Produktübersicht

SnapManager for SAP

NetApp
November 04, 2025

Inhalt

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 Tablespaces 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.

- Erstellung platzsparender Backup-Klone auf primärem oder sekundärem Storage

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 SAP 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 den Speicherort für das Archivprotokoll im Bereich Flash Recovery angeben, müssen Sie sicherstellen, dass Sie auch den Speicherort für das Archivprotokoll im angeben `archive_log_dest` Parameter.

Konsolidierung von Archivierungsprotokolldaten

SnapManager (3.2 oder höher) für SAP konsolidiert die Archiv-Log-Backups, um eine Mindestanzahl an Backups für Archiv-Log-Dateien zu erhalten. SnapManager für SAP 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.

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-Dokumentation"

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 protokolliert `sm_gui.log` Datei: [WARNUNG]: `SMSAP-01106: Error occurred while querying the repository: No more data to read from socket`. 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.

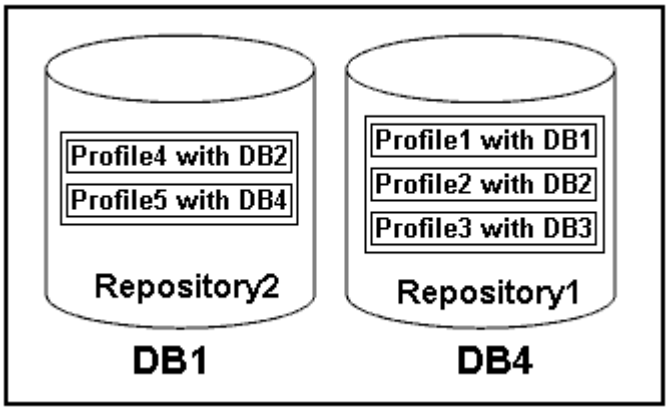
Welche Profile sind

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.

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.

Betriebsstatus	Beschreibung
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. Sie können den erstellten Klon aufteilen. 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.
- 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 zu `$ORACLE_HOME` Auf dem Zielcomputer löschen und löschen `sm_lock_ TargetDBName` Datei: Nach dem Löschen der Datei müssen Sie den SnapManager für SAP-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 über hinzugefügt werden `smsap credential set -host` Befehl.
- 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 im SnapManager-Benutzeranmeldeinformationen speichern `smsap credential set -host` Befehl.

> Der `smsap credential set -host` Der Befehl speichert Ihre Anmeldeinformationen, wenn der verwendet wird `host.credentials.persist` Die Eigenschaft in der Datei smsap.config ist auf festgelegt **`true`**.

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 nonprofilbefehlen wie dump und ausführen `system verify` Auf Host1.

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 Datenbanksystemkennung in das ein `oratab` Datei:

  Fügen Sie einen Eintrag in das ein `oratab` Datei für jede zu verwaltende Datenbank. SnapManager verlässt sich auf das `oratab` Datei zur Bestimmung des Home-Office von Oracle.

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

- 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.

SAP verwendet ein Standard-Layout für die Installation von Oracle Datenbanken. In diesem Layout speichert SAP Kopien der Oracle-Kontrolldatei in `E:\oracle\SID\origlogA, E:\oracle\SID\origlogB`, und `E:\oracle\SID\sapdata1 file systems`.

Die Kontrolldatei im sapdata1-Dateisystem steht in Konflikt mit den SnapManager-Anforderungen für die Trennung der Steuerdateien und Datendateien in separate Volumes und muss angepasst werden, damit eine schnelle Wiederherstellung möglich ist.

Da BR*Tools-Backups die Oracle- und SAP-Profile im dbs-Unterverzeichnis der Oracle-Installation enthalten, muss sich die Oracle-Installation im Storage befinden.

Im Falle einer neuen Installation können Sie den Speicherort der Steuerdateien mit SAPINST ändern und die Steuerdatei, die normalerweise im sapdata1-Dateisystem abgelegt wird, in ein Dateisystem verschieben, das

sich nicht im selben Volume befindet wie die Datendateien. (SAPINST ist das Tool, das SAP zur Installation von SAP-Systemen bereitstellt.)

Im Falle eines bereits installierten Systems müssen Sie jedoch die Steuerdatei vom Dateisystem verschieben, um eine schnelle Wiederherstellung mit SnapManager zu ermöglichen. Sie können dies tun, indem Sie ein neues Dateisystem in einem Volume erstellen, das keine Datendateien enthält, die Steuerdatei auf dieses Dateisystem verschieben und dann einen symbolischen Link aus dem vorherigen Dateisystem in das Verzeichnis für das neue Dateisystem erstellen. Um Datenbankfehler zu vermeiden, müssen SAP und die Oracle-Datenbank beim Verschieben der Kontrolldatei angehalten werden.

Bevor Sie Änderungen vornehmen, könnte die Liste der Dateien im sapdata1-Verzeichnis mit der Kontrolldatei wie folgt aussehen:

```
hostname:/
#  ls -l /oracle/SID/sapdata1/cntrl
-rw-r----- 1 orasid  dba  9388032 Jun 19 01:51 cntrlSID.dbf
```

Nach der Änderung könnte die Liste wie folgt aussehen:

```
hostname:/
# ls -sl /oracle/SID/sapdata1
0 lrwxrwxrwx 1 root root 19 2008-08-06 14:55 cntrl -> /oracle/SID/control
0 -rw-r--r-- 1 root root 0 2008-08-06 14:57 data01.dbf

# ls -sl /oracle/SID/control
0 -rw-r--r-- 1 root root 0 2008-08-06 14:56 cntrlSID.dbf
```

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 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.

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 5 x Oder Oracle Enterprise Linux 5-mal	Ja.	Nein	Nein	Ext3*
Red hat Enterprise Linux 6x 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***

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

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:

  - Stamm=*`host name`*
  - 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* (Multipliziert) Oracntrl02_ *sid* (Multipliziert)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_ *sid* (Multipliziert) Oralogen02_ *sid* (Multipliziert)	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	Oratep_ *dbname*	Ja.	Aus
Kontrolldateien	Oracntrl01_ *dbname* (Multipliziert) Oracntrl02_ *dbname* (Multipliziert)	Ja.	Aus

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Wiederherstellungsprotokolle	Oralogen01_ *dbname* (Multipliziert) Oralogen02_ *dbname* (Multipliziert)	Ja.	Aus
Archivprotokolle	Oraarch_ *dbname*	Ja.	Aus
Cluster-Dateien	Oracrs_ *clustername*	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 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

- 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

- 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.
- 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.

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 auswählen `-resetlogs` Option.

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 das `profile create` Für Vorgänge, die über die SnapManager GUI generiert werden, gibt es keine Verlaufskonfigurationsoptionen.

  Sie können das nicht verwenden `profile create` Befehl zum Konfigurieren der Verlaufs-Aufbewahrungseinstellungen über die SnapManager-CLI.

- 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 7-Mode verwenden und eine VBSR für die Backups ausführen möchten, die in den Volumes erstellt wurden, über die SnapMirror Beziehungen festgelegt wurden, können Sie die festlegen `override-vbsr-snapmirror-check` Option auf **ON** In SnapDrive für UNIX.

  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"

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 SAP unterstützt keine Migration von Vserver, wie sie von Clustered Data ONTAP nicht unterstützt wird
- SnapManager für SAP 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 Version 10gR2 und unterstützt Oracle 10gR1 nicht als Repository oder Zieldatenbank.
- Oracle Cluster File System (OCFS) wird von SnapManager nicht unterstützt.
- 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

"Interoperabilitätsmatrix"

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