Microsoft SQL Server Datenbanken schützen

SnapCenter Software 4.9

NetApp
March 20, 2024

Inhalt

Microsoft SQL Server Datenbanken schützen

SnapCenter Plug-in für Microsoft SQL Server

SnapCenter Plug-in für Microsoft SQL Server – Übersicht

Das SnapCenter Plug-in für Microsoft SQL Server ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das Management der applikationsgerechten Datensicherung von Microsoft SQL Server Datenbanken ermöglicht. Das Plug-in für SQL Server automatisiert Backups, Verifizierungen, Restores und Klonvorgänge in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für SQL Server installiert ist, können Sie mithilfe von SnapCenter mit NetApp SnapMirror Technologie gespiegelte Kopien von Backups auf einem anderen Volume erstellen. In Verbindung mit der NetApp SnapVault Technologie können Sie eine Disk-to-Disk-Backup-Replizierung zwecks Standard-Compliance oder Archivierung durchführen.

Welche Möglichkeiten bietet das SnapCenter Plug-in für Microsoft SQL Server

Wenn das SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung installiert ist, können Sie mit SnapCenter die SQL Server Datenbanken sichern, wiederherstellen und klonen.

Sie können die folgenden Aufgaben durchführen, die Backup-Vorgänge, Restore-Vorgänge und Klonvorgänge von SQL Server-Datenbanken und Datenbankressourcen unterstützen:

- Sichern Sie SQL Server Datenbanken und zugehörige Transaktionsprotokolle

  Sie können keine Protokollsicherung für Master- und msdb-Systemdatenbanken erstellen. Sie können jedoch Protokoll-Backups für Modell-System-Datenbank erstellen.

- Stellen Sie Datenbankressourcen wieder her
  - Sie können Stammsystemdatenbanken, msdb-Systemdatenbanken wiederherstellen und Systemdatenbanken modellieren.
  - Sie können nicht mehrere Datenbanken, Instanzen und Verfügbarkeitsgruppen wiederherstellen.
  - Sie können die Systemdatenbank nicht in einem anderen Pfad wiederherstellen.
- Erstellung zeitpunktgenauer Klone von Produktionsdatenbanken

  Sie können keine Backup-, Wiederherstellungs-, Klon- und Klonvorgänge auf tempdb-Systemdatenbanken durchführen.

- Umgehende Überprüfung der Backup-Vorgänge oder Vermeidung von Verifizierungen bis zu einem späteren Zeitpunkt

  Die Überprüfung der SQL Server Systemdatenbank wird nicht unterstützt. SnapCenter klont die Datenbanken, um einen Verifizierungsvorgang durchzuführen. SnapCenter kann SQL Server Systemdatenbanken nicht klonen. Daher wird die Überprüfung dieser Datenbanken nicht unterstützt.

- Planen von Backup-Vorgängen und Klonvorgängen

- Überwachung von Backup-Vorgängen, Restore-Vorgängen und Klonvorgängen

> Das Plug-in für SQL Server unterstützt kein Backup und Recovery von SQL Server Datenbanken auf SMB-Freigaben.

SnapCenter Plug-in für Microsoft SQL Server Funktionen

Das Plug-in für SQL Server ist in Microsoft SQL Server auf dem Windows Host und in die NetApp Snapshot Kopiertechnologie auf dem Storage-System integriert. Um mit dem Plug-in für SQL Server zu arbeiten, verwenden Sie die Schnittstelle SnapCenter.

Das Plug-in für SQL Server umfasst folgende Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche powered by SnapCenter**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die Schnittstelle von SnapCenter ermöglicht die vollständige konsistente Backup- und Restore-Prozesse über Plug-ins hinweg, die zentrale Berichterstellung, die auf einen Blick basierende Dashboard-Ansichten verwenden, die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) einrichten und Jobs in allen Plug-ins überwachen. SnapCenter bietet außerdem eine zentralisierte Planung und ein Richtlinienmanagement zur Unterstützung von Backup- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

  Sie können routinemäßige SQL Server Backups planen, eine richtlinienbasierte Backup-Aufbewahrung konfigurieren und zeitpunktgenaue und minutengenaue Restore-Vorgänge einrichten. Zudem lässt sich die SQL Server Umgebung proaktiv überwachen, indem SnapCenter zum Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Unterbrechungsfreie NetApp Snapshot Kopie-Technologie**

  Das Plug-in für SQL Server verwendet NetApp Snapshot Kopiertechnologie mit dem NetApp SnapCenter Plug-in für Microsoft Windows. So können Sie Datenbanken in Sekundenschnelle sichern und schnell wiederherstellen, ohne SQL Server offline schalten zu müssen. Snapshot Kopien belegen nur minimalen Speicherplatz.

Zusätzlich zu diesen wichtigen Funktionen bietet das Plug-in für SQL Server folgende Vorteile:

- Unterstützung für Workflows für Backup, Wiederherstellung, Klonen und Verifizierung
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation
- Erstellung platzsparender und zeitpunktgenauer Kopien von Produktionsdatenbanken für Test- oder Datenextraktion mit der NetApp FlexClone Technologie

  Es ist eine FlexClone Lizenz auf dem Storage-System erforderlich, auf dem der Klon gespeichert ist.

- Unterbrechungsfreie und automatisierte Backup-Verifizierung
- Die Möglichkeit, mehrere Backups gleichzeitig über mehrere Server hinweg auszuführen
- PowerShell cmdlets zur Skripte von Backup-, Verifizierungs-, Wiederherstellungs- und Klonvorgängen
- Unterstützung von AlwaysOn Availability Groups (AGs) in SQL Server, um die Einrichtung, Backups und Restores von AGs zu beschleunigen

- In-Memory-Datenbank und Buffer Pool Extension (BPE) als Teil von SQL Server 2014
- Unterstützung von Backups von LUNs und Virtual Machine Disks (VMDKs)
- Unterstützung physischer und virtualisierter Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM) und VMDK über NFS und VMFS

> NAS Volumes sollten eine standardmäßige Exportrichtlinie in Storage Virtual Machine (SVM) verwenden.

- Unterstützung von FileStream und Dateigruppen in Standalone-Datenbanken von SQL Server

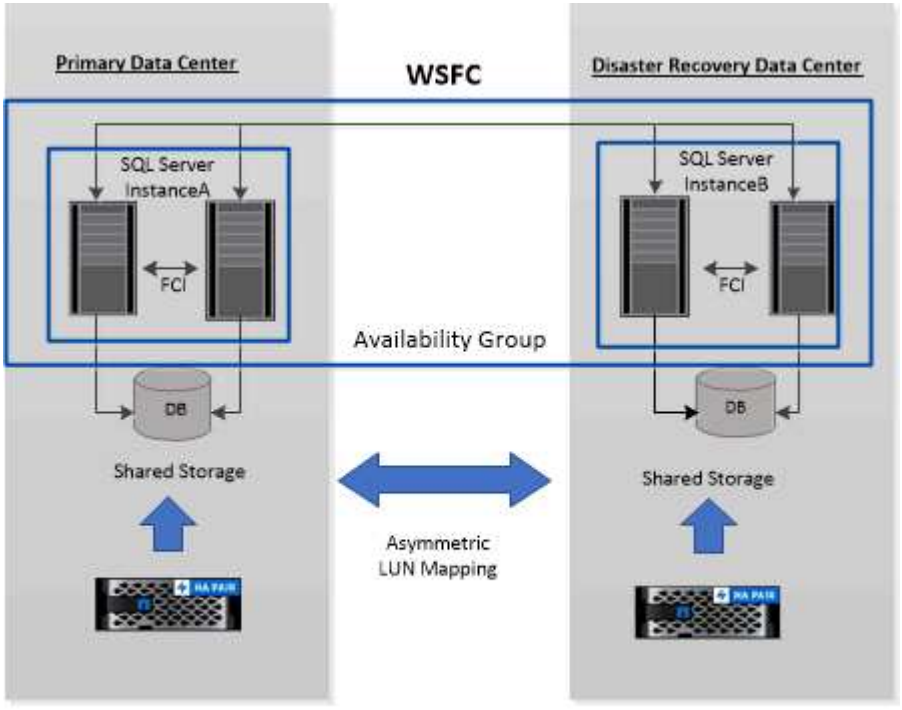
Unterstützung für asymmetrische LUN-Zuordnung in Windows Clustern

Das SnapCenter Plug-in für Microsoft SQL Server unterstützt die Erkennung in SQL Server 2012 und höher sowie ALM-Konfigurationen (Asymmetric LUN Mapping) für Hochverfügbarkeit und Verfügbarkeitsgruppen für Disaster Recovery. Bei der Ermittlung von Ressourcen erkennt SnapCenter Datenbanken auf lokalen Hosts und Remote-Hosts in ALM-Konfigurationen.

Eine ALM-Konfiguration ist ein einzelnes Windows Server Failover Cluster, das einen oder mehrere Nodes in einem primären Datacenter und einen oder mehrere Nodes in einem Disaster Recovery Center enthält.

Nachfolgend ein Beispiel für eine ALM-Konfiguration:

- Zwei Failover-Cluster-Instanzen (FCI) in einem Datacenter mit mehreren Standorten
- FCI für lokale Hochverfügbarkeit (HA) und Availability Group (AG) für Disaster Recovery mit Standalone-Instanz am Disaster-Recovery-Standort



WSFC----Windows Server Failover Cluster

Der Storage im primären Datacenter wird von den FCI-Nodes gemeinsam genutzt, die sich im primären Datacenter befinden. Der Storage im Disaster-Recovery-Datacenter wird von den FCI-Nodes geteilt, die sich im Disaster-Recovery-Datacenter befinden.

Der Storage im primären Datacenter ist für die Nodes im Disaster Recovery-Datacenter nicht sichtbar und umgekehrt.

ALM-Architektur kombiniert zwei von FCI verwendete Shared Storage-Lösungen mit einer nicht gemeinsam genutzten oder dedizierten Storage-Lösung, die von der SQL AG verwendet wird. Die AG Lösung verwendet identische Laufwerksbuchstaben für gemeinsam genutzte Festplattenressourcen über alle Datacenter hinweg. Diese Anordnung des Storage, bei der ein Cluster-Laufwerk von einem Teil der Nodes innerhalb eines WSFC gemeinsam genutzt wird, wird als ALM bezeichnet.

Storage-Typen, die von SnapCenter Plug-ins für Microsoft Windows und Microsoft SQL Server unterstützt werden

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines. Sie müssen überprüfen, ob Ihr Speichertyp unterstützt wird, bevor Sie das Paket für Ihren Host installieren.

SnapCenter Provisioning und Datensicherung werden unter Windows Server unterstützt. Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische SnapCenter Benutzeroberfläche (GUI) oder PowerShell Commandlets	
Physischer Server	ISCSI-verbundene LUNs	SnapCenter GUI oder PowerShell Commandlets	
Physischer Server	SMB3 (CIFS) Shares auf einer Storage Virtual Machine (SVM)	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. SnapCenter kann kein Backup von Daten und Freigaben über das SMB-Protokoll verwenden.
VMware VM	RDM-LUNs, die über einen FC- oder iSCSI-HBA verbunden sind	PowerShell Commandlets	
VMware VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
VMware VM	Virtual Machine File Systems (VMFS) oder NFS-Datastores	VMware vSphere	
VMware VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. SnapCenter kann kein Backup von Daten und Freigaben über das SMB-Protokoll verwenden.
Hyper-V VM	Virtuelle FC-LUNs (VFC), die über einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Sie müssen Hyper-V Manager verwenden, um virtuelle FC (VFC) LUNs bereitzustellen, die über einen virtuellen Fibre Channel Switch verbunden sind. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.
Hyper-V VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. SnapCenter kann kein Backup von Daten und Freigaben über das SMB-Protokoll verwenden. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Empfehlungen für das Storage-Layout für das SnapCenter Plug-in für Microsoft SQL Server

Mit dem gut durchdachten Storage-Layout kann SnapCenter Server Ihre Datenbanken entsprechend den Recovery-Vorgaben sichern. Bei der Definition des Storage-Layouts sollten Sie mehrere Faktoren berücksichtigen, darunter die Größe der Datenbank, die Änderungsrate der Datenbank und die Häufigkeit, mit der Sie Backups durchführen.

In den folgenden Abschnitten werden die Empfehlungen und Einschränkungen des Storage-Layouts für LUNs und Virtual Machine Disks (VMDKs) mit dem SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung definiert.

In diesem Fall können LUNs VMware RDM-Festplatten und die dem Gast zugeordneten iSCSI-Direct-Attached LUNs enthalten.

LUN- und VMDK-Anforderungen

Sie können optional dedizierte LUNs oder VMDKs für eine optimale Performance und ein optimales Management für die folgenden Datenbanken verwenden:

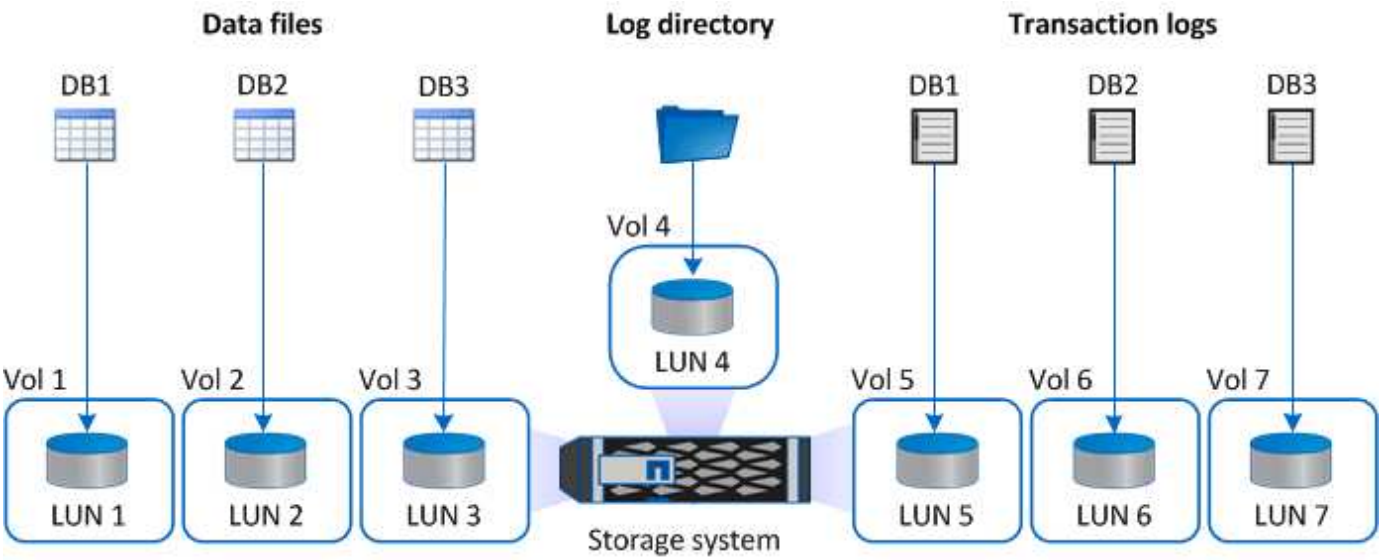
- Master- und Modellsystemdatenbanken
- Tempdb
- Benutzerdatenbankdateien (.mdf und .ndf)
- Log-Dateien der Benutzerdatenbank-Transaktionen (.ldf)
- Protokollverzeichnis

Zur Wiederherstellung großer Datenbanken empfiehlt es sich, dedizierte LUNs oder VMDKs zu verwenden. Die zur Wiederherstellung einer vollständigen LUN oder VMDK benötigte Zeit beträgt weniger als die Zeit zur Wiederherstellung der in der LUN oder VMDK gespeicherten einzelnen Dateien.

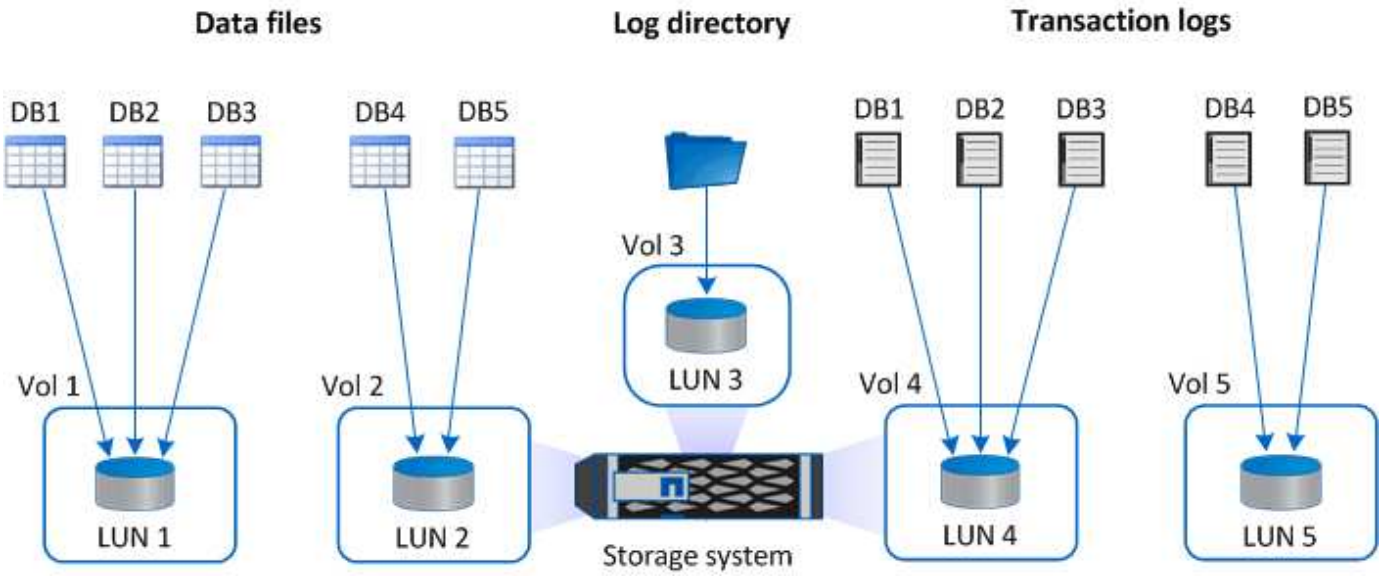
Für das Log-Verzeichnis sollten Sie eine separate LUN oder VMDK erstellen, damit genügend freier Speicherplatz in den Daten- oder Log-Datei-Disks vorhanden ist.

Beispiellayouts für LUN und VMDK

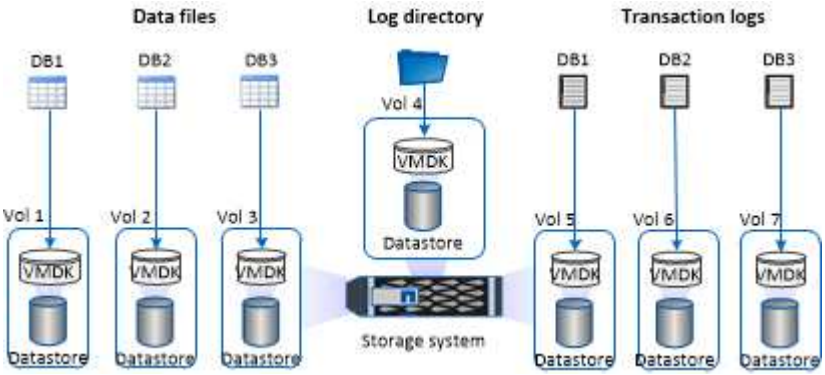
Die folgende Grafik zeigt, wie Sie das Storage-Layout für große Datenbanken auf LUNs konfigurieren können:



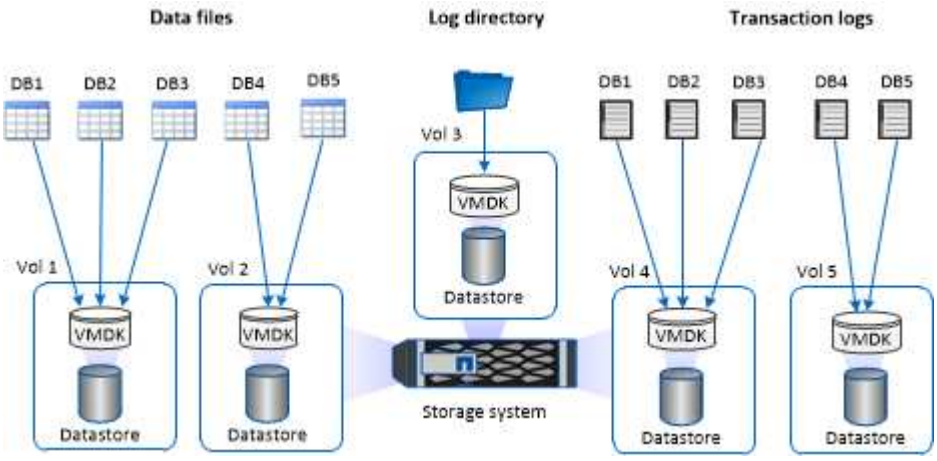
Die folgende Grafik zeigt, wie Sie das Storage-Layout für mittelgroße oder kleine Datenbanken auf LUNs konfigurieren können:



Die folgende Grafik zeigt, wie Sie das Storage-Layout für große Datenbanken auf VMDKs konfigurieren können:



Die folgende Grafik zeigt, wie Sie das Storage-Layout für mittelgroße oder kleine Datenbanken auf VMDKs konfigurieren können:



Minimale ONTAP-Berechtigungen für SQL Plug-in erforderlich

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

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - 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
  - die lun-Größe wird geändert
  - lun seriell
  - lun anzeigen
  - 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
  - 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
- 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
- Netzwerkschnittstelle
- Netzwerkschnittstelle wird angezeigt
- vserver
- MetroCluster zeigen

Storage-Systeme für SnapMirror und SnapVault Replizierung für Plug-in für SQL Server vorbereiten

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.

SnapCenter führt die Updates an SnapMirror und SnapVault durch, nachdem der Vorgang der Snapshot Kopie abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

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".

SnapCenter unterstützt keine **Sync_mirror** Replikation.

Backup-Strategie für SQL Server-Ressourcen

Backup-Strategie für SQL Server-Ressourcen definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, können Sie sicherstellen, dass Sie über die Backups verfügen, die Sie benötigen, um Ihre Datenbanken erfolgreich wiederherzustellen oder zu klonen. Ihre Backup-Strategie wird durch Ihre Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) weitgehend bestimmt.

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich

Verfügbarkeit und Performance des Service. Die RTO ist der Zeitpunkt, zu dem ein Geschäftsprozess nach einer Service-Unterbrechung wiederhergestellt werden muss. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Backup-Strategie bei.

Art der unterstützten Backups

Für das Sichern des SQL Server-Systems und der Benutzerdatenbanken mit SnapCenter müssen Sie den Ressourcentyp auswählen, z. B. Datenbanken, SQL Server-Instanzen und Verfügbarkeitsgruppen (AG). Mithilfe der Snapshot Kopiertechnologie lassen sich online schreibgeschützte Kopien der Volumes erstellen, auf denen sich die Ressourcen befinden.

Sie können die Option nur kopieren auswählen, um anzugeben, dass der SQL-Server die Transaktionsprotokolle nicht schneidet. Sie sollten diese Option verwenden, wenn Sie auch SQL Server mit anderen Backup-Anwendungen verwalten. Wenn die Transaktionsprotokolle intakt bleiben, kann jede Backup-Anwendung die Systemdatenbanken wiederherstellen. Backups, bei denen nur Kopien erstellt werden, sind unabhängig von der Sequenz geplanter Backups und haben keine Auswirkungen auf die Backup- und Restore-Vorgänge der Datenbank.

Backup-Typ	Beschreibung	Copy-Only-Option mit Backup-Typ
Vollständiges Backup und Backup von Protokollen	Sichert die Systemdatenbank und schneidet die Transaktionsprotokolle ab. Der SQL Server schneidet die Transaktionsprotokolle ab, indem die Einträge entfernt werden, die bereits in der Datenbank gespeichert sind. Nach Abschluss der vollständigen Sicherung erstellt diese Option ein Transaktionsprotokoll, das die Transaktionsinformationen erfasst. Normalerweise sollten Sie diese Option wählen. Wenn Ihre Backup-Zeit jedoch kurz ist, können Sie wählen, keine Transaktions-Log-Backup mit vollständiger Sicherung auszuführen. Sie können keine Protokollsicherung für Master- und msdb-Systemdatenbanken erstellen. Sie können jedoch Protokoll-Backups für Modell-System-Datenbank erstellen.	Sichert die Systemdatenbankdateien und die Transaktions-Logs, ohne die Protokolle zu beeinträchtigen. Ein Backup nur für Kopien kann nicht als differenzielles Basis- oder differenzielles Backup dienen und hat keine Auswirkungen auf die Differentialbasis. Die Wiederherstellung eines nur-Kopie-Vollbackups ist mit der Wiederherstellung eines anderen vollständigen Backups identisch.

Backup-Typ	Beschreibung	Copy-Only-Option mit Backup-Typ
Vollständiges Datenbank-Backup	Sichert die Systemdatenbankdateien. Sie können vollständige Datenbank-Backup für Master-, Modell- und msdb-Systemdatenbanken erstellen.	Sichert die Systemdatenbankdateien.
Transaktions-Log-Backup	Sichert die gekürzten Transaktionsprotokolle, kopiert nur die Transaktionen, die seit dem letzten Transaktions-Log gesichert wurden. Wenn Sie häufige Transaktions-Log-Backups neben vollständigen Datenbank-Backups planen, können Sie granulare Recovery-Punkte auswählen.	Sicherung der Transaktions-Logs, ohne sie zu beeinträchtigen Diese Sicherungsart hat keine Auswirkung auf die Sequenzierung von regelmäßigen Protokollsicherungen. Backups nur-Kopien-Protokolle sind für die Durchführung von Online-Wiederherstellungen nützlich.

Backup-Pläne für Plug-in für SQL Server

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. 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, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen. So könnten beispielsweise regelmäßige Transaktions-Log-Backups ausreichen, um sicherzustellen, dass Sie die Backups haben, die Sie benötigen. Je öfter Sie Ihre Datenbanken sichern, desto weniger Transaktions-Logs benötigt SnapCenter zum Zeitpunkt der Wiederherstellung, was zu schnelleren Restore-Vorgängen führen kann.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen

auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. 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. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Datenbanken erforderlichen Backup-Jobs

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

Die Anzahl der von Ihnen gewählten Backup-Aufgaben hängt bei Datenbank-Backups in der Regel von der Anzahl der Volumes ab, auf denen Sie Ihre Datenbanken platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Datenbanken auf einem Volume und einer großen Datenbank auf einem anderen Volume platziert haben, können Sie einen Backup-Job für die kleinen Datenbanken und einen Backup-Job für die große Datenbank erstellen.

Backup-Namenskonventionen für SQL Server

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.

Optionen zur Backup-Aufbewahrung für Plug-in für SQL Server

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

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

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Wie lange werden Transaktions-Log-Backups auf dem Quell-Storage-System aufbewahrt

Das SnapCenter Plug-in für Microsoft SQL Server benötigt Transaktions-Log-Backups, um minutengenaue Restore-Vorgänge durchzuführen, bei denen Ihre Datenbank zwischen zwei vollständigen Backups wiederhergestellt wird.

Wenn z. B. ein Plug-in für SQL Server um 8:00 Uhr ein komplettes Backup erstellt hat Zusammen mit einem weiteren vollständigen Backup um 5:00 Uhr konnte die Datenbank jederzeit zwischen 8:00 Uhr und nach dem letzten Transaktions-Log-Backup wiederhergestellt werden Und um 5:00 Uhr Wenn keine Transaktionsprotokolle verfügbar sind, kann das Plug-in für SQL Server nur zeitpunktgenaue Restore-Vorgänge durchführen, die eine Datenbank so lange wiederherstellen, wie das Plug-in für SQL Server ein komplettes Backup abgeschlossen hat.

In der Regel erfordern Sie minutengenaue Restore-Vorgänge nur für einen oder zwei Tage. SnapCenter speichert standardmäßig mindestens zwei Tage.

Mehrere Datenbanken auf demselben Volume

Sie können alle Datenbanken auf demselben Volume ablegen, da die Backup-Richtlinie die Möglichkeit hat, die maximale Datenbank pro Backup festzulegen (Standardwert ist 100).

Wenn Sie beispielsweise 200 Datenbanken auf demselben Volume haben, werden zwei Snapshot Kopien mit je 100 Datenbanken in beiden Snapshot Kopien erstellt.

Verifizierung von Backup-Kopien für SQL Server mithilfe des primären oder sekundären Storage Volumes

Sie können Backup-Kopien auf dem primären Storage Volume oder auf dem sekundären SnapMirror oder SnapVault Storage Volume überprüfen. Bei der Überprüfung und

Verwendung eines sekundären Storage-Volumes wird die Last für das primäre Storage Volume verringert.

Wenn Sie ein Backup auf dem primären oder sekundären Storage Volume überprüfen, werden alle primären und sekundären Snapshot Kopien als überprüft markiert.

Zur Überprüfung von Backup-Kopien auf dem sekundären SnapVault Storage Volume ist eine SnapRestore Lizenz erforderlich.

Wann werden Überprüfungsaufträge geplant

SnapCenter kann Backups zwar sofort nach der Erstellung überprüfen, kann aber die zum Abschließen des Backup-Jobs erforderliche Zeit erheblich verlängern und ist ressourcenintensiv. Daher ist es fast immer am besten, die Verifizierung in einem separaten Job für ein späteres Mal zu planen. Wenn Sie beispielsweise eine Datenbank um 5:00 Uhr sichern Sie können jeden Tag eine Verifizierung planen, und zwar eine Stunde später um 6:00 Uhr

Aus dem gleichen Grund ist es in der Regel nicht erforderlich, die Backup-Verifizierung jedes Mal, wenn Sie ein Backup ausführen. Eine Überprüfung in regelmäßigen, aber weniger häufigen Abständen durchzuführen, reicht normalerweise aus, um die Integrität des Backups zu gewährleisten. Ein einziger Verifizierungsauftrag kann mehrere Backups gleichzeitig überprüfen.

Wiederherstellungsstrategie für SQL Server

Definieren einer Wiederherstellungsstrategie für SQL Server

Durch die Definition einer Wiederherstellungsstrategie für SQL Server können Sie Ihre Datenbank erfolgreich wiederherstellen.

Quellen und Ziele für einen Wiederherstellungsvorgang

Sie können eine SQL Server Datenbank aus einer Backup-Kopie auf einem primären oder sekundären Storage wiederherstellen. Sie können die Datenbank zusätzlich zum ursprünglichen Speicherort auch an verschiedenen Zielen wiederherstellen, sodass Sie das Ziel auswählen können, das Ihre Anforderungen unterstützt.

Quellen für einen Wiederherstellungsvorgang

Sie können Datenbanken aus primärem oder sekundärem Storage wiederherstellen.

Ziele für einen Wiederherstellungsvorgang

Sie können Datenbanken an verschiedenen Zielen wiederherstellen:

Ziel	Beschreibung
Der ursprüngliche Standort	Standardmäßig stellt SnapCenter die Datenbank an demselben Speicherort auf derselben SQL Serverinstanz wieder her.

Ziel	Beschreibung
Ein anderer Ort	Sie können die Datenbank an einem anderen Ort auf einer beliebigen SQL Server-Instanz innerhalb desselben Hosts wiederherstellen.
Ursprünglicher oder anderer Speicherort unter Verwendung unterschiedlicher Datenbanknamen	Sie können die Datenbank mit einem anderen Namen als jede SQL Server-Instanz auf demselben Host wiederherstellen, auf dem das Backup erstellt wurde.

Wiederherstellung eines alternativen Hosts über ESX Server für SQL-Datenbanken auf VMDKs (NFS- und VMFS-Datastores) wird nicht unterstützt.

Von SnapCenter unterstützte SQL Server Recovery-Modelle

Jedem Datenbanktyp werden standardmäßig spezifische Recovery-Modelle zugewiesen. Der SQL Server Datenbankadministrator kann jede Datenbank einem anderen Recovery-Modell zuweisen.

SnapCenter unterstützt drei Arten von SQL Server Recovery-Modellen:

- Einfaches Recovery-Modell

  Wenn Sie das einfache Wiederherstellungsmodell verwenden, können Sie keine Backups der Transaktions-Logs erstellen.

- Vollständiges Recovery-Modell

  Wenn Sie das vollständige Recovery-Modell verwenden, können Sie eine Datenbank vom Zeitpunkt eines Ausfalls auf ihren vorherigen Zustand wiederherstellen.

- Recovery-Modell mit Massenprotokollierter

  Wenn Sie das Recovery-Modell mit der Massenprotokollierfunktion verwenden, müssen Sie den protokollierten Massenvorgang manuell erneut ausführen. Sie müssen den protokollierten Massenvorgang durchführen, wenn das Transaktionsprotokoll, das den Verschiebdatensatz des Vorgangs enthält, vor der Wiederherstellung nicht gesichert wurde. Wenn der Bulk Logged-Vorgang 10 Millionen Zeilen in eine Datenbank einfügt und die Datenbank vor dem Backup des Transaktionsprotokolls ausfällt, enthält die wiederhergestellte Datenbank nicht die Zeilen, die von der protokollierten Massenoperation eingefügt wurden.

Arten von Wiederherstellungsvorgängen

Sie können SnapCenter verwenden, um verschiedene Arten von Wiederherstellungsvorgängen auf SQL Server-Ressourcen durchzuführen.

- Wiederherstellung im Minutenschnoch
- Wiederherstellung auf einen früheren Zeitpunkt

In den folgenden Situationen lassen sich Wiederherstellungen bis zur Minute durchführen oder ein Recovery auf einen früheren Zeitpunkt durchführen:

- Wiederherstellung aus sekundärem SnapMirror oder SnapVault Storage
- Wiederherstellung auf alternativem Pfad (Speicherort)

SnapCenter bietet keine Unterstützung für Volume-basierte SnapRestore.

Führen Sie Wiederherstellungen minutengenau durch

In einem up-to-the-minute-Wiederherstellungsvorgang (standardmäßig ausgewählt) werden Datenbanken bis zum Fehlerpunkt wiederhergestellt. SnapCenter erreicht dies durch folgende Sequenz:

1. Sichert das letzte aktive Transaktionsprotokoll vor dem Wiederherstellen der Datenbank.
2. Stellt die Datenbanken aus dem vollständigen Datenbank-Backup wieder her, das Sie auswählen.
3. Wendet alle Transaktionsprotokolle an, die nicht den Datenbanken zugeschrieben wurden (einschließlich Transaktions-Logs aus den Backups vom Zeitpunkt der Erstellung des Backups bis zum aktuellsten Zeitpunkt).

   Transaktionsprotokolle werden nach vorne verschoben und auf alle ausgewählten Datenbanken angewendet.

Für eine minutengenaue Wiederherstellung ist ein zusammenhängender Satz von Transaktionsprotokollen erforderlich.

Da der SnapCenter die Transaktionsprotokolle der SQL Server-Datenbank nicht aus den Log-shipping Backup-Dateien wiederherstellen kann (durch die Protokollversand können Sie Transaktions-Log-Backups automatisch von einer primären Datenbank auf einer primären Serverinstanz an eine oder mehrere sekundäre Datenbanken auf separaten sekundären Serverinstanzen senden), Sie können keine up-to-the-minute-Wiederherstellung aus den Transaktions-Log-Backups durchführen. Aus diesem Grund sollten Sie den SnapCenter verwenden, um Ihre Transaktions-Log-Dateien für die SQL Server-Datenbank zu sichern.

Wenn Sie keine up-to-the-minute-Wiederherstellung für alle Backups benötigen, können Sie die Transaktions-Log-Backup-Aufbewahrung Ihres Systems mithilfe der Backup-Richtlinien konfigurieren.

Beispiel für einen minutengenauen Restore-Vorgang

Angenommen, Sie führen das SQL Server-Backup täglich mittags und mittwochs um 4:00 Uhr aus Sie müssen eine Wiederherstellung aus einem Backup durchführen. Aus irgendeinem Grund, die Sicherung von Mittwoch Mittag nicht überprüft, so entscheiden Sie sich für die Wiederherstellung von Dienstag Mittag Backup. Wenn das Backup wiederhergestellt wird, werden alle Transaktionsprotokolle nach vorn verschoben und auf die wiederhergestellten Datenbanken angewendet, beginnend mit denen, die nicht begangen wurden, als Sie am Dienstag das Backup erstellt haben und das letzte Transaktions-Log, das am Mittwoch um 4:00 Uhr geschrieben wurde, durchgehen (Wenn die Transaktions-Logs gesichert wurden).

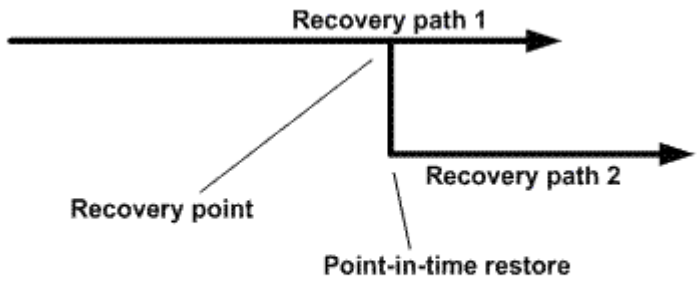
Wiederherstellung auf einen früheren Zeitpunkt

In einer zeitpunktgenauen Restore-Operation werden Datenbanken nur auf eine bestimmte Zeit aus der Vergangenheit wiederhergestellt. Ein Point-in-Time-Wiederherstellungsvorgang findet in den folgenden Situationen statt:

- Die Datenbank wird zu einem bestimmten Zeitpunkt in einem gesicherten Transaktions-Log wiederhergestellt.
- Die Datenbank ist wiederhergestellt, und nur ein Teil der gesicherten Transaktions-Logs wird angewendet.

Durch das Wiederherstellen einer Datenbank zu einem bestimmten Zeitpunkt wird ein neuer Recovery-Pfad benötigt.

Die folgende Abbildung zeigt die Probleme bei der Durchführung eines Point-in-Time-Restore-Vorgangs:



Im Image besteht der Recovery-Pfad 1 aus einem kompletten Backup gefolgt von mehreren Transaktions-Log-Backups. Sie stellen die Datenbank zu einem bestimmten Zeitpunkt wieder her. Nach dem zeitpunktgenauen Restore werden neue Transaktions-Log-Backups erstellt, was Recovery-Pfad 2 zur Folge hat. Die neuen Transaktions-Log-Backups werden ohne neue vollständige Sicherung erstellt. Aufgrund von Datenbeschädigungen oder anderen Problemen können Sie die aktuelle Datenbank nicht wiederherstellen, bis ein neues vollständiges Backup erstellt wird. Darüber hinaus ist es nicht möglich, die in Recovery-Pfad 2 erstellten Transaktionsprotokolle auf das vollständige Backup des Recovery-Pfads 1 anzuwenden.

Wenn Sie Backups des Transaktionsprotokolls anwenden, können Sie auch ein bestimmtes Datum und eine bestimmte Uhrzeit angeben, zu der Sie die Anwendung der gesicherten Transaktionen beenden möchten. Dazu geben Sie ein Datum und eine Uhrzeit innerhalb des verfügbaren Bereichs an, und der SnapCenter entfernt alle Transaktionen, die vor diesem Zeitpunkt nicht durchgeführt wurden. Mit dieser Methode können Sie Datenbanken bis zu einem Zeitpunkt vor einer Beschädigung wiederherstellen oder nach einer versehentlichen Datenbank- oder Tabellenlöschung wiederherstellen.

Beispiel für einen Point-in-Time Restore-Vorgang

Angenommen, Sie erstellen um Mitternacht volle Datenbank-Backups und ein Transaktions-Log-Backup jede Stunde. Die Datenbank stürzt um 9:45 Uhr ab, aber Sie sichern immer noch die Transaktionsprotokolle der fehlgeschlagenen Datenbank. Es stehen folgende Point-in-Time-Wiederherstellungsszenarien zur Auswahl:

- Stellen Sie das vollständige Datenbank-Backup um Mitternacht wieder her und akzeptieren Sie den Verlust der danach vorgenommenen Datenbankänderungen. (Option: Keine)
- Stellen Sie das vollständige Datenbank-Backup wieder her, und wenden Sie alle Transaktions-Log-Backups bis 9:45 Uhr an (Option: Bis protokollieren)
- Stellen Sie die vollständige Datenbank-Sicherung wieder her und wenden Sie Transaktions-Log-Backups an. Geben Sie dabei die Zeit an, die die Transaktionen von den letzten Transaktions-Log-Backups wiederherstellen sollen. (Option: Nach bestimmter Zeit)

In diesem Fall würden Sie das Datum und die Uhrzeit berechnen, zu der ein bestimmter Fehler gemeldet wurde. Alle Transaktionen, die vor dem angegebenen Datum und der angegebenen Uhrzeit nicht begangen wurden, werden entfernt.

Definieren Sie eine Klonstrategie für SQL Server

Wenn Sie eine Klonstrategie definieren, können Sie Ihre Datenbank erfolgreich klonen.

1. Prüfen Sie die Einschränkungen hinsichtlich von Klonvorgängen.
2. Legen Sie den für Sie erforderlichen Klontyp fest.

Einschränkungen von Klonvorgängen

Die Einschränkungen von Klonvorgängen sollten Sie beachten, bevor Sie die Datenbanken klonen.

- Wenn Sie eine Version von Oracle von 11.2.0.4 bis 12.1.0.1 verwenden, befindet sich der Klonvorgang in Status Hung, wenn Sie den Befehl „*renamedg*“ ausführen. Sie können den Oracle Patch 19544733 anwenden Um dieses Problem zu beheben.
- Klonen von Datenbanken aus einer LUN, die direkt an einen Host angebunden ist (beispielsweise mittels Microsoft iSCSI Initiator auf einem Windows Host) zu einer VMDK oder einem RDM LUN auf dem gleichen Windows-Host oder ein anderer Windows-Host oder umgekehrt wird nicht unterstützt.
- Das Stammverzeichnis des Volume-Bereitstellungspunkts kann kein freigegebenes Verzeichnis sein.
- Wenn Sie eine LUN verschieben, die einen Klon in ein neues Volume enthält, kann der Klon nicht gelöscht werden.

Typen von Klonvorgängen

Sie können SnapCenter verwenden, um ein Backup einer SQL Server Datenbank oder eine Produktionsdatenbank zu klonen.

- Klonen aus einem Datenbank-Backup

  Die geklonte Datenbank dient als Basis für die Entwicklung neuer Applikationen und isoliert Daten Anwendungsfehler, die in der Produktionsumgebung auftreten. Darüber hinaus kann die geklonte Datenbank verwendet werden Wird für die Wiederherstellung nach Soft-Datenbank-Fehlern verwendet.

- Lebenszyklus von Klonen

  Sie können SnapCenter verwenden, um wiederkehrende Klonjobs zu planen, die bei der Produktion stattfinden Datenbank ist nicht belegt.

Schnellstart zur Installation des SnapCenter-Plug-ins für Microsoft SQL Server

Vorbereiten der Installation von SnapCenter Server und Plug-in

Enthält einen zusammengefassten Satz von Vorbereitungsanweisungen für die Installation des SnapCenter-Servers und des SnapCenter-Plug-ins für Microsoft SQL Server.

Anforderungen an Domäne und Arbeitsgruppe

SnapCenter Server kann auf Systemen installiert werden, die sich entweder in einer Domäne oder in einer Arbeitsgruppe befinden.

Wenn Sie eine Active Directory-Domäne verwenden, sollten Sie einen Domänenbenutzer mit lokalen Administratorrechten verwenden. Der Domänenbenutzer sollte Mitglied der lokalen Administratorgruppe auf dem Windows-Host sein.

Wenn Sie Arbeitsgruppen verwenden, sollten Sie ein lokales Konto mit lokalen Administratorrechten verwenden.

Lizenzanforderungen

Die Art der Lizenzen, die Sie installieren, hängt von Ihrer Umgebung ab.

Lizenz	Bei Bedarf
SnapCenter Standard Controller-basiert	Für FAS oder AFF Storage Controller erforderlich Bei der SnapCenter Standard Lizenz handelt es sich um eine Controller-basierte Lizenz und ist im Rahmen des Premium Bundle enthalten. Wenn Sie die Lizenz für die SnapManager Suite besitzen, erhalten Sie auch die Standardlizenz von SnapCenter. Wenn Sie SnapCenter auf Testbasis mit FAS oder AFF Storage installieren möchten, wenden Sie sich an den Vertriebsmitarbeiter, um eine Evaluierungslizenz für das Premium Bundle zu erhalten.
Kapazitätsbasierte SnapCenter Lösung	Erforderlich für ONTAP Select und Cloud Volumes ONTAP Als Cloud Volumes ONTAP- oder ONTAP Select-Kunde müssen Sie eine kapazitätsbasierte Lizenz pro TB erwerben, die auf den von SnapCenter gemanagten Daten basiert. Standardmäßig liefert SnapCenter eine integrierte kapazitätsbasierte SnapCenter-Testlizenz mit 90 TB und 100 Tagen im Umfang von TB aus. Weitere Informationen erhalten Sie von dem Vertriebsmitarbeiter.
SnapMirror oder SnapVault	ONTAP Wenn die Replizierung in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault Lizenz erforderlich.
Zusätzliche Lizenzen (optional)	Siehe "SnapCenter-Lizenzen".
SnapCenter-Standardlizenzen (optional)	Sekundäre Ziele Es wird empfohlen, aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standardlizenzen nicht für sekundäre Ziele aktiviert sind, können Sie nach einem Failover-Vorgang SnapCenter nicht für ein Backup von Ressourcen auf dem sekundären Ziel verwenden. Allerdings ist eine FlexClone Lizenz für sekundäre Ziele erforderlich, um Klon- und Verifizierungsvorgänge durchzuführen.

Anforderungen an Host und Port

Für die Mindestanforderungen des ONTAP und Applikations-Plug-ins siehe "Interoperabilitäts-Matrix-Tool".

Hosts	Mindestanforderungen
Betriebssystem (64 Bit)	Siehe "Interoperabilitäts-Matrix-Tool"
CPU	• Server-Host: 4 Kerne • Plug-in-Host: 1 Kern
RAM	• Server-Host: 8 GB • Plug-in-Host: 1 GB
Festplattenspeicherplatz	Server-Host: • 4 GB für SnapCenter-Serversoftware und -Protokolle • 6 GB für SnapCenter-Repository • Jeder Plug-in-Host: 2 GB für Plug-in-Installationen und -Logs, dies ist nur erforderlich, wenn Plug-in auf einem dedizierten Host installiert ist.
Bibliotheken von anderen Anbietern	Erforderlich auf Host und Plug-in-Host des SnapCenter Servers: • Microsoft .NET Framework 4.7.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher
Browser	Chrome, Internet Explorer und Microsoft Edge

Porttyp	Standardport
SnapCenter-Port	8146 (HTTPS), bidirektional, anpassbar, wie in der URL *https://server:8146*
SnapCenter SMCore-Kommunikations-Port	8145 (HTTPS), bidirektional, anpassbar
Repository-Datenbank	3306 (HTTPS), bidirektional
Windows Plug-in-Hosts	135, 445 (TCP) Neben den Ports 135 und 445 sollte auch der von Microsoft festgelegte dynamische Portbereich geöffnet sein. Remote-Installationsvorgänge verwenden den Windows Management Instrumentation (WMI)-Dienst, der diesen Portbereich dynamisch durchsucht. Informationen zum unterstützten dynamischen Portbereich finden Sie unter "Serviceübersicht und Netzwerkanschlussanforderungen für Windows".

Porttyp	Standardport
SnapCenter Plug-in für Windows	8145 (HTTPS), bidirektional, anpassbar
ONTAP-Cluster oder SVM-Kommunikations-Port	443 (HTTPS), bidirektional; 80 (HTTP), bidirektional Der Port wird für die Kommunikation zwischen dem SnapCenter-Serverhost, dem Plug-in-Host und der SVM oder dem ONTAP-Cluster verwendet.

Anforderungen des SnapCenter Plug-ins für Microsoft SQL Server

Sie sollten einen Benutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host haben. Wenn Sie Cluster-Nodes verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster.

Sie sollten einen Benutzer mit sysadmin-Berechtigungen auf dem SQL Server haben. Das Plug-in verwendet Microsoft VDI Framework, für das ein Sysadmin-Zugriff erforderlich ist.

Wenn Sie SnapManager für Microsoft SQL Server verwenden und Daten von SnapManager für Microsoft SQL Server in SnapCenter importieren möchten, lesen Sie "Importieren Sie archivierte Backups"

Installieren Sie SnapCenter Server für Microsoft SQL Server

Enthält eine zusammengefasste Reihe von Installationsanweisungen für die Installation des SnapCenter-Servers für Microsoft SQL Server.

Schritt 1: Downloaden und installieren Sie SnapCenter Server

1. Laden Sie das Installationspaket für den SnapCenter-Server von herunter "NetApp Support Website" Doppelklicken Sie anschließend auf die exe.

   Nach Beginn der Installation werden alle Vorabprüfungen durchgeführt und wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt. Sie können die Warnmeldungen ignorieren und mit der Installation fortfahren. Fehler sollten jedoch behoben werden.

2. Überprüfen Sie die für die SnapCenter Server-Installation erforderlichen vordefinierten Werte, und ändern Sie sie, falls erforderlich.

   Sie müssen das Kennwort für die MySQL Server Repository-Datenbank nicht angeben. Während der Installation des SnapCenter Servers wird das Passwort automatisch generiert.

   Das Sonderzeichen „%“ wird im benutzerdefinierten Pfad für die Installation nicht unterstützt. Wenn Sie „%“ in den Pfad aufnehmen, schlägt die Installation fehl.

3. Klicken Sie Auf **Jetzt Installieren**.

Schritt 2: Melden Sie sich bei SnapCenter an

1. Starten Sie SnapCenter über eine Verknüpfung auf dem Host-Desktop oder über die von der Installation bereitgestellte URL (*https://server:8146* für Standardport 8146, auf dem SnapCenter-Server installiert ist).

2. Geben Sie die Anmeldeinformationen ein.

   Verwenden Sie für ein integriertes Benutzerbenutzerformat für den Domänenadministrator: *NetBIOS\<username>* oder *<username>@<Domain>* oder *<DomainFQDN>\<username>*.

   Verwenden Sie für ein integriertes lokales Format für den Admin-Benutzernamen *<username>*.

3. Klicken Sie Auf **Anmelden**.

Schritt 3: Fügen Sie eine Controller-basierte SnapCenter Standard-Lizenz hinzu

1. Loggen Sie sich über die ONTAP-Befehlszeile beim Controller ein und geben Sie Folgendes ein:

   ```
   system license add -license-code <license_key>
   ```

2. Überprüfen Sie die Lizenz:

   ```
   license show
   ```

Schritt 4: Fügen Sie eine kapazitätsbasierte SnapCenter Lizenz hinzu

1. Klicken Sie im linken Fensterbereich der SnapCenter-Benutzeroberfläche auf **Einstellungen > Software**, und klicken Sie dann im Abschnitt Lizenz auf **+**.
2. Wählen Sie eine von zwei Methoden für den Erwerb der Lizenz aus:
   - Geben Sie Ihre Anmeldedaten für die NetApp Support Site ein, um Lizenzen zu importieren.
   - Navigieren Sie zum Speicherort der NetApp Lizenzdatei und klicken Sie auf **Öffnen**.
3. Verwenden Sie auf der Seite Benachrichtigungen des Assistenten den standardmäßigen Kapazitätsschwellenwert von 90 Prozent.
4. Klicken Sie Auf **Fertig Stellen**.

Schritt 5: Einrichten von Verbindungen zum Storage-System

1. Klicken Sie im linken Fensterbereich auf **Speichersysteme > Neu**.
2. Führen Sie auf der Seite Add Storage System folgende Schritte aus:
   a. Geben Sie den Namen oder die IP-Adresse des Speichersystems ein.
   b. Geben Sie die Anmeldeinformationen ein, die für den Zugriff auf das Speichersystem verwendet werden.
   c. Aktivieren Sie die Kontrollkästchen, um EMS (Event Management System) und AutoSupport zu aktivieren.
3. Klicken Sie auf **Mehr Optionen**, wenn Sie die Standardwerte ändern möchten, die Plattform, Protokoll, Port und Timeout zugewiesen sind.
4. Klicken Sie Auf **Absenden**.

Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server

Enthält einen zusammengefassten Satz von Installationsanweisungen für das SnapCenter-Plug-in für Microsoft SQL Server.

Schritt 1: Richten Sie Run As Credentials ein, um das Plug-in für Microsoft SQL Server zu installieren

1. Klicken Sie im linken Fensterbereich auf **Einstellungen > Anmeldeinformationen > Neu**.
2. Geben Sie die Anmeldeinformationen ein.

   Verwenden Sie für ein integriertes Benutzerbenutzerformat für den Domänenadministrator: *NetBIOS\<username>* oder *<username>@<Domain>* oder *<DomainFQDN>\<username>*.

   Verwenden Sie für ein integriertes lokales Format für den Admin-Benutzernamen *<username>*.

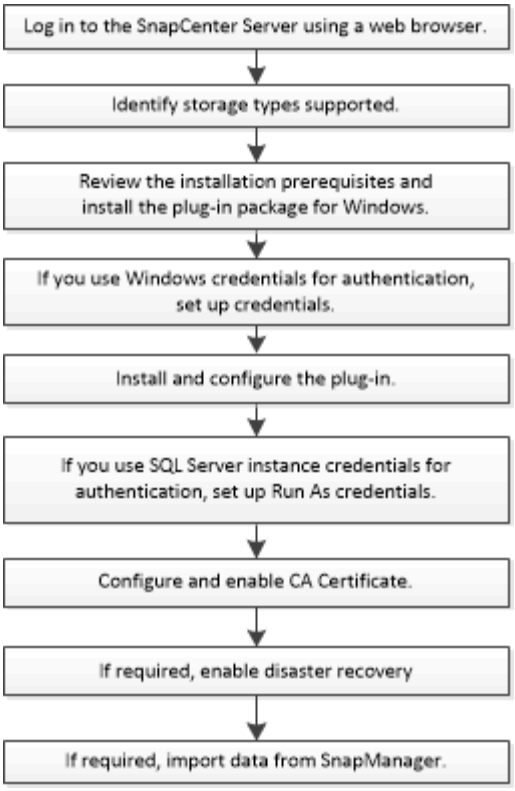
Schritt 2: Fügen Sie einen Host hinzu und installieren Sie das Plug-in für Microsoft SQL Server

1. Klicken Sie im linken Fensterbereich der SnapCenter-Benutzeroberfläche auf **Hosts > verwaltete Hosts > Hinzufügen**.
2. Führen Sie auf der Seite Hosts des Assistenten folgende Schritte durch:
   a. Host-Typ: Wählen Sie den Windows-Host-Typ.
   b. Hostname: Verwenden Sie den SQL-Host oder geben Sie den FQDN eines dedizierten Windows-Hosts an.
   c. Anmeldedaten: Wählen Sie den gültigen Namen der Anmeldeinformationen des von Ihnen erstellten Hosts aus oder erstellen Sie neue Anmeldedaten.
3. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die Option **Microsoft SQL Server** aus.
4. Klicken Sie auf **Weitere Optionen**, um die folgenden Details anzugeben:
   a. Port: Behalten Sie entweder die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an.
   b. Installationspfad: Der Standardpfad ist *C:\Programme\NetApp\SnapCenter*. Optional können Sie den Pfad anpassen.
   c. Fügen Sie alle Hosts im Cluster hinzu: Aktivieren Sie dieses Kontrollkästchen, wenn Sie SQL im WSFC verwenden.
   d. Prüfung vor der Installation überspringen: Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben, oder Sie nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
5. Klicken Sie Auf **Absenden**.

Bereiten Sie die Installation des SnapCenter-Plug-ins für Microsoft SQL Server vor

Installations-Workflow für das SnapCenter Plug-in für Microsoft SQL Server

Sie sollten das SnapCenter Plug-in für Microsoft SQL Server installieren und einrichten, wenn Sie SQL Server-Datenbanken schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter-Plug-ins für Microsoft SQL Server

Bevor Sie einen Host hinzufügen und die Plug-ins-Pakete installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen über einen Benutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen über einen Benutzer mit sysadmin-Berechtigungen auf dem SQL Server verfügen.

  Das SnapCenter Plug-in für Microsoft SQL Server verwendet Microsoft VDI Framework, für das ein sysadmin-Zugriff erforderlich ist.

  "Microsoft Support-Artikel 2926557: Für Backup- und Restore-Vorgänge für SQL Server VDI sind Sysadmin-Berechtigungen erforderlich"

- 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.
- Wenn SnapManager für Microsoft SQL Server installiert ist, müssen Sie den Service und die Zeitpläne angehalten oder deaktiviert haben.

  Wenn Sie Backup- oder Klonaufträge in SnapCenter importieren möchten, deinstallieren Sie SnapManager für Microsoft SQL Server nicht.

- Der Host muss auf den vollständig qualifizierten Domänennamen (FQDN) vom Server resolable sein.

  Wenn die Host-Datei geändert wird, damit sie resolable ist, und wenn sowohl der Kurzname als auch der FQDN in der Datei Hosts angegeben sind, erstellen Sie einen Eintrag in der Datei SnapCenter Hosts im folgenden Format: <ip_Address> <Host_fqdn> <Host_Name>

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
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.

Element	Anforderungen
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 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". Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-ins-Paket für Windows ein

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.

Bevor Sie beginnen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.
- Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.
- SQL-Authentifizierung auf Windows Hosts

  Nach der Installation von Plug-ins müssen Sie SQL-Anmeldedaten einrichten.

  Wenn Sie SnapCenter-Plug-in für Microsoft SQL Server bereitstellen, müssen Sie nach der Installation von Plug-ins SQL-Anmeldedaten einrichten. Richten Sie eine Anmeldedaten für einen Benutzer mit den sysadmin-Berechtigungen von SQL Server ein.

  Die SQL-Authentifizierungsmethode authentifiziert sich anhand einer SQL Server-Instanz. Das bedeutet, dass eine SQL Server-Instanz in SnapCenter erkannt werden muss. Daher müssen Sie vor dem Hinzufügen von SQL-Anmeldeinformationen einen Host hinzufügen, Plug-in-Pakete installieren und Ressourcen aktualisieren. Sie benötigen die SQL Server-Authentifizierung für Vorgänge wie Planung oder Ermittlung von Ressourcen.

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.
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domain-Administrator Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • 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.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten. Wenn Sie den SQL-Authentifizierungsmodus auswählen, müssen Sie auch die SQL-Serverinstanz und den Host angeben, auf dem sich die SQL-Instanz befindet.

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 Wartung der Anmeldeinformationen zuweisen.

Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource

Sie können Anmeldedaten für die Durchführung von Datensicherungsjobs für einzelne SQL Server-Ressourcen für jeden Benutzer konfigurieren. Sie können die Anmeldeinformationen zwar global konfigurieren, aber dies ist möglicherweise nur für eine bestimmte Ressource erforderlich.

Über diese Aufgabe

- Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie vor der Installation von Plug-ins die Anmeldedaten einrichten.

  Wenn Sie jedoch eine SQL Server-Instanz zur Authentifizierung verwenden, müssen Sie nach der Installation von Plug-ins die Anmeldeinformationen hinzufügen.

- Wenn Sie die SQL-Authentifizierung beim Einrichten der Anmeldeinformationen aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Farbvorhängeschloss-Symbol angezeigt.

  Wenn das Vorhängeschloss-Symbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, um die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzuzufügen.

- Sie müssen die Anmeldedaten einem Benutzer mit rollenbasierter Zugriffssteuerung (Role-Based Access Control, RBAC) ohne sysadmin-Zugriff zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Die Anmeldeinformationen werden einer SQL-Instanz zugewiesen.
  - Die SQL Instanz oder der Host wird einem RBAC-Benutzer zugewiesen.

    Der Benutzer muss sowohl über die Ressourcengruppe als auch über die Sicherungsberechtigungen verfügen.

Schritt 1: Anmeldeinformationen hinzufügen und konfigurieren

1. Wählen Sie im linken Navigationsbereich **Einstellungen**.
2. Wählen Sie auf der Seite Einstellungen die Option **Credential** aus.
   a. Um eine neue Anmeldeinformation hinzuzufügen, wählen Sie **Neu**.
   b. Konfigurieren Sie auf der Seite Anmeldeinformationen:

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 ein, der für die SQL Server-Authentifizierung verwendet wird. • 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 Administratorgruppe gehört, wenn das Benutzerkonto über erweiterte Berechtigungen oder den Benutzer verfügt Die Zugriffskontrollfunktion ist auf dem Hostsystem deaktiviert. Das zulässige Format für das Feld **Benutzername** lautet: *Username*
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den SQL Server-Authentifizierungsmodus aus. Sie können auch die Windows-Authentifizierung auswählen, wenn der Windows-Benutzer sysadmin-Berechtigungen auf dem SQL-Server hat.
Host	Wählen Sie den Host aus.
SQL Server Instanz	Wählen Sie die SQL Server-Instanz aus.

c. Wählen Sie **OK**, um die Zugangsdaten hinzuzufügen.

Schritt 2: Instanzen konfigurieren

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Instanz** aus.
   a. Wählen Sie [Filtersymbol]Und wählen Sie dann den Hostnamen aus, um die Instanzen zu filtern.
   b. Wählen Sie [Filtersymbol] Um den Filterbereich zu schließen.
3. Schützen Sie die Instanz auf der Seite Instance Protect, und wählen Sie bei Bedarf **Credentials konfigurieren**.

   Wenn der beim SnapCenter-Server angemeldete Benutzer keinen Zugriff auf das SnapCenter-Plugin für Microsoft SQL-Server hat, muss der Benutzer die Anmeldeinformationen konfigurieren.

   Die Anmeldeinformationsoption gilt nicht für Datenbanken und Verfügbarkeitsgruppen.

4. Wählen Sie **Ressourcen Aktualisieren**.

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.

Bevor Sie beginnen

- 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.

Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server

Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Windows

Sie müssen die Seite SnapCenter **Add Host** verwenden, um Hosts hinzuzufügen und das Plug-ins-Paket zu installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Bevor Sie beginnen

- 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, sollten Sie UAC auf dem Host deaktivieren, wenn Sie keine integrierten Anmeldeinformationen angeben.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange in Betrieb ist.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

"Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2012 oder höher für SQL"

Über diese Aufgabe

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

Sie können einen Host hinzufügen und die Plug-in-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie die Plug-ins auf einem Cluster oder Windows Server Failover Clustering (WSFC) installieren, werden die Plug-ins auf allen Knoten des Clusters installiert.

Informationen zum Verwalten von Hosts finden Sie unter "Management von Hosts".

Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie Windows als Hosttyp aus. Der SnapCenter-Server fügt den Host hinzu und installiert dann das Plug-in für Windows, wenn das Plug-in nicht bereits auf dem Host installiert ist. Wenn Sie auf der Seite Plug-ins die Option Microsoft SQL Server auswählen, installiert der SnapCenter-Server das Plug-in für SQL Server.
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. Die IP-Adresse wird nur für nicht vertrauenswürdige Domänenhosts unterstützt, wenn sie auf den FQDN auflöst. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • WSFC Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.

Für dieses Feld…	Tun Sie das…
Anmeldedaten	Wählen Sie den Anmeldeinformationsnamen aus, den Sie erstellt haben oder neue Anmeldeinformationen erstellen. 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.

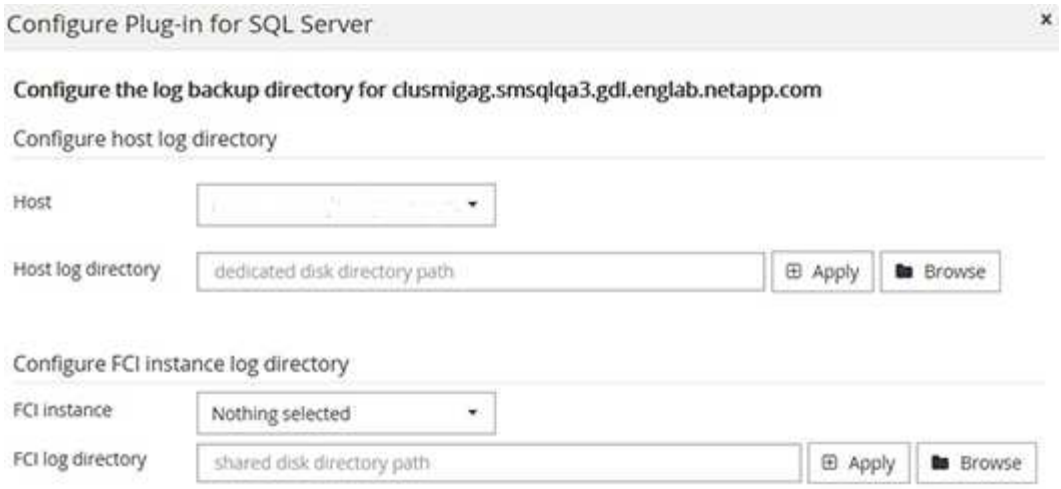
5. Wählen Sie im Abschnitt **Plug-ins zur Installation auswählen** die zu installierenden Plug-ins aus.
6. Wählen Sie **Weitere Optionen**.

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.
Installationspfad	Der Standardpfad ist C:\Programmdateien\NetApp\SnapCenter. Optional können Sie den Pfad anpassen.

Für dieses Feld…	Tun Sie das…
Fügen Sie alle Hosts im Cluster hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einer WSFC- oder SQL-Verfügbarkeitsgruppe hinzuzufügen. Sie sollten alle Cluster-Knoten hinzufügen, indem Sie das entsprechende Kontrollkästchen Cluster in der GUI aktivieren, wenn Sie mehrere verfügbare SQL-Verfügbarkeitsgruppen in einem Cluster verwalten und identifizieren möchten.
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 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€. Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und sys Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

7. Wählen Sie **Senden**.
8. Wählen Sie für das SQL-Plug-in den Host aus, um das Protokollverzeichnis zu konfigurieren.
   a. Wählen Sie **Protokollverzeichnis konfigurieren** und wählen Sie auf der Seite Hostprotokoll konfigurieren **Durchsuchen** aus, und führen Sie die folgenden Schritte aus:

      Nur NetApp LUNs (Laufwerke) werden zur Auswahl aufgeführt. SnapCenter sichert und repliziert im Rahmen des Backup-Vorgangs das Host-Protokollverzeichnis.



i. Wählen Sie den Laufwerksbuchstaben oder den Bereitstellungspunkt auf dem Host aus, auf dem das Hostprotokoll gespeichert werden soll.

ii. Wählen Sie ggf. ein Unterverzeichnis aus.

iii. Wählen Sie **Speichern**.

9. Wählen Sie **Senden**.

   Wenn Sie das Kontrollkästchen **Vorabprüfungen** nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob er 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.

10. Überwachen Sie den Installationsfortschritt.

Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server mithilfe von Cmdlets auf mehreren Remote Hosts

Sie können das SnapCenter-Plug-in für Microsoft SQL Server auf mehreren Hosts gleichzeitig installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

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 SnapCenter-Plug-in für Microsoft SQL Server auf mehreren Remote-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 bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

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

Installieren Sie das SnapCenter-Plug-in für Microsoft SQL Server im Hintergrund über die Befehlszeile

Sie sollten das SnapCenter Plug-in für Microsoft SQL Server über die Benutzeroberfläche von SnapCenter installieren. Wenn Sie jedoch aus irgendeinem Grund nicht in der Lage sind, das Installationsprogramm Plug-in für SQL Server unbeaufsichtigt im Silent-Modus von der Windows-Befehlszeile aus auszuführen.

Bevor Sie beginnen

- Vor der Installation müssen Sie die frühere Version des SnapCenter-Plug-ins für Microsoft SQL Server löschen.

  Weitere Informationen finden Sie unter "So installieren Sie ein SnapCenter-Plug-in manuell und direkt über den Plug-in-Host".

Schritte

1. Überprüfen Sie, ob der Ordner C:\temp auf dem Plug-in-Host vorhanden ist und der angemeldete Benutzer vollen Zugriff darauf hat.
2. Laden Sie das Plug-in für SQL Server unter C:\ProgramData\NetApp\SnapCenter\Package Repository herunter.

   Auf diesen Pfad kann von dem Host zugegriffen werden, auf dem der SnapCenter-Server installiert ist.

3. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-in installieren möchten.
4. Navigieren Sie von einer Windows-Eingabeaufforderung auf dem lokalen Host zum Verzeichnis, in das Sie die Plug-in-Installationsdateien gespeichert haben.
5. Installieren Sie das Plug-in für SQL Server:

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

   Ersetzen Sie die Platzhalterwerte durch Ihre Daten

   - Debug_Log_Path ist der Name und der Speicherort der Protokolldatei für das Installationsprogramm der Suite.

- Log_Path ist der Speicherort der Installationsprotokolle der Plug-in-Komponenten (SCW, SCSCSQL und SMCore).
- Num ist der Port, an dem SnapCenter mit SMCore kommuniziert
- Install_Directory_Path ist das Installationsverzeichnis des Host-Plug-in-Pakets.
- Domain\Administrator ist das SnapCenter-Plug-in für Microsoft Windows-Webservice-Konto.
- Passwort ist das Passwort für das SnapCenter-Plug-in für Microsoft Windows Webservice-Konto.

```
"snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCSQL
```

Bei der Installation von Plug-in für SQL Server müssen alle Parameter beachtet werden.

6. Überwachen Sie den Windows Task Scheduler, die Hauptinstallationsprotokolldatei C:\Installdebug.log und die zusätzlichen Installationsdateien in C:\Temp.
7. Überwachen Sie das Verzeichnis %temp%, um zu überprüfen, ob die msiexe.exe Installationsprogramme fehlerfrei installiert werden.

Die Installation des Plug-ins für SQL Server registriert das Plug-in auf dem Host und nicht auf dem SnapCenter-Server. Sie können das Plug-in auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Nach dem Hinzufügen des Hosts wird das Plug-in automatisch erkannt.

Überwachen Sie den Status der Installation des Plug-ins für SQL Server

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. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden, gehen Sie wie folgt vor:
   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.

CA Certificate RSA-Schlüssel sollten mindestens 3072 Bit lang sein.

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 vor dem Erwerb des Zertifikats das Feld alternativer Antragstellername (SAN) ausfüllen. 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 hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate 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 und *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

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.

Bevor Sie beginnen

- 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**.

Nachdem Sie fertig sind

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.

Konfiguration der Disaster Recovery

Disaster Recovery eines SnapCenter Plug-ins für SQL Server

Wenn das SnapCenter-Plug-in für SQL Server ausfällt, führen Sie die folgenden Schritte aus, um zu einem anderen SQL-Host zu wechseln und die Daten wiederherzustellen.

Bevor Sie beginnen

- Der sekundäre Host sollte das gleiche Betriebssystem, die gleiche Anwendung und den gleichen Hostnamen wie der primäre Host haben.
- Schieben Sie das SnapCenter-Plug-in für SQL Server auf einen anderen Host, indem Sie die Seite **Add Host** oder **Modify Host** verwenden. Siehe "Management von Hosts" Finden Sie weitere Informationen.

Schritte

1. Wählen Sie den Host auf der Seite **Hosts** aus, um das SnapCenter-Plug-in für SQL Server zu ändern und zu installieren.
2. (Optional) Ersetzen Sie das SnapCenter-Plug-in für SQL Server-Konfigurationsdateien vom Disaster Recovery-Backup (DR) auf die neue Maschine.
3. Importieren Sie Windows- und SQL-Zeitpläne aus dem SnapCenter-Plug-in für SQL Server-Ordner aus dem DR-Backup.

Verwandte Informationen

Siehe "Disaster Recovery-APIs" Video:

Storage Disaster Recovery (DR) für SnapCenter Plug-in für SQL Server

Sie können das SnapCenter Plug-in für SQL Server Storage wiederherstellen, indem Sie den DR-Modus für Storage auf der Seite Globale Einstellungen aktivieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass sich die Plug-ins im Wartungsmodus befinden.
- SnapMirror/SnapVault Beziehung aufheben "SnapMirror Beziehungen unterbrechen"
- Verbinden Sie die LUN aus dem sekundären Server mit dem gleichen Laufwerksbuchstaben.
- Stellen Sie sicher, dass alle Laufwerke mit denselben Laufwerksbuchstaben verbunden sind, die vor der DR verwendet wurden.
- MSSQL-Serverdienst neu starten.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

Über diese Aufgabe

Disaster Recovery (DR) wird auf VMDK- und RDM-Konfigurationen nicht unterstützt.

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **Disaster Recovery**.
2. Wählen Sie **Disaster Recovery Aktivieren**.
3. Klicken Sie Auf **Anwenden**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Monitor** > **Jobs** klicken.

Nachdem Sie fertig sind

- Falls neue Datenbanken nach dem Failover erstellt werden, befinden sich die Datenbanken außerhalb des DR-Modus.

  Die neuen Datenbanken laufen weiterhin so wie vor dem Failover.

- Die neuen Backups, die im DR-Modus erstellt wurden, werden auf der Topologieseite unter SnapMirror oder SnapVault (sekundär) aufgeführt.

  Neben den neuen Backups wird ein „i“-Symbol angezeigt, das angibt, dass diese Backups während des DR-Modus erstellt wurden.

- Sie können das SnapCenter-Plug-in für SQL Server Backups löschen, die während des Failovers erstellt wurden, entweder mit der UI oder mit dem folgenden Cmdlet: `Remove-SmBackup`
- Wenn sich nach dem Failover einige der Ressourcen nicht im DR-Modus befinden sollen, verwenden Sie das folgende Cmdlet: `Remove-SmResourceDRMode`

  Weitere Informationen finden Sie im "SnapCenter Software Cmdlet Referenzhandbuch".

- SnapCenter Server verwaltet die einzelnen Storage-Ressourcen (SQL-Datenbanken) im DR- oder nicht-DR-Modus, jedoch nicht die Ressourcengruppe mit Storage-Ressourcen, die sich im DR-Modus oder nicht im DR-Modus befinden.

Failback von sekundärem SnapCenter Plug-in für SQL Server Storage auf den Primärspeicher

Nachdem das SnapCenter Plug-in für den primären SQL Server Storage wieder online ist, sollten Sie ein Failback auf den primären Storage durchführen.

Bevor Sie beginnen

- Setzen Sie das SnapCenter-Plug-in für SQL Server auf der Seite Managed Hosts in den **Maintenance** -Modus.
- Trennen Sie den sekundären Speicher vom Host, und stellen Sie eine Verbindung zum primären Speicher her.
- Für ein Failback auf den primären Storage stellen Sie sicher, dass die Beziehungsrichtung vor dem Failover unverändert bleibt, indem Sie den umgekehrten Resync-Vorgang durchführen.

  Um die Rollen des primären und sekundären Speichers nach der umgekehrten Resynchronisierung beizubehalten, führen Sie den umgekehrten Resynchronisierungsvorgang erneut aus.

  Weitere Informationen finden Sie unter "Spiegelbeziehungen neu synchronisieren"
- MSSQL-Serverdienst neu starten.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

> Beim Failover oder Failback des Plug-ins wird der Gesamtstatus des Plug-ins nicht sofort aktualisiert. Der Gesamtstatus von Host und Plug-in wird während der nachfolgenden Aktualisierung des Hosts aktualisiert.

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **Disaster Recovery**.
2. Deaktivieren Sie Die Option * Disaster Recovery Aktivieren*.
3. Klicken Sie Auf **Anwenden**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Monitor** > **Jobs** klicken.

Nachdem Sie fertig sind

Sie können das SnapCenter-Plug-in für SQL Server Backups löschen, die während des Failovers erstellt wurden, entweder mit der UI oder mit dem folgenden Cmdlet: `Remove-SmDRFailoverBackups`

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 Microsoft SQL Server

Bevor Sie mit der Verwendung des Plug-ins für SQL Server beginnen, muss der SnapCenter-Administrator SnapCenter Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich bei SnapCenter an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen oder zuweisen und Anmeldedaten erstellen.

  SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss über einen eindeutigen Namen verfügen.

- Fügen Sie Hosts hinzu, installieren Sie die Plug-ins, ermitteln Sie die Ressourcen und konfigurieren Sie die Plug-ins.
- Verschieben Sie eine vorhandene Microsoft SQL Server-Datenbank von einer lokalen Festplatte auf eine NetApp LUN oder umgekehrt mit Invoke-SmConfigureResources.

  Informationen zum Ausführen des Cmdlet finden Sie im "SnapCenter Software Cmdlet Referenzhandbuch"

- Wenn Sie SnapCenter Server zum Schutz von SQL Datenbanken nutzen, die sich auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren. Die Dokumentation zum SnapCenter Plug-in für VMware vSphere enthält weitere Informationen.

  "Dokumentation zum SnapCenter Plug-in für VMware vSphere"

- Führen Sie die Host-seitige Storage-Bereitstellung mit dem SnapCenter Plug-in für Microsoft Windows durch.
- Richten Sie SnapMirror- und SnapVault-Beziehungen ein, falls Sie eine Backup-Replizierung möchten.

Weitere Informationen finden Sie unter SnapCenter Installationsinformationen.

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere,

das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für SnapCenter 4.3.x-Anwender enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Filesysteme mithilfe des Linux-basierten SnapCenter Plug-ins für VMware vSphere Virtual Appliance (Open Virtual Appliance Format).

"Dokumentation zum SnapCenter Plug-in für VMware vSphere"

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SQL Server verwendet werden

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 Datenbanken, Datenbankinstanzen oder Microsoft SQL Server Verfügbarkeitsgruppen, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster.

  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.

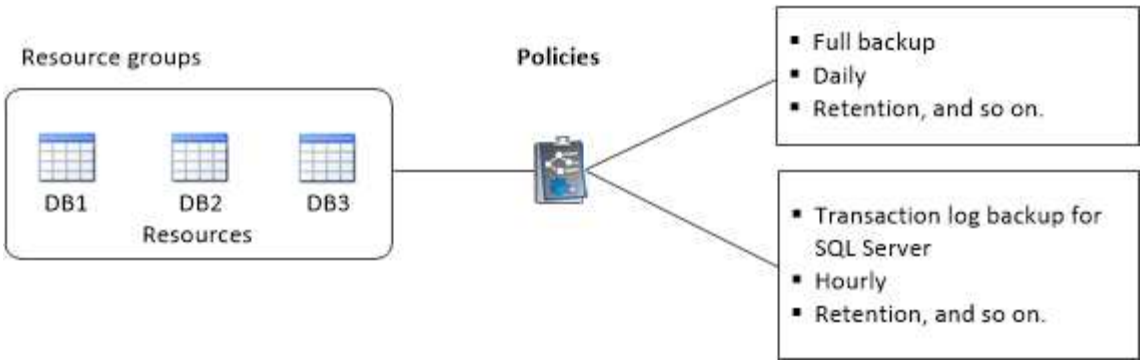
  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, die Aufbewahrung von Kopien, die Replizierung, Skripte und andere Merkmale 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.

Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme des Hosts enthält. 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 Ressourcengruppe so konfigurieren, dass sie täglich ein vollständiges Backup durchführt, und einen anderen Zeitplan, der stündlich Protokoll-Backups durchführt.

Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe

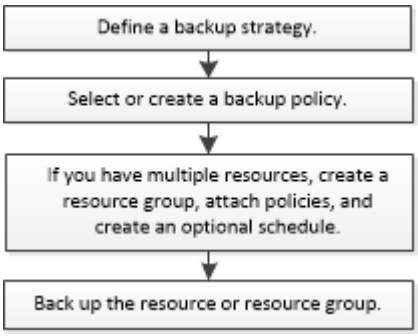
Backup-Workflow

Wenn Sie das SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung installieren, können Sie mit SnapCenter die SQL Server Ressourcen sichern.

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden.

Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden.

Der folgende Workflow zeigt die Reihenfolge, in der Sie die Backup-Vorgänge durchführen müssen:



Die Optionen „Jetzt sichern“, „Wiederherstellen“, „Backups verwalten“ und „Klonen“ auf der Seite „Ressourcen“ werden deaktiviert, wenn Sie eine nicht von NetApp stammende LUN, eine beschädigte Datenbank oder eine wiederhergestellte Datenbank auswählen.

Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder in der "SnapCenter Software Cmdlet Referenzhandbuch"

Wie SnapCenter Datenbanken sichert

SnapCenter nutzt Snapshot-Kopiertechnologie für das Backup der SQL Server Datenbanken, die sich auf LUNs oder VMDKs befinden. SnapCenter erstellt das Backup, indem Snapshot Kopien der Datenbanken erstellt werden.

Wenn Sie auf der Seite Ressourcen eine Datenbank für ein vollständiges Datenbank-Backup auswählen, wählt

SnapCenter automatisch alle anderen Datenbanken aus, die sich auf demselben Storage Volume befinden. Wenn die LUN oder VMDK nur eine einzige Datenbank speichert, können Sie die Datenbank einzeln löschen oder erneut auswählen. Wenn die LUN oder VMDK mehrere Datenbanken enthält, müssen Sie die Datenbanken als Gruppe löschen oder neu auswählen.

Alle Datenbanken, die sich auf einem einzelnen Volume befinden, werden mithilfe von Snapshot-Kopien gleichzeitig gesichert. Wenn die maximale Anzahl gleichzeitiger Backup-Datenbanken 35 beträgt und mehr als 35 Datenbanken in einem Storage Volume residieren, entspricht die Gesamtzahl der erstellten Snapshot-Kopien der Anzahl der Datenbanken, die durch 35 geteilt werden.

Sie können die maximale Anzahl von Datenbanken für jede Snapshot-Kopie in der Backup-Richtlinie konfigurieren.

Wenn SnapCenter eine Snapshot Kopie erstellt, wird das gesamte Storage-System-Volume in der Snapshot Kopie erfasst. Das Backup ist jedoch nur für den SQL-Hostserver gültig, für den das Backup erstellt wurde.

Wenn sich Daten von anderen SQL Host Servern auf demselben Volume befinden, können diese Daten nicht aus der Snapshot Kopie wiederhergestellt werden.

Weitere Informationen

"Sichern Sie Ressourcen mit PowerShell cmdlets"

"Fehler beim Quiesce oder Gruppieren von Ressourcen"

Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind

Ressourcen sind die Datenbanken, Applikationsinstanzen, Verfügbarkeitsgruppen und ähnliche Komponenten, die von den installierten Plug-ins gewartet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsjobs ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie zur Verfügung haben. Das ermitteln der verfügbaren Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen.
- Um die Microsoft SQL-Datenbanken zu ermitteln, sollte eine der folgenden Bedingungen erfüllt sein.
  - Der Benutzer, der zum Hinzufügen des Plug-in-Hosts zum SnapCenter Server verwendet wurde, sollte über die erforderlichen Berechtigungen (Sysadmin) auf dem Microsoft SQL Server verfügen.
  - Wenn die oben genannte Bedingung nicht erfüllt ist, sollten Sie im SnapCenter-Server den Benutzer konfigurieren, der über die erforderlichen Berechtigungen (sysadmin) auf dem Microsoft SQL-Server verfügt. Der Benutzer sollte auf der Ebene der Microsoft SQL Server-Instanz konfiguriert werden und der Benutzer kann ein SQL- oder Windows-Benutzer sein.
- Um die Microsoft SQL-Datenbanken in einem Windows-Cluster zu ermitteln, müssen Sie den TCP/IP-Port (Failover Cluster Instance) für die Failover-Cluster-Instanz (FCI) freigeben.
- Wenn Datenbanken auf VMware RDM-LUNs oder VMDKs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.

Weitere Informationen finden Sie unter "Implementieren Sie das SnapCenter Plug-in für VMware vSphere"

- Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und System Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

Über diese Aufgabe

Datenbanken können nicht gesichert werden, wenn die Option **Gesamtstatus** auf der Seite Details auf nicht verfügbar für Backups eingestellt ist. Die Option **Gesamtstatus** ist für die Sicherung auf nicht verfügbar eingestellt, wenn eine der folgenden Optionen zutrifft:

- Datenbanken sind nicht auf einer NetApp LUN.
- Datenbanken befinden sich nicht im normalen Zustand.

  Datenbanken befinden sich nicht im normalen Zustand, wenn sie offline sind, sie wiederherstellen, ausstehende Wiederherstellung, Verdacht usw.

- Datenbanken verfügen über unzureichende Berechtigungen.

  Wenn ein Benutzer beispielsweise nur Zugriff auf die Datenbank hat, können Dateien und Eigenschaften der Datenbank nicht identifiziert werden und können daher nicht gesichert werden.

SnapCenter kann nur die primäre Datenbank sichern, wenn Sie eine Verfügbarkeitsgruppe auf der SQL Server Standard Edition haben.

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 Dropdown-Liste **Ansicht** * oder **Instanz** oder **Verfügbarkeitsgruppe** aus.

   Klicken Sie Auf Und wählen Sie den Hostnamen und die SQL Server-Instanz aus, um die Ressourcen zu filtern. Sie können dann auf klicken Um den Filterbereich zu schließen.

3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden in den SnapCenter-Serverbestand aktualisiert.

   Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Host- oder Cluster-Name, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn die Datenbank auf Storage anderer Anbieter liegt, `Not available for backup` Wird in der Spalte **Gesamtstatus** angezeigt.

     Sie können keine Datensicherungsvorgänge für eine Datenbank ausführen, die sich auf einem Storage-System anderer Anbieter befindet.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, `Not protected` Wird in der Spalte **Gesamtstatus** angezeigt.

- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, wird auf der Benutzeroberfläche angezeigt `Backup not run` Meldung in der Spalte **Gesamtstatus**.
- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn das Backup für die Datenbank ausgelöst wird, wird die Benutzeroberfläche angezeigt `Backup succeeded` Meldung in der Spalte **Gesamtstatus**.

Wenn Sie beim Einrichten der Anmeldeinformationen eine SQL-Authentifizierung aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Vorhängeschloss-Symbol angezeigt. Wenn das Vorhängeschloss-Symbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, damit die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzugefügt werden kann.

1. Nachdem der SnapCenter-Administrator einem RBAC-Benutzer die Ressourcen zuweist, muss sich der RBAC-Benutzer anmelden und auf **Ressourcen aktualisieren** klicken, um die neuesten **Gesamtstatus** der Ressourcen anzuzeigen.

Migrieren von Ressourcen auf ein NetApp Storage-System

Nachdem Sie Ihr NetApp Storage-System mit dem SnapCenter Plug-in für Microsoft Windows bereitgestellt haben, können Sie Ihre Ressourcen auf das NetApp Storage-System oder von einer NetApp LUN zu einer anderen NetApp LUN migrieren. Hierzu stehen entweder die SnapCenter Graphical User Interface (GUI) oder die PowerShell Commandlets zur Verfügung.

Bevor Sie beginnen

- Sie müssen dem SnapCenter-Server Storage-Systeme hinzugefügt haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. In den folgenden Informationen werden einige der Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

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 Dropdown-Liste **Ansicht** die Option **Datenbank** oder **Instanz** aus.
3. Wählen Sie entweder die Datenbank oder die Instanz aus der Liste aus und klicken Sie auf **Migrieren**.
4. Führen Sie auf der Seite Ressourcen die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Datenbankname (optional)	Wenn Sie eine Instanz für die Migration ausgewählt haben, müssen Sie die Datenbanken dieser Instanz aus der Dropdown-Liste **Databases** auswählen.

Für dieses Feld…	Tun Sie das…
Wählen Sie Reiseziele	Wählen Sie den Zielspeicherort für Daten- und Protokolldateien aus. Die Daten- und Log-Dateien werden in den Daten- bzw. Log-Ordner unter dem ausgewählten NetApp-Laufwerk verschoben. Wenn kein Ordner in der Ordnerstruktur vorhanden ist, wird ein Ordner erstellt und die Ressource migriert.
Details zur Datenbankdatei anzeigen (optional)	Wählen Sie diese Option aus, wenn Sie mehrere Dateien einer einzigen Datenbank migrieren möchten. Diese Option wird nicht angezeigt, wenn Sie die Ressource **Instanz** auswählen.
Optionen	Wählen Sie **Kopie der migrierten Datenbank am ursprünglichen Speicherort löschen**, um die Kopie der Datenbank aus der Quelle zu löschen. Optional: **UPDATE-STATISTIKEN auf Tabellen AUSFÜHREN, bevor Sie die Datenbank entfernen**.

5. Führen Sie auf der Seite Verifizieren die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Optionen Zur Datenbankkonsistenzprüfung	Wählen Sie **vorher ausführen** aus, um die Integrität der Datenbank vor der Migration zu überprüfen. Wählen Sie **nach** ausführen, um die Integrität der Datenbank nach der Migration zu überprüfen.

Für dieses Feld…	Tun Sie das…
DBCC CHECKDB Optionen	• Wählen Sie die Option **PHYSICAL_ONLY**, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um zerrissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen. • Wählen Sie die Option **NO_INFOMSGS**, um alle Informationsmeldungen zu unterdrücken. • Wählen Sie die Option **ALL_ERRORMSGS** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen. • Wählen Sie die Option **NOINDEX** aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten. Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen. Sie können diese Option auswählen, um die Ausführungszeit zu verkürzen. • Wählen Sie die Option **TABLOCK**, um die Prüfungen zu begrenzen und Sperren zu erhalten, anstatt eine interne Snapshot-Kopie der Datenbank zu verwenden.

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

Erstellen von Backup-Richtlinien für SQL Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, bevor Sie SnapCenter zum Sichern von SQL Server-Ressourcen verwenden. Alternativ können Sie beim Erstellen einer Ressourcengruppen oder beim Sichern einer einzelnen Ressource eine Backup-Richtlinie erstellen.

Bevor Sie beginnen

- Sie müssen Ihre Datensicherungsstrategie definiert haben.
- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Storage-System abschließen.
- Sie müssen das Host-Protokollverzeichnis für die Protokollsicherung konfiguriert haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

- Wenn Sie Snapshot Kopien in eine Spiegelung oder einen Vault replizieren, muss der SnapCenter Administrator Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch die Ziel-Volumes zugewiesen haben.

  Informationen darüber, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den SnapCenter Installationsinformationen.

- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des Parameters usePowershellProcessforScripts in der Datei Web.config auf true setzen.

  Der Standardwert ist false.

Über diese Aufgabe

Eine Backup-Richtlinie ist eine Reihe von Regeln, die festlegen, wie Backups gemanagt und aufbewahrt werden und wie oft die Ressourcen- oder Ressourcengruppe gesichert wird. Außerdem können Sie Replizierungs- und Skript-Einstellungen festlegen. Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.

DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET API verwenden, um den Wert der Taste anzuzeigen. SET-API wird nicht unterstützt.

Schritt: Richtliniennamen Erstellen

1. Wählen Sie im linken Navigationsbereich **Einstellungen**.
2. Wählen Sie auf der Seite Einstellungen die Option **Richtlinien** aus.
3. Wählen Sie **Neu**.
4. Geben Sie auf der Seite **Name** den Namen und die Beschreibung der Richtlinie ein.

Schritt 2: Konfigurieren von Backup-Optionen

1. Wählen Sie Ihren Sicherungstyp aus

Vollständige Sicherung und Protokollsicherung

Sichern Sie die Datenbankdateien und Transaktionsprotokolle und verkürzen Sie die Transaktionsprotokolle.

1. Wählen Sie **Vollbackup und Log Backup** aus.
2. Geben Sie die maximale Anzahl an Datenbanken ein, die für jede Snapshot Kopie gesichert werden sollen.

> Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.

Vollständiges Backup

Sichern Sie die Datenbankdateien.

1. Wählen Sie * Vollbackup* aus.
2. Geben Sie die maximale Anzahl an Datenbanken ein, die für jede Snapshot Kopie gesichert werden sollen. Der Standardwert ist 100

> Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.

Backup Protokollieren

Sichern Sie die Transaktionsprotokolle. . Wählen Sie **Backup protokollieren**.

Backup Nur Kopieren

1. Wenn Sie Ihre Ressourcen mithilfe einer anderen Backup-Anwendung sichern, wählen Sie **nur Backup kopieren**.

Wenn die Transaktionsprotokolle intakt bleiben, kann jede Backup-Anwendung die Datenbanken wiederherstellen. In der Regel sollten Sie die Option nur kopieren unter anderen Umständen nicht verwenden.

> Microsoft SQL unterstützt nicht die Option **nur kopieren Backup** zusammen mit der Option **Vollbackup und Log Backup** für sekundären Speicher.

1. Führen Sie im Abschnitt Einstellungen für Verfügbarkeitsgruppen die folgenden Aktionen durch:

   a. Nur Backup auf bevorzugtem Backup-Replikat.

      Wählen Sie diese Option aus, um nur auf dem bevorzugten Backup-Replikat zu sichern. Über die für die AG im SQL Server konfigurierten Backup-Einstellungen wird das bevorzugte Backup-Replikat entschieden.

   b. Wählen Sie Replikate für das Backup aus.

      Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für das Backup aus.

   c. Backup-Priorität auswählen (minimale und maximale Backup-Priorität)

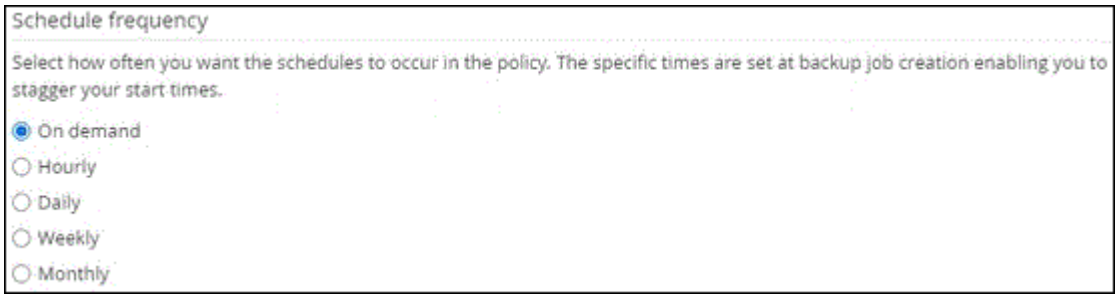
Geben Sie eine Mindestanzahl der Backup-Prioritäten und eine Nummer der maximalen Backup-Priorität an, die das AG-Replikat für das Backup entscheidet. Sie können beispielsweise eine Mindestpriorität von 10 und eine maximale Priorität von 50 haben. In diesem Fall werden alle AG-Replikate mit einer Priorität von mehr als 10 und weniger als 50 für Backups in Betracht gezogen.

Standardmäßig ist die Mindestpriorität 1 und die maximale Priorität 100.

Bei Cluster-Konfigurationen werden die Backups entsprechend den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Node des Clusters aufbewahrt. Wenn sich der Owner-Knoten der AG ändert, werden die Backups gemäß den Aufbewahrungseinstellungen erstellt und die Backups des vorherigen Owner-Knotens beibehalten. Die Aufbewahrung für AG ist nur auf Node-Ebene anwendbar.

2. Planen Sie die Backup-Häufigkeit für diese Richtlinie. Geben Sie den Zeitplantyp an, indem Sie entweder **On Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

   Sie können nur einen Plantyp für eine Richtlinie auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang festlegen, während Sie eine Ressourcengruppe erstellen. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

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

Schritt 3: Konfigurieren der Aufbewahrungseinstellungen

Führen Sie auf der Seite Aufbewahrung je nach dem auf der Seite Backup-Typ ausgewählten Backup-Typ eine oder mehrere der folgenden Aktionen durch:

1. Führen Sie in den Aufbewahrungseinstellungen für den Abschnitt „minutengenaue Wiederherstellung“ eine der folgenden Aktionen aus:

Bestimmte Anzahl von Kopien

Behalten Sie nur eine bestimmte Anzahl von Snapshot Kopien bei.

1. Wählen Sie die Option **Protokoll-Backups aufbewahren, die für die letzte <Zahl> Tage** gelten, und geben Sie die Anzahl der zu beheldenden Tage an. Wenn Sie diesem Limit nahe kommen, können Sie ältere Kopien löschen.

Bestimmte Anzahl von Tagen

Bewahren Sie die Backup-Kopien für eine bestimmte Anzahl von Tagen auf.

1. Wählen Sie die Option **Protokoll-Backups aufbewahren, die für die letzten <number> Tage voller Backups** gelten, und geben Sie die Anzahl der Tage an, um die Backup-Kopien des Protokolls zu behalten.

1. Führen Sie im Abschnitt **vollständige Backup-Aufbewahrungs-Einstellungen** für die Einstellungen für On Demand-Aufbewahrung die folgenden Aktionen aus:
   a. Geben Sie die Gesamtzahl der zu bewahrenden Snapshot Kopien an
      i. Um die Anzahl der zu bewahrenden Snapshot Kopien anzugeben, wählen Sie **Summe der zu bewahrenden Snapshot Kopien** aus.
      ii. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden.

Standardmäßig ist der Wert der Aufbewahrungsanzahl auf 2 festgelegt. 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.

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.

1. Dauer der Aufbewahrung von Snapshot Kopien
   a. Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshot Kopien behalten möchten, bevor Sie sie löschen, wählen Sie **Snapshot Kopien für** beibehalten aus.
2. Geben Sie im Abschnitt **vollständige Backup-Aufbewahrungseinstellungen** für die Einstellungen für die stündliche, tägliche, wöchentliche und monatliche Aufbewahrung die Aufbewahrungseinstellungen für den Terminplantyp an, der auf der Seite Backup-Typ ausgewählt wurde.
   a. Geben Sie die Gesamtzahl der zu bewahrenden Snapshot Kopien an
      i. Um die Anzahl der zu bewahrenden Snapshot Kopien anzugeben, wählen Sie **Summe der zu bewahrenden Snapshot Kopien** aus. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden.

Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. 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.

1. Dauer der Aufbewahrung von Snapshot Kopien
   a. Um die Anzahl der Tage anzugeben, für die Sie die Snapshot-Kopien vor dem Löschen behalten möchten, wählen Sie **Snapshot-Kopien behalten für** aus.

Die Aufbewahrung der Snapshot Kopie für dieses Protokoll ist standardmäßig auf 7 Tage festgelegt. Verwenden Sie Set-SmPolicy Cmdlet, um die Aufbewahrung von Snapshot-Protokollkopien zu ändern.

In diesem Beispiel wird die Aufbewahrung von Snapshot-Kopien für das Protokoll auf 2 festgelegt:

Beispiel 1. Beispiel Anzeigen

```
Set-SmPolicy -PolicyName 'newpol' -PolicyTyp 'Backup' -PluginPolicyTyp 'SCSQL' -sqlbackuptyp
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='hourly';RetentionCount=2},@{2}@{2}
BackupType='LOG';ScheduleType='hourly'
```

"SnapCenter behält Snapshot Kopien der Datenbank bei"

Schritt 4: Konfigurieren der Replikationseinstellungen

1. Geben Sie auf der Seite „Replikation“ die Replikation auf das sekundäre Speichersystem an:

SnapMirror aktualisieren

Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie.

1. Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu erstellen.

Aktualisieren Sie SnapVault

Aktualisieren Sie SnapVault nach dem Erstellen einer Snapshot Kopie.

1. Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.

Sekundäre Richtlinienbezeichnung

1. 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.

Fehler Anzahl Der Wiederholungen

1. Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

Schritt 5: Konfigurieren der Skripteinstellungen

1. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Backup ausgeführt werden sollen.

   Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren und Protokolle zu senden.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

   Sie müssen die SnapMirror Aufbewahrungsrichtlinie in ONTAP konfigurieren, damit der sekundäre Storage die maximale Anzahl an Snapshot Kopien nicht erreicht.

Schritt 6: Konfigurieren Sie die Überprüfungseinstellungen

Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

1. Wählen Sie im Abschnitt Überprüfung ausführen für folgende Backup-Pläne die Zeitplanhäufigkeit aus.
2. Führen Sie im Abschnitt Optionen für die Datenbankkonsistenzprüfung die folgenden Aktionen durch:
   a. Beschränkung der Integritätsstruktur auf die physische Struktur der Datenbank (PHYSICAL_ONLY)
      i. Wählen Sie **Beschränkung der Integritätsstruktur auf physische Struktur der Datenbank**

(PHYSICAL_ONLY) aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um gerissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen.

b. Alle Informationsmeldungen unterdrücken (KEINE INFOMSGS)

   i. Wählen Sie * Alle Informationsmeldungen (NO_INFOMSGS)* aus, um alle Informationsmeldungen zu unterdrücken. Standardmäßig ausgewählt.

c. Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGS)

   i. Wählen Sie **Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGS)** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen.

d. Nicht geclusterte Indizes (NOINDEX) nicht prüfen

   i. Wählen Sie * nicht gruppierte Indizes (NOINDEX)* aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten. Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.

e. Beschränken Sie die Prüfungen, und erhalten Sie die Sperren anstelle einer internen Snapshot-Kopie der Datenbank (TABLOCK).

   i. Wählen Sie **Limit the Checks und erhalten Sie die Sperren anstatt eine interne Datenbank Snapshot Kopie (TABLOCK)** zu verwenden, um die Prüfungen zu begrenzen und Sperren zu erhalten, anstatt eine interne Datenbank Snapshot Kopie zu verwenden.

3. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss bestätigen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
4. Geben Sie im Abschnitt **Verification Script settings** den Pfad und die Argumente des Vorskripts bzw. Postscript ein, die vor oder nach dem Verifizierungsvorgang ausgeführt werden sollen.

> ⓘ Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

Schritt 7: Zusammenfassung überprüfen

1. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server

Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie gemeinsam 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.

Sie können Ressourcen einzeln schützen, ohne eine neue Ressourcengruppe zu erstellen. Sie können Backups auf der geschützten Ressource erstellen.

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 **Datenbank** aus.

   Wenn Sie kürzlich eine Ressource zu SnapCenter hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie Auf **Neue Ressourcengruppe**.
4. Führen Sie auf der Seite Name die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der 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	Optional: Geben Sie einen Namen und ein Format für die benutzerdefinierte Snapshot Kopie ein. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.

5. Führen Sie auf der Seite Ressourcen die folgenden Schritte aus:
   a. Wählen Sie den Hostnamen, den Ressourcentyp und die SQL Server-Instanz aus Dropdown-Listen aus, um die Liste der Ressourcen zu filtern.

      Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

   b. So verschieben Sie Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** in den Abschnitt Ausgewählte Ressourcen:
      - Wählen Sie **Automatische Auswahl aller Ressourcen auf demselben Speichervolumen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
      - Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Pfeil nach rechts, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
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 im Abschnitt Zeitpläne für ausgewählte Richtlinien konfigurieren auf + In der Spalte Zeitplan konfigurieren für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

c. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **OK** klicken.

Sie müssen dies für jede in der Richtlinie angegebene Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte angewendete Zeitpläne im Abschnitt **Zeitpläne für ausgewählte Richtlinien konfigurieren** aufgelistet.

d. Wählen Sie den Microsoft SQL Server Scheduler aus.

Sie müssen auch eine Planer-Instanz auswählen, die der Planungsrichtlinie zugeordnet werden soll.

Wenn Sie den Microsoft SQL Server Scheduler nicht auswählen, ist der Standard Microsoft Windows Scheduler.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden. Sie sollten die Zeitpläne nicht ändern und den Backupjob umbenennen, der in Windows Scheduler oder SQL Server Agent erstellt wurde.

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

a. Wählen Sie den Verifikationsserver aus der Dropdown-Liste **Überprüfungsserver** aus.

Die Liste enthält alle SQL Server, die in SnapCenter hinzugefügt wurden. Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).

Die Version des Verifizierungsservers sollte mit der Version und Edition des SQL-Servers übereinstimmen, der die primäre Datenbank hostet.

a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror und SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.

b. Wählen Sie die Richtlinie aus, für die Sie Ihren Verifizierungszeitplan konfigurieren möchten, und klicken Sie dann auf + .

c. Führen Sie im Dialogfeld Add Verification Schedules Policy_Name die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen**.

d. Klicken Sie auf **OK**.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt. Sie können die Daten überprüfen und dann bearbeiten, indem Sie auf * klicken  * Oder löschen Sie sie, indem Sie auf * klicken ✖ *.

8. Wählen Sie auf der Benachrichtigungsseite 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. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   ⓘ Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

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

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

Anforderungen für das Backup von SQL Ressourcen

Bevor Sie eine SQL-Ressource sichern, müssen Sie sicherstellen, dass mehrere Anforderungen erfüllt sind.

- Sie müssen eine Ressource von einem nicht-NetApp Storage-System in ein NetApp Storage-System migriert haben.
- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung zu 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.
- Der von einem Active Directory (AD)-Benutzer initiierte Backup-Vorgang schlägt fehl, wenn die SQL-Instanz-Anmeldeinformationen nicht dem AD-Benutzer oder der AD-Gruppe zugewiesen sind. Sie müssen die SQL-Instanz-Anmeldeinformationen AD-Benutzer oder -Gruppe über die Seite **Einstellungen** > **Benutzerzugriff** zuweisen.
- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts enthält, kann der Backup-Vorgang auf einigen Hosts aufgrund von Netzwerkproblemen spät ausgelöst werden. Sie sollten den Wert von FMaxRetryForUninitializedHosts in Web.config mit dem Cmdlet Set-SmConfigSettings PS konfigurieren.

Backup von SQL-Ressourcen

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

Über diese Aufgabe

- Für die Authentifizierung von Windows-Anmeldeinformationen müssen Sie die Anmeldeinformationen einrichten, bevor Sie die Plug-ins installieren.

- Für die Authentifizierung der SQL Server-Instanz müssen Sie die Anmeldeinformationen nach der Installation der Plug-ins hinzufügen.
- Für die gMSA-Authentifizierung müssen Sie gMSA beim Registrieren des Hosts mit SnapCenter auf der Seite **Add Host** oder **Modify Host** einrichten, um den gMSA zu aktivieren und zu verwenden.
- Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und System Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen * Datenbank* oder **Instanz** oder **Verfügbarkeitsgruppe** aus der Dropdown-Liste **Ansicht** aus.

   a. Wählen Sie die Datenbank, die Instanz oder die Verfügbarkeitsgruppe aus, die Sie sichern möchten.

      Wenn Sie eine Sicherungskopie einer Instanz erstellen, sind die Informationen zum letzten Sicherungsstatus oder zum Zeitstempel dieser Instanz auf der Seite Ressourcen nicht verfügbar.

   In der Topologieansicht lässt sich nicht unterscheiden, ob der Backup-Status, der Zeitstempel oder das Backup für eine Instanz oder eine Datenbank gilt.

3. Aktivieren Sie auf der Seite Ressourcen das Kontrollkästchen **Custom Name Format for Snapshot copy** und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot Kopie verwenden möchten.

   Beispiel: Custtext_Policy_hostname oder Resource_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.

4. Führen Sie auf der Seite Richtlinien die folgenden Aufgaben aus:

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

      Sie können eine Richtlinie erstellen, indem Sie * auswählen  * Um den Policy Wizard zu starten.

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

   b. Wählen Sie  In der Spalte Zeitplan konfigurieren für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. In der Option * Pläne für Police hinzufügen* `policy_name` Konfigurieren Sie den Zeitplan, und wählen Sie dann **OK**.

      Hier `policy_name` Ist der Name der Richtlinie, die Sie ausgewählt haben.

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

   a. Wählen Sie den Microsoft SQL Server Scheduler verwenden* aus, und wählen Sie dann die Planerinstanz aus der Dropdown-Liste **Scheduler Instance** aus, die mit der Planungsrichtlinie verknüpft ist.

5. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

a. Wählen Sie den Verifikationsserver aus der Dropdown-Liste **Überprüfungsserver** aus.

   Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).

   Die Version des Verifizierungsservers sollte gleich oder höher sein als die Version der Edition des SQL-Servers, der die primäre Datenbank hostet.

a. Wählen Sie **sekundäre Lokatoren laden, um Backups auf dem sekundären Speichersystem zu überprüfen**, um Ihre Backups auf dem sekundären Speichersystem zu überprüfen.

b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und wählen Sie dann * aus  *.

c. Führen Sie im Dialogfeld Add Verification Schedules_Policy_Name_ die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen**.

   Wenn der Verifikationsserver keine Speicherverbindung hat, schlägt der Verifizierungsvorgang mit Fehler fehl: Datenträger konnte nicht bereitgestellt werden.

d. Wählen Sie **OK**.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

6. Wählen Sie auf der Benachrichtigungsseite 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. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

7. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

   Die Seite der Datenbanktopologie wird angezeigt.

8. Wählen Sie **Jetzt sichern**.
9. 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. Wählen Sie zur Überprüfung Ihres Backups **nach dem Backup**.

c. Wählen Sie **Backup**.

> Sie sollten den im Windows Scheduler oder SQL Server Agent erstellten Sicherungsauftrag nicht umbenennen.

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.

Es wird eine implizite Ressourcengruppe erstellt. Sie können dies anzeigen, indem Sie auf der Seite „Benutzerzugriff“ den jeweiligen Benutzer oder die jeweilige Gruppe auswählen. Der implizite Gruppentyp lautet „`Ressource`“.

10. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Nachdem Sie fertig sind

- In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung erkennen.

  "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_scvservice. In diesem Skript, das `do_start method` Befehl startet den SnapCenter-VMware-Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

"Sichern Sie Ressourcen mit PowerShell cmdlets"

"Backup-Vorgänge schlagen wegen der Verzögerung im TCP_TIMEOUT bei MySQL-Verbindungsfehler fehl"

"Das Backup schlägt mit dem Windows Scheduler-Fehler fehl"

"Fehler beim Quiesce oder Gruppieren von Ressourcen"

Sichern Sie SQL Server-Ressourcengruppen

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 Namens der Ressourcengruppe im Suchfeld oder durch Auswählen von * durchsuchen[Filtersymbol]* Und dann das Tag auswählen. Sie

können dann * auswählen[Filtersymbol]* Zum Schließen des Filterfensters.

3. Wählen Sie auf der Seite Ressourcengruppen die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
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. Wählen Sie nach dem Backup **Verify** aus, um das On-Demand-Backup zu überprüfen.

      Die Option **Verify** in der Richtlinie gilt nur für geplante Jobs.

   c. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

"Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server"

"Sichern Sie Ressourcen mit PowerShell cmdlets"

"Backup-Vorgänge schlagen wegen der Verzögerung im TCP_TIMEOUT bei MySQL-Verbindungsfehler fehl"

"Das Backup schlägt mit dem Windows Scheduler-Fehler fehl"

Monitoring von Backup-Vorgängen

Überwachen Sie die Backup-Vorgänge für SQL-Ressourcen auf der Seite SnapCenter-Jobs

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 Sie Datenschutzvorgänge für SQL-Ressourcen im Bereich „Aktivität“

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 Vorgangsdetails auf der Seite **Job-Details** aufgeführt.

Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um Datensicherungsvorgänge durchzuführen.

Bevor Sie beginnen

- 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 Management-LIF-IP-Adresse verfügen.

Schritte

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

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

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

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

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   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 werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

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

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 Ressourcen mit PowerShell cmdlets

Sie können die PowerShell Commandlets zum Sichern von SQL Server-Datenbanken oder Windows-Dateisystemen verwenden. Dazu gehört die Sicherung einer SQL Server-Datenbank oder eines Windows-Dateisystems, einschließlich der Herstellung einer

Verbindung mit dem SnapCenter-Server, der Ermittlung der SQL Server-Datenbankinstanzen oder Windows-Dateisysteme, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppe, das Sichern und das Überprüfen des Backups.

Bevor Sie beginnen

- Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.
- Sie müssen die Speichersystemverbindung hinzugefügt und Anmeldedaten erstellt haben.
- Sie müssen Hosts hinzugefügt und Ressourcen erkannt 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. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem SQL Backup-Typ von FullBackup:

   ```
   PS C:\> Add-SmPolicy -PolicyName TESTPolicy
   -PluginPolicyType SCSQL -PolicyType Backup
   -SqlBackupType FullBackup -Verbose
   ```

   In diesem Beispiel wird eine neue Backup-Richtlinie mit einem Backup-Typ von CrashConsistent für Windows File-Systeme erstellt:

   ```
   PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
   -PluginPolicyType SCW -PolicyType Backup
   -ScwBackupType CrashConsistent -Verbose
   ```

3. Ermitteln Sie Host-Ressourcen mit dem Cmdlet "Get-SmResources".

   Dieses Beispiel ermittelt die Ressourcen für das Microsoft SQL Plug-in auf dem angegebenen Host:

   ```
   C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
   -PluginCode SCSQL
   ```

   In diesem Beispiel werden Ressourcen für Windows File-Systeme auf dem angegebenen Host ermittelt:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Fügen Sie mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter hinzu.

   In diesem Beispiel wird eine neue Ressourcengruppe für die Sicherung von SQL-Datenbanken mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   Dieses Beispiel erstellt eine neue Windows Dateisystem-Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

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

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

   In diesem Beispiel wird ein Job-Summary-Bericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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".

Abbrechen des SnapCenter-Plug-ins für Microsoft SQL Server-Backup-Vorgänge

Sie können laufende, in die Warteschlange eingereihte oder nicht reaktionsfähige Backup-Vorgänge abbrechen. Wenn Sie einen Backup-Vorgang abbrechen, stoppt der SnapCenter-Server den Vorgang und entfernt alle Snapshot-Kopien aus dem Storage, falls das erstellte Backup nicht beim SnapCenter Server registriert ist. Wenn das Backup

bereits beim SnapCenter Server registriert ist, wird die bereits erstellte Snapshot-Kopie nicht wieder zurückgeführt, auch wenn der Vorgang ausgelöst wird.

Bevor Sie beginnen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.
- Sie können nur das Protokoll oder die vollständigen Backup-Vorgänge abbrechen, die in die Warteschlange gestellt werden oder ausgeführt werden.
- Sie können den Vorgang nicht abbrechen, nachdem die Überprüfung gestartet wurde.

  Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Verifizierungsvorgang wird nicht durchgeführt.
- Sie können einen Sicherungsvorgang entweder über die Seite Überwachen oder über den Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter GUI können Sie PowerShell cmdlets verwenden, um 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

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Wählen Sie im linken Navigationsbereich **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und wählen Sie **Job abbrechen** .
Aktivitätsbereich	1. Wählen Sie nach dem Initiieren des Backupjobs aus Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. 2. Wählen Sie den Vorgang aus. 3. Wählen Sie auf der Seite Job-Details die Option **Job abbrechen** aus.

Ergebnis

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt. Wenn der Vorgang, den Sie abgebrochen haben, im Status „Abbrechen“ oder „Ausführen“ nicht reagiert, sollten Sie den ausführen `Cancel-SmJob -JobID <int> -Force` Cmdlet zum gewaltsamen Beenden des Backup-Vorgangs.

Sehen Sie sich SQL Server 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

Auf der Seite Topology 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.

Sie können die folgenden Symbole in der Ansicht **Kopien verwalten** anzeigen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Vault-Kopien).

-  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.

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 entweder 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 ausgewählte Ressource eine geklonte Datenbank ist, schützen Sie die geklonte Datenbank, wird die Quelle des Klons auf der Seite Topologie angezeigt. Klicken Sie auf **Details**, um das zum Klonen verwendete Backup anzuzeigen.

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

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt **Übersichtskarte** wird die Gesamtzahl der 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 Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

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

7. Wählen Sie einen Klon aus der Tabelle aus und klicken Sie auf **Clone Split**.
8. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie anschließend auf .

Entfernen Sie Backups mithilfe von PowerShell Cmdlets

Mit dem Cmdlet "Remove-SmBackup" können Sie Backups löschen, wenn Sie diese nicht mehr für andere Datenschutzvorgänge benötigen.

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. Löschen Sie ein oder mehrere Backups mit dem Cmdlet "Remove-SmBackup".

   In diesem Beispiel werden zwei Backups mithilfe der Backup-IDs gelöscht:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets

Sie können das Cmdlet "Remove-SmBackup" verwenden, um die Anzahl der Backups für

sekundäre Backups zu bereinigen, die keine Snapshot-Kopien haben. Sie möchten dieses Cmdlet vielleicht verwenden, wenn die gesamten Snapshot Kopien, die in der Topologie zum Managen von Kopien angezeigt werden, nicht mit der Einstellung zum Speichern von sekundären Storage Snapshot Kopien übereinstimmen.

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. Bereinigen Sie die Anzahl der sekundären Backups mit dem Parameter -CleanupSecondaryBackups.

   Dieses Beispiel bereinigt die Anzahl der Backups für sekundäre Backups ohne Snapshot-Kopien:

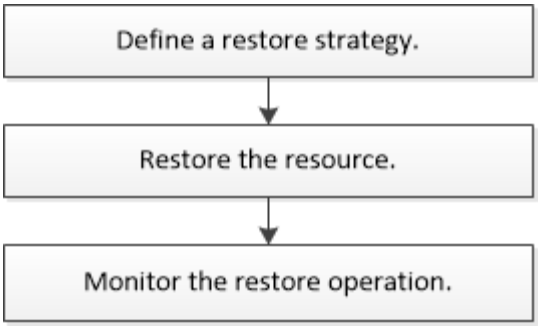
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Stellen Sie SQL Server-Ressourcen wieder her

Wiederherstellung des Workflows

Sie können SnapCenter verwenden, um SQL Server Datenbanken wiederherzustellen, indem Sie die Daten von einem oder mehreren Backups auf Ihr aktives File-System wiederherstellen und dann die Datenbank wiederherstellen. Sie können auch Datenbanken wiederherstellen, die sich in Verfügbarkeitsgruppen befinden, und dann die wiederhergestellten Datenbanken der Verfügbarkeitsgruppe hinzufügen. Vor dem Wiederherstellen einer SQL Server-Datenbank müssen Sie mehrere vorbereitende Aufgaben ausführen.

Im folgenden Workflow wird die Reihenfolge angezeigt, in der Sie die Datenbankwiederherstellungen durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder in der "SnapCenter Software Cmdlet Referenzhandbuch"

Weitere Informationen

"Wiederherstellung einer SQL Server-Datenbank aus dem sekundären Storage"

"Stellen Sie Ressourcen mithilfe von PowerShell cmdlets wieder her"

"Der Wiederherstellungsvorgang kann unter Windows 2008 R2 fehlschlagen"

Anforderungen für das Wiederherstellen einer Datenbank

Bevor Sie eine SQL Server-Datenbank aus einem SnapCenter Plug-in für Microsoft SQL Server-Backup wiederherstellen, müssen Sie sicherstellen, dass mehrere Anforderungen erfüllt sind.

- Die Ziel-SQL Server-Instanz muss online sein und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.

  Dies gilt sowohl für Restore-Vorgänge bei der Benutzerdatenbank als auch für die Wiederherstellung von Systemdatenbanken.

- SnapCenter Vorgänge, die für die wiederherzustellende SQL Server Daten ausgeführt werden, müssen deaktiviert werden, einschließlich sämtlicher Jobs, die auf Remote Management- oder Remote Verifizierungs-Servern geplant sind.
- Wenn Systemdatenbanken nicht funktionsfähig sind, müssen Sie zuerst die Systemdatenbanken mithilfe eines SQL Server-Dienstprogramms neu erstellen.
- Wenn Sie das Plug-in installieren, stellen Sie sicher, dass Sie Berechtigungen für andere Rollen erteilen, um die Backups der Verfügbarkeitsgruppe (AG) wiederherzustellen.

  Die Wiederherstellung der AG schlägt fehl, wenn eine der folgenden Bedingungen erfüllt ist:

  - Wenn das Plug-in durch RBAC-Benutzer installiert wird und ein Administrator versucht, ein AG-Backup wiederherzustellen
  - Wenn das Plug-in von einem Administrator installiert wird und ein RBAC-Benutzer versucht, ein AG-Backup wiederherzustellen
- Wenn Sie benutzerdefinierte Protokollverzeichnis-Backups auf einen alternativen Host wiederherstellen, müssen der SnapCenter Server und der Plug-in-Host dieselbe SnapCenter-Version installiert haben.

- Sie müssen Microsoft Hotfix, KB2887595, installiert haben. Die Microsoft Support Site enthält weitere Informationen über KB2887595.

  "Microsoft Support-Artikel 2887595: Windows RT 8.1, Windows 8.1 und Windows Server 2012 R2 Update Rollup: November 2013"

- Sie müssen die Ressourcengruppen oder die Datenbank gesichert haben.
- Wenn Sie Snapshot Kopien in einen Spiegel oder Vault replizieren, muss dem SnapCenter Administrator die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch die Ziel-Volumes zugewiesen haben.

  Informationen darüber, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den SnapCenter Installationsinformationen.

- Alle Backup- und Klonjobs müssen vor der Wiederherstellung der Datenbank angehalten werden.
- Wenn sich die Datenbankgröße in Terabyte (TB) befindet, kann der Restore-Vorgang einen Timeout durchführen.

  Sie müssen den Wert des RESTTimeout-Parameters von SnapCenter Server auf 20000000 ms erhöhen, indem Sie den folgenden Befehl ausführen: Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}. Je nach Größe der Datenbank kann der Zeitüberschreitungswert geändert werden, und der Maximalwert, den Sie einstellen können, beträgt 86400000 ms.

Wenn Sie wiederherstellen möchten, während die Datenbanken online sind, sollte die Option Online-Wiederherstellung auf der Seite Wiederherstellen aktiviert sein.

Stellen Sie Backups von SQL Server Datenbanken wieder her

Sie können SnapCenter verwenden, um gesicherte SQL Server-Datenbanken wiederherzustellen. Die Wiederherstellung der Datenbank ist ein mehrphasiger Prozess, der alle Daten- und Protokollseiten von einem bestimmten SQL Server-Backup in eine angegebene Datenbank kopiert.

Über diese Aufgabe

- Sie können die gesicherten SQL Server Datenbanken auf einer anderen SQL Server-Instanz auf demselben Host wiederherstellen, auf dem das Backup erstellt wurde.

  Sie können SnapCenter verwenden, um die gesicherten SQL Server Datenbanken auf einem anderen Pfad wiederherzustellen, sodass Sie keine Produktionsversion ersetzen.

- SnapCenter kann Datenbanken in einem Windows Cluster wiederherstellen, ohne die SQL Server Cluster-Gruppe offline zu schalten.
- Wenn ein Cluster ausfällt (ein Vorgang zum Verschieben der Cluster-Gruppe) während eines Wiederherstellungsvorgangs auftritt (z. B. wenn der Node, der die Ressourcen besitzt, ausfällt), müssen Sie die Verbindung zur SQL Server Instanz wiederherstellen und dann den Wiederherstellungsvorgang neu starten.
- Sie können die Datenbank nicht wiederherstellen, wenn die Benutzer oder die SQL Server Agent-Jobs auf die Datenbank zugreifen.
- Systemdatenbanken können nicht auf einem alternativen Pfad wiederhergestellt werden.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der

SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET API verwenden, um den Wert der Taste anzuzeigen. SET-API wird nicht unterstützt.

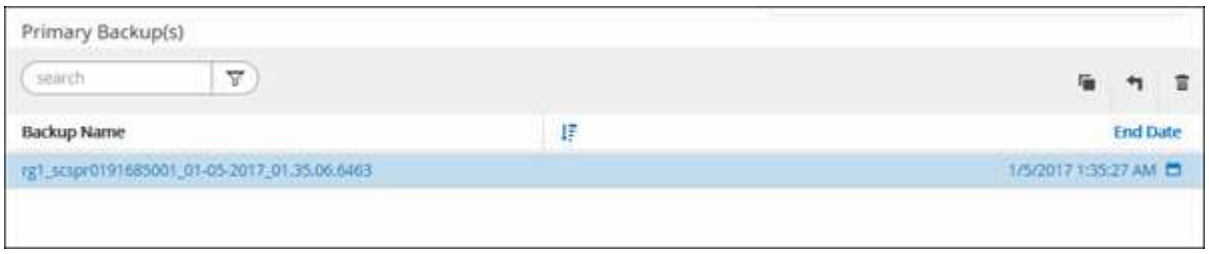
- Die meisten Felder auf den Seiten des Assistenten Wiederherstellen sind selbsterklärend. In den folgenden Informationen werden die Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.

   Die Topologieseite wird angezeigt.

4. Wählen Sie aus der Ansicht Kopien verwalten im Speichersystem **Backups** aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf das  Symbol.



6. Wählen Sie auf der Seite „Bereich wiederherstellen“ eine der folgenden Optionen aus:

Option	Beschreibung
Stellen Sie die Datenbank auf demselben Host wieder her, auf dem das Backup erstellt wurde	Wählen Sie diese Option aus, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Backups erstellt werden.

Option	Beschreibung
Wiederherstellung der Datenbank auf einem alternativen Host	Wählen Sie diese Option aus, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem Backups erstellt werden. Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen ein (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an. Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateiendung der ursprünglichen Datenbankdatei identisch sein. Wenn die Option **Datenbank auf alternativen Host** wiederherstellen nicht auf der Seite „Bereich wiederherstellen“ angezeigt wird, löschen Sie den Browser-Cache.
Stellen Sie die Datenbank mithilfe vorhandener Datenbankdateien wieder her	Wählen Sie diese Option aus, wenn die Datenbank auf einem anderen SQL Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem Backups erstellt werden. Die Datenbankdateien sollten bereits auf den angegebenen Dateipfaden vorhanden sein. Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen ein (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an.

7. Wählen Sie auf der Seite „Recovery Scope“ eine der folgenden Optionen aus:

Option	Beschreibung
Keine	Wählen Sie **Keine** aus, wenn Sie nur das vollständige Backup ohne Protokolle wiederherstellen müssen.
Alle Log-Backups	Wählen Sie **Alle Log-Backups** Backup-Restore-Vorgang up-to-the-minute, um alle verfügbaren Log-Backups nach der vollständigen Sicherung wiederherzustellen.

Option	Beschreibung
Durch Backups bis protokollieren	Wählen Sie **nach Log-Backups**, um einen Point-in-Time-Wiederherstellungsvorgang durchzuführen, der die Datenbank basierend auf Backup-Protokollen bis zum ausgewählten Datum wiederherstellt.
Nach einem bestimmten Datum bis	Wählen Sie **nach einem bestimmten Datum bis**, um Datum und Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht auf die wiederhergestellte Datenbank angewendet werden. Dieser Point-in-Time-Wiederherstellungsvorgang stoppt die Wiederherstellung von Transaktions-Log-Einträgen, die nach dem angegebenen Datum und der angegebenen Zeit aufgezeichnet wurden.
Benutzerdefiniertes Protokollverzeichnis verwenden	Wenn Sie **Alle Log-Backups**, **durch Log-Backups** oder **nach einem bestimmten Datum bis** ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie **Benutzerdefiniertes Log-Verzeichnis verwenden** und geben Sie dann den Speicherort an. Die Option **Benutzerdefiniertes Logverzeichnis verwenden** ist nur verfügbar, wenn Sie **Datenbank auf einen alternativen Host wiederherstellen** oder **Datenbank mit vorhandenen Datenbankdateien wiederherstellen** ausgewählt haben. Sie können auch den freigegebenen Pfad verwenden, aber sicherstellen, dass der SQL-Benutzer auf den Pfad zugreifen kann. Das benutzerdefinierte Protokollverzeichnis wird für die Verfügbarkeitsgruppendatenbank nicht unterstützt.

8. Führen Sie auf der Seite Pre Ops die folgenden Schritte aus:

   a. Wählen Sie auf der Seite Optionen vor der Wiederherstellung eine der folgenden Optionen aus:

      - Wählen Sie **Überschreiben Sie die Datenbank mit demselben Namen während der Wiederherstellung** aus, um die Datenbank mit dem gleichen Namen wiederherzustellen.
      - Wählen Sie **SQL-Datenbankreplikationseinstellungen beibehalten** aus, um die Datenbank wiederherzustellen und die vorhandenen Replikationseinstellungen beizubehalten.
      - Wählen Sie **Sicherung des Transaktionsprotokolls vor der Wiederherstellung** aus, um ein Transaktionsprotokoll zu erstellen, bevor der Wiederherstellungsvorgang beginnt.
      - Wählen Sie **Wiederherstellen, wenn die Sicherung des Transaktionsprotokolls vor der**

Wiederherstellung fehlschlägt aus, um den Wiederherstellungsvorgang abzubrechen, wenn die Sicherung des Transaktionsprotokolls fehlschlägt.

b. Geben Sie optionale Skripte an, die ausgeführt werden sollen, bevor Sie einen Wiederherstellungsauftrag ausführen.

Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

9. Führen Sie auf der Seite „Post Ops“ die folgenden Schritte aus:

a. Wählen Sie im Abschnitt Datenbank nach Abschluss der Wiederherstellung auswählen eine der folgenden Optionen aus:

- Wählen Sie **Operational, aber nicht verfügbar für die Wiederherstellung weiterer Transaktionsprotokolle**, wenn Sie jetzt alle notwendigen Backups wiederherstellen.

  Dies ist das Standardverhalten, das die Datenbank durch ein Rollback der nicht gesicherten Transaktionen einsatzbereit macht. Sie können erst dann weitere Transaktionsprotokolle wiederherstellen, wenn Sie ein Backup erstellen.

- Wählen Sie **nicht betriebsbereit, aber verfügbar für die Wiederherstellung weiterer Transaktionsprotokolle**, um die Datenbank nicht betriebsbereit zu lassen, ohne die nicht gesicherten Transaktionen zurückzurollen.

  Zusätzliche Transaktions-Logs können wiederhergestellt werden. Sie können die Datenbank erst verwenden, wenn sie wiederhergestellt ist.

- Wählen Sie **schreibgeschützter Modus, der zur Wiederherstellung weiterer Transaktionsprotokolle** verfügbar ist, um die Datenbank im schreibgeschützten Modus zu belassen.

  Mit dieser Option werden nicht gesicherte Transaktionen rückgängig gemacht, die nicht rückgängig gemachte Aktionen werden jedoch in einer Standby-Datei gespeichert, sodass Recovery-Effekte rückgängig gemacht werden können.

Wenn die Option „Verzeichnis aufheben“ aktiviert ist, werden mehr Transaktionsprotokolle wiederhergestellt. Wenn der Wiederherstellungsvorgang für das Transaktionsprotokoll nicht erfolgreich ist, können die Änderungen zurückgesetzt werden. Die SQL Server-Dokumentation enthält weitere Informationen.

b. Geben Sie optionale Skripts an, die ausgeführt werden sollen, nachdem ein Wiederherstellungsauftrag ausgeführt wurde.

Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

10. Wählen Sie auf der Benachrichtigungsseite 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.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs**.

Verwandte Informationen

"Stellen Sie Ressourcen mithilfe von PowerShell cmdlets wieder her"

"Wiederherstellung einer SQL Server-Datenbank aus dem sekundären Storage"

Wiederherstellung einer SQL Server-Datenbank aus dem sekundären Storage

Sie können die gesicherten SQL Server Datenbanken von den physischen LUNs (RDM, iSCSI oder FCP) auf einem sekundären Speichersystem wiederherstellen. Die Funktion „Restore“ ist ein mehrphasiger Prozess, bei dem alle Daten und Protokollseiten von einem bestimmten SQL Server Backup im sekundären Storage-System in eine angegebene Datenbank kopiert werden.

Bevor Sie beginnen

- Sie müssen die Snapshot Kopien vom primären zum sekundären Storage-System replizieren.
- Sie müssen sicherstellen, dass der SnapCenter-Server und der Plug-in-Host eine Verbindung zum sekundären Speichersystem herstellen können.
- Die meisten Felder auf den Seiten des Assistenten Wiederherstellen werden im grundlegenden Wiederherstellungsprozess erläutert. In den folgenden Informationen werden einige der Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **SnapCenter-Plug-in für SQL Server** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** die Option **Datenbank** oder **Ressourcengruppe** aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.

   Die Topologieseite für die Datenbank- oder Ressourcengruppe wird angezeigt.

4. Wählen Sie im Abschnitt Kopien verwalten aus dem sekundären Speichersystem (gespiegelt oder Tresor) **Backups** aus.
5. Wählen Sie das Backup aus der Liste aus, und klicken Sie dann auf  .
6. Wählen Sie auf der Seite Standort das Zielvolume für die Wiederherstellung der ausgewählten Ressource aus.
7. Schließen Sie den Wiederherstellungs-Assistenten ab, überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Wenn Sie eine Datenbank auf einem anderen Pfad wiederherstellen, der von anderen Datenbanken gemeinsam genutzt wird, sollten Sie eine vollständige Backup- und Backup-Verifizierung durchführen, um zu bestätigen, dass Ihre wiederhergestellte Datenbank frei von Beschädigungen auf physischer Ebene ist.

Datenbanken der Verfügbarkeitsgruppe erneut erstellen

Erneutes Seeding ist eine Option zur Wiederherstellung von Datenbanken der Availability Group (AG). Sollte die Synchronisierung einer sekundären Datenbank mit der primären Datenbank in einer AG nicht mehr synchronisiert werden, können Sie die sekundäre Datenbank erneut speichern.

Bevor Sie beginnen

- Sie müssen ein Backup der sekundären AG-Datenbank erstellt haben, die Sie wiederherstellen möchten.
- Der SnapCenter-Server und der Plug-in-Host müssen dieselbe SnapCenter-Version installiert haben.

Über diese Aufgabe

- Ein erneutes Seeding von primären Datenbanken kann nicht durchgeführt werden.
- Ein erneutes Seeding kann nicht ausgeführt werden, wenn die Datenbank des Replikats aus der Verfügbarkeitsgruppe entfernt wird. Wenn das Replikat entfernt wird, schlägt der erneute Seeding fehl.
- Während Sie den Vorgang für erneutes Seeding in der Datenbank der SQL Availability Group ausführen, sollten Sie keine Protokoll-Backups auf den Replikatdatenbanken dieser Availability Group-Datenbank auslösen. Wenn Sie während des erneuten Seeding-Vorgangs Protokollsicherungen auslösen, schlägt der Vorgang des erneuten Seeding mit der Spiegeldatenbank fehl. „Database_Name“ verfügt über unzureichende Transaktions-Log-Daten, um die Backup-Kette der Hauptdatenbank-Fehlermeldung zu erhalten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **SnapCenter-Plug-in für SQL Server** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Datenbank** aus.
3. Wählen Sie die sekundäre AG-Datenbank aus der Liste aus.
4. Klicken Sie Auf **Erneut**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

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".

Überwachung von Restore-Vorgängen bei SQL-Ressourcen

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 **Job Details** 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.

Wiederherstellungsvorgänge für SQL-Ressourcen abbrechen

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge 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 Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

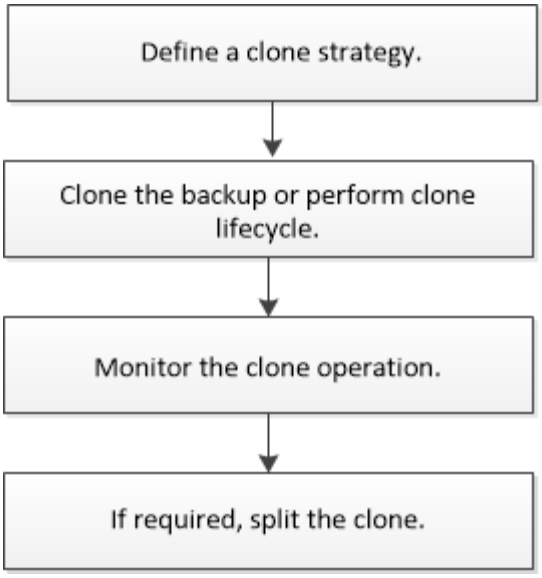
Klonen von SQL Server Datenbankressourcen

Klon-Workflow

Vor dem Klonen von Datenbankressourcen aus einem Backup müssen Sie mehrere Aufgaben mit SnapCenter Server ausführen. Beim Datenbankklonen wird eine zeitpunktgenaue Kopie einer Produktionsdatenbank oder des zugehörigen Backup-Satzes erstellt. Sie können Datenbanken klonen, um Funktionen zu testen, die mit der aktuellen Datenbankstruktur und dem Inhalt während der Anwendungsentwicklungszyklen implementiert werden müssen, um die Werkzeuge zur Datenextraktion und -Bearbeitung beim Befüllen von Data Warehouses zu verwenden oder Daten, die versehentlich gelöscht oder geändert wurden, wiederherzustellen.

Bei einem Datenbankklonen werden Berichte auf Basis der Job-IDs erstellt.

Im folgenden Workflow ist die Reihenfolge aufgeführt, in der Sie die Klonvorgänge ausführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder in der "SnapCenter Software Cmdlet Referenzhandbuch"

Weitere Informationen

"Klonen aus einem Backup der SQL Server Datenbank"

"Führen Sie Den Klon-Lebenszyklus Durch"

"Der Klonvorgang kann fehlschlagen oder längere Zeit zum Abschließen mit dem Standardwert für TCP_TIMEOUT benötigen"

Klonen aus einem Backup der SQL Server Datenbank

Sie können das Backup einer SQL Server Datenbank mit SnapCenter klonen. Wenn Sie auf eine ältere Version der Daten zugreifen oder diese wiederherstellen möchten, können Sie Datenbank-Backups nach Bedarf klonen.

Bevor Sie beginnen

- Sie sollten sich auf den Datenschutz vorbereiten, indem Sie Aufgaben wie das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Speichersystem abschließen.
- Sie sollten Datenbanken oder Ressourcengruppen gesichert haben.
- Der Sicherungstyp wie Mirror, Vault oder Mirror-Vault für Daten-LUN und Protokoll-LUN sollte dieselben sein, um sekundäre Lokatoren beim Klonen zu einem alternativen Host mithilfe von Protokoll-Backups zu erkennen.
- Wenn das gemountete Klonlaufwerk während eines SnapCenter Klonvorgangs nicht gefunden werden kann, sollten Sie den Parameter CloneRetryTimeout von SnapCenter Server in 300 ändern.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.

Über diese Aufgabe

- Stellen Sie beim Klonen auf eine eigenständige Datenbankinstanz sicher, dass der Mount-Point-Pfad

vorhanden ist und dass es sich um eine dedizierte Festplatte handelt.

- Beim Klonen in eine Failover Cluster-Instanz (FCI) stellen Sie sicher, dass die Mount-Punkte vorhanden sind, dass es sich um eine freigegebene Festplatte handelt, und der Pfad und die FCI sollten zur gleichen SQL-Ressourcengruppe gehören.
- Stellen Sie sicher, dass nur ein VFC- oder FC-Initiator mit jedem Host verbunden ist. Der Grund dafür ist, dass SnapCenter nur einen Initiator pro Host unterstützt.
- Wenn sich die Quelldatenbank oder die Zielinstanz auf einem gemeinsam genutzten Cluster-Volume (csv) befindet, befindet sich die geklonte Datenbank auf dem csv.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit zu verwenden.

  Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

  Sie können die GET API verwenden, um den Wert der Taste anzuzeigen. SET-API wird nicht unterstützt.

Stellen Sie für virtuelle Umgebungen (VMDK/RDM) sicher, dass der Bereitstellungspunkt eine dedizierte Festplatte ist.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann **SnapCenter Plug-in für SQL Server** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.

   Das Klonen eines Backups einer Instanz wird nicht unterstützt.

3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** das Backup entweder aus dem primären oder sekundären (gespiegelten oder gewölbten) Speichersystem aus.
5. Wählen Sie die Sicherung aus, und wählen Sie dann * aus  *.
6. Führen Sie auf der Seite **Clone Options** die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Kloninstanz	Wählen Sie eine Kloninstanz aus, zu der Sie das Datenbank-Backup klonen möchten. Diese SQL-Instanz muss sich auf dem angegebenen Klon-Server befinden.

Für dieses Feld…	Tun Sie das…
Suffix klonen	Geben Sie ein Suffix ein, das an den Namen der Klondatei angehängt wird, um zu identifizieren, dass die Datenbank ein Klon ist. Beispiel: *db1_Clone*. Wenn Sie an demselben Speicherort wie die Originaldatenbank klonen, müssen Sie ein Suffix bereitstellen, um die geklonte Datenbank von der ursprünglichen Datenbank zu unterscheiden. Andernfalls schlägt der Vorgang fehl.
Automatisches Zuweisen von Mount-Punkten oder automatische Zuweisung von Volume-Mount-Punkten unter Pfad	Legen Sie fest, ob unter einem Pfad automatisch ein Mount-Punkt oder ein Volume-Mount-Punkt zugewiesen werden soll. Automatisches Zuweisen von Volume-Mount-Punkt unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht es Ihnen, ein bestimmtes Verzeichnis bereitzustellen. Die Mount-Punkte werden innerhalb dieses Verzeichnisses erstellt. Bevor Sie diese Option auswählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich eine Datenbank im Verzeichnis befindet, befindet sich die Datenbank nach dem Mount-Vorgang in einem ungültigen Status.

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

Für dieses Feld…	Tun Sie das…
Keine	Wählen Sie diese Option, wenn Sie nur das vollständige Backup ohne Logs klonen möchten.
Alle Log-Backups	Wählen Sie diese Option, um alle verfügbaren Protokoll-Backups zu klonen, die nach der vollständigen Sicherung datiert sind.
Durch Backups bis protokollieren	Wählen Sie diese Option, um die Datenbank auf Basis der Backup-Protokolle zu klonen, die bis zum Backup-Protokoll mit dem ausgewählten Datum erstellt wurden.

Für dieses Feld…	Tun Sie das…
Nach einem bestimmten Datum bis	Geben Sie Datum und Uhrzeit an, nach denen die Transaktionsprotokolle nicht auf die geklonte Datenbank angewendet werden. Dieser Point-in-Time-Klon stoppt den Klon der Transaktions-Log-Einträge, die nach dem angegebenen Datum und der angegebenen Zeit aufgezeichnet wurden.

8. Geben Sie auf der Seite **Script** das Skript-Timeout, den Pfad und die Argumente des Prescript oder Postscript ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.

   Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

   > Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

   Das Standard-Skript-Timeout beträgt 60 Sekunden.

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. Wenn Sie den Bericht über den ausgeführten Klonvorgang anhängen möchten, wählen Sie **Job-Bericht anhängen** aus.

   > Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

   Informationen zu EMS finden Sie unter "EMS-Datenerfassung managen"

10. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Nachdem Sie fertig sind

Nach dem Erstellen des Klons sollten Sie ihn nicht mehr umbenennen.

Verwandte Informationen

"Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe"

"Klonen von Backups mit PowerShell Cmdlets"

"Der Klonvorgang kann fehlschlagen oder längere Zeit zum Abschließen mit dem Standardwert für TCP_TIMEOUT benötigen"

"Der Datenbankklon für die Failover-Cluster-Instanz ist fehlgeschlagen"

Klonen von Backups 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.

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. Listen Sie die Backups auf, die mit dem Cmdlet "Get-SmBackup" oder "Get-SmResourceGroup" geklont werden können.

   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     Full Backup
                                         11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                         11:23:17 AM
```

   In diesem Beispiel werden Informationen über eine bestimmte Ressourcengruppe, ihre Ressourcen und zugehörige Richtlinien angezeigt:

```
PS C:\> Get-SmResourceGroup -ListResources –ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
```

```
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
```

```
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup mit dem Cmdlet "New-SmClone".

   Dieses Beispiel erstellt einen Klon aus einem angegebenen Backup mit allen Protokollen:

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

In diesem Beispiel wird ein Klon für eine angegebene Microsoft SQL Server-Instanz erstellt:

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Zeigen Sie den Status des Clone-Jobs mit dem Cmdlet Get-SmCloneReport an.

   In diesem Beispiel wird ein Klonbericht für die angegebene Job-ID angezeigt:

```
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}
```

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".

Führen Sie Den Klon-Lebenszyklus Durch

Mit SnapCenter können Sie Klone aus einer Ressourcengruppe oder Datenbank erstellen. Sie können entweder einen On-Demand-Klon durchführen oder wiederkehrende Klonvorgänge einer Ressourcengruppe oder Datenbank planen. Wenn Sie ein Backup regelmäßig klonen, können Sie mit dem Klon Applikationen entwickeln, Daten ausfüllen oder Daten wiederherstellen.

SnapCenter ermöglicht die Planung mehrerer Klonvorgänge zur gleichzeitigen Ausführung über mehrere Server hinweg.

Bevor Sie beginnen

- Stellen Sie beim Klonen auf eine eigenständige Datenbankinstanz sicher, dass der Mount-Point-Pfad vorhanden ist und dass es sich um eine dedizierte Festplatte handelt.
- Beim Klonen in eine Failover Cluster-Instanz (FCI) stellen Sie sicher, dass die Mount-Punkte vorhanden sind, dass es sich um eine freigegebene Festplatte handelt, und der Pfad und die FCI sollten zur gleichen SQL-Ressourcengruppe gehören.
- Wenn sich die Quelldatenbank oder die Zielinstanz auf einem gemeinsam genutzten Cluster-Volume (csv) befindet, befindet sich die geklonte Datenbank auf dem csv.

Stellen Sie für virtuelle Umgebungen (VMDK/RDM) sicher, dass der Bereitstellungspunkt eine dedizierte Festplatte ist.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit zu verwenden.

  Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

  Sie können die GET API verwenden, um den Wert der Taste anzuzeigen. SET-API wird nicht unterstützt.

- Die meisten Felder auf den Seiten des Clone Lifecycle Wizard sind selbsterklärend. In den folgenden Informationen werden die Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Ressourcengruppe oder -Datenbank aus, und klicken Sie dann auf **Lebenszyklus klonen**.
4. Führen Sie auf der Seite Optionen die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Auftragsname klonen	Geben Sie den Namen des Jobs für den Lebenszyklus des Klons an, der die Überwachung und Änderung des Lebenszyklusjobs unterstützt.
Klonserver	Wählen Sie den Host aus, auf dem der Klon platziert werden soll.
Kloninstanz	Wählen Sie die Kloninstanz aus, zu der Sie die Datenbank klonen möchten. Diese SQL-Instanz muss sich auf dem angegebenen Klon-Server befinden.

Für dieses Feld…	Tun Sie das…
Suffix klonen	Geben Sie ein Suffix ein, das an die Klondatenbank angehängt wird, um das es sich um einen Klon handelt. Jede SQL-Instanz, die zum Erstellen einer Clone-Ressourcengruppe verwendet wird, muss über einen eindeutigen Datenbanknamen verfügen. Wenn die Clone Resource Group beispielsweise eine Quelldatenbank „db1“ aus einer SQL-Instanz „inst1“ enthält und „db1“ in „inst1“ geklont wurde, sollte der Name der Klondatenbank „ db1*Clone*“ lauten. „Clone“ ist ein vom Benutzer definiertes Suffix, da die Datenbank in derselben Instanz geklont wird. Wenn “db1” zur SQL-Instanz „inst2“ geklont wird, kann der Name der Klondatenbank „db1“ bleiben (das Suffix ist optional), da die Datenbank auf eine andere Instanz geklont wird.
Automatisches Zuweisen von Mount-Punkten oder automatische Zuweisung von Volume-Mount-Punkten unter Pfad	Legen Sie fest, ob unter einem Pfad automatisch ein Mount-Punkt oder ein Volume-Mount-Punkt zugewiesen werden soll. Wenn Sie die Option auswählen, einen Volume-Bereitstellungspunkt unter einem Pfad automatisch zuzuweisen, können Sie ein bestimmtes Verzeichnis angeben. Die Mount-Punkte werden innerhalb dieses Verzeichnisses erstellt. Bevor Sie diese Option auswählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich eine Datenbank im Verzeichnis befindet, befindet sich die Datenbank nach dem Mount-Vorgang in einem ungültigen Status.

5. Wählen Sie auf der Seite Speicherort einen Speicherort aus, um einen Klon zu erstellen.
6. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.

   Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

   Das Standard-Skript-Timeout beträgt 60 Sekunden.

7. Führen Sie auf der Seite Zeitplan eine der folgenden Aktionen durch:
   - Wählen Sie **Jetzt ausführen** aus, wenn Sie den Klon-Job sofort ausführen möchten.
   - Wählen Sie **Configure Schedule** aus, wenn Sie bestimmen möchten, wie häufig der Klonvorgang stattfinden soll, wann der Klonzeitplan beginnen soll, an welchem Tag der Klonvorgang stattfinden soll, wann der Zeitplan abläuft und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.

8. Wählen Sie auf der Benachrichtigungsseite 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. Wenn Sie den Bericht über den ausgeführten Klonvorgang anhängen möchten, wählen Sie **Job-Bericht anhängen** aus.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

   Informationen zu EMS finden Sie unter "EMS-Datenerfassung managen"

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

Sie sollten den Klonprozess über die Seite **Monitor** > **Jobs** überwachen.

Überwachen Sie die Klonvorgänge von SQL 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 Jobdetails auf **Protokolle anzeigen**.

Klonvorgänge für SQL-Ressourcen abbrechen

Sie können Klonvorgänge in die Warteschlange abbrechen.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Klonvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Klonvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen ausgeführten Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Klonvorgänge abzubrechen.
- 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 Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Vorgang aus, und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Initiieren des Klonvorgangs auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite **Job Details** auf **Job abbrechen**.

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 **Manage Copies** 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.

Verwandte Informationen

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