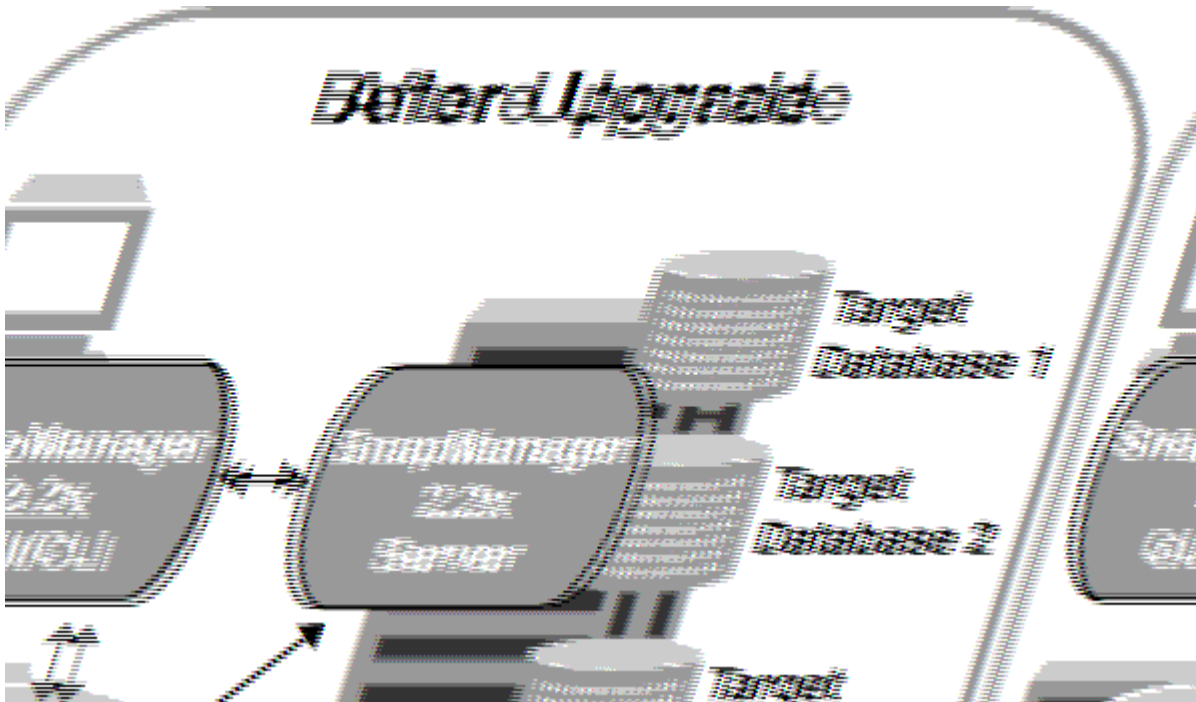
Mit SnapManager 3.0 oder einer älteren Version konnten Sie nur alle Hosts gleichzeitig aktualisieren. Dies führte zu Ausfallzeiten aller SnapManager-Hosts und der geplanten Betrieb während des Upgrade-Vorgangs.

Das Rolling Upgrade bietet folgende Vorteile:

- Verbesserte SnapManager Performance, da nur ein Host gleichzeitig aktualisiert wird.
- Fähigkeit, die neuen Funktionen auf einem SnapManager Server Host zu testen, bevor ein Upgrade der anderen Hosts durchgeführt wird



Rolling Upgrades können nur über die Befehlszeilenschnittstelle (CLI) durchgeführt werden.



Nach erfolgreichem Abschluss des Rolling Upgrade verfügen die SnapManager Hosts, Profile, Zeitpläne, Backups, Klone, die mit den Profilen der Zieldatenbanken verbunden sind, werden von der Repository-Datenbank der früheren SnapManager Version in die Repository-Datenbank der neuen Version migriert. Details zu den Vorgängen, die mithilfe der Profile, Zeitpläne, Backups und Klone, die in der früheren SnapManager Version erstellt wurden, stehen nun in der Repository-Datenbank der neuen Version zur Verfügung. Sie können die GUI mit den Standardkonfigurationswerten des `start user.config` Datei: Die im konfigurierten Werte `user.config` Datei der früheren Version von SnapManager wird nicht berücksichtigt.

Der aktualisierte SnapManager-Server kann jetzt mit der aktualisierten Repository-Datenbank kommunizieren. Die Hosts, die kein Upgrade durchgeführt haben, können ihre Zieldatenbanken mithilfe des Repositories der früheren Version von SnapManager managen. Somit können die in der früheren Version verfügbaren Funktionen genutzt werden.



Bevor Sie ein Rolling Upgrade durchführen, müssen Sie sicherstellen, dass alle Hosts unter der Repository-Datenbank aufgelöst werden können. Informationen zum Beheben der Hosts finden Sie im Abschnitt Fehlerbehebung in *SnapManager for SAP Administration Guide for UNIX*.

Verwandte Informationen

Voraussetzungen für Rolling Upgrades

Bevor Sie ein Rolling Upgrade durchführen, müssen Sie sicherstellen, dass Ihre Umgebung bestimmte Anforderungen erfüllt.

- Wenn Sie eine ältere Version als SnapManager 3.1 verwenden und ein Rolling Upgrade auf SnapManager 3.3 oder höher durchführen möchten, müssen Sie zuerst auf 3.2 und dann auf die neueste Version aktualisieren.

Sie können direkt von SnapManager 3.2 auf SnapManager 3.3 oder höher aktualisieren.

- Externe Skripte, die zur Durchführung externer Datensicherung oder Datenaufbewahrung verwendet werden, müssen gesichert werden.
- Die SnapManager-Version, auf die Sie aktualisieren möchten, muss installiert sein.



Wenn Sie ein Upgrade von einer älteren Version als SnapManager 3.1 auf SnapManager 3.3 oder höher durchführen, müssen Sie zuerst SnapManager 3.2 installieren und ein Rolling Upgrade durchführen. Nach dem Upgrade auf 3.2 können Sie SnapManager 3.3 oder höher installieren und ein weiteres Rolling Upgrade auf SnapManager 3.3 oder höher durchführen.

- Die SnapDrive für UNIX-Version, die von der SnapManager-Version unterstützt wird, auf die Sie aktualisieren möchten, muss installiert sein.

Die SnapDrive-Dokumentation enthält Details zur Installation von SnapDrive.

- Die Repository-Datenbank muss gesichert werden.
- Die SnapManager Repository-Auslastung sollte mindestens betragen.
- Wenn der zu aktualisierende Host ein Repository verwendet, dürfen SnapManager-Vorgänge nicht auf den anderen Hosts ausgeführt werden, die dasselbe Repository verwenden.

Die Vorgänge, die auf den anderen Hosts geplant oder ausgeführt werden, warten bis das Rolling Upgrade abgeschlossen ist.



Es wird empfohlen, ein Rolling Upgrade durchzuführen, wenn das Repository am wenigsten ausgelastet ist, z. B. über das Wochenende oder wenn Vorgänge nicht geplant sind.

- Profile, die auf dieselbe Repository-Datenbank verweisen, müssen mit unterschiedlichen Namen in den SnapManager-Server-Hosts erstellt werden.

Wenn Sie Profile mit dem gleichen Namen verwenden, schlägt das Rolling Upgrade der Repository-Datenbank ohne Warnung fehl.

- SnapManager-Vorgänge dürfen nicht auf dem Host ausgeführt werden, der gerade aktualisiert wird.



Das Rolling Upgrade wird länger ausgeführt, wenn die Anzahl der Backups der Hosts, die zusammen aktualisiert werden, steigt. Die Dauer des Upgrades kann je nach Anzahl der Profile und Backups variieren, die mit einem bestimmten Host verbunden sind.

Führen Sie Rolling Upgrade auf einem einzelnen oder mehreren Hosts durch

Sie können Rolling Upgrades für einen einzelnen oder mehrere SnapManager Server Hosts über die Befehlszeilenschnittstelle (CLI) durchführen. Der aktualisierte SnapManager-Server-Host wird dann nur mit der späteren Version von SnapManager verwaltet.

Was Sie benötigen

Sie müssen sicherstellen, dass alle Voraussetzungen für das Durchführen eines Rolling Upgrades abgeschlossen sind.

Schritte

1. Geben Sie den folgenden Befehl ein, um ein Rolling Upgrade auf einem einzelnen Host durchzuführen:

```
smsap repository rollingupgrade -repository-dbname repo_service_name -host  
repo_host -login -username repo_username -port repo_port -upgradehost  
host_with_target_database -force [-quiet | -verbose]
```

Beispiel

Der folgende Befehl führt das Rolling Upgrade aller auf HostA eingebundenen Zieldatenbanken und einer Repository-Datenbank namens repoA auf repo_Host durch:

```
smsap repository rollingupgrade  
  -repository  
    -dbname repoA  
    -host repo_host  
  -login  
    -username repouser  
    -port 1521  
  -upgradehost hostA
```

2. Geben Sie den folgenden Befehl ein, um ein Rolling Upgrade auf mehreren Hosts durchzuführen: **smsap repository rollingupgrade -repository -dbname *repo_service_name* -host *repo_host* -login -username *repo_username* -port *repo_port* -upgradehost *host_with_target_database1,host_with_target_database2* -force [-quiet | -verbose]**



Geben Sie bei mehreren Hosts die durch Komma getrennten Hostnamen ein, und stellen Sie sicher, dass Sie keinen Speicherplatz zwischen dem Komma und dem nächsten Hostnamen angeben. Wenn Sie eine RAC-Konfiguration (Real Application Clusters) verwenden, müssen Sie alle RAC-verbundenen Hosts manuell aktualisieren. Verwenden Sie können `-allhosts` So führen Sie das Rolling Upgrade aller Hosts durch.

Beispiel

Der folgende Befehl führt das Rolling Upgrade aller auf den Hosts eingebundenen Zieldatenbanken, hostA und hostB sowie einer Repository-Datenbank namens repoA auf repo_Host durch:

```
smsap repository rollingupgrade
  -repository
    -dbname repoA
    -host repo_host
    -login
      -username repouser
      -port 1521
    -upgradehost hostA,hostB
```

3. Um ein Rolling Upgrade auf allen Hosts einer Repository-Datenbank durchzuführen, geben Sie den folgenden Befehl ein:

```
smsap repository rollingupgrade -repository -dbname repo_service_name -host  
repo_host -login -username repo_username -port repo_port -allhosts -force [-  
quiet | -verbose]
```

Nachdem Sie die Repository-Datenbank erfolgreich aktualisiert haben, können Sie alle SnapManager-Vorgänge auf der Zieldatenbank ausführen.

Beispiel

Der folgende Befehl führt das Rolling Upgrade aller Zieldatenbanken durch, die in einer Repository-Datenbank mit dem Namen „repoA“ auf repo_Host verfügbar sind:

```
smsap repository rollingupgrade
  -repository
    -dbname repoA
    -host repo_host
    -login
      -username repouser
      -port 1521
    -allhosts
```

Nachdem Sie fertig sind

- Wenn der SnapManager-Server automatisch startet, müssen Sie den Server neu starten, um sicherzustellen, dass Sie die Zeitpläne anzeigen können.
- Wenn Sie einen der beiden zugehörigen Hosts aktualisieren, müssen Sie nach dem ersten Upgrade des zweiten Hosts ein Upgrade durchführen.

Wenn Sie beispielsweise einen Klon von Host A nach Host B erstellt oder ein Backup von Host A an Host B angehängt haben, hängen die Hosts A und B miteinander zusammen. Wenn Sie Host A aktualisieren, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, den Host B bald nach dem Upgrade von Host A zu aktualisieren



Die Warnmeldungen werden angezeigt, obwohl der Klon gelöscht wurde oder das Backup während des Rolling Upgrades von Host A von Host B abgehängt wurde. Dies liegt daran, dass Metadaten im Repository für die Vorgänge vorhanden sind, die auf dem Remote-Host durchgeführt werden.

Was ist ein Rollback

Mit dem Rollback-Vorgang können Sie nach einem Rolling Upgrade auf eine frühere SnapManager-Version zurücksetzen.



Bevor Sie ein Rollback durchführen können, müssen Sie sicherstellen, dass alle Hosts unter der Repository-Datenbank aufgelöst werden können.

Wenn Sie ein Rollback durchführen, werden die folgenden Schritte zurückgesetzt:

- Backups, die erstellt, freigegeben und gelöscht wurden, verwenden Sie dazu die SnapManager Version, von der Sie ein Rollback durchführen
- Klone, die anhand eines Backups erstellt wurden, die mit der SnapManager Version erstellt wurden, von der aus Sie ein Rollback durchführen
- Profildaten wurden mithilfe der SnapManager-Version geändert, von der aus Sie ein Rollback ausführen
- Sicherungsstatus des Backups, das mit der SnapManager-Version geändert wurde, von der aus Sie ein Rollback durchführen

Die Funktionen, die in der von Ihnen verwendeten SnapManager-Version verfügbar waren, aber in der Version, auf die Sie zurückrollt, nicht verfügbar sind, werden nicht unterstützt. Wenn Sie beispielsweise ein Rollback von SnapManager 3.3 oder neuer zu SnapManager 3.1 durchführen, wird die Verlaufsconfiguration für Profile in SnapManager 3.3 oder höher nicht auf die Profile in SnapManager 3.1 zurückgesetzt. Dies liegt daran, dass die Verlaufsconfiguration in SnapManager 3.1 nicht verfügbar war.

Einschränkungen bei der Durchführung eines Rollbacks

Sie müssen die Szenarien kennen, in denen Sie kein Rollback durchführen können. In einigen dieser Szenarien können Sie jedoch einige zusätzliche Aufgaben ausführen, bevor Sie das Rollback durchführen.

Die Szenarien, in denen Sie kein Rollback durchführen können oder die zusätzlichen Aufgaben ausführen müssen, sind wie folgt:

- Wenn Sie nach einem Rolling Upgrade einen der folgenden Vorgänge ausführen:
 - Erstellen Sie ein neues Profil.
 - Teilen Sie einen Klon auf.
 - Ändern Sie den Schutzstatus des Profils.
 - Zuweisung von Sicherungsrichtlinien, Aufbewahrungsklassen oder SnapVault- und SnapMirror-Beziehungen

In diesem Szenario müssen Sie nach dem Durchführen eines Rollback die zugewiesene Sicherungsrichtlinie, die Aufbewahrungsklasse oder die zugewiesene SnapVault- und SnapMirror-Beziehung manuell entfernen.

- Ändern Sie den Mount-Status des Backups.

In diesem Szenario müssen Sie zuerst den Mount-Status in den ursprünglichen Zustand ändern und dann ein Rollback durchführen.

- Stellen Sie ein Backup wieder her.
- Ändern Sie den Authentifizierungsmodus von der Datenbankauthentifizierung in die Betriebssystemauthentifizierung.

In diesem Szenario müssen Sie nach einem Rollback den Authentifizierungsmodus manuell von OS in die Datenbank ändern.

- Wenn der Hostname des Profils geändert wird
- Wenn Profile getrennt sind, um Archiv-Log-Backups zu erstellen

In diesem Szenario können Sie keine Rollbacks auf eine Version durchführen, die früher als SnapManager 3.2 ist.

Voraussetzungen für die Durchführung eines Rollbacks

Bevor Sie ein Rollback durchführen, müssen Sie sicherstellen, dass Ihre Umgebung bestimmte Anforderungen erfüllt.

- Wenn Sie SnapManager 3.3 oder höher verwenden und zu einer älteren Version als SnapManager 3.1 zurückkehren möchten, müssen Sie ein Rollback auf 3.2 und dann auf die gewünschte Version durchführen.
- Externe Skripte, die zur Durchführung externer Datensicherung oder Datenaufbewahrung verwendet werden, müssen gesichert werden.
- Die SnapManager-Version, auf die Sie einen Rollback ausführen möchten, muss installiert sein.



Wenn Sie ein Rollback von SnapManager 3.3 oder neuer auf eine Version vor SnapManager 3.1 durchführen möchten, müssen Sie zuerst SnapManager 3.2 installieren und ein Rollback durchführen. Nach einem Rollback auf 3.2 können Sie SnapManager 3.1 oder eine frühere Version installieren und ein weiteres Rollback auf diese Version durchführen.

- Die SnapDrive für UNIX-Version, die mit der SnapManager-Version unterstützt wird, zu der Sie einen Rollback ausführen möchten, muss installiert sein.

Informationen zum Installieren von SnapDrive finden Sie unter SnapDrive-Dokumentationssatz.

- Die Repository-Datenbank muss gesichert werden.
- Wenn der zurückzugerollte Host ein Repository verwendet, dürfen SnapManager-Vorgänge nicht auf den anderen Hosts ausgeführt werden, die dasselbe Repository verwenden.

Der geplante oder auf den anderen Hosts ausgeführte Betrieb wartet auf den Abschluss des Rollbacks.

- Profile, die auf dieselbe Repository-Datenbank verweisen, müssen mit unterschiedlichen Namen in den SnapManager-Server-Hosts erstellt werden.

Wenn Sie Profile mit demselben Namen verwenden, schlägt der Rollback-Vorgang mit dieser Repository-Datenbank ohne Warnung fehl.

- SnapManager-Vorgänge dürfen nicht auf dem Host ausgeführt werden, den Sie zurücksetzen möchten.

Wenn ein Vorgang ausgeführt wird, müssen Sie warten, bis dieser Vorgang abgeschlossen ist, und bevor Sie mit dem Rollback fortfahren.



Der Rollback-Vorgang wird längere Zeit ausgeführt, da sich die kumulative Anzahl von Backups der Hosts, die gemeinsam wieder erstellt werden, erhöht. Die Dauer des Rollbacks kann je nach Anzahl der Profile und Backups, die mit einem bestimmten Host verbunden sind, variieren.

["Dokumentation auf der NetApp Support Site: mysupport.netapp.com"](https://mysupport.netapp.com)

Führen Sie ein Rollback auf einem oder mehreren Hosts durch

Sie können auf einem oder mehreren SnapManager Server Hosts ein Rollback durchführen, indem Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Was Sie benötigen

Sie müssen sicherstellen, dass alle Voraussetzungen für die Durchführung eines Rollbacks abgeschlossen sind.

Schritte

1. Geben Sie den folgenden Befehl ein, um ein Rollback auf einem einzelnen Host durchzuführen:

```
smsap repository rollback -repository -dbname repo_service_name -host  
repo_host -login -username repo_username -port repo_port -rollbackhost  
host_with_target_database
```

Beispiel

Das folgende Beispiel zeigt den Befehl zum Rollback aller Zieldatenbanken, die auf hostA gemountet sind, und eine Repository-Datenbank namens repoA, die sich auf dem Repository-Host, repo_Host, befindet:

```
smsap repository rollback  
  -repository  
    -dbname repoA  
    -host repo_host  
  -login  
    -username repouser  
    -port 1521  
  -rollbackhost hostA
```

2. Geben Sie den folgenden Befehl ein, um ein Rollback auf mehreren Hosts durchzuführen:

```
smsap repository rollback -repository-database repo_service_name -host repo_host  
-login -username repo_username -port repo_port -rollbackhost  
host_with_target_database1,host_with_target_database2
```



Geben Sie bei mehreren Hosts die durch Komma getrennten Hostnamen ein, und stellen Sie sicher, dass zwischen dem Komma und dem nächsten Hostnamen kein Platz vorhanden ist.

Wenn Sie die Real Application Clusters (RAC)-Konfiguration verwenden, müssen Sie alle RAC-verbundenen Hosts manuell wiederherstellen. Verwenden Sie können `-allhosts` Um ein Rollback aller Hosts durchzuführen.

Beispiel

Das folgende Beispiel zeigt den Befehl zum Rollback aller Zieldatenbanken, die auf den Hosts gemountet sind, `hostA`, `hostB` und eine Repository-Datenbank namens `repoA` auf dem Repository-Host, `repo_host`:

```
smsap repository rollback
  -repository
    -dbname repoA
    -host repo_host
    -login
      -username repouser
      -port 1521
    -rollbackhost hostA,hostB
```

Die Hosts, Profile, Zeitpläne, Backups und Klone, die mit den Profilen der Zieldatenbanken für den Host verbunden sind, werden in das frühere Repository zurückgesetzt.

Aufgaben nach dem Rollback ausführen

Sie müssen einige weitere Schritte durchführen, nachdem Sie eine Repository-Datenbank zurückgesetzt und den SnapManager-Host von SnapManager 3.2 auf SnapManager 3.0 heruntergestuft haben, um die Zeitpläne anzuzeigen, die in der früheren Version der Repository-Datenbank erstellt wurden.

Schritte

1. Navigieren Sie zu `cd /opt/NetApp/smsap/repositories`.

Der `repositories` Das Verzeichnis kann zwei Dateien für jedes Repository enthalten. Der Dateiname mit dem Zahlenzeichen (#) wird mit SnapManager 3.1 oder höher erstellt und der Dateiname mit dem Bindestrich (-) wird mit dem SnapManager 3.0 erstellt.

Beispiel

Die Dateinamen können wie folgt lauten:

- `repository#SMSAP300a#SMSAPREPO1#10.72.197.141#1521`
- `repository-smsap300a-smsaprep01-10.72.197.141-1521`

2. Ersetzen Sie das Zahlenzeichen (#) im Dateinamen durch den Bindestrich (-).

Beispiel

Der Dateiname, der das Zahlenzeichen (#) hatte, enthält jetzt Bindestrich (-): repository-SMSAP300a-SMSAPREPO1-10.72.197.141-1521.

Weitere Schritte

Nach der Installation von SnapManager und dem erfolgreichen Erstellen eines Backups können Sie mit SnapManager Wiederherstellungs-, Recovery- und Klonvorgänge durchführen. Zusätzlich erhalten Sie eventuell Informationen zu anderen SnapManager Funktionen, wie zum Beispiel Planung, Management des SnapManager Betriebs und Aufrechterhaltung der Historie von Aktivitäten.

Weitere Informationen zu diesen Funktionen sowie Informationen zur Version von SnapManager finden Sie in der folgenden Dokumentation. Alle Informationen finden Sie im ["NetApp Support"](#).

- ["SnapManager 3.4.1 für SAP – Administratorhandbuch für UNIX"](#)

Beschreibt die Konfiguration von SnapManager für SAP. Die Themen umfassen das Konfigurieren, Sichern, Wiederherstellen und Klonen von Datenbanken, das Durchführen von Sekundärschutz, Außerdem eine Erläuterung der CLI-Befehle.

- ["Versionshinweise zu SnapManager 3.4 für SAP"](#)

Beschreibt neue Funktionen, feste Probleme, wichtige Vorsichtsmaßnahmen, bekannte Probleme und Einschränkungen für SnapManager for SAP.

- *SnapManager for SAP Online-Hilfe*

Beschreibt die Schritt-für-Schritt-Verfahren zur Durchführung verschiedener SnapManager-Vorgänge mithilfe der SnapManager-Benutzeroberfläche.



Die *Online-Hilfe* ist in die SnapManager-Benutzeroberfläche integriert und steht nicht auf der Support-Website zur Verfügung.

- ["Technischer Bericht 3761: SnapManager für Oracle: Best Practices"](#)

Beschreibt die Best Practices von SnapManager für Oracle.

- ["NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage"](#)

Beschreibt Best Practices zur Konfiguration von Oracle Datenbanken auf NetApp Storage-Systemen.

- ["Technischer Bericht 3442: SAP with Oracle on UNIX and NFS and NetApp Storage"](#)

Beschreibt Best Practices für die Implementierung von NetApp Storage für den Support von SAP-Lösungen.

Verwandte Informationen

["NetApp Support"](#)

["NetApp Dokumentation: Produktbibliothek A-Z"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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