Schutz von Microsoft Exchange Server Datenbanken

SnapCenter Software 5.0

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-50/protect-sce/concept_snapcenter_plug_in_for_exchange_server_overview.html on October 15, 2025. Always check docs.netapp.com for the latest.

Inhalt

Schutz von Microsoft Exchange Server Datenbanken . . . 1
SnapCenter Plug-in für Microsoft Exchange Server-Konzepte . . . 1
Übersicht über das SnapCenter Plug-in für Microsoft Exchange Server . . . 1
Ihre Möglichkeiten mit dem SnapCenter Plug-in für Microsoft Exchange Server . . . 1
Storage-Typen, die von SnapCenter Plug-in für Microsoft Windows und für Microsoft Exchange Server unterstützt werden . . . 1
Minimale ONTAP-Berechtigungen, die für das Exchange Plug-in erforderlich sind . . . 3
Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten . . . 6
Backup-Strategie für Exchange Server-Ressourcen definieren . . . 6
Festlegen einer Restore-Strategie für Exchange-Datenbanken . . . 9
Installieren Sie das SnapCenter Plug-in für Microsoft Exchange Server . . . 10
Installations-Workflow des SnapCenter Plug-ins für Microsoft Exchange Server . . . 10
Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter Plug-ins für Microsoft Exchange Server . . . 11
Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-in für Windows ein . . . 15
Konfigurieren Sie gMSA unter Windows Server 2012 oder höher . . . 16
Fügen Sie Hosts hinzu und installieren Sie das Plug-in für Exchange . . . 18
Installieren Sie das Plug-in für Exchange über den SnapCenter Server Host mithilfe von PowerShell Cmdlets . . . 23
Installieren Sie das SnapCenter Plug-in für Exchange im Hintergrund über die Befehlszeile . . . 24
Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets . . . 26
Konfigurieren Sie das CA-Zertifikat . . . 26
Konfigurieren Sie SnapManager 7.x für Exchange und SnapCenter, um koexistieren zu können . . . 30
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 32
Bereitstellen eines CA-Zertifikats . . . 32
Konfigurieren Sie die CRL-Datei . . . 32
Bereiten Sie sich auf die Datensicherung vor . . . 32
Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für Microsoft Exchange Server . . . 32
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von Exchange Server verwendet werden . . . 33
Exchange-Ressourcen sichern . . . 34
Backup-Workflow . . . 34
Exchange Datenbank und Backup-Verifizierung . . . 35
Bestimmen Sie, ob Exchange Ressourcen für Backups verfügbar sind . . . 35
Erstellen von Backup-Richtlinien für Exchange Server-Datenbanken . . . 37
Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Exchange-Server . . . 44
Backup von Exchange Datenbanken . . . 47
Sichern von Exchange-Ressourcengruppen . . . 49
Erstellen Sie eine Storage-Systemverbindung und Zugangsdaten mit PowerShell cmdlets für Exchange Server . . . 51
Sichern Sie Exchange Ressourcen mit PowerShell Cmdlets . . . 52
Monitoring von Backup-Vorgängen . . . 54
Abbrechen der Backup-Vorgänge für die Exchange-Datenbank . . . 55

Entfernen Sie Exchange Backups mithilfe von PowerShell Cmdlets . . . 56
Zeigen Sie Exchange-Backups auf der Seite Topologie an . . . 57
Stellen Sie Exchange Ressourcen wieder her . . . 58
Wiederherstellung des Workflows . . . 58
Anforderungen für die Wiederherstellung einer Exchange-Datenbank . . . 59
Exchange Datenbanken wiederherstellen . . . 59
Granulares Recovery von Mails und Mailboxen . . . 62
Wiederherstellung einer Exchange Server-Datenbank aus dem sekundären Storage . . . 62
Stellen Sie Exchange Ressourcen mithilfe von PowerShell cmdlets wieder her . . . 63
Erneutes Seeding eines passiven Exchange Node-Replikats . . . 65
Erneutes Seeding mit PowerShell cmdlets für Exchange Datenbank . . . 66
Überwachen von Restore-Vorgängen . . . 66
Abbrechen von Wiederherstellungsvorgängen für Exchange-Datenbank . . . 67

Schutz von Microsoft Exchange Server Datenbanken

SnapCenter Plug-in für Microsoft Exchange Server-Konzepte

Übersicht über das SnapCenter Plug-in für Microsoft Exchange Server

Das SnapCenter Plug-in für Microsoft Exchange Server ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das Management der applikationsspezifischen Datensicherung von Exchange Datenbanken ermöglicht. Das Plug-in für Exchange automatisiert Backup und Restore von Exchange Datenbanken in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für Exchange installiert ist, können Sie mithilfe von SnapCenter mit NetApp SnapMirror Technologie gespiegelte Kopien von Backups auf einem anderen Volume erstellen. In diesem Fall ermöglicht NetApp SnapVault Technologie eine Disk-to-Disk-Backup-Replizierung, um Standard-Compliance- oder Archivierungszwecke zu erfüllen.

Wenn Sie E-Mails oder Mailboxen statt der gesamten Exchange Datenbank wiederherstellen möchten, können Sie die Single Mailbox Recovery (SMBR) Software verwenden. Die Einstellung der Verfügbarkeit für NetApp Single Mailbox Recovery (EOA) steht am 12. Mai 2023 fest. NetApp unterstützt Kunden, die für den Zeitraum der Support-Berechtigung Mailbox-Kapazität, Wartung und Support erworben haben, weiterhin über die am 24. Juni 2020 eingeführten Marketing-Teilenummern.

NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. OnTrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können von Ontrack (bis licensingteam@ontrack.com) neue Ontrack PowerControls Softwarelizenzen und Ontrack PowerControls Wartungs- und Supportverlängerungen für eine granulare Mailbox-Recovery erwerben.

Ihre Möglichkeiten mit dem SnapCenter Plug-in für Microsoft Exchange Server

Mit dem Plug-in für Exchange können Sie Exchange Server Datenbanken sichern und wiederherstellen.

- Überwachen und managen Sie aktive Bestände an Exchange Database Availability Groups (DAGs), Datenbanken und Replikatsets
- Definition von Richtlinien mit den Sicherungseinstellungen für die Backup-Automatisierung
- Weisen Sie den Ressourcengruppen Richtlinien zu
- Sicherung einzelner DAGs und Datenbanken
- Backup von primären und sekundären Exchange Mailbox-Datenbanken
- Wiederherstellung von Datenbanken aus primären und sekundären Backups

Storage-Typen, die von SnapCenter Plug-in für Microsoft Windows und für Microsoft Exchange Server unterstützt werden

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen

Computern als auch auf Virtual Machines. Sie müssen überprüfen, ob Ihr Speichertyp unterstützt wird, bevor Sie das Paket für Ihren Host installieren.

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

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische SnapCenter Benutzeroberfläche (GUI) oder PowerShell Commandlets	
Physischer Server	ISCSI-verbundene LUNs	SnapCenter GUI oder PowerShell Commandlets	
VMware VM	RDM-LUNs, die über einen FC- oder iSCSI-HBA verbunden sind	PowerShell Commandlets	Nur physische Kompatibilität VMDKs werden nicht unterstützt.
VMware VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	VMDKs werden nicht unterstützt.

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	Virtuelle FC-LUNs (VFC), die über einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Sie müssen Hyper-V Manager verwenden, um virtuelle FC (VFC) LUNs bereitzustellen, die über einen virtuellen Fibre Channel Switch verbunden sind. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.
Hyper-V VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Minimale ONTAP-Berechtigungen, die für das Exchange Plug-in erforderlich sind

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

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher

- Event Generate-AutoSupport-log
- Job-Verlauf wird angezeigt
- Job beenden
- lun
- lun erstellen
- lun erstellen
- lun erstellen
- lun löschen
- lun Initiatorgruppe hinzufügen
- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele

- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen
- Show-Disk-Nutzung für Volume-Dateien
- Volume ist offline
- Das Volume ist online
- Volume-Änderung
- Erstellen von Volume-qtree
- Volume qtree löschen
- Änderung des Volume-qtree
- Volume-qtree anzeigen
- Volume-Einschränkung
- Volumen anzeigen
- Erstellen von Volume-Snapshots
- Volume Snapshot löschen
- Ändern des Volume-Snapshots
- Umbenennung von Volume-Snapshots
- Wiederherstellung von Volume Snapshots
- Restore-Datei für Volume Snapshots
- Volume-Snapshot werden angezeigt
- Volume-Aufhängung nicht verfügbar
- cifs von vserver
- erstellung von cifs-Freigaben von vserver
- cifs-Freigabe von vserver: Löschen
- vserver cifs shadowcopy anzeigen
- cifs-Freigabe von vserver wird angezeigt
- vserver cifs zeigen
- vserver Exportrichtlinie
- Erstellung von vserver Exportrichtlinien
- vserver: Löschen der Exportrichtlinie
- Erstellung von vserver Export-Policy-Regel
- vserver: Export-Policy-Regel anzeigen

- vserver Export-Policy wird angezeigt
- vserver iscsi
- vserver iscsi-Verbindung wird angezeigt
- vserver zeigen

- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle wird angezeigt
  - vserver

Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

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

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

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

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

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

SnapCenter unterstützt keine **Sync_mirror** Replikation.

Backup-Strategie für Exchange Server-Ressourcen definieren

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

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

Arten von Backups, die für Exchange-Datenbank unterstützt werden

Für das Backup von Exchange Mailboxen mit SnapCenter müssen Sie den Ressourcentyp auswählen, beispielsweise Datenbanken und Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAG). Mithilfe der Snapshot Technologie werden schreibgeschützte Online-Kopien der Volumes erstellt, auf denen sich die Ressourcen befinden.

Backup-Typ	Beschreibung
Vollständiges Backup und Backup für Protokolle	Backups der Datenbanken und aller Transaktions-Logs, einschließlich der gekürzten Logs. Nach Abschluss eines vollständigen Backups schneidet der Exchange Server die Transaktions-Logs ab, die bereits in die Datenbank übernommen wurden. Normalerweise sollten Sie diese Option wählen. Wenn Ihre Backup-Zeit jedoch kurz ist, können Sie wählen, keine Transaktions-Log-Backup mit vollständiger Sicherung auszuführen.
Vollständiges Backup	Sicherung von Datenbanken und Transaktionsprotokollen. Die gekürzten Transaktionsprotokolle werden nicht gesichert.
Backup-Protokollierung	Sichert alle Transaktions-Logs. Die gekürzten Protokolle, die bereits in die Datenbank geschrieben sind, werden nicht gesichert. Wenn Sie regelmäßige Transaktions-Log-Backups zwischen vollständigen Datenbank-Backups planen, können Sie granulare Recovery-Punkte auswählen.

Backup-Pläne für Datenbank-Plug-ins

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus

dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

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

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Backups konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Datenbanken erforderlichen Backup-Jobs

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

Konventionen bei Backup-Namen

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

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
resourcegroupname_hostname_timestamp
```

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

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

In diesem Beispiel haben die Syntaxelemente folgende Bedeutungen:

- *Dts1* ist der Name der Ressourcengruppe.
- *Mach1x88* ist der Hostname.
- *03-12-2015_23.17.26* ist das Datum und der Zeitstempel.

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

Optionen zur Backup-Aufbewahrung

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

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

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

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

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

Wie lange dauert die Speicherung von Transaktions-Log-Backups auf dem Quell-Storage Volume für Exchange Server

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

Beispiel: Wenn das Plug-in für Exchange um 8:00 Uhr ein vollständiges Backup des Transaktionsprotokolls und um 5:00 Uhr ein weiteres vollständiges Backup des Transaktionsprotokolls erstellt hat, es könnte die letzte Transaktionsprotokoll-Sicherung verwenden, um die Datenbank jederzeit zwischen 8:00 und 5:00 Uhr wiederherzustellen. wenn Transaktionsprotokolle nicht verfügbar sind, kann Plug-in für Exchange nur Point-in-Time-Wiederherstellungsvorgänge durchführen. die eine Datenbank so lange wiederherstellen, wie Plug-in für Exchange ein vollständiges Backup abgeschlossen hat.

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

Festlegen einer Restore-Strategie für Exchange-Datenbanken

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

Quellen für eine Wiederherstellung in Exchange Server

Sie können eine Exchange Server Datenbank aus einer Backup-Kopie im Primärspeicher wiederherstellen.

Sie können Datenbanken nur aus dem Primärspeicher wiederherstellen.

Arten von Wiederherstellungsvorgängen, die für Exchange Server unterstützt werden

Mit SnapCenter können Sie verschiedene Arten von Restore-Vorgängen für Exchange Ressourcen ausführen.

- Wiederherstellung im Minutenschnoch
- Wiederherstellung auf einen früheren Zeitpunkt

Führen Sie Wiederherstellungen minutengenau durch

In einem up-to-the-minute-Wiederherstellungsvorgang werden Datenbanken bis zu dem Punkt des Ausfalls wiederhergestellt. SnapCenter erreicht dies durch folgende Sequenz:

1. Stellt die Datenbanken aus dem vollständigen Datenbank-Backup wieder her, das Sie auswählen.
2. Wendet alle gesicherten Transaktionsprotokolle sowie alle neuen Protokolle an, die seit dem letzten Backup erstellt wurden.

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

   Exchange erstellt nach Abschluss einer Wiederherstellung eine neue Protokollkette.

   Best Practice: Es wird empfohlen, nach Abschluss einer Wiederherstellung ein neues vollständiges Backup durchzuführen und zu protokollieren.

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

   Nach der Durchführung eines up-to-the-minute-Restores ist das Backup, das Sie für die Wiederherstellung verwendet haben, nur für zeitpunktgenaue Restore-Vorgänge verfügbar.

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

Wiederherstellung auf einen früheren Zeitpunkt

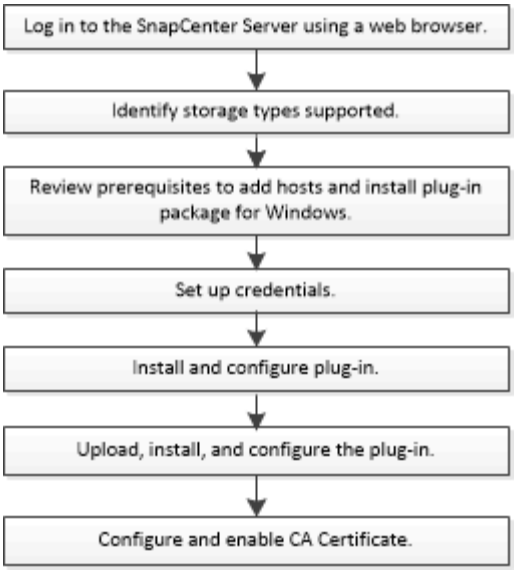
In einer zeitpunktgenauen Restore-Operation werden Datenbanken nur auf eine bestimmte Zeit aus der Vergangenheit wiederhergestellt. Ein Point-in-Time-Wiederherstellungsvorgang findet in den folgenden Situationen statt:

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

Installieren Sie das SnapCenter Plug-in für Microsoft Exchange Server

Installations-Workflow des SnapCenter Plug-ins für Microsoft Exchange Server

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



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

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

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Sie müssen Microsoft Exchange Server 2013, 2016 oder 2019 für Standalone- und Database Availability Group-Konfigurationen verwenden.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen über einen Benutzer mit Administratorrechten auf dem Exchange Server verfügen.
- Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, müssen Sie den von SnapDrive für Windows verwendeten VSS Hardware Provider deinstallieren, bevor Sie Plug-in für Exchange auf demselben Exchange-Server installieren, um den erfolgreichen Datenschutz mit SnapCenter zu gewährleisten.
- Wenn SnapManager für Microsoft Exchange Server und das Plug-in für Exchange auf demselben Server installiert sind, müssen Sie alle vom SnapManager für Microsoft Exchange Server erstellten Zeitpläne aussetzen oder löschen.
- Der Host muss auf den vollständig qualifizierten Domänennamen (FQDN) vom Server resolable sein. Wenn die Hosts-Datei geändert wird, damit sie resolable ist und wenn sowohl der Kurzname als auch der FQDN in der Datei Hosts angegeben sind, erstellen Sie einen Eintrag in der Datei SnapCenter Hosts im folgenden Format: *<ip_Address> <Host_fqdn> <Host_Name>*.
- Stellen Sie sicher, dass die folgenden Ports in der Firewall nicht blockiert sind, da sonst der Vorgang zum Hinzufügen eines Hosts fehlschlägt. Um dieses Problem zu lösen, müssen Sie den dynamischen Portbereich konfigurieren. Weitere Informationen finden Sie unter "Microsoft-Dokumentation".

- Port-Bereich 50000 - 51000 für Windows 2016 und Exchange 2016
- Port-Bereich 6000 - 6500 für Windows 2012 R2 und Exchange 2013
- Portbereich 49152 - 65536 für Windows 2019

Führen Sie die folgenden Befehle aus, um den Port-Bereich zu identifizieren:

- Netsh int ipv4 show dynamicport tcp
- Netsh int ipv4 show dynamicport udp
- Netsh int ipv6 show dynamicport tcp
- Netsh int ipv6 show dynamicport udp

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Berechtigungen für Exchange Server erforderlich

Damit SnapCenter das Hinzufügen von Exchange Server oder DAG sowie die Installation des SnapCenter Plug-ins für Microsoft Exchange Server auf einem Host oder einer DAG aktivieren kann, müssen Sie SnapCenter mit Anmeldedaten für einen Benutzer mit einem Minimum an Berechtigungen und Berechtigungen konfigurieren.

Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten verfügen, und über lokale Anmeldeberechtigungen auf dem entfernten Exchange-Host sowie über Administratorberechtigungen auf allen Knoten in der DAG. Der Domänenbenutzer benötigt die folgenden Mindestberechtigungen:

- Add-MailboxDatabaseCopy
- Datenbank Entmounten
- Get-AdServerSettings
- Get-DatabaseVerfügbarkeitGroup
- Get-ExchangeServer
- Get-Mailboxdatenbank
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistik
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatenbank
- Move-DatabasePath - KonfigurationNur: €true
- Mount-Datenbank
- Neue Postboxdatenbank
- New-PublicFolderDatabase
- Mailboxdatenbank entfernen
- Entfernen Sie-MailboxDatabaseCopy
- Entfernen Sie die-PublicFolderDatabase

- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-mailboxdatenbank -allowfilerestore: €true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-in für Windows ein

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

Über diese Aufgabe

Sie müssen Anmeldedaten für die Installation von Plug-ins auf Windows-Hosts einrichten. Obwohl Sie nach der Implementierung von Hosts und der Installation von Plug-ins Anmeldedaten für Windows erstellen können, sollten Sie vor der Implementierung von Hosts und Plug-ins zunächst die Anmeldedaten nach dem Hinzufügen von SVMs erstellen.

Richten Sie die Anmeldedaten mit Administratorrechten ein, einschließlich Administratorrechten auf dem Remote-Host.

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

Schritte

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

   Das Fenster Credential wird angezeigt.

4. Gehen Sie auf der Seite Credential wie folgt vor:

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

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen ein, der für die Authentifizierung verwendet wird. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld Benutzername lautet: `UserName`
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierung	Wählen Sie Windows als Authentifizierungsmodus aus.

5. Klicken Sie auf **OK**.

Konfigurieren Sie gMSA unter Windows Server 2012 oder höher

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

Bevor Sie beginnen

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

Schritte

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

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

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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

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

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

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


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

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

a. Starten Sie den Host neu.

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

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

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

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

Fügen Sie Hosts hinzu und installieren Sie das Plug-in für Exchange

Sie können die Seite SnapCenter Add Host verwenden, um Windows Hosts hinzuzufügen. Das Plug-in für Exchange wird automatisch auf dem angegebenen Host installiert. Dies ist die empfohlene Methode zum Installieren von Plug-ins. Sie können einen Host hinzufügen und ein Plug-in entweder für einen einzelnen Host oder ein Cluster installieren.

Bevor Sie beginnen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Plug-in-Installations- und Deinstallationsberechtigungen verfügt, wie z. B. die SnapCenter-Admin
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Der Nachrichtenwarteschlange-Service muss ausgeführt werden.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2012 oder höher für Microsoft Exchange Server".

Über diese Aufgabe

- Sie können einen SnapCenter-Server nicht als Plug-in-Host zu einem anderen SnapCenter-Server hinzufügen.
- Sie können einen Host hinzufügen und Plug-in-Pakete für einen einzelnen Host oder Cluster installieren.
- Ist ein Exchange-Knoten Teil einer DAG, kann der SnapCenter-Server nicht nur einen Knoten hinzufügen.
- Wenn Sie Plug-ins auf einem Cluster (Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert, selbst wenn einige Knoten keine Datenbanken auf NetApp LUNs haben.

Ab SnapCenter 4.6 unterstützt SCE die Mandantenfähigkeit und Sie können einen Host über die folgenden Methoden hinzufügen:

Fügen Sie einen Host-Vorgang hinzu	4.5 und früher	4.6 und höher
Fügen Sie IP-lose DAG in einer anderen Domäne oder anderen Domäne hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP-DAGs mit eindeutigen Namen hinzu. Diese befinden sich in derselben oder in mehreren Domänen	Unterstützt	Unterstützt
Fügen Sie mehrere IP- oder IP-lose DAGs mit denselben Host-Namen und/oder DB-Namen in Cross-Domain hinzu	Nicht unterstützt	Unterstützt
Hinzufügen mehrerer IP/IP-loser DAGs mit demselben Namen und domänenübergreifender	Nicht unterstützt	Unterstützt
Fügen Sie mehrere Standalone-Hosts mit demselben Namen und domänenübergreifender Infrastruktur hinzu	Nicht unterstützt	Unterstützt

Plug-in für Exchange hängt vom SnapCenter Plug-ins-Paket für Windows ab, die Versionen müssen identisch sein. Während der Installation von Plug-in für Exchange wird das SnapCenter Plug-ins Paket für Windows standardmäßig ausgewählt und zusammen mit dem VSS-Hardwareanbieter installiert.

Falls SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, Und Sie möchten Plug-in für Exchange auf demselben Exchange-Server installieren, müssen Sie den von SnapDrive für Windows verwendeten VSS Hardware-Anbieter deaktivieren, da er mit dem VSS Hardware Provider, der mit Plug-in für Exchange und SnapCenter Plug-ins Package für Windows installiert ist, nicht kompatibel ist. Weitere Informationen finden Sie unter "So registrieren Sie den Data ONTAP VSS Hardware Provider manuell".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Vergewissern Sie sich, dass **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie als Hosttyp * Windows* aus. SnapCenter Server fügt den Host hinzu und installiert dann auf dem Host das Plug-in für Windows und das Plug-in für Exchange, falls sie nicht bereits installiert sind. Plug-in für Windows und Plug-in für Exchange müssen die gleiche Version sein. Wenn zuvor eine andere Version des Plug-ins für Windows installiert wurde, aktualisiert SnapCenter die Version als Teil der Installation.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den vollständig qualifizierten Domänennamen (FQDN) einzugeben. Eine IP-Adresse wird nur für nicht vertrauenswürdige Domänenhosts unterstützt, wenn sie auf den FQDN auflöst. Wenn Sie einen Host mit SnapCenter hinzufügen und dieser Teil einer Unterdomäne ist, müssen Sie den FQDN angeben. Sie können IP-Adressen oder den FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Exchange DAG Vorteile einer Exchange DAG: ◦ Fügen Sie eine DAG hinzu, indem Sie den DAG-Namen, die DAG-IP-Adresse, den Node-Namen oder die Node-IP-Adresse angeben. ◦ Fügen Sie den DAG-Cluster ohne IP hinzu, indem Sie die IP-Adresse oder den FQDN eines der DAG-Cluster-Nodes angeben. ◦ Fügen Sie IP-lose DAG hinzu, die sich in derselben Domäne oder einer anderen Domäne befindet. Sie können auch mehrere IP/IP-basierte DAGs mit demselben Namen und aber verschiedenen Domänen hinzufügen. Für einen eigenständigen Host oder eine Exchange-DAG (domänenübergreifend oder gleiche Domäne) wird empfohlen, FQDN oder die IP-Adresse des Hosts oder der DAG bereitzustellen.

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

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

   Wenn Sie Plug-in für Exchange auswählen, wird das SnapCenter-Plug-in für Microsoft SQL Server automatisch deaktiviert. Microsoft empfiehlt, dass SQL Server und Exchange-Server aufgrund der verwendeten Speichermenge und anderer von Exchange benötigten Ressourcen nicht auf demselben System installiert werden.

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

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

Für dieses Feld…	Tun Sie das…
Installationspfad	Der Standardpfad ist `C:\Program Files\NetApp\SnapCenter`. Optional können Sie den Pfad anpassen.
Fügen Sie alle Hosts in der DAG hinzu	Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine DAG hinzufügen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: *Domainname\AccountName€*. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird der Host validiert, um zu bestimmen, ob er die Anforderungen für die Installation des Plug-ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden die entsprechenden Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit Speicherplatz oder RAM zusammenhängt, können Sie die Datei Web.config in WebApp aktualisieren `C:\Program Files\NetApp\SnapCenter` , 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. Überwachen Sie den Installationsfortschritt.

Installieren Sie das Plug-in für Exchange über den SnapCenter Server Host mithilfe von PowerShell Cmdlets

Sie sollten das Plug-in für Exchange über die SnapCenter-Benutzeroberfläche installieren. Wenn Sie die GUI nicht verwenden möchten, können Sie PowerShell Cmdlets auf dem SnapCenter Server Host oder auf einem Remote Host verwenden.

Bevor Sie beginnen

- SnapCenter-Server muss installiert und konfiguriert worden sein.
- Sie müssen ein lokaler Administrator auf dem Host oder ein Benutzer mit Administratorrechten sein.
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen Plug-in, Installation und Deinstallation verfügt, wie z. B. SnapCenter Admin
- Vor der Installation des Plug-ins für Exchange müssen Sie die Installationsanforderungen und die Typen der unterstützten Konfigurationen geprüft haben.
- Der Host, auf dem das Plug-in für Exchange installiert werden soll, muss ein Windows-Host sein.

Schritte

1. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, und geben Sie dann Ihre Anmeldeinformationen ein.
2. Fügen Sie den Host hinzu, auf dem Sie das Plug-in für Exchange installieren möchten, mit dem Cmdlet *Add-SmHost* mit den erforderlichen Parametern.

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

   Es kann sich dabei um einen Standalone-Host oder eine DAG handeln. Wenn Sie eine DAG angeben, ist der Parameter *-IsDAG* erforderlich.

3. Installieren Sie das Plug-in für Exchange mit dem Cmdlet *Install-SmHostPackage* mit den erforderlichen Parametern.

   Dieser Befehl installiert das Plug-in für Exchange auf dem angegebenen Host und registriert dann das Plug-in mit SnapCenter.

Installieren Sie das SnapCenter Plug-in für Exchange im Hintergrund über die Befehlszeile

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

Bevor Sie beginnen

- Sie müssen Ihre Microsoft Exchange Server-Ressourcen gesichert haben.
- Sie müssen die SnapCenter-Plug-in-Pakete installiert haben.
- Vor der Installation müssen Sie die frühere Version des SnapCenter-Plug-ins für Microsoft SQL Server löschen.

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

Schritte

1. Überprüfen Sie, ob der Ordner *C:\temp* auf dem Plug-in-Host vorhanden ist und der angemeldete Benutzer vollständigen Zugriff darauf hat.

2. Laden Sie das SnapCenter Plug-in für Microsoft Windows von *C:\ProgramData\NetApp\SnapCenter\Paket* Repository herunter.

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

3. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-in installieren möchten.
4. Navigieren Sie von einer Windows-Eingabeaufforderung auf dem lokalen Host zum Verzeichnis, in das Sie die Plug-in-Installationsdateien gespeichert haben.
5. Geben Sie den folgenden Befehl ein, um das Plug-in zu installieren.

   _Snapcenter_Windows_Host_Plugin.exe"/silent /debuglog“<Debug_Log_Path>“ /log“<Log_Path>“ BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR=“<Install_Directory_Path>“ BI_SERVICEACCOUNT=<Domain\<Administrator> BI_SERVICECEPWD= SCHEICE= SCHEINSW

   Beispiel:

   _C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_Windows_Host_Plugin.exe“/silent /debuglog„C:\HPPW_SCSQL_Install.log“ /log„C:\temp“ BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR=„C:\Programme\NetApp\\BI_SERVICECOUNT,SPERW_Administrator,SPEICEICE_DER_DER_SPREN,SnapCenter,SCEICEICEICHTE_DER_DER_DER_DER_Administrator_SPREN,SPREN

   Alle während der Installation von Plug-in für Exchange übergebenen Parameter gelten bei der Groß-/Kleinschreibung.

   Geben Sie die folgenden Werte für die Variablen ein:

Variabel	Wert
/Debuglog“<Debug_Log_Path>	Geben Sie den Namen und den Speicherort der Protokolldatei für das Installationsprogramm der Suite an, wie im folgenden Beispiel: *Setup.exe /debuglog„C:\PathToLog\setupexe.log*
BI_SNAPCENTER_PORT	Geben Sie den Port an, auf dem SnapCenter mit SMCore kommuniziert.
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis für das Host-Plug-in-Paket an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter-Plug-in für das Web-Service-Konto von Microsoft Windows an.
BI_SERVICEPWD	Geben Sie das Passwort für das SnapCenter-Plug-in für das Microsoft Windows-Webservice-Konto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host implementiert werden soll.

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

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

Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

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

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange

Schritte

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat

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

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

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

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

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

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

Importieren von CA-Zertifikaten

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

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

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

Abrufen des Daumenabdrucks für das CA-Zertifikat

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

Schritte

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

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

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

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

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

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

Schritte

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

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

   Beispiel:

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

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

   Beispiel:

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

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nachdem Sie fertig sind

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

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

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

Konfigurieren Sie SnapManager 7.x für Exchange und SnapCenter, um koexistieren zu können

Damit das SnapCenter Plug-in für Microsoft Exchange Server gemeinsam mit SnapManager für Microsoft Exchange Server eingesetzt werden kann, müssen Sie das SnapCenter Plug-in für Microsoft Exchange Server auf demselben Exchange Server installieren, auf dem SnapManager für Microsoft Exchange Server installiert ist, indem Sie die Zeitpläne für SnapManager für Exchange deaktivieren. Und neue Zeitpläne und Backups mit dem SnapCenter Plug-in für Microsoft Exchange Server konfigurieren.

Bevor Sie beginnen

- SnapManager für Microsoft Exchange Server und SnapDrive für Windows sind bereits installiert und Backups von SnapManager für Microsoft Exchange Server sind im System und im SnapInfo Verzeichnis vorhanden.
- Sie sollten die von SnapManager für Microsoft Exchange Server erstellten Backups gelöscht oder zurückgewonnen haben, die Sie nicht mehr benötigen.
- Sie sollten alle Zeitpläne ausgesetzt oder gelöscht haben, die von SnapManager für Microsoft Exchange Server aus dem Windows-Scheduler erstellt wurden.
- Das SnapCenter Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server können parallel auf demselben Exchange Server eingesetzt werden. Sie können jedoch kein Upgrade von bestehenden SnapManager für Microsoft Exchange Server Installationen auf SnapCenter durchführen.

  SnapCenter bietet keine Upgrade-Option.

- SnapCenter unterstützt nicht die Wiederherstellung von Exchange Datenbanken aus SnapManager für Microsoft Exchange Server Backups.

  Wenn Sie SnapManager für Microsoft Exchange Server nach der Installation des SnapCenter Plug-ins für Microsoft Exchange Server nicht deinstallieren und später ein Backup von SnapManager für Microsoft Exchange Server wiederherstellen möchten, müssen Sie weitere Schritte durchführen.

Schritte

1. Bestimmen Sie mithilfe von PowerShell auf allen DAG-Knoten, ob der SnapDrive für Windows VSS Hardware Provider registriert ist: *Vssadmin list Providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
   Version: 7. 1. 4. 6845
```

2. Aus dem SnapDrive-Verzeichnis den VSS Hardware Provider von SnapDrive für Windows: *navssprv.exe -r Service -U*
3. Überprüfen Sie, ob der VSS Hardware Provider entfernt wurde: *Vssadmin list Providers*
4. Fügen Sie den Exchange Host zu SnapCenter hinzu, und installieren Sie dann das SnapCenter Plug-in für Microsoft Windows und das SnapCenter Plug-in für Microsoft Exchange Server.
5. Überprüfen Sie im SnapCenter-Plug-in für Microsoft Windows-Verzeichnis auf allen DAG-Knoten, ob der VSS-Hardwareanbieter registriert ist: *Vssadmin list Providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. Beenden Sie die Backup-Zeitpläne für SnapManager für Microsoft Exchange Server.
7. Erstellen Sie über die GUI von SnapCenter On-Demand-Backups, konfigurieren Sie geplante Backups und konfigurieren Sie Aufbewahrungseinstellungen.
8. Deinstallieren Sie SnapManager für Microsoft Exchange Server.

   Wenn Sie SnapManager für Microsoft Exchange Server nicht jetzt deinstallieren und später ein Backup von SnapManager für Microsoft Exchange Server wiederherstellen möchten:

   a. Heben Sie das SnapCenter Plug-in für Microsoft Exchange Server von allen DAG-Knoten auf: *navssprv.exe -r Service -U*

      ```
      C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
      Windows>navssprv.exe -r service -u
      ```

   b. Aus dem Verzeichnis *C:\Programme\NetApp\SnapDrive* registrieren Sie SnapDrive für Windows auf allen DAG Knoten: *navssprv.exe -r Service -a hostname\\username -p password*

Installieren Sie das SnapCenter Plug-in für VMware vSphere

Wenn Ihre Datenbank oder Ihr Dateisystem auf virtuellen Maschinen (VMs) gespeichert ist oder Sie VMs und Datastores schützen möchten, müssen Sie das virtuelle SnapCenter-Plug-in für VMware vSphere-Gerät bereitstellen.

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

Informationen zum Konfigurieren des CA-Zertifikats mit SnapCenter-Plug-in für VMware vSphere finden Sie unter "Erstellen oder importieren Sie ein SSL-Zertifikat".

Konfigurieren Sie die CRL-Datei

Das SnapCenter Plug-in für VMware vSphere sucht die CRL-Dateien in einem vorkonfigurierten Verzeichnis. Das Standardverzeichnis der CRL-Dateien für das SnapCenter Plug-in für VMware vSphere ist */opt/netapp/config/crl*.

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

Bereiten Sie sich auf die Datensicherung vor

Bevor Sie Datensicherungsvorgänge wie Backup-, Klon- oder Restore-Vorgänge durchführen, müssen Sie Ihre Strategie definieren und die Umgebung festlegen. Sie können den SnapCenter Server auch zur Verwendung von SnapMirror und SnapVault Technologie einrichten.

Um von der SnapVault und SnapMirror Technologie zu profitieren, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes auf dem Storage-Gerät konfigurieren und initialisieren. Sie können entweder NetApp System Manager verwenden oder die Storage-Konsole verwenden, um diese Aufgaben auszuführen.

Weitere Informationen

"Erste Schritte mit der REST API"

Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für Microsoft Exchange Server

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

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

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

- Fügen Sie Hosts hinzu, installieren Sie das SnapCenter Plug-in für Microsoft Windows und das SnapCenter Plug-in für Microsoft Exchange Server und ermitteln Sie die Ressourcen (aktualisieren).
- Führen Sie die Host-seitige Storage-Bereitstellung mit dem SnapCenter Plug-in für Microsoft Windows durch.
- Wenn Sie SnapCenter Server zum Schutz von Exchange Datenbanken verwenden, die sich auf VMware RDM LUNs befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren. Die Dokumentation zum SnapCenter Plug-in für VMware vSphere enthält weitere Informationen.

  VMDKs werden nicht unterstützt.

- Verschieben Sie eine vorhandene Microsoft Exchange Server-Datenbank von einem lokalen Laufwerk auf unterstützten Speicher mithilfe von Microsoft Exchange-Tools.
- Richten Sie SnapMirror- und SnapVault-Beziehungen ein, falls Sie eine Backup-Replizierung möchten.

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für SnapCenter 4.3.x-Anwender enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Filesysteme mithilfe des Linux-basierten SnapCenter Plug-ins für VMware vSphere Virtual Appliance (Open Virtual Appliance Format).

"Dokumentation zum SnapCenter Plug-in für VMware vSphere"

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

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit den durchzustellenden Backup-, Restore- und erneuten Seeding-Operationen zu verstehen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind typischerweise Mailbox-Datenbanken oder Microsoft Exchange Database Availability Group (DAG), die Sie mit SnapCenter sichern.
- Eine SnapCenter Ressourcengruppe ist eine Ansammlung von Ressourcen auf einem Host oder einer Exchange DAG, und die Ressourcengruppe kann entweder eine ganze DAG oder einzelne Datenbanken enthalten.

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

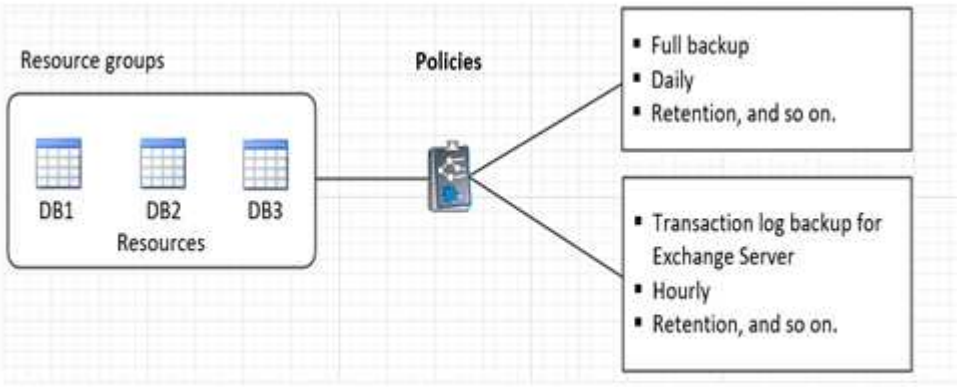
  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

  Die Ressourcengruppen wurden früher als Datensätze bezeichnet.

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

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

Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts enthält. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass sie täglich ein vollständiges Backup durchführt, und einen anderen Zeitplan, der stündlich Protokoll-Backups durchführt. Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



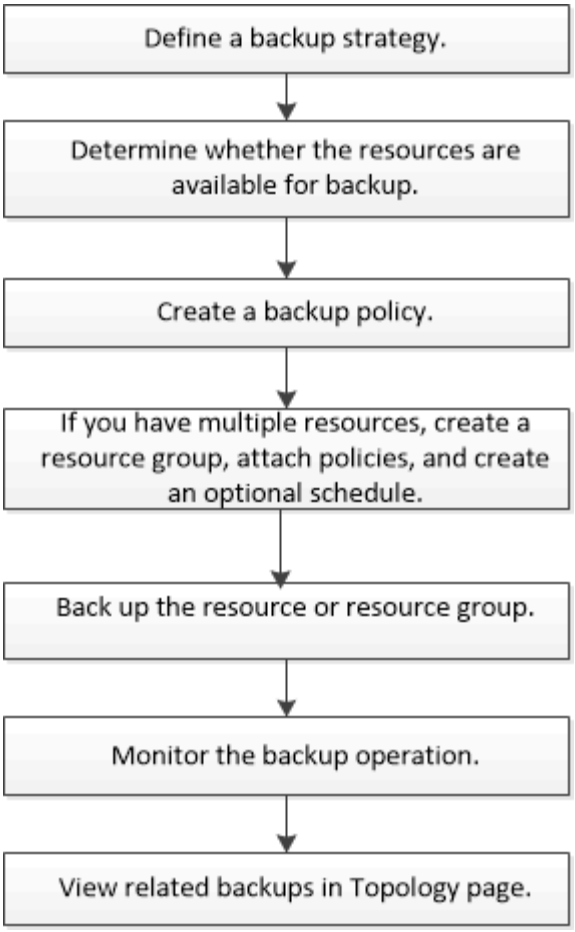
Exchange-Ressourcen sichern

Backup-Workflow

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

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden. Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden. Aktive und passive Backup-Kopien auf demselben Volume werden nicht unterstützt.

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



Exchange Datenbank und Backup-Verifizierung

Das SnapCenter Plug-in für Microsoft Exchange Server bietet keine Backup-Überprüfung. Sie können jedoch das mit Exchange zur Verfügung gestellte Eseutil Tool verwenden, um Exchange-Datenbanken und Backups zu überprüfen.

Das Microsoft Exchange Eseutil Tool ist ein Befehlszeilen-Dienstprogramm, das in Ihrem Exchange Server enthalten ist. Das Dienstprogramm ermöglicht die Durchführung von Konsistenzprüfungen zur Überprüfung der Integrität von Exchange-Datenbanken und Backups.

Best Practice: Es ist nicht erforderlich, Konsistenzprüfungen auf Datenbanken durchzuführen, die Teil einer Database Availability Group (DAG) Konfiguration mit mindestens zwei Replikaten sind.

Weitere Informationen finden Sie unter "Microsoft Exchange Server-Dokumentation".

Bestimmen Sie, ob Exchange Ressourcen für Backups verfügbar sind

Ressourcen sind die Datenbanken, Exchange Database Availability Groups, die von den von Ihnen installierten Plug-ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsjobs ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie zur Verfügung haben. Das ermitteln der verfügbaren Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen, das Hinzufügen von Anmeldeinformationen und das Installieren des Plug-ins für Exchange.
- Um die Funktionen der Single Mailbox Recovery Software nutzen zu können, müssen Sie Ihre aktive Datenbank auf dem Exchange Server befinden, wo die Single Mailbox Recovery Software installiert ist.
- Wenn Datenbanken auf VMware RDM LUNs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in bei SnapCenter registrieren. Das "Dokumentation zum SnapCenter Plug-in für VMware vSphere" hat weitere Informationen.

Über diese Aufgabe

- Datenbanken können nicht gesichert werden, wenn die Option **Gesamtstatus** auf der Seite Details auf nicht verfügbar für Backups eingestellt ist. Die Option **Gesamtstatus** ist für die Sicherung auf nicht verfügbar eingestellt, wenn eine der folgenden Optionen zutrifft:
  - Datenbanken sind nicht auf einer NetApp LUN.
  - Datenbanken befinden sich nicht im normalen Zustand.

    Datenbanken befinden sich nicht im normalen Zustand, wenn sie sich im Mount-, Unmount-, erneutes Seeding oder Recovery-Wartezustand befinden.
- Wenn Sie über eine Datenbankverfügbarkeitsgruppe (DAG) verfügen, können Sie alle Datenbanken in der Gruppe sichern, indem Sie den Sicherungsauftrag von der DAG ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann in der Dropdown-Liste Plug-ins in der oberen linken Ecke der Seite Ressourcen * Microsoft Exchange Server* aus.
2. Wählen Sie auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** die Option **Datenbank**, oder **Database Availability Group** oder **Ressourcengruppe** aus.

   Alle Datenbanken und DAGs werden mit ihren DAG- oder Hostnamen im FQDN-Format angezeigt, sodass Sie zwischen mehreren Datenbanken unterscheiden können.

   Klicken Sie auf , und wählen Sie den Hostnamen und den Exchange Server aus, um die Ressourcen zu filtern. Sie können dann klicken , um den Filterbereich zu schließen.
3. Klicken Sie Auf **Ressourcen Aktualisieren**.

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

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

   Die Ressourcen werden zusammen mit Informationen wie Ressourcenname, Name der Datenbankverfügbarkeitsgruppe, Server, auf dem sich die Datenbank zurzeit befindet, Server mit Kopien, Zeitpunkt des letzten Backups und Gesamtstatus angezeigt.
   - Wenn sich die Datenbank auf einem Speicher außerhalb von NetApp befindet, wird in der Spalte Status insgesamt kein Backup verfügbar angezeigt.

     Wenn sich in einer DAG die aktive Datenbankkopie auf einem Storage anderer Anbieter befindet und

mindestens eine passive Datenbankkopie auf NetApp Storage ist, wird in der Spalte **Gesamtstatus** nicht geschützt angezeigt.

Sie können keine Datensicherungsvorgänge für eine Datenbank ausführen, die sich auf einem Storage-Typ außerhalb von NetApp befindet.

- Wenn sich die Datenbank auf NetApp Storage befindet und nicht geschützt ist, wird sie in der Spalte **Gesamtstatus** nicht geschützt angezeigt.
- Wenn sich die Datenbank auf einem NetApp Storage System befindet und geschützt ist, zeigt die Benutzeroberfläche die Meldung Backup not run in der Spalte **Gesamtstatus** an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist und das Backup für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche die Meldung Sicherung erfolgreich in der Spalte **Gesamtstatus** an.

Erstellen von Backup-Richtlinien für Exchange Server-Datenbanken

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

Bevor Sie beginnen

- Sie müssen Ihre Datensicherungsstrategie definiert haben.

  Weitere Informationen finden Sie in den Informationen zur Definition einer Datensicherungsstrategie für Exchange Datenbanken.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Storage-System abschließen.
- Sie müssen die Exchange Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss der SnapCenter Administrator Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.
- Wenn Sie die PowerShell-Skripte in Verordnungen und Postskripten ausführen möchten, sollten Sie den Wert des Parameters in der Datei auf true setzen `usePowershellProcessforScripts` `web.config` .

  Der Standardwert ist false

Über diese Aufgabe

- Eine Backup-Richtlinie ist eine Reihe von Regeln, die festlegen, wie Backups gemanagt und aufbewahrt werden und wie oft die Ressourcen- oder Ressourcengruppe gesichert wird. Außerdem können Sie Skripteinstellungen festlegen. Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.
- Eine vollständige Backup-Aufbewahrung ist spezifisch für eine bestimmte Richtlinie. Eine Datenbank oder Ressource, die Richtlinien A mit einer vollständigen Backup-Aufbewahrung von 4 verwendet, behält 4 volle Backups bei und hat keine Auswirkungen auf Richtlinie B für die gleiche Datenbank oder Ressource, die möglicherweise eine Aufbewahrung von 3 haben, um 3 vollständige Backups aufzubewahren.

- Die Backup-Aufbewahrung von Protokollen ist über alle Richtlinien hinweg wirksam und wird für alle Backup-Protokollierung einer Datenbank oder Ressource angewendet. Wenn ein vollständiges Backup mit Richtlinie B durchgeführt wird, wirkt sich die Einstellung für die Protokollaufbewahrung auf die von Richtlinie A erstellten Protokoll-Backups in derselben Datenbank oder Ressource aus. Ebenso wirkt sich die Einstellung für die Protokollaufbewahrung für Policy A auf die von Richtlinie B erstellten Protokoll-Backups in derselben Datenbank aus.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

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

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

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

  Best Practice: Es ist am besten, dass Sie die sekundäre Aufbewahrungsrichtlinie auf der Grundlage der Anzahl der vollständigen und Log-Backups insgesamt konfigurieren, die Sie behalten möchten. Wenn Sie sekundäre Aufbewahrungsrichtlinien konfigurieren, beachten Sie, dass bei Datenbanken und Protokollen, die sich auf verschiedenen Volumes befinden, jedes Backup drei Snapshots haben kann. Wenn sich Datenbanken und Protokolle auf demselben Volume befinden, kann jedes Backup zwei Snapshots haben.

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.

    Wenn Sie eine Snapshot-Sperrfrist festlegen, wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.

    Bei ONTAP 9.12.1 und älteren Versionen übernehmen die über die SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

  Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritte

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

   a. Wählen Sie den Sicherungstyp:

Ihr Ziel ist	Tun Sie das…
Sichern Sie die Datenbankdateien und die erforderlichen Transaktions-Logs	Wählen Sie **Vollbackup und Log Backup** aus. Datenbanken werden durch Log-Verkürzung gesichert und alle Protokolle werden gesichert, einschließlich der gekürzten Protokolle. Dies ist der empfohlene Backup-Typ.
Sichern Sie die Datenbankdateien und die nicht gesicherten Transaktionsprotokolle	Wählen Sie * Vollbackup* aus. Datenbanken werden durch Log-Verkürzung gesichert, gekürzte Protokolle werden nicht gesichert.
Sichern Sie alle Transaktions-Logs	Wählen Sie **Backup protokollieren**. Alle Transaktions-Logs auf dem aktiven File-System werden gesichert, und es gibt keine Log-Verkürzung. Ein Verzeichnis *sceBackupinfo* wird auf derselben Festplatte erstellt wie das Live Log. Dieses Verzeichnis enthält den Zeiger auf die inkrementellen Änderungen für die Exchange-Datenbank und entspricht nicht den vollständigen Log-Dateien.
Sichern Sie alle Datenbank- und Transaktions-Logs, ohne die Transaktions-Log-Dateien zu beeinträchtigen	Wählen Sie **Backup Kopieren**. Alle Datenbanken und Protokolle werden gesichert, und es gibt keine Log-Verkürzung. In der Regel verwenden Sie diesen Backup-Typ für das erneutes Seeding einer Kopie oder zum Testen oder zur Diagnose eines Problems.

Sie sollten den für die Protokoll-Backups benötigten Speicherplatz basierend auf der vollständigen Backup-Aufbewahrung definieren, nicht auf der Grundlage einer up-to-the-minute-Aufbewahrung (UTM).

Erstellen Sie beim Umgang mit Exchange Volumes (LUNs) separate Vault-Richtlinien für Protokolle und Datenbanken, und setzen Sie die Keep (Retention) für die Protokollrichtlinie auf die doppelte Anzahl für jedes Label wie die Datenbankrichtlinie unter Verwendung derselben Labels. Weitere Informationen finden Sie unter: "Bei Backups mit SnapCenter für Exchange wird nur die Hälfte der Snapshots auf dem Ziel-Log-Volume von Vault gespeichert"

b. Wählen Sie im Abschnitt Einstellungen für Datenbankverfügbarkeitsgruppen eine Aktion aus:

Für dieses Feld…	Tun Sie das…
Sichern Sie aktive Kopien	Wählen Sie diese Option aus, um nur die aktiven Kopien der ausgewählten Datenbank zu sichern. Bei Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAGs) werden mit dieser Option nur aktive Kopien aller Datenbanken in der DAG gesichert. Passive Kopien werden nicht gesichert.
Sichern Sie Kopien auf Servern, die zum Erstellungszeitpunkt des Backup-Jobs ausgewählt werden sollen	Wählen Sie diese Option aus, um alle Kopien der Datenbanken auf den ausgewählten Servern zu sichern, sowohl aktiv als auch passiv. Bei DAGs sichert diese Option sowohl aktive als auch passive Kopien aller Datenbanken auf den ausgewählten Servern.

Bei Cluster-Konfigurationen werden die Backups entsprechend den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Node des Clusters aufbewahrt. Wenn sich der Owner-Node des Clusters ändert, werden die Backups des vorherigen Owner-Node beibehalten. Die Aufbewahrung gilt nur auf Node-Ebene.

c. Wählen Sie im Abschnitt Terminfrequenz einen oder mehrere der Frequenztypen aus: **On Demand**, **hourly**, **Daily**, **Weekly** und **Monthly**.

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

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

6. Konfigurieren Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen.

   Die angezeigten Optionen hängen vom Backup-Typ und vom Frequenztyp ab, den Sie zuvor ausgewählt haben.

Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.

Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

a. Wählen Sie im Abschnitt Einstellungen für die Aufbewahrung von Protokollsicherungen eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Bewahren Sie nur eine bestimmte Anzahl von Protokoll-Backups auf	Wählen Sie **Anzahl der vollständigen Backups, für die Protokolle aufbewahrt werden**, und geben Sie die Anzahl der vollständigen Backups an, für die Sie eine zeitnahe Wiederherstellung wünschen. Die up-to-the-minute (UTM) Aufbewahrung gilt für die Protokollierung der Backups, die über vollständige Backups oder das Log-Backup erstellt wurden. Wenn die UTM-Aufbewahrungseinstellungen beispielsweise so konfiguriert sind, dass die Protokollsicherungen der letzten 5 vollständigen Backups gespeichert werden, werden die Protokoll-Backups der letzten 5 vollständigen Backups beibehalten. Die im Rahmen der vollständigen und der Log-Backups erstellten Protokollordner werden automatisch als Teil von UTM gelöscht. Sie können die Protokollordner nicht manuell löschen. Wenn z. B. die Aufbewahrungseinstellung für vollständige oder vollständige Backup und Log-Sicherung für einen Monat festgelegt ist und die UTM-Aufbewahrung auf 10 Tage festgelegt ist, wird der im Rahmen dieser Backups erstellte Log-Ordner wie pro UTM gelöscht. Dadurch sind nur 10 Tage Protokollordner vorhanden und alle anderen Backups sind für die Point-in-Time-Wiederherstellung markiert. Sie können den UTM-Aufbewahrungswert auf 0 einstellen, wenn Sie keine minutengenaue Wiederherstellung durchführen möchten. Dies ermöglicht den Point-in-Time Restore-Vorgang. **Best Practice:** Es ist am besten, dass die Einstellung gleich der Einstellung für Total Snapshots (Full Backups) im Abschnitt Full Backup Retention Settings sein muss. Dadurch wird sichergestellt, dass Protokolldateien für jedes vollständige Backup aufbewahrt werden.

Ihr Ziel ist	Tun Sie das…
Bewahren Sie die Backup-Kopien für eine bestimmte Anzahl von Tagen auf	Wählen Sie die Option **Protokollsicherungen für letzte** aufbewahren und geben Sie die Anzahl der Tage an, um die Backup-Kopien des Protokolls zu behalten. Aufbewahrung der Log-Backups bis zur Anzahl von Tagen voller Backups.
Sperrfrist von Snapshots	Wählen Sie **Sperrfrist der Snapshot-Kopie** aus und wählen Sie Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

Wenn Sie als Backup-Typ **Log Backup** ausgewählt haben, werden Log-Backups als Teil der up-to-the-minute-Aufbewahrungseinstellungen für vollständige Backups beibehalten.

b. Wählen Sie im Abschnitt Einstellungen für vollständige Backups eine der folgenden Optionen für On-Demand-Backups aus, und wählen Sie dann eine für vollständige Backups aus:

Für dieses Feld…	Tun Sie das…
Bewahren Sie nur eine bestimmte Anzahl von Snapshots auf	Wenn Sie die Anzahl der vollständigen Backups angeben möchten, die beibehalten werden sollen, wählen Sie die Option **Total Snapshot Copies to keep** aus, und geben Sie die Anzahl der Snapshots (Full Backups) an, die beibehalten werden sollen. Wenn die Anzahl der vollständigen Backups die angegebene Anzahl überschreitet, werden die vollständigen Backups, die die angegebene Anzahl überschreiten, gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.
Bewahren Sie vollständige Backups für eine bestimmte Anzahl an Tagen auf	Wählen Sie die Option **Snapshot Kopien behalten für** und geben Sie die Anzahl der Tage an, die Snapshots behalten werden sollen (vollständige Backups).
Sperrfrist von Snapshots	Wählen Sie **Sperrfrist der Snapshot-Kopie** aus und wählen Sie Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

Wenn Sie eine Datenbank mit nur Protokollsicherungen und keinen vollständigen Backups auf einem Host in einer DAG-Konfiguration haben, werden die Protokoll-Backups auf folgende Weise beibehalten:

- Standardmäßig findet SnapCenter auf allen anderen Hosts in der DAG das älteste volle Backup dieser Datenbank und löscht alle Log-Backups auf diesem Host, die vor dem vollständigen Backup erstellt wurden.
- Sie können das oben genannte Standard-Aufbewahrungsverhalten für eine Datenbank auf einem Host in einer DAG mit nur Protokoll-Backups überschreiben, indem Sie den Schlüssel **MaxLogBackupOnlyCountWithfullBackup** in der Datei *C:\Programme\NetApp\SnapCenter WebApp\Web.config* hinzufügen.

  ```
  <add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
  ```

  Im Beispiel bedeutet der Wert 10, dass Sie bis zu 10 Log-Backups auf dem Host aufbewahren.

7. Wählen Sie auf der Seite Replikation eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Siehe "Zeigen Sie Exchange-Backups auf der Seite Topologie an".	Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu behalten.
Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.

Für dieses Feld…	Tun Sie das…
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

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

8. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Backup ausgeführt werden sollen.
   - Zu den vorkript-Backup-Argumenten gehören „` USD Datenbank`“ und „` USD ServerInstance`“.
   - Zu den PostScript-Backup-Argumenten gehören „` USD Datenbank`“, „` USD ServerInstance`“, „` USD BackupName`“, „` USD LogDirectory`“ und „` USD LogSnapshot`“.

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

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

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Exchange-Server

Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des zu erfütienden Datenschutzauftrags und den Schutzzeitplan zu definieren.

Über diese Aufgabe

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

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

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Microsoft Exchange Server-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Datenbank** aus.

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

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

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

5. Führen Sie auf der Seite Ressourcen die folgenden Schritte aus:
   a. Wählen Sie in den Dropdown-Listen den Ressourcentyp und die Datenbankverfügbarkeitsgruppe aus, um die Liste der verfügbaren Ressourcen zu filtern.

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

      In den Abschnitten Verfügbare Ressourcen und ausgewählte Ressourcen wird der Datenbankname mit dem FQDN des Hosts angezeigt. Dieser FQDN gibt nur an, dass die Datenbank auf diesem spezifischen Host aktiv ist und möglicherweise keine Sicherungskopie auf diesem Host erstellt. Wählen Sie einen oder mehrere Backup-Server aus der Serverauswahl aus, wo Sie eine Sicherung erstellen möchten, falls Sie in der Richtlinie die Option **Sicherungskopien auf Servern ausgewählt haben, die bei der Erstellung von Sicherungsjobs** ausgewählt werden sollen.

   b. Geben Sie den Namen der Ressource in das Suchfeld ein, oder scrollen Sie, um nach einer Ressource zu suchen.
   c. Führen Sie einen der folgenden Schritte aus, um Ressourcen aus dem Abschnitt Verfügbare Ressourcen in den Abschnitt Ausgewählte Ressourcen zu verschieben:
      - Wählen Sie **Automatische Auswahl aller Ressourcen auf demselben Speichervolumen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
      - Wählen Sie im Abschnitt „Verfügbare Ressourcen“ die Ressourcen aus, und klicken Sie dann auf den Pfeil nach rechts, um sie in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.

        Ressourcengruppen von SnapCenter für Microsoft Exchange Server dürfen nicht mehr als 30 Datenbanken pro Snapshot enthalten. Wenn mehr als 30 Datenbanken in einer Ressourcengruppe vorhanden sind, wird ein zweiter Snapshot für die zusätzlichen Datenbanken erstellt. Deshalb werden 2 Unterjobs unter dem Hauptsicherungsjob erzeugt. Für Backups mit sekundärer Replikation, während SnapMirror oder SnapVault Update läuft, kann es Szenarien geben, in denen sich das Update für die beiden Unterjobs überlappen. Der wichtigste Backup-Job läuft dauerhaft, auch wenn die Protokolle darauf hindeuten, dass der Job abgeschlossen ist.

6. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

      Wenn eine Richtlinie die Option **Sicherungskopien auf Servern enthält, die bei der Erstellung von Sicherungsjobs** ausgewählt werden sollen, wird eine Serverauswahloption angezeigt, die einen oder mehrere Server auswählt. Die Serverauswahl-Option listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf dem NetApp Storage befindet.

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

   b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies auf * **in der Spalte *Configure Schedules** für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

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

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

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

7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   Für E-Mail-Benachrichtigungen müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl angegeben haben `Set-SmSmtpServer`.

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

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

Backup von Exchange Datenbanken

Wenn eine Datenbank nicht Teil einer Ressourcengruppe ist, können Sie die Datenbank oder die Datenbankverfügbarkeitsgruppe auf der Seite Ressourcen sichern.

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Sie müssen das Aggregat, das vom Backup-Vorgang verwendet wird, der SVM zugewiesen haben, die von der Datenbank verwendet wird.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Wenn Sie ein Backup einer Datenbank oder einer Database Availability Group durchführen möchten, die über eine aktiv/Passiv-Datenbankkopie auf NetApp Storage und Storage anderer Anbieter verfügt, Und Sie haben **aktive Kopien sichern** oder **Sicherungskopien auf Servern ausgewählt, die während der Erstellung von Sicherungsaufträgen ausgewählt werden sollen** Option in der Richtlinie wird der Sicherungsauftrag in den Warnstatus versetzt. Das Backup führt erfolgreich eine aktive/passive Datenbankkopie auf NetApp Storage durch und ein Backup schlägt fehl bei der aktiv/passiven Datenbankkopie auf Storage anderer Anbieter.

  Best Practice: führen Sie keine Backups aktiver und passiver Datenbanken gleichzeitig aus. Es kann zu einem Wettlauf kommen, und eine der Sicherungen schlägt möglicherweise fehl.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das **Microsoft Exchange Server Plug-in** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder **Datenbank** oder **Datenbank-Verfügbarkeitsgruppe** aus der Liste **Ansicht** aus.

   Auf der Seite „Ressourcen“ gibt das Symbol an, dass sich die Datenbank auf Storage anderer Anbieter befindet.

   Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Storage anderer Anbieter befindet und mindestens eine passive Datenbankkopie auf einem NetApp Storage gespeichert ist, können Sie die Datenbank schützen.

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

- Wenn Sie eine Datenbank sichern möchten, klicken Sie auf den Datenbanknamen.
  a. Wenn die Topologieansicht angezeigt wird, klicken Sie auf **schützen**.
  b. Wenn der Assistent „Datenbank – Ressourcen schützen“ angezeigt wird, fahren Sie mit Schritt 3 fort.
- Wenn Sie eine Datenbankverfügbarkeitsgruppe sichern möchten, klicken Sie auf den Namen der Datenbankverfügbarkeitsgruppe.
  a. Wenn Sie einen benutzerdefinierten Snapshot-Namen angeben möchten, aktivieren Sie auf der Seite Ressourcen das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden**, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

     Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

  b. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
     i. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

     Wenn eine Richtlinie die Option **Sicherungskopien auf Servern enthält, die bei der Erstellung von Sicherungsjobs** ausgewählt werden sollen, wird eine Serverauswahloption angezeigt, die einen oder mehrere Server auswählt. Die Serverauswahl-Option listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf einem NetApp Storage befindet.

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

  c. Klicken Sie in der Spalte Zeitpläne konfigurieren auf die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
  d. Konfigurieren Sie im Fenster Add Schedules for Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

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

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt. . Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

+ Sie müssen außerdem die E-Mail-Adressen des Absenders und Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des auf der Ressource durchgeführten Sicherungsvorgangs anhängen möchten, wählen Sie **Job-Bericht anhängen**.

+ HINWEIS: Für E-Mail-Benachrichtigungen müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl Set-SmtpServer angegeben haben.

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

   Die Seite der Datenbanktopologie wird angezeigt.

ii. Klicken Sie auf **Jetzt sichern**.

iii. Führen Sie auf der Seite Backup die folgenden Schritte aus:

e. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

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

f. Klicken Sie Auf **Backup**.

   i. Überwachen Sie den Fortschritt des Backups, indem Sie im Aktivitätsbereich unten auf der Seite auf den Job doppelklicken, um die Seite „Jobdetails“ anzuzeigen.

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

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

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

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

Sichern von Exchange-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG, und die Ressourcengruppe kann entweder eine vollständige DAG oder individuelle Datenbanken enthalten. Sie können die Ressourcengruppen auf der Seite Ressourcen sichern.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Sie müssen das Aggregat, das vom Backup-Vorgang verwendet wird, der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts enthält, kann der Backup-Vorgang bei einigen Hosts aufgrund von Netzwerkproblemen zu spät beginnen. Sie sollten den Wert von in mit dem PowerShell Cmdlet konfigurieren `MaxRetryForUninitializedHosts` `web.config` `Set-SmConfigSettings` .
- Wenn Sie in einer Ressourcengruppe eine Datenbank- oder Database Availability Group mit aktiver/passiver Datenbankkopie auf einem NetApp Storage und nicht-NetApp Storage einschließen, und Sie haben **aktive Kopien sichern** oder **Sichern von Kopien auf Servern ausgewählt, die während der Erstellung von Sicherungsjobs ausgewählt werden sollen**-Option in der Richtlinie, Dann werden die Sicherungsjobs in den Warnstatus gehen.

  Das Backup führt erfolgreich eine aktive/passive Datenbankkopie auf NetApp Storage durch und ein Backup schlägt fehl bei der aktiv/passiven Datenbankkopie auf Storage anderer Anbieter.

Über diese Aufgabe

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das **Microsoft Exchange Server Plug-in** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf , klicken und dann das Tag auswählen. Sie können dann klicken , um den Filterbereich zu schließen.
3. Wählen Sie auf der Seite Ressourcengruppen die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

   b. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Backups, indem Sie im Aktivitätsbereich unten auf der Seite auf den Job doppelklicken, um die Seite „Jobdetails“ anzuzeigen.

Erstellen Sie eine Storage-Systemverbindung und Zugangsdaten mit PowerShell cmdlets für Exchange Server

Bevor Sie PowerShell cmdlets verwenden können, müssen Sie eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, um ein Backup und eine Wiederherstellung durchzuführen.

Bevor Sie beginnen

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

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

- Speichersystemnamen sollten eindeutig sein.

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

Schritte

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

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

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

2. Erstellen Sie mit dem Cmdlet eine neue Verbindung zum Speichersystem `Add-SmStorageConnection` .

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

3. Erstellen Sie mit dem Cmdlet ein neues Run As-Konto `Add-Credential` .

   In diesem Beispiel wird ein neuer Lauf als Konto mit dem Namen ExchangeAdmin mit Windows-Anmeldeinformationen erstellt:

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

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

Sichern Sie Exchange Ressourcen mit PowerShell Cmdlets

Das Sichern einer Exchange Server-Datenbank umfasst die Einrichtung einer Verbindung mit dem SnapCenter-Server, die Ermittlung der Exchange Server-Datenbank, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppe, das Sichern und das Anzeigen des Backup-Status.

Bevor Sie beginnen

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

Das Plug-in für Exchange unterstützt keine Klonvorgänge. Daher wird der CloneType-Parameter für das Cmdlet "Add-SmPolicy" für Plug-in für Exchange nicht unterstützt

Schritte

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

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

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

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

   In diesem Beispiel wird eine neue Backup-Richtlinie mit einem vollständigen Exchange Backup-Typ für Backups und Protokollierung erstellt:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

   Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem stündlichen vollständigen Backup und Log Backup-Typ für Exchange Backup:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

In diesem Beispiel wird eine neue Backup-Richtlinie erstellt, in der nur Exchange-Protokolle gesichert werden:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

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

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

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

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

   In diesem Beispiel wird eine neue Backup-Ressourcengruppe für die Exchange Server-Datenbank mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bk
p_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

   Dieses Beispiel erstellt eine neue Exchange Database Availability Group (DAG) Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode SCE
-Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bk
p_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability
Group";"Names"="DAGSCE0102"}
```

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

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

   Dieses Beispiel erstellt ein neues Backup im Sekundärspeicher:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

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

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

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

   Dieses Beispiel zeigt einen Job-Übersichtsbericht für eine bestimmte Job-ID an:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

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

Monitoring von Backup-Vorgängen

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

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.

c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.

d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.

e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.

4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

> Obwohl der Status des Sicherungsauftrags angezeigt wird, wird beim Klicken auf Jobdetails möglicherweise angezeigt ✔ , dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

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

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

Überwachen Sie die Vorgänge im Teilfenster „Aktivität“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

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

Abbrechen der Backup-Vorgänge für die Exchange-Datenbank

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

Entfernen Sie Exchange Backups mithilfe von PowerShell Cmdlets

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

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

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

Schritte

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

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

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

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

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

Zeigen Sie Exchange-Backups auf der Seite Topologie an

Wenn Sie die Datensicherung vorbereiten, ist es Ihnen eventuell hilfreich, eine grafische Darstellung aller Backups auf den primären und sekundären Speichern anzuzeigen.

Über diese Aufgabe

Auf der Seite Topology sehen Sie alle Backups, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details zu diesen Backups anzeigen und sie zur Durchführung von Datensicherungsvorgängen auswählen.

Mithilfe des folgenden Symbols in der Ansicht Kopien verwalten können Sie bestimmen, ob die Backups auf dem primären oder sekundären Speicher verfügbar sind (gespiegelte Kopien oder Vault-Kopien).

- Zeigt die Anzahl der Backups an, die auf dem primären Speicher verfügbar sind.
- Zeigt die Anzahl der Backups an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.
- Zeigt die Anzahl der Backups an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.
  - Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden.

    Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Best Practice: um sicherzustellen, dass die korrekte Anzahl replizierter Backups angezeigt wird, empfehlen wir, die Topologie zu aktualisieren.

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 Datenbank, die Ressource oder die Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

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

4. Lesen Sie den Abschnitt „Übersichtskarte“, um eine Zusammenfassung der Anzahl der Backups anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

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

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine

genaue Anzahl anzuzeigen.

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

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

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

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

   Die Details der Backups werden in einem Tabellenformat angezeigt.

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

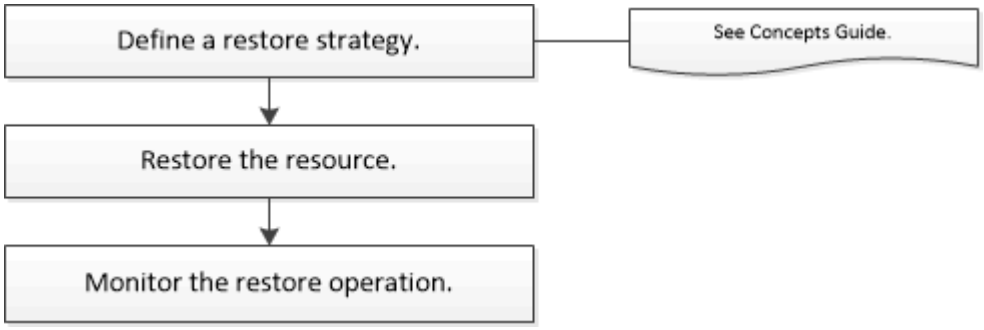
   Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen. Das Löschen von Snapshots wird von den ONTAP-Aufbewahrungseinstellungen übernommen.

Stellen Sie Exchange Ressourcen wieder her

Wiederherstellung des Workflows

Mit SnapCenter können Exchange-Datenbanken wiederhergestellt werden, indem ein oder mehrere Backups auf dem aktiven File-System wiederhergestellt werden.

Im folgenden Workflow wird die Reihenfolge angezeigt, in der Sie die Wiederherstellungsvorgänge der Exchange-Datenbank durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup- und Restore-Vorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder unter "SnapCenter Software Cmdlet Referenzhandbuch".

Anforderungen für die Wiederherstellung einer Exchange-Datenbank

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

Um die Wiederherstellungsfunktion vollständig nutzen zu können, müssen Sie sowohl SnapCenter Server als auch das SnapCenter Plug-in für die Exchange-Datenbank auf 4.6 aktualisieren.

- Der Exchange Server muss online sein und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.
- Die Datenbanken müssen auf dem Exchange Server vorhanden sein.

  Die Wiederherstellung gelöschter Datenbanken wird nicht unterstützt.
- SnapCenter-Zeitpläne für die Datenbank müssen ausgesetzt werden.
- Der SnapCenter Server und das SnapCenter Plug-in für Microsoft Exchange Server Host müssen mit dem primären und sekundären Storage verbunden sein, der die wiederherzustellenden Backups enthält.

Exchange Datenbanken wiederherstellen

Mit SnapCenter können Sie gesicherte Exchange Datenbanken wiederherstellen.

Bevor Sie beginnen

- Sie müssen die Ressourcengruppen, die Datenbank oder die Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAGs) gesichert haben.
- Wenn die Exchange-Datenbank zu einem anderen Speicherort migriert wird, funktioniert der Wiederherstellungsvorgang nicht für alte Backups.
- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.
- Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Storage anderer Anbieter befindet und Sie die passive Datenbankkopie eines Backups in einem NetApp Storage wiederherstellen möchten, erstellen Sie in einer DAG die passive Kopie (NetApp Storage) als aktive Kopie, aktualisieren Sie die Ressourcen und führen Sie den Wiederherstellungsvorgang aus.

  Führen Sie den Befehl aus `Move-ActiveMailboxDatabase` , um die passive Datenbankkopie als aktive Datenbankkopie zu erstellen.

  Das "Microsoft-Dokumentation" enthält Informationen zu diesem Befehl.

Über diese Aufgabe

- Wenn ein Restore-Vorgang für eine Datenbank durchgeführt wird, wird die Datenbank wieder auf demselben Host gemountet und es wird kein neues Volume erstellt.
- DAG-Backups müssen aus einzelnen Datenbanken wiederhergestellt werden.
- Die vollständige Wiederherstellung der Festplatte wird nicht unterstützt, wenn andere Dateien als die Exchange-Datenbank (.edb)-Datei vorhanden sind.

Plug-in für Exchange führt keine vollständige Wiederherstellung auf einer Festplatte durch, wenn das Laufwerk Exchange-Dateien wie die zur Replizierung verwendeten enthält. Wenn eine vollständige Wiederherstellung möglicherweise die Exchange-Funktionalität beeinträchtigt, führt das Plug-in für Exchange einen Wiederherstellungsvorgang für eine einzelne Datei durch.

- Das Plug-in für Exchange kann BitLocker-verschlüsselte Laufwerke nicht wiederherstellen.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

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

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich oben links auf der Seite Ressource auf **Ressourcen**.
2. Wählen Sie das Exchange Server-Plug-in aus der Dropdown-Liste aus.
3. Wählen Sie auf der Seite Ressourcen in der Liste Ansicht die Option **Datenbank** aus.
4. Wählen Sie die Datenbank aus der Liste aus.
5. Wählen Sie in der Ansicht Manage Copies die Option **Backups** aus der Tabelle Primary Backups aus, und klicken Sie dann auf * * .
6. Wählen Sie auf der Seite Optionen eine der folgenden Backup-Optionen für Protokolle aus:

Option	Beschreibung
Alle Log-Backups	Wählen Sie * Alle Log-Backups*, um eine Backup-Wiederherstellung durchzuführen, um alle verfügbaren Log-Backups nach der vollständigen Sicherung wiederherzustellen.

Option	Beschreibung
Durch Backups bis protokollieren	Wählen Sie **by log Backups bis**, um einen Point-in-Time-Wiederherstellungsvorgang durchzuführen, der die Datenbank basierend auf Protokollsicherungen bis zum ausgewählten Protokoll wiederherstellt. Die Anzahl der in der Dropdown-Liste angezeigten Protokolle basiert auf UTM. Wenn beispielsweise die vollständige Backup-Aufbewahrung 5 ist und die UTM-Aufbewahrung 3 ist, sind die Anzahl der verfügbaren Log-Backups 5, aber im Drop-down-Menü werden nur 3 Protokolle aufgeführt, um den Wiederherstellungsvorgang durchzuführen.
Nach einem bestimmten Datum bis	Wählen Sie **nach einem bestimmten Datum bis**, um das Datum und die Uhrzeit anzugeben, auf die Transaktionsprotokolle auf die wiederhergestellte Datenbank angewendet werden. Mit diesem Point-in-Time-Wiederherstellungsvorgang werden die Transaktions-Log-Einträge wiederhergestellt, die bis zum letzten Backup am angegebenen Datum und Uhrzeit aufgezeichnet wurden.
Keine	Wählen Sie **Keine**, wenn Sie nur die vollständige Sicherung ohne Log-Backups wiederherstellen müssen.

Sie können eine der folgenden Aktionen durchführen:

- **Datenbank wiederherstellen und mounten nach der Wiederherstellung** - Diese Option ist standardmäßig ausgewählt.
- **Die Integrität der Transaktionsprotokolle im Backup vor der Wiederherstellung nicht überprüfen** - standardmäßig überprüft SnapCenter die Integrität der Transaktionsprotokolle in einem Backup, bevor ein Restore durchgeführt wird.

  Best Practice: Du solltest diese Option nicht wählen.

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

   Prescript-Argumente für die Wiederherstellung umfassen Datenbanken in US-Dollar und ServerInstance in US-Dollar.

   Zu den Argumenten für die Wiederherstellung nach dem Skript gehören Datenbanken in US-Dollar, ServerInstance, Backup-Name in US-Dollar, LogDirectory und TargetServerInstance in US-Dollar.

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

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

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Sie können den Status des Wiederherstellungsjobs anzeigen, indem Sie unten auf der Seite das Feld „Aktivität“ erweitern.

    Sie sollten den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs** überwachen.

Wenn Sie eine aktive Datenbank aus einem Backup wiederherstellen, weist die passive Datenbank möglicherweise einen Status „ausgesetzt“ oder „ausgefallen“ auf, wenn eine Verzögerung zwischen dem Replikat und der aktiven Datenbank vorhanden ist.

Die Statusänderung kann auftreten, wenn die Protokollkette der aktiven Datenbank sich gabelt und einen neuen Zweig startet, der die Replikation unterbrochen. Exchange Server versucht, das Replikat zu reparieren. Wenn es jedoch nicht möglich ist, sollten Sie nach der Wiederherstellung ein neues Backup erstellen und dann das Replikat erneut übertragen.

Granulares Recovery von Mails und Mailboxen

Die Single Mailbox Recovery Software (SMBR) ermöglicht es Ihnen, Mails oder Postfächer anstelle der gesamten Exchange Datenbank wiederherzustellen.

Das Wiederherstellen einer vollständigen Datenbank für die Wiederherstellung einer einzelnen Mail benötigt viel Zeit und Ressourcen. SMBR hilft bei der schnellen Wiederherstellung der Mails durch die Erstellung von Klonkopien des Snapshots und dann mit Microsoft APIs, um die Mailbox in SMBR zu mounten. Informationen zur Verwendung von SMBR finden Sie unter "SMBR-Administrationshandbuch".

Weitere Informationen zu SMBR finden Sie nachfolgend:

- "Anleitung zur manuellen Wiederherstellung eines einzelnen Elements mit SMBR (gilt auch für Wiederherstellungen bei Ontrack Power Control)"
- "Wiederherstellung aus dem sekundären Storage in SMBR mit SnapCenter"
- "Wiederherstellung von Microsoft Exchange Mail über SnapVault mit SMBR"

Wiederherstellung einer Exchange Server-Datenbank aus dem sekundären Storage

Sie können eine gesicherte Exchange Server Datenbank aus dem sekundären Storage (Spiegel oder Vault) wiederherstellen.

Sie müssen die Snapshots vom primären Speicher auf einen sekundären Speicher repliziert haben.

Über diese Aufgabe

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

Schritte

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

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

Stellen Sie Exchange Ressourcen mithilfe von PowerShell cmdlets wieder her

Beim Wiederherstellen einer Exchange-Datenbank wird eine Verbindungssitzung mit dem SnapCenter-Server initiiert, die Backups aufgeführt, Backup-Informationen abgerufen und ein Backup wiederhergestellt.

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

Über diese Aufgabe

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

Schritte

1. Starten Sie mit dem Cmdlet eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer `Open-SmConnection` .

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
   ```
2. Rufen Sie mit dem Cmdlet die Informationen über ein oder mehrere Backups ab, die Sie wiederherstellen möchten `Get-SmBackup` .

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
PS C:\> Get-SmBackup

BackupId                        BackupName                      BackupTime
BackupType
--------                        ----------                      ----------
----------
341                             ResourceGroup_36304978_UTM... 12/8/2017
4:13:24 PM          Full Backup
342                             ResourceGroup_36304978_UTM... 12/8/2017
4:16:23 PM          Full Backup
355                             ResourceGroup_06140588_UTM... 12/8/2017
6:32:36 PM          Log Backup
356                             ResourceGroup_06140588_UTM... 12/8/2017
6:36:20 PM          Full Backup
```

3. Stellen Sie Daten aus dem Backup mit dem Cmdlet wieder `Restore-SmBackup` her.

   In diesem Beispiel wird ein minutengenaue Backup wiederhergestellt:

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -IsRecoverMount:$true
```

   In diesem Beispiel wird ein zeitpunktgenaues Backup wiederhergestellt:

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -IsRecoverMount:$true
-LogRestoreType ByTransactionLogs -LogCount 2
```

   In diesem Beispiel wird ein Backup auf sekundärem Storage auf einen primären Erfahrungsbericht wiederhergestellt:

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2' -BackupId
81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

   Mit dem `-archive` Parameter können Sie die primären und sekundären Volumes angeben, die Sie für die Wiederherstellung verwenden möchten.

   Mit dem `-IsRecoverMount:$true` Parameter können Sie die Datenbank nach der Wiederherstellung mounten.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden

können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Erneutes Seeding eines passiven Exchange Node-Replikats

Wenn Sie eine Replikatkopie erneut übertragen müssen, beispielsweise wenn eine Kopie beschädigt ist, können Sie sie mithilfe der Funktion zum erneuten Seeding in SnapCenter erneut in das neueste Backup übertragen.

Bevor Sie beginnen

- Sie müssen SnapCenter Server 4.1 oder höher und Plug-in für Exchange 4.1 oder höher verwenden.

  Erneutes Seeding eines Replikats wird in SnapCenter-Versionen vor 4.1 nicht unterstützt.

- Sie müssen eine Sicherung der Datenbank erstellt haben, die Sie erneut senden möchten.

Best Practice: um einen Rückgang zwischen den Knoten zu vermeiden, empfehlen wir Ihnen, entweder ein neues Backup zu erstellen, bevor Sie einen erneuten Vorgang durchführen, oder den Host mit dem neuesten Backup auszuwählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **Microsoft Exchange Server Plug-in** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die entsprechende Option aus der Liste Ansicht aus:

Option	Beschreibung
Zum erneuten Seeding einer einzelnen Datenbank	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Zum erneuten Seeding von Datenbanken in einer DAG	Wählen Sie in der Liste View die Option **Database Availability Group** aus.

3. Wählen Sie die Ressource aus, die erneut gesendet werden soll.
4. Klicken Sie auf der Seite Kopien verwalten auf **erneut**.
5. Wählen Sie aus der Liste der ungesunden Datenbankkopien im Assistenten zum erneuten Seeding den aus, den Sie erneut speichern möchten, und klicken Sie dann auf **Weiter**.
6. Wählen Sie im Host-Fenster den Host mit dem Backup aus, von dem Sie erneut starten möchten, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
9. Sie können den Status des Jobs anzeigen, indem Sie das Aktivitätsfenster unten auf der Seite erweitern.

Ein erneutes Seeding wird nicht unterstützt, wenn die passive Datenbankkopie auf Storage anderer Anbieter liegt.

Erneutes Seeding mit PowerShell cmdlets für Exchange Datenbank

Sie können PowerShell Cmdlets verwenden, um eine fehlerhafte Kopie wiederherzustellen, indem Sie entweder die aktuellste Kopie auf demselben Host oder die aktuellste Kopie von einem alternativen Host verwenden.

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

Schritte

1. Starten Sie mit dem Cmdlet eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer `Open-SmConnection` .

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

2. Erneutes Seeding der Datenbank mit dem `reseed-SmDagReplicaCopy` Cmdlet.

   In diesem Beispiel wird die fehlgeschlagene Kopie der Datenbank namens execdb auf dem Host „mva-rx200.netapp.com" unter Verwendung des neuesten Backups auf diesem Host erneut bereitgestellt.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   In diesem Beispiel wird die fehlgeschlagene Kopie der Datenbank namens execdb erneut mit dem neuesten Backup der Datenbank (Produktion/Kopie) auf einem alternativen Host „mva-rx201.netapp.com.""“ neu definiert

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

Überwachen von Restore-Vorgängen

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

Über diese Aufgabe

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

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

Abbrechen von Wiederherstellungsvorgängen für Exchange-Datenbank

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

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

Über diese Aufgabe

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

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Nachdem Sie den Wiederherstellungsvorgang gestartet haben, klicken Sie auf das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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