Schutz von SAP HANA Datenbanken

SnapCenter Software 4.5

NetApp
January 18, 2024

Inhalt

Schutz von SAP HANA Datenbanken . . . 1
SnapCenter Plug-in für SAP HANA Datenbanken . . . 1
Bereiten Sie sich auf die Installation des SnapCenter-Plug-ins für die SAP HANA-Datenbank vor . . . 14
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 35
Bereiten Sie sich auf die Datensicherung vor . . . 36
SAP HANA-Ressourcen sichern . . . 37
Wiederherstellung von SAP HANA Datenbanken . . . 64
Backups von SAP HANA Ressourcen klonen . . . 75

Schutz von SAP HANA Datenbanken

SnapCenter Plug-in für SAP HANA Datenbanken

SnapCenter-Plug-in für SAP HANA-Datenbank – Überblick

Das SnapCenter Plug-in für SAP HANA Database ist eine Host-seitige Komponente der NetApp SnapCenter Software, die ein applikationsgerechtes Datensicherungsmanagement für SAP HANA Datenbanken ermöglicht. Das Plug-in für SAP HANA Database automatisiert das Backup, Restore und Klonen von SAP HANA Datenbanken in der SnapCenter Umgebung.

SnapCenter unterstützt einzelne Container und mandantenfähige Datenbank-Container (MDC). Sie können das Plug-in für SAP HANA Datenbanken sowohl in Windows- als auch in Linux-Umgebungen verwenden. Das Plug-in, das nicht auf dem HANA-Datenbank-Host installiert ist, wird als zentrales Host-Plug-in bezeichnet. Das zentralisierte Host Plug-in kann mehrere HANA-Datenbanken über verschiedene Hosts hinweg managen.

Wenn das Plug-in für SAP HANA Datenbank installiert ist, kann SnapCenter mit NetApp SnapMirror Technologie verwendet werden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Mithilfe des Plug-ins in mit NetApp SnapVault Technologie lässt sich darüber hinaus eine Disk-to-Disk-Backup-Replizierung zur Einhaltung von Standards durchführen.

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

Wenn Sie das Plug-in für SAP HANA Datenbank in Ihrer Umgebung installieren, können Sie mit SnapCenter SAP HANA Datenbanken und deren Ressourcen sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Hinzufügen von Datenbanken:
- Backups erstellen.
- Restore aus Backups:
- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

SnapCenter Plug-in für SAP HANA Database Funktionen

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Zur Nutzung mit dem Plug-in für SAP HANA-Datenbank verwenden Sie die grafische Benutzeroberfläche von SnapCenter.

- **Einheitliche grafische Benutzeroberfläche**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore- und Klonvorgänge über

alle Plug-ins hinweg, die zentralisierte Berichterstellung, die Schnellübersicht über Dashboard-Ansichten, die Einrichtung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Jobs in allen Plug-ins.

- **Automatisierte zentrale Verwaltung**

  Sie können Backup-Vorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Unterbrechungsfreie NetApp Snapshot Kopie-Technologie**

  SnapCenter nutzt die NetApp Snapshot-Kopiertechnologie mit dem Plug-in für SAP HANA Datenbanken, um Ressourcen zu sichern.

Die Nutzung des Plug-ins für SAP HANA Database bietet darüber hinaus folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

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

- Erstellung platzsparender und zeitpunktgenauer Kopien von Ressourcen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

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

- Unterstützung der Snapshot-Kopie der Konsistenzgruppe (CG) von ONTAP im Rahmen der Erstellung von Backups
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshot Kopien konsolidiert, wenn Ressourcen eines einzelnen Hosts dasselbe Volume gemeinsam nutzen.

- Funktion zum Erstellen von Snapshot Kopien mithilfe externer Befehle.
- Unterstützung für dateibasierte Backups.
- Unterstützung für Linux LVM auf XFS-Dateisystem.

Storage-Typen, die vom SnapCenter Plug-in für SAP HANA Database unterstützt werden

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines (VMs). Sie müssen die Unterstützung Ihres Speichertyps überprüfen, bevor Sie das SnapCenter-Plug-in für SAP HANA Database installieren.

Maschine	Storage-Typ
Physische und virtuelle Server	FC-verbundene LUNs

Maschine	Storage-Typ
Physischer Server	ISCSI-verbundene LUNs
Physische und virtuelle Server	Volumes mit NFS-Anbindung

Mindestberechtigungen für ONTAP erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
Event Generate-AutoSupport-log
Job-Verlauf wird angezeigt Job beenden

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
lun
lun erstellen
lun löschen
lun Initiatorgruppe hinzufügen
lun-Initiatorgruppe wird erstellt
lun-Initiatorgruppe löschen
lun igroup umbenennen
lun-Initiatorgruppe wird angezeigt
lun Mapping Add-Reporting-Nodes
lun-Zuordnung erstellen
lun-Zuordnung löschen
lun Mapping remove-Reporting-Nodes
lun-Zuordnung wird angezeigt
lun ändern
lun-Verschiebung in Volume
lun ist offline
lun ist online
lun Persistent-Reservierung löschen
die lun-Größe wird geändert
lun seriell
lun anzeigen

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
SnapMirror Richtlinie Add-Rule änderungsregel für snapmirror Remove-Rule für snapmirror-Richtlinie snapmirror-Richtlinie anzeigen snapmirror Wiederherstellung snapmirror zeigen snapmirror Vorgeschichte snapmirror Update snapmirror Update-ls-Set snapmirror Listenziele
Version

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
Erstellung von Volume-Klonen
Klon von Volume anzeigen
Split-Start des Volume-Klons
Split-Stopp für Volume-Klon
Volume erstellen
Volume destroy
Erstellen eines Volume-Dateiklonen
Show-Disk-Nutzung für Volume-Dateien
Volume ist offline
Das Volume ist online
Volume-Änderung
Erstellen von Volume-qtree
Volume qtree löschen
Änderung des Volume-qtree
Volume-qtree anzeigen
Volume-Einschränkung
Volumen anzeigen
Erstellen von Volume-Snapshots
Volume Snapshot löschen
Ändern des Volume-Snapshots
Umbenennung von Volume-Snapshots
Wiederherstellung von Volume Snapshots
Restore-Datei für Volume Snapshots
Volume-Snapshot werden angezeigt
Volume-Aufhängung nicht verfügbar

All-Access-Befehle: Mindestberechtigungen erforderlich für ONTAP 8.2.*x* und höher
cifs von vserver
erstellung von cifs-Freigaben von vserver
cifs-Freigabe von vserver: Löschen
vserver cifs shadowcopy anzeigen
cifs-Freigabe von vserver wird angezeigt
vserver cifs zeigen
vserver Exportrichtlinie
Erstellung von vserver Exportrichtlinien
vserver: Löschen der Exportrichtlinie
Erstellung von vserver Export-Policy-Regel
vserver: Export-Policy-Regel anzeigen
vserver Export-Policy wird angezeigt
vserver iscsi
vserver iscsi-Verbindung wird angezeigt
vserver zeigen

Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.2.*x* und höher erforderlich
Netzwerkschnittstelle
Netzwerkschnittstelle wird angezeigt
vserver

Vorbereiten der Storage-Systeme für SnapMirror und SnapVault Replizierung für SAP HANA Datenbanken

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

> Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

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.

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

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Informationen zu Beziehungen zwischen Versionen und SnapMirror sowie deren Einrichtung finden Sie im "ONTAP-Dokumentation".

Backup-Strategie für SAP HANA Datenbanken

Backup-Strategie für SAP HANA Datenbanken definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre Ressourcen erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Über diese Aufgabe

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.
2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Entscheiden Sie, ob Sie eine Richtlinie auf Basis von Snapshot Kopien erstellen möchten, um applikationskonsistente Snapshot Kopien der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie die Integrität der Datenbank überprüfen möchten.
6. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
7. Legen Sie die Aufbewahrungsdauer für die Snapshot Kopien auf dem Quell-Storage-System und dem SnapMirror Ziel fest.
8. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Automatische Ermittlung von Ressourcen auf Linux-Host

Ressourcen sind SAP HANA Datenbanken und nicht-Daten-Volumes auf dem Linux-Host, die von SnapCenter gemanagt werden. Nach der Installation des SnapCenter-Plug-

ins für SAP HANA-Datenbank 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:

- Einzelne Container

  Nach der Installation oder dem Upgrade des Plug-ins werden die einzelnen Container-Ressourcen in einem zentralen Host-Plug-in als manuell zusätzliche Ressourcen fortgesetzt.

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

- Mandantenfähiger Datenbank-Container (MDC)

  Nach der Installation oder dem Upgrade des Plug-ins werden die MDC-Ressourcen auf einem zentralen Host-Plug-in als manuell hinzugefügte Ressource fortgesetzt.

  Nach dem Upgrade auf SnapCenter 4.3 müssen Sie weiterhin die MDC-Ressourcen auf dem zentralen Host-Plug-in manuell hinzufügen.

  Bei direkt in SnapCenter registrierten SAP HANA Linux-Hosts wird durch die Installation oder ein Upgrade des Plug-ins eine automatische Ermittlung der Ressourcen auf dem Host ausgelöst. 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 ermittelt und in SnapCenter registriert. Die neue Ressource befindet sich im Status gesperrt.

  Wenn sich beispielsweise in SnapCenter 4.2 die 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.

Der Data Protection Guide for SAP HANA Databases enthält weitere Informationen zur Zusammenarbeit mit der neuen MDC-Ressource auf einem SnapCenter-Plug-in-Host für Datensicherungsvorgänge

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

  Falls die oben genannten Ressourcen ermittelt werden, werden die Datensicherungsvorgänge von diesen Ressourcen nicht unterstützt.

- HANA Konfiguration für mehrere Hosts
- HANA System Replication
- Mehrere Instanzen auf demselben Host

Art der unterstützten Backups

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

Dateibasiertes Backup

Dateibasierte Backups bestätigen die Integrität der Datenbank. Sie können den dateibasierten Backup-Vorgang in bestimmten Intervallen planen. Es werden nur aktive Mandanten gesichert. Sie können dateibasierte Backups nicht aus SnapCenter wiederherstellen und klonen.

Backup auf Basis von Snapshot Kopien

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

Das SnapCenter Plug-in für SAP HANA Database verwendet Snapshot Kopien von Konsistenzgruppen

Sie können das Plug-in verwenden, um Snapshot Kopien von Konsistenzgruppen für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes beherbergen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe sind gleichzeitige Snapshot Kopien mehrerer Volumes und liefert konsistente Kopien einer Volume-Gruppe.

Sie können auch die Wartezeit für den Storage Controller angeben, um Snapshot Kopien konsistent zu gruppieren. Die verfügbaren Optionen für Wartezeiten sind **dringend**, **Medium** und **entspannt**. Sie können die Synchronisierung des Write Anywhere File Layout (WAFL) auch während eines konsistenten Snapshot Kopiervorgangs aktivieren oder deaktivieren. WAFL Sync verbessert die Performance von Snapshot Kopien von Konsistenzgruppen.

SnapCenter managt die allgemeine Ordnung und Sauberkeit von Protokoll- und Daten-Backups

SnapCenter managt die allgemeine Ordnung und Sauberkeit der Protokoll- und Daten-Backups auf den Ebenen des Storage-Systems und des Filesystems und innerhalb des SAP HANA Backup-Katalogs.

Die Snapshot-Kopien auf dem primären oder sekundären Storage und ihre entsprechenden Einträge im SAP HANA Katalog werden auf Grundlage der Aufbewahrungseinstellungen gelöscht. Die SAP HANA-Katalogeinträge werden auch beim Backup und beim Löschen von Ressourcengruppen gelöscht.

Überlegungen bei der Ermittlung von Backup-Zeitplänen für die SAP HANA Datenbank

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, die Service Level Agreement (SLA) und den Recovery Point Objective (RPO).

Backup-Zeitpläne haben zwei Teile:

- Backup-Häufigkeit (Häufigkeit der Durchführung von Backups)

  Die Backup-Häufigkeit, die auch als Zeitplantyp für einige Plug-ins bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau dann, wenn Backups durchgeführt werden sollen

Backup-Zeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird

Anzahl der für SAP HANA-Datenbanken erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Backup-Namenskonventionen für SAP HANA Datenbanken

Sie können entweder die standardmäßige Namenskonvention für Snapshot Kopien verwenden oder eine individuelle Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt einen Zeitstempel zu den Namen von Snapshot Kopien hinzu, der Ihnen hilft, zu identifizieren, wann die Kopien erstellt wurden.

Die Snapshot Kopie verwendet die folgende standardmäßige Namenskonvention:

```
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 Bedeutungen:

- *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 Namensformat für die Snapshot-Kopie angeben und Ressourcen oder Ressourcengruppen schützen, indem Sie **Verwenden Sie benutzerdefiniertes Namensformat für die Snapshot-Kopie** wählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Namen der Snapshot Kopie das Suffix mit dem Zeitstempel hinzugefügt.

Restore- und Recovery-Strategie für SAP HANA Datenbanken

Restore- und Recovery-Strategie für SAP HANA-Ressourcen definieren

Sie müssen eine Strategie definieren, bevor Sie Ihre Datenbank wiederherstellen und wiederherstellen, damit Restore- und Recovery-Vorgänge erfolgreich durchgeführt werden können.

Schritte

1. Legen Sie die Wiederherstellungsstrategien fest, die für manuell hinzugefügte SAP HANA-Ressourcen unterstützt werden

2. Legen Sie die Wiederherstellungsstrategien fest, die für automatisch erkannte SAP HANA-Datenbanken unterstützt werden
3. Geben Sie die Art der Recovery-Vorgänge an, die Sie ausführen möchten.

Arten von Wiederherstellungsstrategien werden für manuell hinzugefügte SAP HANA-Ressourcen unterstützt

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen. Manuell hinzugefügte SAP HANA-Ressourcen können nicht wiederhergestellt werden.

> Manuell hinzugefügte SAP HANA-Ressourcen können nicht wiederhergestellt werden.

Komplette Ressourcenwiederherstellung

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

> Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshot Kopien, die nach der zum Wiederherstellen ausgewählten Snapshot Kopie auf solchen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

Wiederherstellung auf Dateiebene

- Wiederherstellung von Dateien aus Volumes, qtrees oder Verzeichnissen
- Stellt nur die ausgewählten LUNs wieder her

Arten von Wiederherstellungsstrategien werden für automatisch erkannte SAP HANA-Datenbanken unterstützt

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

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her
  - Die Option **Volume revert** sollte ausgewählt werden, um das gesamte Volume wiederherzustellen.

> Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshot Kopien, die nach der zum Wiederherstellen ausgewählten Snapshot Kopie auf solchen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

Mandanten-Datenbank

- Stellt die Mandantendatenbank wieder her

Wenn die Option **Tenant Database** ausgewählt ist, müssen HANA Studio oder HANA Recovery Scripts außerhalb von SnapCenter verwendet werden, um den Recovery-Vorgang durchzuführen.

Arten von Wiederherstellungsvorgängen für automatisch erkannte SAP HANA-Datenbanken

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

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

- Wenn das für die Wiederherstellung ausgewählte Backup auf Versionen vor SnapCenter 4.3 durchgeführt wird, und nur, wenn die Option **Complete Resource**ausgewählt ist
- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und wenn 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 **vollständige Ressource** ausgewählt ist
- Für mandantenfähige Datenbank-Container (MDC), wenn das für die Wiederherstellung ausgewählte Backup auf SnapCenter 4.3 übernommen wird, und die Option **Tenant Database** ausgewählt ist
- Wenn der ausgewählte Backup von einem sekundären Standort SnapMirror oder SnapVault 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 dann, wenn die Option **Complete Resource** ausgewählt ist
- Wenn Backups in SnapCenter 4.3 erstellt werden und nur dann, wenn die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem sekundären Standort SnapMirror oder SnapVault ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Connect-and-Copy-Based Restore 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

> **Complete Resource**, **Volume Revert** und **Tenant Database** Optionen sind auf der Seite „Bereich wiederherstellen“ verfügbar.

Arten von Recovery-Vorgängen unterstützt für SAP HANA-Datenbanken

SnapCenter ermöglicht Ihnen die Durchführung verschiedener Recovery-Vorgänge für SAP HANA Datenbanken.

- Wiederherstellung der Datenbank im aktuellsten Zustand
- Wiederherstellung der Datenbank zu einem bestimmten Zeitpunkt

  Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.

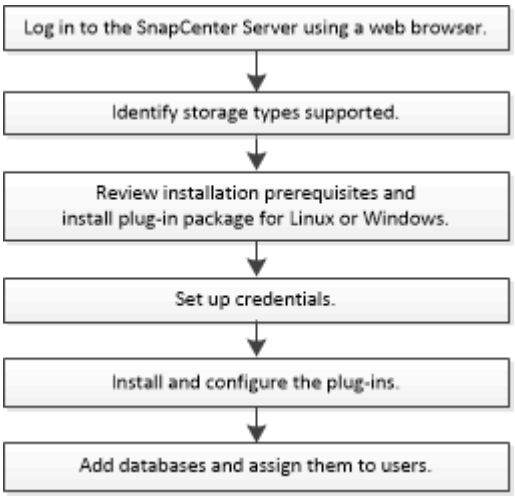
- Wiederherstellung der Datenbank in einem bestimmten Daten-Backup

SnapCenter bietet auch die Option „kein Recovery“ für SAP HANA Datenbanken.

Bereiten Sie sich auf die Installation des SnapCenter-Plug-ins für die SAP HANA-Datenbank vor

Installationsworkflow des SnapCenter Plug-ins für SAP HANA Database

Sie sollten das SnapCenter Plug-in für SAP HANA Database installieren und einrichten, wenn Sie SAP HANA Datenbanken schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter Plug-ins für SAP HANA Database

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Das SnapCenter Plug-in für SAP HANA Database ist sowohl in Windows als auch in Linux Umgebungen verfügbar.

- Sie müssen Java 1.8 64-bit auf Ihrem Host installiert haben.

  IBM Java wird nicht unterstützt.

- Sie müssen das interaktive Terminal (HDBSQL-Client) der SAP HANA-Datenbank auf dem Host installiert haben.
- Für Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „`LocalSystem`“ ausgeführt werden. Dies ist das Standardverhalten, wenn Plug-in für SAP HANA Database als Domänenadministrator installiert wird.
- Unter Windows sollten Benutzer-Speicherschlüssel als SYSTEMBENUTZER erstellt werden.

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört. Das SnapCenter Plug-in für Microsoft Windows wird standardmäßig mit dem SAP HANA Plug-in auf Windows Hosts implementiert.
- Für Linux-Host werden HDB Secure User Store-Schlüssel als HDBSQL OS-Benutzer aufgerufen.
- Der SnapCenter-Server sollte Zugriff auf den 8145-Port oder den benutzerdefinierten Port des Plug-ins für SAP HANA-Datenbank-Host haben.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Bei der Installation von Plug-in für SAP HANA-Datenbank auf einem Windows-Host wird das SnapCenter Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 1.8 64-bit auf Ihrem Windows-Host installiert haben.

  "Java-Downloads für alle Betriebssysteme"

  Der "Interoperabilitäts-Matrix-Tool" Enthält die neuesten Informationen zu Anforderungen.

Linux-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 1.8 64-bit auf Ihrem Linux-Host installiert haben.

  "Java-Downloads für alle Betriebssysteme"

  Der "Interoperabilitäts-Matrix-Tool" Enthält die neuesten Informationen zu Anforderungen.

- Für SAP HANA-Datenbanken, die auf einem Linux-Host ausgeführt werden und das Plug-in für SAP HANA Database installieren, wird das SnapCenter-Plug-in für UNIX automatisch installiert.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.5.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux

Bevor Sie das SnapCenter Plug-ins-Paket für Linux installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Host-Systems vertraut sein.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit der Datensicherungsvorgänge. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 1.8.x (64-Bit)Oracle Java und OpenJDK Varianten Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist. Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". .

Anmeldedaten für das SnapCenter-Plug-in für SAP HANA-Datenbank einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken oder Windows-Dateisystemen erstellen.

Über diese Aufgabe

- Linux-Hosts

  Sie müssen Anmeldedaten für die Installation von Plug-ins auf Linux-Hosts einrichten.

  Sie müssen die Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

  Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen zu erstellen, bevor Sie Hosts bereitstellen und Plug-ins installieren.

- Windows Hosts

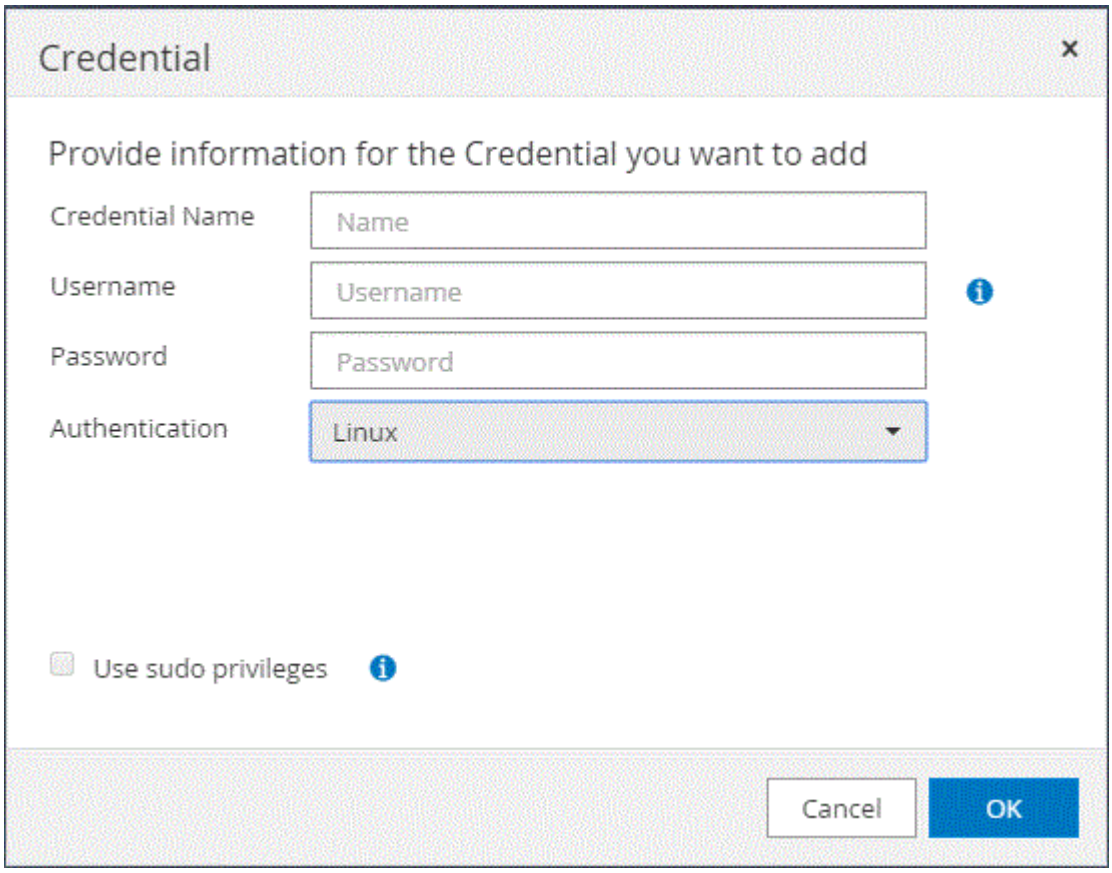
  Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.

  Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf **Credential**.
3. Klicken Sie Auf **Neu**.



4. Geben Sie auf der Seite **Credential** die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username* Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten. ⓘ Nur für Linux-Benutzer verfügbar.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite **Benutzer und Zugriff** die Pflege von Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2012 oder höher

Mit Windows Server 2012 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Was Sie brauchen

- Sie sollten einen Windows Server 2012 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2012 oder höher-Host haben, der Mitglied der Domain ist.

Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

   ```
    domainName\accountName$
   .. Fügen Sie der Gruppe Computerobjekte hinzu.
   .. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
   erstellen.
   ```

   Beispiel:

   ```
    New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
   -PrincipalsAllowedToRetrieveManagedPassword <group>
   -ServicePrincipalNames <SPN1,SPN2,…>
   .. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des
   Dienstkontos.
   ```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:
   a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Starten Sie den Host neu.

b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`

c. Überprüfen Sie Ihr gMSA-Konto, indem Sie folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`

5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter-Server angeben.

   SnapCenter-Server installiert die ausgewählten Plug-ins auf dem Host, und das angegebene gMSA wird während der Plug-in-Installation als Service-Login-Konto verwendet.

Das SnapCenter-Plug-in für SAP HANA Datenbanken installieren

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen Hosts über die Seite SnapCenter Add Host hinzufügen hinzufügen und dann die Plug-ins-Pakete installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und Plug-in-Pakete für einen einzelnen Host oder für ein Cluster installieren.

Was Sie brauchen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.

- Die Administrationsdokumentation enthält Informationen zum Verwalten von Hosts.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfiguration des Gruppenverwaltungsservice-Kontos unter Windows Server 2012 oder höher für SAP HANA"

Über diese Aufgabe

Sie können einen SnapCenter-Server nicht als Plug-in-Host zu einem anderen SnapCenter-Server hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite **Hosts** folgende Aktionen durch:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ aus: • Windows • Linux Das Plug-in für SAP HANA ist auf dem HDBSQL-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System installiert sein.
Host-Name	Geben Sie den Hostnamen der Kommunikation ein. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie müssen den HDBSQL-Client und den HDBUserStore auf diesem Host konfigurieren.

Für dieses Feld…	Tun Sie das…
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Installationspfad	Das Plug-in für SAP HANA ist auf dem HDBSQL-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System installiert sein. • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. Optional können Sie den Pfad anpassen. • Für das SnapCenter Plug-ins-Paket für Linux lautet der Standardpfad: /Opt/NetApp/snapcenter. Optional können Sie den Pfad anpassen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, der RAM, die PowerShell-Version, die .NET-Version, der Speicherort (für Windows-Plug-ins) und die Java-Version (für Linux-Plug-ins) werden anhand der Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\Programme\NetApp\SnapCenter WebApp aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.

   Wenn Sie in einem HA-Setup die Datei „Web.config“ aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und Senden**.

   In einer Cluster-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

   > Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Log-Dateien befinden sich unter /Custom_Location/snapcenter/logs.

Installieren Sie SnapCenter Plug-in-Pakete für Linux oder Windows auf mehreren Remote Hosts mithilfe von Cmdlets

Sie können die SnapCenter-Plug-in-Pakete für Linux oder Windows gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Was Sie brauchen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

   Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

   Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Installieren Sie das SnapCenter-Plug-in für SAP HANA-Datenbanken auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten das SnapCenter-Plug-in für SAP HANA-Datenbank über die SnapCenter-Benutzeroberfläche installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie das Plug-in für SAP HANA-Datenbank entweder im Konsolenmodus oder im Silent-Modus installieren, indem Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Was Sie brauchen

- Sie sollten das Plug-in für die SAP HANA-Datenbank auf jedem Linux-Host installieren, auf dem sich der HDBSQL-Client befindet.
- Der Linux-Host, auf dem Sie das SnapCenter-Plug-in für SAP HANA Database installieren, muss die Anforderungen der abhängigen Software, der Datenbank und des Betriebssystems erfüllen.

  Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu unterstützten Konfigurationen.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Das SnapCenter-Plug-in für SAP HANA-Datenbank ist Teil des SnapCenter Plug-ins-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins Paket für Linux installieren, sollten Sie bereits SnapCenter auf einem Windows-Host installiert haben.

Schritte

1. Kopieren Sie das SnapCenter Plug-ins-Paket für die Linux-Installationsdatei (snapcenter_linux_Host_Plugin.bin) aus C:\ProgramData\NetApp\SnapCenter\Paket-Repository auf den Host, auf dem Sie das Plug-in für SAP HANA-Datenbank installieren möchten.

   Sie können von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie die Installationsdatei kopiert haben.
3. Installieren Sie das Plug-in:
   `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT gibt den HTTPS-Kommunikationsport SMCore an.
   - -DSERVER_IP gibt die IP-Adresse des SnapCenter-Servers an.
   - -DSERVER_HTTPS_PORT gibt den HTTPS-Port des SnapCenter-Servers an.
   - -DUSER_INSTALL_dir gibt das Verzeichnis an, in dem das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
   - DINSTALL_LOG_NAME gibt den Namen der Protokolldatei an.

   ```
   /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
   -DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
   -DUSER_INSTALL_DIR=/opt
   -DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
   -DCHOSEN_FEATURE_LIST=CUSTOM
   ```

4. Bearbeiten Sie die Datei /<Installationsverzeichnis>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties und fügen SIE dann DEN Parameter PLUGINS_ENABLED = hana:3.0 hinzu.
5. Fügen Sie den Host mit dem Cmdlet "Add-Smhost" und den erforderlichen Parametern zum SnapCenter-Server hinzu.

   Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen Sie den Status der Installation des Plug-ins für SAP HANA

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Gehen Sie auf der Seite **Jobs** folgendermaßen vor, um die Liste so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden:
   a. Klicken Sie Auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

> Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster **Snap-ins** die Option **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster **Zertifikate Snap-in** die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

> Der Import des Zertifikats sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12, *.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „persönlich“.

Abrufen des Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   a. Doppelklicken Sie auf das Zertifikat.
   b. Klicken Sie im Dialogfeld Zertifikat auf die Registerkarte **Details**.
   c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter-Server und allen Plug-in-Hosts durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Beispiel:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Binden Sie das neu installierte Zertifikat an die Windows Host Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
   ```

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert appid="$guid"
   ```

   Beispiel:

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Konfigurieren des CA-Zertifikats für den SnapCenter-SAP HANA-Plug-ins-Service auf dem Linux-Host

Sie sollten das Passwort des benutzerdefinierten Plug-ins Keystore und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für den benutzerdefinierten Plug-ins Trust-Store konfigurieren und das CA-signierte Schlüsselpaar auf benutzerdefinierte Plug-ins Trust-Store mit SnapCenter Custom Plug-ins Service konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Benutzerdefinierte Plug-ins verwenden die Datei 'keystore.jks', die sich unter */opt/NetApp/snapcenter/scc/etc* sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können benutzerdefinierte Plug-in Schlüsselspeicher Standardpasswort aus benutzerdefinierten Plug-in Agent Eigenschaftsdatei abrufen.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im
   Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher
   verwendet wird:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

> Das Kennwort für den benutzerdefinierten Plug-in-Schlüsselspeicher und für alle zugeordneten Alias-Passwörter des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel als benutzerdefinierten Plug-in-Vertrauensspeicher konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in keystore: /Opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder
   Zwischenzertifikate in einen benutzerdefinierten Plug-in Trust-Store
   konfiguriert haben.
   ```

> Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher

Sie sollten das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-in Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in keystore /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das benutzerdefinierte Standard-Plug-in-Schlüsselspeicher-Passwort ist der Wert der SCHLÜSSELDATEI KEYSTORE_PASS in agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Wenn der Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen enthält („*",","), ändern Sie den Alias-Namen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
agent.properties.
```

Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

8. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins

Über diese Aufgabe

- Benutzerdefinierte SnapCenter-Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter Custom Plug-ins ist ' opt/NetApp/snapcenter/scc/etc/crl'.

Schritte

1. Sie können das Standardverzeichnis in der Datei agent.properties mit dem Schlüssel CRL_PATH ändern und aktualisieren.

   Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Konfigurieren des CA-Zertifikats für den SnapCenter-SAP HANA-Plug-ins-Service auf dem Windows-Host

Sie sollten das Passwort des benutzerdefinierten Plug-ins Keystore und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für den benutzerdefinierten Plug-ins Trust-Store konfigurieren und das CA-signierte Schlüsselpaar auf benutzerdefinierte Plug-ins Trust-Store mit SnapCenter Custom Plug-ins Service konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Benutzerdefinierte Plug-ins verwenden die Datei *keystore.jks*, die sich unter *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* befindet, sowohl als Vertrauensspeicher als auch als Schlüsselspeicher.

Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können benutzerdefinierte Plug-in Schlüsselspeicher Standardpasswort aus benutzerdefinierten Plug-in Agent Eigenschaftsdatei abrufen.

   Es ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

   > Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

   C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

4. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

   > Das Kennwort für den benutzerdefinierten Plug-in-Schlüsselspeicher und für alle zugeordneten Alias-Passwörter des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel als benutzerdefinierten Plug-in-Vertrauensspeicher konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in Schlüsselspeicher *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

   Keytool -Import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder Zwischenzertifikate in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

   > Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher

Sie sollten das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-in Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in Schlüsselspeicher *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu.

   Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

   Keytool -list -V -keystore keystore.jks

6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das benutzerdefinierte Standard-Plug-in-Schlüsselspeicher-Passwort ist der Wert der SCHLÜSSELDATEI KEYSTORE_PASS in agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

9. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins

Über diese Aufgabe

- Informationen zum Herunterladen der neuesten CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten im SnapCenter CA-Zertifikat".
- Benutzerdefinierte SnapCenter-Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für benutzerdefinierte SnapCenter Plug-ins ist *'C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\crl'*.

Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* mit dem Schlüssel CRL_PATH ändern und aktualisieren.

2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Was Sie brauchen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nach Ihrer Beendigung

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

Wenn Ihre Datenbanken auf Virtual Machines (VMs) gespeichert sind oder VMs und Datastores geschützt werden sollen, müssen Sie das SnapCenter Plug-in für die virtuelle Appliance VMware vSphere implementieren.

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

Informationen zur Konfiguration des CA-Zertifikats mit dem SnapCenter-Plug-in für VMware vSphere finden Sie unter "Erstellen oder importieren Sie ein SSL-Zertifikat".

Konfigurieren Sie die CRL-Datei

Das SnapCenter Plug-in für VMware vSphere sucht die CRL-Dateien in einem vorkonfigurierten Verzeichnis. Das Standardverzeichnis der CRL-Dateien für das SnapCenter Plug-in für VMware vSphere ist */opt/netapp/config/crl*.

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Bereiten Sie sich auf die Datensicherung vor

Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für SAP HANA-Datenbanken

Bevor Sie das SnapCenter-Plug-in für die SAP HANA-Datenbank verwenden, muss der SnapCenter-Administrator den SnapCenter-Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten erstellen.
- Installieren Sie Java 1.7 oder Java 1.8 auf Ihrem Linux- oder Windows-Host.

  Sie müssen den Java-Pfad in der Umgebungspfadvariable des Host-Rechners festlegen.

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.
- Installieren Sie den HDBSQL-Client auf dem Host, auf dem Sie das Plug-in für SAP HANA-Datenbank installieren.

  Konfigurieren Sie die Benutzerspeicherschlüssel für die SAP HANA-Knoten, die Sie über diesen Host verwalten möchten.

- Wenn Sie ein SAP HANA-Datenbankbenutzerkonto verwenden, stellen Sie für die SAP HANA-Datenbank 2.0SPS05 sicher, dass Sie über die folgenden Berechtigungen zum Durchführen von Backup-, Wiederherstellungs- und Klonvorgängen im SnapCenter-Server verfügen:
  - Backup-Admin
  - Katalog gelesen
  - Datenbank-Backup-Administrator
  - Operator für Datenbank-Wiederherstellung

Verwendung von Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SAP HANA Datenbanken

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind typischerweise SAP HANA Datenbanken, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter-Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

  Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, Replizierung, Skripte und andere Eigenschaften von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

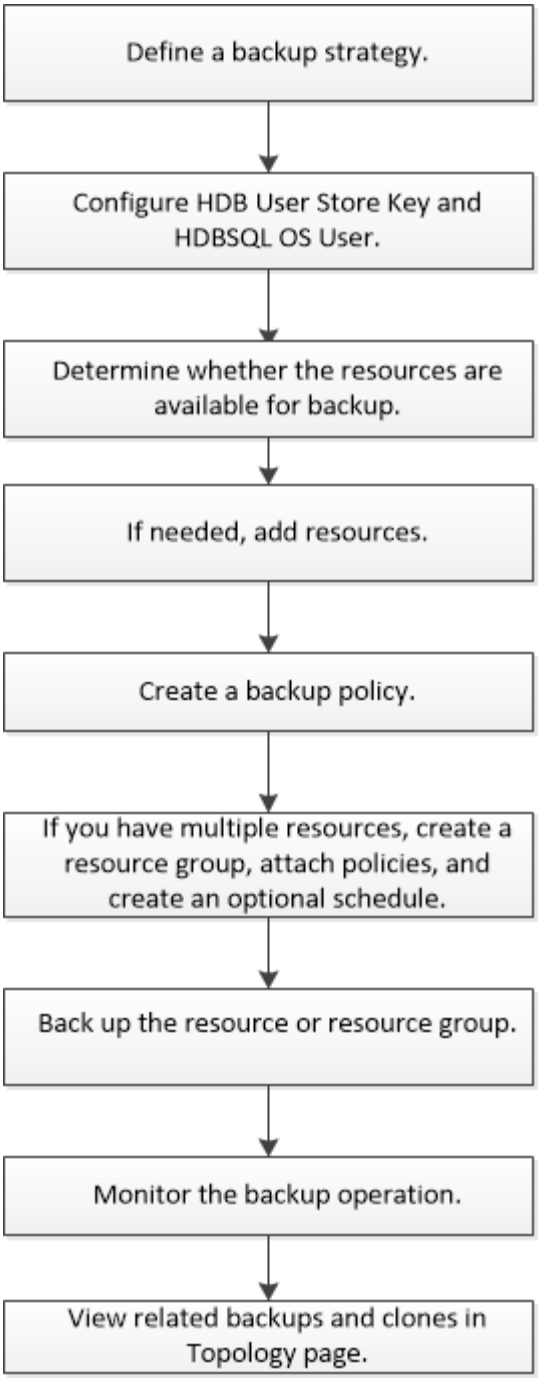
Stellen Sie sich eine Ressourcengruppe vor, die definiert, was Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Richtlinie, die definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts umfasst. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein vollständiges Backup durchführen.

SAP HANA-Ressourcen sichern

SAP HANA-Ressourcen sichern

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Datenbanken, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets.https://library.netapp.com/ecm/ecm_download_file/ECMLP2877143["SnapCenter Software Cmdlet Referenzhandbuch"^].

Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank

Sie müssen den HDB-Benutzerspeicherschlüssel und den HDBSQL OS-Benutzer konfigurieren, um Datenschutzvorgänge in SAP HANA-Datenbanken durchzuführen.

Was Sie brauchen

- Wenn in der SAP HANA-Datenbank nicht der HDB Secure User Store Key und der HDB SQL OS User konfiguriert sind, wird nur für die automatisch erkannten Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS Benutzer so konfigurieren, dass sie die Datenbank schützen oder einer Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.
- Sie müssen HDB SQL OS User konfigurieren, um auf die Systemdatenbank zugreifen zu können. Wenn HDB SQL OS User für den Zugriff auf nur die Mandantendatenbank konfiguriert ist, schlägt der Erkennungsvorgang fehl.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann SnapCenter-Plug-in für SAP HANA-Datenbank aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** den Ressourcentyp aus der Liste **Ansicht** aus.
3. (Optional) Klicken Sie Auf Und wählen Sie den Hostnamen aus.

   Sie können dann auf klicken Um den Filterbereich zu schließen.
4. Wählen Sie die Datenbank aus, und klicken Sie dann auf **Datenbank konfigurieren**.
5. Geben Sie im Abschnitt Datenbankeinstellungen konfigurieren den HDB-Schlüssel für sicheren Benutzerspeicher ein.

   Der Plug-in-Hostname wird angezeigt und HDB SQL OS User wird automatisch in <sid>ADM eingetragen.
6. Klicken Sie auf **OK**.

Sie können die Datenbankkonfiguration auf der Seite Topology ändern.

Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor

Automatische Erkennung von Datenbanken

Ressourcen sind SAP HANA Datenbanken und nicht-Daten-Volumes auf dem Linux-Host, die von SnapCenter gemanagt werden. Diese Ressourcen können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge durchzuführen, nachdem die verfügbaren SAP HANA Datenbanken ermittelt wurden.

Was Sie brauchen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. die Installation des SnapCenter-Servers, das Hinzufügen des HDB-Benutzerspeicherschlüssels, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS-Benutzer auf dem Linux-Host konfiguriert haben.

    - Sie müssen den HDB-Benutzerspeicherschlüssel mit dem SID-Adm-Benutzer konfigurieren. Für HANA-Systeme mit A22 als SID muss beispielsweise der HDB User Store Key mit a22adm konfiguriert werden.
- Das SnapCenter Plug-in für SAP HANA Database unterstützt nicht das automatische Auffinden der Ressourcen in virtuellen RDM/VMDK-Umgebungen. Sie müssen Storage-Informationen für virtuelle Umgebungen bereitstellen und gleichzeitig Datenbanken manuell hinzufügen.

Über diese Aufgabe

Nach der Installation des Plug-ins werden alle Ressourcen auf diesem Linux-Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Die automatisch ermittelten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für SAP HANA aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** den Ressourcentyp aus der Liste Ansicht aus.
3. (Optional) Klicken Sie Auf , und wählen Sie dann den Hostnamen aus.

   Sie können dann auf * klicken * Zum Schließen des Filterfensters.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, wird in der Spalte Status insgesamt nicht geschützt angezeigt.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn kein Backup-Vorgang durchgeführt wird, wird in der Spalte Gesamtstatus der Eintrag Backup Not Run angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

> Wenn in der SAP HANA-Datenbank kein HDB-sicherer Benutzerspeicherschlüssel konfiguriert ist, wird neben der Ressource ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.

Nach Ihrer Beendigung

Sie müssen den HDB Secure User Store Key und den HDBSQL OS User so konfigurieren, dass sie die Datenbank schützen oder zur Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

Mandantenfähige Datenbank-Container werden für die Datensicherung vorbereitet

Bei direkt in SnapCenter registrierten SAP HANA Hosts wird das Installieren oder Upgrade des SnapCenter Plug-ins für SAP HANA Database eine automatische Ermittlung der Ressourcen auf dem Host auslösen. Nach der Installation oder dem Upgrade des Plug-ins werden für alle MDC-Ressourcen (Multi-Tenant-Datenbank-Container), 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 Status „`gesperrt`“.

Über diese Aufgabe

Wenn sich beispielsweise in SnapCenter 4.2 die 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 Backups, die mit der Ressource von SnapCenter 4.2 und älteren Versionen verbunden sind, müssen bis zum Ablauf der Aufbewahrungsfrist aufbewahrt werden. Nach Ablauf des Aufbewahrungszeitraums können Sie die alte MDC-Ressource löschen und die neue automatisch erkannte MDC-Ressource weiterhin verwalten.

`Old MDC resource` Ist die MDC-Ressource für einen Plug-in-Host, der manuell in SnapCenter 4.2 oder früheren Versionen hinzugefügt wurde.

Führen Sie die folgenden Schritte durch, um die in SnapCenter 4.3 entdeckte neue Ressource für Datensicherungsvorgänge zu verwenden:

Schritte

1. Wählen Sie auf der Seite **Ressourcen** die alte MDC-Ressource mit Backups aus, die der früheren Version von SnapCenter hinzugefügt wurden, und legen Sie sie auf der Topologieseite in den „`maintute Mode`“.

   Wenn die Ressource Teil einer Ressourcengruppe ist, legen Sie die Ressourcengruppe in den „`mBetriebszustand`“.

2. Konfigurieren Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie die neue Ressource auf der Seite Ressourcen auswählen.

   „`Neue MDC-Ressource`“ ist die neu entdeckte MDC-Ressource, die erkannt wurde, nachdem der SnapCenter-Server und der Plug-in-Host auf 4.3 aktualisiert wurden. Die neue MDC-Ressource kann als Ressource mit demselben SID wie die alte MDC-Ressource, für einen bestimmten Host und mit einem roten Vorhängeschloss-Symbol daneben auf der Seite Ressourcen identifiziert werden.

3. Schützen Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie Schutzrichtlinien, Zeitpläne und Benachrichtigungseinstellungen auswählen.
4. Löschen Sie die Backups, die in SnapCenter 4.2 oder früheren Versionen basierend auf den Aufbewahrungseinstellungen erstellt wurden.
5. Löschen Sie die Ressourcengruppe auf der Seite Topologie.
6. Löschen Sie die alte MDC-Ressource von der Seite Ressourcen.

   Beispiel: Wenn die Aufbewahrungsdauer der primären Snapshot Kopien 7 Tage beträgt und die

Aufbewahrung von sekundären Snapshot Kopien 45 Tage beträgt, nach 45 Tagen abgeschlossen sind und nachdem alle Backups gelöscht wurden, müssen Sie die Ressourcengruppe und die alte MDC-Ressource löschen.

Weitere Informationen

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

"Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an"

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

Automatische Erkennung wird für bestimmte HANA-Instanzen nicht unterstützt. Sie müssen diese Ressourcen manuell hinzufügen.

Was Sie brauchen

Sie müssen Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen des HDB-Benutzerspeicherschlüssels abgeschlossen haben.

Über diese Aufgabe

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

> Falls die oben genannten Ressourcen ermittelt werden, werden die Datensicherungsvorgänge von diesen Ressourcen nicht unterstützt.

- HANA Konfiguration für mehrere Hosts
- HANA System Replication
- Mehrere Instanzen auf demselben Host

Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter-Plug-in für SAP HANA-Datenbank aus der Dropdown-Liste aus und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite **Ressourcen** auf **SAP HANA-Datenbank hinzufügen**.
3. Führen Sie auf der Seite **Ressourcendetails angeben** die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Ressourcentyp	Geben Sie den Ressourcentyp ein. Ressourcentypen sind Single-Container, Multitenant Database Container (MDC) und Non-Data-Volume.

Für dieses Feld…	Tun Sie das…
HANA-Systemname	Geben Sie den beschreibenden SAP HANA-Systemnamen ein. Diese Option ist nur verfügbar, wenn Sie einzelne Container- oder MDC-Ressourcentypen ausgewählt haben.
SID	Geben Sie die System-ID (SID) ein. Das installierte SAP HANA System wird durch eine einzige SID identifiziert.
Plug-in-Host	Wählen Sie den Plug-in-Host aus.
HDB Secure User Store Keys	Geben Sie den Schlüssel für die Verbindung zum SAP HANA-System ein. Der Schlüssel enthält die Anmeldeinformationen, um eine Verbindung zur Datenbank herzustellen.
HDBSQL OS-Benutzer	Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist. Für Windows ist es erforderlich, dass der HDBSQL OS-Benutzer der SYSTEMBENUTZER ist. Daher müssen Sie den HDB Secure User Store Key für den SYSTEMBENUTZER konfigurieren.

4. Wählen Sie auf der Seite * Storage Footprint* ein Speichersystem aus, und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Speichern**.

   Optional: Klicken Sie auf das Symbol + Symbol, um weitere Volumes, LUNs und qtrees von anderen Speichersystemen hinzuzufügen.

5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Datenbanken werden zusammen mit Informationen wie SID, Plugin-Host, zugehörigen Ressourcengruppen und Richtlinien sowie Gesamtstatus angezeigt

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie den Benutzern die Ressourcen zuweisen. Auf diese Weise können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

"Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"

Nach dem Hinzufügen der Datenbanken können Sie die Details der SAP HANA-Datenbank ändern.

Folgendes kann nicht geändert werden, wenn der SAP HANA-Mitarbeiter Backups zugeordnet sind:

- Mandantenfähige Datenbank-Container (MDC): SID- oder HDBSQL Client (Plug-in)-Host
- Einzelner Container: SID- oder HDBSQL-Client (Plug-in)-Host
- Kein Datenvolumen: Ressourcenname, zugehöriger SID oder Plug-in-Host

Backup-Richtlinien für SAP HANA Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden, müssen Sie eine Backup-Richtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Was Sie brauchen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen zur Definition einer Datensicherungsstrategie für SAP HANA Datenbanken finden Sie in den Informationen.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das Hinzufügen von Ressourcen ausführen.
- Der SnapCenter Administrator muss Ihnen die SVMs für die Quell- und Ziel-Volumes zuweisen, falls Sie Snapshot Kopien in eine Spiegelung oder einen Vault replizieren.

  Außerdem können Sie in der Richtlinie Replizierungs-, Skript- und Applikationseinstellungen festlegen. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Schritte

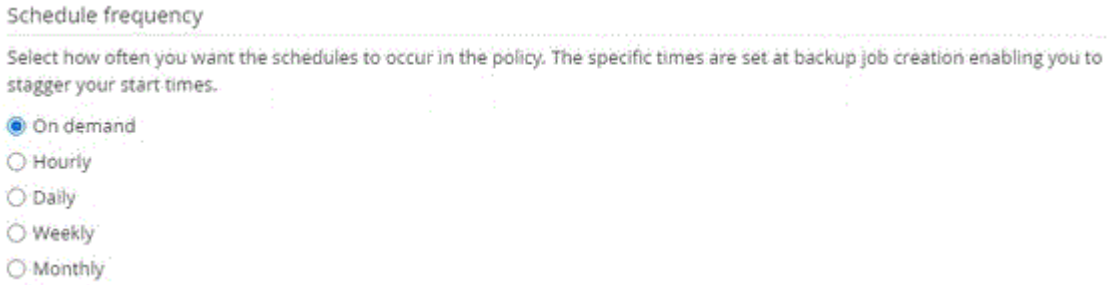
1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf **Richtlinien**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite **Name** den Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite **Einstellungen** die folgenden Schritte aus:

   - Wählen Sie den Sicherungstyp:

Ihr Ziel ist	Tun Sie das…
Führen Sie eine Integritätsprüfung der Datenbank durch	Wählen Sie * File-Based Backup* Aus. Es werden nur aktive Mandanten gesichert.
Erstellen Sie mit Snapshot-Kopiertechnologie ein Backup	Wählen Sie **Snapshot-Basiert** Aus.

   - Geben Sie den Terminplantyp an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien und Backup-Häufigkeit verwenden, aber auch die Möglichkeit haben, den einzelnen Richtlinien unterschiedliche Backup-Zeitpläne zuzuweisen.



Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

  Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.

6. Geben Sie auf der Seite **Retention** die Aufbewahrungseinstellungen für den Backup-Typ und den auf der Seite Backup-Typ ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…
Aufbewahrung einer bestimmten Anzahl von Snapshot Kopien	Wählen Sie **Gesamtanzahl der zu behenden Snapshot-Kopien** aus, und geben Sie dann die Anzahl der Snapshot-Kopien an, die beibehalten werden sollen. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Wenn Sie Snapshot Backups auf Basis von Kopien aktivieren SnapVault möchten, müssen Sie die Aufbewahrungsanzahl auf 2 oder höher festlegen. Wenn Sie die Aufbewahrungsanzahl auf 1 festlegen, kann der Aufbewahrungsvorgang möglicherweise fehlschlagen, da die erste Snapshot Kopie die Referenzkopie für die SnapVault-Beziehung ist, bis eine neuere Snapshot Kopie auf das Ziel repliziert wird.
Behalten Sie die Snapshot Kopien für eine bestimmte Anzahl von Tagen bei	Wählen Sie **Snapshot Kopien behalten für** aus, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshot Kopien behalten möchten, bevor Sie sie löschen.

7. Geben Sie für Snapshot-Kopie-basierte Backups die Replikationseinstellungen auf der Seite **Replikation** an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Wenn die Sicherungsbeziehung in ONTAP vom Typ Mirror und Vault beträgt und wenn Sie nur diese Option auswählen, wird die auf dem primären Volume erstellte Snapshot Kopie nicht an das Ziel übertragen, sondern dort aufgeführt. Wenn diese Snapshot Kopie aus dem Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird der sekundäre Speicherort für die ausgewählte Fehlermeldung „vaulted/mirrored Backup“ angezeigt.
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen.
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Abhängig von dem ausgewählten Etikett der Snapshot Kopie wendet ONTAP die Aufbewahrungsrichtlinie für sekundäre Snapshot Kopien an, die mit dem Etikett übereinstimmt. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Anzahl der Wiederholversuche	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um zu vermeiden, dass die maximale Anzahl an Snapshot Kopien auf dem sekundären Storage erreicht wird.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf der Seite **Ressourcen** auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite **Name** die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot Kopie verwenden möchten. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.

4. Wählen Sie auf der Seite **Ressourcen** einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den

rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.

6. Gehen Sie auf der Seite **Anwendungseinstellungen** wie folgt vor:

   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der Snapshot-Vorgang der Konsistenzgruppe abgeschlossen ist	Wählen Sie **dringendst**, **Medium** oder **relaxed** aus, um die Wartezeit zum Abschluss des Snapshot-Kopiervorgangs anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+

   a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die vor- und Post-Befehle für quiesce, Snapshot copy und unquiesce Operations ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

   b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die für alle Datenschutzvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
ARCHIVE_LOG_DIR	Change_info_Directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüsselwerterpaare werden für SAP HANA Linux-Plug-in-Systeme unterstützt und nicht für SAP HANA-Datenbanken unterstützt, die als zentrales Windows-Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot-Kopie-Tool**, um das Tool zum Erstellen von Snapshot-Kopien auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu nutzen und das Filesystem in einen konsistenten Zustand zu versetzen, bevor eine Snapshot Kopie erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus. Diese Option ist für das SnapCenter-Plug-in für SAP HANA Database nicht verfügbar.

Ihre Situation	Dann…
SnapCenter zum Erstellen einer Snapshot Kopie auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um eine Snapshot Kopie zu erstellen.

7. Führen Sie auf der Seite **Richtlinien** die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

   Sie können eine Richtlinie auch erstellen, indem Sie auf * klicken + *.

   Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

   b. Klicken Sie in der Spalte Zeitplan konfigurieren auf + Für die Richtlinie, die Sie konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

   Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

   Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

SAP HANA Datenbanken sichern

Wenn eine Ressource noch nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Was Sie brauchen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

- Stellen Sie beim Backup-Vorgang auf Basis von Snapshot Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Wenn Sie ein dateibasiertes Backup erstellen möchten, wenn eine oder mehrere Mandanten-Datenbanken nicht verfügbar sind, setzen Sie DEN PARAMETER ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT in der HANA-Eigenschaftendatei unter Verwendung des Cmdlet Set-SmConfigSettings auf **JA**.

  Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können, und deren Beschreibungen können durch Ausführen von Get-Help *Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch"

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Filtern Sie auf der Seite **Ressource** die Ressourcen aus der Dropdown-Liste **Ansicht** nach Ressourcentyp.

   Klicken Sie Auf , und wählen Sie dann den Host-Namen und den Ressourcentyp, um die Ressourcen zu filtern. Sie können dann auf klicken Um den Filterbereich zu schließen.
3. Klicken Sie auf die Ressource, die Sie sichern möchten.
4. Wählen Sie auf der Seite **Ressource Benutzerdefiniertes Namensformat für Snapshot Copy** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot-Kopie verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.
5. Gehen Sie auf der Seite **Anwendungseinstellungen** wie folgt vor:
   - Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der „Consistency Group Snapshot“-Vorgang abgeschlossen ist	Wählen Sie **dringendst**, oder **Medium**, oder **relaxed** aus, um die Wartezeit bis zum Abschluss der Snapshot-Kopie anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   - Klicken Sie auf den Pfeil **Scripts**, um vor- und Post-Befehle für quiesce, Snapshot copy und unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

- Klicken Sie auf den Pfeil **Custom Configurations**und geben Sie dann die für alle Jobs mit dieser Ressource erforderlichen benutzerdefinierten Wertpaare ein.
- Klicken Sie auf den Pfeil **Snapshot-Kopie-Tool**, um das Tool zum Erstellen von Snapshot-Kopien auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen einer Snapshot Kopie auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter verwendet das Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und anschließend eine Snapshot Kopie zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Geben Sie den Befehl ein, um eine Snapshot Kopie zu erstellen	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um eine Snapshot Kopie zu erstellen.

6. Führen Sie auf der Seite **Richtlinien** die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

   Sie können eine Richtlinie auch erstellen, indem Sie auf * klicken + *.

   Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken Sie Auf + In der Spalte Zeitplan konfigurieren für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

   Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

7. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

9. Klicken Sie auf **Jetzt sichern**.
10. Führen Sie auf der Seite **Backup** die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

       Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

    b. Klicken Sie Auf **Backup**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
    - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung erkennen.

      Weitere Informationen finden Sie unter: "SnapMirror oder SnapVault-Beziehung kann nach MetroCluster Failover nicht erkannt werden"

    - Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java Heap-Größe für das SnapCenter-Plug-in für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

      Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei */opt/netapp/init_scripts/scvservice*. In diesem Skript startet der Befehl *do_Start method* den SnapCenter VMware Plug-in-Dienst. Aktualisieren Sie diesen Befehl auf Folgendes: *Java -jar -Xmx8192M -Xms4096M*

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Was Sie brauchen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Über diese Aufgabe

Sie können eine Ressourcengruppe nach Bedarf auf der Seite **Ressourcen** sichern. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe entweder durch Eingabe des Ressourcengruppennamens in das Suchfeld oder durch Klicken durchsuchen , Und dann das Tag auswählen. Sie können dann auf klicken Um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite Ressourcengruppen die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Erstellen einer Storage-Systemverbindung und einer Zertifizierung mit PowerShell cmdlets für SAP HANA Datenbank

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um SAP HANA Datenbanken zu sichern, wiederherzustellen oder zu klonen.

Was Sie brauchen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt

werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mit dem Cmdlet Open-SmConnection.

```
PS C:\> Open-SmStorageConnection
```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel wird das Erstellen einer neuen Anmeldeinformationen namens FinanceAdmin mit Windows-Anmeldeinformationen angezeigt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Fügen Sie den SAP HANA-Kommunikationshost dem SnapCenter-Server hinzu.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Installieren Sie das Paket und das SnapCenter-Plug-in für SAP HANA-Datenbank auf dem Host.

   Für Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

   Für Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Legen Sie den Pfad zum HDBSQL-Client fest.

   Für Windows:

   ```
   PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
   hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
   Files\sap\hdbclient\hdbsql.exe"}
   ```

   Für Linux:

   ```
   Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
   -PluginCode hana -configSettings
   @{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
   ```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Sichern Sie Datenbanken mit PowerShell Cmdlets

Das Sichern einer Datenbank umfasst die Einrichtung einer Verbindung mit dem SnapCenter-Server, das Hinzufügen von Ressourcen, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppen und das Sichern von Ressourcen.

Was Sie brauchen

- Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.
- Sie müssen die Speichersystemverbindung hinzugefügt und Anmeldedaten erstellt haben.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
   ```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Mit dem Cmdlet "Add-SmResources" können Sie Ressourcen hinzufügen.

   Dieses Beispiel zeigt, wie eine SAP HANA-Datenbank des SingleContainer-Typs hinzugefügt wird:

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"})
-SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys 'HS10'
-osdbuser 'h10adm' -filebackupprefix 'H10_'
```

In diesem Beispiel wird das Hinzufügen einer SAP HANA-Datenbank mit MultipleContainers-Typ beschrieben:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType MultipleContainers
-StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.netapp.
com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType 'MultiTenant'
```

Dieses Beispiel zeigt, wie Sie eine Ressource erstellen, die nicht auf dem Datenvolumen ist:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   In diesem Beispiel wird eine Backup-Richtlinie für ein auf Snapshot Kopien basierendes Backup erstellt:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
-PluginPolicyType hana -BackupType SnapShotBasedBackup
```

   In diesem Beispiel wird eine Backup-Richtlinie für ein dateibasiertes Backup erstellt:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.

   Dieses Beispiel schützt eine einzelne Container-Ressource:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description test
-usesnapcenterwithoutfilesystemconsistency
```

Dieses Beispiel schützt eine Ressource mit mehreren Containern:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

In diesem Beispiel wird eine neue Ressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Dieses Beispiel erstellt eine Ressourcengruppe ohne Daten-Volume:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDataVolume\
S10\NonDataVolume";"PluginName"="hana"}) -Policies hanaprimary
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   Dieses Beispiel sichert eine geschützte Ressource:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"} -Policy
hana_Filebased
```

6. Überwachen Sie den Job-Status (ausgeführt, abgeschlossen oder fehlgeschlagen) mit dem Cmdlet "Get-smJobSummaryReport".

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Überwachen Sie die Details zu Backup-Jobs wie Backup-ID, Backup-Name zum Wiederherstellen oder Klonen mit dem Cmdlet "Get-SmBackupReport".

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Monitoring von Backup-Vorgängen

Monitoring von Backup-Vorgängen bei SAP HANA Datenbanken

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie Auf Filtern der Liste, sodass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   > Der Status des Backupjobs wird zwar angezeigt Wenn Sie auf die Jobdetails klicken, wird möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Backup-Vorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite **Jobdetails** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen von Datensicherungsvorgängen in SAP HANA-Datenbanken im Bereich „Activity“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt. Wenn Sie Plug-in für SQL Server oder Plug-in für Exchange Server verwenden,

werden im Aktivitätsbereich auch Informationen über den erneuten Seeding angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie Auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt.

   Wenn Sie auf einen der Vorgänge klicken, werden die Arbeitsdetails auf der Seite Jobdetails aufgeführt.

Abbrechen der Backup-Vorgänge für SAP HANA

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Klicken Sie nach dem Starten des Backup-Vorgangs auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

- Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapMirror Technologie auf dem sekundären Storage gespiegelt werden.
- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault Technologie auf dem sekundären Storage repliziert werden.

  Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Auf der Seite **Topologie** sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Lesen Sie die **Übersichtskarte** durch, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

Im Abschnitt **Summary Card** wird die Gesamtzahl der dateibasierten Backups, Snapshot-Kopien-Backups und Klone angezeigt.

Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

5. Klicken Sie in der Ansicht **Kopien verwalten** auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf die Datensicherungssymbole, um Restore-, Klon- und Löschvorgänge durchzuführen.

   Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

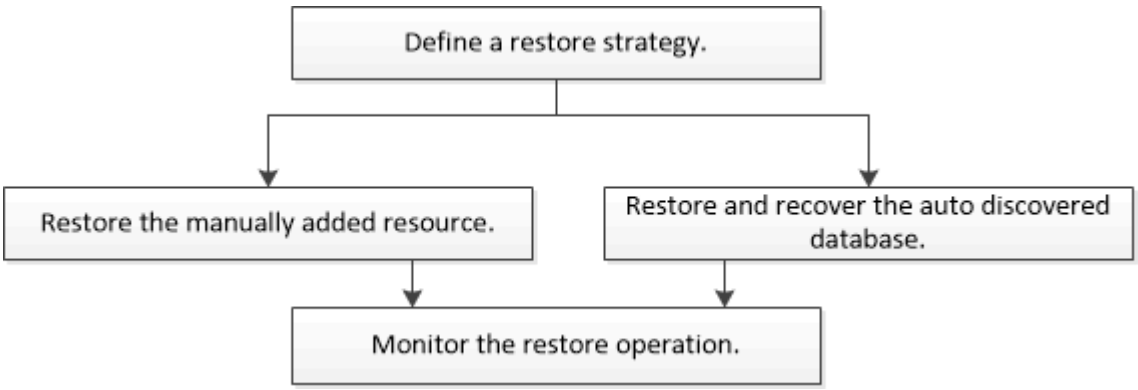
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie anschließend auf .
8. Wenn Sie einen Klon aufteilen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .

Wiederherstellung von SAP HANA Datenbanken

Wiederherstellung des Workflows

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

"SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt

werden.

Was Sie brauchen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.

Über diese Aufgabe

- Dateibasierte Backup-Kopien können nicht aus SnapCenter wiederhergestellt werden.
- Nach einem Upgrade auf SnapCenter 4.3 können die in SnapCenter 4.2 erstellten Backups wiederhergestellt werden, können aber nicht wiederhergestellt werden. Zur Wiederherstellung der in SnapCenter 4.2 erstellten Backups muss HANA Studio oder HANA-Recovery-Skripte außerhalb von SnapCenter verwendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Filtern Sie auf der Seite **Ressourcen** die Ressourcen aus der Dropdown-Liste **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

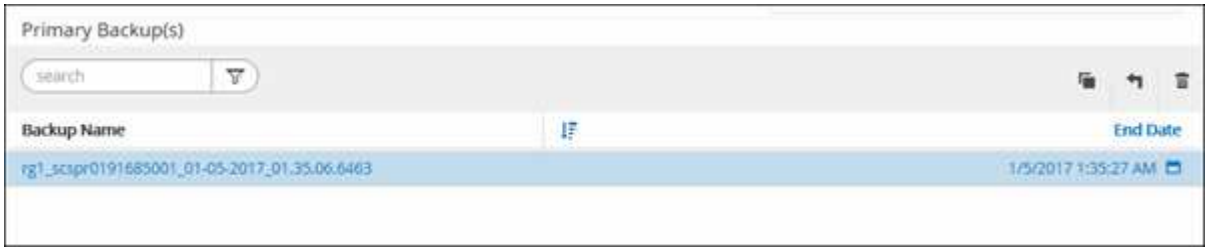
   > Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle primäre(n) Backups das Backup aus, von dem Sie wiederherstellen möchten, und klicken Sie dann auf .



6. Wählen Sie auf der Seite **Bereich wiederherstellen** die Option **vollständige Ressource** oder **Dateiebene** aus.

   a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumen der SAP HANA Datenbank wiederhergestellt.

      Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshot Kopien, die nach der zum Wiederherstellen ausgewählten Snapshot Kopie auf solchen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf denselben Volumes oder qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

   b. Wenn Sie **File Level** auswählen, können Sie entweder **Alle** auswählen oder die spezifischen Volumes oder qtrees auswählen und dann den Pfad eingeben, der mit diesen Volumes oder qtrees verbunden ist, getrennt durch Kommas

      - Sie können mehrere Volumes und qtrees auswählen.
      - Wenn der Ressourcentyp LUN ist, wird die gesamte LUN wiederhergestellt.

        Sie können mehrere LUNs auswählen.

> Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, qtrees oder LUNs wiederhergestellt.

7. Geben Sie auf der Seite **Pre OPS** die Befehle Pre Restore und Unmount ein, die ausgeführt werden sollen, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

8. Geben Sie auf der Seite **Post OPS** die Befehle Mount und Post Restore ein, die ausgeführt werden sollen, nachdem ein Wiederherstellungsauftrag ausgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Was Sie brauchen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.

Über diese Aufgabe

- Dateibasierte Backup-Kopien können nicht aus SnapCenter wiederhergestellt werden.
- Nach einem Upgrade auf SnapCenter 4.3 können die in SnapCenter 4.2 erstellten Backups wiederhergestellt werden, können aber nicht wiederhergestellt werden. Zur Wiederherstellung der in SnapCenter 4.2 erstellten Backups muss HANA Studio oder HANA-Recovery-Skripte außerhalb von SnapCenter verwendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Filtern Sie auf der Seite **Ressourcen** die Ressourcen aus der Dropdown-Liste **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

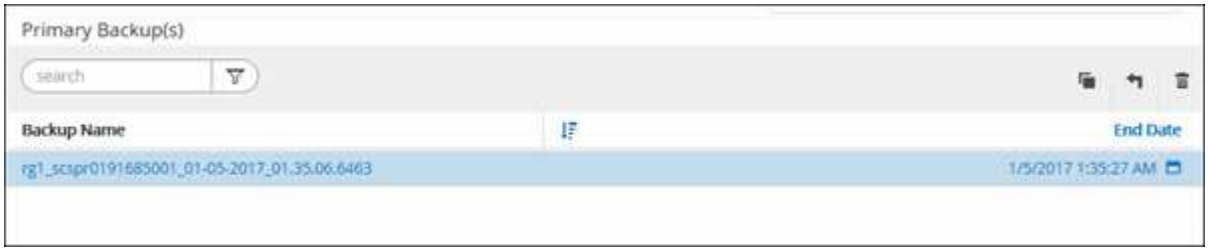
   > Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle primäre(n) Backups das Backup aus, von dem Sie wiederherstellen möchten, und klicken Sie dann auf .



6. Wählen Sie auf der Seite **Restore Scope** die Option **Complete Resource** aus, um die konfigurierten Datenvolumen der SAP HANA-Datenbank wiederherzustellen.

   > Sie können entweder **Complete Resource** (mit oder ohne **Volume revert**) oder **Tenant Database** auswählen.

   Der Wiederherstellungsvorgang wird von SnapCenter Server für mehrere Mandanten nicht unterstützt, wenn der Benutzer entweder die Option **Tenant Database** oder **Complete Restore** wählt. Sie müssen

HANA Studio oder HANA Python Script verwenden, um die Wiederherstellung durchzuführen.

a. Wählen Sie **Volume revert** aus, wenn Sie das gesamte Volume wiederherstellen möchten.

   Diese Option steht für Backups zur Verfügung, die in SnapCenter 4.3 in NFS-Umgebungen erstellt wurden.

   Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshot Kopien, die nach der zum Wiederherstellen ausgewählten Snapshot Kopie auf solchen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht. Dies gilt, wenn die Option **Complete Resource** mit **Volume revert** zur Wiederherstellung ausgewählt ist.

b. Wählen Sie **Tenant Database**.

   Diese Option ist nur für MDC-Ressourcen verfügbar.

   Stellen Sie sicher, dass die Mandantendatenbank angehalten wird, bevor Sie den Wiederherstellungsvorgang ausführen.

Wenn Sie die Option **Tenant Database** wählen, müssen Sie HANA Studio verwenden oder HANA Recovery Scripts außerhalb von SnapCenter verwenden, um den Recovery-Vorgang durchzuführen.

7. Wählen Sie auf der Seite **Wiederherstellungsumfang** eine der folgenden Optionen aus:

Sie suchen…	Tun Sie das…
Möchten so nah wie möglich bis zur aktuellen Zeit wiederherstellen	Wählen Sie **Wiederherstellen in aktuellster Zustand**. Bei einzelnen Container-Ressourcen legen Sie einen oder mehrere Backup-Standorte für Protokolle und Kataloge fest. Bei mandantenfähigen Datenbank-Containern (MDC) müssen ein oder mehrere Log-Backup-Standorte und der Backup-Katalog-Speicherort angegeben werden. Bei MDC-Ressourcen sollte der Pfad sowohl Systemdatenbank- als auch Mandantendatenbankprotokolle enthalten.

Sie suchen…	Tun Sie das…
Wiederherstellung auf den angegebenen Zeitpunkt	Wählen Sie **Wiederherstellen zu Zeitpunkt**. a. Wählen Sie die Zeitzone aus. Die Browser-Zeitzone wird standardmäßig ausgefüllt. Die ausgewählte Zeitzone wird zusammen mit der Eingangszeit in absolute GMT umgewandelt. b. Geben Sie Datum und Uhrzeit ein. Beispielsweise befindet sich der HANA Linux-Host in Sunnyvale, Kalifornien, und der Benutzer in Raleigh, North Carolina, USA, stellt die Anmeldung bei SnapCenter wieder bereit. Der Zeitunterschied zwischen diesen beiden Speicherorten beträgt 3 Stunden. Da sich der Benutzer in Raleigh, North Carolina, angemeldet hat, ist die Standardzeitzone für den Browser, die in der Benutzeroberfläche ausgewählt wird, GMT-04:00. Wenn der Benutzer eine Wiederherstellung auf 5 a.m .Sunnyvale, CA durchführen möchte, dann muss der Benutzer die Browser-Zeitzone auf die HANA Linux Host Zeitzone einstellen, die GMT-07:00 ist und das Datum und die Zeit als 5:00 Uhr angeben Bei einzelnen Container-Ressourcen legen Sie einen oder mehrere Backup-Standorte für Protokolle und Kataloge fest. Geben Sie bei MDC-Ressourcen einen oder mehrere Backup-Speicherorte und den Speicherort des Backup-Katalogs an. Bei MDC-Ressourcen sollte der Pfad sowohl Systemdatenbank- als auch Mandantendatenbankprotokolle enthalten.
Recovery für ein bestimmtes Daten-Backup erforderlich	Wählen Sie **Wiederherstellen in spezifizierter Datensicherung**.
Möchten Sie nicht wiederherstellen	Wählen Sie **Keine Erholung**. Sie müssen den Recovery-Vorgang manuell aus dem HANA Studio durchführen.

Sie können nur die Backups wiederherstellen, die nach einem Upgrade auf SnapCenter 4.3 erstellt

wurden, sofern sowohl der Host als auch das Plug-in auf SnapCenter 4.3 aktualisiert werden. Die für die Wiederherstellung ausgewählten Backups werden nach der Konvertierung der Ressource oder der Entdeckung als automatisch erkannte Ressource erstellt.

8. Geben Sie auf der Seite **Pre OPS** die Befehle Pre Restore und Unmount ein, die ausgeführt werden sollen, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. Geben Sie auf der Seite **Post OPS** die Befehle Mount und Post Restore ein, die ausgeführt werden sollen, nachdem ein Wiederherstellungsauftrag ausgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

    Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Wiederherstellung von SAP HANA Datenbanken mit PowerShell cmdlets

Im Rahmen des Restore eines SAP HANA Datenbank-Backups wird eine Verbindungssitzung mit dem SnapCenter Server initiiert, die Backups aufgeführt, Backup-Informationen abgerufen und ein Backup wiederhergestellt.

Was Sie brauchen

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Identifizieren Sie das wiederherzustellende Backup mit den Cmdlets Get-SmBackup und Get-SmBackupReport.

   Dieses Beispiel zeigt, dass zwei Backups für die Wiederherstellung verfügbar sind:

```
 PS C:\> Get-SmBackup

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32 AM
Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17 AM
```

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015 an:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Starten Sie den Recovery-Prozess im HANA-Studio.

Die Datenbank wird heruntergefahren.

4. Stellen Sie Daten aus dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

> AppObjectId ist „Host\Plugin\UID“, wobei UID = SID für Ressource des einzelnen Containertyps und UID = MDC\SID für mehrere Container ist. Sie erhalten die ResourceID aus dem Cmdlet "Get-smResources".

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
```

Dieses Beispiel zeigt, wie die Datenbank aus dem primären Speicher wiederhergestellt wird:

```
Restore-SmBackup -PluginCode HANA -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 3
```

In diesem Beispiel wird gezeigt, wie die Datenbank aus dem sekundären Speicher wiederhergestellt wird:

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

Die Backups werden im HANA Studio für die Recovery verfügbar sein.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32 AM
Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17 AM
```

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015 an:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Stellen Sie Daten aus dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen von Restore-Vorgängen bei SAP HANA Datenbanken

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie Auf So filtern Sie die Liste, damit nur Wiederherstellungsvorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Jobdetails** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

> Nach der Volume-basierten Wiederherstellung werden die Backup-Metadaten aus dem SnapCenter-Repository gelöscht, die Backup-Katalogeinträge bleiben aber im SAP HANA-Katalog. Der Status des Wiederherstellungsjobs wird angezeigt , Sie sollten auf Jobdetails klicken, um das Warnzeichen einiger der untergeordneten Aufgaben anzuzeigen. Klicken Sie auf das Warnschild und löschen Sie die angezeigten Backup-Katalog-Einträge.

Backups von SAP HANA Ressourcen klonen

Klon-Workflow

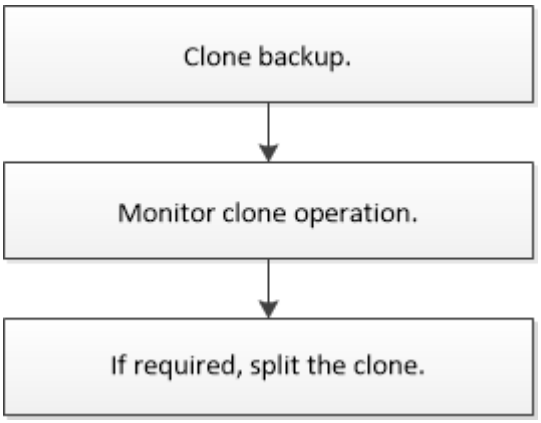
Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

- Sie können auf dem SAP HANA-Quellserver klonen.
- Sie können Ressourcen-Backups aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses

- Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

Klonen eines Backups einer SAP HANA Datenbank

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen.

Was Sie brauchen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Sie können keine dateibasierten Backups klonen.
- Der Ziel-Klon-Server sollte dieselbe SAP HANA-Instanz-SID haben, die im Feld Ziel-Klon-SID bereitgestellt wird.

Informationen zu dieser Aufgabe Informationen zu Einschränkungen bei der Klonteiloperation finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Filtern Sie auf der Seite **Ressourcen** die Ressourcen aus der Dropdown-Liste **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugeordnete Ressourcengruppen und -Richtlinien sowie Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

   Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf .
6. Führen Sie auf der Seite **Ort** die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Plug-in-Host	Wählen Sie den Host aus, auf dem der Klon gemountet werden soll, und das Plug-in ist installiert.
Ziel Klon-SID	Geben Sie die SAP HANA Instanz-ID ein, die aus den vorhandenen Backups geklont werden soll.
NFS-Export-IP-Adresse	Geben Sie IP-Adressen oder Hostnamen ein, auf denen die geklonten Volumes exportiert werden.
ISCSI-Initiator	Geben Sie den iSCSI-Initiatornamen des Hosts ein, an den die LUNs exportiert werden. Diese Option ist nur verfügbar, wenn Sie den Ressourcentyp LUN ausgewählt haben.
Protokoll	Geben Sie das LUN-Protokoll ein. Diese Option ist nur verfügbar, wenn Sie den Ressourcentyp LUN ausgewählt haben.

Wenn die ausgewählte Ressource eine LUN ist und Sie aus einem sekundären Backup klonen, werden die Ziel-Volumes aufgelistet. Es können mehrere Ziel-Volumes an einer einzigen Quelle vorhanden sein.

> Vor dem Klonen müssen Sie sicherstellen, dass der iSCSI-Initiator oder das FCP vorhanden ist und bei alternativen Hosts konfiguriert und angemeldet sind.

7. Führen Sie auf der Seite **Skripts** die folgenden Schritte aus:

> Die Skripte werden auf dem Plug-in-Host ausgeführt.

   a. Geben Sie die Befehle für den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
      - Befehl Pre Clone: Löschen Sie vorhandene Datenbanken mit demselben Namen
      - Befehl nach Clone: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.
   b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

      Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:

      Beispiel für NFS:

```
mount VSERVER_DATA_IP:%{VOLUME_NAME_Clone} /mnt
```

8. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Klonen von Backups von SAP HANA Datenbanken mit PowerShell Cmdlets

Der Klon-Workflow umfasst die Planung, die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Rufen Sie die Backups für den Klonvorgang mit dem Cmdlet Get-SmBackup ab.

   Dieses Beispiel zeigt, dass zwei Backups zum Klonen verfügbar sind:

   ```
    C:\PS> Get-SmBackup

           BackupId                        BackupName
   BackupTime                     BackupType
           --------                        ----------
   ----------                     ----------
            1                      Payroll Dataset_vise-f6_08... 8/4/2015
   11:02:32 AM          Full Backup
            2                      Payroll Dataset_vise-f6_08... 8/4/2015
   11:23:17 AM
   ```

3. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

Dieses Beispiel zeigt, dass für das zu klonendes Backup eine NFSExportIPs-Adresse von 10.232.206.169 vorhanden ist:

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

Wenn NFSExportIPs nicht angegeben sind, wird der Standardwert auf den Klon-Zielhost exportiert.

4. Überprüfen Sie, ob die Backups erfolgreich geklont wurden, indem Sie das Cmdlet "Get-SmCloneReport" verwenden, um die Details zu den Klonjobs anzuzeigen.

   Sie können Details wie Klon-ID, Startdatum und -Zeit, Enddatum und -Zeit anzeigen.

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

Überwachung von Klonvorgängen für SAP HANA Datenbanken

Sie können den Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem

vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie Auf Filtern der Liste, sodass nur Klonvorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Teilen Sie einen Klon auf

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon ist unabhängig von der übergeordneten Ressource.

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu Einschränkungen für den Klon-Split-Vorgang finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".

- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** die entsprechende Option aus der Liste Ansicht aus:

Option	Beschreibung
Für Datenbankapplikationen	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Für File-Systeme	Wählen Sie in der Liste Ansicht **Pfad** aus.

3. Wählen Sie die entsprechende Ressource aus der Liste aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht Kopien managen die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Clone-Splitvorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet "Stop-SmJob" ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragzeit benötigen, um zu prüfen, ob der Klon geteilt ist oder nicht, können Sie den Wert von *CloneSplitStatusCheckPollTime* Parameter in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Clone Split-Vorgangs angezeigt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klontrennung schlägt fehl, wenn gerade Backup-, Wiederherstellungs- oder andere Klonsplitonen durchgeführt werden. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Weitere Informationen

"Der SnapCenter Klon oder die Überprüfung schlägt fehl, wenn das Aggregat nicht vorhanden ist"

Löschen oder teilen Sie SAP HANA Datenbankklone nach dem Upgrade der SnapCenter

Nach einem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource, aus der die Klone erstellt wurden, aufteilen.

Über diese Aufgabe

Um den Platzbedarf für die versteckten Klone zu ermitteln, führen Sie den folgenden Befehl aus: `Get-SmClone -ListStorageFootprint`

Schritte

1. Löschen Sie die Backups der geklonten Ressourcen mit dem Cmdlet "remove-smbackup".
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mit dem Cmdlet "remove-sresourcgruppe".
3. Entfernen Sie den Schutz der geklonten Ressource mit dem Cmdlet "remove-smprotectResource".
4. Wählen Sie die übergeordnete Ressource auf der Seite **Ressourcen** aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie aus der Ansicht **Manage Copies** die Klone entweder aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.
6. Wählen Sie die Klone aus, und klicken Sie dann auf Zum Löschen von Klonen oder Klicken auf Um die Klone aufzuteilen.
7. Klicken Sie auf **OK**.