Schützen Sie benutzerdefinierte Anwendungen

SnapCenter Software 4.6

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-46/protect-scc/concept_snapcenter_custom_plug_ins_overview.html on September 29, 2025. Always check docs.netapp.com for the latest.

Inhalt

Schützen Sie benutzerdefinierte Anwendungen . . . 1
Benutzerdefinierte SnapCenter Plug-ins . . . 1
Überblick über benutzerdefinierte SnapCenter Plug-ins . . . 1
Welche Möglichkeiten bieten benutzerdefinierte SnapCenter Plug-ins und Storage Plug-ins . . . 1
Benutzerdefinierte SnapCenter Plug-ins-Funktionen . . . 2
Von benutzerdefinierten SnapCenter Plug-ins unterstützte Storage-Typen . . . 3
Minimale ONTAP-Berechtigungen, die für benutzerdefiniertes Plug-in erforderlich sind . . . 3
Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replizierung auf benutzerdefinierte Plug-ins vor . . . 7
Backup-Strategie definieren . . . 8
Backup-Strategie für benutzerdefinierte Plug-ins . . . 8
Arten von Wiederherstellungsstrategien werden für manuell hinzugefügte benutzerdefinierte Plug-in-Ressourcen unterstützt . . . 9
Entwickeln Sie ein Plug-in für Ihre Applikation . . . 10
Überblick . . . 10
PERL-basierte Entwicklung . . . 12
NATIVER Stil . . . 21
Java-Stil . . . 24
Benutzerdefiniertes Plug-in in SnapCenter . . . 32
Bereiten Sie die Installation von benutzerdefinierten SnapCenter-Plug-ins vor . . . 36
Installationsworkflow von benutzerdefinierten SnapCenter Plug-ins . . . 36
Voraussetzungen für das Hinzufügen von Hosts und die Installation benutzerdefinierter SnapCenter Plug-ins . . . 36
Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux . . . 37
Richten Sie Anmeldedaten für benutzerdefinierte SnapCenter-Plug-ins ein . . . 38
Konfigurieren Sie gMSA unter Windows Server 2012 oder höher . . . 41
Installieren Sie die benutzerdefinierten SnapCenter-Plug-ins . . . 42
Konfigurieren Sie das CA-Zertifikat . . . 49
Bereiten Sie sich auf die Datensicherung vor . . . 57
Voraussetzungen für die Verwendung der benutzerdefinierten SnapCenter-Plug-ins . . . 57
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz benutzerdefinierter Plug-in-Ressourcen verwendet werden . . . 58
Sichern Sie benutzerdefinierte Plug-in-Ressourcen . . . 59
Sichern Sie benutzerdefinierte Plug-in-Ressourcen . . . 59
Benutzerdefinierte SnapCenter Plug-ins mit Ressourcen ergänzen . . . 59
Erstellen von Richtlinien für benutzerdefinierte Plug-in-Ressourcen . . . 62
Erstellen von Ressourcengruppen und Anhängen von Richtlinien . . . 66
Sicherung individueller Plug-in-Ressourcen . . . 69
Sichern Sie Ressourcengruppen benutzerdefinierter Plug-in-Ressourcen . . . 72
Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets . . . 73
Sichern Sie Ressourcen mit PowerShell cmdlets . . . 74
Überwachen Sie benutzerdefinierte Backup-Vorgänge für Plug-in-Ressourcen . . . 76
Abbrechen der Backup-Vorgänge für benutzerdefinierte Plug-ins . . . 77

Sehen Sie sich auf der Seite Topologie benutzerdefinierte Backups und Klone zu den Plug-in-Ressourcen an . . . 78
Stellen Sie benutzerdefinierte Plug-in-Ressourcen wieder her . . . 79
Stellen Sie benutzerdefinierte Plug-in-Ressourcen wieder her . . . 79
Wiederherstellen eines Ressourcenbackups . . . 80
Überwachen Sie benutzerdefinierte Restore-Vorgänge für Plug-in-Ressourcen . . . 82
Klonen benutzerdefinierter Plug-in-Ressourcen-Backups . . . 83
Klonen benutzerdefinierter Plug-in-Ressourcen-Backups . . . 83
Klonen aus einem Backup . . . 84
Klonen von Backups mit PowerShell Cmdlets . . . 86
Überwachung benutzerdefinierter Plug-in-Klonvorgänge . . . 89

Schützen Sie benutzerdefinierte Anwendungen

Benutzerdefinierte SnapCenter Plug-ins

Überblick über benutzerdefinierte SnapCenter Plug-ins

Sie können benutzerdefinierte Plug-ins für Applikationen entwickeln, die Sie verwenden. Anschließend können Sie diese Applikationen mit SnapCenter sichern, wiederherstellen oder klonen. Wie andere SnapCenter Plug-ins fungieren auch Ihre individuellen Plug-ins als Host-seitige Komponenten der NetApp SnapCenter Software und ermöglichen so die applikationsorientierte Datensicherung und das Management von Ressourcen.

Sobald benutzerdefinierte Plug-ins installiert sind, können Sie SnapCenter mit NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Außerdem können Sie mithilfe der NetApp SnapVault Technologie eine Disk-to-Disk-Backup-Replizierung durchführen. Die benutzerdefinierten Plug-ins können sowohl in Windows- als auch in Linux-Umgebungen verwendet werden.

SnapCenterCLI unterstützt keine benutzerdefinierten Plug-ins-Befehle von SnapCenter.

NetApp stellt das Storage Plug-in zur Verfügung, um mithilfe des individuellen Plug-in Frameworks von SnapCenter Datensicherungsvorgänge des Daten-Volumes auf dem ONTAP Storage durchzuführen.

Sie können das benutzerdefinierte Plug-in und das Speicher-Plug-in über die Seite Host hinzufügen installieren.

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

NetApp bietet darüber hinaus MySQL, MAXDB, DB2, SYBASE, DPGLUE, Benutzerdefinierte MongoDB, ORASCPM und PostgreSQL Plug-ins. Diese Plug-ins können von heruntergeladen werden "NetApp Storage Automation Store".

Die SnapCenter Support-Richtlinie unterstützt das individuelle SnapCenter Plug-in Framework, die Core Engine und die zugehörigen APIs. Der Plug-in-Quellcode und die zugehörigen Skripte, die auf dem benutzerdefinierten Plug-in-Framework basieren, werden nicht unterstützt.

Sie können Ihre eigenen benutzerdefinierten Plug-ins erstellen, indem Sie auf verweisen "Entwickeln Sie ein Plug-in für Ihre Applikation".

Welche Möglichkeiten bieten benutzerdefinierte SnapCenter Plug-ins und Storage Plug-ins

Sie können die benutzerdefinierten SnapCenter Plug-ins für Datensicherungsvorgänge verwenden.

Benutzerdefiniertes Plug-in

- Fügen Sie Ressourcen wie Datenbanken, Instanzen, Dokumente oder Tabellen hinzu.
- Backups erstellen.
- Restore aus Backups:

- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

Storage-Plug-in

Sie können das Storage Plug-in für Datensicherungsvorgänge verwenden.

- Erstellen Sie Snapshot Kopien der Storage Volumes über ONTAP Cluster hinweg.
- Führen Sie Backups individueller Applikationen mithilfe des integrierten Pre- und Post-Scripting Frameworks durch

  Sie können ein Backup für das ONTAP Volume, die LUN oder einen qtree erstellen.

- Aktualisierung der auf dem primären Volume erstellten Snapshot Kopien auf einem sekundären ONTAP System unter Nutzung der vorhandenen Replizierungsbeziehung (SnapVault/SnapMirror/Unified Replication) mithilfe der SnapCenter Richtlinie

  Als primäres und sekundäres ONTAP werden ONTAP FAS, AFF, Select oder Cloud ONTAP bezeichnet.

- Stellen Sie komplette ONTAP Volumes, LUNs oder Dateien wieder her.

  Sie sollten den entsprechenden Dateipfad manuell angeben, da die Funktionen zum Durchsuchen oder zur Indizierung nicht im Produkt integriert sind.

  Die Wiederherstellung von qtree oder Verzeichnissen wird nicht unterstützt, aber Sie können nur den Qtree klonen und exportieren, wenn der Backup-Umfang auf Qtree-Ebene definiert ist.

Benutzerdefinierte SnapCenter Plug-ins-Funktionen

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Um mit benutzerdefinierten Plug-ins 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-, Recovery- und Klonvorgänge über alle Plug-ins hinweg, zentralisierte Berichterstellung, Dashboard-Ansichten auf einen Blick, rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Aufgaben über alle Plug-ins hinweg.

- **Automatisierte zentrale Verwaltung**

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

- **Unterbrechungsfreie NetApp Snapshot Kopie-Technologie**

  SnapCenter nutzt die NetApp Snapshot-Kopiertechnologie mit den benutzerdefinierten Plug-ins von

SnapCenter, um Ressourcen zu sichern. Snapshot Kopien belegen nur minimalen Speicherplatz.

Mithilfe der Funktion „Custom Plug-ins“ ergeben sich darüber hinaus folgende Vorteile:

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

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

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

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

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

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

- Funktion zum Erstellen von Snapshot Kopien mithilfe externer Befehle.
- Funktion zur Erstellung dateisystemkonsistenter Snapshot Kopien in Windows Umgebungen

Von benutzerdefinierten SnapCenter Plug-ins unterstützte Storage-Typen

SnapCenter unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf Virtual Machines. Sie müssen die Unterstützung Ihres Speichertyps überprüfen, bevor Sie benutzerdefinierte SnapCenter-Plug-ins installieren.

Maschine	Storage-Typ
Physische und NFS-direkte Mounts auf den VM Hosts (VMDKs und RDM LUNs werden nicht unterstützt.)	FC-verbundene LUNs
Physische und NFS-direkte Mounts auf den VM Hosts (VMDKs und RDM LUNs werden nicht unterstützt.)	ISCSI-verbundene LUNs
Physische und NFS-direkte Mounts auf den VM Hosts (VMDKs und RDM LUNs werden nicht unterstützt.)	Volumes mit NFS-Anbindung

Minimale ONTAP-Berechtigungen, die für benutzerdefiniertes Plug-in erforderlich sind

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

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
Event Generate-AutoSupport-log
Job-Verlauf wird angezeigt Job beenden
lun-Attribut anzeigen lun erstellen lun löschen lun-Geometrie lun Initiatorgruppe hinzufügen lun-Initiatorgruppe wird erstellt lun-Initiatorgruppe löschen lun igroup umbenennen lun-Initiatorgruppe wird angezeigt lun Mapping Add-Reporting-Nodes lun-Zuordnung erstellen lun-Zuordnung löschen lun Mapping remove-Reporting-Nodes lun-Zuordnung wird angezeigt lun ändern lun-Verschiebung in Volume lun ist offline lun ist online die lun-Größe wird geändert lun seriell lun anzeigen
Netzwerkschnittstelle

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
SnapMirror Richtlinie Add-Rule änderungsregel für snapmirror Remove-Rule für snapmirror-Richtlinie snapmirror-Richtlinie anzeigen snapmirror Wiederherstellung snapmirror zeigen snapmirror Vorgeschichte snapmirror Update snapmirror Update-ls-Set snapmirror Listenziele
Version

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
Erstellung von Volume-Klonen
Klon von Volume anzeigen
Split-Start des Volume-Klons
Split-Stopp für Volume-Klon
Volume erstellen
Volume destroy
Erstellen eines Volume-Dateiklonen
Show-Disk-Nutzung für Volume-Dateien
Volume ist offline
Das Volume ist online
Volume-Änderung
Erstellen von Volume-qtree
Volume qtree löschen
Änderung des Volume-qtree
Volume-qtree anzeigen
Volume-Einschränkung
Volumen anzeigen
Erstellen von Volume-Snapshots
Volume Snapshot löschen
Ändern des Volume-Snapshots
Umbenennung von Volume-Snapshots
Wiederherstellung von Volume Snapshots
Restore-Datei für Volume Snapshots
Volume-Snapshot werden angezeigt
Volume-Aufhängung nicht verfügbar

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
cifs von vserver
erstellung von cifs-Freigaben von vserver
cifs-Freigabe von vserver: Löschen
vserver cifs shadowcopy anzeigen
cifs-Freigabe von vserver wird angezeigt
vserver cifs zeigen
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-Verbindung wird angezeigt
vserver zeigen

Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
Netzwerkschnittstelle

Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replizierung auf benutzerdefinierte Plug-ins 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.

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

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

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

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

SnapCenter unterstützt keine **Sync_mirror** Replikation.

Backup-Strategie definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, stellen Sie sicher, dass Sie über die Backups verfügen, 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 Snapshot Kopien der Konsistenzgruppe vorhanden sein sollen, und entscheiden Sie sich für geeignete Optionen zum Löschen von Snapshot Kopien der Konsistenzgruppe.
5. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
6. Legen Sie die Aufbewahrungsdauer für die Snapshot Kopien 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.

Backup-Strategie für benutzerdefinierte Plug-ins

Backup-Pläne für benutzerdefinierte Plug-in-Ressourcen

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Je öfter Sie Ihre Ressourcen sichern, desto weniger Archivprotokolle, die SnapCenter für die Wiederherstellung verwenden muss, was zu schnelleren Restore-Vorgängen führen kann.

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).

Im Rahmen des SLA wird das erwartete Service-Level definiert und es werden zahlreiche Service-bezogene Probleme behandelt, darunter Verfügbarkeit und Performance des Service. 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 und RPO tragen zur Datensicherungsstrategie bei.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Frequenz (wie oft Backups durchgeführt werden sollen), auch als Zeitplantyp für einige Plug-ins bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren. Über die SnapCenter-Benutzeroberfläche können Sie auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressource oder Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird Sie können in der SnapCenter-Benutzeroberfläche auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** klicken, das entsprechende Plug-in auswählen und auf **Ansicht** > **Ressourcengruppe** klicken.

Anzahl der 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).

Die Anzahl der ausgewählten Backup-Jobs hängt in der Regel von der Anzahl der Volumes ab, von denen Sie Ihre Ressourcen platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Ressourcen auf einem Volume und einer großen Ressource auf einem anderen Volume platziert haben, können Sie für die kleinen Ressourcen einen Backup-Job und für die große Ressource einen Backup-Job erstellen.

Arten von Wiederherstellungsstrategien werden für manuell hinzugefügte benutzerdefinierte Plug-in-Ressourcen unterstützt

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte benutzerdefinierte Plug-in-Ressourcen.

Sie können keine manuell hinzugefügten benutzerdefinierten Plug-in-Ressourcen wiederherstellen.

Komplette Ressourcenwiederherstellung

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

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

Wiederherstellung auf Dateiebene

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

Entwickeln Sie ein Plug-in für Ihre Applikation

Überblick

Der SnapCenter Server ermöglicht die Implementierung und das Management von Applikationen als Plug-ins für SnapCenter. Die Applikationen Ihrer Wahl können zur Datensicherung und zu Managementfunktionen in den SnapCenter Server integriert werden.

Mit SnapCenter können Sie benutzerdefinierte Plug-ins mit unterschiedlichen Programmiersprachen entwickeln. Sie können ein benutzerdefiniertes Plug-in über Perl, Java, BATCH oder andere Skriptsprachen entwickeln.

Um benutzerdefinierte Plug-ins in SnapCenter zu verwenden, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen Sie ein Plug-in für Ihre Anwendung mithilfe der Anweisungen in diesem Handbuch
- Erstellen Sie eine Beschreibungsdatei
- Exportieren Sie das benutzerdefinierte Plug-in, um es auf dem SnapCenter-Host zu installieren
- Laden Sie die Plug-in-ZIP-Datei auf den SnapCenter-Server hoch

Allgemeine Plug-in-Bearbeitung bei allen API-Aufrufen

Verwenden Sie für jeden API-Aufruf die folgenden Informationen:

- Plug-in-Parameter
- Exit-Codes
- Fehlermeldungen protokollieren
- Datenkonsistenz

Verwenden Sie Plug-in-Parameter

Bei jedem API-Aufruf wird eine Reihe von Parametern an das Plug-in übergeben. In der folgenden Tabelle sind die spezifischen Informationen für die Parameter aufgeführt.

Parameter	Zweck
AKTION	Legt den Workflow-Namen fest. Entdecken Sie zum Beispiel, sichern, fileOrVolRestore oder cloneVolAndRun
RESSOURCEN	Listet Ressourcen auf, die geschützt werden sollen. Eine Ressource wird durch UID und Typ identifiziert. Die Liste wird dem Plug-in im folgenden Format angezeigt: „<UID>,<TYPE>;<UID>,<TYPE>“. Beispiel: „Instance1,instance;Instance2\\DB1,Database“
APP_NAME	Bestimmt, welches Plug-in verwendet wird. Zum Beispiel DB2, MYSQL. SnapCenter Server bietet integrierte Unterstützung für die aufgeführten Applikationen. Bei diesem Parameter wird die Groß-/Kleinschreibung beachtet.
APP_IGNORE_ERROR	(J oder N) Dies führt dazu, dass SnapCenter beendet wird oder nicht beendet wird, wenn ein Anwendungsfehler auftritt. Dies ist nützlich, wenn Sie Backups mehrerer Datenbanken durchführen und nicht möchten, dass der Backup-Vorgang durch einen einzelnen Fehler unterbrochen wird.
<RESOURCE_NAME>__APP_INSTANCE_USERNAME	SnapCenter-Anmeldeinformationen für die Ressource festgelegt.
<RESOURCE_NAME>_APP_INSTANCE_PASSWORD	SnapCenter-Anmeldeinformationen für die Ressource festgelegt.
<RESOURCE_NAME>_<CUSTOM_PARAM>	Jeder benutzerdefinierte Schlüsselwert auf Ressourcenebene steht für Plug-ins zur Verfügung, die mit „<RESOURCE_NAME>_“ vordefiniert sind. Wenn ein benutzerdefinierter Schlüssel beispielsweise „MASTER_SLAVE“ für eine Ressource namens „MySQLDB“ ist, wird er als MySQLDB_MASTER_SLAVE verfügbar sein

Exit-Codes verwenden

Das Plug-in gibt den Status des Vorgangs über Exit-Codes zurück an den Host. Jeder Code hat eine bestimmte Bedeutung, und das Plug-in verwendet den richtigen Exit-Code, um die gleiche anzuzeigen.

Die folgende Tabelle zeigt Fehlercodes und deren Bedeutung.

Beenden Sie den Code	Zweck
0	Erfolgreicher Betrieb.
99	Der angeforderte Vorgang wird nicht unterstützt oder implementiert.
100	Fehlgeschlagener Vorgang, unquiesce überspringen und beenden. Deaktivieren ist standardmäßig.
101	Fehlgeschlagener Vorgang; fahren Sie mit dem Backup-Vorgang fort.
Andere	Vorgang fehlgeschlagen, Ausführung unquiesce und Beenden.

Fehlermeldungen protokollieren

Die Fehlermeldungen werden vom Plug-in an den SnapCenter-Server übergeben. Die Meldung enthält die Meldung, die Protokollebene und den Zeitstempel.

In der folgenden Tabelle sind die Ebenen und ihre Zwecke aufgeführt.

Parameter	Zweck
INFO	Informationsmeldung
WARNEN	Warnmeldung
FEHLER	Fehlermeldung
DEBUGGEN	Debug-Nachricht
VERFOLGEN	Trace-Nachricht

Wahrung der Datenkonsistenz

Benutzerdefinierte Plug-ins bewahren Daten zwischen Operationen derselben Workflow-Ausführung auf. Ein Plug-in kann zum Beispiel Daten am Ende der Stilllegung speichern, die auch während des Betriebs ausgeführt werden können.

Die zu haltenden Daten werden als Teil des Ergebnisobjekts durch Plug-in festgelegt. Es folgt einem bestimmten Format und wird im Detail unter jedem Stil der Plug-in-Entwicklung beschrieben.

PERL-basierte Entwicklung

Bei der Entwicklung des Plug-ins mittels PERL müssen Sie bestimmte Konventionen beachten.

- Inhalte müssen lesbar sein
- Obligatorische Operationen setenv, quiesce und unquiesce implementieren müssen
- Sie müssen eine bestimmte Syntax verwenden, um die Ergebnisse an den Agenten weiterzuleiten
- Der Inhalt sollte als <PLUGIN_NAME>.pm Datei gespeichert werden

Verfügbare Operationen sind

- Setenv
- Version
- Stilllegen
- Unquiesce
- Clone_Pre, Clone_Post
- Restore_Pre, Restore
- Bereinigung

Allgemeine Plug-in-Handhabung

Verwenden des Ergebnisobjekts

Jeder benutzerdefinierte Plug-in-Vorgang muss das Ergebnisobjekt definieren. Dieses Objekt sendet Nachrichten, Exit Code, stdout und stderr zurück an den Host-Agent.

Ergebnisobjekt:

```
my $result = {
```

```
      exit_code => 0,
      stdout => "",
      stderr => "",
};
```

Ergebnisobjekt wird zurückgegeben:

```
return $result;
```

Wahrung der Datenkonsistenz

Es ist möglich, Daten zwischen den Operationen (außer Bereinigung) als Teil der gleichen Workflow-Ausführung zu erhalten. Dies erfolgt mit Schlüsselwert-Paaren. Die Daten werden als Teil des Ergebnisobjekts festgelegt und sind in den nachfolgenden Operationen desselben Workflows erhalten und verfügbar.

Im folgenden Codebeispiel werden die zu haltenden Daten festgelegt:

```
my $result = {
  exit_code => 0,
  stdout => "",
  stderr => "",
};
  $result->{env}->{'key1'} = 'value1';
  $result->{env}->{'key2'} = 'value2';
  ….
  return $result
```

Der obige Code setzt zwei Schlüssel-Wert-Paare, die als Eingabe in der nachfolgenden Operation zur Verfügung stehen. Auf die beiden Schlüsselwertware kann über folgenden Code zugegriffen werden:

```
sub setENV {
    my ($self, $config) = @_;
    my $first_value = $config->{'key1'};
    my $second_value = $config->{'key2'};
    …
}
```

```
 === Logging error messages
Jeder Vorgang kann Nachrichten an den Host-Agent senden, der den Inhalt
anzeigt und speichert. Eine Nachricht enthält die Nachrichtenebene, einen
Zeitstempel und einen Nachrichtentext. Mehrzeilare Nachrichten werden
unterstützt.
```

```
Load the SnapCreator::Event Class:
my $msgObj = new SnapCreator::Event();
my @message_a = ();
```

Verwenden Sie msgObj, um eine Nachricht mithilfe der Erfassungsmethode zu erfassen.

```
$msgObj->collect(\@message_a, INFO, "My INFO Message");
$msgObj->collect(\@message_a, WARN, "My WARN Message");
$msgObj->collect(\@message_a, ERROR, "My ERROR Message");
$msgObj->collect(\@message_a, DEBUG, "My DEBUG Message");
$msgObj->collect(\@message_a, TRACE, "My TRACE Message");
```

Meldungen auf das Ergebnisobjekt anwenden:

```
$result->{message} = \@message_a;
```

Verwendung von Plug-in-Stiften

Benutzerdefinierte Plug-ins müssen Plug-in-Stiche enthalten. Dies sind Methoden, die der SnapCenter-Server auf Grundlage eines Workflows aufruft.

Steckschraube	Optional/Erforderlich	Zweck
Setenv	Erforderlich	Dieser Stub legt die Umgebung und das Konfigurationsobjekt fest. Hier sollte eine Analyse oder Handhabung der Umgebung durchgeführt werden. Jedes Mal, wenn ein Stub genannt wird, wird die setenv stub kurz zuvor aufgerufen. Es ist nur für PERL-Plug-ins erforderlich.
Version	Optional	Diese Stub wird verwendet, um die Anwendungsversion zu erhalten.
Ermitteln	Optional	Mit diesem Stub werden Anwendungsobjekte wie beispielsweise die auf dem Agenten oder Host gehostete Instanz oder Datenbank ermittelt. Das Plug-in wird voraussichtlich im Rahmen der Antwort erkannte Applikationsobjekte in einem bestimmten Format zurückgeben. Dieser Stub wird nur verwendet, wenn die Anwendung in SnapDrive für Unix integriert ist. Linux-Dateisystem (Linux-Varianten) wird unterstützt. AIX/Solaris (Unix-Varianten) werden nicht unterstützt.

Steckschraube	Optional/Erforderlich	Zweck
Discovery_complete	Optional	Mit diesem Stub werden Anwendungsobjekte wie beispielsweise die auf dem Agenten oder Host gehostete Instanz oder Datenbank ermittelt. Das Plug-in wird voraussichtlich im Rahmen der Antwort erkannte Applikationsobjekte in einem bestimmten Format zurückgeben. Dieser Stub wird nur verwendet, wenn die Anwendung in SnapDrive für Unix integriert ist. Linux-Dateisystem (Linux-Varianten) wird unterstützt. AIX und Solaris (Unix-Varianten) werden nicht unterstützt.
Stilllegen	Erforderlich	Diese Stub ist für das Ausführen eines Quiesce zuständig, das bedeutet, die Applikation in einen Zustand zu legen, in dem Sie eine Snapshot Kopie erstellen können. Dies wird vor dem Vorgang der Snapshot Kopie aufgerufen. Die zu behaltenden Metadaten der Applikation sollten im Rahmen der Antwort festgelegt werden, die bei einem nachfolgenden Klon oder bei Wiederherstellungen auf der entsprechenden Storage Snapshot Kopie in Form von Konfigurationsparametern zurückgegeben werden müssen.
Nicht Stilllegen	Erforderlich	Diese Stub ist verantwortlich für die Durchführung eines Unquiesce, das bedeutet, Anwendung in einen normalen Zustand. Dies wird aufgerufen, nachdem Sie eine Snapshot Kopie erstellt haben.

Steckschraube	Optional/Erforderlich	Zweck
Clone_Pre	Optional	Diese Stub ist für das Durchführen von Preclone-Aufgaben zuständig. Voraussetzung dafür ist, dass Sie die integrierte SnapCenter Server Klonschnittstelle verwenden und beim Ausführen eines Klonvorgangs ausgelöst wird.
Clone_Post	Optional	Diese Stub ist für das Durchführen von Aufgaben nach dem Klonen verantwortlich. Hierbei wird vorausgesetzt, dass Sie die integrierte SnapCenter Server Klonschnittstelle verwenden und nur beim Ausführen eines Klonvorgangs ausgelöst wird.
Wiederherstellen_Pre	Optional	Diese Stub ist für die Durchführung von Vorratstore-Aufgaben zuständig. Hierbei wird vorausgesetzt, dass Sie die integrierte SnapCenter Server Restore-Schnittstelle verwenden und während der Wiederherstellung ausgelöst werden.
Wiederherstellen	Optional	Diese Stub ist für die Durchführung von Aufgaben zur Wiederherstellung von Anwendungen verantwortlich. Hierbei wird vorausgesetzt, dass Sie die integrierte SnapCenter Server-Wiederherstellungsschnittstelle verwenden und nur bei der Durchführung einer Wiederherstellung ausgelöst wird.

Steckschraube	Optional/Erforderlich	Zweck
Bereinigung	Optional	Diese Stub ist für die Durchführung der Bereinigung nach Backup-, Wiederherstellungs- oder Klonvorgängen verantwortlich. Die Bereinigung kann während der normalen Workflow-Ausführung oder bei einem Workflow-Ausfall erfolgen. Sie können den Workflow-Namen infilern, unter dem die Bereinigung aufgerufen wird, indem Sie auf die Konfiguration Parameter AKTION, die Backup, KlonVolAndLun oder fileOrVolRestore sein kann. Der Konfigurationsparameter ERROR_MESSAGE gibt an, ob beim Ausführen des Workflows Fehler aufgetreten sind. Wenn ERROR_MESSAGE definiert ist und NICHT Null, wird die Bereinigung während der Ausführung des Workflow-Fehlers aufgerufen.
App_Version	Optional	Diese Stub wird von SnapCenter verwendet, um Anwendungsversionsdetails zu erhalten, die vom Plug-in verwaltet werden.

Informationen zum Plug-in-Paket

Jedes Plug-in muss folgende Informationen haben:

```
package MOCK;
our @ISA = qw(SnapCreator::Mod);
=head1 NAME
MOCK - class which represents a MOCK module.
=cut
=head1 DESCRIPTION
MOCK implements methods which only log requests.
=cut
use strict;
use warnings;
use diagnostics;
use SnapCreator::Util::Generic qw ( trim isEmpty );
use SnapCreator::Util::OS qw ( isWindows isUnix getUid
createTmpFile );
use SnapCreator::Event qw ( INFO ERROR WARN DEBUG COMMENT ASUP
CMD DUMP );
my $msgObj = new SnapCreator::Event();
my %config_h = ();
```

Betrieb

Sie können verschiedene Vorgänge wie Setenv, Version, Quiesce und Unquiesce codieren, die von den benutzerdefinierten Plug-ins unterstützt werden.

Vorgang setenv

Für Plug-ins, die mit PERL erstellt wurden, ist die setenv-Operation erforderlich. Sie können die ENV einstellen und problemlos auf Plug-in-Parameter zugreifen.

```
sub setENV {
    my ($self, $obj) = @_;
    %config_h = %{$obj};
    my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
    };
    return $result;
}
```

Versionsbetrieb

Der Versionsvorgang gibt die Versionsinformationen der Anwendung zurück.

```
sub version {
  my $version_result = {
    major => 1,
    minor => 2,
    patch => 1,
    build => 0
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $version_result->{message} = \@message_a;
  return $version_result;
}
```

Betrieb stilllegen

Der Quiesce-Vorgang führt einen Quiesce-Vorgang der Anwendung für Ressourcen durch, die im PARAMETER RESSOURCEN aufgeführt sind.

```
sub quiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

Vorgang nicht stilllegen

Um die Anwendung stillzulegen, muss der Vorgang nicht stillgelegt werden. Die Liste der Ressourcen ist im PARAMETER RESSOURCEN verfügbar.

```
sub unquiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::unquiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

NATIVER Stil

SnapCenter unterstützt zur Erstellung von Plug-ins nicht-PERL-Programmierung oder Skriptsprachen. Dies wird als NATIVE Stil-Programmierung bekannt, die Skript- oder BATCH-Datei sein kann.

Die Plug-ins IM NATIVEN Stil müssen den folgenden Konventionen entsprechen:

Das Plug-in muss ausführbar sein

- Bei Unix-Systemen muss der Benutzer, der den Agenten ausführt, über Ausführungsberechtigungen auf dem Plug-in verfügen
- Bei Windows-Systemen müssen PowerShell-Plug-ins das Suffix .ps1 aufweisen, andere Windows-Skripte müssen entweder über ein Suffix .cmd oder .bat verfügen und müssen vom Benutzer ausführbar sein
- Die Plug-ins müssen auf Befehlszeilenargumente wie „-quiesce“, „-unquiesce“ reagieren
- Die Plug-ins müssen Exit Code 99 zurückgeben, falls keine Operation oder Funktion implementiert ist
- Die Plug-ins müssen eine bestimmte Syntax verwenden, um Ergebnisse an den Server weiterzuleiten

Allgemeine Plug-in-Handhabung

Protokollieren von Fehlermeldungen

Jeder Vorgang kann Nachrichten an den Server senden, der den Inhalt anzeigt und speichert. Eine Nachricht enthält die Nachrichtenebene, einen Zeitstempel und einen Nachrichtentext. Mehrzeilare Nachrichten werden unterstützt.

Format:

```
SC_MSG#<level>#<timestamp>#<message>
SC_MESSAGE#<level>#<timestamp>#<message>
```

Verwendung von Plug-in-Stiften

SnapCenter-Plug-ins müssen Plug-in-Stiche implementieren. Hierbei handelt es sich um Methoden, die der SnapCenter-Server basierend auf einem bestimmten Workflow aufruft.

Steckschraube	Optional/Erforderlich	Zweck
Stilllegen	Erforderlich	Diese Stub ist für die Durchführung eines Stilllegeses verantwortlich. Dadurch wird die Applikation in einen Zustand versetzt, in dem wir eine Snapshot Kopie erstellen können. Dies wird vor dem Vorgang der Snapshot-Kopie des Storage aufgerufen.
Unquiesce	Erforderlich	Diese Stub ist für die Durchführung eines Unstillzulegen verantwortlich. Die Anwendung wird in den normalen Zustand versetzt. Dies wird nach dem Vorgang der Snapshot Kopie des Storage aufgerufen.
Clone_Pre	Optional	Diese Stub ist für die Durchführung von Aufgaben vor dem Klonen verantwortlich. Angenommen, Sie verwenden die integrierte SnapCenter Klonschnittstelle und wird auch nur ausgelöst, wenn Sie die Aktion „Clone_vol oder Clone_lun“ ausführen.
Clone_Post	Optional	Diese Stub ist für das Durchführen von Aufgaben nach dem Klonen verantwortlich. Angenommen, Sie verwenden die integrierte SnapCenter Klonschnittstelle und wird auch nur ausgelöst, wenn Sie „Clone_vol oder Clone_lun“ Vorgänge ausführen.
Wiederherstellen_Pre	Optional	Diese Stub ist für die Durchführung von Aufgaben vor der Wiederherstellung verantwortlich. Angenommen, Sie verwenden die integrierte SnapCenter Restore-Schnittstelle und wird nur während des Restore-Vorgangs ausgelöst.

Steckschraube	Optional/Erforderlich	Zweck
Wiederherstellen	Optional	Diese Stub ist für alle Wiederherstellungsmaßnahmen verantwortlich. Dies setzt voraus, dass Sie keine integrierte Wiederherstellungsschnittstelle verwenden. Sie wird während des Wiederherstellungsvorgangs ausgelöst.

Beispiele

Windows PowerShell

Überprüfen Sie, ob das Skript auf Ihrem System ausgeführt werden kann. Wenn Sie das Skript nicht ausführen können, setzen Sie Set-ExecutionPolicy Bypass für das Skript ein, und wiederholen Sie den Vorgang.

```
if ($args.length -ne 1) {
  write-warning "You must specify a method";
  break;
}
function log ($level, $message) {
  $d = get-date
  echo "SC_MSG#$level#$d#$message"
}
function quiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Quiescing application using script $app_name";
  log "INFO" "Quiescing application finished successfully"
}
function unquiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Unquiescing application using script $app_name";
  log "INFO" "Unquiescing application finished successfully"
}
  switch ($args[0]) {
    "-quiesce" {
    quiesce;
}
"-unquiesce" {
    unquiesce;
}
default {
    write-error "Function $args[0] is not implemented";
    exit 99;
  }
}
exit 0;
```

Java-Stil

Ein benutzerdefiniertes Java Plug-in interagiert direkt mit einer Applikation wie Datenbank, Instanz usw.

Einschränkungen

Es gibt bestimmte Einschränkungen, die Sie beim entwickeln eines Plug-ins mit Java-Programmiersprache beachten sollten.

Steckkennlinie	Java Plug-in
Komplexität	Niedrig bis mittel

Steckkennlinie	Java Plug-in
Platzbedarf für Arbeitsspeicher	Bis zu 10-20 MB
Abhängigkeiten von anderen Bibliotheken	Bibliotheken für die Anwendungskommunikation
Anzahl der Threads	1
Thread-Laufzeit	Weniger als eine Stunde

Grund für Java-Einschränkungen

Ziel des SnapCenter-Agenten ist es, eine kontinuierliche, sichere und robuste Anwendungsintegration zu gewährleisten. Durch die Unterstützung von Java-Plug-ins ist es möglich, dass Plug-ins Speicherlecks und andere unerwünschte Probleme einführen. Diese Probleme sind schwer zu bewältigen, vor allem, wenn das Ziel ist, die Dinge einfach zu bedienen. Wenn die Komplexität eines Plug-ins nicht zu komplex ist, ist es viel seltener wahrscheinlich, dass die Entwickler die Fehler verursacht hätten. Die Gefahr eines Java-Plug-ins besteht darin, dass sie in derselben JVM laufen wie der SnapCenter-Agent selbst. Wenn das Plug-in abstürzt oder Speicher leckt, kann es auch negative Auswirkungen auf den Agent haben.

Unterstützte Methoden

Methode	Erforderlich	Beschreibung	Wann und von wem gerufen?
Version	Ja.	Muss die Version des Plug-ins zurückgeben.	Vom SnapCenter-Server oder -Agent, um die Version des Plug-ins anzufordern.
Stilllegen	Ja.	Muss die Applikation stilllegen. In den meisten Fällen bedeutet dies, die Applikation in einen Zustand zu versetzen, in dem der SnapCenter Server ein Backup erstellen kann (z. B. eine Snapshot Kopie).	Bevor der SnapCenter-Server eine Snapshot(s)-Kopie erstellt oder ein Backup im Allgemeinen durchführt.
Nicht Stilllegen	Ja.	Muss die Applikation stilllegen. In den meisten Fällen bedeutet dies, dass die Applikation wieder in einen normalen Betriebszustand zurückversetzt wird.	Nachdem der SnapCenter Server eine Snapshot Kopie erstellt hat oder ein Backup im Allgemeinen ausgeführt hat.

Methode	Erforderlich	Beschreibung	Wann und von wem gerufen?
Bereinigung	Nein	Verantwortlich für die Reinigung von allen, die das Plug-in braucht, um zu reinigen.	Wenn ein Workflow auf dem SnapCenter-Server beendet ist (erfolgreich oder mit einem Fehler).
KlonVorr	Nein	Sollte Aktionen durchführen, die vor der Durchführung eines Klonvorgangs ausgeführt werden müssen.	Wenn ein Benutzer eine Aktion „KlonVol“ oder „cloneRun“ auslöst und den integrierten Klon-Assistenten (GUI/CLI) verwendet.
KlonPost	Nein	Sollte Aktionen durchführen, die nach der Durchführung eines Klonvorgangs ausgeführt werden müssen.	Wenn ein Benutzer eine Aktion „KlonVol“ oder „cloneRun“ auslöst und den integrierten Klon-Assistenten (GUI/CLI) verwendet.
WiederherstellungPre	Nein	Sollte Aktionen durchführen, die vor dem Wiederherstellungsvorgang ausgeführt werden müssen.	Wenn ein Benutzer einen Wiederherstellungsvorgang auslöst.
Wiederherstellen	Nein	Verantwortlich für die Durchführung einer Wiederherstellung/Wiederherstellung der Anwendung.	Wenn ein Benutzer einen Wiederherstellungsvorgang auslöst.
AppVersion	Nein	Zum Abrufen der vom Plug-in verwalteten Anwendungsversion.	Im Rahmen von ASUP Datenerfassung in jedem Workflow, wie beispielsweise Backup/Restore/Klonen,

Lernprogramm

In diesem Abschnitt wird beschrieben, wie Sie ein benutzerdefiniertes Plug-in mithilfe der Java-Programmiersprache erstellen.

Sonnenfinsternis einrichten

1. Erstellen Sie ein neues Java-Projekt "TutorialPlugin" in Eclipse
2. Klicken Sie Auf **Fertig Stellen**
3. Klicken Sie mit der rechten Maustaste auf das **neue Projekt → Eigenschaften → Java Build Path → Bibliotheken → Externe Jars hinzufügen**

4. Navigieren Sie zum Ordner ../lib/ des Host Agent, und wählen Sie Jars scAgent-5.0-core.jar und common-5.0.jar aus
5. Wählen Sie das Projekt aus und klicken Sie mit der rechten Maustaste auf den Ordner **src** → **Neu** → **Paket** und erstellen Sie ein neues Paket mit dem Namen com.netapp.snapcreator.agent.plugin.TutorialPlugin
6. Klicken Sie mit der rechten Maustaste auf das neue Paket, und wählen Sie Neu → Java-Klasse.
   a. Geben Sie den Namen als TutorialPlugin ein.
   b. Klicken Sie auf die Schaltfläche zum Durchsuchen von Superclass und suchen Sie nach "*AbstractPlugin". Es sollte nur ein Ergebnis angezeigt werden:

```
 "AbstractPlugin - com.netapp.snapcreator.agent.nextgen.plugin".
.. Klicken Sie Auf *Fertig Stellen*.
.. Java-Klasse:
```

```
package com.netapp.snapcreator.agent.plugin.TutorialPlugin;
import
com.netapp.snapcreator.agent.nextgen.common.result.Describe
Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.VersionR
esult;
import
com.netapp.snapcreator.agent.nextgen.context.Context;
import
com.netapp.snapcreator.agent.nextgen.plugin.AbstractPlugin;
public class TutorialPlugin extends AbstractPlugin {
  @Override
  public DescribeResult describe(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result quiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result unquiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public VersionResult version() {
    // TODO Auto-generated method stub
    return null;
  }
}
```

Umsetzung der erforderlichen Methoden

Quiesce, unquiesce und Version sind obligatorische Methoden, die jedes benutzerdefinierte Java Plug-in implementieren muss.

Die folgende Versionsmethode gibt die Version des Plug-ins zurück.

```
@Override
public VersionResult version() {
    VersionResult versionResult = VersionResult.builder()
                                                .withMajor(1)
                                                .withMinor(0)
                                                .withPatch(0)
                                                .withBuild(0)
                                                .build();
    return versionResult;
}
```

```
Below is the implementation of quiesce and unquiesce method. These will be
interacting with   the application, which is being protected by SnapCenter
Server. As this is just a tutorial, the
application part is not explained, and the focus is more on the
functionality that SnapCenter   Agent provides the following to the plug-
in developers:
```

```
@Override
  public Result quiesce(Context context) {
    final Logger logger = context.getLogger();
    /*
      * TODO: Add application interaction here
    */
```

```
logger.error("Something bad happened.");
logger.info("Successfully handled application");
```

```
    Result result = Result.builder()
                    .withExitCode(0)
                    .withMessages(logger.getMessages())
                    .build();
    return result;
}
```

Die Methode wird in einem Kontextobjekt übergeben. Dazu gehören mehrere Helfer, zum Beispiel ein Logger und ein Context Store, sowie die Informationen über den aktuellen Vorgang (Workflow-ID, Job-ID). Wir können den Logger erhalten, indem wir den endgültigen Logger Logger = context.getLogger(); anrufen. Das Logger-Objekt bietet ähnliche Methoden, die von anderen Protokollierungs-Frameworks bekannt sind, z. B. Logback. Im Ergebnisobjekt können Sie auch den Exit-Code angeben. In diesem Beispiel wird Null zurückgegeben, da kein Problem aufgetreten ist. Andere Exit-Codes können verschiedenen Fehlerszenarien zugeordnet werden.

Ergebnisobjekt wird verwendet

Das Ergebnisobjekt enthält die folgenden Parameter:

Parameter	Standard	Beschreibung
Konfigurations	Leere Konfiguration	Mit diesem Parameter können Konfigurationsparameter zurück an den Server gesendet werden. Es kann Parameter sein, die das Plug-in aktualisieren möchte. Ob diese Änderung sich tatsächlich in der Konfiguration auf dem SnapCenter-Server wiederfindet, hängt vom PARAMETER APP_CONF_PERSISTENZ=Y oder N in der Konfiguration ab.
Code-Code	0	Zeigt den Status des Vorgangs an. Ein „0“ bedeutet, dass der Vorgang erfolgreich ausgeführt wurde. Andere Werte weisen auf Fehler oder Warnungen hin.
Stdout	Leere Liste	Damit können stdout-Nachrichten an den SnapCenter-Server zurückgesendet werden.
Stderr	Leere Liste	Damit können stderr-Nachrichten an den SnapCenter-Server zurückgesendet werden.
Nachrichten	Leere Liste	Diese Liste enthält alle Meldungen, die ein Plug-in zum Server zurückkehren möchte. Der SnapCenter-Server zeigt diese Meldungen in der CLI oder GUI an.

Der SnapCenter Agent stellt Builders zur Verfügung ("Baumuster") Für alle seine Ergebnistypen. Daher ist es sehr einfach, sie zu verwenden:

```
Result result = Result.builder()
                    .withExitCode(0)
                    .withStdout(stdout)
                    .withStderr(stderr)
                    .withConfig(config)
                    .withMessages(logger.getMessages())
                    .build()
```

Setzen Sie beispielsweise den Exit-Code auf 0, legen Sie Listen für stdout und stderr fest, legen Sie die

Konfigurationsparameter fest und fügen Sie die Protokollmeldungen an, die an den Server zurückgesendet werden. Wenn Sie nicht alle Parameter benötigen, senden Sie nur die erforderlichen Parameter. Da jeder Parameter einen Standardwert hat, ist das Ergebnis unberührt, wenn Sie .withExitCode(0) aus dem unten stehenden Code entfernen:

```
Result result = Result.builder()
                      .withExitCode(0)
                      .withMessages(logger.getMessages())
                      .build();
```

VersionResult

Der VersionResult informiert den SnapCenter-Server über die Plug-in-Version. Da es auch vom Ergebnis erbt, enthält es die Parameter config, exitCode, stdout, stderr und Nachrichten.

Parameter	Standard	Beschreibung
Major	0	Hauptversionsfeld des Plug-ins.
Gering	0	Kleines Versionsfeld des Plug-ins.
Patch	0	Feld für die Patch-Version des Plug-ins.
Entwickeln	0	Build-Versionsfeld des Plug-ins.

Beispiel:

```
VersionResult result = VersionResult.builder()
                                    .withMajor(1)
                                    .withMinor(0)
                                    .withPatch(0)
                                    .withBuild(0)
                                    .build();
```

Verwenden des Kontextobjekts

Das Kontextobjekt bietet folgende Methoden:

Kontextsethode	Zweck
String getWorkflowId();	Gibt die Workflow-id zurück, die vom SnapCenter-Server für den aktuellen Workflow verwendet wird.
Config getconfig();	Gibt die Konfiguration zurück, die vom SnapCenter-Server an den Agenten gesendet wird.

Workflow-ID

Die Workflow-ID ist die id, die der SnapCenter-Server verwendet, um auf einen bestimmten laufenden Workflow zu verweisen.

Konfigurations

Dieses Objekt enthält (die meisten) Parameter, die ein Benutzer in der Konfiguration auf dem SnapCenter-Server festlegen kann. Aus Sicherheitsgründen können jedoch einige dieser Parameter auf Server-Seite gefiltert werden. Nachfolgend ein Beispiel für den Zugriff auf die Konfiguration und den Abruf eines Parameters:

```
final Config config = context.getConfig();
String myParameter =
config.getParameter("PLUGIN_MANDATORY_PARAMETER");
```

""// myParameter" enthält jetzt den Parameter, der aus der Konfiguration auf dem SnapCenter-Server gelesen wird Wenn ein Parameterkschlüssel nicht vorhanden ist, wird ein leerer String (") zurückgegeben.

Das Plug-in wird exportiert

Sie müssen das Plug-in exportieren, um es auf dem SnapCenter-Host zu installieren.

Führen Sie in Eclipse die folgenden Aufgaben aus:

1. Klicken Sie mit der rechten Maustaste auf das Basispaket des Plug-ins (in unserem Beispiel com.netapp.snapcreator.agent.plugin.TutorialPlugin).
2. Wählen Sie **Export → Java → Jar-Datei**
3. Klicken Sie Auf **Weiter**.
4. Geben Sie im folgenden Fenster den Ziel-JAR-Dateipfad an: tutorial_plugin.jar die Basisklasse des Plug-ins heißt TutorialPlugin.class, das Plug-in muss einem Ordner mit dem gleichen Namen hinzugefügt werden.

Wenn Ihr Plug-in von zusätzlichen Bibliotheken abhängt, können Sie den folgenden Ordner erstellen: Lib/

Sie können JAR-Dateien hinzufügen, von denen das Plug-in abhängig ist (z. B. ein Datenbanktreiber). Wenn SnapCenter das Plug-in lädt, ordnet es automatisch alle JAR-Dateien in diesem Ordner zu und fügt sie dem Klassenpfad hinzu.

Benutzerdefiniertes Plug-in in SnapCenter

Benutzerdefiniertes Plug-in in SnapCenter

Das benutzerdefinierte Plug-in, das mit Java, PERL oder NATIVEM Stil erstellt wurde, kann über SnapCenter Server auf dem Host installiert werden, um die Datensicherung Ihrer Anwendung zu ermöglichen. Sie müssen das Plug-in exportiert haben, um es auf dem SnapCenter-Host zu installieren. Verwenden Sie dazu das in diesem Tutorial beschriebene Verfahren.

Erstellen einer Plug-in-Beschreibungsdatei

Für jedes erstellte Plug-in müssen Sie eine Beschreibungsdatei haben. Die Beschreibungsdatei beschreibt die Details des Plug-ins. Der Name der Datei muss Plugin_descriptor.XML sein.

Verwenden der Attribute der Plug-in-Deskriptordatei und ihrer Bedeutung

Attribut	Beschreibung
Name	Name des Plug-ins. Alphanumerische Zeichen sind zulässig. Zum Beispiel DB2, MYSQL, MongoDB Stellen Sie bei Plug-ins, die im NATIVEN Stil erstellt wurden, sicher, dass Sie nicht die Erweiterung der Datei bereitstellen. Wenn der Plug-in-Name beispielsweise MongoDB.sh lautet, geben Sie den Namen als MongoDB an.
Version	Plug-in-Version: Kann sowohl die Haupt- als auch die Nebenversion enthalten. Beispiel: 1.0, 1.1, 2.0, 2.1
DisplayName	Der Plug-in-Name, der im SnapCenter-Server angezeigt werden soll. Wenn mehrere Versionen desselben Plug-ins geschrieben werden, stellen Sie sicher, dass der Anzeigename bei allen Versionen gleich ist.
PluginType	Sprache zum Erstellen des Plug-ins. Unterstützte Werte sind Perl, Java und Native. Nativer Plug-in-Typ umfasst Unix/Linux Shell-Skripte, Windows-Skripte, Python oder andere Skriptsprache.
OSName	Der Host-OS-Name, auf dem das Plug-in installiert ist. Gültige Werte sind Windows und Linux. Es ist möglich, dass ein einzelnes Plug-in für die Implementierung auf mehreren Betriebssystemtypen, wie BEISPIELSWEISE PERL-Plug-in, zur Verfügung steht.
OSVersion	Die Host-Betriebssystemversion, bei der das Plug-in installiert ist.
Einfindungsname	Name des Ressourcentyps, den das Plug-in unterstützen kann. Zum Beispiel Datenbank, Instanz, Sammlungen.
Übergeordnet	Wenn der ResourceName hierarchisch von einem anderen Ressourcentyp abhängig ist, bestimmt Parent den übergeordneten ResourceType. Zum Beispiel, DB2-Plug-in, die ResourceName „Datenbank“ hat eine übergeordnete „Instanz“.
RequireFileSystemPlugin	Ja oder Nein Legt fest, ob die Registerkarte Wiederherstellung im Wiederherstellungsassistenten angezeigt wird.

Attribut	Beschreibung
ResourceRequiesAuthentifizierung	Ja oder Nein Legt fest, ob die Ressourcen, die automatisch erkannt werden oder nicht automatisch erkannt wurden, Anmeldeinformationen benötigen, um die Datensicherungsvorgänge nach der Ermittlung des Storage auszuführen.
RequireFileSystemClone	Ja oder Nein Stellt fest, ob das Plug-in eine Filesystem-Plug-in-Integration für Klon-Workflow erforderlich ist.

Ein Beispiel für die Datei Plugin_descriptor.xml für benutzerdefinierte Plug-in DB2 ist wie folgt:

```
<Plugin>
<SMSServer></SMSServer>
<Name>DB2</Name>
<Version>1.0</Version>
<PluginType>Perl</PluginType>
<DisplayName>Custom DB2 Plugin</DisplayName>
<SupportedOS>
<OS>
<OSName>windows</OSName>
<OSVersion>2012</OSVersion>
</OS>
<OS>
<OSName>Linux</OSName>
<OSVersion>7</OSVersion>
</OS>
</SupportedOS>
<ResourceTypes>
<ResourceType>
<ResourceName>Database</ResourceName>
<Parent>Instance</Parent>
</ResourceType>
<ResourceType>
<ResourceName>Instance</ResourceName>
</ResourceType>
</ResourceTypes>
<RequireFileSystemPlugin>no</RequireFileSystemPlugin>
<ResourceRequiresAuthentication>yes</ResourceRequiresAuthentication>
<SupportsApplicationRecovery>yes</SupportsApplicationRecovery>
</Plugin>
```

ZIP-Datei wird erstellt

Nachdem ein Plug-in entwickelt wurde und eine Deskriptordatei erstellt wurde, müssen Sie die Plug-in-Dateien und die Datei Plugin_descriptor.xml in einen Ordner einfügen und entpacken.

Vor dem Erstellen einer ZIP-Datei müssen Sie Folgendes berücksichtigen:

- Der Skriptname muss mit dem Plug-in-Namen übereinstimmen.
- Für PERL-Plug-in muss der ZIP-Ordner einen Ordner mit der Skriptdatei enthalten und die Deskriptordatei außerhalb dieses Ordners liegen. Der Ordnername muss mit dem Plug-in-Namen identisch sein.
- Bei anderen Plug-ins als DEM PERL Plug-in muss der ZIP-Ordner den Deskriptor und die Skriptdateien enthalten.
- Die Betriebssystemversion muss eine Zahl sein.

Beispiele:

- DB2-Plugin: Fügen Sie DB2.pm und Plugin_descriptor.xml Datei zu "DB2.zip".
- Plug-in entwickelt mit Java: Fügen Sie JAR-Dateien, abhängige JAR-Dateien und Plugin_descriptor.xml-Datei in einen Ordner und ZIP es.

Hochladen der ZIP-Datei für das Plug-in

Sie müssen die Plug-in-ZIP-Datei auf den SnapCenter-Server hochladen, damit das Plug-in für die Bereitstellung auf dem gewünschten Host zur Verfügung steht.

Sie können das Plug-in über die UI oder Cmdlets hochladen.

UI:

- Laden Sie die Plug-in-ZIP-Datei als Teil des **Add**- oder **Modify Host**-Workflow-Assistenten hoch
- Klicken Sie auf * „Wählen Sie, um benutzerdefinierte Plug-in hochzuladen“*

PowerShell:

- Cmdlet "Upload-SmPluginPackage"

  Beispiel: PS> Upload-SmPluginPackage -AbsolutePath c:\DB2_1.zip

  Ausführliche Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder in den Cmdlet Referenzinformationen.

"SnapCenter Software Cmdlet Referenzhandbuch".

Bereitstellen benutzerdefinierter Plug-ins

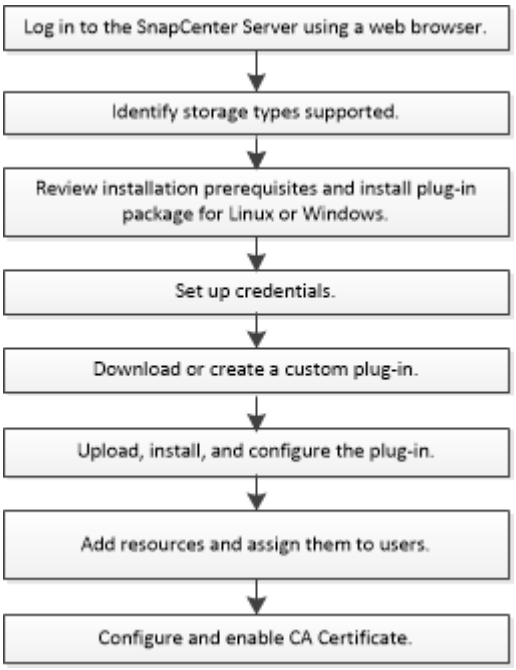
Das hochgeladene benutzerdefinierte Plug-in steht nun als Teil des Workflows **Add** und **Modify Host** für die Bereitstellung auf dem gewünschten Host zur Verfügung. Sie können mehrere Plug-ins-Versionen auf den SnapCenter-Server hochladen lassen, und Sie können die gewünschte Version für die Bereitstellung auf einem bestimmten Host auswählen.

Weitere Informationen zum Hochladen des Plug-ins finden Sie unter: "Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts"

Bereiten Sie die Installation von benutzerdefinierten SnapCenter-Plug-ins vor

Installationsworkflow von benutzerdefinierten SnapCenter Plug-ins

Sie sollten benutzerdefinierte SnapCenter-Plug-ins installieren und einrichten, wenn Sie benutzerdefinierte Plug-in-Ressourcen schützen möchten.



"Entwickeln Sie ein Plug-in für Ihre Applikation"

Voraussetzungen für das Hinzufügen von Hosts und die Installation benutzerdefinierter SnapCenter Plug-ins

Bevor Sie einen Host hinzufügen und die Plug-ins-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Die benutzerdefinierten Plug-ins können sowohl in Windows- als auch in Linux-Umgebungen verwendet werden.

- Sie müssen ein benutzerdefiniertes Plug-in erstellt haben. Weitere Informationen finden Sie in den Entwicklerinformationen.

  "Entwickeln Sie ein Plug-in für Ihre Applikation"

- Wenn Sie MySQL oder DB2 Applikationen managen möchten, müssen Sie die benutzerdefinierten Plug-ins für MySQL und DB2 von NetApp heruntergeladen haben.
- Sie müssen Java 1.8, 64-Bit auf Ihrem Linux- oder Windows-Host installiert haben.
- 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.
- Die benutzerdefinierten Plug-ins müssen auf dem Client-Host verfügbar sein, von dem aus der Add-Host-Vorgang ausgeführt wird.

Allgemein

Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.

Linux-Hosts

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

  Wenn Sie Windows 2019 oder Windows 2016 für den SnapCenter-Server-Host verwenden, müssen Sie Java 1.8, 64-Bit installieren. Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu Anforderungen.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-Tool"

- Sie müssen sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen. Fügen Sie die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux hinzu. Beispiel:

  ```
  Cmnd_Alias SCCMD = /opt/NetApp/snapcenter/scc/bin/scc <non_root_user>
  ALL=(ALL) NOPASSWD:SETENV: SCCMD
  ```

  Non_root_user ist der Name des nicht-Root-Benutzers, den Sie erstellt haben.

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

Bevor Sie das SnapCenter-Plug-ins-Paket für Linux installieren, sollten Sie sicherstellen, dass der Host die Anforderungen erfüllt.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
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 von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 1.8 (64-bit)Oracle Java oder OpenJDK Varianten Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool"

Richten Sie Anmeldedaten für benutzerdefinierte SnapCenter-Plug-ins ein

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

Was Sie brauchen

- 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.

- Benutzerdefinierte Plug-ins-Applikationen

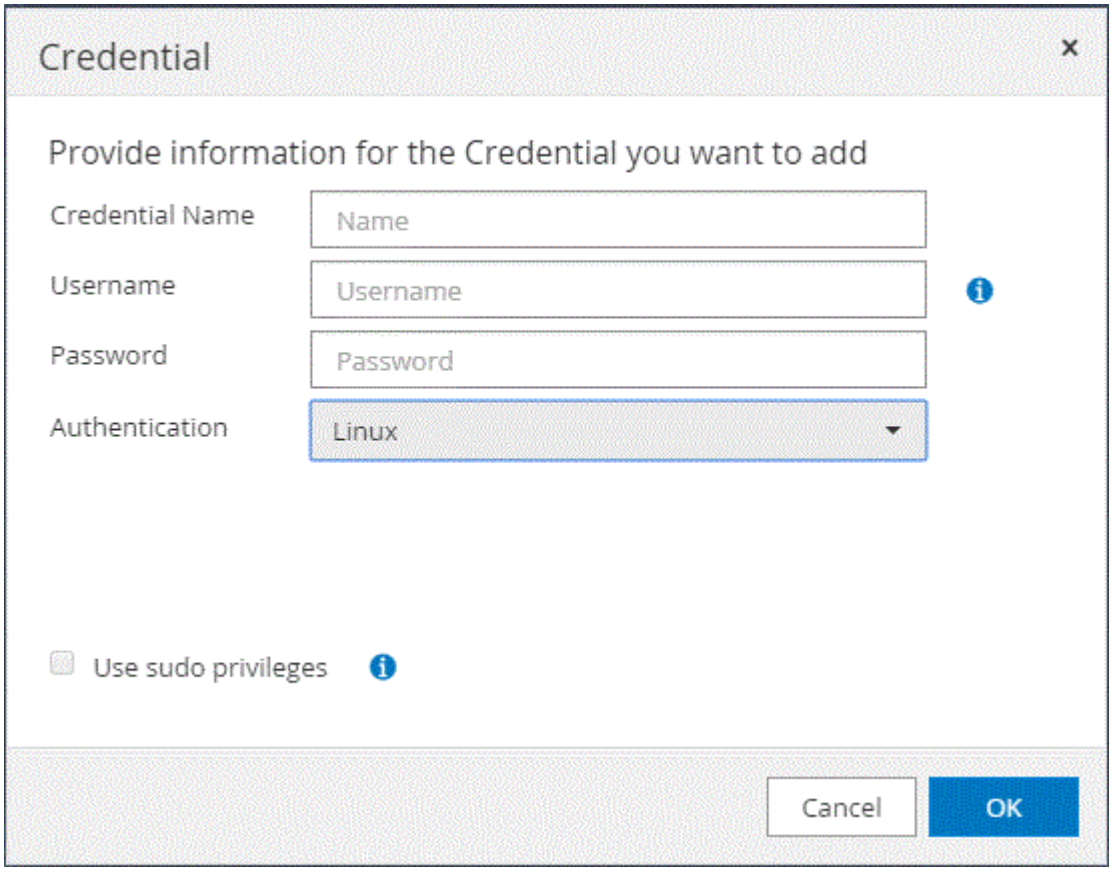
  Das Plug-in verwendet die Anmeldeinformationen, die beim Hinzufügen einer Ressource ausgewählt oder erstellt wurden. Wenn eine Ressource während des Datenschutzvorgangs keine Anmeldeinformationen benötigt, können Sie die Anmeldeinformationen auf **Keine** setzen.

Über diese Aufgabe

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.
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*
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 2012 oder höher

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

Was Sie brauchen

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

Schritte

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

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

   Beispiel:

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

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

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

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

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


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

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

a. Starten Sie den Host neu.

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

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

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

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

Installieren Sie die benutzerdefinierten SnapCenter-Plug-ins

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

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

Was Sie brauchen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

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

Über diese Aufgabe

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

Wenn Sie Plug-ins auf einem Cluster (WSFC) installieren, werden die Plug-ins auf allen Nodes des Clusters installiert.

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 Die benutzerdefinierten Plug-ins können sowohl in Windows als auch in Linux Umgebungen verwendet werden.
Host-Name	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. In Windows-Umgebungen wird die IP-Adresse nur für nicht vertrauenswürdige Domänen-Hosts unterstützt, wenn sie in den FQDN auflöst. Sie können die IP-Adressen oder FQDN eines eigenständigen Hosts eingeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.

Für dieses Feld…	Tun Sie das…
Anmeldedaten	Wählen Sie 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 zur Installation auswählen** die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer 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	Die benutzerdefinierten Plug-ins können entweder auf einem Windows-System oder auf einem Linux-System installiert 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. • Für die benutzerdefinierten SnapCenter Plug-ins: i. Klicken Sie im Abschnitt Benutzerdefinierte Plug-ins auf **Durchsuchen** und wählen Sie den Ordner mit dem gezippten benutzerdefinierten Plug-in aus. Der Ordner mit gezippten Daten enthält den benutzerdefinierten Plug-in-Code und die XML-Datei Deskriptor. Navigieren Sie zum Storage Plug-in zu *C:\ProgramData\NetApp\SnapCenter\Package Repository*, und wählen Sie aus `Storage.zip` Ordner. ii. Klicken Sie Auf **Upload**. Die XML-Datei Deskriptor im Ordner gezipptes benutzerdefiniertes Plug-in wird vor dem Hochladen des Pakets validiert. Die benutzerdefinierten Plug-ins, die auf den SnapCenter-Server hochgeladen werden, werden aufgelistet. Wenn Sie MySQL oder DB2 Applikationen managen möchten, können Sie die benutzerdefinierten MySQL und DB2 Plug-ins verwenden, die von NetApp zur Verfügung gestellt werden. Die benutzerdefinierten MySQL und DB2 Plug-ins sind im verfügbar "NetApp Automation Store"

Für dieses Feld…	Tun Sie das…
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

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

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

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

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

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

9. Überwachen Sie den Installationsfortschritt.

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

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

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

Was Sie brauchen

Der Benutzer, der einen Host hinzugefügt hat, sollte über die Administratorrechte auf dem Host verfügen.

Schritte

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

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

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

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

Installieren Sie die benutzerdefinierten SnapCenter-Plug-ins auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten die benutzerdefinierten SnapCenter-Plug-ins über die SnapCenter-Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie die benutzerdefinierten Plug-ins entweder im Konsolenmodus oder im Ruhemodus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Schritte

1. Kopieren Sie das SnapCenter Plug-ins Paket für die Linux Installationsdatei (snapcenter_linux_Host_Plugin.bin) von C:\ProgramData\NetApp\SnapCenter\Paket-Repository auf den Host, auf dem Sie die benutzerdefinierten Plug-ins 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. Fügen Sie den Host mit dem Cmdlet "Add-Smhost" und den erforderlichen Parametern zum SnapCenter-Server hinzu.

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

5. Melden Sie sich bei SnapCenter an und laden Sie das benutzerdefinierte Plug-in über die UI oder mithilfe von PowerShell Cmdlets hoch.

   Sie können das benutzerdefinierte Plug-in über die Benutzeroberfläche hochladen. Verwenden Sie dazu die Verweis "Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts" Abschnitt.

   Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets.

   "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen Sie den Status der Installation benutzerdefinierter Plug-ins

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

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

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

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

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

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

Importieren von CA-Zertifikaten

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

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins 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, *.p7b).

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

Abrufen des Daumenabdrucks für das CA-Zertifikat

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

Schritte

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

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

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten

und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Kopieren Sie den Daumendruck.

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

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

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

Schritte

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

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

   Beispiel:

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

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

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

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

   Beispiel:

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

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

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

Benutzerdefinierte Plug-ins verwenden die Datei 'keystore.jks', die sich unter */opt/NetApp/snapcenter/scc/etc*

sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

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

Schritte

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

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

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

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

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

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

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

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

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

Schritte

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

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

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

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

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

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

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

Schritte

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

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

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

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

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

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

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

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

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

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

Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

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

Schritte

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

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

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

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

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

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

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

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

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

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

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

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

Schritte

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

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

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

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

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

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

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

Schritte

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

Keytool -list -V -keystore keystore.jks

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

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

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

   Keytool -list -V -keystore keystore.jks

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

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

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

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

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

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

Über diese Aufgabe

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

Schritte

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

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Was Sie brauchen

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

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

Schritte

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

Nach Ihrer Beendigung

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

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

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

Bereiten Sie sich auf die Datensicherung vor

Voraussetzungen für die Verwendung der benutzerdefinierten SnapCenter-Plug-ins

Bevor Sie benutzerdefinierte SnapCenter-Plug-ins 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.
- Fügen Sie Hosts hinzu, und installieren und laden Sie die Plug-ins hoch.
- Installieren Sie ggf. Java 1.7 oder Java 1.8 auf dem Plug-in-Host.
- Wenn Sie mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration haben, können Sie Folgendes mithilfe der SnapCenter-CLI auf dem Datenbank-Host durchführen:

- Standardmäßig werden alle IP-Adressen des Datenbank-Hosts der Richtlinie für den NFS-Storage-Export in der Storage Virtual Machine (SVM) für die geklonten Volumes hinzugefügt. Wenn Sie eine bestimmte IP-Adresse haben oder auf eine Teilmenge der IP-Adressen beschränken möchten, führen Sie die CLI Set-PreferredHostIPsInStorageExportPolicy aus.
- Wenn in SVMs mehrere Datenpfade (LIFs) vorhanden sind, wählt SnapCenter den entsprechenden Datenpfad (LIF) zur Mounten des geklonten NFS-Volumes. Wenn Sie jedoch einen bestimmten Datenpfad (LIF) angeben möchten, müssen Sie die CLI Set-SvmPreferredDataPath ausführen. Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Command Reference Guide".

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.
- Stellen Sie sicher, dass Port 9090 von keiner anderen Anwendung auf dem Host verwendet wird.

  Port 9090 muss zusätzlich zu den anderen von SnapCenter benötigten Ports für die Verwendung durch benutzerdefinierte SnapCenter-Plug-ins reserviert werden.

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz benutzerdefinierter Plug-in-Ressourcen verwendet werden

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

- Ressourcen sind normalerweise Datenbanken, Windows File-Systeme oder VMs, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster.

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

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

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

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

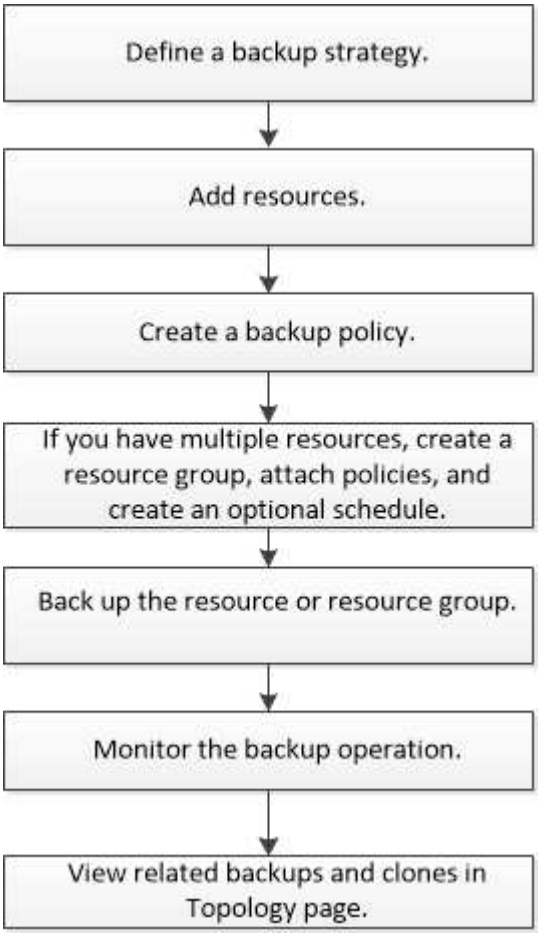
Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme des Hosts enthält. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein dateibasiertes Backup durchführen, und einen anderen Zeitplan, der stündliche Snapshot-basierte Backups durchführt.

Sichern Sie benutzerdefinierte Plug-in-Ressourcen

Sichern Sie benutzerdefinierte Plug-in-Ressourcen

Der Backup-Workflow umfasst die Planung, die Ermittlung der Backup-Ressourcen, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

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



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

Benutzerdefinierte SnapCenter Plug-ins mit Ressourcen ergänzen

Sie müssen die Ressourcen hinzufügen, die Sie sichern oder klonen möchten. Je nach Umgebung können sich die Ressourcen entweder um Datenbankinstanzen oder Sammlungen handeln, die Sie sichern oder klonen möchten.

Was Sie brauchen

- Sie müssen Aufgaben wie das Installieren des SnapCenter-Servers, das Hinzufügen von Hosts, das

Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.

- Sie müssen ein benutzerdefiniertes Plug-in erstellt haben.

  "Entwickeln Sie ein Plug-in für Ihre Applikation"

- Sie müssen die Plug-ins auf SnapCenter Server hochgeladen haben.

Über diese Aufgabe

Sie können auch Ressourcen für MySQL- und DB2-Anwendungen hinzufügen. Diese Plug-ins können von heruntergeladen werden "NetApp Storage Automation Store".

Schritte

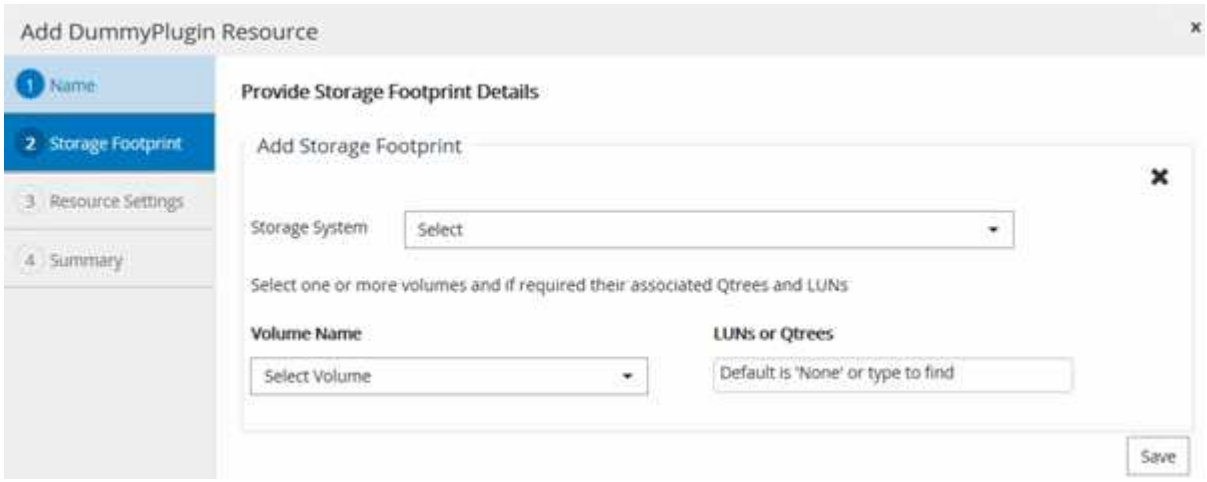
1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf der Seite Ressourcen auf **Ressource hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressource ein.
Host-Name	Wählen Sie den Host aus.
Typ	Wählen Sie den Typ aus. Der Typ ist gemäß der Plug-in-Beschreibungsdatei Benutzerdefiniert. Beispiel: Datenbank und Instanz. Wenn der ausgewählte Typ ein übergeordnetes Element hat, geben Sie die Details des übergeordneten Typs ein. Wenn der Typ beispielsweise „Datenbank“ und „übergeordnetes Objekt“ ist, geben Sie die Details der Instanz ein.
Name der Anmeldeinformationen	Wählen Sie Anmeldedaten aus oder erstellen Sie eine neue Berechtigung.
Mount-Pfade	Geben Sie die Mount-Pfade ein, auf denen die Ressource angehängt ist. Dies gilt nur für einen Windows-Host.

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

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

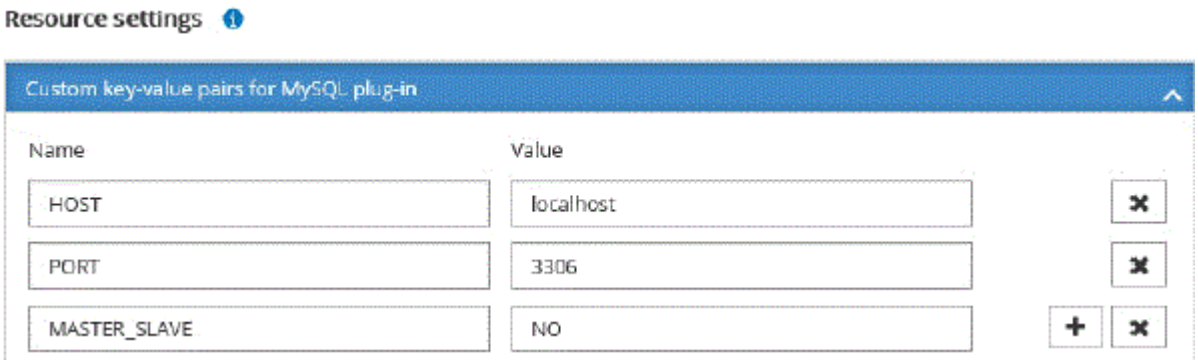
Die benutzerdefinierten Plug-ins von SnapCenter unterstützen nicht die automatische Erkennung von Ressourcen und Storage-Details für physische und virtuelle Umgebungen. Sie müssen Storage-Informationen für physische und virtuelle Umgebungen bereitstellen und gleichzeitig Ressourcen erstellen.



5. Stellen Sie auf der Seite „Ressourceneinstellungen“ benutzerdefinierte Key-Value-Paare für die Ressource bereit.

   Verwenden Sie die benutzerdefinierten Schlüssel-Wert-Paare, wenn Sie ressourcenspezifische Informationen übergeben möchten. Wenn Sie beispielsweise das MySQL-Plug-in verwenden, müssen Sie einen HOST als HOST=hostname, PORT =Port-no angeben, der für MySQL und Master-Slave-Konfiguration als MASTER_SLAVE = „YES“ oder „NO“ verwendet wird (Name ist MASTER_SLAVE und Wert ist „JA“ oder „NO“).

   Stellen Sie sicher, dass DIE Wörter HOST und PORT in Großbuchstaben stehen.



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

Ergebnis

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

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

Nach Ihrer Beendigung

Wenn Sie anderen Benutzern Zugriff auf die Assets gewähren möchten, muss der SnapCenter-Administrator diesen Benutzern Assets zuweisen. Auf diese Weise können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

Nachdem Sie die Ressourcen hinzugefügt haben, können Sie die Ressourcendetails ändern. Wenn einer benutzerdefinierten Plug-in-Ressource Backups zugeordnet sind, können die folgenden Felder nicht geändert werden: Ressourcenname, Ressourcentyp und Hostname.

Erstellen von Richtlinien für benutzerdefinierte Plug-in-Ressourcen

Bevor Sie mit SnapCenter benutzerdefinierte Plug-in-spezifische Ressourcen sichern, müssen Sie eine Backup-Richtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten.

Was Sie brauchen

- Sie sollten Ihre Backup-Strategie definiert haben.

  Weitere Informationen finden Sie in den Informationen zur Definition einer Datensicherungsstrategie für benutzerdefinierte Plug-ins.

- Sie sollten sich auf die Datensicherung vorbereiten.

  Die Vorbereitung auf die Datensicherung umfasst Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erstellen von Verbindungen zum Storage-System und das Hinzufügen von Ressourcen.

- Die Storage Virtual Machines (SVMs) sollten Ihnen für Spiegelungs- oder Vault-Vorgänge zugewiesen werden.

  Der SnapCenter Administrator muss Ihnen die SVMs für die Quell- und Ziel-Volumes zuweisen, falls Sie Snapshot Kopien in eine Spiegelung oder einen Vault replizieren.

- Sie sollten die Ressourcen, die Sie schützen möchten, manuell hinzugefügt haben.

Über diese Aufgabe

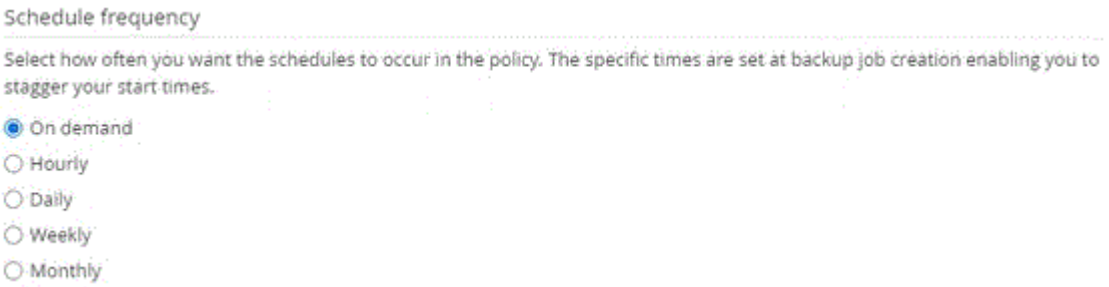
- Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln. Außerdem können Sie Replizierungs-, Skript- und Applikationseinstellungen festlegen.
- Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.

Schritte

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

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

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



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

- Geben Sie im Abschnitt Benutzerdefinierte Backup-Einstellungen alle spezifischen Backup-Einstellungen an, die an das Plug-in-in-Schlüsselwert-Format übergeben werden müssen. Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.

6. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

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

7. Geben Sie auf der Seite Replikation die Replikationseinstellungen an:

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

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

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

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

Schritte

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

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

4. Optional: 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

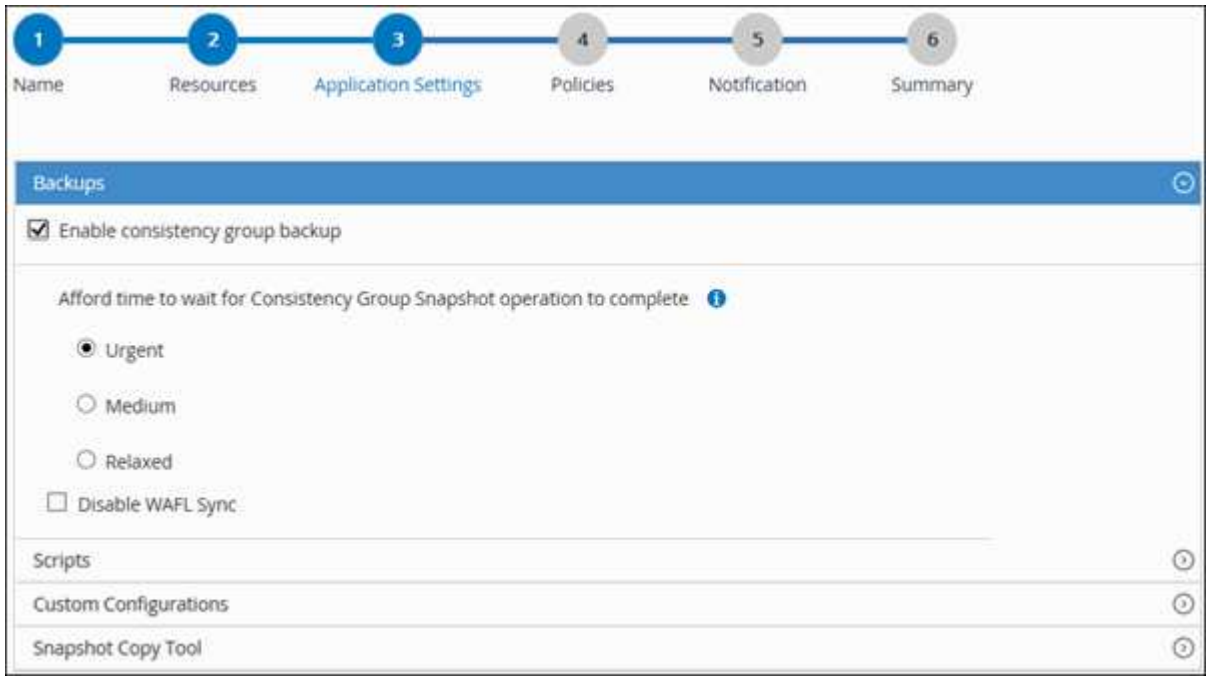
rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.

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

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

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

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

+ 

   a. Klicken Sie auf den Pfeil „Skripte“ und geben Sie die vor- und Post-Befehle für quiesce, Snapshot copy 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 Datensicherungsvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

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

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

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

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu nutzen und das Filesystem in einen konsistenten Zustand zu versetzen, bevor eine Snapshot Kopie erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie SnapCenter mit Filesystem-Konsistenz aus. Diese Option ist für das SnapCenter-Plug-in für SAP HANA Database nicht verfügbar.
SnapCenter zum Erstellen einer Snapshot Kopie auf Storage-Ebene	Wählen Sie SnapCenter ohne File System Consistency aus.

Ihre Situation	Dann…
Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie „Sonstige“ aus, und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um eine Snapshot Kopie zu erstellen.

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

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

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

      Die Richtlinien sind im Abschnitt * Zeitpläne für ausgewählte Richtlinien konfigurieren* aufgeführt.

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

   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_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**.

Sicherung individueller Plug-in-Ressourcen

Wenn eine einzelne benutzerdefinierte Plug-in-Ressource nicht zu einer Ressourcengruppe gehört, können Sie die Ressource über die Seite Ressourcen sichern. Sie können die Ressource nach Bedarf sichern, oder wenn die Ressource über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Was Sie brauchen

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

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.

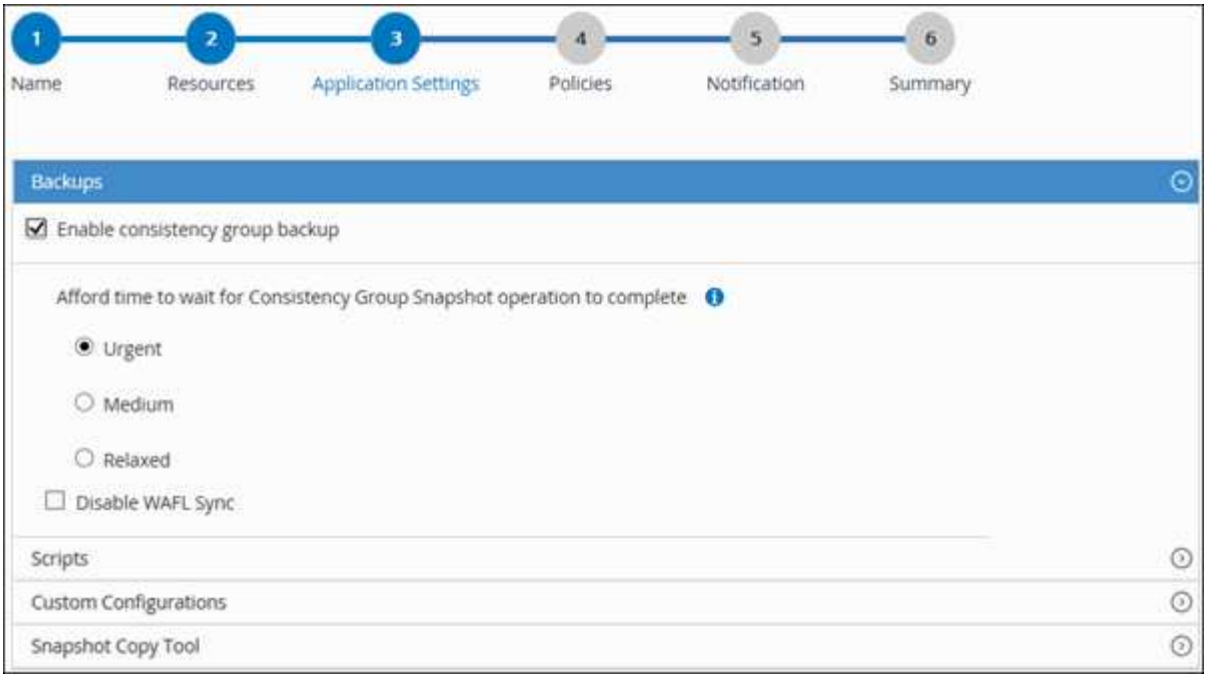
   Klicken Sie Auf Und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auf klicken Um den Filterbereich zu schließen.
3. Klicken Sie auf die Ressource, die Sie sichern möchten.
4. Wenn Sie auf der Seite „Ressource“ einen benutzerdefinierten Namen verwenden möchten, aktivieren Sie das Kontrollkästchen **benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** und geben dann ein benutzerdefiniertes Namensformat für den Namen der Snapshot-Kopie ein.

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

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

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

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

+ 

a. Klicken Sie auf den Pfeil **Scripts**, um vor- und Post-Befehle für quiesce, Snapshot copy und unquiesce-Vorgänge auszuführen. Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen.

   Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen**, und geben Sie dann die für alle Aufträge, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.

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

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

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

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

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

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

aufgelistet.

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

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

Dabei ist *Policy_Name* 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 klicken Sie dann auf **Fertig stellen**.

Die Seite „Ressourcen-Topologie“ wird angezeigt.

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

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

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

Sichern Sie Ressourcengruppen benutzerdefinierter Plug-in-Ressourcen

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.

Was Sie brauchen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung zum 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.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.

2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.

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

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

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

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

     "SnapMirror oder SnapVault-Beziehung kann nach MetroCluster Failover nicht erkannt werden"

   - Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java Heap-Größe für das SnapCenter-Plug-in für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen. Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei /opt/netapp/init_scvservice. In diesem Skript, das `do_start method` Befehl startet den SnapCenter-VMware-Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

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

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

Was Sie brauchen

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

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

- Speichersystemnamen sollten eindeutig sein.

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

Schritte

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

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

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

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

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

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

   In diesem Beispiel werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

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

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

Sichern Sie Ressourcen mit PowerShell cmdlets

Das Sichern einer Ressource umfasst die Einrichtung einer Verbindung mit dem SnapCenter-Server, das Hinzufügen von Ressourcen, das Hinzufügen von Richtlinien, das Erstellen einer Backup-Ressourcengruppe und das Sichern von Ressourcen.

Was Sie brauchen

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

Über diese Aufgabe

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

Schritte

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

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

Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

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

   In diesem Beispiel werden Ressourcen hinzugefügt:

```
Add-SmResource -HostName '10.232.206.248' -PluginCode 'DB2'
-ResourceName NONREC1 -ResourceType Database -StorageFootPrint ( @
{"VolumeName"="DB2_NONREC1DB";"LunName"="DB2_NONREC1DB";"Vserver"="vserv
er_scauto_secondary"}) -Instance db2inst1
```

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

   Dieses Beispiel erstellt eine neue Backup-Richtlinie:

```
Add-SMPolicy -PolicyName 'db2VolumePolicy' -PolicyType 'Backup'
-PluginPolicyType DB2  -description 'VolumePolicy'
```

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

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

```
Add-SmResourceGroup -ResourceGroupName
'Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix' -Resources @(@
{"Host"="10.232.206.248";"Uid"="db2inst2\NONREC"},@{"Host"="10.232.206.2
48";"Uid"="db2inst1\NONREC"}) -Policies db2ManualPolicy
```

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

```
New-SMBackup -DatasetName
Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix -Policy
db2ManualPolicy
```

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

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

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

Überwachen Sie benutzerdefinierte Backup-Vorgänge für Plug-in-Ressourcen

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

Abbrechen der Backup-Vorgänge für benutzerdefinierte Plug-ins

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

Sehen Sie sich auf der Seite Topologie benutzerdefinierte Backups und Klone zu den Plug-in-Ressourcen 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. 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.

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.

  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.

- 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 erstellt haben, um nur 4 Backups aufzubewahren, werden die Anzahl der angezeigten Backups 6 angezeigt.

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

Schritte

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

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

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

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone angezeigt.

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

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

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

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

   Sie können Backups, die sich auf dem sekundären Speichersystem befinden, nicht umbenennen oder löschen.

   Sie können die Backups, die sich auf dem primären Speichersystem befinden, nicht umbenennen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie auf Um den Klon zu löschen.

Stellen Sie benutzerdefinierte Plug-in-Ressourcen wieder her

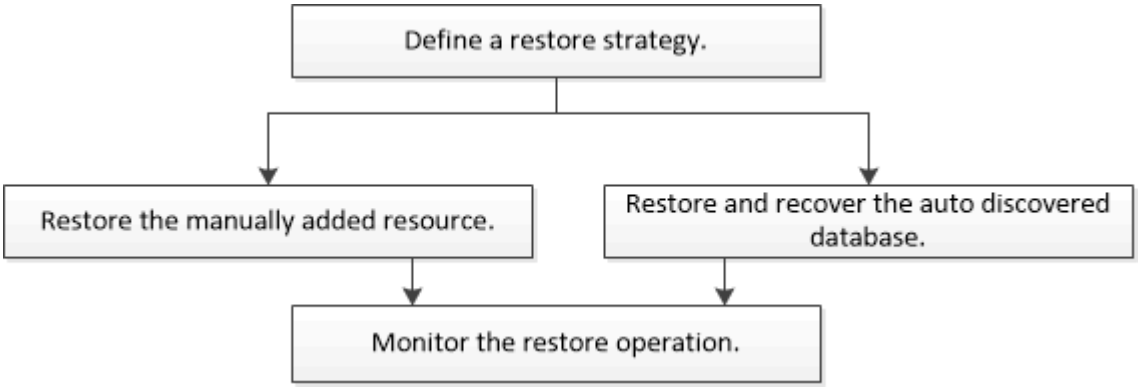
Stellen Sie benutzerdefinierte Plug-in-Ressourcen wieder her

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-

Vorgängen und Monitoring von Vorgängen.

Über diese Aufgabe

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. Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder im "SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines Ressourcenbackups

Mit SnapCenter können Sie Ressourcen wiederherstellen. Die Funktionen der Restore-Vorgänge hängen vom verwendeten Plug-in ab.

Was Sie brauchen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Der SnapCenter Administrator muss Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch Ziel-Volumes zugewiesen haben, wenn Sie Snapshot Kopien in einer Spiegelung oder einem Vault replizieren.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die wiederhergestellt werden soll.

Über diese Aufgabe

Der Standardwiederherstellungsvorgang stellt nur Storage-Objekte wieder her. Restore-Vorgänge auf Applikationsebene können nur durchgeführt werden, wenn das benutzerdefinierte Plug-in diese Funktion bietet.

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- oder Cluster-Name, zugeordnete Ressourcengruppen und -Richtlinien sowie der Status angezeigt.

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

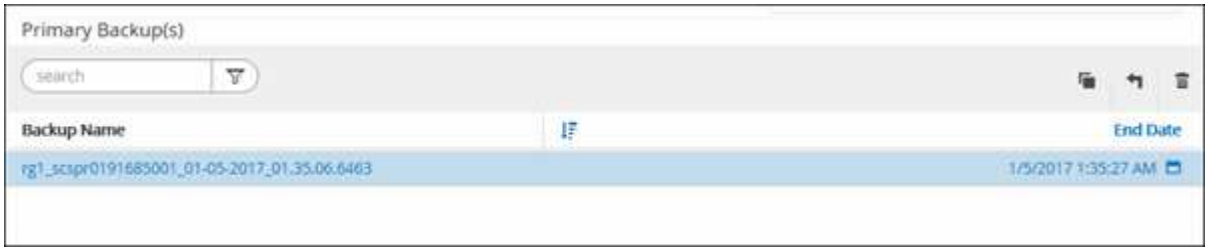
Wenn die Ressource nicht geschützt ist, wird *Not Protected* in der Spalte **Gesamtstatus** angezeigt.

Der Status *not protected* in der Spalte **Gesamtstatus** kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem 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 gewölbten) Speichersystemen aus.
5. Wählen Sie in der Tabelle primäre(n) Backups das Backup aus, von dem Sie wiederherstellen möchten, und klicken Sie dann auf .



6. Wählen Sie auf der Seite „Bereich wiederherstellen“ die Option **vollständige Ressource** oder **Dateiebene** aus.
   a. Wenn Sie **Complete Resource** ausgewählt haben, wird die Ressourcen-Sicherung wiederhergestellt.

      Wenn die Ressource Volumes oder qtrees als Storage-Platzbedarf enthält, werden neuere Snapshot Kopien auf solchen Volumes oder qtrees gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf denselben Volumes oder qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

   b. Wenn Sie **File Level** ausgewählt haben, können Sie entweder **Alle** auswählen oder Volumes oder qtrees auswählen und dann den Pfad eingeben, der mit den Volumes oder qtrees verbunden ist, die durch Kommas getrennt ausgewählt werden.
      - Sie können mehrere Volumes und qtrees auswählen.
      - Wenn der Ressourcentyp LUN ist, wird die gesamte LUN wiederhergestellt. Sie können mehrere LUNs auswählen. + HINWEIS: Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, qtrees oder LUNs wiederhergestellt.
7. Führen Sie auf der Seite Wiederherstellungstyp die folgenden Schritte aus: Wählen Sie Option, um Protokolle anzuwenden. Vergewissern Sie sich, dass Ihr Plugin alle Protokolle und Protokolle unterstützt, bis Sie den Typ wiederherstellen, bevor Sie ihn auswählen.

Ihr Ziel ist	Tun Sie das…
Wiederherstellung aller Protokolle	Wählen Sie **Alle Protokolle**. Stellen Sie sicher, dass das Plug-in **Alle Protokolle** unterstützt.
Stellen Sie alle Protokolle bis zur angegebenen Zeit wieder her	Wählen Sie **Protokolle bis**. Stellen Sie sicher, dass das Plug-in **Logs bis** unterstützt.
Stellen Sie das Ressourcen-Backup wieder her	Wählen Sie **Keine**.

8. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.
9. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.
10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

    Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Überwachen Sie benutzerdefinierte Restore-Vorgänge für Plug-in-Ressourcen

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

Über diese Aufgabe

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.

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

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

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

Klonen benutzerdefinierter Plug-in-Ressourcen-Backups

Klonen benutzerdefinierter Plug-in-Ressourcen-Backups

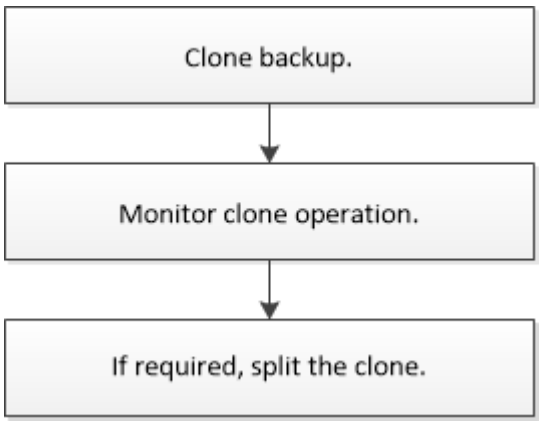
Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

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. Ausführliche Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder in der "SnapCenter Software Cmdlet Referenzhandbuch".

Klonen aus einem Backup

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen. Die Funktionen der Klonvorgänge hängen vom verwendeten Plug-in ab.

Was Sie brauchen

- Sie müssen die Ressourcen oder Ressourcengruppe gesichert haben.
- Bei dem Standardklonvorgang werden nur Storage-Objekte geklont. Klonvorgänge auf Applikationsebene können nur durchgeführt werden, wenn das benutzerdefinierte Plug-in diese Funktion bietet.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.

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- oder Cluster-Name, zugeordnete Ressourcengruppen und -Richtlinien sowie der 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 Standorte die folgenden Schritte aus:

Für dieses Feld…	Tun Sie das…
Klonserver	Standardmäßig wird der Quell-Host befüllt. Wenn Sie einen anderen Host angeben möchten, wählen Sie den Host aus, auf dem der Klon gemountet werden soll, und das Plug-in ist installiert.

Für dieses Feld…	Tun Sie das…
Suffix klonen	Dies ist obligatorisch, wenn das Klonziel mit der Quelle identisch ist. Geben Sie ein Suffix ein, das an den neu geklonten Ressourcennamen angehängt wird. Das Suffix stellt sicher, dass die geklonte Ressource auf dem Host eindeutig ist. Beispiel: rs1_Clone. Wenn Sie auf demselben Host wie die Originalressource klonen, müssen Sie ein Suffix bereitstellen, um die geklonte Ressource von der ursprünglichen Ressource zu differenzieren. Andernfalls schlägt der Vorgang fehl.

Wenn die ausgewählte Ressource eine LUN ist und wenn Sie über ein sekundäres Backup klonen, werden die Ziel-Volumes aufgelistet. Es kann mehrere Ziel-Volumes vorhanden sein.

7. Führen Sie auf der Seite Einstellungen folgende Schritte aus:

Für dieses Feld…	Tun Sie das…
Name des Initiators	Geben Sie den Host-Initiatornamen ein. Dieser ist entweder ein IQDN oder ein WWPN.
IGroup-Protokoll	Wählen Sie das iGroup-Protokoll aus.

Einstellungsseite wird nur angezeigt, wenn der Speichertyp LUN ist.

8. Geben Sie auf der Seite „Skripts“ die Befehle für den vor- bzw. Nachklon ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

   Beispiel:

   - Befehl Pre Clone: Löschen Sie vorhandene Datenbanken mit demselben Namen
   - Befehl nach Clone: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.

     Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:
     Mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

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.

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

Klonen von Backups mit PowerShell Cmdlets

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

Was Sie brauchen

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

Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder im "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

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

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

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

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

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

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

   In diesem Beispiel werden Informationen über eine bestimmte Ressourcengruppe angezeigt:

```
PS C:\> Get-SmResourceGroup

    Description                 :
    CreationTime                : 10/10/2016 4:45:53 PM
    ModificationTime            : 10/10/2016 4:45:53 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
```

```
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               : SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Completed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassCredential            : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
    IsInternal                  : False
    EnableEmailAttachment       : False
    VerificationSettings        : {}
    Name                        : NFS_DB
    Type                        : Group
    Id                          : 2
    Host                        :
    UserName                    :
    Passphrase                  :
    Deleted                     : False
    Auth                        : SMCoreContracts.SmAuth
    IsClone                     : False
    CloneLevel                  : 0
    Hosts                       :
    StorageName                 :
    ResourceGroupNames          :
    PolicyNames                 :

    Description                 :
    CreationTime                : 10/10/2016 4:51:36 PM
    ModificationTime            : 10/10/2016 5:27:57 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
```

```
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               : SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Failed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassRunAs                 : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
    IsInternal                  : False
    EnableEmailAttachment       : False
    VerificationSettings        : {}
    Name                        : Test
    Type                        : Group
    Id                          : 3
    Host                        :
    UserName                    :
    Passphrase                  :
    Deleted                     : False
    Auth                        : SMCoreContracts.SmAuth
    IsClone                     : False
    CloneLevel                  : 0
    Hosts                       :
    StorageName                 :
    ResourceGroupNames          :
    PolicyNames                 :
```

3. Initiieren Sie einen Klonvorgang aus einer Clone Ressourcengruppe oder einer vorhandenen Sicherung mit dem Cmdlet "New-SmClone".

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

```
New-SmClone -BackupName Verify_delete_clone_on_qtree_windows_scc54_10-
04-2016_19.05.48.0886 -Resources
@{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"}  -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

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

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

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

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

Überwachung benutzerdefinierter Plug-in-Klonvorgänge

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.