



SnapCenter Plug-in für SAP HANA-Datenbanken

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-61/protect-hana/concept_snapcenter_plug_in_for_sap_hana_database_overview.html on November 06, 2025.
Always check docs.netapp.com for the latest.

Inhalt

SnapCenter Plug-in für SAP HANA-Datenbanken	1
Übersicht über das SnapCenter -Plug-in für die SAP HANA-Datenbank	1
Was Sie mit dem SnapCenter Plug-in für die SAP HANA-Datenbank tun können	1
SnapCenter Plug-in für SAP HANA-Datenbankfunktionen	1
Vom SnapCenter Plug-in für die SAP HANA-Datenbank unterstützte Speichertypen	2
Für das SAP HANA-Plug-In sind mindestens ONTAP Berechtigungen erforderlich	3
Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für SAP HANA-Datenbanken	6
Backup-Strategie für SAP HANA-Datenbanken	6
Definieren Sie eine Sicherungsstrategie für SAP HANA-Datenbanken	6
Automatische Erkennung von Ressourcen auf Linux-Hosts	7
Unterstützte Sicherungstypen	8
So verwendet das SnapCenter -Plug-in für die SAP HANA-Datenbank Snapshots der Konsistenzgruppe	8
So verwaltet SnapCenter die Verwaltung von Protokoll- und Datensicherungen	9
Überlegungen zur Festlegung von Sicherungszeitplänen für die SAP HANA-Datenbank	9
Anzahl der für SAP HANA-Datenbanken benötigten Sicherungsaufträge	9
Sicherungsnamenskonventionen für Plug-in für SAP HANA-Datenbanken	9
Wiederherstellungsstrategie für SAP HANA-Datenbanken	10
Definieren Sie eine Wiederherstellungsstrategie für SAP HANA-Ressourcen	10
Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen	10
Unterstützte Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken	11
Arten von Wiederherstellungsvorgängen für automatisch erkannte SAP HANA-Datenbanken	11
Für SAP HANA-Datenbanken unterstützte Arten von Wiederherstellungsvorgängen	12

SnapCenter Plug-in für SAP HANA-Datenbanken

Übersicht über das SnapCenter -Plug-in für die SAP HANA-Datenbank

Das SnapCenter -Plug-in für SAP HANA-Datenbanken ist eine hostseitige Komponente der NetApp SnapCenter software , die ein anwendungsbewusstes Datenschutzmanagement von SAP HANA-Datenbanken ermöglicht. Das Plug-in für SAP HANA-Datenbanken automatisiert die Sicherung, Wiederherstellung und das Klonen von SAP HANA-Datenbanken in Ihrer SnapCenter Umgebung.

SnapCenter unterstützt Einzelcontainer und Multitenant-Datenbankcontainer (MDC). Sie können das Plug-in für die SAP HANA-Datenbank sowohl in Windows- als auch in Linux-Umgebungen verwenden. Das Plug-In, das nicht auf dem HANA-Datenbankhost installiert ist, wird als zentralisiertes Host-Plug-In bezeichnet. Das zentralisierte Host-Plug-In kann mehrere HANA-Datenbanken auf verschiedenen Hosts verwalten.

Wenn das Plug-in für die SAP HANA-Datenbank installiert ist, können Sie SnapCenter mit der NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen. Sie können das Plug-in auch mit der NetApp SnapVault -Technologie verwenden, um eine Disk-to-Disk-Backup-Replikation zur Einhaltung von Standards durchzuführen.

Das Plug-in für die SAP HANA-Datenbank unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie ein transparentes Failover durchführen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

Was Sie mit dem SnapCenter Plug-in für die SAP HANA-Datenbank tun können

Wenn Sie das Plug-in für die SAP HANA-Datenbank in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von SAP HANA-Datenbanken und deren Ressourcen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Datenbanken hinzufügen.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

SnapCenter Plug-in für SAP HANA-Datenbankfunktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem

Speichersystem integrieren. Um mit dem Plug-in für die SAP HANA-Datenbank zu arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter .

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Kopiertechnologie**

SnapCenter verwendet die NetApp Snapshot-Technologie mit dem Plug-in für die SAP HANA-Datenbank zum Sichern von Ressourcen.

Die Verwendung des Plug-ins für die SAP HANA-Datenbank bietet außerdem folgende Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung für die Consistency Group (CG) Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Unterstützung für dateibasierte Sicherung.
- Unterstützung für Linux LVM auf dem XFS-Dateisystem.

Vom SnapCenter Plug-in für die SAP HANA-Datenbank unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen Maschinen als auch auf virtuellen Maschinen (VMs). Sie müssen die Unterstützung für

Ihren Speichertyp überprüfen, bevor Sie das SnapCenter -Plug-in für die SAP HANA-Datenbank installieren.

Maschine	Speichertyp
Physischer Server	<ul style="list-style-type: none"> • FC-verbundene LUNs • Über iSCSI verbundene LUNs • Über NFS verbundene Volumes
VMware ESXi	<ul style="list-style-type: none"> • RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. <p>Sie können die Datei LinuxConfig.pm unter <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> bearbeiten, um den Wert des Parameters SCSI_HOSTS_OPTIMIZED_RESCAN auf 1 zu setzen und nur die HBAs erneut zu scannen, die in <code>HBA_DRIVER_NAMES</code> aufgeführt sind.</p> <ul style="list-style-type: none"> • iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datenspeichern • VMDKs auf VMFS erstellt • NFS-Volumes, die direkt mit dem Gastsystem verbunden sind • vVol-Datenspeicher auf NFS und SAN <p>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p>

Für das SAP HANA-Plug-In sind mindestens ONTAP Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
 - Ereignis generieren-Autosupport-Protokoll
 - Jobverlauf anzeigen
 - Jobstopp
 - Montag
 - LUN erstellen

- LUN erstellen
- LUN erstellen
- LUN löschen
- lun igrup hinzufügen
- lun igrup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- LUN-Igroup umbenennen
- lun igrup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN persistent-reservation clear
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror>Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen

- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen

- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
 - Netzwerkschnittstelle
 - Netzwerkschnittstelle anzeigen
 - vServer

Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für SAP HANA-Datenbanken

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter -Jobs durchgeführt. Wenn Sie SnapMirror Active Sync verwenden, verwenden Sie die Standardzeitpläne von SnapMirror oder SnapVault sowohl für SnapMirror Active Sync als auch für asynchrone Beziehungen.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär > Spiegel > Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im "[ONTAP-Dokumentation](#)" .

Backup-Strategie für SAP HANA-Datenbanken

Definieren Sie eine Sicherungsstrategie für SAP HANA-Datenbanken

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge verfügen Sie über die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich

der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

Schritte

1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.
4. Entscheiden Sie, ob Sie eine auf Snapshot-Kopien basierende Richtlinie erstellen möchten, um anwendungskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie die Integrität der Datenbank überprüfen möchten.
6. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
7. Bestimmen Sie die Aufbewahrungszeit für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
8. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

Automatische Erkennung von Ressourcen auf Linux-Hosts

Ressourcen sind SAP HANA-Datenbanken und Nicht-Datenvolumes auf dem Linux-Host, die von SnapCenter verwaltet werden. Nach der Installation des SnapCenter -Plug-ins für das SAP HANA-Datenbank-Plug-in werden die SAP HANA-Datenbanken auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.

Die automatische Erkennung wird für die folgenden SAP HANA-Ressourcen unterstützt:

- Einzelbehälter

Nach der Installation oder Aktualisierung des Plug-ins werden die einzelnen Containerressourcen auf einem zentralen Host-Plug-in als manuell hinzugefügte Ressourcen weitergeführt.

Nach der Installation oder Aktualisierung des Plug-Ins werden die SAP HANA-Datenbanken automatisch nur auf den SAP HANA Linux-Hosts erkannt, die direkt bei SnapCenter registriert sind.

- Multitenant-Datenbankcontainer (MDC)

Nach der Installation oder Aktualisierung des Plug-Ins werden die auf einem zentralen Host-Plug-In befindlichen MDC-Ressourcen weiterhin als manuell hinzugefügte Ressourcen verwendet.

Sie müssen die MDC-Ressourcen nach dem Upgrade auf SnapCenter 4.3 weiterhin manuell zum zentralen Host-Plug-In hinzufügen.

Bei SAP HANA Linux-Hosts, die direkt in SnapCenter registriert sind, löst die Installation oder Aktualisierung des Plug-Ins eine automatische Erkennung von Ressourcen auf dem Host aus. Nach dem Upgrade des Plug-Ins wird für jede MDC-Ressource, die sich auf dem Plug-In-Host befand, automatisch eine andere MDC-Ressource mit einem anderen GUID-Format erkannt und in SnapCenter registriert. Die neue Ressource befindet sich im gesperrten Zustand.

Wenn sich beispielsweise in SnapCenter 4.2 eine E90-MDC-Ressource auf dem Plug-In-Host befand und

manuell registriert wurde, wird nach dem Upgrade auf SnapCenter 4.3 eine weitere E90-MDC-Ressource mit einer anderen GUID erkannt und in SnapCenter registriert.

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts



Falls die oben genannten Ressourcen erkannt werden, werden die Datenschutzvorgänge für diese Ressourcen nicht unterstützt.

- HANA-Konfiguration mit mehreren Hosts
- Mehrere Instanzen auf demselben Host
- Mehrstufige Scale-Out-HANA-Systemreplikation
- Kaskadierte Replikationsumgebung im Systemreplikationsmodus

Unterstützte Sicherungstypen

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt dateibasierte Backups und Snapshot-Kopien-basierte Backup-Typen für SAP HANA-Datenbanken.

Dateibasierte Sicherung

Dateibasierte Backups überprüfen die Integrität der Datenbank. Sie können den dateibasierten Sicherungsvorgang so planen, dass er in bestimmten Intervallen erfolgt. Es werden nur aktive Mandanten gesichert. Sie können dateibasierte Sicherungen von SnapCenter nicht wiederherstellen und klonen.

Snapshot-Kopie-basierte Sicherung

Auf Snapshot-Kopien basierende Backups nutzen die NetApp Snapshot-Technologie, um schreibgeschützte Online-Kopien der Volumes zu erstellen, auf denen sich die SAP HANA-Datenbanken befinden.

So verwendet das SnapCenter -Plug-in für die SAP HANA-Datenbank Snapshots der Konsistenzgruppe

Sie können das Plug-In verwenden, um Konsistenzgruppen-Snapshots für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes aufnehmen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe besteht aus gleichzeitigen Snapshots mehrerer Volumes, die konsistente Kopien einer Volumengruppe bereitstellen.

Sie können auch die Wartezeit angeben, die der Speichercontroller benötigt, um Snapshots konsistent zu gruppieren. Die verfügbaren Wartezeitzptionen sind **Dringend**, **Mittel** und **Entspannt**. Sie können die WAFL-Synchronisierung (Write Anywhere File Layout) auch während des konsistenten Gruppen-Snapshot-Vorgangs aktivieren oder deaktivieren. Die WAFL Synchronisierung verbessert die Leistung eines Konsistenzgruppen-Snapshots.

So verwaltet SnapCenter die Verwaltung von Protokoll- und Datensicherungen

SnapCenter verwaltet die Verwaltung von Protokoll- und Datensicherungen auf Speichersystem- und Dateisystemebene sowie innerhalb des SAP HANA-Sicherungskatalogs.

Die Snapshots auf dem Primär- oder Sekundärspeicher und die entsprechenden Einträge im SAP HANA-Katalog werden basierend auf den Aufbewahrungseinstellungen gelöscht. Beim Sichern und Löschen der Ressourcengruppe werden auch die SAP HANA-Katalogeinträge gelöscht.

Überlegungen zur Festlegung von Sicherungszeitplänen für die SAP HANA-Datenbank

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen)

Die Sicherungshäufigkeit, bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau wann Backups durchgeführt werden sollen)

Sicherungszeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird.

Anzahl der für SAP HANA-Datenbanken benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Sicherungsnamenskonventionen für Plug-in für SAP HANA-Datenbanken

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

`resourcegroupname_hostname_timestamp`

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen.

Beispiel: `customtext_resourcegroup_policy_hostname` oder `resourcegroup_hostname`. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

Wiederherstellungsstrategie für SAP HANA-Datenbanken

Definieren Sie eine Wiederherstellungsstrategie für SAP HANA-Ressourcen

Sie müssen vor der Wiederherstellung Ihrer Datenbank eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.

Schritte

1. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen
2. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken.
3. Entscheiden Sie sich für die Art der Wiederherstellungsvorgänge, die Sie durchführen möchten.

Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen. Sie können manuell hinzugefügte SAP HANA-Ressourcen nicht wiederherstellen.



Sie können manuell hinzugefügte SAP HANA-Ressourcen nicht wiederherstellen.

Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

Wiederherstellung auf Dateiebene

- Stellt Dateien aus Volumes, Qtrees oder Verzeichnissen wieder her
- Stellt nur die ausgewählten LUNs wieder her

Unterstützte Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken.

Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her
 - Um das gesamte Volume wiederherzustellen, sollte die Option **Volume Revert** ausgewählt werden.



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

Mandantendatenbank

- Stellt die Mandantendatenbank wieder her

Wenn die Option **Mandantendatenbank** ausgewählt ist, müssen für die Durchführung des Wiederherstellungsvorgangs externe HANA-Studio- oder HANA-Wiederherstellungsskripte von SnapCenter verwendet werden.

Arten von Wiederherstellungsvorgängen für automatisch erkannte SAP HANA-Datenbanken

SnapCenter unterstützt Volume-basiertes SnapRestore (VBSR), Single File SnapRestore und Connect-and-Copy-Wiederherstellungstypen für automatisch erkannte SAP HANA-Datenbanken.

Volume-basiertes SnapRestore (VBSR) wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn die für die Wiederherstellung ausgewählte Sicherung auf Versionen vor SnapCenter 4.3 erstellt wird und nur, wenn die Option **Ressource vollständig** ausgewählt ist
- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und die Option **Volume Revert** ausgewählt ist

Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und nur die Option **Complete Resource** ausgewählt ist

- Für Multitenant-Datenbankcontainer (MDC), wenn die für die Wiederherstellung ausgewählte Sicherung auf SnapCenter 4.3 erstellt wird und die Option **Tenant-Datenbank** ausgewählt ist
- Wenn das ausgewählte Backup von einem SnapMirror oder SnapVault Sekundärspeicherort stammt und die Option **Complete Resource** ausgewählt ist

Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn Backups auf Versionen vor SnapCenter 4.3 erstellt werden und nur, wenn die Option **Complete Resource** ausgewählt ist
- Wenn Backups in SnapCenter 4.3 erstellt werden und nur, wenn die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem SnapMirror oder SnapVault Sekundärspeicherort ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Eine auf Verbinden und Kopieren basierende Wiederherstellung wird in SAN-Umgebungen für das folgende Szenario durchgeführt:

- Für MDC, wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und die Option **Tenant Database** ausgewählt ist



Auf der Seite „Wiederherstellungsbereich“ sind die Optionen „Ressource vollständig“ und „Volume wiederherstellen“ verfügbar.

Für SAP HANA-Datenbanken unterstützte Arten von Wiederherstellungsvorgängen

Mit SnapCenter können Sie verschiedene Arten von Wiederherstellungsvorgängen für SAP HANA-Datenbanken durchführen.

- Wiederherstellen der Datenbank bis zum aktuellsten Stand
 - Wiederherstellen der Datenbank bis zu einem bestimmten Zeitpunkt
- Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.
- Wiederherstellen der Datenbank bis zu einer bestimmten Datensicherung

SnapCenter bietet auch die Option „Keine Wiederherstellung“ für SAP HANA-Datenbanken.

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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERINER 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.