



Installation and Setup for UNIX 7-Mode

SnapManager for SAP

NetApp
November 04, 2025

This PDF was generated from <https://docs.netapp.com/de-de/snapmanager-sap/unix-installation-7mode/reference-smsap-isg-snapmanager-architecture.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Installation and Setup for UNIX 7-Mode	1
Produktübersicht	1
SnapManager Highlights	1
Architektur von SnapManager	2
Implementierungs-Workflow	4
Vorbereitungen für die Implementierung	5
SnapManager Lizenzierung	5
Unterstützte Konfigurationen	6
Unterstützte Speichertypen	6
UNIX Host-Anforderungen	6
Konfigurieren von Datenbanken	7
Installation von SnapManager	7
SnapManager einrichten	7
Vorbereiten der Speichersysteme für die SnapMirror- und SnapVault-Replizierung	7
Verständnis der Unterschiede zwischen SnapMirror und SnapVault	7
Sichern und Überprüfen Ihrer Datenbanken	8
SnapManager Backup – Überblick	8
Backup-Strategie definieren	8
Upgrade von SnapManager	11
SnapManager wird vorbereitet	11
Aufgaben nach dem Upgrade	11
Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade	12
Weitere Schritte	17

Installation and Setup for UNIX 7-Mode

Produktübersicht

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

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

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

SnapManager Highlights

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

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

- Erstellung platzsparender Backups auf primärem oder sekundärem Storage

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

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

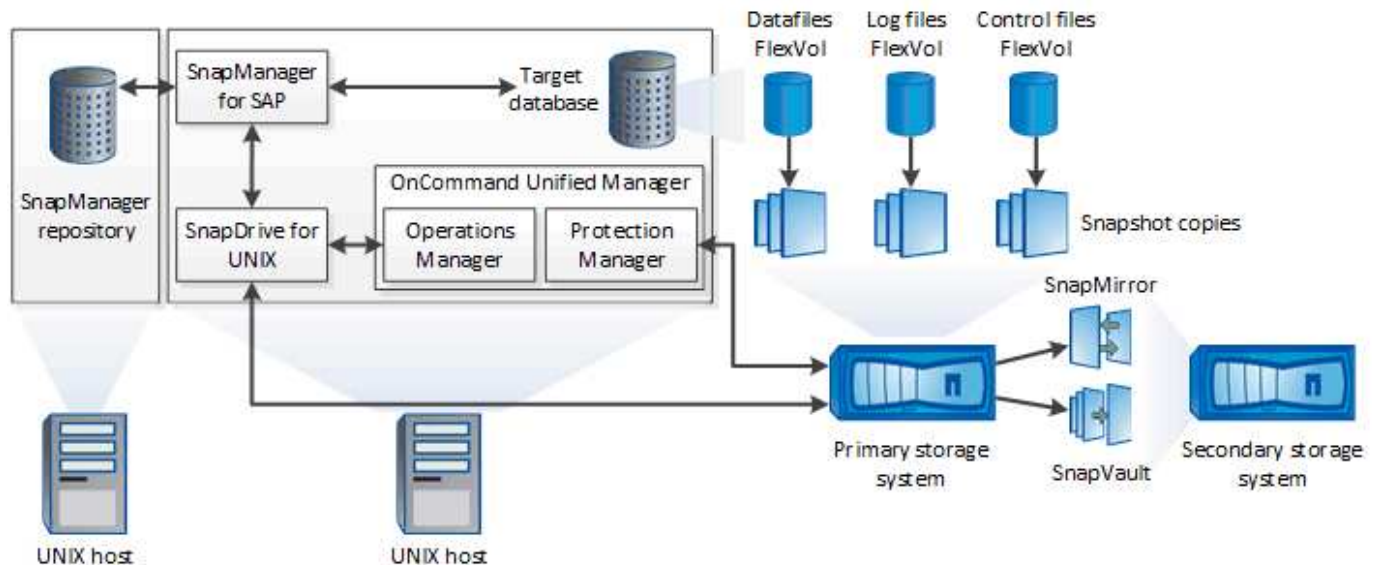
Ein Profil enthält Informationen über die Datenbank, die von SnapManager gemanagt werden soll.

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

SnapManager ermöglicht Ihnen die Aufteilung eines Datenbankklonen.

Architektur von SnapManager

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



SnapDrive für UNIX

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

SnapManager für SAP

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

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



Die unterstützte JRE-Version ist 1.8.

Zielt Datenbank

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

Die Zielt Datenbank kann eine eigenständige Real Application Clusters (RAC) sein oder auf Oracle Automatic Storage Management (ASM)-Volumes residieren. Weitere Informationen zu den unterstützten Oracle

Datenbankversionen, Konfigurationen, Betriebssystemen und Protokollen finden Sie im NetApp Interoperabilitäts-Matrix-Tool.

SnapManager Repository

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

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

OnCommand Unified Manager Core-Paket

Das zentrale OnCommand Unified Manager Paket umfasst die Funktionen von Operations Manager, Protection Manager und Provisioning Manager. Sie zentralisiert die Implementierung, das Klonen, Backup und Recovery sowie DR-Richtlinien. Durch die Integration dieser Funktionen können viele Management-Funktionen über ein einzelnes Tool ausgeführt werden.

Operations Manager

Operations Manager ist die webbasierte Benutzeroberfläche (UI) des Kernpakets von OnCommand Unified Manager. Sie wird für das tägliche Storage Monitoring, Problemwarnungen und die Berichterstellung in der Storage- und Storage-System-Infrastruktur genutzt. Die Integration von SnapManager nutzt die RBAC-Funktionen von Operations Manager.

Protection Manager

Protection Manager bietet Administratoren eine benutzerfreundliche Management-Konsole für die schnelle Konfiguration und Steuerung aller SnapMirror- und SnapVault-Vorgänge. Mit dieser Applikation können Administratoren einheitliche Datensicherungsrichtlinien anwenden, komplexe Datensicherungsprozesse automatisieren und Backup- und Replizierungsressourcen bündeln, um eine höhere Auslastung zu erzielen.

Die Schnittstelle für Protection Manager ist die NetApp Management Console, die Client-Plattform für NetApp Management Software-Applikationen. TheNetApp Management Console läuft auf einem Windows- oder Linux-System, das sich von dem Server unterscheidet, auf dem der OnCommand-Server installiert ist. So können Storage-, Applikations- und Serveradministratoren tägliche Aufgaben durchführen, ohne zwischen verschiedenen UIs wechseln zu müssen. Die Applikationen, die in der NetApp Management Console ausgeführt werden, sind Protection Manager, Provisioning Manager und Performance Advisor.

Primärspeicher

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

Sekundäres Storage-System

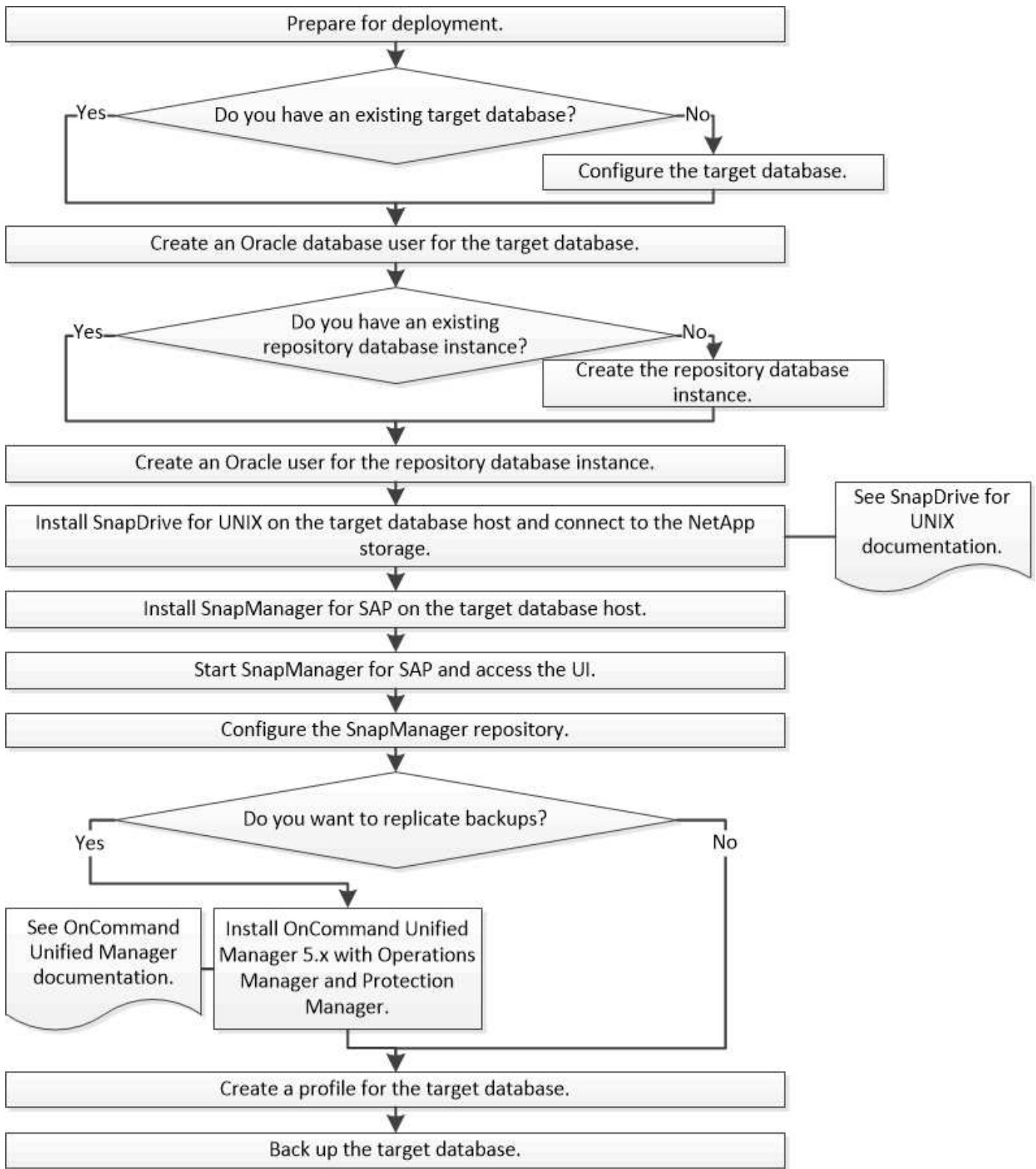
Wenn Sie die Datensicherung in einem Datenbankprofil ermöglichen, werden die Backups, die von SnapManager auf dem primären Storage-System erstellt wurden, mithilfe von SnapVault und SnapMirror Technologien auf ein sekundäres NetApp Storage-System repliziert.

Verwandte Informationen

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

Implementierungs-Workflow

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



Vorbereitungen für die Implementierung

SnapManager Lizenzierung

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

Die SnapManager Lizenzanforderungen lauten wie folgt:

Lizenz	Beschreibung	Bei Bedarf
SnapManager pro Server	Eine Host-seitige Lizenz für einen bestimmten Datenbank-Host. Lizenzen sind nur für Datenbank-Hosts erforderlich, auf denen SnapManager installiert ist. Für das Storage-System ist keine SnapManager Lizenz erforderlich.	Auf dem SnapManager-Host. Auf primären und sekundären Storage-Systemen ist keine SnapManager-Lizenz erforderlich, wenn die Lizenzierung pro Server verwendet wird.
SnapManager pro Storage-System	Eine Storage-seitige Lizenz, die eine beliebige Anzahl von Datenbank-Hosts unterstützt. Nur erforderlich, wenn Sie keine Serverlizenz auf dem Datenbank-Host verwenden.	Auf primären und sekundären Storage-Systemen.
SnapRestore	Eine erforderliche Lizenz zum Wiederherstellen von Datenbanken durch SnapManager.	Auf primären und sekundären Storage-Systemen. Erforderlich auf SnapVault Zielsystemen, um eine Datei aus einem Backup wiederherzustellen.
FlexClone	Eine optionale Lizenz zum Klonen von Datenbanken.	Auf primären und sekundären Storage-Systemen. erforderlich auf SnapVault Zielsystemen beim Erstellen von Klonen aus einem Backup.
SnapMirror	Eine optionale Lizenz zum Spiegeln von Backups auf ein Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
SnapVault	Eine optionale Lizenz zur Archivierung von Backups auf einem Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.

Lizenz	Beschreibung	Bei Bedarf
Protokolle	NFS-, iSCSI- oder FC-Lizenzen sind abhängig vom verwendeten Protokoll erforderlich.	Auf primären und sekundären Storage-Systemen. Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.

Unterstützte Konfigurationen

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

Informationen zu unterstützten Konfigurationen finden Sie im ["Interoperabilitäts-Matrix-Tool"](#).

Verwandte Informationen

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

Unterstützte Speichertypen

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

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

UNIX Host-Anforderungen

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

- Sie müssen SnapDrive auf dem Datenbank-Host installieren, bevor Sie SnapManager installieren.
- Sie können SnapManager entweder auf physischen oder virtuellen Maschinen installieren.
- Sie müssen dieselbe SnapManager-Version auf allen Hosts installieren, die sich dasselbe Repository teilen.

- Sie müssen Oracle Patch installieren 13366202 Wenn Sie Oracle Datenbanken 11.2.0.2 oder 11.2.0.3 verwenden.

Wenn Sie DNFS verwenden, müssen Sie außerdem die Patches installieren, die im Bericht My Oracle Support (MOS) aufgeführt sind 1495104 . 1 Für maximale Leistung und Stabilität.

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

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



SnapManager arbeitet auch in der virtualisierten VMware ESX Umgebung.

Konfigurieren von Datenbanken

Installation von SnapManager

SnapManager einrichten

Vorbereiten der Speichersysteme für die SnapMirror- und SnapVault-Replizierung

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

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

Verständnis der Unterschiede zwischen SnapMirror und SnapVault

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

Diese Ziele berücksichtigen das unterschiedliche Gleichgewicht, das jede Technologie zwischen den Zielen

der Backup-Währung und der Backup-Aufbewahrung findet:

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

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

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

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

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

Sichern und Überprüfen Ihrer Datenbanken

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

SnapManager Backup – Überblick

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

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

Backup-Strategie definieren

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



Informationen zu den Best Practices für SnapManager finden Sie unter *TR 3761*.

Welcher Modus für SnapManager Backups benötigen Sie?

SnapManager unterstützt zwei Backup-Modi:

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

Welche Art von SnapManager-Backup benötigen Sie?

SnapManager unterstützt drei Arten von Backups:

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

Was für ein Datenbankprofil benötigen Sie?

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

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

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

Welche Namenskonventionen sollten für Snapshot Kopien verwendet werden?

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



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

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

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

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

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

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

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



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

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

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

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



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

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

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

Upgrade von SnapManager

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

SnapManager wird vorbereitet

Die Umgebung, in der Sie ein SnapManager-Upgrade durchführen möchten, muss die spezifischen Software-, Hardware-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Aktuelle Informationen zu den Anforderungen finden Sie im ["Interoperabilitätsmatrix"](#).

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

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

Verwandte Informationen

["Interoperabilitätsmatrix"](#)

Aufgaben nach dem Upgrade

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



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

Prozessarten wiederherstellen

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

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

Sie können die zum Erstellen des Backups verwendete SnapManager-Version bestimmen, indem Sie den Befehl `-Backup show` ausführen.

Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade

Der Rolling Upgrade-Ansatz, mit dem Sie Hosts auf gestaffelte, Host-für-Host-Art aktualisieren können, wird von SnapManager 3.1 unterstützt.

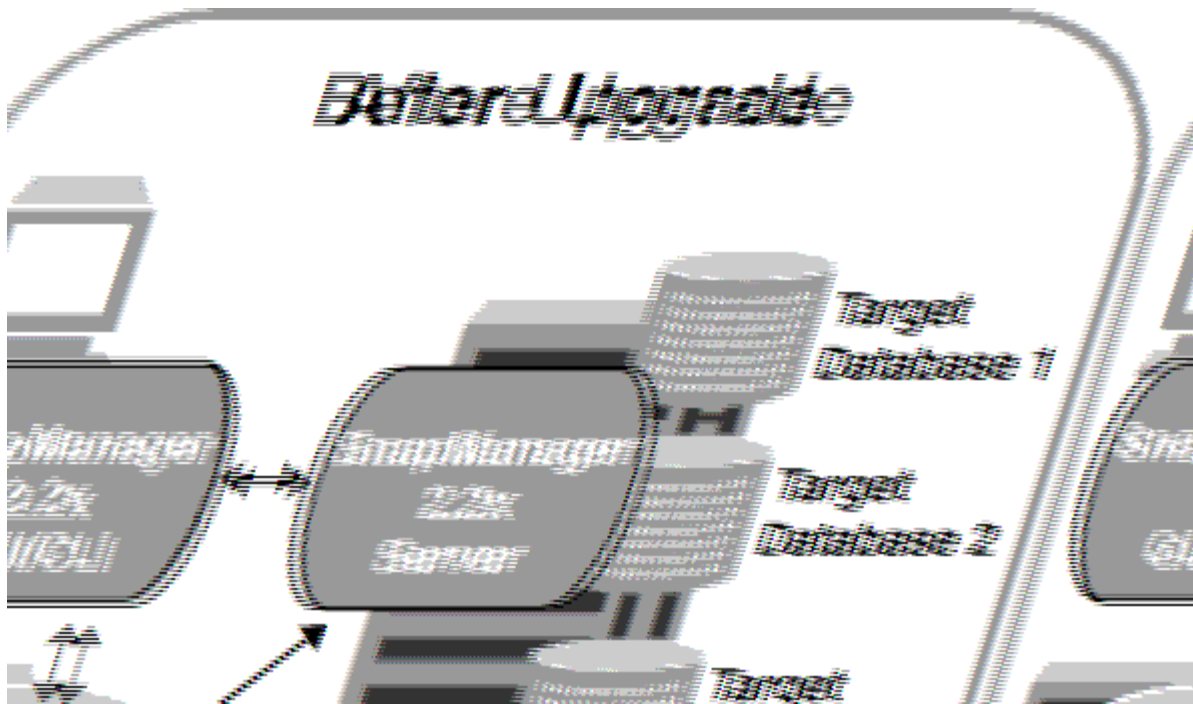
Mit SnapManager 3.0 oder einer älteren Version konnten Sie nur alle Hosts gleichzeitig aktualisieren. Dies führte zu Ausfallzeiten aller SnapManager-Hosts und der geplanten Betrieb während des Upgrade-Vorgangs.

Das Rolling Upgrade bietet folgende Vorteile:

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



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



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

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



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

Verwandte Informationen

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

Voraussetzungen für Rolling Upgrades

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

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

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

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



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

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

Die SnapDrive-Dokumentation enthält Details zur Installation von SnapDrive.

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

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



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

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

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

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



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

Verwandte Informationen

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

Was ist ein Rollback

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



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

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

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

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

Einschränkungen bei der Durchführung eines Rollbacks

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

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

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

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

- Ändern Sie den Mount-Status des Backups.

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

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

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

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

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

Voraussetzungen für die Durchführung eines Rollbacks

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

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



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

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

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

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

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

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

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

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

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



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

Verwandte Informationen

["Dokumentation auf der NetApp Support Site"](#)

Aufgaben nach dem Rollback ausführen

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

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

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

Beispiel

Die Dateinamen können wie folgt lauten:

- `repository#SMSAP300a#SMSAPREPO1#10.72.197.141#1521`
- `repository-smsap300a-smsaprepo1-10.72.197.141-1521`

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

Beispiel

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

Weitere Schritte

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

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

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

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

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

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

- [SnapManager for SAP Online-Hilfe](#)

Beschreibt die Schritt-für-Schritt-Verfahren zur Durchführung verschiedener SnapManager-Vorgänge

mithilfe der SnapManager-Benutzeroberfläche.



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

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

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

Verwandte Informationen

["NetApp Support"](#)

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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