



# **Backup-Strategie für SAP HANA- Datenbanken**

## **SnapCenter software**

NetApp  
November 06, 2025

# Inhalt

Backup-Strategie für SAP HANA-Datenbanken . . . . .	1
Definieren Sie eine Sicherungsstrategie für SAP HANA-Datenbanken . . . . .	1
Automatische Erkennung von Ressourcen auf Linux-Hosts . . . . .	1
Unterstützte Sicherungstypen . . . . .	2
Dateibasierte Sicherung . . . . .	2
Snapshot-Kopie-basierte Sicherung . . . . .	2
So verwendet das SnapCenter -Plug-in für die SAP HANA-Datenbank Snapshots der Konsistenzgruppe . . . . .	3
So verwaltet SnapCenter die Verwaltung von Protokoll- und Datensicherungen . . . . .	3
Überlegungen zur Festlegung von Sicherungszeitplänen für die SAP HANA-Datenbank . . . . .	3
Anzahl der für SAP HANA-Datenbanken benötigten Sicherungsaufträge . . . . .	4
Sicherungsnamenskonventionen für Plug-in für SAP HANA-Datenbanken . . . . .	4

# 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 Aufbewahrungsdauer 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 Wartezeitoptionen 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.

## 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER 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.