



Schützen Sie Anwendungen mit von NetApp unterstützten Plug-ins

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-61/protect-nsp/netapp_supported_plugins_overview.html on November 06, 2025. Always check docs.netapp.com for the latest.

Inhalt

Schützen Sie Anwendungen mit von NetApp unterstützten Plug-ins	1
Von NetApp unterstützte Plug-Ins	1
Übersicht der von NetApp unterstützten Plug-ins	1
Was Sie mit den von NetApp unterstützten Plug-ins tun können	1
Von NetApp unterstützte Plug-In-Funktionen	2
Von NetApp unterstützte Speichertypen	3
Für das von NetApp unterstützte Plug-In sind mindestens ONTAP -Berechtigungen erforderlich	3
Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für von NetApp unterstützte Plug-Ins vor	6
Definieren Sie eine Sicherungsstrategie	6
Sicherungsstrategie für von NetApp unterstützte Plug-Ins	7
Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte, von NetApp unterstützte Plug-in-Ressourcen unterstützt werden	8
Bereiten Sie die Installation von NetApp unterstützten Plug-Ins vor	8
Installationsablauf der von SnapCenter NetApp unterstützten Plug-Ins	8
Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows, Linux oder AIX	9
Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows	13
Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux und AIX	14
Einrichten von Anmeldeinformationen für von NetApp unterstützte Plug-Ins	15
Konfigurieren von gMSA unter Windows Server 2016 oder höher	18
Installieren Sie die von NetApp unterstützten Plug-Ins	19
CA-Zertifikat konfigurieren	26
Bereiten Sie sich auf den Datenschutz vor	34
Voraussetzungen für die Verwendung der von NetApp unterstützten Plug-Ins	34
So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von NetApp unterstützten Plug-In-Ressourcen verwendet	35
Sichern Sie von NetApp unterstützte Plug-In-Ressourcen	35
Sichern Sie von NetApp unterstützte Plug-In-Ressourcen	36
Ressourcen zu NetApp unterstützten Plug-ins hinzufügen	36
Erstellen Sie Richtlinien für von NetApp unterstützte Plug-In-Ressourcen	41
Erstellen von Ressourcengruppen und Anfügen von Richtlinien	45
Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Ressourcen auf ASA R2-Systemen	49
Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets	52
Sichern Sie einzelne von NetApp unterstützte Plug-In-Ressourcen	53
Sichern Sie Ressourcengruppen von NetApp unterstützten Plug-In-Ressourcen	58
Überwachen Sie die Sicherungsvorgänge für NetApp unterstützte Plug-In-Ressourcen	59
Abbrechen von Sicherungsvorgängen für von NetApp unterstützte Plug-Ins	60
Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“	61
Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen	63

Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen	63
Wiederherstellen einer Ressourcensicherung	63
Überwachen Sie die Wiederherstellungsvorgänge für von NetApp unterstützte Plug-In-Ressourcen . . .	68
Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen	69
Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen	69
Klonen aus einer Sicherung	70
Überwachen Sie von NetApp unterstützte Plug-in-Ressourcenklonvorgänge	76

Schützen Sie Anwendungen mit von NetApp unterstützten Plug-ins

Von NetApp unterstützte Plug-Ins

Übersicht der von NetApp unterstützten Plug-ins

Sie können die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und das Storage-Plug-in für die von Ihnen genutzten Anwendungen verwenden und diese Anwendungen dann mit SnapCenter sichern, wiederherstellen oder klonen. Ihre von NetApp unterstützten Plug-ins fungieren als hostseitige Komponenten der NetApp SnapCenter -Software und ermöglichen anwendungsbewussten Datenschutz und die Verwaltung von Ressourcen.

Wenn von NetApp unterstützte Plug-Ins installiert sind, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und die NetApp SnapVault -Technologie verwenden, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen. Die von NetApp unterstützten Plug-Ins können sowohl in Windows- als auch in Linux-Umgebungen verwendet werden.



SnapCenterCLI unterstützt keine von NetApp unterstützten Plug-In-Befehle.

NetApp stellt das Storage-Plug-in bereit, um Datenschutzvorgänge des Datenvolumens auf dem ONTAP Speicher mithilfe des in SnapCenter integrierten Plug-in-Frameworks durchzuführen.

Sie können die von NetApp unterstützten Plug-Ins von der Seite „Host hinzufügen“ aus installieren.

["Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts."](#)



Die Supportrichtlinien von SnapCenter decken den Support für das Plug-in-Framework, die Core Engine und die zugehörigen APIs ab. Der Support umfasst nicht den Plug-in-Quellcode und die zugehörigen Skripte, die auf dem Plug-in-Framework basieren.

Was Sie mit den von NetApp unterstützten Plug-ins tun können

Sie können die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB und das Storage-Plug-in für Datenschutzvorgänge verwenden.

- Fügen Sie Ressourcen wie Datenbanken, Instanzen, Dokumente oder Tablespace hinzu.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

Sie können die von NetApp unterstützten Plug-Ins für Datenschutzvorgänge verwenden.

- Erstellen Sie Snapshots der Konsistenzgruppe der Speichervolumes über ONTAP -Cluster hinweg.
- Sichern Sie benutzerdefinierte Anwendungen mithilfe des integrierten Pre- und Post-Scripting-Frameworks

Sie können ein ONTAP Volume, LUN oder einen Qtree sichern.

- Aktualisieren Sie Snapshots, die auf dem primären Server erstellt wurden, auf einen ONTAP Sekundärserver und nutzen Sie dabei die vorhandene Replikationsbeziehung (SnapVault/SnapMirror/vereinheitlichte Replikation) mithilfe der SnapCenter Richtlinie

ONTAP Primär- und Sekundärserver können ONTAP FAS, AFF, ASA, ONTAP Select oder Cloud Volumes ONTAP sein.

- Stellen Sie das komplette ONTAP Volume, LUN oder Dateien wieder her.

Sie sollten den jeweiligen Dateipfad manuell angeben, da die Such- oder Indizierungsfunktionen nicht in das Produkt integriert sind.

Qtree- oder Verzeichniswiederherstellung wird nicht unterstützt, Sie können jedoch nur den Qtree klonen und exportieren, wenn der Sicherungsumfang auf Qtree-Ebene definiert ist.

Von NetApp unterstützte Plug-In-Funktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit von NetApp unterstützten Plug-Ins wie MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und Storage-Plug-in 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. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Technologie**

SnapCenter verwendet die NetApp Snapshot-Technologie mit den von NetApp unterstützten Plug-Ins zum Sichern von Ressourcen. Snapshots verbrauchen nur minimalen Speicherplatz.

Die von NetApp unterstützten Plug-Ins bieten außerdem die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

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

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

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

- Unterstützung für die Consistency Group (CG) Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

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

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Möglichkeit zum Erstellen dateisystemkonsistenter Snapshots in Windows-Umgebungen.

Von NetApp unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen auf physischen und virtuellen Maschinen. Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie von NetApp unterstützte Plug-Ins installieren.

Maschine	Speichertyp
Physische und NFS-Direktmounts auf den VM-Hosts (VMDKs und RDM-LUNs werden nicht unterstützt.)	FC-verbundene LUNs
Physische und NFS-Direktmounts auf den VM-Hosts (VMDKs und RDM-LUNs werden nicht unterstützt.)	Über iSCSI verbundene LUNs
Physische und NFS-Direktmounts auf den VM-Hosts (VMDKs und RDM-LUNs werden nicht unterstützt.)	Über NFS verbundene Volumes
VMware ESXi	vVol-Datenspeicher auf NFS und SAN vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Für das von NetApp unterstützte Plug-In sind mindestens ONTAP -Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
 - Ereignis generieren-Autosupport-Protokoll
 - Jobverlauf anzeigen

- Jobstopp
- LUN-Attribut anzeigen
- LUN erstellen
- LUN löschen
- LUN-Geometrie
- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- lun igroup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Netzwerkschnittstelle
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start

- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
 - Netzwerkschnittstelle

Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für von NetApp unterstützte Plug-Ins vor

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



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

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#).

Definieren Sie eine Sicherungsstrategie

Durch das Definieren einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge wird sichergestellt, dass Sie über die Sicherungen verfügen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

Schritte

1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.

4. Entscheiden Sie, ob Sie Konsistenzgruppen-Snapshots möchten, und entscheiden Sie sich für geeignete Optionen zum Löschen von Konsistenzgruppen-Snapshots.
5. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
6. Bestimmen Sie die Aufbewahrungsdauer für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
7. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

Sicherungsstrategie für von NetApp unterstützte Plug-Ins

Sicherungspläne für von NetApp unterstützte Plug-In-Ressourcen

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Je häufiger Sie Ihre Ressourcen sichern, desto weniger Archivprotokolle muss SnapCenter für die Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

SLA definiert das erwartete Serviceniveau und befasst sich mit vielen servicebezogenen Problemen, einschließlich der Verfügbarkeit und Leistung des Dienstes. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren. Sie können in der SnapCenter -GUI auf Richtlinien zugreifen, indem Sie auf **Einstellungen > Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können in der SnapCenter -GUI auf die Zeitpläne der Ressourcengruppe zugreifen, indem Sie auf **Ressourcen** klicken, dann das entsprechende Plug-In auswählen und auf **Anzeigen > Ressourcengruppe** klicken.

Anzahl der benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Die Anzahl der von Ihnen ausgewählten Sicherungsaufträge hängt normalerweise von der Anzahl der Datenträger ab, auf denen Sie Ihre Ressourcen platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Ressourcen auf einem Volume und eine große Ressource auf einem anderen Volume platziert haben, können Sie einen Sicherungsauftrag für die kleinen Ressourcen und einen Sicherungsauftrag für die große Ressource erstellen.

Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte, von NetApp unterstützte Plug-in-Ressourcen unterstützt werden

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte, von NetApp unterstützte Plug-In-Ressourcen.



Sie können manuell hinzugefügte, von NetApp unterstützte Plug-In-Ressourcen nicht wiederherstellen.

Vollständige Ressourcenwiederherstellung

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



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

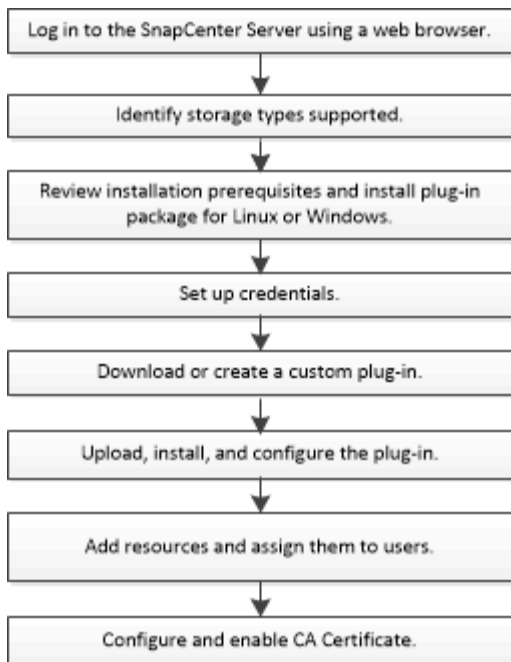
Wiederherstellung auf Dateiebene

- Stellt Dateien aus Volumes, Qtrees oder Verzeichnissen wieder her
- Stellt nur die ausgewählten LUNs wieder her

Bereiten Sie die Installation von NetApp unterstützten Plug-Ins vor

Installationsablauf der von SnapCenter NetApp unterstützten Plug-Ins

Sie sollten von SnapCenter NetApp unterstützte Plug-Ins installieren und einrichten, wenn Sie von NetApp unterstützte Plug-In-Ressourcen schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows, Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-In-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Die von NetApp unterstützten Plug-Ins werden in Windows-, Linux- und AIX-Umgebungen unterstützt.



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

- Sie müssen Java 11 auf Ihrem Linux-, Windows- oder AIX-Host installiert haben.



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

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB und Storage-Plug-in müssen auf dem Client-Host verfügbar sein, von dem aus der Vorgang zum Hinzufügen des Hosts ausgeführt wird.

Allgemein

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

Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Wenn Sie Clusterknoten in SnapCenter verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Knoten im Cluster.

- Sie müssen das SnapCenter Plug-in für Microsoft Windows manuell auswählen.

["JAVA für Windows herunterladen"](#)

Linux- und AIX-Hosts



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

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

Wenn Sie Windows Server 2019 oder Windows Server 2016 für den SnapCenter Server-Host verwenden, müssen Sie Java 11 installieren. Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den Anforderungen.

["Laden Sie JAVA für Linux herunter"](#)

["Laden Sie JAVA für AIX herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Sie müssen Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu gewähren. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.



Stellen Sie sicher, dass Sie Sudo Version 1.8.7 oder höher verwenden.

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

LINUX_USER ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei **sc_unix_plugins_checksum.txt** abrufen, die sich hier befindet:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt*, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt*, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

AIX-Hostanforderungen

Sie sollten sicherstellen, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter Plug-Ins-Paket für AIX installieren.



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.



Das SnapCenter -Plug-in für UNIX, das Teil des SnapCenter Plug-in-Pakets für AIX ist, unterstützt keine gleichzeitigen Volume-Gruppen.

Artikel	Anforderungen
Betriebssysteme	AIX 7.1 oder höher
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	4 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	2 GB Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Artikel	Anforderungen
Erforderliche Softwarepakete	Java 11 IBM Java Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#) .

Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host

SnapCenter 4.4 und höher ermöglicht es einem Nicht-Root-Benutzer, das SnapCenter Plug-ins-Paket für AIX zu installieren und den Plug-in-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

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

Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall`

- /benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/bin/spl

Schritte

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

```

Cmd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei /etc/sudoers hinzufügen: „/<crs_home>/bin/olsnodes“

Sie können den Wert von *crs_home* aus der Datei */etc/oracle/olr.loc* abrufen.

AIX_USER ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei *sc_unix_plugins_checksum.txt* abrufen, die sich hier befindet:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt*, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt*, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems

vertraut sein.

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	5 GB  Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux und AIX

Sie sollten sicherstellen, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter Plug-Ins-Paket für Linux oder AIX installieren.



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

Artikel	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	2 GB  Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java oder OpenJDK Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#)

Einrichten von Anmeldeinformationen für von NetApp unterstützte Plug-Ins

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Datenbanken oder Windows-Dateisystemen erstellen.

Bevor Sie beginnen

- Linux- oder AIX-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux- oder AIX-Hosts einrichten.

Sie müssen die Anmeldeinformationen für den Root-Benutzer oder für einen Nicht-Root-Benutzer mit Sudo-Berechtigungen einrichten, um den Plug-In-Prozess zu installieren und zu starten.

Best Practice: Obwohl Sie Anmeldeinformationen für Linux erstellen dürfen, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs 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 Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

- Von NetApp unterstützte Plug-In-Anwendungen

Das Plug-In verwendet die Anmeldeinformationen, die beim Hinzufügen einer Ressource ausgewählt oder erstellt werden. Wenn für eine Ressource während Datenschutzvorgängen keine Anmeldeinformationen erforderlich sind, können Sie die Anmeldeinformationen auf **Keine** festlegen.

Informationen zu diesem Vorgang

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite **Anmeldeinformationen** die zum Konfigurieren der Anmeldeinformationen erforderlichen Informationen an:

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.

Für dieses Feld...	Machen Sie Folgendes...
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 beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind: ◦ <i>NetBIOS\Benutzername</i> ◦ <i>Domänen-FQDN\Benutzername</i> • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i>
Passwort	Geben Sie das zur Authentifizierung verwendete Passwort ein.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, den Sie verwenden möchten.
Verwenden Sie Sudo-Berechtigungen	Aktivieren Sie das Kontrollkästchen Sudo-Berechtigungen verwenden, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.  Gilt nur für Linux- und AIX-Benutzer.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne 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-Domänencontroller aus: Add-KDSRootKey -Effectivelmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
 - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

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

Zum 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.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
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.

- Starten Sie Ihren Host neu.
 - Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
 - Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
- Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
 - 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 Dienstanmeldekonto verwendet.

Installieren Sie die von NetApp unterstützten Plug-Ins

Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu 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.

Bevor Sie beginnen

- Sie sollten ein Benutzer sein, dem eine Rolle zugewiesen ist, die über die Berechtigungen zum Installieren und Deinstallieren von Plug-Ins verfügt, beispielsweise die SnapCenter Administratorrolle.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

"Konfigurieren Sie ein gruppenverwaltetes Dienstkonto auf Windows Server 2016 oder höher für benutzerdefinierte Anwendungen"

- Für den Windows-Host müssen Sie sicherstellen, dass Sie das SnapCenter -Plug-in für Windows auswählen.

Informationen zu diesem Vorgang

- 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 Knoten des Clusters installiert.

Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Hosttyp	Wählen Sie den Hosttyp aus: • Windows • Linux • AIX  Die von NetApp unterstützten Plug-Ins können in Windows-, Linux- und AIX-Umgebungen verwendet werden.  Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

Für dieses Feld...	Machen Sie Folgendes...
Hostname	Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben. In Windows-Umgebungen wird die IP-Adresse für nicht vertrauenswürdige Domänenhosts nur unterstützt, wenn sie in den FQDN aufgelöst wird. Sie können die IP-Adressen oder den FQDN eines eigenständigen Hosts eingeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.
Anmeldeinformationen	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remotehost verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.  Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

5. Wählen Sie im Abschnitt **Zu installierende Plug-ins auswählen** die zu installierenden Plug-ins aus.

Sie können die folgenden Plug-Ins aus der Liste installieren:

- MongoDB
- ORASCPM (angezeigt als Oracle-Anwendungen)
- SAP ASE
- SAP MaxDB
- Storage

6. (Optional) Wählen Sie **Weitere Optionen**, um die anderen Plug-Ins zu installieren.

Für dieses Feld...	Machen Sie Folgendes...
Hafen	Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an. Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.  Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Die von NetApp unterstützten Plug-Ins können entweder auf einem Windows- oder einem Linux-System installiert werden. - Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter. Optional können Sie den Pfad anpassen. - Für SnapCenter Plug-ins Package für Linux und SnapCenter Plug-ins Package für AIX ist der Standardpfad /opt/NetApp/snapcenter . Optional können Sie den Pfad anpassen.
Vorinstallationsprüfungen überspringen	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.

Für dieses Feld...	Machen Sie Folgendes...
Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen	Aktivieren Sie für Windows-Hosts dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.  Geben Sie den gMSA-Namen im folgenden Format an: Domänenname\Kontoname\$.  gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.

7. Wählen Sie **Senden**.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt.

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



Wenn Sie in einem HA-Setup SnapManager.Web.UI.dll.config aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren und den SnapCenter App Pool neu starten.

Der Windows-Standardpfad ist C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

Der Standardpfad für Linux ist

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und wählen Sie dann **Bestätigen und senden**.



Die Überprüfung des Fingerabdrucks ist obligatorisch, auch wenn derselbe Host zuvor zu SnapCenter hinzugefügt und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

Die installationsspezifischen Protokolldateien befinden sich unter /custom_location/snapcenter/Protokolle.

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

Sie können die SnapCenter -Plug-in-Pakete für Linux, Windows oder AIX mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

Bevor Sie beginnen

Der Benutzer, der einen Host hinzufügt, sollte über Administratorrechte für den Host verfügen.



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-In auf mehreren Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Sie können die Option -skippercheck verwenden, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

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

Installieren Sie die von NetApp unterstützten Plug-Ins auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle

Sie sollten die von NetApp unterstützten Plug-Ins mithilfe der SnapCenter -Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie die von NetApp unterstützten Plug-Ins entweder im Konsolenmodus oder im Hintergrundmodus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Schritte

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

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

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das 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 SMCore HTTPS-Kommunikationsport 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 Sie das SnapCenter Plug-Ins-Paket für Linux installieren möchten.
- _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.

Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

5. Melden Sie sich bei SnapCenter an und laden Sie das von NetApp unterstützte Plug-In über die Benutzeroberfläche oder mithilfe von PowerShell-Cmdlets hoch.

Sie können das von NetApp unterstützte Plug-In von der Benutzeroberfläche hochladen, indem Sie auf ["Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren"](#) Abschnitt.

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

["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Überwachen Sie den Status der Installation von NetApp unterstützten Plug-Ins

Sie können den Fortschritt der Installation des SnapCenter -Plug-In-Pakets auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Installationsfortschritt überprüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

-  Im Gange
-  Erfolgreich abgeschlossen
-  Fehlgeschlagen
-  Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
-  In der Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
3. Um auf der Seite **Jobs** die Liste so zu filtern, dass nur Plug-In-Installationsvorgänge aufgeführt werden, gehen Sie wie folgt vor:
 - a. Klicken Sie auf **Filter**.
 - b. Optional: Geben Sie das Start- und Enddatum an.
 - c. Wählen Sie im Dropdown-Menü „Typ“ die Option „Plug-in-Installation“ aus.
 - d. Wählen Sie im Dropdown-Menü „Status“ den Installationsstatus aus.
 - e. Klicken Sie auf **Übernehmen**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

CA-Zertifikat konfigurieren

CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



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

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

Schritte

1. Gehen Sie zur Microsoft-Verwaltungskontrolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.

2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

In diesem Assistentenfenster ...	Gehen Sie wie folgt vor...
Privaten Schlüssel importieren	Wählen Sie die Option Ja , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf Weiter .
Importdateiformat	Nehmen Sie keine Änderungen vor; klicken Sie auf Weiter .
Sicherheit	Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf Weiter .
Abschließen des Zertifikatimport-Assistenten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf Fertig , um den Import zu starten.



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

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

Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

Schritte

1. Führen Sie auf der GUI Folgendes aus:
 - 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 **Fingerabdruck**.
 - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
 - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

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

2. Führen Sie in PowerShell Folgendes aus:

- a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-ChildItem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

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 aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

Schritte

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

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

Beispiel:

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

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Beispiel:

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

Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten Plug-In-Dienst auf dem Linux-Host

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

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

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

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

Schritte

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

Dies ist der Wert, der dem Schlüssel „KEYSTORE_PASS“ entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```

. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

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

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE_PASS in der Datei *agent.properties*.

3. Starten Sie den Dienst nach der Änderung des Kennworts neu.



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

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

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

Schritte

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

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

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

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



Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

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

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

Schritte

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

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

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem 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. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

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

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

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

Aktualisieren Sie diesen Wert anhand des Schlüssels `SCC_CERTIFICATE_ALIAS`.

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

Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

Informationen zu diesem Vorgang

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

Schritte

1. Sie können das Standardverzeichnis in der Datei `agent.properties` anhand des Schlüssels `CRL_PATH` ändern und aktualisieren.

Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen. Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten Plug-In-Dienst auf dem Windows-Host

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

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

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

Schritte

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

Es handelt sich um den Wert, der dem Schlüssel `KEYSTORE_PASS` entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

```
C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

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

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE_PASS in der Datei *agent.properties*.

4. Starten Sie den Dienst nach der Änderung des Kennworts neu.



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

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

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

Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

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

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

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



Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

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

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

Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

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

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem 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. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

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

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

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

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC_CERTIFICATE_ALIAS.

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

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

Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe ["So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat"](#).
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist 'C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\crl'.

Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* anhand des Schlüssels CRL_PATH ändern und aktualisieren.
2. Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen.

Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

CA-Zertifikate für Plug-Ins aktivieren

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter -Server und den entsprechenden Plug-In-Hosts bereitstellen. Sie sollten die CA-Zertifikatvalidierung für die Plug-Ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „*Set-SmCertificateSettings*“ aktivieren oder deaktivieren.
- Den Zertifikatsstatus der Plug-ins können Sie sich mit *Get-SmCertificateSettings* anzeigen lassen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie einzelne oder mehrere Plug-In-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung aktivieren**.

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss 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 ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.

Bereiten Sie sich auf den Datenschutz vor

Voraussetzungen für die Verwendung der von NetApp unterstützten Plug-Ins

Bevor Sie die von SnapCenter NetApp unterstützten Plug-Ins verwenden, muss der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich beim SnapCenter -Server an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen und gegebenenfalls Anmeldeinformationen erstellen.
- Fügen Sie Hosts hinzu und installieren und laden Sie die Plug-Ins hoch.
- Installieren Sie gegebenenfalls Java 11 auf dem Plug-In-Host.
- Wenn Sie über mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration verfügen, können Sie mithilfe der SnapCenter -CLI auf dem Datenbankhost Folgendes ausführen:
 - Standardmäßig werden alle IP-Adressen des Datenbankhosts zur NFS-Speicherexportrichtlinie 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 Sie mehrere Datenpfade (LIFs) in SVMs haben, wählt SnapCenter den entsprechenden Datenpfad (LIF) zum Mounten des geklonten NFS-Volumes aus. Wenn Sie jedoch einen bestimmten

Datenpfad (LIF) angeben möchten, müssen Sie die CLI „Set-SvmPreferredDataPath“ ausführen. Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "[SnapCenter Software-Befehlsreferenzhandbuch](#)".

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.
- 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 von NetApp unterstützte Plug-Ins reserviert werden.

So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von NetApp unterstützten Plug-In-Ressourcen verwendet

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind normalerweise Datenbanken, Windows-Dateisysteme 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 Zeitplan aus, den Sie für die Ressourcengruppe angeben.

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

- Die Richtlinien legen die Sicherungshäufigkeit, die Aufbewahrung von Kopien, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

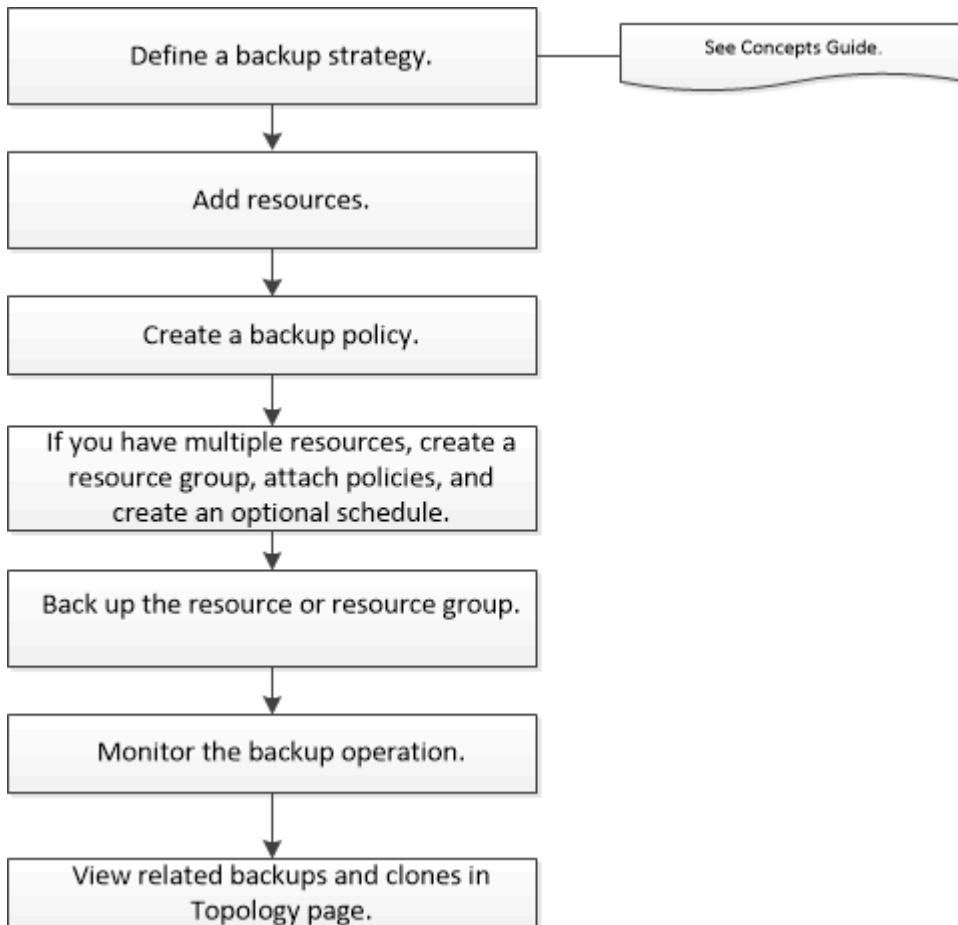
Stellen Sie sich eine Ressourcengruppe so vor, als würde sie definieren, *was* Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als würde sie definieren, *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme auf dem Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine dateibasierte Sicherung durchgeführt wird, und einen anderen Zeitplan, der stündlich eine Snapshot-basierte Sicherung durchführt.

Sichern Sie von NetApp unterstützte Plug-In-Ressourcen

Sichern Sie von NetApp unterstützte Plug-In-Ressourcen

Der Sicherungsworkflow umfasst die Planung, die Identifizierung der Ressourcen für die Sicherung, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

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



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#)

Ressourcen zu NetApp unterstützten Plug-ins hinzufügen

Sie müssen die Ressourcen hinzufügen, die Sie sichern oder klonen möchten. Abhängig von Ihrer Umgebung können die Ressourcen entweder Datenbankinstanzen oder Sammlungen sein, die Sie sichern oder klonen möchten.

Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Sie müssen die Plug-Ins auf den SnapCenter -Server hochgeladen haben.

Schritte

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

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie den Namen der Ressource ein.
Hostname	Wählen Sie den Host aus.
Typ	Wählen Sie den Typ aus. Der Typ wird gemäß der Plug-In-Beschreibungsdatei vom Benutzer definiert. Zum Beispiel Datenbank und Instanz. Falls der ausgewählte Typ ein übergeordnetes Element hat, geben Sie die Details des übergeordneten Elements ein. Wenn der Typ beispielsweise „Datenbank“ und das übergeordnete Element „Instanz“ ist, geben Sie die Details der Instanz ein.
Anmeldeinformationsname	Wählen Sie Anmeldeinformationen aus oder erstellen Sie neue Anmeldeinformationen.
Bergpfade	Geben Sie die Mount-Pfade ein, in denen die Ressource gemountet ist. Dies gilt nur für einen Windows-Host.

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ ein Speichersystem und ein oder mehrere Volumes, LUNs und Qtrees aus und wählen Sie dann **Speichern**.

Optional: Wählen Sie die  Symbol, um weitere Volumes, LUNs und Qtrees aus anderen Speichersystemen hinzuzufügen.



Von NetApp unterstützte Plug-Ins unterstützen keine automatische Erkennung der Ressourcen. Auch die Speicherdetails physischer und virtueller Umgebungen werden nicht automatisch erkannt. Sie müssen beim Erstellen der Ressourcen die Speicherinformationen für physische und virtuelle Umgebungen angeben.

5. Geben Sie auf der Seite „Ressourceneinstellungen“ benutzerdefinierte Schlüssel-Wert-Paare für die Ressource an.



Stellen Sie sicher, dass der Name des benutzerdefinierten Schlüssels in Großbuchstaben geschrieben ist.

Resource settings

Name	Value
HOST	localhost
PORT	3306
MASTER_SLAVE	NO

Die jeweiligen Plug-In-Parameter finden Sie unter "[Parameter zum Konfigurieren der Ressource](#)"

6. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Ergebnis

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



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

Nach Abschluss

Wenn Sie anderen Benutzern Zugriff auf die Assets gewähren möchten, muss der SnapCenter Administrator diesen Benutzern Assets zuweisen. Dadurch 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 von NetApp unterstützten Plug-In-Ressourcen Sicherungen zugeordnet sind, können die folgenden Felder nicht geändert werden: Ressourcenname, Ressourcentyp und Hostname.

Parameter zum Konfigurieren der Ressource

Wenn Sie die Plug-Ins manuell hinzufügen, können Sie die Ressource auf der Seite „Ressourceneinstellungen“ mit den folgenden Parametern konfigurieren.

Plug-in für MongoDB

Ressourceneinstellungen:

- MONGODB_APP_SERVER=(für Ressourcentyp als Sharded Cluster) oder MONGODB_REPLICASET_SERVER=(für Ressourcentyp als Replikatsatz)
- OPLOG_PATH=(Optionaler Parameter, falls er von MongoDB.propertiesfile bereitgestellt wird)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN für LDAP-Authentifizierung und Keine für andere)

Sie müssen die folgenden Parameter in der Datei MongoDB.properties angeben:

- DISABLE_STARTING_STOPPING_SERVICES=
 - N, wenn die Start-/Stopp-Dienste vom Plug-In ausgeführt werden.
 - Y, wenn Start-/**Stopp-Dienste vom Benutzer ausgeführt werden.
 - Optionaler Parameter, da der Standardwert auf N gesetzt ist.
- OPLOG_PATH_ = (Optionaler Parameter, falls er bereits als benutzerdefiniertes Schlüssel-Wert-Paar in SnapCenter bereitgestellt wird).

Plug-in für MaxDB

Ressourceneinstellungen:

- XUSER_ENABLE (Y|N) aktiviert oder deaktiviert die Verwendung eines Xusers für MaxDB, sodass für den Datenbankbenutzer kein Kennwort erforderlich ist.
- HANDLE_LOGWRITER (Y|N) führt die Operationen „Logwriter anhalten“ (N) oder „Logwriter fortsetzen“ (Y) aus.
- DBMCLICMD (path_to_dbmcli_cmd) gibt den Pfad zum MaxDB-dbmcli-Befehl an. Wenn nicht festgelegt, wird dbmcli im Suchpfad verwendet.



In einer Windows-Umgebung muss der Pfad in doppelte Anführungszeichen ("...") eingeschlossen sein.

- SQLCLICMD (path_to_sqlcli_cmd) gibt den Pfad zum MaxDB-SQLCLI-Befehl an. Wenn der Pfad nicht festgelegt ist, wird sqlcli auf den Suchpfad angewendet.
- MAXDB_UPDATE_HIST_LOG (Y|N) weist das MaxDB-Sicherungsprogramm an, ob es das MaxDB-Verlaufsprotokoll aktualisieren soll.
- MAXDB_CHECK_SNAPSHOT_DIR: Beispiel: SID1:Verzeichnis[,Verzeichnis...]; [SID2:Verzeichnis[,Verzeichnis...]] prüft, ob ein Snap Creator-Snapshot-Kopiervorgang erfolgreich ist, und stellt sicher, dass der Snapshot erstellt wird.

Dies gilt nur für NFS. Das Verzeichnis muss auf den Speicherort verweisen, der das Verzeichnis .snapshot enthält. Mehrere Verzeichnisse können in einer durch Kommas getrennten Liste enthalten sein.

In MaxDB 7.8 und späteren Versionen wird die Datenbanksicherungsanforderung im Sicherungsverlauf als „Fehlgeschlagen“ markiert.

- **MAXDB_BACKUP_TEMPLATES:** Gibt eine Sicherungsvorlage für jede Datenbank an.

Die Vorlage muss vorhanden sein und ein externer Typ einer Sicherungsvorlage sein. Um die Snapshot-Integration für MaxDB 7.8 und höher zu aktivieren, müssen Sie über die MaxDB-Hintergrundserverfunktionalität und eine bereits konfigurierte MaxDB-Sicherungsvorlage des Typs **EXTERNAL** verfügen.

- **MAXDB_BG_SERVER_PREFIX:** Gibt das Präfix für den Hintergrundservernamen an.

Wenn der Parameter **MAXDB_BACKUP_TEMPLATES** festgelegt ist, müssen Sie auch den Parameter **MAXDB_BG_SERVER_PREFIX** festlegen. Wenn Sie das Präfix nicht festlegen, wird der Standardwert **na_bg_** verwendet.

Plug-in für SAP ASE

Ressourceneinstellungen:

- **SYBASE_SERVER** (*data_server_name*) gibt den Namen des Sybase-Datenservers an (Option **-S** im **isql**-Befehl). Zum Beispiel **p_test**.
- **SYBASE_DATABASES_EXCLUDE** (*db_name*) ermöglicht das Ausschließen von Datenbanken, wenn die Konstruktion „ALL“ verwendet wird.

Sie können mehrere Datenbanken angeben, indem Sie eine durch Semikolon getrennte Liste verwenden. Beispiel: **pubs2;test_db1**.

- **SYBASE_USER:** *user_name* gibt den Betriebssystembenutzer an, der den **isql**-Befehl ausführen kann.

Erforderlich für UNIX. Dieser Parameter ist erforderlich, wenn der Benutzer, der die Start- und Stoppbefehle des Snap Creator Agent ausführt (normalerweise der Root-Benutzer), und der Benutzer, der den **isql**-Befehl ausführt, unterschiedlich sind.

- **SYBASE_TRAN_DUMP** *db_name:directory_path* ermöglicht Ihnen, nach dem Erstellen eines Snapshots einen Sybase-Transaktionsdump durchzuführen. Beispiel: **pubs2:/sybasedumps/pubs2**

Sie müssen jede Datenbank angeben, die einen Transaktionsdump erfordert.

- **SYBASE_TRAN_DUMP_COMPRESS** (Y|N) aktiviert oder deaktiviert die native Sybase-Transaktionsdump-Komprimierung.
- **SYBASE_ISQL_CMD** (z. B. **/opt/sybase/OCS-15_0/bin/isql**) definiert den Pfad zum **isql**-Befehl.
- Mit **SYBASE_EXCLUDE_TEMPDB** (Y|N) können Sie vom Benutzer erstellte temporäre Datenbanken automatisch ausschließen.

Plug-in für Oracle-Anwendungen (ORASCPM)

Ressourceneinstellungen:

- **SQLPLUS_CMD** gibt den Pfad zu SQLplus an.
- **ORACLE_DATABASES** listet die zu sichernden Oracle-Datenbanken und den entsprechenden Benutzer (Datenbank:Benutzer) auf.
- **CNTL_FILE_BACKUP_DIR** gibt das Verzeichnis für die Sicherung der Steuerdatei an.
- **ORA_TEMP** gibt das Verzeichnis für temporäre Dateien an.

- ORACLE_HOME gibt das Verzeichnis an, in dem die Oracle-Software installiert ist.
- ARCHIVE_LOG_ONLY gibt an, ob die Archivprotokolle gesichert werden sollen oder nicht.
- ORACLE_BACKUPMODE gibt an, ob eine Online- oder Offline-Sicherung durchgeführt werden soll.
- ORACLE_EXPORT_PARAMETERS gibt an, ob die oben definierten Umgebungsvariablen während der Ausführung von `/bin/su <Benutzer, der sqlplus ausführt> -c sqlplus /nolog <cmd>` erneut exportiert werden sollen. Dies ist normalerweise der Fall, wenn der Benutzer, der sqlplus ausführt, nicht alle Umgebungsvariablen festgelegt hat, die für die Verbindung mit der Datenbank mithilfe von `connect / as sysdba` erforderlich sind.

Erstellen Sie Richtlinien für von NetApp unterstützte Plug-In-Ressourcen

Bevor Sie SnapCenter zum Sichern von Plug-in-spezifischen Ressourcen verwenden, die von NetApp unterstützt werden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten.

Bevor Sie beginnen

- Sie sollten Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für von NetApp unterstützte Plug-Ins.

- Sie sollten sich auf den Datenschutz vorbereitet haben.

Zur Vorbereitung des Datenschutzes gehören Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Ressourcen.

- Die virtuellen Speichermaschinen (SVMs) sollten Ihnen für Spiegelungs- oder Tresorvorgänge zugewiesen werden.

Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

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

Informationen zu diesem Vorgang

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren. Darüber hinaus können Sie Replikations-, Skript- und Anwendungseinstellungen angeben.
- Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.
- SnapLock
 - Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.
 - Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.
 - Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.



Die primären SnapLock -Einstellungen werden in der SnapCenter -Sicherungsrichtlinie verwaltet und die sekundären SnapLock -Einstellungen werden von ONTAP verwaltet.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
 - a. Wählen Sie den Speichertyp aus.
 - b. Geben Sie im Abschnitt „Benutzerdefinierte Sicherungseinstellungen“ alle spezifischen Sicherungseinstellungen an, die im Schlüssel-Wert-Format an das Plug-In übergeben werden müssen.

Sie können mehrere Schlüsselwerte angeben, die an das Plug-In übergeben werden sollen.
6. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:
 - a. Geben Sie den Zeitplantyp an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



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

- a. Geben Sie im Abschnitt „Snapshot-Einstellungen“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

Wenn Sie wollen...	Dann...
Behalten Sie eine bestimmte Anzahl von Snapshots	Wählen Sie Zu behaltende Kopien und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.  Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.  Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden ONTAP Version unterstützt wird.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie Kopien aufbewahren für und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.
Sperrzeitraum für Snapshot-Kopien	Wählen Sie Sperrzeitraum für Snapshot-Kopien und geben Sie Tage, Monate oder Jahre an. Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.

b. Wählen Sie eine Richtlinienbezeichnung aus.



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

7. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation). Wenn die Schutzbeziehung in ONTAP vom Typ „Mirror und Vault“ ist und Sie nur diese Option auswählen, wird der auf dem primären Server erstellte Snapshot nicht zum Ziel übertragen, sondern im Ziel aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird die folgende Fehlermeldung angezeigt: „Der sekundäre Speicherort ist für die ausgewählte gewölbte/gespiegelte Sicherung nicht verfügbar.“ Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche Aktualisieren auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden. Sehen "Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“" .

Für dieses Feld...	Machen Sie Folgendes...
Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups). Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche Aktualisieren auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden. Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche Aktualisieren auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird. Weitere Informationen zu SnapLock Vault finden Sie unter „Snapshots an WORM auf einem Tresorziel übermitteln“. Sehen "Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“" .
Fehler bei der Wiederholungsanzahl	Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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

Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Damit können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.

2. Wählen Sie auf der Seite „Ressourcen“ die Option „Neue Ressourcengruppe“ aus.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Hinweis: Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten. Beispiel: <i>customtext_resource</i> <i>group_policy_hostname</i> oder <i>resource</i> <i>group_hostname</i>. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Optional: Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und den Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

Dies hilft, Informationen auf dem Bildschirm zu filtern.

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

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

Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

Für dieses Feld...	Machen Sie Folgendes...
Planen Sie Zeit ein, um auf den Abschluss des Consistency Group Snapshot-Vorgangs zu warten	Wählen Sie „Dringend“, „Mittel“ oder „Entspannt“ aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.

Für dieses Feld...	Machen Sie Folgendes...
WAFL -Synchronisierung deaktivieren	Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.

1 Name 2 Resources 3 Application Settings 4 Policies 5 Notification 6 Summary

Backups

☒ Enable consistency group backup

Afford time to wait for Consistency Group Snapshot operation to complete ⓘ

☒ Urgent

☐ Medium

☐ Relaxed

☐ Disable WAFL Sync

Scripts ⓘ

Custom Configurations ⓘ

Snapshot Copy Tool ⓘ

- Wählen Sie den Pfeil „Skripts“ aus und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die Vorbefehle eingeben, die im Falle eines Fehlers vor dem Beenden ausgeführt werden sollen.
- Wählen Sie den Pfeil „Benutzerdefinierte Konfigurationen“ aus und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

Parameter	Einstellung	Beschreibung
ARCHIV_LOG_ENABLE	(J/N)	Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle.
ARCHIV_LOG_RETENTION	Anzahl_der_Tage	Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein.
ARCHIVE_LOG_DIR	change_info_directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Erweiterungslänge der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.16151855 1942 9 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(J/N)	Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.

c. Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Falls Sie es wollen...	Dann...
SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie * SnapCenter mit Dateisystemkonsistenz*. Diese Option ist für das SnapCenter -Plug-in für die SAP HANA-Datenbank nicht anwendbar.
SnapCenter zum Erstellen eines Snapshots auf Speicherebene	Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.
Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshots zu erstellen.	Wählen Sie Andere aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen.

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

a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.



Sie können auch eine Richtlinie erstellen, indem Sie * auswählen. *.

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

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

- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen*“ den Zeitplan und wählen Sie „OK“ aus.

Dabei ist „Richtliniennamen“ der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet. Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

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

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

9. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Ressourcen auf ASA R2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA R2-Systemen befinden. Sie können den sekundären Schutz auch beim Erstellen der Ressourcengruppe bereitstellen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

- Der sekundäre Schutz ist nur verfügbar, wenn dem angemeldeten Benutzer die Rolle zugewiesen ist, für die die Funktion **SecondaryProtection** aktiviert ist.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nachdem die primäre und sekundäre Konsistenzgruppe erstellt wurden, wird der Wartungsmodus der Ressourcengruppe beendet.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

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



Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

- b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie

später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

- c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

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



Sie sollten genau dasselbe Ziel verwenden, das in der Anwendung festgelegt wurde, gegebenenfalls einschließlich Präfix.

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



Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

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



Sie können eine Richtlinie auch erstellen, indem Sie auf  .

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

- b. Klicken  in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Wenn der sekundäre Schutz für die von Ihnen ausgewählte Richtlinie aktiviert ist, wird die Seite „Sekundärer Schutz“ angezeigt und Sie müssen die folgenden Schritte ausführen:
 - a. Wählen Sie den Typ der Replikationsrichtlinie aus.



Die synchrone Replikationsrichtlinie wird nicht unterstützt.

- b. Geben Sie das Konsistenzgruppensuffix an, das Sie verwenden möchten.
- c. Wählen Sie aus den Dropdown-Menüs „Zielcluster“ und „Ziel-SVM“ den Peering-Cluster und die SVM aus, die Sie verwenden möchten.



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



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

1. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
 - a. Klicken Sie auf **Locators laden**, um die SnapMirror oder SnapVault -Volumes zu laden und die Überprüfung auf dem sekundären Speicher durchzuführen.
 - b. Klicken  in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
 - c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtliniennamen) die folgenden Aktionen aus:

Wenn Sie wollen...	Machen Sie Folgendes...
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie Überprüfung nach Sicherung ausführen .
Planen Sie eine Überprüfung	Wählen Sie Geplante Überprüfung ausführen und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

- d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.
- e. Klicken Sie auf **OK**.

Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.



Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtServer“ angegeben haben.

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

Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Ausführen von Datenschutzvorgängen verwenden.

Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Verwaltungs-LIF-IP-Adresse haben.

Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets `Open-SmConnection`.

Dieses Beispiel öffnet eine PowerShell-Sitzung:

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

2. Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

3. Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

In diesem Beispiel wird eine neue Anmeldeinformation mit dem Namen „FinanceAdmin“ mit Windows-Anmeldeinformationen erstellt:

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Sichern Sie einzelne von NetApp unterstützte Plug-In-Ressourcen

Wenn eine einzelne von NetApp unterstützte Plug-In-Ressource nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern. Sie können die Ressource bei Bedarf sichern. Wenn für die Ressource eine Richtlinie festgelegt und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

SnapCenter -Benutzeroberfläche

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 **Anzeigen** basierend auf dem Ressourcentyp.

Klicken  und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auf , um den Filterbereich zu schließen.

3. Klicken Sie auf die Ressource, die Sie sichern möchten.
4. Wenn Sie auf der Ressourcenseite einen benutzerdefinierten Namen verwenden möchten, aktivieren Sie das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** und geben Sie dann ein benutzerdefiniertes Namensformat für den Snapshot-Namen ein.

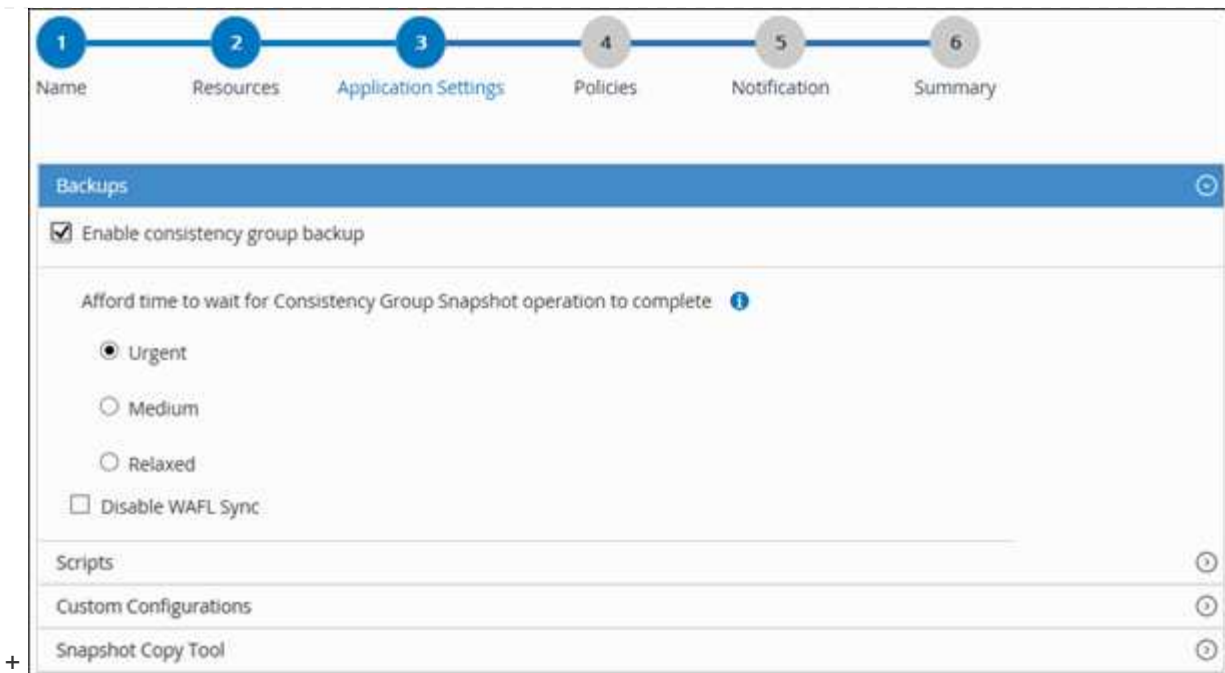
Beispiel: *customtext_policy_hostname* oder *resource_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

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

Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

Für dieses Feld...	Machen Sie Folgendes...
Planen Sie Zeit ein, um auf den Abschluss des Consistency Group Snapshot-Vorgangs zu warten	Wählen Sie „Dringend“, „Mittel“ oder „Entspannt“ aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.
WAFL -Synchronisierung deaktivieren	Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.



- a. Klicken Sie auf den Pfeil **Skripts**, um Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen. Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen.

Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

- b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Falls Sie es wollen...	Dann...
SnapCenter zum Erstellen eines Snapshots auf Speicherebene	Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.
SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.
So geben Sie den Befehl zum Erstellen eines Snapshots ein	Wählen Sie Andere und geben Sie dann den Befehl zum Erstellen eines Snapshots ein.

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

- a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.



Sie können eine Richtlinie auch erstellen, indem Sie auf  .

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

- b.  in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamenname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers 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**.

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Klicken Sie auf **Jetzt sichern**.

10. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

- b. Klicken Sie auf **Sichern**.

11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

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

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Fügen Sie Ressourcen mithilfe des Cmdlets Add-SmResources hinzu.

In diesem Beispiel werden Ressourcen hinzugefügt:

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QTREENAME"="qtree
Voll1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

In diesem Beispiel wird eine neue Sicherungsrichtlinie erstellt:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

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

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

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

```
Get-SmBackupReport -JobId 149
```

```
BackedUpObjects      : {QTREE2, QTREE}
FailedObjects        : {}
IsScheduled           : False
HasMetadata           : False
SmBackupId            : 1
SmJobId               : 149
StartDateTime         : 1/15/2024 1:35:17 AM
EndDateTime          : 1/15/2024 1:36:19 AM
Duration              : 00:01:02.4265750
CreatedDateTime       : 1/15/2024 1:35:51 AM
Status                : Completed
ProtectionGroupName   :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId   : 1
PolicyName            : test2
SmPolicyId            : 4
BackupName            :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus    : NotApplicable
VerificationStatuses  :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses    :
ReportDataCreatedDateTime :
PluginCode            : SCC
PluginName            : DummyPlugin
PluginDisplayName     : DummyPlugin
JobTypeId             :
JobHost               : scc55.sscore.test.com
```

Sichern Sie Ressourcengruppen von NetApp unterstützten Plug-In-Ressourcen

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror -Beziehung zum sekundären Speicher sichern möchten, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn

Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „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 „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf  und wählen Sie das Tag aus. Sie können dann auf , 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 „Sichern“ die folgenden Schritte aus:
 - a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

- b. Klicken Sie auf **Sichern**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.
 - In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung 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 for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl. Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei /opt/netapp/init_scripts/scvservice. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`.

Überwachen Sie die Sicherungsvorgänge für NetApp unterstützte Plug-In-Ressourcen

Sie können den Fortschritt verschiedener Sicherungsvorgänge mithilfe der SnapCenterJobs-Seite überwachen. Möglicherweise möchten Sie den Fortschritt überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

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

-  Im Gange
-  Erfolgreich abgeschlossen
-  Fehlgeschlagen

-  Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
-  In der Warteschlange
-  Abgesagt

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  um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
 - b. Geben Sie das Start- und Enddatum an.
 - c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
 - d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
 - e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.



Obwohl der Status des Sicherungsauftrags angezeigt wird  Wenn Sie auf die Auftragsdetails klicken, sehen Sie möglicherweise, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt werden oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

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

Abbrechen von Sicherungsvorgängen für von NetApp unterstützte Plug-Ins

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzuberechnen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der...	Aktion
Monitorseite	- Klicken Sie im linken Navigationsbereich auf Monitor > Jobs. - Wählen Sie den Vorgang aus und klicken Sie dann auf Auftrag abbrechen.
Aktivitätsbereich	- Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. - Wählen Sie den Vorgang aus. - Klicken Sie auf der Seite „Auftragsdetails“ auf Auftrag abbrechen.

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzuzeigen. Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

Informationen zu diesem Vorgang

Sie können die folgenden Symbole in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die Sicherungen und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).

-  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 Speicher gespiegelt werden.



Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

•



zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.

Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups. Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.



Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

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 die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Ressourcendetailansicht oder aus der Ressourcengruppendetailansicht aus.

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

4. Überprüfen Sie die Karte „Zusammenfassung“, um eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen und Klone anzuzeigen.

Im Abschnitt „Zusammenfassungskarte“ wird die Gesamtzahl der Sicherungen und Klone angezeigt.

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

Wenn eine SnapLock -fähige Sicherung durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock aktualisiert. Ein wöchentlicher Zeitplan aktualisiert auch die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock .

Wenn die Anwendungsressource auf mehrere Volumes verteilt ist, entspricht die SnapLock -Ablaufzeit für die Sicherung der längsten SnapLock -Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock -Ablaufzeit wird von ONTAP abgerufen.

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

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

Die Details der Backups und Klone werden in einem Tabellenformat angezeigt.

6. Wählen Sie die Sicherung aus der Tabelle aus und klicken Sie dann auf die Datenschutzsymbole, um Wiederherstellungs-, Klon-, Umbenennungs- und Löschvorgänge durchzuführen.



Sie können Sicherungen, die sich auf dem sekundären Speichersystem befinden, weder umbenennen noch löschen.



Sie können die Sicherungen, 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.

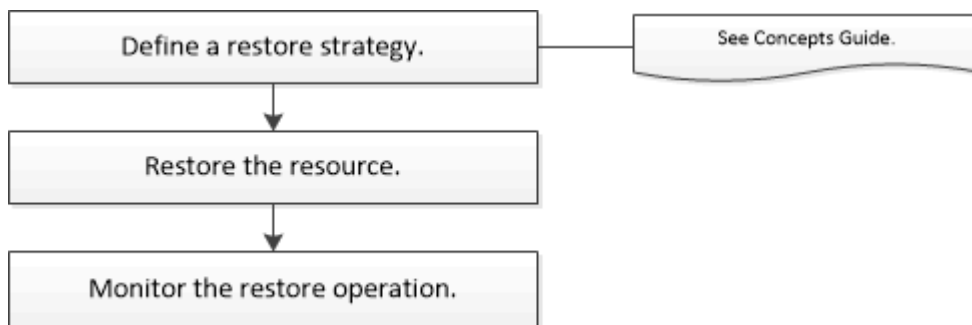
Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen

Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

Informationen zu diesem Vorgang

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



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Informationen zu PowerShell-Cmdlets finden Sie in der Hilfe zu SnapCenter -Cmdlets oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

Wiederherstellen einer Ressourcensicherung

Sie können SnapCenter zum Wiederherstellen von Ressourcen verwenden. Die Möglichkeiten der Wiederherstellungsvorgänge hängen vom verwendeten Plug-In ab.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.

Informationen zu diesem Vorgang

- Der Standardwiederherstellungsvorgang stellt nur Speicherobjekte wieder her. Wiederherstellungsvorgänge auf Anwendungsebene können nur durchgeführt werden, wenn das von NetApp unterstützte Plug-In diese Funktion bietet.

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

SnapCenter -Benutzeroberfläche

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 **Anzeigen** basierend auf dem Ressourcentyp.

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



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte **Gesamtstatus** *Nicht geschützt* angezeigt.

Der Status *Nicht geschützt* 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 und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Kopien verwalten** die Option **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf .



Primary Backup(s)	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ entweder **Vollständige Ressource** oder **Dateiebene** aus.

- a. Wenn Sie **Ressource vervollständigen** ausgewählt haben, wird die Ressourcensicherung wiederhergestellt.

Wenn die Ressource Volumes oder Qtrees als Speicherbedarf enthält, werden neuere Snapshots auf solchen Volumes oder Qtrees gelöscht und können nicht wiederhergestellt werden. Wenn eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

- b. Wenn Sie **Dateiebene** ausgewählt haben, können Sie entweder **Alle** auswählen oder Volumes oder Qtrees auswählen und dann den Pfad zu den ausgewählten Volumes oder Qtrees durch Kommas getrennt eingeben.

- 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. Geben Sie auf der Seite **Pre ops** die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
8. Geben Sie auf der Seite **Post Ops** Mount- und Post Restore-Befehle ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
9. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer.

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

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

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

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

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

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

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

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

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Überwachen Sie die Wiederherstellungsvorgänge für von NetApp unterstützte Plug-In-Ressourcen

Sie können den Fortschritt verschiedener SnapCenter -Wiederherstellungsvorgänge mithilfe der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Fortschritt eines Vorgangs überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Zustände nach der Wiederherstellung beschreiben den Zustand der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsaktionen, die Sie durchführen können.

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

-  Im Gange
-  Erfolgreich abgeschlossen
-  Fehlgeschlagen
-  Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
-  In der Warteschlange
-  Abgesagt

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  um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
 - b. Geben Sie das Start- und Enddatum an.
 - c. Wählen Sie aus der Dropdownliste **Typ** die Option **Wiederherstellen** aus.
 - d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
 - e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie den Wiederherstellungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

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

Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen

Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen

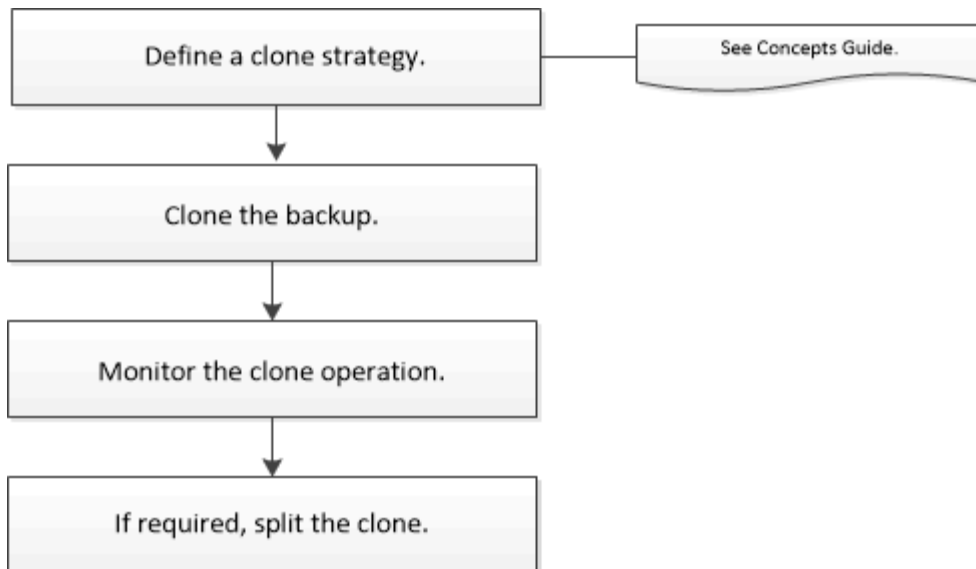
Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Informationen zu diesem Vorgang

Sie können Ressourcensicherungen aus den folgenden Gründen klonen:

- Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
- Für Datenextraktions- und Manipulationstools beim Befüllen von Data Warehouses
- So stellen Sie versehentlich gelöschte oder geänderte Daten wieder her

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

Klonen aus einer Sicherung

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen. Die Möglichkeiten der Klonvorgänge hängen vom verwendeten Plug-In ab.

Bevor Sie beginnen

- Sie müssen die Ressourcen oder Ressourcengruppe gesichert haben.
- Der Standardklonvorgang kloniert nur Speicherobjekte. Klonvorgänge auf Anwendungsebene können nur durchgeführt werden, wenn das von NetApp unterstützte Plug-In diese Funktion bietet.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.

Informationen zu diesem Vorgang

Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

SnapCenter -Benutzeroberfläche

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 **Anzeigen** basierend auf dem Ressourcentyp.

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

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

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

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standorte“ die folgenden Schritte aus:

Für dieses Feld...	Machen Sie Folgendes...
Server klonen	Standardmäßig ist der Quellhost ausgefüllt. Wenn Sie einen anderen Host angeben möchten, wählen Sie den Host aus, auf dem der Klon gemountet und das Plug-In installiert werden soll.
Klonsuffix	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 denselben Host wie die ursprüngliche Ressource klonen, müssen Sie ein Suffix angeben, um die geklonte Ressource von der ursprünglichen Ressource zu unterscheiden. Andernfalls schlägt der Vorgang fehl.

Wenn es sich bei der ausgewählten Ressource um eine LUN handelt und Sie von einer sekundären Sicherung klonen, werden die Zielvolumes aufgelistet. Eine einzelne Quelle kann mehrere Zielvolumes haben.

7. Führen Sie auf der Seite **Einstellungen** Folgendes aus:

Für dieses Feld...	Machen Sie Folgendes...
Name des Initiators	Geben Sie den Host-Initiatornamen ein, der entweder ein IQDN oder ein WWPN ist.
Igroup-Protokoll	Wählen Sie das Igroup-Protokoll.



Die Einstellungsseite wird nur angezeigt, wenn der Speichertyp LUN ist.

- Geben Sie auf der Seite „Skripte“ die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Beispiel:

- Befehl vor dem Klonen: Löschen Sie vorhandene Datenbanken mit demselben Namen
- Befehl nach dem Klonen: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.

Mount-Befehl für ein Volume oder einen Qtree auf einer Linux-Maschine:

```
mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>
```

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

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben.

- Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.
- Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

PowerShell-Cmdlets

Schritte

- Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

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

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

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
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 zu einer angegebenen 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 : {}
HostResourceMapping : {}
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                   : {}
HostResourceMapping        : {}
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. Starten Sie mit dem Cmdlet New-SmClone einen Klonvorgang aus einer Klonressourcengruppe oder einer vorhandenen Sicherung.

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 Klonauftrags mithilfe des Cmdlets Get-SmCloneReport an.

Dieses Beispiel zeigt einen Klonbericht für die angegebene Job-ID an:

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

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

Überwachen Sie von NetApp unterstützte Plug-in-Ressourcenklonvorgänge

Sie können den Fortschritt der SnapCenter -Klonvorgänge auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Fortschritt eines Vorgangs überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

-  Im Gange
-  Erfolgreich abgeschlossen
-  Fehlgeschlagen
-  Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
-  In der Warteschlange
-  Abgesagt

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  um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
 - b. Geben Sie das Start- und Enddatum an.
 - c. Wählen Sie aus der Dropdownliste **Typ** die Option **Klon** aus.
 - d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
 - e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie den Klonauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite „Auftragsdetails“ 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 IRGEND EINER 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.