



Schützen Sie IBM Db2

SnapCenter software

NetApp

November 06, 2025

This PDF was generated from <https://docs.netapp.com/de-de/snapcenter-61/protect-db2/snapcenter-plugin-in-for-ibm-db2-overview.html> on November 06, 2025. Always check docs.netapp.com for the latest.

Inhalt

Schützen Sie IBM Db2	1
SnapCenter Plug-in für IBM Db2	1
Übersicht über das SnapCenter -Plug-in für IBM Db2	1
Was Sie mit dem SnapCenter Plug-in für IBM Db2 tun können	1
SnapCenter Plug-in für IBM Db2-Funktionen	2
Vom SnapCenter Plug-in für IBM Db2 unterstützte Speichertypen	2
Für das IBM Db2-Plug-In erforderliche Mindest ONTAP Berechtigungen	3
Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für IBM Db2	6
Backup-Strategie für IBM Db2	6
Wiederherstellungs- und Recovery-Strategie für IBM Db2	9
Vorbereiten der Installation des SnapCenter -Plug-ins für IBM Db2	10
Installationsworkflow des SnapCenter Plug-ins für IBM Db2	10
Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows, Linux oder AIX	11
Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows	16
Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux	17
Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für IBM Db2	18
Konfigurieren von gMSA unter Windows Server 2016 oder höher	21
Installieren Sie das SnapCenter -Plug-in für IBM Db2	22
CA-Zertifikat konfigurieren	28
Bereiten Sie sich auf den Datenschutz vor	36
Voraussetzungen für die Verwendung des SnapCenter Plug-Ins für IBM Db2	37
So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von IBM Db2 verwendet	37
Sichern von IBM Db2-Ressourcen	38
Sichern von IBM Db2-Ressourcen	38
Automatisches Erkennen der Datenbanken	40
Ressourcen manuell zum Plug-In-Host hinzufügen	40
Erstellen von Sicherungsrichtlinien für IBM Db2	42
Erstellen von Ressourcengruppen und Anfügen von Richtlinien	44
Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für IBM Db2- Ressourcen auf ASA r2-Systemen	48
Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell- Cmdlets für IBM Db2	51
Sichern von Db2-Datenbanken	52
Sichern von Ressourcengruppen	59
Überwachen von IBM Db2-Sicherungsvorgängen	60
Abbrechen von Sicherungsvorgängen für IBM Db2	61
Anzeigen von IBM Db2-Sicherungen und -Klonen auf der Seite „Topologie“	62
IBM Db2 wiederherstellen	64
Wiederherstellungs-Workflow	64
Wiederherstellen einer manuell hinzugefügten Ressourcensicherung	65
Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung	69
Überwachen von IBM Db2-Wiederherstellungsvorgängen	71

Klonen von IBM Db2-Ressourcensicherungen	72
Klon-Workflow	72
Klonen einer IBM Db2-Sicherung	72
Überwachen von IBM Db2-Klonvorgängen	79
Einen Klon teilen	80
Löschen oder Aufteilen von IBM Db2-Datenbankklonen nach dem Upgrade von SnapCenter.....	81

Schützen Sie IBM Db2

SnapCenter Plug-in für IBM Db2

Übersicht über das SnapCenter -Plug-in für IBM Db2

Das SnapCenter Plug-in für IBM Db2-Datenbanken ist eine hostseitige Komponente der NetApp SnapCenter software , die eine anwendungsbewusste Datenschutzverwaltung von IBM Db2-Datenbanken ermöglicht. Das Plug-in für IBM Db2-Datenbanken automatisiert die Sicherung, Wiederherstellung und das Klonen von IBM Db2-Datenbanken in Ihrer SnapCenter Umgebung.

- SnapCenter 6.0 unterstützt IBM Db2 10.5 und höher.
- SnapCenter 6.0.1 unterstützt IBM Db2 9.7.x und höher. Ab SnapCenter 6.0.1 wird außerdem IBM Db2 auf AIX unterstützt.

SnapCenter unterstützt Db2-Setups mit einer oder mehreren Instanzen. Sie können das Plug-in für die IBM Db2-Datenbank sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird Db2 als manuelle Ressource unterstützt.



Db2 pureScale-Umgebungen und Db2 Multi Node (DPF)-Systeme werden nicht unterstützt.

Wenn das Plug-in für die IBM Db2-Datenbank installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen. Sie können das Plug-in auch mit der NetApp SnapVault -Technologie verwenden, um eine Disk-to-Disk-Backup-Replikation zur Einhaltung von Standards durchzuführen.

Das SnapCenter -Plug-in für Db2 unterstützt NFS und SAN auf ONTAP und Azure NetApp Dateispeicherlayouts.

Das virtuelle Speicherlayout VMDK, vVol und RDM wird unterstützt.

Was Sie mit dem SnapCenter Plug-in für IBM Db2 tun können

Wenn Sie das Plug-in für IBM Db2-Datenbanken in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von IBM Db2-Datenbanken und deren Ressourcen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Datenbanken hinzufügen.
- 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.

SnapCenter Plug-in für IBM Db2-Funktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit dem Plug-in für die IBM Db2-Datenbank 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-Kopiertechnologie**

SnapCenter verwendet die Snapshot-Technologie von NetApp mit dem Plug-in für die IBM Db2-Datenbank, um Ressourcen zu sichern.

Die Verwendung des Plug-ins für IBM Db2 bietet 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.
- Unterstützung für Linux LVM auf dem XFS-Dateisystem.

Vom SnapCenter Plug-in für IBM Db2 unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen Maschinen als auch auf virtuellen Maschinen (VMs). Sie müssen die Unterstützung für

Ihren Speichertyp überprüfen, bevor Sie das SnapCenter Plug-in für IBM Db2 installieren.

Maschine	Speichertyp
Physischer Server	• FC-verbundene LUNs • Über iSCSI verbundene LUNs • Über NFS verbundene Volumes
VMware ESXi	• RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei LinuxConfig.pm unter <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> bearbeiten, um den Wert des Parameters SCSI_HOSTS_OPTIMIZED_RESCAN auf 1 zu setzen und nur die HBAs erneut zu scannen, die in HBA_DRIVER_NAMES aufgeführt sind. • iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datenspeichern • VMDKs auf VMFS erstellt • NFS-Volumes, die direkt mit dem Gastsystem verbunden sind • vVol-Datenspeicher auf NFS und SAN vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Für das IBM Db2-Plug-In erforderliche Mindest ONTAP Berechtigungen

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
 - Montag
 - LUN erstellen
 - LUN erstellen
 - LUN erstellen

- LUN löschen
- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- 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 persistent-reservation clear
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- 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-Modify-Snaplock-Ablaufzeit
- 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
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
 - Netzwerkschnittstelle

- Netzwerkschnittstelle anzeigen
- vServer

Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für IBM Db2

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"](#).

Backup-Strategie für IBM Db2

Definieren Sie eine Sicherungsstrategie für IBM Db2

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge verfügen Sie über die Sicherungen, 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 eine auf Snapshot-Kopien basierende Richtlinie erstellen möchten, um anwendungskonsistente Snapshots der Datenbank zu sichern.
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.

Automatische Erkennung von Ressourcen auf Linux-Hosts

Ressourcen sind IBM Db2-Datenbanken und Instanzen auf dem Linux-Host, die von SnapCenter verwaltet werden. Nach der Installation des SnapCenter -Plug-ins für IBM Db2 werden die IBM Db2-Datenbanken aller Instanzen auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.

Unterstützte Sicherungstypen

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot-Kopien basierenden Sicherungstyp für IBM Db2-Datenbanken.

Snapshot-Kopie-basierte Sicherung

Auf Snapshot-Kopien basierende Backups nutzen die Snapshot-Technologie von NetApp , um schreibgeschützte Online-Kopien der Volumes zu erstellen, auf denen sich die IBM Db2-Datenbanken befinden.

So verwendet das SnapCenter Plug-in für IBM Db2 Konsistenzgruppen-Snapshots

Sie können das Plug-In verwenden, um Konsistenzgruppen-Snapshots für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes aufnehmen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe besteht aus gleichzeitigen Snapshots mehrerer Volumes und bietet konsistente Kopien einer Volumengruppe.

Sie können auch die Wartezeit angeben, die der Speichercontroller benötigt, um Snapshots konsistent zu gruppieren. Die verfügbaren Wartezeitoptionen sind **Dringend**, **Mittel** und **Entspannt**. Sie können die WAFL-Synchronisierung (Write Anywhere File Layout) auch während des konsistenten Gruppen-Snapshot-Vorgangs aktivieren oder deaktivieren. Die WAFL Synchronisierung verbessert die Leistung eines Konsistenzgruppen-Snapshots.

So verwaltet SnapCenter die Datensicherung

SnapCenter verwaltet die Datensicherungen auf Speichersystem- und Dateisystemebene.

Die Snapshots auf dem primären oder sekundären Speicher und die entsprechenden Einträge im IBM Db2-Katalog werden basierend auf den Aufbewahrungseinstellungen gelöscht.

Überlegungen zur Festlegung von Sicherungszeitplänen für IBM Db2

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. 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).

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen)

Die Sicherungshäufigkeit, bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen)

Sicherungszeitpläne 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.

Anzahl der für IBM Db2 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).

Sicherungsnamenskonventionen für Plug-in für IBM Db2-Datenbanken

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

Wiederherstellungs- und Recovery-Strategie für IBM Db2

Definieren Sie eine Wiederherstellungsstrategie für IBM Db2-Ressourcen

Sie müssen vor der Wiederherstellung Ihrer Datenbank eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.



Es wird nur die manuelle Wiederherstellung der Datenbank unterstützt.

Schritte

1. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für manuell hinzugefügte IBM Db2-Ressourcen
2. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für automatisch erkannte IBM Db2-Datenbanken

Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte IBM Db2-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte IBM Db2-Ressourcen.



Sie können manuell hinzugefügte IBM Db2-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 für die 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.

Art der unterstützten Wiederherstellungsstrategie für automatisch erkanntes IBM Db2

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit

SnapCenter erfolgreich durchführen können.

Die vollständige Ressourcenwiederherstellung ist die unterstützte Wiederherstellungsstrategie für automatisch erkannte IBM Db2-Datenbanken. Dadurch werden alle Volumes, Qtrees und LUNs einer Ressource wiederhergestellt.

Arten von Wiederherstellungsvorgängen für automatisch erkanntes IBM Db2

Das SnapCenter -Plug-in für IBM Db2 unterstützt Single File SnapRestore und Connect-and-Copy-Wiederherstellungstypen für automatisch erkannte IBM Db2-Datenbanken.

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

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das ausgewählte Backup von einem SnapMirror oder SnapVault Sekundärspeicherort stammt und die Option **Complete Resource** ausgewählt ist

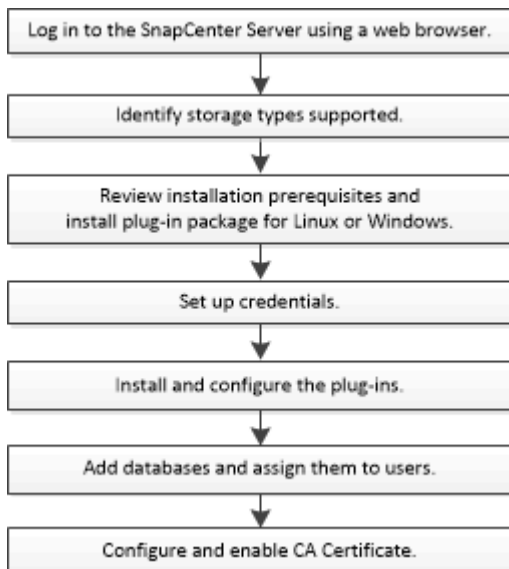
Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das Backup von einem SnapMirror oder SnapVault Sekundärspeicherort ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Vorbereiten der Installation des SnapCenter -Plug-ins für IBM Db2

Installationsworkflow des SnapCenter Plug-ins für IBM Db2

Sie sollten das SnapCenter -Plug-in für IBM Db2 installieren und einrichten, wenn Sie IBM Db2-Datenbanken 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. SnapCenter -Plug-in für IBM Db2 wird in Windows-, Linux- und AIX-Umgebungen unterstützt.

- Sie müssen Java 11 auf Ihrem Host installiert haben.



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

- Unter Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „LocalSystem“ ausgeführt werden. Dies ist das Standardverhalten, wenn das Plug-in für IBM Db2 als Domänenadministrator installiert wird.
- 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. Das SnapCenter -Plug-in für Microsoft Windows wird standardmäßig mit dem IBM Db2-Plug-in auf Windows-Hosts bereitgestellt.
- Der SnapCenter -Server sollte Zugriff auf den 8145- oder benutzerdefinierten Port des Plug-ins für den IBM Db2-Host haben.

Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Während der Installation des Plug-ins für IBM Db2 auf einem Windows-Host wird das SnapCenter -Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Windows-Host installiert haben.

["JAVA für Windows herunterladen"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

Linux- und AIX-Hosts

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

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

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

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Bei IBM Db2-Datenbanken, die auf einem Linux-Host ausgeführt werden, wird bei der Installation des Plug-ins für IBM Db2 automatisch das SnapCenter Plug-in für UNIX installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

Ergänzende Befehle

Um einen zusätzlichen Befehl auf dem SnapCenter -Plug-in für IBM Db2 auszuführen, müssen Sie ihn in die Datei *allowed_commands.config* aufnehmen.

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

Um zusätzliche Befehle auf dem Plug-In-Host zuzulassen, öffnen Sie die Datei *allowed_commands.config* in einem Editor. Geben Sie jeden Befehl in einer separaten Zeile ein. Bei den Befehlen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen (") einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: mount

Befehl: umount

Befehl: "C:\Programme\ NetApp\ SnapCreator commands\ sdcli.exe"

Befehl: myscript.bat

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

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."

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

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."



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

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

SnapCenter ermöglicht einem Nicht-Root-Benutzer, das SnapCenter -Plug-In-Paket für Linux 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.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei */etc/ssh/ssh_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/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/bin/spl

Schritte

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

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias 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

```



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.

`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.

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.

- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- 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.

```

Cmnd_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
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_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
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 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

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

Bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren, sollten Sie mit einigen grundlegenden Anforderungen an Speicherplatz und Größe des Hostsystems vertraut sein.

Artikel	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Artikel	Anforderungen
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 und 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 der Anmeldeinformationen für das SnapCenter -Plug-in für IBM Db2

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.

Informationen zu diesem Vorgang

- Linux-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux-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.

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> Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (<) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als <!10, kleiner als 10 <!, Backtick `12.
Passwort	Geben Sie das zur Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus 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-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 -EffectivelImmediately
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 das SnapCenter -Plug-in für IBM Db2

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 Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren.

Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
 - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
 - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.

- 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.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zur Verwaltung von Hosts.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

["Konfigurieren Sie das gruppenverwaltete Dienstkonto unter Windows Server 2016 oder höher für IBM Db2"](#)

Informationen zu diesem Vorgang

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **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  Das Plug-in für IBM Db2 wird auf dem IBM Db2-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.
Hostname	Geben Sie den Hostnamen für die Kommunikation ein. 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.

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationen	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host 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.

Wenn Sie die REST-API zum Installieren des Plug-ins für Db2 verwenden, müssen Sie die Version als 3.0 übergeben. Beispiel: Db2:3.0

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

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.

Für dieses Feld...	Machen Sie Folgendes...
Installationspfad	Das Plug-in für IBM Db2 wird auf dem IBM Db2-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein. - Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter. Optional können Sie den Pfad anpassen. - Für das SnapCenter Plug-ins-Paket für Linux 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.
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. Klicken Sie auf **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 11 (für Windows- und 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 unter C:\Programme\ NetApp\ SnapCenter WebApp aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.



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

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

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



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

9. Überwachen Sie den Installationsfortschritt.

- Für Windows-Plug-Ins befinden sich die Installations- und Upgrade-Protokolle unter: `C:\Windows\SnapCenter plugin\Install<JOBID>\`
- Für Linux-Plug-Ins befinden sich die Installationsprotokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log` und die Upgrade-Protokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log`

Nach Abschluss

Wenn Sie auf SnapCenter 6.0 oder höher aktualisieren möchten, wird das vorhandene PERL-basierte Plug-in für Db2 vom Remote-Plug-in-Server deinstalliert.

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

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

Bevor Sie beginnen

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

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 das SnapCenter -Plug-in für IBM Db2 auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle

Sie sollten das SnapCenter Plug-in für die IBM Db2-Datenbank mithilfe der SnapCenter -Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie das Plug-In für die IBM Db2-Datenbank entweder im Konsolenmodus oder im Hintergrundmodus

mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Bevor Sie beginnen

- Sie sollten das Plug-in für die IBM Db2-Datenbank auf jedem Linux-Host installieren, auf dem sich der IBM Db2-Client befindet.
- Der Linux-Host, auf dem Sie das SnapCenter -Plug-in für die IBM Db2-Datenbank installieren, muss die abhängigen Software-, Datenbank- und Betriebssystemanforderungen erfüllen.

Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den unterstützten Konfigurationen.

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Das SnapCenter -Plug-in für die IBM Db2-Datenbank ist Teil des SnapCenter Plug-in-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins-Paket für Linux installieren, sollten Sie SnapCenter bereits auf einem Windows-Host installiert haben.

Informationen zu diesem Vorgang

Wenn keine Parameter angegeben sind, wird SnapCenter mit Standardwerten installiert.

Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter Plug-ins-Pakets für Linux (snapcenter_linux_host_plugin.bin) von C:\ProgramData\NetApp\ SnapCenter\Package Repository auf den Host, auf dem Sie das Plug-in für IBM Db2 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. Bearbeiten Sie die Datei /<Installationsverzeichnis>/
NetApp/snapcenter/scc/etc/SC_SMS_Services.properties und fügen Sie dann den Parameter

PLUGINS_ENABLED = DB2:3.0 hinzu.

5. 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"](#) .

Überwachen Sie den Status der Installation des Plug-ins für IBM Db2

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-Verwaltungskonsolle (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 SnapCenter IBM Db2 Plug-Ins-Dienst auf dem Linux-Host

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

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

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

Schritte

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

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 Schlüsselspeicherkenwort.

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 SnapCenter IBM Db2 Plug-Ins-Dienst auf dem Windows-Host

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

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

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

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

Schritte

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

Es 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 Schlüsselspeicherkennwort.

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 des SnapCenter Plug-Ins für IBM Db2

Bevor Sie das SnapCenter -Plug-in für IBM Db2 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.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

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

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.

So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von IBM Db2 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.

- Bei den Ressourcen handelt es sich in der Regel um IBM Db2-Datenbanken, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem 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, 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.

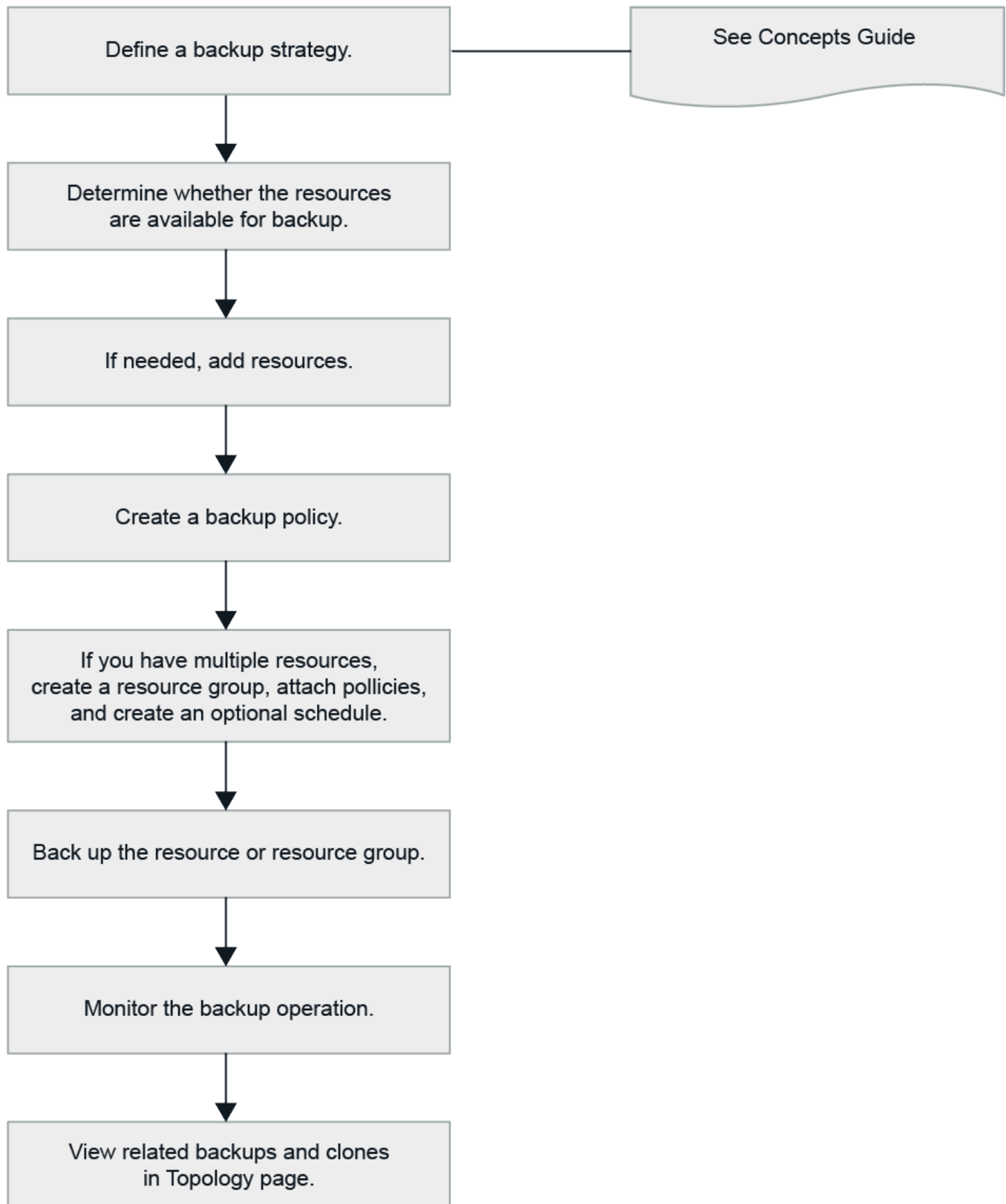
Stellen Sie sich eine Ressourcengruppe so vor, dass sie definiert, was Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als ob sie definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken im 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 vollständige Sicherung durchgeführt wird.

Sichern von IBM Db2-Ressourcen

Sichern von IBM Db2-Ressourcen

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Sicherungsworkflow umfasst die Planung, die Identifizierung der zu sichernden Datenbanken, 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. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets. ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

Automatisches Erkennen der Datenbanken

Ressourcen sind IBM Db2-Datenbanken auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren IBM Db2-Datenbanken ermittelt haben.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen abgeschlossen haben.
- Das SnapCenter Plug-in für IBM Db2 unterstützt keine automatische Erkennung der in virtuellen RDM/VMDK-Umgebungen vorhandenen Ressourcen. Sie müssen die Speicherinformationen für virtuelle Umgebungen angeben, während Sie die Datenbanken manuell hinzufügen.

Informationen zu diesem Vorgang

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

Die automatisch erkannten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für IBM Db2 aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste „Anzeigen“ aus.
3. (Optional) Klicken Sie auf  * und wählen Sie dann den Hostnamen aus.

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

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

Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp -Speichersystem befindet und geschützt ist und kein Sicherungsvorgang ausgeführt wird, wird in der Spalte „Gesamtstatus“ die Meldung „Sicherung nicht ausgeführt“ angezeigt. Andernfalls ändert sich der Status basierend auf dem letzten Sicherungsstatus in „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“.



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

Ressourcen manuell zum Plug-In-Host hinzufügen

Die automatische Erkennung wird auf Windows-Hosts nicht unterstützt. Sie müssen Db2-Instanzen und Datenbankressourcen manuell hinzufügen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Die manuelle Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und dann das SnapCenter Plug-in für IBM Db2 aus der Dropdown-Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **IBM DB2-Ressource hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie den Datenbanknamen an.
Hostname	Geben Sie den Hostnamen ein.
Typ	Wählen Sie eine Datenbank oder Instanz aus.
Beispiel	Geben Sie den Namen der Instanz an, die der Datenbank übergeordnet ist.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen aus oder fügen Sie Informationen zu den Anmeldeinformationen hinzu. Dies ist optional.

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

Optional: Sie können auf das * klicken  * Symbol zum Hinzufügen weiterer Volumes, LUNs und Qtrees aus anderen Speichersystemen.

5. Optional: Geben Sie auf der Seite „Ressourceneinstellungen“ für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für das IBM Db2-Plug-In ein.
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

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

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

["Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"](#)

Nachdem Sie die Datenbanken hinzugefügt haben, können Sie die Details der IBM Db2-Datenbank ändern.

Erstellen von Sicherungsrichtlinien für IBM Db2

Bevor Sie SnapCenter zum Sichern von IBM Db2-Ressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren.

Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für IBM Db2-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen von Ressourcen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

Darüber hinaus können Sie in der Richtlinie Replikations-, Skript- und Anwendungseinstellungen angeben. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Informationen zu diesem Vorgang

- 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.

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 Aktionen aus.

- a. Geben Sie die Zeitplanhäufigkeit 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 auch jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



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

- a. Führen Sie im Abschnitt „Snapshot-Einstellungen“ die folgenden Aktionen aus:

Wenn Sie wollen...	Dann...
Behalten Sie eine bestimmte Anzahl von Schnappschüssen	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.
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.



Für Snapshot-Kopien-basierte Backups müssen Sie 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.

- b. Geben Sie die Richtlinienbezeichnung an.

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). Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.
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).
Fehleranzahl der Wiederholungsversuche	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. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzjobs zu definieren, den Sie ausführen möchten.

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.

Schritte

- Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
- Klicken Sie auf der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
- 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.  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: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen 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. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- a. Klicken Sie auf den Pfeil **Backups**, 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 Snapshot-Vorgangs der Konsistenzgruppe zu warten	Wählen Sie Dringend, Mittel oder Entspannt aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs anzugeben. 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.

- Klicken Sie auf den Pfeil **Skripts** 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.
- Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** 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.



Die benutzerdefinierten Schlüssel-Wert-Paare werden für IBM Db2 Linux-Plug-in-Systeme unterstützt, jedoch nicht für IBM Db2-Datenbanken, die als zentrales Windows-Plug-in registriert sind.

- c. Klicken Sie auf 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*.
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 Snapshot-Kopien 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 auf * klicken.  *.

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

b.

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

c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist „policy_name“ 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 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. Der SMTP-Server muss unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für IBM Db2-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“ (Richtlinienname) 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.

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

Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für IBM Db2

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern, Wiederherstellen oder Klonen von IBM Db2-Datenbanken 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 Daten-LIF-IP-Adresse haben.

Schritte

- Klicken Sie auf **SnapCenterPS**, um PowerShell Core zu starten.
- Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

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

Dieses Beispiel zeigt, wie Sie mit Windows-Anmeldeinformationen neue Anmeldeinformationen mit dem Namen „FinanceAdmin“ erstellen:

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux  
-AuthenticationType PasswordBased -Credential db2hostuser  
-EnableSudoPrivileges:$true
```

- Fügen Sie den IBM Db2-Kommunikationshost zum SnapCenter Server hinzu.

Für Linux:

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

Für Windows:

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. Installieren Sie das Paket und das SnapCenter -Plug-in für IBM Db2 auf dem Host.

Für Linux:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2
```

Für Windows:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2, SCW
```

6. Legen Sie den Pfad zur SQLLIB fest.

Für Windows verwendet das Db2-Plug-In den Standardpfad für den SQLLIB-Ordner:
„C:\Programme\IBM\SQLLIB\BIN“.

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

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
```

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 von Db2-Datenbanken

Das Sichern einer Datenbank umfasst das Herstellen einer Verbindung mit dem SnapCenter -Server, das Hinzufügen von Ressourcen, das Hinzufügen einer Richtlinie, das Erstellen einer Sicherungsressourcengruppe und das Sichern.

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.
- Stellen Sie bei Sicherungsvorgängen auf Basis von Snapshot-Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Bei Pre- und Post-Befehlen für Quiesce-, Snapshot- und Unquiesce-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
 - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



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

SnapCenter -Benutzeroberfläche

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

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

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

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:

- Wählen Sie den Pfeil **Backups** aus, 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 Vorgangs „Consistency Group Snapshot“ zu warten	Wählen Sie Dringend , Mittel oder Entspannt aus, um die Wartezeit für die Fertigstellung 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.

- Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle 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.

- Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- Wählen Sie 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 auch eine Richtlinie erstellen, indem Sie auf * klicken. *.

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

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

policy_name ist 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 wählen Sie dann **Fertig**.

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Wählen Sie **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. Wählen Sie **Backup**.

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

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

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

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
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

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

Dieses Beispiel zeigt, wie eine IBM Db2-Instanz hinzugefügt wird:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

Für die Db2-Datenbank:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.
4. Schützen Sie die Ressource oder fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.
5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert wird:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

In diesem Beispiel wird eine Db2-Instanz gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
db2_policy
```

In diesem Beispiel wird eine Db2-Datenbank gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCD";"PluginName"="DB2"
} -Policy db2_policy
```

6. Überwachen Sie den Auftragsstatus (wird ausgeführt, abgeschlossen oder fehlgeschlagen) mithilfe des Cmdlets Get-smJobSummaryReport.

```
PS C:\> Get-SmJobSummaryReport -JobId 467
```

```
SmJobId           : 467
JobCreatedDateTime :
JobStartDateTime  : 27-Jun-24 01:40:09
JobEndDateTime    : 27-Jun-24 01:41:15
JobDuration       : 00:01:06.7013330
JobName           : Backup of Resource Group
                  : 'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
                  : 'snapshot-based-db2'
JobDescription    :
Status            : Completed
IsScheduled       : False
JobError          :
JobType           : Backup
PolicyName        : db2_policy
JobResultData     :
```

7. Überwachen Sie die Details des Sicherungsauftrags wie Sicherungs-ID und Sicherungsname, um mithilfe des Cmdlets Get-SmBackupReport Wiederherstellungs- oder Klonvorgänge durchzuführen.

```
PS C:\> Get-SmBackupReport -JobId 467
```

```
BackedUpObjects      : {WINCIR}
FailedObjects        : {}
IsScheduled          : False
HasMetadata          : False
SmBackupId           : 84
SmJobId              : 467
StartDateTime        : 27-Jun-24 01:40:09
EndDateTime          : 27-Jun-24 01:41:15
Duration             : 00:01:06.7013330
CreatedDateTime      : 27-Jun-24 18:39:45
Status               : Completed
ProtectionGroupName  : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId  : 23
PolicyName           : db2_policy
SmPolicyId           : 13
BackupName           : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError           :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : DB2
PluginDisplayName     : IBM DB2
JobTypeId            :
JobHost              : HOSTFQDN
```

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 von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie 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.

Informationen zu diesem Vorgang

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.

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“ 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 indem Sie  und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „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. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Überwachen von IBM Db2-Sicherungsvorgängen

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.

Überwachen Sie Datenschutzvorgänge für IBM Db2-Datenbanken im Aktivitätsbereich

Im Aktivitätsbereich werden die fünf zuletzt ausgeführten Vorgänge angezeigt. Im Aktivitätsbereich wird auch angezeigt, wann der Vorgang gestartet wurde und welchen Status er hat.

Im Aktivitätsbereich werden Informationen zu Sicherungs-, Wiederherstellungs-, Klon- und geplanten Sicherungsvorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.

Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Auftragsdetails** aufgelistet.

Abbrechen von Sicherungsvorgängen für IBM Db2

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

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

Anzeigen von IBM Db2-Sicherungen und -Klonen 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.

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.



• 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.

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.

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 Ressourcengruppdetailansicht aus.

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

4. Überprüfen Sie die **Zusammenfassungskarte**, um eine Zusammenfassung der Anzahl der auf dem primären und sekundären Speicher verfügbaren Backups und Klone anzuzeigen.

Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Klone an.

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- und Löschvorgänge durchzuführen.



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

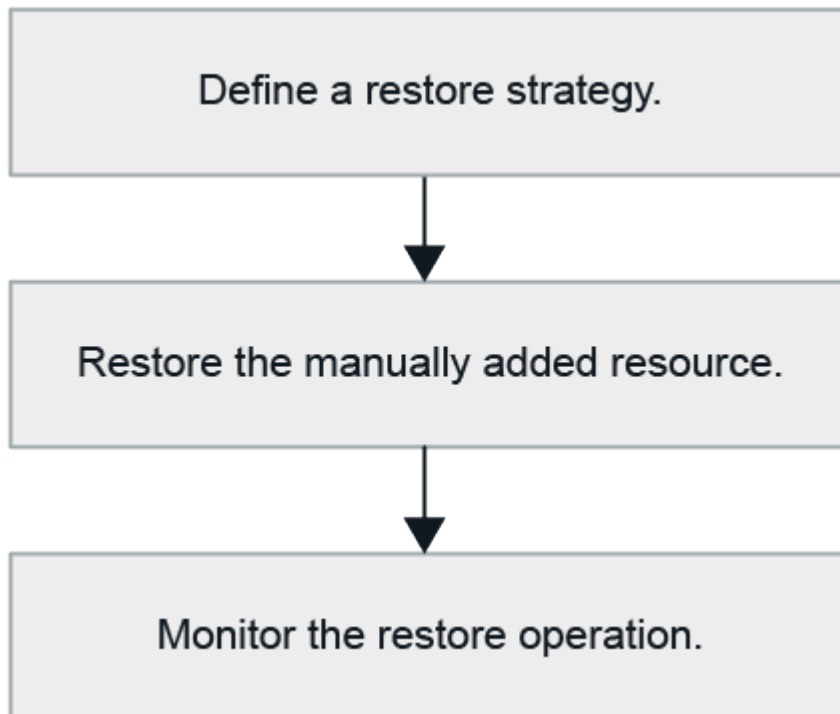
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

IBM Db2 wiederherstellen

Wiederherstellungs-Workflow

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

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

Wiederherstellen einer manuell hinzugefügten Ressourcensicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
 - Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



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

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 Typ, Host, 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. Dies 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“ **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)	
search	
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“ die Option **Vollständige Ressource** aus.
 - a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumes der IBM Db2-Datenbank wiederhergestellt.

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 eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

Sie können mehrere LUNs auswählen.



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

7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
9. 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 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.

Nach Abschluss

Eine Wiederherstellung ist nur möglich, wenn der Rollforward-Status „DB ausstehend“ lautet. Dieser Status gilt für Db2-Datenbanken mit aktivierter Archivprotokollierung.

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. Identifizieren Sie die Sicherung, die Sie wiederherstellen möchten, mithilfe der Cmdlets `Get-SmBackup` und `Get-SmBackupReport`.

Dieses Beispiel zeigt, dass für die Wiederherstellung zwei Sicherungen zur Verfügung stehen:

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library
```

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

AM Full Backup
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.



AppObjectId ist „Host\Plugin\UID“, wobei UID = <Instanzname> für die manuell ermittelte DB2-Instanzressource und UID = <Instanzname>\<Datenbankname> für die IBM Db2-Datenbankressource steht. Sie können die ResourceID über das Cmdlet „Get-smResources“ abrufen.

```
Get-smResources -HostName cn24.sccore.test.com -PluginCode DB2
```

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

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

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

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>"; "Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"})
```

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"](#) .

Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
 - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



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

Informationen zu diesem Vorgang

- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Die automatische Wiederherstellung wird nicht unterstützt.
- 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.

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 Typ, Host, 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. Dies 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“ **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)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ **Vollständige Ressource** aus, um die konfigurierten Datenvolumes der IBM Db2-Datenbank wiederherzustellen.
7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Unmount-Befehle erforderlich.

8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle erforderlich.

9. 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 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.

Nach Abschluss

Eine Wiederherstellung ist nur möglich, wenn der Rollforward-Status „DB ausstehend“ lautet. Dieser Status gilt für Db2-Datenbanken mit aktivierter Archivprotokollierung.

Überwachen von IBM Db2-Wiederherstellungsvorgängen

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 von IBM Db2-Ressourcensicherungen

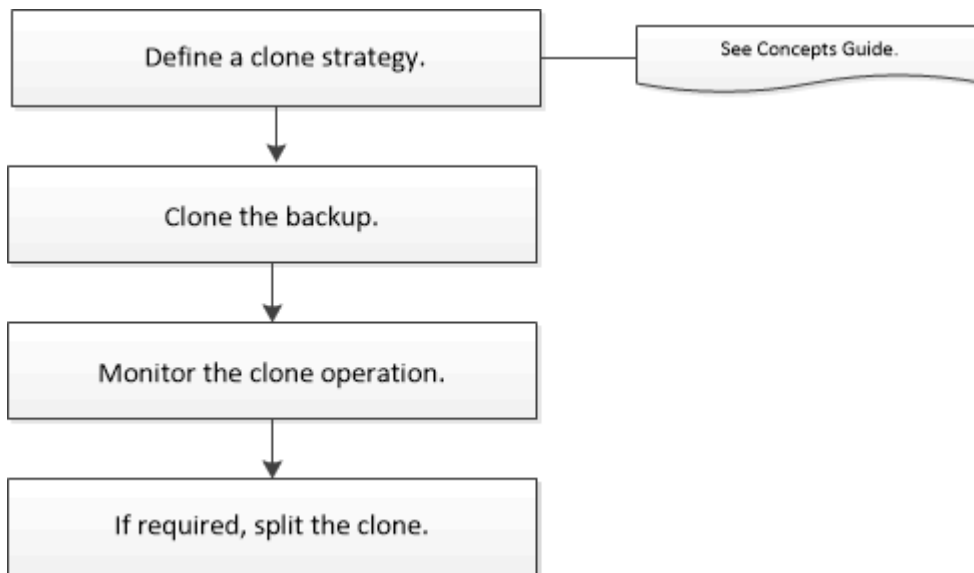
Klon-Workflow

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

Informationen zu diesem Vorgang

- Sie können auf dem IBM Db2-Quellserver klonen.
- 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. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

Nach Abschluss

Nach dem Klonen der automatisch erkannten Db2-Ressourcen wird die geklonte Ressource als manuelle Ressource markiert. Klicken Sie auf **Ressourcen aktualisieren**, um die geklonte Db2-Ressource wiederherzustellen. Wenn Sie den Klon löschen, werden auch der Speicher und der Host bereinigt.

Wenn Sie die Ressourcen nach dem Klonvorgang nicht aktualisieren und versuchen, den Klon zu löschen, werden der Speicher und der Host nicht bereinigt. Sie müssen die Einträge manuell in der fstab löschen.

Klonen einer IBM Db2-Sicherung

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen.

Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Beim Erstellen eines Klons für Db2 auf einem alternativen Host müssen Sie für den Mountpfad des Klons eine n-1-Verzeichnisstruktur erstellen, die mit dem ursprünglichen Mountpfad auf dem anderen Host identisch ist. Der Mount-Pfad sollte über die Ausführungsberechtigung 755 verfügen.
- Bei Befehlen vor oder nach dem Klonen sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
 - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



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

Informationen zu diesem Vorgang

- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume"] .
- 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, 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 „Standort“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Server klonen	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Zielklon-Instanz	Geben Sie die Ziel-ID der Db2-Kloninstanz ein, die aus den vorhandenen Sicherungen geklont werden soll. Dies gilt nur für Ressourcen des Speichertyps ANF.
Name des Zielklons	Geben Sie den Namen des Klons ein. Dies gilt nur für Db2-Datenbankressourcen.
NFS-Export-IP-Adresse	Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden. Dies gilt nur für Ressourcen des NFS-Speichertyps.
Max. Durchsatz des Kapazitätspools (MiB/s)	Geben Sie den maximalen Durchsatz eines Kapazitätspools ein.

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



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

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

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

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

8. 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.

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

Nach Abschluss

Nach dem Klonen der automatisch erkannten Db2-Ressourcen wird die geklonte Ressource als manuelle Ressource markiert. Klicken Sie auf **Ressourcen aktualisieren**, um die geklonte Db2-Ressource wiederherzustellen. Wenn Sie den Klon löschen, werden auch der Speicher und der Host bereinigt.

Wenn Sie die Ressourcen nach dem Klonvorgang nicht aktualisieren und versuchen, den Klon zu löschen, werden der Speicher und der Host nicht bereinigt. Sie müssen die Einträge manuell in der fstab löschen.

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
```

2. 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, ihren Ressourcen und zugehörigen Richtlinien angezeigt:

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

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCOREContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCOREContracts.SmVerificationServerInfo
SchedulersSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}

```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. Starten Sie einen Klonvorgang aus einer vorhandenen Sicherung mithilfe des Cmdlets New-SmClone.

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

```

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

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

```

In diesem Beispiel wird ein Klon einer angegebenen Microsoft SQL Server-Instanz erstellt:

```

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

```

4. Zeigen Sie den Status des 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}
```

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 von IBM Db2-Klonvorgängen

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**.

Einen Klon teilen

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

Informationen zu diesem Vorgang

- Sie können den Klon-Split-Vorgang nicht auf einem Zwischenklon durchführen.

Nachdem Sie beispielsweise Klon1 aus einer Datenbanksicherung erstellt haben, können Sie eine Sicherung von Klon1 erstellen und diese Sicherung dann klonen (Klon2). Nachdem Sie Klon2 erstellt haben, ist Klon1 ein Zwischenklon und Sie können den Klonaufteilungsvorgang nicht auf Klon1 durchführen. Sie können den Klon-Split-Vorgang jedoch auf Klon2 durchführen.

Nachdem Sie Klon2 geteilt haben, können Sie den Klon-Teilungsvorgang für Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Sicherungskopien und Klonaufträge des Klons gelöscht.
- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter ["Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume"](#) .
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Speichersystem online ist.

Schritte

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

Option	Beschreibung
Für Datenbankanwendungen	Wählen Sie Datenbank aus der Ansichtsliste.
Für Dateisysteme	Wählen Sie Pfad aus der Ansichtsliste.

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

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Kopien verwalten** die geklonte Ressource (z. B. die Datenbank oder LUN) aus und klicken Sie dann auf  *.
5. Überprüfen Sie die geschätzte Größe des aufzuteilenden Klon und den erforderlichen verfügbaren Speicherplatz auf dem Aggregat und klicken Sie dann auf **Start**.
6. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Der Klon-Split-Vorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet „Stop-SmJob“ ausführen, um den Klon-Split-Vorgang zu stoppen, und ihn dann erneut versuchen.

Wenn Sie eine längere oder kürzere Abfragezeit wünschen, um zu überprüfen, ob der Klon aufgeteilt ist oder nicht, können Sie den Wert des Parameters *CloneSplitStatusCheckPollTime* in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall festzulegen, in dem SMCore den Status des Klonaufteilungsvorgangs abfragt. Der Wert wird in Millisekunden angegeben und der Standardwert beträgt 5 Minuten.

Beispiel:

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

Der Startvorgang für die Klonaufteilung schlägt fehl, wenn eine Sicherung, Wiederherstellung oder eine andere Klonaufteilung ausgeführt wird. Sie sollten den Klon-Split-Vorgang erst neu starten, nachdem die laufenden Vorgänge abgeschlossen sind.

Ähnliche Informationen

["SnapCenter -Klon oder -Verifizierung schlägt fehl, da Aggregat nicht vorhanden ist"](#)

Löschen oder Aufteilen von IBM Db2-Datenbankklonen nach dem Upgrade von SnapCenter

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

Informationen zu diesem Vorgang

Wenn Sie den Speicherbedarf der versteckten Klone ermitteln möchten, führen Sie den folgenden Befehl aus:
Get-SmClone -ListStorageFootprint

Schritte

1. Löschen Sie die Sicherungen der geklonten Ressourcen mithilfe des Cmdlets „remove-smbbackup“.
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mithilfe des Cmdlets „remove-smresourcegroup“.
3. Entfernen Sie den Schutz der geklonten Ressource mithilfe des Cmdlets „remove-smprotectresource“.
4. Wählen Sie die übergeordnete Ressource auf der Seite „Ressourcen“ aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht „Kopien verwalten“ die Klone entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.

6. Wählen Sie die Klone aus und klicken Sie dann auf  , um Klone zu löschen, oder klicken Sie auf  um die Klone zu teilen.
7. Klicken Sie auf **OK**.

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.