Produktübersicht

SnapManager Oracle

NetApp
November 04, 2025

Inhalt

Produktübersicht

SnapManager für Oracle automatisiert und vereinfacht komplexe, manuelle und zeitintensive Prozesse, die im Zusammenhang mit Backup, Recovery und Klonen von Oracle 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 lässt sich mit nativen Oracle Technologien wie Oracle Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) und Direct NFS über FC-, iSCSI- und NFS-Protokolle integrieren. Optional können mit SnapManager erstellte Backups mit dem Oracle Recovery Manager (RMAN) katalogisiert werden, um die Backup-Informationen zu erhalten. Diese Backups können später in Restore-Vorgängen auf Blockebene oder in zeitpunktgenauen Recovery-Vorgängen verwendet werden.

SnapManager Highlights

SnapManager ermöglicht die nahtlose Integration mit Oracle Datenbanken auf dem UNIX Host und über das Backend mit NetApp Snapshot, SnapRestore und FlexClone Technologien 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

  Sie können die Datendateien und Protokolldateien separat archivieren.

- Planen von Backups
- Wiederherstellung von vollständigen oder teilweisen 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.

- Erstellung platzsparender Backup-Klone auf primären oder sekundären Storage-Systemen

  SnapManager ermöglicht Ihnen die Aufteilung eines Datenbankklonen.

Backups mit Snapshot Kopien erstellen

Mit SnapManager können Sie Backups auf dem primären (lokalen) Storage und auch auf dem sekundären (Remote-) Storage mithilfe von Sicherungsrichtlinien oder Nachbearbeitungsskripten erstellen.

Als Snapshot-Kopien erstellte Backups sind virtuelle Kopien der Datenbank und werden auf demselben physischen Medium wie die Datenbank gespeichert. Der Backup-Vorgang dauert daher weniger Zeit und erfordert deutlich weniger Speicherplatz als vollständige Disk-to-Disk Backups. Mit SnapManager können Sie Folgendes sichern:

- Alle Datendateien, archivierte Log-Dateien und Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces, alle Archivprotokolldateien und Kontrolldateien

Mit SnapManager 3.2 oder höher können Sie optional folgende Daten sichern:

- Alle Datendateien und die Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces zusammen mit den Kontrolldateien
- Archivierung von Protokolldateien

Die Datendateien, Archiv-Log-Dateien und Kontrolldateien können auf verschiedenen Storage-Systemen, Storage-System-Volumes oder LUNs (Logical Unit Numbers) abgelegt werden. Sie können SnapManager auch zum Backup einer Datenbank verwenden, wenn sich mehrere Datenbanken auf demselben Volume oder LUN befinden.

Warum sollten Sie Archiv Log-Dateien beschneiden

Mit SnapManager für Oracle können Sie Archivprotokolldateien aus dem aktiven, bereits gesicherten Dateisystem löschen.

Durch Beschneidung kann SnapManager Backups einzelner Archiv-Log-Dateien erstellen. Durch Beschneidung und die Richtlinie zur Aufbewahrung von Backups wird beim Säuberen von Backups der Speicherplatz für das Archiv-Protokoll freigegeben.

Sie können die Archivprotokolldateien nicht beschneiden, wenn der Flash Recovery Area (FRA) für Archivprotokolldateien aktiviert ist. Wenn Sie im Bereich Flash Recovery den Speicherort für das Archivprotokoll angeben, müssen Sie im Parameter Archive_log_dest auch den Speicherort für das Archivprotokoll angeben.

Konsolidierung von Archivierungsprotokolldaten

Mit SnapManager (3.2 oder höher) für Oracle werden die Archiv-Log-Backups konsolidiert, um eine Mindestanzahl an Backups für Archivierungs-Log-Dateien beizubehalten. SnapManager für Oracle erkennt und befreit die Backups, die Archivprotokolle enthalten, die Teilmengen anderer Backups sind.

Vollständige oder teilweise Wiederherstellung von Datenbanken

SnapManager bietet die Flexibilität, komplette Datenbanken, bestimmte Tabellen, Dateien, Kontrolldateien oder eine Kombination dieser Einheiten wiederherzustellen. SnapManager ermöglicht die Wiederherstellung von Daten mithilfe eines dateibasierten Wiederherstellungsprozesses mit einem schnelleren, Volume-basierten Wiederherstellungsprozess. Datenbankadministratoren können den Prozess auswählen, den sie verwenden möchten, oder SnapManager entscheiden lassen, welcher Prozess für Sie geeignet ist.

SnapManager ermöglicht Datenbankadministratoren (DBAs) die Vorschau von Restore-Vorgängen. Mit der Vorschaufunktion können DBAs jeden Wiederherstellungsvorgang auf Datei-für-Datei-Basis anzeigen.

Datenbankadministratoren können das Level angeben, auf das SnapManager bei der Durchführung von Restore-Vorgängen wiederhergestellt und Informationen wiederhergestellt werden. Beispielsweise können DBAs Daten zu bestimmten Zeitpunkten wiederherstellen. Der Wiederherstellungspunkt kann ein Datum und eine Uhrzeit oder eine Oracle System Change Number (SCN) sein.

Datenbankadministratoren können die Datenbank mit SnapManager wiederherstellen und ein anderes Tool verwenden, um die Informationen wiederherzustellen. DBAs müssen für beide Vorgänge keine SnapManager verwenden.

Mit SnapManager (3.2 oder höher) können Datenbank-Backups automatisch und ohne Eingriff des Datenbankadministrators wiederhergestellt werden. Sie können SnapManager verwenden, um Backups für Archivprotokolle zu erstellen und dann diese Backups für Archivprotokolle zu verwenden, um die Datenbank-Backups wiederherzustellen und wiederherzustellen. Selbst wenn die Archivprotokolldateien des Backups in einem externen Archivprotokoll verwaltet werden, können Sie diesen externen Speicherort angeben, damit diese Archivprotokolle zur Wiederherstellung der wiederhergestellten Datenbank beitragen können.

Überprüfen des Backup-Status

SnapManager kann die Integrität des Backups mithilfe von standardmäßigen Oracle-Backup-Verifizierungsvorgängen bestätigen.

Datenbankadministratoren (DBAs) können die Verifizierung im Rahmen des Backup-Vorgangs oder einer anderen Zeit durchführen. Datenbankadministratoren können den Verifizierungsvorgang so einstellen, dass er bei geringerer Auslastung des Host-Servers oder während eines geplanten Wartungsfensters ausgeführt wird.

Datenbank-Backup-Klone

SnapManager erstellt mithilfe der FlexClone Technologie einen beschreibbaren, platzsparenden Klon eines Datenbank-Backups. Sie können einen Klon ändern, ohne die Backup-Quelle zu ändern.

Möglicherweise möchten Sie Datenbanken klonen, um Tests oder Upgrades in nicht produktiven Umgebungen zu ermöglichen. Sie können eine Datenbank mit einem primären oder sekundären Storage klonen. Ein Klon kann sich auf demselben Host oder einem anderen Host befinden wie die Datenbank.

Mit der FlexClone Technologie können SnapManager Snapshot-Kopien der Datenbank verwenden, sodass

keine vollständige physische Disk-to-Disk-Kopie erstellt werden muss. Snapshot Kopien benötigen weniger Erstellungszeit und belegen deutlich weniger Speicherplatz als physische Kopien.

In der Data ONTAP Dokumentation finden Sie weitere Informationen zur FlexClone Technologie.

Verwandte Informationen

"Data ONTAP documentation: mysupport.netapp.com/documentation/productsatoz/index.html"

Verfolgen Sie die Details und erstellen Sie Berichte

SnapManager bietet nicht nur detaillierte Datenbankadministratoren, die den Status verschiedener Vorgänge verfolgen müssen, sondern mithilfe von Methoden, die Vorgänge über eine einheitliche Benutzeroberfläche überwachen.

Nachdem Administratoren festlegen, welche Datenbanken gesichert werden sollen, identifiziert SnapManager die Datenbankdateien für das Backup automatisch. SnapManager zeigt Informationen zu Repositorys, Hosts, Profilen, Backups und Klonen an. Sie können die Vorgänge auf bestimmten Hosts oder Datenbanken überwachen.Sie können auch die geschützten Backups identifizieren und bestimmen, ob die Backups in Bearbeitung sind oder geplant werden.

Repositories

SnapManager organisiert die Informationen in Profile, die dann den Repositories zugeordnet werden. Profile enthalten Informationen über die zu verwaltende Datenbank, während das Repository Daten zu den Vorgängen enthält, die auf Profilen ausgeführt werden.

Das Repository zeichnet auf, wann ein Backup durchgeführt wurde, welche Dateien gesichert wurden und ob ein Klon aus dem Backup erstellt wurde. Wenn Datenbankadministratoren eine Datenbank wiederherstellen oder einen Teil davon wiederherstellen, fragt SnapManager das Repository ab, um zu ermitteln, was gesichert wurde.

Da das Repository die Namen der während des Backup erstellten Datenbank-Snapshot-Kopien speichert, kann die Repository-Datenbank nicht in derselben Datenbank vorhanden sein und kann auch nicht Teil derselben Datenbank sein, die von SnapManager gesichert wird. Sie müssen mindestens zwei Datenbanken (die SnapManager Repository-Datenbank und die von SnapManager gemanagte Zieldatenbank) einrichten und ausführen, wenn Sie SnapManager Vorgänge ausführen.

Wenn Sie versuchen, die grafische Benutzeroberfläche (GUI) zu öffnen, wenn die Repository-Datenbank nicht verfügbar ist, wird die folgende Fehlermeldung in der Datei sm_gui.log protokolliert: [WARNUNG]: SMO-01106: Beim Abfragen des Repository ist ein Fehler aufgetreten: Keine Daten mehr aus dem Socket zu lesen. Außerdem schlägt das SnapManager-Verfahren fehl, wenn die Repository-Datenbank ausfällt. Weitere Informationen zu den verschiedenen Fehlermeldungen finden Sie unter *Fehlerbehebung bekannter Probleme*.

Sie können jeden beliebigen Host-Namen, Dienstnamen oder Benutzernamen verwenden, um Vorgänge auszuführen. Damit ein Repository SnapManager-Vorgänge unterstützt, müssen der Projektarchiv-Benutzername und der Dienstname nur aus den folgenden Zeichen bestehen: Alphabetische Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-), Unterstrich (_) und Punkt (.).

Der Repository-Port kann eine beliebige gültige Portnummer sein, und der Repository-Hostname kann einen beliebigen gültigen Hostnamen sein. Der Hostname muss aus alphabetischen Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-) und Periode (.) bestehen, jedoch nicht aus einem Unterstrich (_).

Das Repository muss in einer Oracle-Datenbank erstellt werden. Die von SnapManager verwendete Datenbank sollte gemäß den Oracle Verfahren für die Datenbankkonfiguration eingerichtet werden.

Ein einziges Repository kann Informationen über mehrere Profile enthalten, jedoch ist jede Datenbank normalerweise nur mit einem Profil verknüpft. Sie können mehrere Repositorys haben, wobei jedes Repository mehrere Profile enthält.

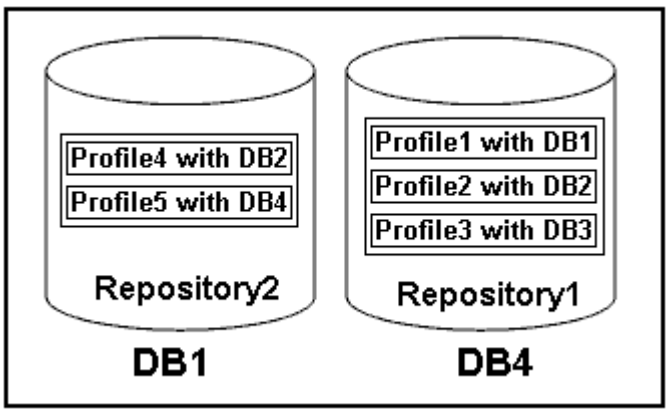
Welche Profile sind

SnapManager verwendet Profile, um die zur Durchführung von Operationen in einer bestimmten Datenbank erforderlichen Informationen zu speichern. Ein Profil enthält die Informationen zur Datenbank einschließlich aller Anmeldeinformationen, Backups und Klone. Wenn Sie ein Profil erstellen, müssen Sie keine Datenbankdetails angeben, wenn Sie eine Operation in dieser Datenbank ausführen.

Ein Profil kann nur auf eine Datenbank verweisen. Auf dieselbe Datenbank kann mit mehr als einem Profil verwiesen werden. Auf Backups, die mit einem Profil erstellt werden, kann nicht über ein anderes Profil zugegriffen werden, auch wenn beide Profile auf dieselbe Datenbank verweisen.

Profilinformationen werden in einem Repository gespeichert. Das Repository enthält sowohl die Profilinformationen für die Datenbank als auch Informationen zu den Snapshot-Kopien, die als Datenbank-Backup dienen. Die tatsächlichen Snapshot Kopien werden im Storage-System gespeichert. Die Namen der Snapshot Kopie werden im Repository gespeichert, das das Profil für diese Datenbank enthält. Wenn Sie einen Vorgang in einer Datenbank ausführen, müssen Sie das Profil aus dem Repository auswählen.

Die folgende Abbildung zeigt, wie Repositories mehrere Profile aufnehmen können, aber auch dass jedes Profil nur eine Datenbank definieren kann:



Im vorhergehenden Beispiel befindet sich Repository2 auf Datenbank DB1 und Repository1 befindet sich auf der Datenbank DB4.

Jedes Profil enthält die Anmeldeinformationen für die Datenbank, die mit dem Profil verknüpft ist. Mit den Anmeldeinformationen kann SnapManager eine Verbindung zur Datenbank herstellen und mit der Datenbank arbeiten. Die gespeicherten Anmeldeinformationen umfassen den Benutzernamen und die Kennwortpaare für den Zugriff auf den Host, das Repository, die Datenbank und die erforderlichen Verbindungsinformationen, wenn Sie Oracle Recovery Manager (RMAN) verwenden.

Sie können nicht auf ein Backup zugreifen, das mit einem Profil aus einem anderen Profil erstellt wurde, auch wenn beide Profile mit derselben Datenbank verknüpft sind. SnapManager legt eine Sperre auf die Datenbank ab, um zu verhindern, dass zwei inkompatible Vorgänge gleichzeitig ausgeführt werden.

Profil zur Erstellung vollständiger und partieller Backups

Sie können Profile erstellen, um vollständige Backups oder partielle Backups zu erstellen.

Die Profile, die Sie zur Erstellung der vollständigen und partiellen Backups angeben, enthalten sowohl die Datendateien als auch die Archivprotokolldateien. SnapManager erlaubt solche Profile nicht, die Backups des Archivprotokolls von den Backups der Datendatei zu trennen. Die vollständigen und teilweisen Backups werden basierend auf den vorhandenen Richtlinien zur Backup-Aufbewahrung aufbewahrt und basierend auf den vorhandenen Sicherungsrichtlinien geschützt. Sie können vollständige und teilweise Backups basierend auf der zu Ihnen passt Uhrzeit und Häufigkeit planen.

Profile für die Erstellung von datenbasierten Backups und nur-Archiv-Backups

Mit SnapManager (3.2 oder höher) können Sie Profile erstellen, die Backups der Archivprotokolldateien getrennt von den Datendateien machen. Nachdem Sie das Profil zur Trennung der Backup-Typen verwendet haben, können Sie entweder Datendateien-only-Backups oder lediglich Archiv-Log-Backups der Datenbank erstellen. Sie können auch ein Backup erstellen, das sowohl die Datendateien als auch die Archivprotokolldateien enthält.

Die Aufbewahrungsrichtlinie gilt für alle Datenbank-Backups, wenn die Archiv-Log-Backups nicht getrennt sind. Nachdem Sie die Backups für das Archivprotokoll getrennt haben, können Sie in SnapManager unterschiedliche Aufbewahrungszeiträume und Sicherungsrichtlinien für die Backups des Archivierungsprotokolls festlegen.

Aufbewahrungsrichtlinie

SnapManager legt fest, ob ein Backup aufbewahrt werden soll, indem sowohl die Anzahl der Aufbewahrung (z. B. 15 Backups) als auch die Aufbewahrungsdauer (z. B. 10 Tage tägliche Backups) berücksichtigt werden. Ein Backup läuft ab, wenn sein Alter die für seine Aufbewahrungsklasse festgelegte Aufbewahrungsdauer überschreitet und die Anzahl der Backups die Anzahl der Backups übersteigt. Beispiel: Wenn die Backup-Anzahl 15 beträgt (was bedeutet, dass SnapManager 15 erfolgreiche Backups erstellt hat) und die Dauer für tägliche Backups von 10 Tagen festgelegt wurde, verfallen die fünf ältesten, erfolgreichen und infrage kommenden Backups.

Aufbewahrungsdauer des Archivprotokolls

Nach Trennung der Backup-Protokolle werden sie basierend auf der Aufbewahrungsdauer des Archivprotokolls aufbewahrt. Backups von Archivprotokolldateien, die mit Backups von Datendateien erstellt werden, werden immer zusammen mit Backups dieser Datendateien aufbewahrt, unabhängig von der Aufbewahrungsdauer für das Archivprotokoll.

Verwandte Informationen

Profilverwaltung für effiziente Backups

Die Status der SnapManager-Operation lauten

SnapManager-Vorgänge (Backup, Wiederherstellung und Klon) können den jeweiligen Status aufweisen, wobei jeder Status den Fortschritt des Vorgangs angibt.

Betriebsstatus	Beschreibung
Erfolgreich	Die Operation wurde erfolgreich abgeschlossen.
Wird Ausgeführt	Der Vorgang wurde gestartet, ist aber noch nicht abgeschlossen. Ein Backup, das zwei Minuten dauert, wird beispielsweise um 11:00 Uhr morgens erstellt. Wenn Sie die Registerkarte **Zeitplan** um 11:01 Uhr aufrufen, wird der Vorgang als ausgeführt angezeigt.
Kein Vorgang gefunden	Der Zeitplan wurde nicht ausgeführt oder das letzte Backup wurde gelöscht.
Fehlgeschlagen	Der Vorgang ist fehlgeschlagen. SnapManager hat den Abbruchvorgang automatisch ausgeführt und den Vorgang bereinigt. **Hinweis:** Sie können den erstellten Klon teilen. Wenn Sie den geteilten Klon-Vorgang beenden, den Sie gestartet haben und der Vorgang erfolgreich angehalten wurde, wird der Status des Klon-Split-Vorgangs als fehlgeschlagen angezeigt.

Wiederherstellbare und nicht wiederherstellbare Ereignisse

Ein wiederherstellbares SnapManager Ereignis hat die folgenden Probleme:

- Die Datenbank wird nicht auf einem Storage-System gespeichert, auf dem Data ONTAP ausgeführt wird.
- Eine ASM-Datenbank (Automatic Storage Management) wird konfiguriert, die ASM-Instanz wird jedoch nicht ausgeführt.
- SnapDrive für UNIX ist nicht installiert oder kann nicht auf das Speichersystem zugreifen.
- SnapManager erstellt keine Snapshot Kopie bzw. stellt keinen Storage bereit, wenn das Volume über keinen freien Speicherplatz verfügt, die maximale Anzahl an Snapshot Kopien erreicht oder eine unerwartete Ausnahme auftritt.

Wenn ein wiederherstellbares Ereignis eintritt, wird SnapManager abgebrochen und versucht, den Host, die Datenbank und das Storage-System auf den Startstatus zurückzusetzen. Schlägt der Abbruchvorgang fehl, behandelt SnapManager den Vorfall als nicht wiederherstellbares Ereignis.

Wenn eines der folgenden Ereignisse eintritt, tritt ein nicht behebbares (Out-of-Band)-Ereignis auf:

- Ein Systemproblem tritt auf, z. B. wenn ein Host ausfällt.
- Der SnapManager-Prozess wird angehalten.
- Der Abbruch innerhalb des Band schlägt fehl, wenn das Speichersystem ausfällt, die Nummer der logischen Einheit (LUN) oder das Speichervolume offline ist oder das Netzwerk ausfällt.

Wenn ein nicht behebbares Ereignis eintritt, wird SnapManager sofort abgebrochen. Der Host, die Datenbank und das Speichersystem sind möglicherweise nicht an den ursprünglichen Status zurückgekehrt. In diesem Fall müssen Sie nach Ausfall des SnapManager-Vorgangs eine Bereinigung durchführen, indem Sie die verwaiste Snapshot Kopie löschen und die SnapManager-Sperrdatei entfernen.

Wenn Sie die SnapManager-Sperrdatei löschen möchten, navigieren Sie auf dem Zielcomputer zu Oracle_HOME €und löschen Sie die Datei SM_Lock_TargetDBName. Nach dem Löschen der Datei müssen Sie den SnapManager für Oracle-Server neu starten.

Wie SnapManager die Sicherheit gewährleistet

Sie können SnapManager Vorgänge nur ausführen, wenn Sie die entsprechenden Anmeldedaten besitzen. Die Sicherheit in SnapManager unterliegt der Benutzerauthentifizierung und der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC). RBAC ermöglicht Datenbankadministratoren die Einschränkung von Vorgängen, die SnapManager auf den Volumes und LUNs ausführen kann, die die Datendateien in einer Datenbank enthalten.

Datenbankadministratoren ermöglichen die rollenbasierte Zugriffssteuerung für SnapManager mithilfe von SnapDrive. Datenbankadministratoren weisen anschließend SnapManager-Rollen Berechtigungen zu und weisen diese Rollen den Benutzern in der grafischen Benutzeroberfläche (GUI) oder der Befehlszeilenschnittstelle (CLI) von Operations Manager zu. RBAC-Berechtigungsprüfungen erfolgen im DataFabric Manager Server.

Zusätzlich zum rollenbasierten Zugriff behält SnapManager die Sicherheit bei, indem er die Benutzerauthentifizierung über Passwortaufforderungen oder die Festlegung von Benutzeranmeldeinformationen anfordert. Ein effektiver Benutzer wird beim SnapManager-Server authentifiziert und autorisiert.

Die SnapManager Anmeldedaten und die Benutzerauthentifizierung unterscheiden sich erheblich von SnapManager 3.0:

- In SnapManager-Versionen vor 3.0 würden Sie bei der Installation von SnapManager ein willkürliches Serverkennwort festlegen. Wer den SnapManager-Server nutzen möchte, braucht das SnapManager-Server-Passwort. Das SnapManager-Server-Passwort muss den Benutzeranmeldeinformationen mit dem smo-Befehl „set-serm“ hinzugefügt werden.
- In SnapManager (3.0 und höher) wurde das SnapManager-Serverpasswort durch die Authentifizierung des individuellen Betriebssystems (OS) ersetzt. Wenn Sie den Client nicht vom selben Server wie den Host ausführen, führt der SnapManager-Server die Authentifizierung durch, indem Sie die Benutzernamen und Passwörter des Betriebssystems verwenden. Wenn Sie nicht zur Eingabe Ihrer OS-Passwörter aufgefordert werden möchten, können Sie die Daten unter Verwendung des Befehls smo cridential set -Host im SnapManager-Benutzeranmeldungs-Cache speichern.

> Der Befehl smo Anmeldeinformation set -Host speichert Ihre Anmeldeinformationen, wenn die Eigenschaft Host.anmeldungs.persist in der Datei smo.config auf true gesetzt ist.

Beispiel

Benutzer1 und User2 teilen sich ein Profil namens Prof2. User2 kann eine Sicherung von „database1“ in Host1 nicht ohne die Berechtigung zum Zugriff auf Host1 durchführen. User1 kann eine Datenbank nicht ohne Berechtigung zum Zugriff auf host3 klonen.

In der folgenden Tabelle werden die verschiedenen Berechtigungen beschrieben, die den Benutzern zugewiesen sind:

Berechtigungstyp	Benutzer1	Benutzer2

Host-Passwort	Host1, Host2	Host2, Host3
Repository-Kennwort	Repos. 1	Repos. 1
Profilkennwort	Prof1, Prof2	Prof2

Wenn User1 und User2 keine freigegebenen Profile haben, nimmt an, dass User1 Berechtigungen für die Hosts mit Namen Host1 und Host2 hat, und User2 hat Berechtigungen für den Host namens Host2. User2 kann nicht einmal die nicht-profilbefehlen wie dump und System verify auf Host1 ausführen.

Online-Hilfe aufrufen und drucken

Die Online-Hilfe enthält Anweisungen zu den Aufgaben, die Sie über die grafische Benutzeroberfläche von SnapManager ausführen können. Die Online-Hilfe enthält auch Beschreibungen der Felder in den Fenstern und Assistenten.

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Hauptfenster auf **Hilfe** > **Hilfe Inhalt**.
   - Klicken Sie in einem beliebigen Fenster oder Assistenten auf **Hilfe**, um Hilfe für dieses Fenster anzuzeigen.
2. Verwenden Sie das **Inhaltsverzeichnis** im linken Fensterbereich, um durch die Themen zu navigieren.
3. Klicken Sie oben im Hilfefenster auf das Druckersymbol, um einzelne Themen zu drucken.

Empfohlene allgemeine Datenbanklayouts und Speicherkonfigurationen

Durch das Wissen der empfohlenen allgemeinen Datenbank-Layouts und Storage-Konfigurationen können Sie Probleme in Bezug auf Festplattengruppen, Dateitypen und Tablespaces vermeiden.

- Fügen Sie keine Dateien aus mehr als einem SAN-Dateisystem oder Volume-Manager in Ihre Datenbank ein.

  Alle Dateien, die eine Datenbank erstellen, müssen sich auf demselben Dateisystem befinden.

- SnapManager erfordert mehrere 4 KB Blockgröße.
- Fügen Sie die Datenbank-System-ID in die oratab-Datei ein.

  Fügen Sie für jede zu verwaltende Datenbank einen Eintrag in die Oratab-Datei ein. SnapManager verlässt sich darauf, dass die oratab-Datei das Zuhause von Oracle bestimmt.

- Wenn Sie SnapManager-Backups mit dem Oracle Recovery Manager (RMAN) registrieren möchten, müssen Sie RMAN-fähige Profile erstellen.

Wenn Sie die neue Volume-basierte Wiederherstellung oder vollständige Laufwerksgruppenswiederherstellung nutzen möchten, sollten Sie die folgenden Richtlinien in Bezug auf Dateisysteme und Laufwerksgruppen berücksichtigen:

- Mehrere Datenbanken können nicht dieselbe ASM-Laufwerksgruppe (Automatic Storage Management) verwenden.
- Eine Laufwerksgruppe, die Datendateien enthält, kann keine anderen Dateitypen enthalten.
- Die LUN (Logical Unit Number) für die Datendatei-Festplattengruppe muss das einzige Objekt im Storage-Volume sein.

Nachfolgend sind einige Richtlinien für die Volume-Trennung aufgeführt:

- Die Datendateien für nur eine Datenbank müssen sich im Volume befinden.
- Sie müssen separate Volumes für jede der folgenden Dateiklassifizierungen verwenden: Datenbankbinärdateien, Datendateien, Online-Wiederherstellungsprotokolle, archivierte Wiederherstellungsprotokolle und Kontrolldateien.
- Sie müssen kein separates Volume für temporäre Datenbankdateien erstellen, da SnapManager keine temporären Datenbankdateien erstellt.

Definieren des Datenbank-Home mit der oratab-Datei

SnapManager verwendet die oratab-Datei während Operationen, um das Home-Verzeichnis der Oracle-Datenbank zu bestimmen. Ein Eintrag für Ihre Oracle-Datenbank muss in der oratab-Datei sein, damit SnapManager ordnungsgemäß funktionieren kann. Die oratab-Datei wird während der Oracle-Softwareinstallation erstellt.

Die oratab-Datei befindet sich an verschiedenen Orten, basierend auf dem Host-Betriebssystem, wie in der folgenden Tabelle dargestellt:

Host-Betriebssystem	Speicherort der Datei
Linux	/Etc/oratab
Solaris	/Var/opt/oracle/oratab
IBM AIX	/Etc/oratab

Die Beispiel-Oratab-Datei enthält die folgenden Informationen:

```
+ASM1:/u01/app/11.2.0/grid:N   # line added by Agent
oelpro:/u01/app/11.2.0/oracle:N         # line added by Agent
# SnapManager generated entry          (DO NOT REMOVE THIS LINE)
smoclone:/u01/app/11.2.0/oracle:N
```

Nach der Installation von Oracle müssen Sie sicherstellen, dass sich die oratab-Datei in dem in der vorherigen Tabelle angegebenen Speicherort befindet. Wenn sich die oratab-Datei nicht an dem richtigen Ort gemäß Ihrem Betriebssystem befindet, müssen Sie sich an den technischen Support wenden, um Hilfe zu erhalten.

Anforderungen für die Verwendung von RAC-Datenbanken mit SnapManager

Sie müssen die Empfehlungen für die Verwendung von RAC-Datenbanken (Real Application Clusters) mit SnapManager kennen. Die Empfehlungen umfassen Portnummern, Passwörter und den Authentifizierungsmodus.

- Im Datenbankauthentifizierungsmodus muss der Listener auf jedem Knoten, der mit einer Instanz der RAC-Datenbank interagiert, so konfiguriert werden, dass er dieselbe Portnummer verwendet.

  Der Listener, der mit der primären Datenbankinstanz interagiert, muss vor dem Start eines Backups gestartet werden.

- Im Betriebssystem-Authentifizierungsmodus oder in einer ASM-Umgebung (Automatic Storage Management) muss der SnapManager-Server auf jedem Knoten der RAC-Umgebung installiert und ausgeführt werden.
- Das Benutzerpasswort für die Datenbank (z. B. für einen Systemadministrator oder einen Benutzer mit der sysdba-Berechtigung) muss für alle Oracle-Datenbankinstanzen in einer RAC-Umgebung identisch sein.

Anforderungen für die Verwendung von ASM-Datenbanken mit SnapManager

Sie müssen die Anforderungen für die Verwendung von ASM-Datenbanken (Automatic Storage Management) mit SnapManager kennen. Wenn Sie diese Anforderungen kennen, können Sie unter anderem Probleme mit den Spezifikationen ASMLib, Partitionen und Klonen vermeiden.

- SnapManager (3.0.3 oder höher) verwendet die neue sysasm-Berechtigung, die mit Oracle 11gR2 verfügbar ist, anstatt die sysdba-Berechtigung zur Verwaltung einer Oracle ASM-Instanz.

  Wenn Sie die sysdba-Berechtigung zum Ausführen von Administratorbefehlen auf der ASM-Instanz verwenden, wird eine Fehlermeldung angezeigt. Die Datenbank verwendet die sysdba-Berechtigung für den Zugriff auf Laufwerksgruppen. Wenn Sie eine Verbindung mit der ASM-Instanz über die sysasm-Berechtigung herstellen, haben Sie vollständigen Zugriff auf alle verfügbaren Oracle ASM-Festplattengruppen und Verwaltungsfunktionen.

  Wenn Sie Oracle 10gR2 und 11gR1 verwenden, müssen sie weiterhin die sysdba-Berechtigung verwenden.

- SnapManager (3.0.3 oder höher) unterstützt die Sicherung von Datenbanken, die direkt auf ASM-Festplattengruppen gespeichert sind, wenn die Laufwerksgruppe auch ein ACFS-Volume (Automatic Cluster File System) enthält.

  Diese Dateien sind indirekt durch SnapManager geschützt und werden möglicherweise mit dem restlichen Inhalt einer ASM-Festplattengruppe wiederhergestellt, aber SnapManager (3.0.3 oder höher) unterstützt kein ACFS.

  ACFS ist eine plattformübergreifende, skalierbare File-System-Storage-Management-Technologie, die mit Oracle 11gR2 verfügbar ist. ACFS erweitert die ASM-Funktionalität, um Kundendateien zu unterstützen, die außerhalb der Oracle-Datenbank gepflegt werden.

- SnapManager (3.0.3 oder höher) unterstützt die Sicherung von Dateien, die auf ASM-Festplattengruppen gespeichert sind, wenn die Laufwerksgruppe auch OCR-Dateien (Oracle Cluster Registry) oder Abstimmdiskdateien enthält. Wiederherstellungsvorgänge erfordern jedoch eine langsamere, hostbasierte

oder PFSR-Methode (Partial File Snap Restore).

Am besten sollten OCR- und Abstimmfestplatten auf Laufwerksgruppen vorhanden sein, die keine Datenbankdateien enthalten.

- Jedes für ASM verwendete Laufwerk darf nur eine Partition enthalten.
- Die Partition, die die ASM-Daten hostet, muss richtig ausgerichtet sein, um schwere Performanceprobleme zu vermeiden.

  Dies bedeutet, dass die LUN den korrekten Typ haben muss, und die Partition einen Offset mit einem mehrere 4K Byte haben muss.

  Weitere Informationen zum Erstellen von Partitionen, die auf 4K ausgerichtet sind, finden Sie im Knowledge Base-Artikel 1010717.

- ASM-Konfiguration ist nicht als Teil der Klonspezifikation angegeben.

  Sie müssen die ASM-Konfigurationsinformationen in den Klonspezifikationen, die mit SnapManager 2.1 erstellt wurden, manuell entfernen, bevor Sie den Host auf SnapManager (2.2 oder höher) aktualisieren.

- SnapManager 3.1, 3.1p1 und 3.2 oder höher unterstützen ASMLib 2.1.4.
- SnapManager 3.1p4 oder höher unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8.

Unterstützte Partitionsgeräte

Sie müssen die verschiedenen Partitionsgeräte kennen, die in SnapManager unterstützt werden.

Die folgende Tabelle enthält Partitionsinformationen und die Möglichkeit, diese für verschiedene Betriebssysteme zu aktivieren:

Betriebssystem	Einzelne Partition	Mehrere Partitionen	Geräte ohne Partitionierung	Dateisystem oder RAW-Geräte
Red hat Enterprise Linux 5x oder Oracle Enterprise Linux 5-mal	Ja.	Nein	Nein	Ext3*
Red hat Enterprise Linux 6 x oder Oracle Enterprise Linux 6x	Ja.	Nein	Nein	Ext3 oder ext4*
SUSE Linux Enterprise Server 11	Ja.	Nein	Nein	Ext3*
SUSE Linux Enterprise Server 10	Nein	Nein	Ja.	Erw. 3***

Betriebssystem	Einzelne Partition	Mehrere Partitionen	Geräte ohne Partitionierung	Dateisystem oder RAW-Geräte
Red hat Enterprise Linux 5x oder Lateror Oracle Enterprise Linux 5-mal oder höher	Ja.	Nein	Ja.	ASM mit ASMlib**
SUSE Linux Enterprise Server 10 SP4or SUSE Linux Enterprise Server 11	Ja.	Nein	Ja.	ASM mit ASMlib**
SUSE Linux Enterprise Server 10 SP4 oder Lateror SUSE Linux Enterprise Server 11	Ja.	Nein	Nein	ASM ohne ASMlib**

Weitere Informationen zu den unterstützten Betriebssystemversionen finden Sie in der Interoperabilitäts-Matrix.

Unterstützung für ASMLib

SnapManager unterstützt verschiedene Versionen von ASMLib, obwohl es mehrere Faktoren, die Sie bei der Verwendung von SnapManager mit ASMLib berücksichtigen müssen.

SnapManager unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8. Alle SnapManager-Vorgänge können mit ASMLib 2.1.4, 2.1.7 und 2.1.8 ausgeführt werden.

Wenn Sie von ASMLib 2.1.4 auf ASM 2.1.7 aktualisiert haben, können Sie die gleichen Profile und Backups verwenden, die mit ASMLib 2.1.4 erstellt wurden, um die Backups wiederherzustellen und die Klone zu erstellen.

Bei der Verwendung von SnapManager mit ASMLib müssen Sie Folgendes berücksichtigen:

- SnapManager 3.1 unterstützt ASMLib 2.1.7 nicht.

  SnapManager 3.1p4 oder höher unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8.

- Nach einem Rolling Upgrade von SnapManager 3.1 auf 3.2 funktionieren die mit ASMLib 2.1.7 erstellten Backups nur dann, wenn das Repository wieder auf SnapManager 3.1 und ASMLib 2.1.7 zurückgesetzt wird auf ASMLib 2.1.4.
- Nach einem Rolling Upgrade von SnapManager 3.1 auf 3.2 funktionieren Backups, die mit ASMLib 2.1.7 7 erstellt wurden, nicht, wenn das Repository mit ASMLib 2.1 zurück zu SnapManager 3.1 zurückgesetzt wird.

Das Rollback ist erfolgreich, aber die Profile und Backups können nicht verwendet werden.

Unterstützung für ASM-Datenbanken ohne ASMLib

SnapManager unterstützt standardmäßig ASM ohne ASMLib. Die grundlegende Voraussetzung ist, dass die Geräte, die für ASM-Laufwerksgruppen verwendet werden, partitioniert werden müssen.

Wenn ASMLib nicht installiert ist, werden die Geräteberechtigungen für ASM-Laufwerksgruppen in root:Disk geändert, wenn Sie die folgenden Vorgänge ausführen:

- Starten Sie den Host neu
- Wiederherstellen einer Datenbank aus dem primären Storage mithilfe von Volume-basierten SnapRestore (VBSR)
- Wiederherstellung einer Datenbank aus dem sekundären Storage

Sie können die entsprechenden Geräteberechtigungen festlegen, indem Sie der Konfigurationsoption oracleasm.Support.without.asmlib in smo.conf True zuweisen. Die mit den ASM-Laufwerksgruppen verbundenen Geräte werden beim Hinzufügen oder Entfernen neuer Geräte vom Host hinzugefügt oder aus der Datei initasmdisk entfernt. Die Datei initasmdics befindet sich unter /etc/initasmDisks.

Wenn Sie beispielsweise oracleasm.Support.without.asmlib=true festlegen und anschließend eine Sicherungshalterung durchführen, werden neue Geräte zu initasmDisks hinzugefügt. Beim Neustart des Hosts werden die Geräteberechtigungen und die Eigentumsrechte von den Startskripten beibehalten.

Der Standardwert für oracleasm.Support.without.asmlib ist false.

Verwandte Informationen

Unterstützte Partitionsgeräte

Unterstützte Skripte

Die Skripte asmmain.sh und asmquerydisk.sh ermöglichen das Ändern des Grid-Benutzers, der Gruppe und des Benutzers, die alle zur Abfrage der ASM-Laufwerke verwendet werden. Die Skripte müssen immer aus dem Root ausgeführt werden.

Die asmmain.sh ist die Skript-Hauptdatei, die von jedem Vorgang aufgerufen wird, der Geräte hinzufügt oder löscht. Das Skript asmmain.sh ruft intern ein anderes Skript auf, das vom Root ausgeführt werden muss, das über oracle Grid-Anmeldedaten verfügt. Dieses Skript fragt die Geräte der ASM-Laufwerksgruppe ab und fügt diese Einträge in der initasmdisk-Datei mit der Berechtigung und dem Eigentum der Geräte hinzu. Sie können die Berechtigungen und Eigentumsrechte dieser Datei basierend auf Ihrer Umgebung und dem regex-Muster ändern, das nur zur Übereinstimmung mit /dev/mapper/*p1 verwendet wird.

Das Skript asmquerydisk.sh wird verwendet, um die Festplattenliste abzufragen, die zur Erstellung der ASM-Laufwerksgruppe verwendet wird. Je nach Konfiguration müssen Sie Oracle_BASE, ORACLE_HOME und ORACLE_SID Werte zuweisen.

Die Skripte finden sich unter /opt/NetApp/smo/Plugins/examples/noasmlib. Diese Skripte müssen allerdings in die /opt/NetApp/smo/Plugins/noasmlib verschoben werden, bevor der SnapManager für Oracle Server auf dem Host gestartet wird.

Einschränkungen bei der Verwendung von Skripten zur Unterstützung einer ASM-Datenbank ohne ASMLib

Sie müssen sich über bestimmte Einschränkungen bei der Verwendung von Skripten zur Unterstützung einer ASM-Datenbank ohne ASMLib bewusst sein.

- Die Skripte stellen eine alternative Lösung für jede Kernel-Version dar, jedoch nur, wenn ASMLib nicht installiert ist.
- Die Berechtigungen für die Skripte müssen so festgelegt werden, dass Root-, Grid-, oracle- oder vergleichbare Benutzer auf die Skripte zugreifen können.
- Die Skripte unterstützen keine Wiederherstellung von einem sekundären Speicherort.

Implementieren und Ausführen der Skripte

Sie können die Skripte asmmain.sh und asmquerydisk.sh bereitstellen und ausführen, um ASM-Datenbanken ohne ASMLib zu unterstützen.

Diese Skripte folgen nicht der Pre-scripts oder Post-scripts Syntax und Workflow wird aufgerufen, wenn intitasmdisks aktiviert ist. Sie können in den Skripten alles ändern, was mit Ihren Konfigurationseinstellungen zusammenhängt. Es wird empfohlen zu überprüfen, ob alle Skripte mit einem kurzen Trockenlauf wie erwartet funktionieren.

> Diese Skripte schaden Ihrem System weder bei Ausfällen noch werden sie Ihr System beeinträchtigen. Diese Skripte werden ausgeführt, um die ASM-bezogenen Laufwerke zu aktualisieren, um die richtigen Berechtigungen und Eigentumsrechte zu haben, so dass die Festplatten immer unter ASM-Instanz Kontrolle.

1. Erstellen Sie die ASM-Festplattengruppen mit den partitionierten Laufwerken.
2. Erstellen Sie die Oracle-Datenbank auf den FESTPLATTENGRUPPEN.
3. Beenden Sie den SnapManager für Oracle Server.

   > In einer RAC-Umgebung müssen Sie diesen Schritt auf allen RAC-Knoten durchführen.

4. Ändern Sie die smo.conf, um die folgenden Parameter einzuschließen:

   a. Oracleasm.Support.without.asmlib = true
   b. Oracleasm.Support.without.asmlib.Ownership = true
   c. oracleasm.support.without.asmlib.username = Benutzername Ihrer ASM-Instanzumgebung
   d. oracleasm.support.without.asmlib.groupname = Gruppenname Ihrer ASM-Instanzumgebung

   Durch diese Änderungen werden nur die Berechtigungen für den absoluten Pfad festgelegt, was bedeutet, dass anstelle des Partitionsgeräts die Berechtigungen nur für das dm-*-Gerät festgelegt werden.

5. Fügen Sie die Konfigurationseinstellungen in die Skripte der Plug-ins unter /opt/NetApp/smo/examples/noasmlib ein.
6. Kopieren Sie die Skripte in /opt/NetApp/smo/Plugins/noasmlib, bevor Sie den SnapManager für Oracle Server auf dem Host starten.
7. Navigieren Sie zum Verzeichnis /opt/NetApp/smo und führen Sie einen trockenen Lauf durch: sh Plug-ins/noasmlib/asmmain.sh

Die etc/initasmdisks-Datei wird erstellt, was die Hauptdatei ist, die verwendet wird.

Sie können bestätigen, dass die etc/initasmdisks-Datei alle Geräte enthält, die mit der konfigurierten ASM-Datenbank zusammenhängen, wie z. B.:

```
chown -R grid:oinstall /dev/mapper/360a98000316b61396c3f394645776863p1
         chmod 777 /dev/mapper/360a98000316b61396c3f394645776863p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714239p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714239p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714241p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714241p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714243p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714243p1
```

8. Starten Sie den SnapManager für Oracle-Server.
9. Konfigurieren Sie SnapDrive für UNIX, indem Sie die folgende Datei zur snapdrive.conf Datei hinzufügen.Disconnect-luns-before-vbsr=on
10. Starten Sie SnapDrive für UNIX Server neu.

> In einer RAC-Umgebung müssen Sie die Schritte 3 bis 10 für alle RAC-Knoten durchführen.

Die erstellte /etc/initasmdics-Datei muss entweder aus einem der Startskripte oder aus einem Skript ausgeführt werden, das in rc3.d. neu definiert ist Die Datei /etc/initasmdisks sollte immer ausgeführt werden, bevor der oracleha-Dienst gestartet wird.

Beispiel

```
# ls -ltr *ohasd*
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 S96ohasd ->
/etc/init.d/ohasd
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 K15ohasd ->
/etc/init.d/ohasd
```

Im folgenden Beispiel ist sh -x/etc/initasmdisks standardmäßig nicht verfügbar, und Sie müssen es als die erste Zeile der Funktion anhängen `start_stack()` In einem ohasd-Skript:

```
start_stack()
{
sh -x /etc/initasmdisks
# see init.ohasd.sbs for a full rationale case $PLATFORM in Linux
}
```

Unterstützung für Oracle RAC ASM-Datenbanken ohne ASMLib

Wenn Sie Oracle RAC-Datenbanken verwenden, müssen die RAC-Knoten mit der Initasmdics-Datei aktualisiert werden, sobald ein Vorgang im Master RAC-Knoten ausgeführt wird.

Wenn sich vom Master-Knoten aus keine Authentifizierung bei den RAC-Knoten anmelden muss, führt der asmmain.sh eine sichere Kopie (SCP) von InitasmDisks an alle RAC-Knoten aus. Die InitasmDisks-Datei des Master-Knotens wird jedes Mal aufgerufen, wenn eine Wiederherstellung stattfindet. Das Skript asmmain.sh kann aktualisiert werden, um auf alle RAC-Knoten dasselbe Skript aufzurufen.

Die erstellte /etc/initasmdics-Datei, die entweder aus einem der Startskripte oder aus einem neu definierten Skript in rc3.d. ausgeführt werden muss Die Datei /etc/initasmdisks sollte immer ausgeführt werden, bevor der oracleha-Dienst gestartet wird.

Unterstützung für Oracle 10g ASM-Datenbanken ohne ASMLib

Wenn Sie Oracle 10g verwenden, steht der Befehl asmcmd nicht für die Auflistung von Disketten zur Verfügung. Sie können die sql-Abfrage verwenden, um die Festplattenliste abzurufen.

Das Script Disk_list.sql ist in die vorhandenen Skripte enthalten, die im Beispielverzeichnis zur Unterstützung von sql-Abfragen zur Verfügung gestellt werden. Wenn Sie theasmquerydisk.sh Skript ausführen, muss das Script Disk_list.sql manuell ausgeführt werden. Die Beispielzeilen werden mit Kommentaren in der Datei asmquerydisk.sh hinzugefügt. Diese Datei kann entweder am Speicherort /Home/Grid oder an einem anderen Ort Ihrer Wahl platziert werden.

Beispielskripts zur Unterstützung von ASM-Datenbanken ohne ASMLib

Die Beispielskripte sind im Verzeichnis Plugins/examples/noasmlib des Installationsverzeichnisses für SnapManager für Oracle verfügbar.

asmmain.sh

```
#!/bin/bash
griduser=grid
gridgroup=oinstall

# Run the script which takes the disklist from the asmcmd
# use appropriate user , here grid user is being used to run
# asmcmd command.
su -c "plugins/noasmlib/asmdiskquery.sh" -s /bin/sh grid
cat /home/grid/disklist

# Construct the final file as .bak file with propre inputs
awk -v guser=$griduser -v ggroup=$gridgroup '/^\/dev\/mapper/ { print
"chown -R "guser":"ggroup" "$1; print "chmod 777 " $1; }'
/home/grid/disklist > /etc/initasmdisks.bak

# move the bak file to the actual file.
```

```
mv /etc/initasmdisks.bak /etc/initasmdisks

# Set full full permission for this file to be called while rebooting and
restore
chmod 777 /etc/initasmdisks

# If the /etc/initasmdisks needs to be updated in all the RAC nodes
# or /etc/initasmdisks script has to be executed in the RAC nodes, then
the following
# section needs to be uncommented and used.
#
# Note: To do scp or running scripts in remote RAC node via ssh, it needs
password less login
# for root user with ssh keys shared between the two nodes.
#
# The following 2 lines are used for updating the file in the RAC nodes:
# scp /etc/initasmdisks root@racnode1:/etc/initasmdisks
# scp /etc/initasmdisks root@racnode2:/etc/initasmdisks
#
# In order to execute the /etc/initasmdisks in other RAC nodes
# The following must be added to the master RAC node /etc/initasmdisks
file
# from the asmmain.sh script itself. The above scp transfer will make sure
# the permissions and mode for the disk list contents are transferred to
the other RAC nodes
# so now appending any command in the /etc/initasmsdisks will be retained
only in the master RAC node.
# The following lines will add entries to the /etc/initasmsdisks file in
master RAC node only. When this script is executed
#  master RAC node, /etc/initasmdisks in all the RAC nodes will be
executed.
# echo 'ssh racnode1 /etc/initasmdisks' >> /etc/initasmdisks
# echo 'ssh racnode2 /etc/initasmdisks' >> /etc/initasmdisks
```

asmquerydisk.sh

```
#!/bin/bash
export  ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/grid/product/11.2.0.3/grid
export ORACLE_SID=+ASM
export  PATH=$ORACLE_HOME/bin:$PATH

# Get the Disk List and save this in a file called dglist.
asmcmd lsdsk  > /home/grid/disklist

# In oracle 10g the above used command 'asmcmd' is not available so use
SQL
# query can be used to take the disk list. Need to uncomment the following
# line and comment the above incase oracle 10g is being in use.
# The disk_list.sql script is availbe in this noasmlib examples folder
itself
# which can be modified as per customer needs.
# sqlplus "/as sysdba" @/home/grid/disk_list.sql > /home/grid/disklist
```

Disk_list.sql

```
# su - oracle
-bash-4.1$ cat disk_list.sql
select path from v$asm_disk;
exit
-bash-4.1$
```

Anforderungen für die Verwendung von Datenbanken mit NFS und SnapManager

Sie müssen die Anforderungen für die Verwendung von Datenbanken mit Network File System (NFS) und SnapManager kennen. Die Empfehlungen umfassen die Ausführung als root, Attribut-Caching und symbolische Links.

- Sie müssen SnapManager als Root ausführen. SnapManager muss auf die Dateisysteme zugreifen können, die Datendateien, Kontrolldateien, Online-Wiederherstellungsprotokolle, Archivprotokolle und den Datenbank-Home enthalten.

  Legen Sie eine der folgenden NFS-Exportoptionen fest, um sicherzustellen, dass Root auf die Dateisysteme zugreifen kann:

  - Root=Hostname
  - rw=Host-Name, anon=0
- Sie müssen das Attribut-Caching für alle Volumes deaktivieren, die Datenbankdatendateien, Kontrolldateien, Redo- und Archivprotokolle und die Datenbank-Startseite enthalten.

  Exportieren Sie die Volumes mithilfe der optionen noac (für Solaris und AIX) oder actimeo=0 (für Linux).

- Sie müssen die Datenbankdatendateien aus dem lokalen Speicher mit NFS verknüpfen, um nur symbolische Links auf Mount-Punkt-Ebene zu unterstützen.

Beispiel für Datenbank-Volume-Layouts

Weitere Informationen zur Konfiguration Ihrer Datenbank finden Sie unter Beispiel-Datenbank-Volume-Layouts.

Single-Instance-Datenbanken

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_sid	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_sid (Multiplexed) Oralogen02_sid (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Ja.	Aus

RAC-Datenbanken (Real Application Clusters)

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_dbname	Ja.	Aus
Temporäre Datendateien	Oratepp_dbname	Ja.	Aus
Kontrolldateien	Oracntrl01_dbname (Multiplexed) Oracntrl02_dbname (Multiplexed)	Ja.	Aus

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_dbname	Ja.	Aus
Cluster-Dateien	Oracrs_clustername	Ja.	Ein

Einzelne Instanz einer ASM-Datenbank (Automatic Storage Management

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Orabin_Host namelun	Ja.	Ein
Datendateien	Oradata_sid	Oradata_sidlun	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Oratepp_sidlun	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Oracntrl01_sidlun (Multiplexed) Oracntrl02_sidlun (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Oralog01_dbnamelun (Multiplexed) Oralogen02_dbnamelun (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Oraarch_sidlun	Ja.	Aus

ASM RAC-Datenbanken

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Orabin_Host namelun	Ja.	Ein

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Datendateien	Oradata_sid	Oradata_sidlun	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Oratepp_sidlun	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Oracntrl01_sidlun (Multiplexed) Oracntrl02_sidlun (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Oralog01_dbnamelun (Multiplexed) Oralogen02_dbnamelun (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Oraarch_sidlun	Ja.	Aus
Cluster-Dateien	Oracrs_clustername	Oracrs_clusternamelun	Ja.	Ein

Einschränkungen bei der Arbeit mit SnapManager

Sie müssen die Szenarien und Einschränkungen kennen, die sich auf Ihre Umgebung auswirken können.

Einschränkungen im Zusammenhang mit Datenbank-Layouts und Plattformen

- SnapManager unterstützt Steuerdateien auf einem Dateisystem in einer ASM-Laufwerksgruppe und unterstützt keine Steuerdateien auf RAW-Geräten.
- SnapManager arbeitet in einer Microsoft Clustering-Umgebung (MSCS), erkennt jedoch den Status der MSCS-Konfiguration (aktiv oder passiv) nicht und überträgt kein aktives Management eines Repositorys in einen Standby-Server in einem MSCS-Cluster.
- In Red hat Enterprise Linux (RHEL) und Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 und 5.3 wird das ext3-Dateisystem bei der Bereitstellung von Oracle über RAW-Geräte durch Verwendung von dynamischem Multipathing (DMP) in einer Multipath Network I/O (MPIO)-Umgebung nicht unterstützt.

  Dieses Problem ist in SnapManager nur bemerkt, wenn SnapDrive 4.1 für UNIX oder frühere Versionen verwendet wird.

- SnapManager unter RHEL unterstützt die Partitionierung von Festplatten mit dem Dienstprogramm **parted** nicht.

  Dies ist ein Problem mit dem Dienstprogramm RHEL **parted**.

- Wenn in einer RAC-Konfiguration ein Profilname aus RAC-Knoten A aktualisiert wird, wird die Zeitplandatei

für das Profil nur für RAC-Knoten A aktualisiert

Die Zeitplandatei für dasselbe Profil auf RAC-Knoten B wird nicht aktualisiert und enthält die früheren Terminplaninformationen. Wenn ein geplantes Backup von Knoten B ausgelöst wird, schlägt der geplante Backup-Vorgang fehl, da Node B die frühere Zeitplandatei enthält. Der geplante Sicherungsvorgang ist jedoch von Knoten A erfolgreich, auf dem das Profil umbenannt wird. Sie können den SnapManager-Server neu starten, sodass Sie die neueste Zeitplandatei für das Profil auf Knoten B. erhalten

- Die Repository-Datenbank kann auf einem Host vorhanden sein, auf den über mehrere IP-Adressen zugegriffen werden kann.

  Wenn über mehrere IP-Adressen auf das Repository zugegriffen wird, wird die Zeitplandatei für jede der IP-Adressen erstellt. Wenn die Backup-Planung für ein Profil (z. B. Profil A) unter einer der IP-Adressen (z. B. IP1) erstellt wird, wird die Zeitplandatei nur für diese IP-Adresse aktualisiert. Wenn von einer anderen IP-Adresse auf Profil A zugegriffen wird (z. B. IP2), wird das geplante Backup nicht aufgeführt, da die Terminplandatei von IP2 keinen Eintrag für den unter IP1 erstellten Zeitplan hat.

  Sie können warten, bis der Zeitplan von dieser IP-Adresse und der Zeitplandatei ausgelöst wird, oder Sie können den Server neu starten.

Einschränkungen in Bezug auf die SnapManager-Konfiguration

- SnapManager kann für die Katalogisierung von Datenbank-Backups mit RMAN konfiguriert werden.

  Wenn ein RMAN-Wiederherstellungskatalog verwendet wird, muss sich der Wiederherstellungskatalog in einer anderen Datenbank befinden als die gesicherte Datenbank.

- SnapDrive für UNIX unterstützt auf bestimmten Plattformen mehr als einen Filesystem- und Volume-Manager.

  Der für Datenbankdateien verwendete Dateisystem- und Volume-Manager muss in der SnapDrive-Konfigurationsdatei als Standarddateisystem und Volume Manager angegeben werden.

- SnapManager unterstützt Datenbanken auf MultiStore Storage-Systemen unter folgenden Anforderungen:
  - Sie müssen SnapDrive konfigurieren, um Passwörter für MultiStore Storage-Systeme festzulegen.
  - SnapDrive kann keine Snapshot Kopie einer LUN oder Datei in einem qtree in einem MultiStore Storage-System erstellen, wenn sich das zugrunde liegende Volume nicht im selben MultiStore Storage-System befindet.
- SnapManager unterstützt nicht den Zugriff auf zwei SnapManager Server, die auf verschiedenen Ports über einen einzelnen Client laufen (sowohl über CLI als auch über GUI).

  Die Port-Nummern sollten auf dem Ziel- und den Remote-Hosts identisch sein.

- Alle LUNs in einem Volume sollten auf Volume-Ebene oder in qtrees liegen, jedoch nicht beides.

  Das liegt daran, dass die Daten in den qtrees liegen und Sie das Volume mounten, dann sind die Daten in den qtrees nicht geschützt.

- SnapManager-Vorgänge schlagen fehl und Sie können nicht auf die GUI zugreifen, wenn die Repository-Datenbank ausfällt.

  Sie müssen überprüfen, ob die Repository-Datenbank ausgeführt wird, wenn Sie SnapManager-Vorgänge durchführen.

- SnapManager unterstützt keine Live Partition Mobility (LPM) und Live Application Mobility (LAM).
- SnapManager unterstützt Oracle Wallet Manager und Transparent Data Encryption (TDE) nicht.
- MetroCluster-Konfigurationen werden von SnapManager in RDM-Umgebungen (Raw Device Mapping) nicht unterstützt, da MetroCluster-Konfigurationen noch von der Virtual Storage Console (VSC) unterstützt werden müssen.

Einschränkungen im Zusammenhang mit der Profilverwaltung

- Wenn Sie das Profil aktualisieren, um die Backups des Archivprotokolls voneinander zu trennen, können Sie auf dem Host keinen Rollback-Vorgang durchführen.
- Wenn Sie ein Profil von der GUI aktivieren, um Archiv-Protokoll-Backups zu erstellen, und später versuchen, das Profil mithilfe des Fensters „Multi Profile Update“ oder des Fensters „Profile Update“ zu aktualisieren, können Sie dieses Profil nicht ändern, um ein vollständiges Backup zu erstellen.
- Wenn Sie im Fenster Multi Profile Update mehrere Profile aktualisieren und bei einigen Profilen die Option **Backup Archivilogs separat** aktiviert ist und andere Profile die Option deaktiviert haben, ist die Option **Archivprotokolle separat** sichern deaktiviert.
- Wenn Sie mehrere Profile aktualisieren und einige Profile die Option **Backup Archivilogs separat** aktivieren und andere Profile die Option deaktiviert haben, ist die Option **Backup Archivilogs separat** im Fenster Multi Profile Update deaktiviert.
- Wenn Sie das Profil umbenennen, können Sie den Host nicht zurückführen.

Einschränkungen im Zusammenhang mit Rolling Upgrade oder Rollback-Vorgängen

- Wenn Sie versuchen, eine frühere Version von SnapManager für einen Host zu installieren, ohne den Rollback-Vorgang auf dem Host im Repository durchzuführen, können Sie Folgendes möglicherweise nicht ausführen:
  - Sehen Sie sich die Profile an, die in früheren oder neueren Versionen von SnapManager für den Host erstellt wurden.
  - Greifen Sie auf Backups oder Klone zu, die in früheren oder neueren Versionen von SnapManager erstellt wurden.
  - Führen Sie Rolling Upgrade- oder Rollback-Vorgänge auf dem Host durch.
- Nachdem Sie die Profile getrennt haben, um Backups für Archivprotokolle zu erstellen, können Sie im zugehörigen Host Repository keinen Rollback-Vorgang durchführen.

Einschränkungen im Zusammenhang mit Backup-Vorgängen

- Die Backup-Erstellung kann fehlschlagen, wenn Sie SnapManager Vorgänge gleichzeitig auf demselben Host auf einer anderen ASM-Datenbank ausführen.
- Wenn der Backup während der Recovery bereits angehängt ist, mounted SnapManager den Backup nicht erneut und verwendet das bereits bereitgestellte Backup.

  Wenn das Backup von einem anderen Benutzer gemountet wird und Sie keinen Zugriff auf das zuvor bereitgestellte Backup haben, muss der andere Benutzer Ihnen die Berechtigung erteilen.

  Alle Archivprotokolldateien haben Leseberechtigung für Benutzer, die einer Gruppe zugewiesen sind. Sie haben möglicherweise nicht die Zugriffsberechtigung für die Archivprotokolldatei, wenn das Backup von einer anderen Benutzergruppe gemountet wird. Benutzer können die gemounteten Archivprotokolldateien manuell erteilen und den Wiederherstellungsvorgang oder die Wiederherstellung wiederholen.

- SnapManager legt den Backup-Status als „`PROTECTED`“ fest, selbst wenn eine der Snapshot-Kopien des

Datenbank-Backups auf das sekundäre Storage-System übertragen wird.

- Sie können die Aufgabenspezifikationsdatei nur für geplante Backups aus SnapManager 3.2 oder höher verwenden.
- Wenn ein Backup- oder Klonvorgang gleichzeitig auf den 10gR2- und 11gR2 RAC-Datenbanken über ASM ausgeführt wird, schlägt eine der Backup- oder Klonerstellung fehl.

  Dieser Fehler liegt an einer bekannten Oracle Einschränkung.

- SnapManager ist in den Protection Manager integriert und unterstützt das Backup mehrerer Volumes im Primärspeicher zu einem einzigen Volume im Sekundärspeicher von SnapVault und qtree SnapMirror.

  Die dynamische Dimensionierung eines sekundären Volumes wird nicht unterstützt. Weitere Informationen hierzu finden Sie im Provisioning Manager und Protection Manager – Administratorhandbuch für die Verwendung mit DataFabric Manager Server 3.8.

- SnapManager unterstützt mit dem Post-Processing-Skript nicht das Vaulting von Backups.
- Wenn die Repository-Datenbank auf mehr als eine IP-Adresse verweist und jede IP-Adresse einen anderen Hostnamen hat, ist der Backup-Planungsvorgang für eine IP-Adresse erfolgreich, schlägt aber für die andere IP-Adresse fehl.
- Nach einem Upgrade auf SnapManager 3.4 oder höher können alle mit Nachverarbeitungsskripten unter SnapManager 3.3.1 geplanten Backups nicht aktualisiert werden.

  Sie müssen den vorhandenen Zeitplan löschen und einen neuen Zeitplan erstellen.

Einschränkungen im Zusammenhang mit Wiederherstellungsvorgängen

- Wenn Sie eine indirekte Methode zur Durchführung eines Wiederherstellungsvorgangs verwenden und die für die Wiederherstellung erforderlichen Archivprotokolldateien nur bei Backups vom sekundären Speichersystem verfügbar sind, kann SnapManager die Datenbank nicht wiederherstellen.

  Der Grund dafür ist, dass SnapManager das Backup von Archivprotokolldateien nicht vom sekundären Storage-System mounten kann.

- Wenn SnapManager eine Volume-Wiederherstellung durchführt, werden die Backupkopien des Archivprotokolls, die nach der Wiederherstellung des entsprechenden Backups erstellt werden, nicht gelöscht.

  Wenn sich die Datendateien und das Ziel der Archivprotokolldatei auf demselben Volume befinden, können die Datendateien durch eine Wiederherstellung des Volumes wiederhergestellt werden, wenn im Ziel der Archivprotokolldatei keine Archivprotokolldateien vorhanden sind. In einem solchen Szenario gehen die Snapshot Kopien des Archivprotokolls verloren, die nach dem Backup der Dateien erstellt wurden.

  Sie sollten nicht alle Archivprotokolldateien vom Archivprotokollziel löschen.

- Wenn in einer ASM-Umgebung auf einer Laufwerksgruppe, die Datendateien hat, Oracle Cluster Registry (OCR) und Voting Disk-Dateien koexistieren, zeigt der Schnellwiederherstellungsvorgang die falsche Verzeichnisstruktur für den OCR- und Voting-Datenträger an.

Einschränkungen im Zusammenhang mit Klonvorgängen

- Aufgrund der Geschwindigkeit, mit der die Inodes vom Speichersystem erkannt und verarbeitet werden, das das flexible Volume enthält, können Sie keine numerischen Werte zwischen 0 und 100 für den Fortschritt des Clone-Split-Vorgangs anzeigen.

- SnapManager unterstützt nicht das Empfangen von E-Mails nur für erfolgreiche Klontrennvorgänge.
- SnapManager unterstützt nur die Aufteilung eines FlexClone.
- Das Klonen des Online-Datenbank-Backups der RAC-Datenbank, die den Speicherort der externen Archivprotokolldatei verwendet, ist aufgrund eines Fehlers bei der Wiederherstellung fehlgeschlagen.

  Das Klonen schlägt fehl, da Oracle die Archivprotokolldateien nicht für die Wiederherstellung vom externen Archivprotokollspeicherort findet und angewendet. Dies ist eine Einschränkung von Oracle. Weitere Informationen finden Sie unter Oracle Bug ID: 13528007. Oracle wendet Archivprotokoll nicht vom nicht standardmäßigen Speicherort auf dem an "Oracle Support Website". Sie müssen über einen gültigen Oracle metalink-Benutzernamen und ein gültiges Kennwort verfügen.

- SnapManager 3.3 oder höher unterstützt nicht mit der XML-Datei für die Klonspezifikation, die in den Versionen vor SnapManager 3.2 erstellt wurde.
- Wenn sich temporäre Tablespaces an einem anderen Speicherort als dem Datendateien befinden, erstellt ein Klonvorgang die Tabellen im Datendateien.

  Wenn jedoch temporäre Tablespaces Oracle Managed Files (OMFs) sind, die sich an einem anderen Speicherort als dem Datendateien befinden, erstellt der Klonvorgang nicht die Tabellen im Datendateien. Die OMFs werden nicht von SnapManager verwaltet.

- SnapManager kann eine RAC Datenbank nicht klonen, wenn Sie die Option -resetlogs auswählen.

Einschränkungen im Zusammenhang mit Archiv-Log-Dateien und Backups

- SnapManager unterstützt keine Anschnitt von Archiv-Log-Dateien aus dem Flash-Recovery-Bereich Ziel.
- SnapManager unterstützt nicht das Aufheben von Archivprotokolldateien vom Standby-Ziel.
- Die Backups für das Archivprotokoll werden basierend auf der Aufbewahrungsdauer und der standardmäßigen stündlichen Aufbewahrungsklasse beibehalten.

  Wenn die Klasse für die Backup-Aufbewahrung des Archivprotokolls über die SnapManager Befehlszeilenschnittstelle oder Benutzeroberfläche geändert wird, gilt die geänderte Aufbewahrungsklasse nicht für das Backup, da die Backups des Archivprotokolls basierend auf der Aufbewahrungsdauer aufbewahrt werden.

- Wenn Sie die Archivprotokolldateien aus den Zielen des Archivprotokolls löschen, enthält die Backup des Archivprotokolls keine Archivprotokolldateien, die älter sind als die fehlende Archivprotokolldatei.

  Wenn die letzte Archivprotokolldatei fehlt, schlägt die Sicherung des Archivprotokolls fehl.

- Wenn Sie die Archivprotokolldateien aus den Archivprotokollzielen löschen, schlägt das Beschneiden von Archivprotokolldateien fehl.
- SnapManager konsolidiert die Archiv-Log-Backups, selbst wenn Sie die Archiv-Log-Dateien aus den Archiv-Log-Zielen löschen oder wenn die Archiv-Log-Dateien beschädigt sind.

Einschränkungen im Zusammenhang mit der Änderung des Host-Namens der Zieldatenbank

Die folgenden SnapManager Vorgänge werden nicht unterstützt, wenn Sie den Host-Namen der Zieldatenbank ändern:

- Ändern des Host-Namens der Zieldatenbank von der SnapManager-GUI.
- Rollback der Repository-Datenbank nach Aktualisierung des Host-Namens der Zieldatenbank des Profils durchführen.

- Gleichzeitige Aktualisierung mehrerer Profile für einen neuen Hostnamen der Zieldatenbank.
- Ändern des Host-Namens der Zieldatenbank, wenn ein SnapManager-Vorgang ausgeführt wird.

Einschränkungen im Zusammenhang mit der SnapManager CLI oder GUI

- Die CLI-Befehle von SnapManager für den Vorgang zum Erstellen von Profilen, die über die Benutzeroberfläche von SnapManager generiert werden, verfügen über keine Optionen zur Verlaufskonfiguration.

  Mit dem Befehl „Profile create“ können Sie die Verlaufs-Aufbewahrungseinstellungen über die SnapManager-CLI konfigurieren.

- SnapManager zeigt die GUI in Mozilla Firefox nicht an, wenn auf dem UNIX-Client keine Java Runtime Environment (JRE) verfügbar ist.
- Wenn beim Aktualisieren des Host-Namens der Zieldatenbank mithilfe der SnapManager CLI eine oder mehrere offene SnapManager GUI-Sitzungen vorliegen, reagieren nicht alle offenen SnapManager GUI-Sitzungen.

Einschränkungen im Zusammenhang mit SnapMirror und SnapVault

- Das SnapVault Post-Processing-Skript wird nicht unterstützt, wenn Sie Data ONTAP 7-Mode verwenden.
- Wenn Sie ONTAP verwenden, können Sie Volume-basierte SnapRestore (VBSR) nicht auf den Backups ausführen, die in den Volumes erstellt wurden, über die SnapMirror Beziehungen festgelegt sind.

  Dies liegt an einer ONTAP Einschränkung, die es Ihnen nicht erlaubt, die Beziehung bei der Durchführung einer VBSR zu unterbrechen. Sie können jedoch eine VBSR beim letzten oder kürzlich erstellten Backup nur ausführen, wenn die Volumes SnapVault Beziehungen eingerichtet haben.

- Wenn Sie Data ONTAP in 7-Mode verwenden und eine VBSR für die Backups ausführen möchten, die in den Volumes erstellt wurden, auf denen SnapMirror Beziehungen festgelegt sind, können Sie die Option override-vbsr-snapmirror-Check in SnapDrive für UNIX auf ON setzen.

  Weitere Informationen dazu finden Sie in der SnapDrive-Dokumentation.

- In einigen Szenarien können Sie das letzte Backup, das mit der ersten Snapshot Kopie verbunden ist, nicht löschen, wenn das Volume eine SnapVault-Beziehung eingerichtet hat.

  Sie können das Backup nur löschen, wenn Sie die Beziehung unterbrechen. Dieses Problem liegt an einer ONTAP-Einschränkung bei Basis-Snapshot-Kopien. In einer SnapMirror Beziehung wird die Snapshot Basiskopie von der SnapMirror Engine erstellt und in einer SnapVault Beziehung ist die Snapshot Basiskopie das Backup, das mit SnapManager erstellt wurde. Die Basis-Snapshot-Kopie verweist bei jedem Update auf das neueste Backup, das mithilfe von SnapManager erstellt wird.

Einschränkungen im Zusammenhang mit Data Guard Standby-Datenbanken

- SnapManager unterstützt keine Standby-Datenbanken für die logische Datenwache.
- SnapManager unterstützt keine Standby-Datenbanken für Active Data Guard.
- SnapManager erlaubt keine Online-Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine partiellen Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt nicht die Wiederherstellung von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine Beschneidung von Archivprotokolldateien für Data Guard Standby-

Datenbanken.

- SnapManager unterstützt den Broker nicht.

Verwandte Informationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

SnapManager Limitierungen für Clustered Data ONTAP

Sie müssen die Einschränkungen für einige Funktionalitäten und SnapManager-Vorgänge kennen, wenn Sie Clustered Data ONTAP verwenden.

Die folgenden Funktionalitäten werden nicht unterstützt, wenn Sie SnapManager auf Clustered Data ONTAP nutzen:

- Datensicherungsfunktionen, wenn SnapManager in OnCommand Unified Manager integriert ist
- Eine Datenbank, in der eine LUN zu einem System gehört, auf dem Data ONTAP 7-Mode und die andere LUN ausgeführt werden, gehört zu einem System mit Clustered Data ONTAP
- SnapManager für Oracle unterstützt keine Migration von Vserver, wie sie von Clustered Data ONTAP nicht unterstützt wird
- SnapManager für Oracle unterstützt die Funktion Clustered Data ONTAP 8.2.1 nicht zur Festlegung verschiedener Exportrichtlinien für Volumes und qtrees

Einschränkungen in Bezug auf Oracle Database

Bevor Sie mit der Arbeit mit SnapManager beginnen, müssen Sie die Einschränkungen in Bezug auf Oracle Database kennen.

Die Einschränkungen sind wie folgt:

- SnapManager unterstützt Oracle Versionen 10gR2, 11gR1, 11gR2 und 12*c*, unterstützt aber Oracle 10gR1 als Repository oder Zieldatenbank nicht.
- SnapManager unterstützt die Verwendung einer SCAN-IP-Adresse anstelle eines Hostnamens nicht.

  SCAN-IP ist eine neue Funktion in Oracle 11gR2.

- Oracle Cluster File System (OCFS) wird von SnapManager nicht unterstützt.
- Oracle 11g in einer Direct NFS-Umgebung (dNFS) ermöglicht zusätzliche Mount-Point-Konfigurationen in der oranfstab-Datei, z. B. mehrere Pfade für den Lastausgleich.

  SnapManager ändert die oranfstab-Datei nicht. Sie müssen in der oranfstab-Datei manuell weitere Eigenschaften hinzufügen, die die geklonte Datenbank verwenden soll.

- Unterstützung für Oracle Database 9i ist veraltet aus SnapManager 3.2.
- Der Support für Oracle Database 10gR2 (früher als 10.2.0.5) ist veraltet aus SnapManager 3.3.1.

Ermitteln Sie die verschiedenen Versionen von Oracle Datenbanken, die durch die Interoperabilitäts-Matrix unterstützt werden.

Verwandte Informationen

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Veraltete Versionen der Oracle-Datenbank

Oracle Database 9i wird von SnapManager 3.2 oder höher nicht unterstützt, und die Oracle Database 10gR2 (früher als 10.2.0.4) wird von SnapManager 3.3.1 oder höher nicht unterstützt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und auf SnapManager 3.2 oder höher aktualisieren möchten, können Sie keine neuen Profile erstellen. Eine Warnmeldung wird angezeigt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und ein Upgrade auf SnapManager 3.2 oder höher durchführen möchten, müssen Sie eine der folgenden Aktionen durchführen:

- Aktualisieren Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken auf entweder Oracle 10gR2 (10.2.0.5), 11gR1 oder 11gR2 Datenbanken und führen Sie ein Upgrade auf SnapManager 3.2 oder 3.3 durch.

  Wenn Sie ein Upgrade auf Oracle 12*c* durchführen, müssen Sie ein Upgrade auf SnapManager 3.3.1 oder höher durchführen.

  Oracle Datenbank 12*c* wird nur von SnapManager 3.3 unterstützt.

- Verwalten Sie die Oracle 9i-Datenbanken mit einer Patch-Version von SnapManager 3.1.

  Sie können SnapManager 3.2 oder 3.3 verwenden, wenn Sie Oracle 10gR2-, 11gR1- oder 11gR2-Datenbanken verwalten und SnapManager 3.3.1 oder höher verwenden möchten, wenn Sie Oracle 12*c* -Datenbanken zusammen mit anderen unterstützten Datenbanken verwalten möchten.

Einschränkungen beim Volume-Management

Bei SnapManager gibt es bestimmte Volume-Management-Einschränkungen, die sich auf Ihre Umgebung auswirken können.

Sie können mehrere Laufwerksgruppen für eine Datenbank haben. Die folgenden Einschränkungen gelten jedoch für alle Festplattengruppen für eine bestimmte Datenbank:

- Plattengruppen für die Datenbank können nur von einem Volume-Manager verwaltet werden.
- Von einem logischen Volume-Manager gesicherte RAW-Geräte werden für den Schutz von Oracle Daten nicht unterstützt.

  RAW Device Storage und Automatic Storage Management (ASM)-Festplattengruppen müssen direkt auf physischen Geräten bereitgestellt werden. In einigen Fällen ist eine Partitionierung erforderlich.

- Eine Linux-Umgebung ohne logisches Volume-Management erfordert eine Partition.