



Was ist SnapManager für SAP

SnapManager for SAP

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/de-de/snapmanager-sap/windows/concept-what-snapmanager-for-oraclesnapmanager-for-sap-does.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

- Was ist SnapManager für SAP 1
 - Was macht SnapManager für SAP 1
 - Integration in andere Applikationen und Technologien von NetApp. 4
 - Vorteile von SnapManager..... 5
 - Was ist die Architektur von SnapManager für SAP 8
 - Repositories 9
 - Welche Profile sind. 10
 - Die Status der SnapManager-Operation lauten 12
 - Wie SnapManager die Sicherheit gewährleistet 13
 - Online-Hilfe aufrufen und drucken 14

Was ist SnapManager für SAP

SnapManager bietet die Tools, die für richtlinienbasiertes Datenmanagement, die Planung und Erstellung von regelmäßigen Datenbank-Backups, die Wiederherstellung von Daten aus diesen Backups im Falle von Datenverlust oder Notfällen und die Erstellung von Datenbankklonen erforderlich sind. Sie können Backups auf dem Primärspeicher erstellen und geschützte Backups auf dem Sekundärspeicher mithilfe von Post-Processing-Skripten erstellen.

SnapManager nutzt NetApp Technologien bei der Integration in die neuesten Datenbankversionen. SnapManager ist in folgende NetApp Applikationen und Technologien integriert:

- SnapDrive automatisiert Storage-Provisionierungsaufgaben und vereinfacht die Erstellung fehlerfreier und Host-konsistenter Snapshot-Kopien des Storage.
- Snapshot (eine Funktion von Data ONTAP) erstellt zeitpunktgenaue Kopien der Datenbank.
- SnapVault (eine lizenzierte Funktion von Data ONTAP) nutzt festplattenbasierte Backups für zuverlässiges Backup und Recovery von Datenbanken mit geringem Overhead.
- SnapMirror (eine lizenzierte Funktion von Data ONTAP) repliziert Datenbankdaten über ein globales Netzwerk mit hoher Geschwindigkeit auf einfache, zuverlässige und kostengünstige Weise.
- SnapRestore (eine lizenzierte Funktion von Data ONTAP) stellt eine vollständige Datenbank innerhalb weniger Sekunden wieder her – unabhängig von der Kapazität oder der Anzahl der Dateien.
- FlexClone (eine lizenzierte Funktion von Data ONTAP) hilft bei der Erstellung schneller, platzsparender Datenbankklone aus den Snapshot Backups.

SnapManager arbeitet mit SAN-Protokollen (FC und iSCSI) zusammen.

Was macht SnapManager für SAP

SnapManager für SAP vereinfacht und automatisiert Backups, Recoverys und das Klonen von Datenbanken mithilfe der Snapshot Kopien, SnapRestore und FlexClone Technologien.

SnapManager bietet Datenbankadministratoren (DBAs) folgende Vorteile:

- Arbeiten mit Datenbankprofilen
 - Sie können Host- und Datenbankinformationen in Profilen organisieren und aufbewahren.

Wenn Sie ein Backup auf der Grundlage eines Profils initiieren, können Sie die Informationen wiederverwenden, anstatt sie für jedes Backup erneut eingeben zu müssen. SnapManager ermöglicht Ihnen darüber hinaus die schnelle Überwachung von Abläufen mithilfe von Profilen.

- Im Profil können Sie die Benennungsmuster für Snapshot Kopien definieren und einen benutzerdefinierten Text (Präfix oder Suffix) eingeben, sodass alle Snapshot Kopien dieselbe Namenskonvention verwenden können, die den Unternehmensrichtlinien entspricht.
- Sie müssen den Namen des Speichersystems nicht kennen, da Datenbankdateien automatisch dem zugehörigen Speicher zugeordnet werden.
- Wenn Sie ein neues Profil erstellen, können Sie die Option zum Trennen des Backup des Archivprotokolls von der Datensicherung der Datendatei angeben.

Sie können das vorhandene Profil auch aktualisieren, um die Sicherung des Archivprotokolls von der Datensicherung der Datendatei zu trennen.

- Durchführen des Datenbank-Backup-Vorgangs

- Backup von kompletten und teilweisen Datenbanken

- Sie können schnell und platzsparend ein vollständiges oder partielles Backup erstellen, sodass Sie Backups häufiger durchführen können.

Das vollständige Datenbank-Backup enthält alle Datendateien, Steuerdateien und Archivprotokolldateien in einem einzigen Backup.

Das partielle Datenbank-Backup enthält bestimmte Datendateien oder Tablespaces, alle Kontrolldateien und alle Archivprotokolldateien.

- Backups können durch Nachverarbeitungsskripte auf den Sekundärspeicher gesichert werden.
 - Die Backups können auf Stundenbasis, wöchentlich, täglich, monatlich oder unbegrenzt geplant werden.
 - Separate Backup von Datendateien und Archivprotokolldateien
 - Mit SnapManager (3.2 oder höher) können Sie die Datendateien und die Log-Dateien zur Archivierung separat sichern. Um diesen Vorgang durchzuführen, müssen Sie die Option zum Trennen der Archivprotokolldateien beim Erstellen oder Aktualisieren des Profils angeben.
 - Sie können in der Aufbewahrungsrichtlinie die Anzahl und die Dauer angeben, für die die Backups der Datendateien aufbewahrt werden sollen.
 - Sie können die Dauer für die Backups der Archivprotokolldatei angeben, die während der Aufbewahrungsdauer des Archivprotokolls aufbewahrt werden soll.
 - SnapManager (3.2 oder höher) konsolidiert außerdem die Archiv-Log-Backups auf eine Mindestanzahl von Backups, indem die Archiv-Log-Backups mit doppelten Archivprotokolldateien freigegeben werden und nur die Archiv-Log-Backups mit einzigartigen Archiv-Log-Dateien vorgehalten werden. Diese Konsolidierung kann jedoch optional deaktiviert werden.

- Verwalten der Archivprotokolldateien

- Mit SnapManager (3.2 oder höher) können Sie die Archivprotokolldateien aus den Archivprotokollzielen beschneiden.

Der von den beschnittenen Archivprotokolldateien belegte Speicherplatz wird freigegeben, wenn die Archiv-Log-Backups, die diese Archivprotokolldateien enthalten, gelöscht werden.

- SnapManager stellt sicher, dass die Archiv-Log-Dateien gesichert werden, bevor sie von den Archiv-Protokollzielen beschnitten werden.

Die nicht gesicherten Archivprotokolldateien werden nicht beschnitten.

- SnapManager stellt sicher, dass die Archivprotokolldateien an die Data Guard-Standby-Datenbank gesendet werden, während Archivprotokolldateien aus einer primären Data Guard-Datenbank beschnitten werden.
 - SnapManager stellt sicher, dass die Archivprotokolldateien vom Oracle Stream Capture-Prozess erfasst werden, falls vorhanden.
 - Empfehlung
 - Um den Zielplatz für Archivprotokolle effektiv zu managen, müssen Sie die Archiv-Log-Backups

erstellen und die Archiv-Log-Dateien damit beschneiden.

- SnapManager konsolidiert die Archiv-Log-Backups und enthält so eine Mindestanzahl von Backups, indem die Archiv-Log-Backups mit duplizierten Archiv-Log-Dateien erstellt und nur die Archiv-Log-Backups genutzt werden.

Diese Konsolidierung kann jedoch optional deaktiviert werden. Die Archiv-Log-Backups, die doppelte Archiv-Log-Dateien enthalten, werden freigegeben und ein einzelnes Backup mit einzigartigen Archiv-Logs bleibt erhalten.

- Durchführen des Datenbankwiederherstellungsvorgangs

- Sie können dateibasierte Restore-Vorgänge durchführen.

Sie können außerdem eine Vorschau der Wiederherstellungsvorgänge anzeigen und eine Datei-für-Datei-Analyse von Wiederherstellungsvorgängen erhalten, bevor der Vorgang ausgeführt wird.

- Mit SnapRestore lässt sich der mittlere Zeitaufwand für die Wiederherstellung einer Datenbank verringern.
- Mit SnapManager (3.2 oder höher) können Sie die Datenbank automatisch wiederherstellen, indem Sie die Archivprotokolldateien aus dem Backup verwenden, selbst wenn die Archivprotokolldateien nicht im Archivprotokollziel verfügbar sind.

SnapManager (3.2 oder höher) bietet auch eine Möglichkeit, die Datenbank durch die Verwendung der Archiv-Log-Dateien aus dem externen Standort in einem bestimmten Ausmaß wiederherzustellen.

- Klonen von Datenbanken für Tests und Entwicklung

- Sie können einen Klon einer Datenbank erstellen, sodass die Datenbank außerhalb der Produktionsumgebung eingerichtet werden kann.

Sie können beispielsweise in der Entwicklungs- und Testumgebung zum Testen von Upgrades auf wichtige Systeme klonen.

- Sie können eine Datenbank auf einem Primärspeichersystem klonen.
- Mit SnapManager (3.2 oder höher) können Sie die Backups der Datendatei mit den im Backup verfügbaren Archivprotokolldateien klonen.
 - Sie können die Backups der Datendatei nur klonen, wenn das Archivprotokoll-Backup miterstellt wird.
 - Sie können die Backups der Datendatei auch klonen, wenn die Archivprotokolldateien in einem bestimmten Umfang separat erstellten Archiv-Log-Backups zur Verfügung stehen.
 - Sie können die Backups einer eigenständigen Datenbank in einem bestimmten Umfang auch mit Archivprotokolldateien von jedem externen Standort aus klonen, auf den Oracle zugreifen kann.
 - Wenn die Backups von einem externen Standort aus verfügbar sind, können Sie den externen Standort beim Klonen angeben, um die geklonte Datenbank in einen konsistenten Status wiederherzustellen.
- Das Klonen der rein archivprotokollbasierten Backups wird nicht unterstützt.

- Allgemein

- Integration in BR*Tools von SAP

Das BR*Tools-Paket umfasst SAP-Tools wie BRARCHIVE, BRBACKUP, BRCONNECT, BRRECOVER, BRRESTORE, BRSCAPE und BRTOOLS.

SnapManager bietet Storage-Administratoren folgende Vorteile:

- Unterstützt unterschiedliche SAN-Protokolle
- Ermöglicht Ihnen die Optimierung von Backups auf der Grundlage der für Ihre Umgebung am besten geeigneten Backup-Art (vollständig oder teilweise).
- Erstellt platzsparende Datenbank-Backups.
- Erstellung platzsparender Klone:

SnapManager arbeitet darüber hinaus mit folgenden Oracle Funktionen zusammen:

- SnapManager kann die Backups mit RMAN von Oracle katalogisieren.

Bei Verwendung von RMAN kann ein DBA die SnapManager Backups nutzen und den Nutzen aller RMAN Funktionen, wie etwa das Restore auf Blockebene, erhalten. Dank SnapManager kann RMAN die Snapshot Kopien bei Recovery- oder Restore-Vorgängen verwenden. So können Sie beispielsweise RMAN zum Wiederherstellen einer Tabelle in einem Tablespace und zum Durchführen vollständiger Restores und Recoverys von Datenbanken und Tablespaces aus Snapshot-Kopien von SnapManager verwenden. Der RMAN-Wiederherstellungskatalog sollte sich nicht in der Datenbank befinden, die gesichert wird.

Integration in andere Applikationen und Technologien von NetApp

SnapManager für SAP ist ein eigenständiges Produkt, das die Funktionen anderer NetApp Produkte integriert und so schnelle Backups ermöglicht, die nur wenig Speicherplatz benötigen.

SnapManager lässt sich mit den folgenden NetApp Applikationen und Technologien integrieren:

Anwendungen und Technologien	Beschreibung
SnapDrive	SnapManager erstellt mithilfe von SnapDrive Snapshot Kopien des Storage. Snapshot-Kopien sorgen dafür, dass Backups platzsparend und schneller erstellt werden können als die Disk-to-Disk-Backups.
FlexClone (eine lizenzierte Funktion von Data ONTAP)	SnapManager erstellt mithilfe der FlexClone Funktion schnelle, platzsparende Klone von Backups.
Snapshot (eine Funktion von Data ONTAP)	Mit der Snapshot Technologie werden zeitpunktgenaue Kopien der Datenbank erstellt.
SnapRestore (eine lizenzierte Funktion von Data ONTAP)	SnapManager reduziert mit SnapRestore die durchschnittliche Zeit zum Recovery einer Datenbank. SnapRestore kann einzelne Dateien auf einem Volume mit mehreren Terabyte wiederherstellen, sodass der Betrieb schnell wieder aufgenommen werden kann.

Anwendungen und Technologien	Beschreibung
SnapVault (eine lizenzierte Funktion von Data ONTAP)	SnapVault nutzt festplattenbasierte Backups für zuverlässiges Backup und Recovery von Datenbanken mit geringem Overhead.
SnapMirror (eine lizenzierte Funktion der Data ONTAP)	SnapMirror repliziert Datenbankdaten einfach, zuverlässig und kostengünstig über ein globales Netzwerk mit hoher Geschwindigkeit.

Vorteile von SnapManager

Mit SnapManager für SAP können verschiedene Aufgaben an den Datenbanken ausgeführt und Daten effizient gemanagt werden.

SnapManager für SAP arbeitet mit Storage-Systemen zusammen und ermöglicht die folgenden Aufgaben:

- Erstellen Sie platzsparende Backups auf primärem oder sekundärem Storage und planen Sie Backups.

Sie können vollständige und teilweise Datenbank-Backups erstellen und Richtlinien für die Aufbewahrungsdauer anwenden. SnapManager (3.2 oder höher) ermöglicht Ihnen, nur die Datendateien und Archivprotokolle zu erstellen.

- SnapManager (3.2 oder höher) ermöglicht die Vorverarbeitung bzw. Nachbearbeitung der Backup- und Restore-Vorgänge vor oder nach der Durchführung.
- SnapManager (3.2 oder höher) ermöglicht Ihnen den Schutz von Backups mithilfe der Nachbearbeitungsskripte.
- Stellen Sie vollständige oder teilweise Datenbanken mithilfe des dateibasierten Wiederherstellungsvorgangs wieder her.
- Automatisches Wiederherstellen und Wiederherstellen von Datenbank-Backups.

SnapManager (3.2 oder höher) ermöglicht die automatische Wiederherstellung und Wiederherstellung von Datenbank-Backups. SnapManager stellt die wiederhergestellte Datenbank automatisch wieder her, indem die Archiv-Log-Dateien aus den Backups erkannt, Mounted und angewendet werden.

- Bei der Erstellung von Backups nur für die Archivprotokolle Archivprotokolldateien aus den Archivprotokollzielen abschneiden.
- Bewahren Sie die minimale Anzahl von Backups für Archivprotokolle automatisch auf, indem Sie nur die Backups mit einzigartigen Archivprotokolldateien aufbewahren.
- Verfolgen Sie die Betriebsdetails und erstellen Sie Berichte nach Host, Profil, Backup oder Klon.
- Überprüfen Sie den Backup-Status.
- Historie der einem Profil zugehörigen SnapManager Vorgänge beibehalten
- Erstellung platzsparender Backup-Klone auf dem Primärspeicher

Backups mit Snapshot Kopien erstellen

SnapManager ermöglicht die Erstellung von Backups auf dem primären (lokalen) Storage und auch auf dem sekundären (Remote-) Storage mithilfe von Nachbearbeitungsskripten.

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 Tablespace, alle Archivprotokolldateien und Kontrolldateien

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

- Alle Datendateien und die Kontrolldateien
- Ausgewählte Datendateien oder Tablespace 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 Säubern 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.

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 auf dem Primärsystem 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.

Was ist die Architektur von SnapManager für SAP

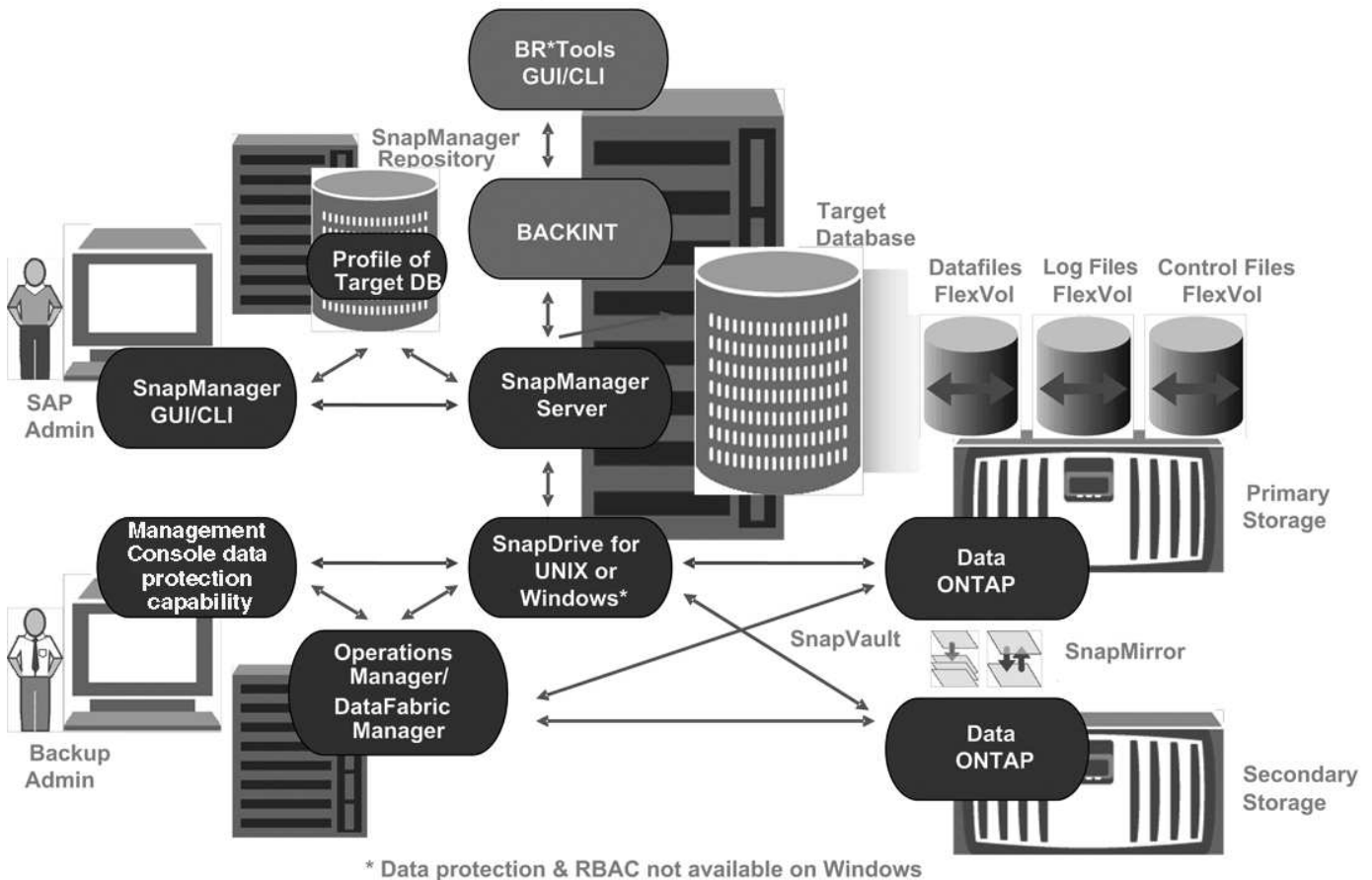
Die Architektur von SnapManager für SAP umfasst viele Komponenten, wie beispielsweise das SnapManager für SAP Host, Client und Repository. Weitere Komponenten sind die primären und sekundären Storage-Systeme und andere NetApp Produkte.

Die Architektur von SnapManager für SAP umfasst die folgenden Architekturkomponenten:

- SnapManager Host
- Grafische SnapManager Benutzeroberfläche oder Befehlszeilenschnittstelle
- SnapManager Repository
- SnapManager für SAP BACKINT Schnittstelle
- Primärspeicher
- Sekundäre Storage-Systeme
- SnapDrive für Windows

Das folgende Bild zeigt die Architektur von SnapManager für SAP und die zugehörigen Komponenten:

SnapManager for SAP Architecture



SnapManager Host

Der SnapManager Host ist ein Windows Server, der auch andere NetApp Produkte ausführt.

Der SnapManager Host wird mit den folgenden Produkten installiert:

- SnapDrive für Windows
- Host Utilities

Der SnapManager-Host wird als Service ausgeführt.

Der SnapManager-Host unterstützt auch die BACKINT-Schnittstelle, die für SAP BR*Tools verwendet wird.

Grafische SnapManager-Benutzer- und Befehlszeilenschnittstellen

Der SnapManager Client enthält eine grafische Benutzeroberfläche (GUI) und eine Befehlszeilenschnittstelle (CLI).

SnapManager Repository

Im Repository werden Informationen zu verschiedenen SnapManager-Vorgängen gespeichert, beispielsweise die Zeit von Backups, Tabellen und Datendateien, die gesichert wurden, bei Storage-Systemen, bei erstellten Klonen und bei Snapshot Kopien.

Die Repository-Datenbank kann nicht in derselben Datenbank vorhanden sein und darf auch nicht Teil derselben Datenbank sein, die von SnapManager gesichert wird. Dies liegt daran, dass das Repository die Namen der Datenbank-Snapshot-Kopien speichert, die während des Backup-Betriebs erstellt wurden. Das Repository muss in einer anderen Datenbank als der zu sichernden Datenbank erstellt werden. Das heißt, Sie müssen mindestens zwei Datenbanken haben: Die SnapManager Repository-Datenbank und die von SnapManager gemanagte Zieldatenbank. Wenn Sie die SnapManager-Services ausführen, müssen beide Datenbanken betriebsbereit sein.



SnapManager-Vorgänge dürfen nicht über die GUI oder die CLI ausgeführt werden, wenn die Repository-Datenbank ausfällt.

SnapDrive auf SnapManager Server

SnapManager erstellt Snapshot Kopien des Storage-Systems mithilfe von SnapDrive für Windows. SnapDrive befindet sich auf demselben Server wie SnapManager.

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 Repositories haben, wobei jedes Repository mehrere Profile enthält.

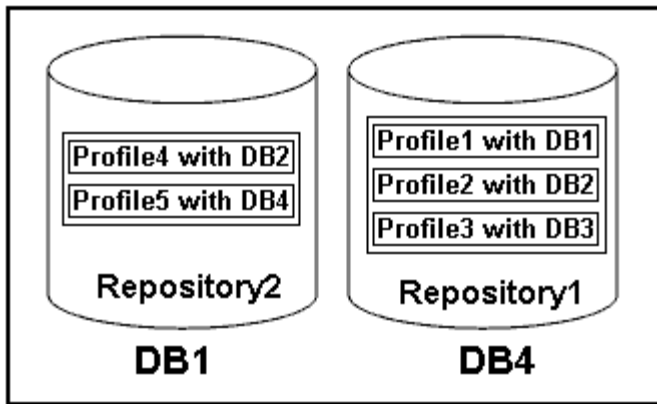
Welche Profile sind

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 gemäß den bestehenden Richtlinien zur Backup-Aufbewahrung aufbewahrt. 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 Archiv-Log-Backups getrennt haben, können Sie mit SnapManager unterschiedliche Aufbewahrungszeiten 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.
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.

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 Windows 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.

SnapManager gewährleistet die Sicherheit, indem die Benutzerauthentifizierung über Passwordeinforderungen oder durch Festlegen von Benutzeranmeldeinformationen angefordert wird. 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` Das Hotel befindet sich im `smsap.config` Die Datei ist auf **true** eingestellt.

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-Profile-Befehle wie `ausführen dump` Und `system verify` Auf Host1.

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.

Schritte

- 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.
- Verwenden Sie das **Inhaltsverzeichnis** im linken Fensterbereich, um durch die Themen zu navigieren.
- Klicken Sie oben im Hilfefenster auf das Druckersymbol, um einzelne Themen zu drucken.

Copyright-Informationen

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT 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.