Schützen Sie PostgreSQL

SnapCenter software

NetApp
January 09, 2026

Inhalt

Schützen Sie PostgreSQL

SnapCenter Plug-in für PostgreSQL

Übersicht über das SnapCenter Plug-in für PostgreSQL

Das SnapCenter Plug-in für PostgreSQL Cluster ist eine Host-seitige Komponente der NetApp SnapCenter Software, die ein applikationsspezifisches Datensicherungsmanagement von PostgreSQL-Clustern ermöglicht. Das Plug-in für PostgreSQL Cluster automatisiert das Backup, die Wiederherstellung und das Klonen von PostgreSQL-Clustern in einer SnapCenter-Umgebung.

SnapCenter unterstützt PostgreSQL-Konfigurationen mit einem und mehreren Clustern. Sie können das Plug-in für PostgreSQL-Cluster sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird PostgreSQL als manuelle Ressource unterstützt.

Nach der Installation des Plug-in für PostgreSQL-Clusters können Sie SnapCenter mit NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Mithilfe des Plug-ins in mit NetApp SnapVault Technologie lässt sich darüber hinaus eine Disk-to-Disk-Backup-Replizierung zur Einhaltung von Standards durchführen.

Das SnapCenter Plug-in für PostgreSQL unterstützt NFS und SAN unter ONTAP und Azure NetApp File Storage Layouts.

Das virtuelle VMDK, vVol und RDM Storage Layout wird unterstützt.

Was Sie mit dem SnapCenter Plug-in für PostgreSQL tun können

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

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

Funktionen des SnapCenter Plug-in für PostgreSQL

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Um mit dem Plug-in für PostgreSQL-Cluster zu arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter.

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore- und Klonvorgänge über alle Plug-ins hinweg, die zentralisierte Berichterstellung, die Schnellübersicht über Dashboard-Ansichten, die Einrichtung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Jobs in allen Plug-ins.

- **Automatisierte zentrale Verwaltung**

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

- **Technologie für unterbrechungsfreie NetApp Snapshot Kopien**

  SnapCenter verwendet NetApp Snapshot-Technologie mit dem Plug-in für PostgreSQL-Cluster, um Ressourcen zu sichern.

Der Einsatz des Plug-in für PostgreSQL bietet zudem folgende Vorteile:

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

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

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

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

- Unterstützung der Snapshot-Funktion von ONTAP für Konsistenzgruppe (CG) beim Erstellen von Backups.
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

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

- Fähigkeit, Snapshots mit externen Befehlen zu erstellen.
- Unterstützung für Linux LVM auf XFS-Dateisystem.

Von SnapCenter Plug-in für PostgreSQL unterstützte Speichertypen

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

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung

Maschine	Storage-Typ
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datastores • VMDKs auf VMFS • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Für das PostgreSQL-Plug-in sind mindestens ONTAP-Berechtigungen 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 9.12.1 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun erstellen
  - lun erstellen
  - lun erstellen
  - lun löschen
  - lun Initiatorgruppe hinzufügen
  - lun-Initiatorgruppe wird erstellt
  - lun-Initiatorgruppe löschen
  - lun igroup umbenennen

- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- 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
    - Volume Snapshot modify-snaplock-expiry-time
    - 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
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle
    - Netzwerkschnittstelle wird angezeigt
    - vserver

Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replication für PostgreSQL vor

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 für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang 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".

Backup-Strategie für PostgreSQL

Backup-Strategie für PostgreSQL definieren

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

Über diese Aufgabe

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

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.

2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Entscheiden Sie, ob Sie eine Richtlinie auf Basis von Snapshot Kopien erstellen möchten, um applikationskonsistente Snapshots des Clusters zu sichern.
5. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
6. Legen Sie den Aufbewahrungszeitraum für die Snapshots auf dem Quell-Storage-System und dem SnapMirror Ziel fest.
7. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Automatische Ermittlung von Ressourcen auf Linux-Host

Ressourcen sind PostgreSQL-Cluster und Instanzen auf dem Linux-Host, die von SnapCenter gemanagt werden. Nach der Installation des SnapCenter Plug-ins für PostgreSQL werden die PostgreSQL-Cluster aller Instanzen auf diesem Linux-Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Art der unterstützten Backups

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot Kopien basierenden Backup-Typ für PostgreSQL Cluster.

Backup auf Basis von Snapshot Kopien

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

Wie das SnapCenter Plug-in für PostgreSQL Snapshots von Konsistenzgruppen verwendet

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

Sie können auch die Wartezeit für den Speicher-Controller angeben, um Snapshots konsistent zu gruppieren. Die verfügbaren Optionen für Wartezeiten sind **dringend**, **Medium** und **entspannt**. Sie können auch die WAFL-Synchronisierung (Write Anywhere File Layout) während eines konsistenten Gruppen-Snapshots aktivieren oder deaktivieren. WAFL Sync verbessert die Performance eines Consistency Group Snapshots.

So managt SnapCenter die Organisation von Daten-Backups

SnapCenter managt die Durchführung von Daten-Backups auf der Storage-System- und File-System-Ebene.

Die Snapshots auf dem primären oder sekundären Speicher und die entsprechenden Einträge im PostgreSQL-Katalog werden basierend auf den Aufbewahrungseinstellungen gelöscht.

Überlegungen zur Festlegung von Backup-Zeitplänen für PostgreSQL

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

Backup-Zeitpläne haben zwei Teile:

- Backup-Häufigkeit (Häufigkeit der Durchführung von Backups)

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

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

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

Anzahl der für PostgreSQL erforderlichen Backup-Jobs

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

Backup-Namenskonventionen für Plug-in für PostgreSQL-Cluster

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Snapshot-Namensformat beim Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Restore- und Recovery-Strategie für PostgreSQL

Definieren Sie eine Wiederherstellungs- und Wiederherstellungsstrategie für PostgreSQL-Ressourcen

Sie müssen vor dem Wiederherstellen und Wiederherstellen des Clusters eine Strategie definieren, damit Sie Wiederherstellungs- und Wiederherstellungsvorgänge erfolgreich durchführen können.

Es wird nur die manuelle Wiederherstellung des Clusters unterstützt.

Schritte

1. Ermitteln Sie die Wiederherstellungsstrategien, die für manuell hinzugefügte PostgreSQL-Ressourcen unterstützt werden
2. Ermitteln Sie die für automatisch erkannte PostgreSQL-Cluster unterstützten Wiederherstellungsstrategien
3. Geben Sie die Art der Recovery-Vorgänge an, die Sie ausführen möchten.

Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte PostgreSQL-Ressourcen unterstützt werden

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können.

Manuell hinzugefügte PostgreSQL-Ressourcen können nicht wiederhergestellt werden.

Komplette Ressourcenwiederherstellung

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

Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshots, die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

HINWEIS: Plug-in für PostgreSQL erstellt ein Backup_Label und tablespace_map im Ordner */<OS_temp_folder>/postgresql_sc_Recovery*<Restore_JobId>/_, um die manuelle Wiederherstellung zu unterstützen.

Art der Wiederherstellungsstrategie, die für automatisch erkannte PostgreSQL unterstützt wird

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können.

Vollständige Ressourcenwiederherstellung ist die Wiederherstellungsstrategie, die für automatisch erkannte PostgreSQL-Cluster unterstützt wird. Dadurch werden alle Volumes, qtrees und LUNs einer Ressource

wiederhergestellt.

Arten von Wiederherstellungsvorgängen für automatisch erkannte PostgreSQL

Das SnapCenter Plug-in für PostgreSQL unterstützt Single File SnapRestore und stellt Wiederherstellungsarten für automatisch erkannte PostgreSQL-Cluster her.

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

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn der ausgewählte Backup von einem sekundären Standort SnapMirror oder SnapVault stammt und die Option **Complete Resource** ausgewählt ist

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

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem sekundären Standort SnapMirror oder SnapVault ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Für PostgreSQL-Cluster unterstützte Arten von Wiederherstellungsvorgängen

Mit SnapCenter können Sie verschiedene Arten von Wiederherstellungsvorgängen für PostgreSQL-Cluster durchführen.

- Stellen Sie den Cluster bis zum letzten Status wieder her
- Wiederherstellung des Clusters bis zu einem bestimmten Zeitpunkt

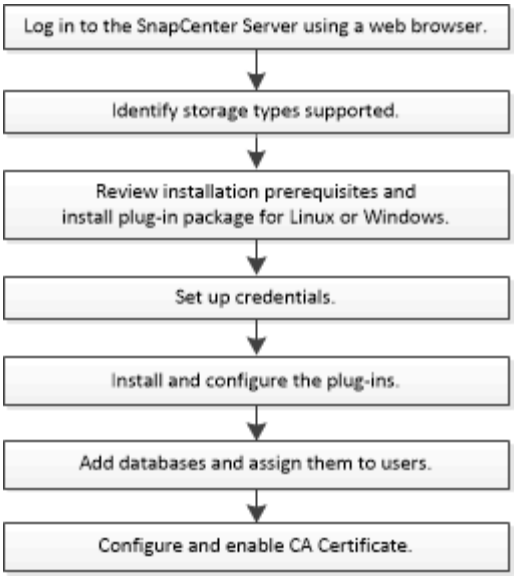
  Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.

SnapCenter bietet auch die Option Keine Wiederherstellung für PostgreSQL-Cluster.

Bereiten Sie die Installation des SnapCenter-Plug-ins für PostgreSQL vor

Installationsworkflow des SnapCenter Plug-in für PostgreSQL

Sie sollten das SnapCenter-Plug-in für PostgreSQL installieren und einrichten, wenn Sie PostgreSQL-Cluster schützen möchten.



Voraussetzungen, um Hosts hinzuzufügen und das SnapCenter-Plug-in für PostgreSQL zu installieren

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

- Sie müssen Java 11 auf Ihrem Host installiert haben.

  IBM Java wird auf Windows- und Linux-Hosts nicht unterstützt.

- Für Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „`LocalSystem`“ ausgeführt werden. Dies ist das Standardverhalten, wenn Plug-in for PostgreSQL als Domänenadministrator installiert wird.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört. Das SnapCenter-Plug-in für Microsoft Windows wird standardmäßig mit dem PostgreSQL-Plug-in auf Windows-Hosts implementiert.
- SnapCenter Server sollte Zugriff auf den 8145 oder benutzerdefinierten Port des Plug-in für PostgreSQL-Hosts haben.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Während der Installation von Plug-in für PostgreSQL auf einem Windows-Host wird das SnapCenter-Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Windows-Host installiert haben.

  "Laden Sie JAVA für alle Betriebssysteme herunter"

Linux-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

  "Laden Sie JAVA für alle Betriebssysteme herunter"

- Bei PostgreSQL-Clustern, die auf einem Linux-Host ausgeführt werden, wird das SnapCenter-Plug-in für UNIX automatisch installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-in-Installation haben.

Zusätzliche Befehle

Um einen zusätzlichen Befehl auf dem SnapCenter Plug-in für PostgreSQL auszuführen, müssen Sie ihn in die Datei *allowed_commands.config* einfügen.

- Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Um zusätzliche Befehle auf dem Plug-in-Host zuzulassen, öffnen Sie die Datei *allowed_commands.config* in einem Editor. Geben Sie jeden Befehl in eine separate Zeile ein, und bei den Befehlen wird die Groß-/Kleinschreibung nicht beachtet. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen („) einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: Mount Befehl: Umount Befehl: "C:\Programme\NetApp\SnapCreator commands\sdcli.exe" Befehl: myscript.bat

Wenn die Datei *allowed_commands.config* nicht vorhanden ist, werden die Befehle oder die Ausführung des Skripts blockiert, und der Workflow schlägt mit dem folgenden Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Wenn der Befehl oder das Skript nicht in *allowed_commands.config* vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit folgendem Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Sie sollten keinen Platzhaltereintrag (*) verwenden, um alle Befehle zuzulassen.

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter kann ein Benutzer, der kein Root-Benutzer ist, das SnapCenter-Plug-in-Paket für Linux installieren und den Plug-in-Prozess starten. Die Plug-in-Prozesse werden als effektiver nicht-Root-Benutzer ausgeführt. Sie sollten sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Stellen Sie für den Benutzer, der nicht root ist, sicher, dass der Name des Benutzers, der nicht root ist, und die Gruppe des Benutzers identisch sein sollten.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren der Konfigurationsdatei neu.

  Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Über diese Aufgabe

Sie sollten sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu ermöglichen:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter-Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux hinzu.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- _C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_plugins_checksum.txt _ wenn SnapCenter-Server auf dem Windows-Host installiert ist.
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

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 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool" .

Element	Anforderungen
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.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting Bundle • PowerShell Core 7.4.2 Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

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

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

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

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit der Datensicherungsvorgänge. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Anmeldedaten für das SnapCenter-Plug-in für PostgreSQL einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldeinformationen für die Durchführung von Datensicherungsvorgängen auf Clustern oder Windows-Filesystemen erstellen.

Über diese Aufgabe

- Linux-Hosts

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

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

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

- Windows Hosts

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

  Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf

dem Remote-Host.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

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

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

5. Klicken Sie auf **OK**.

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

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 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 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 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 PostgreSQL

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

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

Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter-Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zum Verwalten von Hosts.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Group Managed Service-Konto unter Windows Server 2016 oder höher für PostgreSQL"

Über diese Aufgabe

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

Schritte

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

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

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

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Wenn Sie das Plug-in für PostgreSQL mit der REST-API installieren, müssen Sie die Version als 3.0 übergeben. Beispiel: PostgreSQL:3.0

6. (Optional) Klicken Sie Auf **Weitere Optionen**.

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

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

7. Klicken Sie Auf **Absenden**.

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

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

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

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

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

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

9. Überwachen Sie den Installationsfortschritt.
   - Für das Windows Plug-in befinden sich die Installations- und Upgrade-Protokolle unter: *C:\Windows\SnapCenter Plug-in\Install*<JOBID>_
   - Für Linux-Plug-ins befinden sich die Installationsprotokolle unter: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ und die Upgrade-Protokolle befinden sich unter: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

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

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

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 Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

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

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

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

Installieren Sie das SnapCenter-Plug-in für PostgreSQL auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten das SnapCenter-Plug-in für PostgreSQL-Cluster mithilfe der

Benutzeroberfläche (UI) von SnapCenter installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie das Plug-in für PostgreSQL-Cluster entweder im Konsolenmodus oder im unbeaufsichtigten Modus über die Befehlszeilenschnittstelle (CLI) installieren.

Bevor Sie beginnen

- Sie sollten das Plug-in für PostgreSQL-Cluster auf jedem Linux-Host installieren, auf dem sich der PostgreSQL-Client befindet.
- Der Linux-Host, auf dem Sie das SnapCenter-Plug-in für PostgreSQL-Cluster installieren, muss die Anforderungen an die abhängige Software, den Cluster und das Betriebssystem erfüllen.

  Der "Interoperabilitätsmatrix-Tool (IMT)" Enthält die aktuellsten Informationen zu den unterstützten Konfigurationen.

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

Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter-Plug-ins-Pakets für Linux (snapcenter_linux_Host_Plugin.bin) von C:\ProgramData\NetApp\SnapCenter\Package Repository auf den Host, auf dem Sie das Plug-in für PostgreSQL installieren möchten.

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

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

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

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

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

Server hinzu.

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

Überwachen Sie den Status der Installation von Plug-in für PostgreSQL

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.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

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

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

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

Importieren von CA-Zertifikaten

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

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins 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"
```

Konfigurieren Sie das CA-Zertifikat für den SnapCenter-PostgreSQL-Plug-ins-Dienst auf dem Linux-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter-Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter */opt/NetApp/snapcenter/scc/etc* befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.

Schritte

1. Sie können das Standardkennwort für den Plug-In-Keystore aus der Eigenschaftendatei des Plug-In-Agenten abrufen.

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

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

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

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

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

> Das Kennwort für den Plug-In-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den Plug-In-Truststore konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

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

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder
Zwischenzertifikate für den Plug-In-Truststore konfiguriert haben.
```

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

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

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

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

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

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

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

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

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

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

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

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

Über diese Aufgabe

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

Schritte

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

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

Konfigurieren Sie das CA-Zertifikat für den SnapCenter-PostgreSQL-Plug-ins-Dienst auf dem Windows-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-

In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter-Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-Ins verwenden die Datei *keystore.jks*, die sich unter *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.

Schritte

1. Sie können das Standardkennwort für den Plug-In-Keystore aus der Eigenschaftendatei des Plug-In-Agenten abrufen.

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

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

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

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

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

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

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

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

   > Das Kennwort für den Plug-In-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den Plug-In-Truststore konfigurieren.

Schritte

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

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

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

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-Truststore konfiguriert haben.

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

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-in-Schlüsselspeicher enthält: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

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

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

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

   Keytool -list -V -keystore keystore.jks

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

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

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

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

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter-Plug-Ins

Über diese Aufgabe

- Informationen zum Herunterladen der neuesten CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten im SnapCenter CA-Zertifikat".

- SnapCenter-Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter-Plug-ins ist *'C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

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 "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.

Bereiten Sie sich auf die Datensicherung vor

Voraussetzungen für die Verwendung des SnapCenter Plug-ins für PostgreSQL

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

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

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

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von PostgreSQL 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.

- Bei Ressourcen handelt es sich in der Regel um PostgreSQL-Cluster, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter-Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

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

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

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

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

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

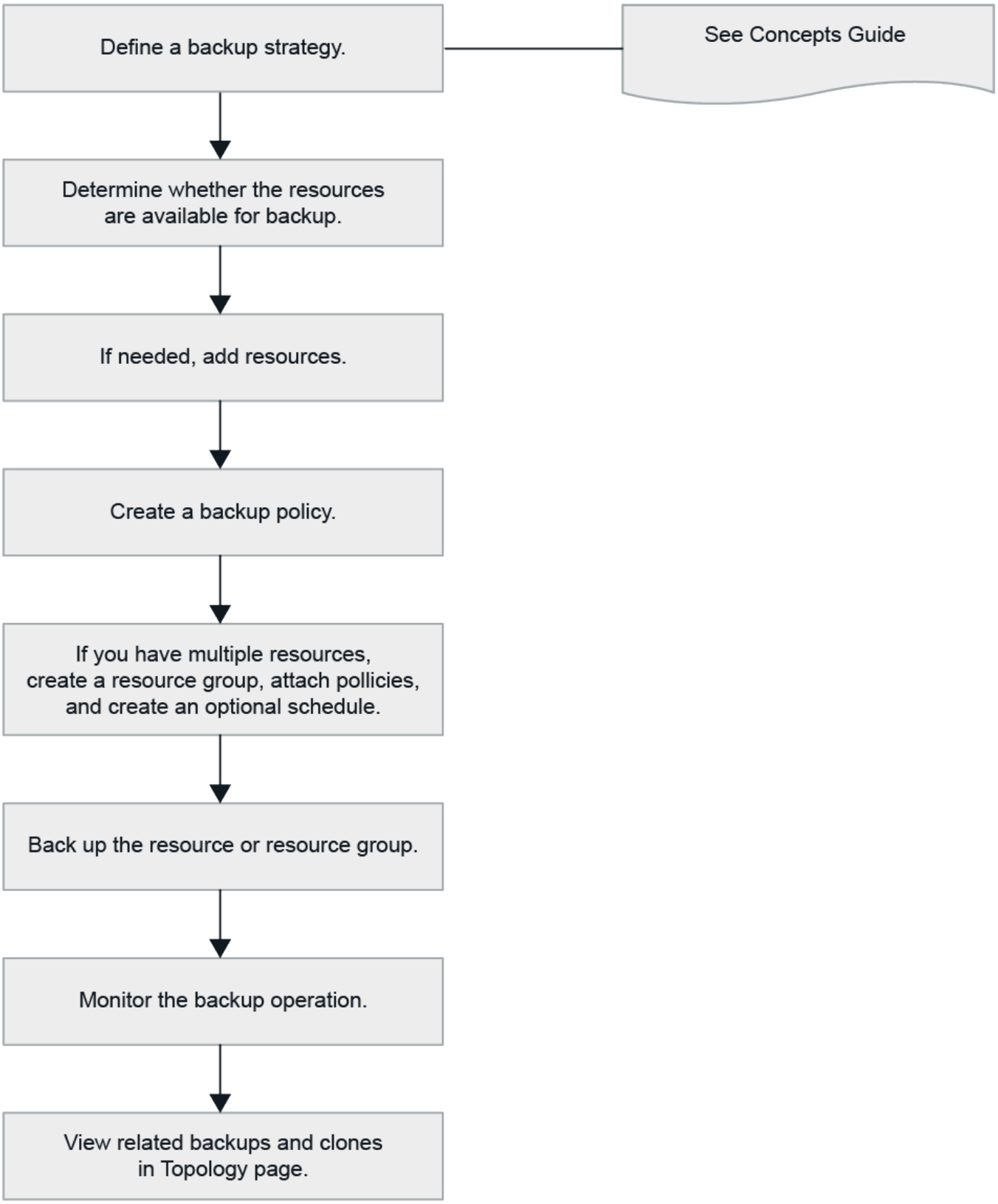
durchführen.

Sichern Sie PostgreSQL-Ressourcen

Sichern Sie PostgreSQL-Ressourcen

Sie können entweder ein Backup einer Ressource (eines Clusters) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Cluster, das Management von Backup-Richtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Backups und die Überwachung von Vorgängen.

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



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

Automatische Erkennung der Cluster

Ressourcen sind PostgreSQL-Cluster auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren PostgreSQL-Cluster erkannt haben.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts und das Einrichten der Verbindungen des Speichersystems ausgeführt haben.
- Das SnapCenter Plug-in für PostgreSQL unterstützt keine automatische Erkennung der Ressourcen in virtuellen RDM/VMDK-Umgebungen.

Über diese Aufgabe

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

Die automatisch ermittelten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

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

   Sie können dann auf * * klicken, um den Filterbereich zu schließen.

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

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

   - Wenn sich das Cluster auf einem NetApp-Speicher befindet und nicht geschützt ist, wird in der Spalte Gesamtstatus nicht geschützt angezeigt.
   - Wenn sich das Cluster auf einem NetApp-Speichersystem befindet und geschützt ist und kein Backup durchgeführt wird, wird in der Spalte Gesamtstatus die Meldung Sicherung nicht ausgeführt angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

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

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

Die automatische Erkennung wird auf dem Windows-Host nicht unterstützt. Sie müssen PostgreSQL-Cluster-Ressourcen manuell hinzufügen.

Bevor Sie beginnen

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

Über diese Aufgabe

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter-Plug-in für PostgreSQL aus der Dropdown-Liste aus, und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite Ressourcen auf **PostgreSQL-Ressourcen hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Cluster-Namen an.
Host-Name	Geben Sie den Hostnamen ein.
Typ	Wählen Sie Cluster aus.
Instanz	Geben Sie den Namen der Instanz an, die das übergeordnete Objekt des Clusters ist.
Anmeldedaten	Wählen Sie die Anmeldeinformationen aus, oder fügen Sie Informationen zu den Anmeldeinformationen hinzu. Dies ist optional.

4. Wählen Sie auf der Seite „Storage Footprint bereitstellen“ einen Speichertyp aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Save**.

   Optional: Sie können auf das * -Symbol klicken , um weitere Volumes, LUNs und qtrees von anderen Storage-Systemen hinzuzufügen.

5. Optional: Geben Sie auf der Seite Resource Settings für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für PostgreSQL-Plug-in ein
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Cluster werden zusammen mit Informationen wie dem Hostnamen, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt

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

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

Nachdem Sie fertig sind

- Nachdem Sie die Cluster hinzugefügt haben, können Sie die Details zum PostgreSQL-Cluster ändern.
- Die migrierten Ressourcen (Tablespace und Cluster) von SnapCenter 5.0 werden in SnapCenter 6.0 als PostgreSQL-Cluster-Typ gekennzeichnet.
- Wenn Sie die manuell hinzugefügten Ressourcen ändern, die von SnapCenter 5.0 oder früher migriert werden, gehen Sie auf der Seite **Ressourceneinstellungen** für benutzerdefinierte Schlüsselwertpaare folgendermaßen vor:
  - Geben Sie den Begriff "PORT" im Feld **Name** an.
  - Geben Sie die Portnummer im Feld **Wert** an.

Erstellen Sie Backup-Richtlinien für PostgreSQL

Bevor Sie PostgreSQL-Ressourcen mit SnapCenter sichern, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen finden Sie unter Definieren einer Datensicherungsstrategie für PostgreSQL-Cluster.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das Hinzufügen von Ressourcen ausführen.
- Der SnapCenter Administrator muss Ihnen die SVMs sowohl für die Quell- als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots zu einem Spiegel oder Vault replizieren.

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

Über diese Aufgabe

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.
  - Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

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

4. Geben Sie auf der Seite Name den Richtliniennamen und Details ein.
5. Führen Sie auf der Seite Richtlinientyp folgende Schritte aus:
   a. Wählen Sie den Speichertyp aus.
   b. Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

      Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.
6. Führen Sie auf der Seite Backup and Replication die folgenden Aktionen durch:
   a. Geben Sie die Zeitplanhäufigkeit an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

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

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

   a. Geben Sie im Abschnitt Snapshot-Einstellungen die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite **Sicherungstyp** ausgewählten Zeitplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Kopien, die behalten werden sollen**, und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird. Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der ONTAP -Version unterstützt wird.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Kopien behalten für**, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots vor dem Löschen aufbewahren möchten.
Sperrzeitraum für Snapshot-Kopien	Wählen Sie **Sperrzeitraum für Snapshot-Kopien** und geben Sie Tage, Monate oder Jahre an. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

7. Wählen Sie eine Richtlinienbezeichnung aus.

   Sie können primären Snapshots SnapMirror Labels für die Remote-Replikation zuweisen, sodass die primären Snapshots den Snapshot-Replikationsvorgang von SnapCenter auf sekundäre ONTAP -Systeme auslagern können. Dies kann erfolgen, ohne die Option SnapMirror oder SnapVault auf der Richtlinienseite zu aktivieren.

8. Wählen Sie im Abschnitt sekundäre Replikationsoptionen auswählen eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Wenn die Sicherungsbeziehung in ONTAP vom Typ „Mirror and Vault“ ist und Sie nur diese Option auswählen, wird auf dem primären Snapshot nicht an das Zielsystem übertragen, sondern auf dem Zielsystem aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wurde, um einen Wiederherstellungsvorgang durchzuführen, wird die folgende Fehlermeldung angezeigt: Sekundärer Speicherort ist für das ausgewählte Backup mit vaulted/mirrored nicht verfügbar. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Siehe "Zeigen Sie auf der Seite Topologie ressourcenbezogene PostgreSQL-Backups und Clones an".

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert. Weitere Informationen zu SnapLock Vault finden Sie unter Festsetzen von Snapshots auf WORM in einem Vault Ziel Siehe "Zeigen Sie auf der Seite Topologie ressourcenbezogene PostgreSQL-Backups und Clones an".
Anzahl der Wiederholversuche	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

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

Über diese Aufgabe

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator

sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

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

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

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

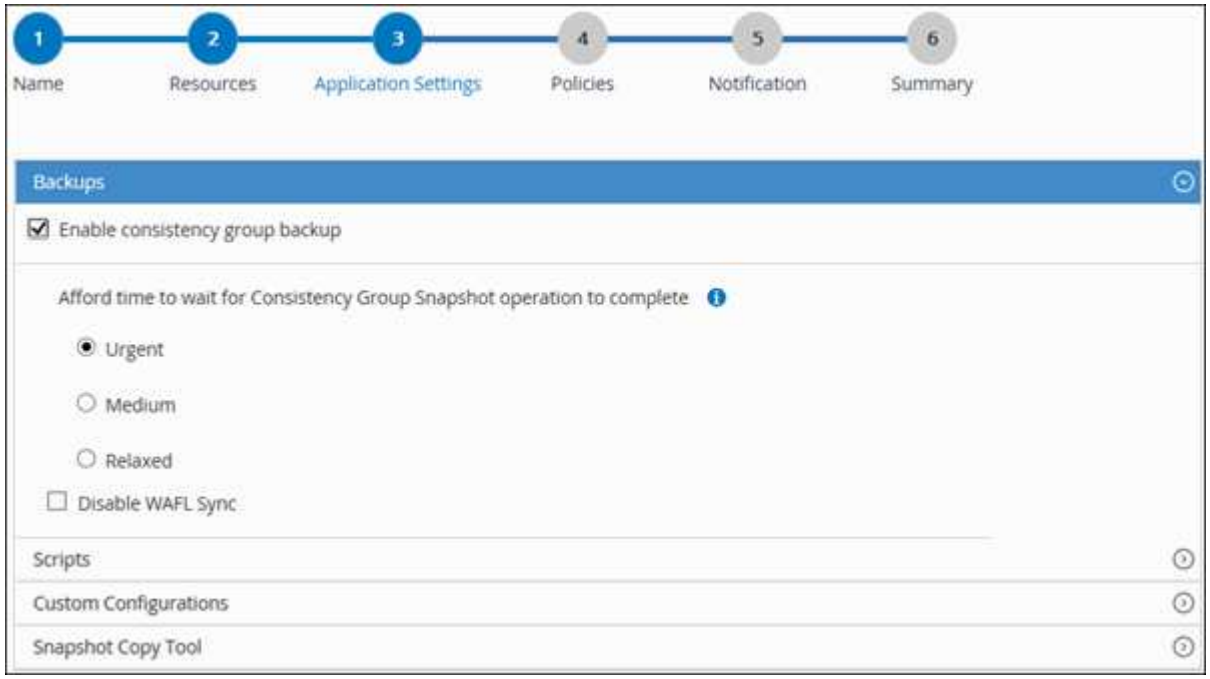
   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

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

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

Für dieses Feld…	Tun Sie das…
Warten Sie die Dauer des Snapshot-Vorgangs der Konsistenzgruppe	Wählen Sie **dringend**, **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+ 

a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

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

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

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
ARCHIVE_LOG_DIR	Change_info_Directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Dateierweiterung der Archivprotokolldatei an. Wenn die Archivprotokolldatei beispielsweise log_backup_0_1.log heißt, geben Sie .log als Dateierweiterung an.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüssel-Wert-Paare werden für PostgreSQL Linux Plug-in-Systeme unterstützt und nicht für PostgreSQL Cluster unterstützt, die als zentralisiertes Windows Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot Copy Tool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu verwenden und das Filesystem vor dem Erstellen eines Snapshots in einen konsistenten Zustand zu versetzen. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.

Ihre Situation	Dann…
Um den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen.

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

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

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

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

   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf * * für die Richtlinie, die Sie konfigurieren möchten.

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

      Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

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

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

8. Wählen Sie auf der 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. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

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

Erstellen Sie Ressourcengruppen und aktivieren Sie sekundären Schutz für PostgreSQL-Ressourcen auf ASA r2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA r2-Systemen befinden. Sie können auch den sekundären Schutz bereitstellen, während Sie die Ressourcengruppe erstellen.

Bevor Sie beginnen

- Sie sollten sicherstellen, dass Sie nicht sowohl ONTAP 9.x-Ressourcen als auch ASA r2-Ressourcen zur gleichen Ressourcengruppe hinzufügen.
- Sie sollten sicherstellen, dass keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen vorhanden ist.

Über diese Aufgabe

- Der sekundäre Schutz ist nur verfügbar, wenn der angemeldete Benutzer der Rolle zugewiesen ist, die die

Funktion **SecondaryProtection** aktiviert hat.

- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nach dem Erstellen der primären und sekundären Konsistenzgruppen wird die Ressourcengruppe aus dem Wartungsmodus versetzt.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf der Seite Ressourcen auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   a. Geben Sie im Feld Name einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

   b. Geben Sie eine oder mehrere Beschriftungen in das Feld Tag ein, um später nach der Ressourcengruppe zu suchen.

      Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.

   c. Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

      Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

   d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

      Sie sollten bei Bedarf genau das gleiche Ziel verwenden, wie es in der Anwendung einschließlich Präfix festgelegt wurde.

4. Wählen Sie auf der Seite Ressourcen den Hostnamen der Datenbank aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden im Abschnitt Verfügbare Ressourcen nur dann aufgelistet, wenn die Ressource erfolgreich ermittelt wurde. Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

5. Wählen Sie die ASA r2-Ressourcen im Abschnitt „Verfügbare Ressourcen“ aus, und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.
6. Wählen Sie auf der Seite Anwendungseinstellungen die Sicherungsoption aus.
7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

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

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

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

Dabei ist *Policy_Name* der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

8. Wenn der sekundäre Schutz für die ausgewählte Richtlinie aktiviert ist, wird die Seite sekundärer Schutz angezeigt, und Sie müssen die folgenden Schritte ausführen:

a. Wählen Sie den Typ der Replikationsrichtlinie aus.

Die Richtlinie für die synchrone Replizierung wird nicht unterstützt.

b. Geben Sie das Suffix für die Konsistenzgruppe an, das Sie verwenden möchten.

c. Wählen Sie in den Drop-Downs Ziel-Cluster und Ziel-SVM den zu verwendenden Peering-Cluster und die SVM aus.

Cluster und SVM-Peering werden von SnapCenter nicht unterstützt. Sie sollten System Manager oder ONTAP CLIs verwenden, um Cluster- und SVM-Peering durchzuführen.

Wenn die Ressourcen bereits außerhalb von SnapCenter geschützt sind, werden diese Ressourcen im Abschnitt sekundäre geschützte Ressourcen angezeigt.

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

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

b. Klicken Sie Auf  In der Spalte Configure Schedules (Zeitpläne konfigurieren), um den Überprüfungsplan für alle Zeitplantypen der Richtlinie zu konfigurieren.

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** und wählen Sie dann den Terminplantyp aus der Dropdown-Liste aus.

d. Wählen Sie **am sekundären Standort überprüfen**, um Ihre Backups auf dem sekundären Speichersystem zu überprüfen.

e. Klicken Sie auf **OK**.

Die konfigurierten Überprüfungszeitpläne sind in der Spalte „angewendete Zeitpläne“ aufgeführt.

2. 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.

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

Erstellen Sie mit PowerShell Cmdlets für PostgreSQL eine Verbindung zum Speichersystem und Zugangsdaten

Sie müssen eine Storage Virtual Machine (SVM)-Verbindung und Zugangsdaten erstellen, bevor Sie mit PowerShell Cmdlets PostgreSQL-Cluster sichern, wiederherstellen oder klonen.

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.

  Host-Plug-in-Installationen dürfen während des Hinzufügens einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Cluster-Status möglicherweise in der SnapCenter-GUI als „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

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

Schritte

1. Starten Sie eine PowerShell Core-Verbindungssitzung mit dem Cmdlet "Open-SmConnection".

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

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

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

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

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

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

4. Fügen Sie den PostgreSQL-Kommunikationshost dem SnapCenter-Server hinzu.

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

5. Installieren Sie das Paket und das SnapCenter-Plug-in für PostgreSQL auf dem Host.

   Für Linux:

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

   Für Windows:

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

6. Pfad auf SQLLIB festlegen.

   Für Windows verwendet das PostgreSQL-Plug-in den Standardpfad für den SQLLIB-Ordner: „C:\Programme\IBM\SQLLIB\BIN“

   Wenn Sie den Standardpfad überschreiben möchten, verwenden Sie den folgenden Befehl.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

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 "SnapCenter Software Cmdlet Referenzhandbuch".

Sichern Sie PostgreSQL

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

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Stellen Sie für Backup-Vorgänge auf Basis von Snapshot Kopien sicher, dass alle Mandanten-Cluster gültig und aktiv sind.
- Für Pre- und Post-Befehle für Stilllegung-, Snapshot- und Stilllegung-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host über die folgenden Pfade verfügbar sind:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Wenn die Befehle in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

UI von SnapCenter

Schritte

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

   Wählen Sie * * , und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um das Filterfenster zu schließen.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Seite Ressource **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.
5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   - Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

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

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

   - Wählen Sie den Pfeil von **Scripts** aus, um Pre- und Post-Befehle für Stilllegung-, Snapshot- und Unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.
   - Wählen Sie den Pfeil **Custom Configurations**, und geben Sie dann die für alle Jobs, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.
   - Wählen Sie den Pfeil **Snapshot Copy Tool** aus, um das Werkzeug zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter zum Verwenden des Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen eines Snapshots einzugeben	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um einen Snapshot zu erstellen.

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

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

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

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

   b. Wählen Sie * * in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann **OK** aus.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

7. Wählen Sie auf der 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. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

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

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

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

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

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

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

PowerShell Commandlets

Schritte

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

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

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Fügen Sie manuelle Ressourcen mit dem Cmdlet "Add-SmResources" hinzu.

   Dieses Beispiel zeigt, wie eine PostgreSQL-Instanz hinzugefügt wird:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.
4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.
5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

   ```
   C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Dieses Beispiel sichert eine geschützte Ressource:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

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

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

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

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

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

Sichern von Ressourcengruppen

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

Bevor Sie beginnen

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

Über diese Aufgabe

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 durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie , auswählen und dann das Tag auswählen. Sie können dann auswählen , um das Filterfenster zu schließen.
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 **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Überwachen von PostgreSQL-Backup-Vorgängen

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 hier , um die Liste so zu filtern, dass 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.

   Obwohl der Status des Sicherungsauftrags angezeigt wird , wird beim Klicken auf Jobdetails möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs 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 Datensicherungsvorgänge auf PostgreSQL-Clustern im Aktivitätsbereich

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.

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 den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Job-Details** aufgeführt.

Backup-Vorgänge für PostgreSQL abbrechen

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

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

Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *, um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

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

Zeigen Sie PostgreSQL-Backups und Clones auf der Seite Topologie an

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

Über diese Aufgabe

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

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

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

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

Auf der Seite 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.

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

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

   Im Abschnitt **Summary Card** wird die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Clones angezeigt.

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

   Wenn ein SnapLock-fähiges Backup durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die primäre und sekundäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen wird. Ein wöchentlicher Zeitplan aktualisiert auch die primäre und sekundäre SnapLock-Ablaufzeit, die von ONTAP abgerufen wird.

   Wenn die Applikationsressource über mehrere Volumes verteilt ist, ist die SnapLock-Ablaufzeit für das Backup die längste SnapLock-Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock-Ablaufzeit wird von ONTAP abgerufen.

   Nach On-Demand-Backup, durch Klicken auf die Schaltfläche * Aktualisieren* aktualisiert die Details der Sicherung oder des Klons.

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

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

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

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

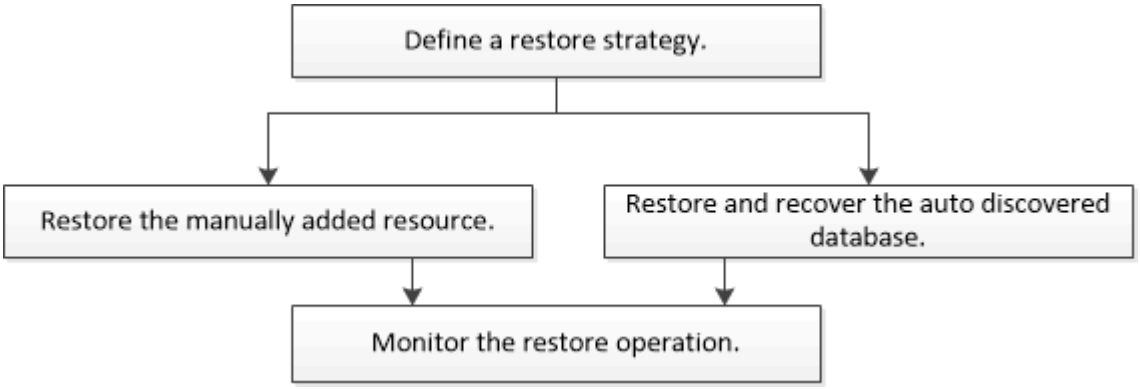
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie anschließend auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

PostgreSQL wiederherstellen

Wiederherstellung des Workflows

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

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



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

"SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups

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

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*

◦ Standardspeicherort auf dem Linux-Host: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Wenn die Befehle in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

Schritte

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

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

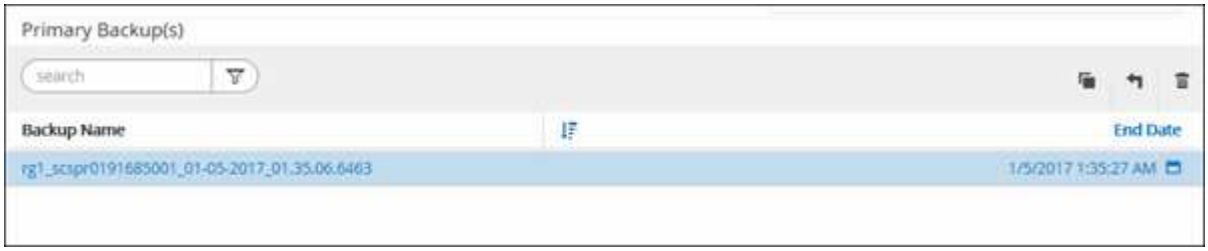
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

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

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

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



6. Wählen Sie auf der Seite Wiederherstellungsbereich die Option **komplette Ressource** aus.

   a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumes des PostgreSQL-Clusters wiederhergestellt.

      Wenn die Ressource Volumes oder qtrees enthält, werden die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf denselben Volumes oder qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

      Sie können mehrere LUNs auswählen.

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

7. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. 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. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

PowerShell Commandlets

Schritte

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

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

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:

```
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 "SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellung und Wiederherstellung einer automatisch erkannten Cluster-Sicherung

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

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem

unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:

- Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Wenn die Befehle in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Dateibasierte Backup-Kopien können nicht aus SnapCenter wiederhergestellt werden.
- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Automatische Wiederherstellung wird nicht unterstützt.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

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

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

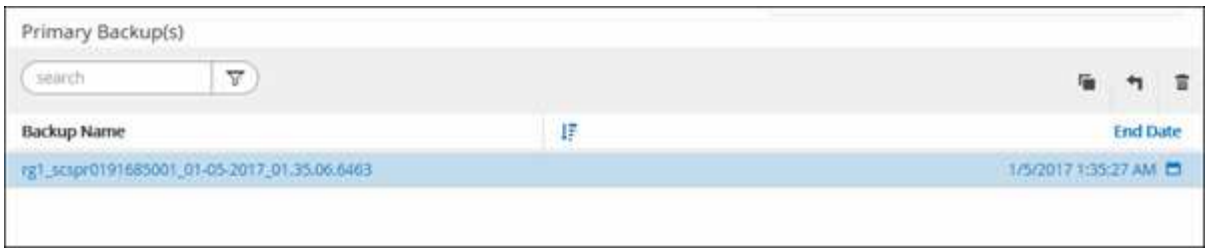
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

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

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

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



6. Wählen Sie auf der Seite Wiederherstellungsumfang die Option **komplette Ressource** aus, um die konfigurierten Datenvolumes des PostgreSQL-Clusters wiederherzustellen.
7. Wählen Sie auf der Seite Recovery Scope eine der folgenden Optionen aus:

Sie suchen…	Tun Sie das…
Möchten so nah wie möglich bis zur aktuellen Zeit wiederherstellen	Wählen Sie **Wiederherstellen in aktuellster Zustand**. Bei einzelnen Container-Ressourcen legen Sie einen oder mehrere Backup-Standorte für Protokolle und Kataloge fest.
Wiederherstellung auf den angegebenen Zeitpunkt	Wählen Sie **Wiederherstellen zu Zeitpunkt**. a. Geben Sie Datum und Uhrzeit ein. Geben Sie Datum und Uhrzeit ein. Der PostgreSQL Linux-Host befindet sich beispielsweise in Sunnyvale, Kalifornien, und der Benutzer in Raleigh, NC, stellt die Protokolle in SnapCenter wieder her. Wenn der Benutzer eine Wiederherstellung auf 5 a.m durchführen will. Sunnyvale, CA, dann muss der Benutzer die Browser-Zeitzone auf die PostgreSQL Linux-Host-Zeitzone einstellen, die GMT-07:00 ist und das Datum und die Uhrzeit als 5:00 Uhr angeben
Möchten Sie nicht wiederherstellen	Wählen Sie **Keine Wiederherstellung**.

Manuell hinzugefügte PostgreSQL-Ressourcen können nicht wiederhergestellt werden.

Das SnapCenter-Plugin für PostgreSQL erstellt ein Backup_Label und eine Tablespace_Map im Ordner */<OS_temp_folder>/postgresql_sc_Recovery*<Restore_JobId>/_, um eine manuelle Wiederherstellung zu ermöglichen.

1. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

2. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

3. 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. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

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

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:

```
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 "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen Sie die PostgreSQL-Wiederherstellungsvorgänge

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 hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet 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.

Klonen von PostgreSQL-Ressourcen-Backups

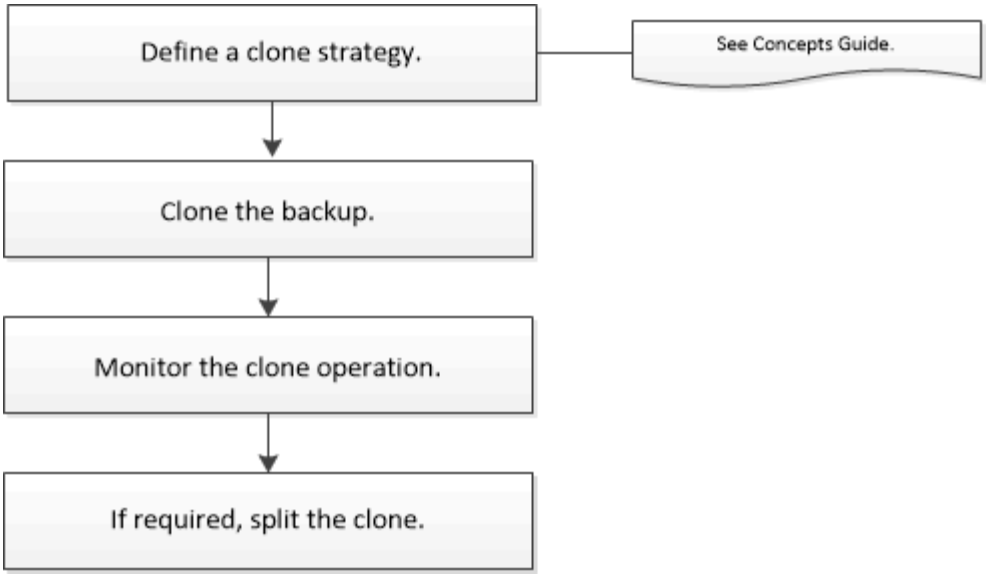
Klon-Workflow

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

Über diese Aufgabe

- Sie können auf dem PostgreSQL-Quellserver klonen.
- Sie können Ressourcen-Backups aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses
  - Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

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



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

Klonen eines PostgreSQL-Backups

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

Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Wenn Sie Befehle vor dem Klonen oder nach dem Klonen ausführen, sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host über folgende Pfade vorhanden sind:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config*

Wenn die Befehle in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Informationen zu den Vorgängen für FlexClone-Volume-Split finden Sie unter, "Teilten Sie ein FlexClone Volume vom übergeordneten Volume auf".
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

Schritte

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

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

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

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

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

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

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Zielport	Geben Sie den PostgreSQL-Zielport ein, der aus den vorhandenen Backups geklont werden soll.
NFS-Export-IP-Adresse	Geben Sie IP-Adressen oder Hostnamen ein, auf denen die geklonten Volumes exportiert werden. Dies gilt nur für Ressource mit NFS-Speichertyp.
Max. Kapazitäts-Pool Durchsatz (MiB/s)	Geben Sie den maximalen Durchsatz eines Kapazitäts-Pools ein. Dies gilt nur für ANF-Speicherressource.

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

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

   a. Geben Sie die Befehle für den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
      - Pre Clone, Befehl: Löschen Sie vorhandene Cluster mit demselben Namen
      - Post Clone-Befehl: Überprüfen Sie ein Cluster oder starten Sie ein Cluster.

b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

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

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Wählen Sie auf der 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.

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

PowerShell Commandlets

Schritte

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

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

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

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

```
 C:\PS> Get-SmBackup

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

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

   Dieses Beispiel zeigt, dass das zu klonende Backup über eine NFSExportIPs-Adresse 10.32.212.14 verfügt:

   Für PostgreSQL-Cluster:

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```

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

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

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

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

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

Überwachen von PostgreSQL-Klonvorgängen

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 hier , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet 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**.

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 den Vorgängen für FlexClone-Volume-Split finden Sie unter, "Teilten Sie ein FlexClone Volume vom übergeordneten Volume auf".
- 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"

Löschen oder teilen Sie PostgreSQL Cluster Clones nach dem Upgrade von SnapCenter

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

Über diese Aufgabe

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

Schritte

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht Kopien managen die Klone entweder auf den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
6. Wählen Sie die Klone aus, und klicken Sie dann auf , um Klone zu löschen, oder klicken Sie auf , um die Klone zu teilen.
7. Klicken Sie auf **OK**.