



Schützen Sie Microsoft Exchange Server-Datenbanken

SnapCenter software

NetApp
November 06, 2025

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

Inhalt

Schützen Sie 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
Was Sie mit dem SnapCenter Plug-in für Microsoft Exchange Server tun können	2
Vom SnapCenter Plug-in für Microsoft Windows und Microsoft Exchange Server unterstützte Speichertypen	2
Für das Exchange-Plug-In sind mindestens ONTAP Berechtigungen erforderlich	3
Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation	6
Definieren Sie eine Sicherungsstrategie für Exchange Server-Ressourcen	6
Definieren einer Wiederherstellungsstrategie für Exchange-Datenbanken	9
Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server	10
Installationsablauf des SnapCenter Plug-ins für Microsoft Exchange Server	11
Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für Microsoft Exchange Server	11
Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für Windows	15
Konfigurieren von gMSA unter Windows Server 2016 oder höher	16
Hosts hinzufügen und Plug-in für Exchange installieren	18
Installieren Sie das Plug-in für Exchange vom SnapCenter Server-Host mithilfe von PowerShell- Cmdlets	24
Installieren Sie das SnapCenter -Plug-in für Exchange im Hintergrund über die Befehlszeile	25
Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets	26
CA-Zertifikat konfigurieren	27
Konfigurieren Sie SnapManager 7.x für die Koexistenz von Exchange und SnapCenter	30
Installieren Sie das SnapCenter Plug-in für VMware vSphere	32
CA-Zertifikat bereitstellen	32
Konfigurieren der CRL-Datei	32
Bereiten Sie sich auf den Datenschutz vor	33
Voraussetzungen für die Verwendung des SnapCenter Plug-Ins für Microsoft Exchange Server	33
So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von Exchange Server verwendet	34
Sichern von Exchange-Ressourcen	35
Sicherungsworkflow	35
Exchange-Datenbank und Backup-Verifizierung	36
Ermitteln, ob Exchange-Ressourcen für die Sicherung verfügbar sind	36
Erstellen von Sicherungsrichtlinien für Exchange Server-Datenbanken	38
Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Exchange-Server hinzu	46
Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell- Cmdlets für Exchange Server	49
Sichern Sie Exchange-Datenbanken	50
Sichern von Exchange-Ressourcengruppen	56
Überwachen von Sicherungsvorgängen	57
Abbrechen von Sicherungsvorgängen für die Exchange-Datenbank	58
Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“	59

Wiederherstellen von Exchange-Ressourcen	61
Wiederherstellungs-Workflow	61
Voraussetzungen für die Wiederherstellung einer Exchange-Datenbank	61
Wiederherstellen von Exchange-Datenbanken	62
Granulare Wiederherstellung von E-Mails und Postfächern	67
Wiederherstellen einer Exchange Server-Datenbank aus einem sekundären Speicher	67
Reseed einer passiven Exchange-Knotenreplik	68
Führen Sie mithilfe von PowerShell-Cmdlets für die Exchange-Datenbank ein erneutes Seeding eines Replikats durch	69
Überwachen von Wiederherstellungsvorgängen	70
Abbrechen von Wiederherstellungsvorgängen für die Exchange-Datenbank	70

Schützen Sie 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 hostseitige Komponente der NetApp SnapCenter -Software, die eine anwendungsbewusste Datenschutzverwaltung von Exchange-Datenbanken ermöglicht. Das Plug-in für Exchange automatisiert die Sicherung und Wiederherstellung von Exchange-Datenbanken in Ihrer SnapCenter -Umgebung.

Wenn das Plug-in für Exchange installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und mit der NetApp SnapVault -Technologie eine Disk-to-Disk-Sicherungsreplikation zur Einhaltung von Standards oder zu Archivierungszwecken durchführen.

Wenn Sie statt der gesamten Exchange-Datenbank E-Mails oder Postfächer wiederherstellen möchten, können Sie die Software Single Mailbox Recovery (SMBR) verwenden. Die Verfügbarkeit von NetApp® Single Mailbox Recovery (EOA) endet am 12. Mai 2023. NetApp wird Kunden, die Postfachkapazität, Wartung und Support über die am 24. Juni 2020 eingeführten Marketing-Teilenummern erworben haben, für die Dauer des Supportanspruchs weiterhin unterstützen.

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

Das Plug-in für Exchange unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie ein transparentes Failover durchführen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

Es unterstützt den asymmetrischen, Failover- oder Nicht-Duplex-Modus von SnapMirror Active Sync. Dies bezieht sich auf die Lösung, bei der der optimierte Pfad nur vom primärseitigen LUN-Eigentümerknoten ausgeht. Alle E/A-Vorgänge auf den sekundären Clusterpfaden werden durch Proxy-Weiterleitung an den primären Cluster abgewickelt. Die synchrone Replikation erfolgt unidirektional, vom Primär- zum Sekundärserver.

- Automatisiert anwendungsorientierte Sicherungs- und Wiederherstellungsvorgänge für Microsoft Exchange Server-Datenbanken und Database Availability Groups (DAGs) in Ihrer SnapCenter Umgebung
- Unterstützt virtualisierte Exchange-Server auf RDM-LUNs, wenn Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.

Was Sie mit dem SnapCenter Plug-in für Microsoft Exchange Server tun können

Sie können das Plug-in für Exchange zum Sichern und Wiederherstellen von Exchange Server-Datenbanken verwenden.

- Anzeigen und Verwalten eines aktiven Inventars von Exchange Database Availability Groups (DAGs), Datenbanken und Replikatsätzen
- Definieren Sie Richtlinien, die die Schutzeinstellungen für die Backup-Automatisierung bereitstellen
- Zuweisen von Richtlinien zu Ressourcengruppen
- Schützen Sie einzelne DAGs und Datenbanken
- Sichern Sie primäre und sekundäre Exchange-Postfachdatenbanken
- Wiederherstellen von Datenbanken aus primären und sekundären Sicherungen

Vom SnapCenter Plug-in für Microsoft Windows und Microsoft Exchange Server unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen als auch auf virtuellen Maschinen. Sie müssen überprüfen, ob für Ihren Speichertyp Unterstützung verfügbar ist, bevor Sie das Paket für Ihren Host installieren.

SnapCenter -Bereitstellungs- und Datenschutzunterstützung ist auf Windows Server verfügbar. Die neuesten Informationen zu unterstützten Versionen finden Sie im <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT> [NetApp Interoperabilitätsmatrix-Tool^].

Maschine	Speichertyp	Bereitstellung mittels	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische Benutzeroberfläche (GUI) von SnapCenter oder PowerShell-Cmdlets	
Physischer Server	Über iSCSI verbundene LUNs	SnapCenter -GUI oder PowerShell-Cmdlets	
VMware VM	Über einen FC- oder iSCSI-HBA verbundene RDM-LUNs	PowerShell-Cmdlets	Nur physikalische Kompatibilität  VMDKs werden nicht unterstützt.
VMware VM	iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind	SnapCenter -GUI oder PowerShell-Cmdlets	 VMDKs werden nicht unterstützt.

Maschine	Speichertyp	Bereitstellung mittels	Support-Hinweise
Hyper-V-VM	Virtuelle FC (vFC) LUNs, die durch einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter -GUI oder PowerShell-Cmdlets	Sie müssen Hyper-V Manager verwenden, um Virtual FC (vFC)-LUNs bereitzustellen, die über einen virtuellen Fibre Channel-Switch verbunden sind.  Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.
Hyper-V-VM	iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind	SnapCenter -GUI oder PowerShell-Cmdlets	 Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.

Für das Exchange-Plug-In sind mindestens ONTAP Berechtigungen erforderlich

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

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
 - Ereignis generieren-Autosupport-Protokoll
 - Jobverlauf anzeigen
 - Jobstopp
 - Montag
 - LUN erstellen
 - LUN erstellen
 - LUN erstellen
 - LUN löschen
 - lun igroup hinzufügen
 - lun igroup erstellen
 - LUN-Igroup löschen
 - LUN-Igroup umbenennen
 - LUN-Igroup umbenennen
 - lun igroup show
 - LUN-Zuordnung Add-Reporting-Nodes
 - LUN-Zuordnung erstellen
 - LUN-Zuordnung löschen
 - LUN-Zuordnung zum Entfernen von Berichtsknoten
 - LUN-Mapping-Show
 - LUN ändern
 - LUN-Einzugsvolumen
 - lun offline
 - lun online
 - LUN persistent-reservation clear
 - LUN-Größe ändern
 - LUN-Seriennummer
 - Lun-Show
 - Snapmirror-Richtlinie Add-Rule
 - Snapmirror-Richtlinienänderungsregel
 - Snapmirror-Richtlinie zum Entfernen der Regel
 - Snapmirror-Richtlinien-Show
 - Snapmirror-Wiederherstellung
 - Snapmirror-Show
 - Snapmirror-Showverlauf
 - Snapmirror-Update
 - Snapmirror-Update-LS-Set

- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen

- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
 - Netzwerkschnittstelle
 - Netzwerkschnittstelle anzeigen
 - vServer

Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation

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

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter -Jobs durchgeführt. Wenn Sie SnapMirror Active Sync verwenden, verwenden Sie die Standardzeitpläne von SnapMirror oder SnapVault sowohl für SnapMirror Active Sync als auch für asynchrone Beziehungen.



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

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



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

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

Definieren Sie eine Sicherungsstrategie für Exchange Server-Ressourcen

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge können Sie sicherstellen, dass Sie über die Sicherungen verfügen, die Sie für eine erfolgreiche Wiederherstellung Ihrer Datenbanken benötigen. Ihre Sicherungsstrategie wird weitgehend von Ihrem Service Level Agreement (SLA),

Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmt.

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

Für die Exchange-Datenbank unterstützte Sicherungstypen

Zum Sichern von Exchange-Postfächern mit SnapCenter müssen Sie den Ressourcentyp auswählen, z. B. Datenbanken und Database Availability Groups (DAG). Mithilfe der Snapshot-Technologie werden schreibgeschützte Onlinekopien der Volumes erstellt, auf denen sich die Ressourcen befinden.

Sicherungstyp	Beschreibung
Vollständige Sicherung und Protokollsicherung	Sichert die Datenbanken und alle Transaktionsprotokolle, einschließlich der gekürzten Protokolle. Nach Abschluss einer vollständigen Sicherung kürzt der Exchange Server die Transaktionsprotokolle, die bereits in der Datenbank gespeichert sind. Normalerweise sollten Sie diese Option wählen. Wenn Ihre Sicherungszeit jedoch kurz ist, können Sie bei einer vollständigen Sicherung auf die Ausführung einer Transaktionsprotokollsicherung verzichten.
Vollständige Sicherung	Sichert Datenbanken und Transaktionsprotokolle. Die gekürzten Transaktionsprotokolle werden nicht gesichert.
Protokollsicherung	Sichert alle Transaktionsprotokolle. Die gekürzten Protokolle, die bereits in der Datenbank gespeichert sind, werden nicht gesichert. Wenn Sie zwischen vollständigen Datenbanksicherungen häufige Transaktionsprotokollsicherungen planen, können Sie granulare Wiederherstellungspunkte auswählen.

Sicherungszeitpläne für Datenbank-Plugins

Die Sicherungshäufigkeit (Zeitplantyp) wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich

der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen. Beispielsweise können regelmäßige Sicherungen des Transaktionsprotokolls ausreichen, um sicherzustellen, dass Sie über die erforderlichen Sicherungen verfügen. Je häufiger Sie Ihre Datenbanken sichern, desto weniger Transaktionsprotokolle muss SnapCenter zum Zeitpunkt der Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können als Sicherungshäufigkeit für die Richtlinie stündlich, täglich, wöchentlich oder monatlich auswählen. Wenn Sie keine dieser Frequenzen auswählen, handelt es sich bei der erstellten Richtlinie um eine Nur-On-Demand-Richtlinie. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Datenbanken benötigten Sicherungsaufträge

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

Namenskonventionen für Backups

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

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
resourcegroupname_hostname_timestamp
```

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

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

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.

- 03-12-2015_23.17.26 ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen.

Beispiel: customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.



Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

Wie lange sollen Transaktionsprotokollsicherungen auf dem Quellspeichervolume für Exchange Server aufbewahrt werden?

Das SnapCenter Plug-in für Microsoft Exchange Server benötigt Transaktionsprotokollsicherungen, um aktuelle Wiederherstellungsvorgänge durchzuführen, die Ihre Datenbank auf einen Zeitpunkt zwischen zwei vollständigen Sicherungen wiederherstellen.

Wenn Plug-in for Exchange beispielsweise um 8:00 Uhr eine vollständige Sicherung plus Transaktionsprotokoll und um 17:00 Uhr eine weitere vollständige Sicherung plus Transaktionsprotokoll erstellt hat, kann es die neueste Transaktionsprotokollsicherung verwenden, um die Datenbank auf einen beliebigen Zeitpunkt zwischen 8:00 und 17:00 Uhr wiederherzustellen. Wenn keine Transaktionsprotokolle verfügbar sind, kann Plug-in for Exchange nur zeitpunktbezogene Wiederherstellungsvorgänge durchführen, die eine Datenbank auf den Zeitpunkt wiederherstellen, zu dem Plug-in for Exchange eine vollständige Sicherung abgeschlossen hat.

Normalerweise benötigen Sie aktuelle Wiederherstellungsvorgänge nur für ein oder zwei Tage. Standardmäßig behält SnapCenter mindestens zwei Tage.

Definieren einer Wiederherstellungsstrategie für Exchange-Datenbanken

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

Quellen für einen Wiederherstellungsvorgang in Exchange Server

Sie können eine Exchange Server-Datenbank aus einer Sicherungskopie auf dem primären Speicher wiederherstellen.

Sie können Datenbanken nur aus dem Primärspeicher wiederherstellen.

Für Exchange Server unterstützte Arten von Wiederherstellungsvorgängen

Sie können SnapCenter verwenden, um verschiedene Arten von Wiederherstellungsvorgängen an Exchange-Ressourcen durchzuführen.

- Aktuelle Wiederherstellung
- Wiederherstellen eines früheren Zeitpunkts

Wiederherstellung auf die Minute genau

Bei einem minutengenauen Wiederherstellungsvorgang werden Datenbanken bis zum Fehlerpunkt wiederhergestellt. SnapCenter erreicht dies durch Ausführen der folgenden Sequenz:

1. Stellt die Datenbanken aus der von Ihnen ausgewählten vollständigen Datenbanksicherung wieder her.
2. Wendet alle gesicherten Transaktionsprotokolle sowie alle neuen Protokolle an, die seit der letzten Sicherung erstellt wurden.

Transaktionsprotokolle werden weitergeleitet und auf alle ausgewählten Datenbanken angewendet.

Exchange erstellt nach Abschluss einer Wiederherstellung eine neue Protokollkette.

Best Practice: Es wird empfohlen, nach Abschluss einer Wiederherstellung eine neue vollständige Sicherung und Protokollsicherung durchzuführen.

Für einen minutengenauen Wiederherstellungsvorgang ist ein zusammenhängender Satz von Transaktionsprotokollen erforderlich.

Nachdem Sie eine minutengenaue Wiederherstellung durchgeführt haben, ist die für die Wiederherstellung verwendete Sicherung nur für zeitpunktbezogene Wiederherstellungsvorgänge verfügbar.

Wenn Sie nicht für alle Sicherungen die Wiederherstellungsfunktion auf die Minute genau benötigen, können Sie die Aufbewahrungsdauer der Transaktionsprotokollsicherungen Ihres Systems über die Sicherungsrichtlinien konfigurieren.

Wiederherstellen eines früheren Zeitpunkts

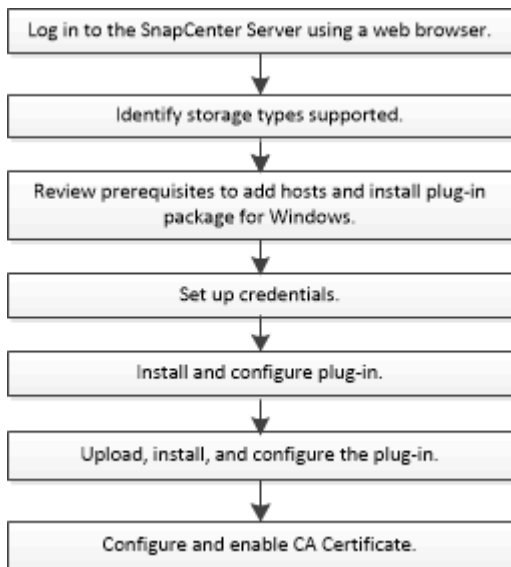
Bei einer zeitpunktbezogenen Wiederherstellung werden Datenbanken nur auf einen bestimmten Zeitpunkt in der Vergangenheit wiederhergestellt. Eine zeitpunktbezogene Wiederherstellung erfolgt in den folgenden Wiederherstellungssituationen:

- Die Datenbank wird zu einem bestimmten Zeitpunkt in einem gesicherten Transaktionsprotokoll wiederhergestellt.
- Die Datenbank wird wiederhergestellt und nur eine Teilmenge der gesicherten Transaktionsprotokolle wird darauf angewendet.

Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server

Installationsablauf 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 zum Hinzufügen von Hosts und Installieren 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 und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Sie müssen Microsoft Exchange Server 2013, 2016 oder 2019 für eigenständige und Datenbankverfügbarkeitsgruppenkonfigurationen verwenden.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Wenn Sie Clusterknoten in SnapCenter verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Knoten im Cluster.
- Sie müssen über einen Benutzer mit Administratorberechtigungen auf dem Exchange-Server verfügen.
- Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, müssen Sie die Registrierung des von SnapDrive für Windows verwendeten VSS-Hardwareanbieters aufheben, bevor Sie das Plug-in für Exchange auf demselben Exchange Server installieren, um einen erfolgreichen Datenschutz mit SnapCenter sicherzustellen.
- Wenn SnapManager für Microsoft Exchange Server und Plug-in für Exchange auf demselben Server installiert sind, müssen Sie alle von SnapManager für Microsoft Exchange Server erstellten Zeitpläne aus dem Windows-Scheduler aussetzen oder löschen.
- Der Host muss vom Server aus in den vollqualifizierten Domännennamen (FQDN) auflösbar sein. Wenn die Hosts-Datei geändert wird, um sie auflösbar zu machen, und wenn sowohl der Kurzname als auch der FQDN in der Hosts-Datei angegeben sind, erstellen Sie einen Eintrag in der SnapCenter -Hosts-Datei im

folgenden Format: <IP-Adresse> <Host-FQDN> <Hostname>.

- Stellen Sie sicher, dass die folgenden Ports in der Firewall nicht blockiert sind, da sonst der Vorgang zum Hinzufügen des Hosts fehlschlägt. Um dieses Problem zu beheben, müssen Sie den dynamischen Portbereich konfigurieren. Weitere Informationen finden Sie unter "[Microsoft-Dokumentation](#)".
 - Portbereich 50000 – 51000 für Windows 2016 und Exchange 2016
 - Portbereich 6000 – 6500 für Windows 2012 R2 und Exchange 2013
 - Portbereich 49152 – 65536 für Windows 2019



Um den Portbereich zu identifizieren, führen Sie die folgenden Befehle aus:

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

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

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im " NetApp Interoperabilitätsmatrix-Tool ".
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	5 GB  Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Artikel	Anforderungen
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Exchange Server-Berechtigungen erforderlich

Damit SnapCenter Exchange Server oder DAG hinzufügen und das SnapCenter Plug-in für Microsoft Exchange Server auf einem Host oder DAG installieren kann, müssen Sie SnapCenter mit Anmeldeinformationen für einen Benutzer mit einem Mindestsatz an Berechtigungen und Berechtigungen konfigurieren.

Sie benötigen einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remote-Exchange-Host sowie Administratorberechtigungen auf allen Knoten in der DAG. Der Domänenbenutzer benötigt die folgenden Mindestberechtigungen:

- Hinzufügen-MailboxDatabaseCopy
- Dismount-Datenbank
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Verschieben-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- Mount-Datenbank
- Neue Mailbox-Datenbank
- Neue PublicFolderDatabase
- Entfernen-MailboxDatabase
- Entfernen-MailboxDatabaseCopy

- Entfernen-PublicFolderDatabase
- Lebenslauf-MailboxDatenbankkopie
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

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

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

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	5 GB  Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Artikel	Anforderungen
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für Windows

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

Informationen zu diesem Vorgang

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Windows-Hosts einrichten. Obwohl Sie Anmeldeinformationen für Windows erstellen können, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, empfiehlt es sich, die Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.

Das Fenster „Anmeldeinformationen“ wird angezeigt.

4. Gehen Sie auf der Seite „Anmeldeinformationen“ wie folgt vor:

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.
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 beliebiges 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 für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: UserName
Passwort	Geben Sie das zur Authentifizierung verwendete Passwort ein.
Authentifizierung	Wählen Sie Windows als Authentifizierungsmodus.

5. Klicken Sie auf **OK**.

Konfigurieren von gMSA unter Windows Server 2016 oder höher

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

Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -EffectivelImmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
 - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

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

Zum Beispiel,

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

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

Führen Sie dazu den folgenden Befehl von PowerShell aus:

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

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

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

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Starten Sie Ihren Host neu.
 - b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der 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 Dienstanmeldekonto verwendet.

Hosts hinzufügen und Plug-in für Exchange installieren

Sie können die SnapCenter -Seite „Host hinzufügen“ 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 einen Cluster installieren.

Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
 - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
 - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise der SnapCenter Administrator.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Der Nachrichtenwarteschlangendienst muss ausgeführt werden.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren. Weitere Informationen finden Sie unter ["Konfigurieren Sie ein gruppenverwaltetes Dienstkonto auf Windows Server 2016 oder höher für Microsoft Exchange Server"](#).

Informationen zu diesem Vorgang

- 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 entweder für einen einzelnen Host oder einen Cluster installieren.
- Wenn ein Exchange-Knoten Teil einer DAG ist, können Sie nicht nur einen Knoten zum SnapCenter -Server hinzufügen.
- Wenn Sie Plug-Ins auf einem Cluster (Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert, auch wenn einige Knoten keine Datenbanken auf NetApp LUNs haben.

Ab SnapCenter 4.6 unterstützt SCE Mandantenfähigkeit und Sie können einen Host mit den folgenden

Methoden hinzufügen:

Hostvorgang hinzufügen	4.5 und früher	4.6 und höher
Fügen Sie einen IP-losen DAG in einer anderen oder einer anderen Domäne hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP-DAGs mit eindeutigen Namen hinzu, die sich in derselben oder einer anderen Domäne befinden.	Unterstützt	Unterstützt
Fügen Sie mehrere IP- oder IP-lose DAGs hinzu, die denselben Hostnamen und/oder DB-Namen domänenübergreifend haben	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP/IP-lose DAGs mit demselben Namen und domänenübergreifend hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere eigenständige Hosts mit demselben Namen und domänenübergreifend hinzu	Nicht unterstützt	Unterstützt

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

Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind und Sie das Plug-in für Exchange auf demselben Exchange Server installieren möchten, müssen Sie die Registrierung des von SnapDrive für Windows verwendeten VSS-Hardwareanbieters aufheben, da dieser nicht mit dem VSS-Hardwareanbieter kompatibel ist, der mit dem Plug-in für Exchange und dem SnapCenter Plug-ins Package für Windows installiert wurde. 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. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Gehen Sie auf der Seite „Hosts“ wie folgt vor:

Für dieses Feld...	Machen Sie Folgendes...
Hosttyp	Wählen Sie Windows als Hosttyp. SnapCenter Server fügt den Host hinzu und installiert dann auf dem Host das Plug-in für Windows und das Plug-in für Exchange, falls diese noch nicht installiert sind. Plug-in für Windows und Plug-in für Exchange müssen dieselbe Version haben. Wenn zuvor eine andere Version des Plug-ins für Windows installiert war, aktualisiert SnapCenter die Version im Rahmen der Installation.

Für dieses Feld...	Machen Sie Folgendes...
Hostname	Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den vollqualifizierten Domännennamen (FQDN) einzugeben. Eine IP-Adresse wird für nicht vertrauenswürdige Domänenhosts nur unterstützt, wenn sie in den FQDN aufgelöst wird. Wenn Sie mit SnapCenter einen Host hinzufügen und dieser Teil einer Subdomäne ist, müssen Sie den FQDN angeben. Sie können IP-Adressen oder den FQDN eines der folgenden Elemente eingeben: • Eigenständiger Host • DAG austauschen Für einen Exchange-DAG können Sie: ◦ Fügen Sie einen DAG hinzu, indem Sie den DAG-Namen, die DAG-IP-Adresse, den Knotennamen oder die Knoten-IP-Adresse angeben. ◦ Fügen Sie den IP-losen DAG-Cluster hinzu, indem Sie die IP-Adresse oder den FQDN eines der DAG-Clusterknoten angeben. ◦ Fügen Sie einen DAG ohne IP hinzu, der sich in derselben oder einer anderen Domäne befindet. Sie können auch mehrere IP/IP-lose DAGs mit demselben Namen, aber unterschiedlichen Domänen hinzufügen.  Für einen eigenständigen Host oder einen Exchange-DAG (domänenübergreifend oder dieselbe Domäne) wird empfohlen, den FQDN oder die IP-Adresse des Hosts oder DAG anzugeben.

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationen	Wählen Sie den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie die neuen Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen einer Anmeldeinformation. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.  Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

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

Wenn Sie „Plug-in für Exchange“ auswählen, wird die Auswahl von „SnapCenter Plug-in für Microsoft SQL Server“ automatisch aufgehoben. Microsoft empfiehlt, SQL Server und Exchange Server aufgrund der Speicherbelegung und anderer von Exchange benötigter Ressourcennutzung nicht auf demselben System zu installieren.

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

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

Für dieses Feld...	Machen Sie Folgendes...
Installationspfad	Der Standardpfad ist <code>C:\Program Files\NetApp\SnapCenter</code> . Optional können Sie den Pfad anpassen.
Alle Hosts in der DAG hinzufügen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie einen DAG hinzufügen.
Vorinstallationsprüfungen überspringen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten. Geben Sie den gMSA-Namen im folgenden Format an: <code>Domänenname\Kontoname\$</code> .  gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.

7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Voraussetzungen für die Installation des Plug-Ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei `web.config` aktualisieren, die sich unter `C:\Program Files\NetApp\SnapCenter WebApp` zum Ändern der Standardwerte. 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.

Konfigurieren Sie einen benutzerdefinierten Port für die NET TCP-Kommunikation

Ab der SnapCenter Version 6.0 verwendet das SnapCenter -Plug-in für Windows standardmäßig den Port 909 für die NET TCP-Kommunikation. Wenn der Port 909 verwendet wird, können Sie einen anderen Port für die NET TCP-Kommunikation konfigurieren.

Schritte

1. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config* in die erforderliche Portnummer. `<add key="NetTCPPort" value="new_port_number" />`
2. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in für Microsoft Windows\SnapDriveService.dll.config* in die erforderliche Portnummer. `<add key="NetTCPPort" value="new_port_number" />`
3. Heben Sie die Registrierung des Dienstes *Data ONTAP VSS Hardware Provider* auf, indem Sie den folgenden Befehl ausführen: `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

Stellen Sie sicher, dass der Dienst nicht in der Liste der Dienste in *services.msc* angezeigt wird.

4. Registrieren Sie den Dienst *Data ONTAP VSS Hardware Provider*, indem Sie den folgenden Befehl ausführen: `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

Überprüfen Sie, ob der Dienst jetzt in der Liste der Dienste in *services.msc* angezeigt wird.

5. Starten Sie den Dienst „Plug-in für Windows“ neu.

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

Sie sollten das Plug-in für Exchange über die SnapCenter -GUI 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 sein.
- Sie müssen ein lokaler Administrator auf dem Host oder ein Benutzer mit Administratorrechten sein.
- Sie müssen ein Benutzer sein, dem eine Rolle mit Plug-In-, Installations- und Deinstallationsberechtigungen zugewiesen ist, beispielsweise der SnapCenter Administrator.
- Sie müssen die Installationsanforderungen und die unterstützten Konfigurationstypen überprüft haben, bevor Sie das Plug-in für Exchange installieren.
- Der Host, auf dem Sie das Plug-in für Exchange installieren möchten, muss ein Windows-Host sein.

Schritte

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

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

Der Host kann ein eigenständiger Host oder ein DAG sein. Wenn Sie einen DAG angeben, ist der Parameter *-IsDAG* erforderlich.

3. Installieren Sie das Plug-in für Exchange mithilfe des Cmdlets *Install-SmHostPackage* mit den erforderlichen Parametern.

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

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

Sie sollten das Plug-in für Exchange über die SnapCenter -Benutzeroberfläche installieren. Wenn dies aus irgendeinem Grund nicht möglich ist, können Sie das Plug-in für Exchange-Installationsprogramm unbeaufsichtigt im Hintergrundmodus über die Windows-Befehlszeile ausführen.

Bevor Sie beginnen

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

Weitere Informationen finden Sie unter ["So installieren Sie ein SnapCenter -Plug-In manuell und direkt vom Plug-In-Host"](#) .

Schritte

1. Überprüfen Sie, ob der Ordner *C:\temp* auf dem Plug-In-Host vorhanden ist und der angemeldete Benutzer vollen Zugriff darauf hat.
2. Laden Sie das SnapCenter -Plug-in für Microsoft Windows von *C:\ProgramData\ NetApp\ SnapCenter\Package Repository* herunter.

Auf diesen Pfad kann vom Host aus 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 zu dem Verzeichnis, in dem 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_Pfad>"  
BI_SERVICEACCOUNT=<Domäne\Administrator> BI_SERVICEPWD=<Passwort>  
ISFeatureInstall=HPPW,SCW,SCE
```

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\ SnapCenter"  
BI_SERVICEACCOUNT=Domäne\Administrator BI_SERVICEPWD=Passwort  
ISFeatureInstall=HPPW,SCW,SCE
```



Bei allen während der Installation des Plug-ins für Exchange übergebenen Parametern wird zwischen Groß- und Kleinschreibung unterschieden.

Geben Sie für die Variablen folgende Werte ein:

Variable	Wert
<code>/debuglog"<Debug_Log_Pfad></code>	Geben Sie den Namen und den Speicherort der Protokolldatei des Suite-Installationsprogramms an, wie im folgenden Beispiel: <code>Setup.exe</code> <code>/debuglog"C:\PfadZurProtokolldatei\setupexe.log</code>
<code>BI_SNAPCENTER_PORT</code>	Geben Sie den Port an, über den SnapCenter mit SMCORE kommuniziert.
<code>SUITE_INSTALLDIR</code>	Geben Sie das Installationsverzeichnis des Host-Plug-In-Pakets an.
<code>BI_SERVICEACCOUNT</code>	Geben Sie das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.
<code>BI_SERVICEPWD</code>	Geben Sie das Kennwort für das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.
<code>ISFeatureInstall</code>	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host bereitgestellt werden soll.

- Überwachen Sie den Windows-Taskplaner, die Hauptinstallationsprotokolldatei `C:\Installdebug.log` und die zusätzlichen Installationsdateien in `C:\Temp`.
- Überwachen Sie das Verzeichnis `%temp%`, um zu überprüfen, ob die `msiexe.exe`-Installationsprogramme die Software ohne Fehler installieren.



Bei der Installation des Plug-ins für Exchange wird das Plug-in auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie können das Plug-In auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder des PowerShell-Cmdlets hinzufügen. Nachdem der Host hinzugefügt wurde, wird das Plug-In automatisch erkannt.

Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets

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

Informationen zu diesem Vorgang

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

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

Schritte

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

CA-Zertifikat konfigurieren

CA-Zertifikat-CSR-Datei generieren

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

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



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

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



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

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

CA-Zertifikate importieren

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

Schritte

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

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



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

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

Abrufen des CA-Zertifikatfingerabdrucks

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

Schritte

1. Führen Sie auf der GUI Folgendes aus:
 - a. Doppelklicken Sie auf das Zertifikat.

- b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
- c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
- d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
- e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

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

2. Führen Sie in PowerShell Folgendes aus:

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

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

- b. Kopieren Sie den Fingerabdruck.

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

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

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

Schritte

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

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

Beispiel:

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

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

Beispiel:

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

CA-Zertifikate für Plug-Ins aktivieren

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

Bevor Sie beginnen

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

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

Schritte

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

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss angezeigt und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

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



Wenn der Status gelb oder grün ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.

Konfigurieren Sie SnapManager 7.x für die Koexistenz von Exchange und SnapCenter

Damit das SnapCenter -Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server gleichzeitig verwendet werden können, müssen Sie das SnapCenter -Plug-in für Microsoft Exchange Server auf demselben Exchange Server

installieren, auf dem SnapManager für Microsoft Exchange Server installiert ist, die Zeitpläne von SnapManager für Exchange deaktivieren und neue Zeitpläne und Sicherungen mithilfe des SnapCenter -Plug-ins für Microsoft Exchange Server konfigurieren.

Bevor Sie beginnen

- SnapManager für Microsoft Exchange Server und SnapDrive für Windows sind bereits installiert und SnapManager für Microsoft Exchange Server-Backups sind auf dem System und im SnapInfo-Verzeichnis vorhanden.
- Sie sollten die von SnapManager für Microsoft Exchange Server erstellten Backups, die Sie nicht mehr benötigen, gelöscht oder wiederhergestellt haben.
- Sie sollten alle von SnapManager für Microsoft Exchange Server erstellten Zeitpläne aus dem Windows-Planer angehalten oder gelöscht haben.
- SnapCenter Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server können auf demselben Exchange Server koexistieren, Sie können jedoch vorhandene SnapManager für Microsoft Exchange Server-Installationen nicht auf SnapCenter aktualisieren.

SnapCenter bietet keine Option für das Upgrade.

- 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 SnapManager für Microsoft Exchange Server-Backup wiederherstellen möchten, müssen Sie zusätzliche Schritte ausführen.

Schritte

1. Ermitteln Sie mithilfe von PowerShell auf allen DAG-Knoten, ob der SnapDrive für Windows VSS-Hardwareanbieter 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. Heben Sie im SnapDrive -Verzeichnis die Registrierung des VSS-Hardwareanbieters von SnapDrive für Windows auf: *navssprv.exe -r service -u*
3. Überprüfen Sie, ob der VSS-Hardwareanbieter 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 Verzeichnis „SnapCenter Plug-in für Microsoft Windows“ 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. Stoppen Sie die Sicherungspläne von SnapManager für Microsoft Exchange Server.
7. Erstellen Sie mithilfe der SnapCenter -GUI 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 jetzt nicht deinstallieren und später ein SnapManager für Microsoft Exchange Server-Backup wiederherstellen möchten:

- a. Heben Sie die Registrierung des SnapCenter -Plug-ins 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. Registrieren Sie SnapDrive für Windows im Verzeichnis *C:\Programme\NetApp\SnapDrive * auf allen DAG-Knoten: *navssprv.exe -r service -a hostname\username -p password*

Installieren Sie das SnapCenter Plug-in for VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter ["Bereitstellungsübersicht"](#) .

CA-Zertifikat bereitstellen

Informationen zum Konfigurieren des CA-Zertifikats mit dem SnapCenter Plug-in for VMware vSphere finden Sie unter ["SSL-Zertifikat erstellen oder importieren"](#) .

Konfigurieren der CRL-Datei

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

Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen. Die eingehenden Zertifikate werden

anhand der einzelnen CRLs überprüft.

Bereiten Sie sich auf den Datenschutz vor

Bevor Sie Datenschutzvorgänge wie Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen, müssen Sie Ihre Strategie definieren und die Umgebung einrichten. Sie können den SnapCenter -Server auch für die Verwendung der SnapMirror und SnapVault -Technologie einrichten.

Um die Vorteile der SnapVault und SnapMirror -Technologie nutzen zu können, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes auf dem Speichergerät konfigurieren und initialisieren. Sie können diese Aufgaben mit NetAppSystem Manager oder über die Befehlszeile der Speicherkonsole ausführen.

Weitere Informationen finden

["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.

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich bei SnapCenter an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen oder zuweisen und Anmeldeinformationen erstellen.



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

- Fügen Sie Hosts hinzu, installieren Sie das SnapCenter -Plug-in für Microsoft Windows und das SnapCenter -Plug-in für Microsoft Exchange Server und ermitteln (aktualisieren) Sie die Ressourcen.
- Führen Sie die hostseitige Speicherbereitstellung 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 for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Weitere Informationen finden Sie in der Dokumentation zum SnapCenter Plug-in for VMware vSphere .



VMDKs werden nicht unterstützt.

- Verschieben Sie eine vorhandene Microsoft Exchange Server-Datenbank mithilfe von Microsoft Exchange-Tools von einer lokalen Festplatte auf einen unterstützten Speicher.
- Richten Sie SnapMirror und SnapVault -Beziehungen ein, wenn Sie eine Backup-Replikation wünschen.

Für Benutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.1.1 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme. Für Benutzer von SnapCenter 4.2.x sowie NetApp Data Broker 1.0 und 1.0.1 enthält die Dokumentation Informationen zum Schutz

virtualisierter Datenbanken und Dateisysteme mithilfe des SnapCenter Plug-in for VMware vSphere, das von der Linux-basierten virtuellen NetApp Data Broker-Appliance (Open Virtual Appliance-Format) bereitgestellt wird. Für Benutzer von SnapCenter 4.3.x enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des Linux-basierten SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance-Format).

["SnapCenter Plug-in for VMware vSphere Dokumentation"](#)

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

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

- Bei den Ressourcen handelt es sich in der Regel um Postfachdatenbanken oder Microsoft Exchange Database Availability Groups (DAGs), die Sie mit SnapCenter sichern.
- Eine SnapCenter -Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG und die Ressourcengruppe kann entweder einen ganzen DAG oder einzelne Datenbanken umfassen.

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

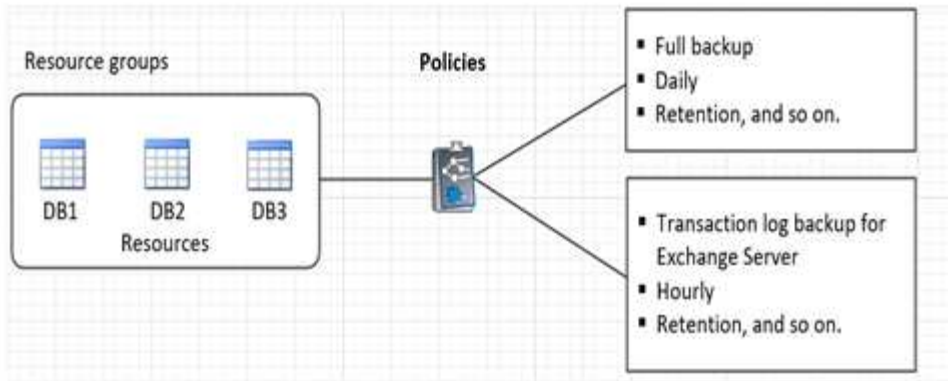
Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

Die Ressourcengruppen wurden früher als Datensätze bezeichnet.

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

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

Stellen Sie sich eine Ressourcengruppe so vor, als würde sie definieren, *was* Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als würde sie definieren, *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anfügen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird, und einen anderen Zeitplan, der stündlich Protokollsicherungen durchführt. Die folgende Abbildung veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



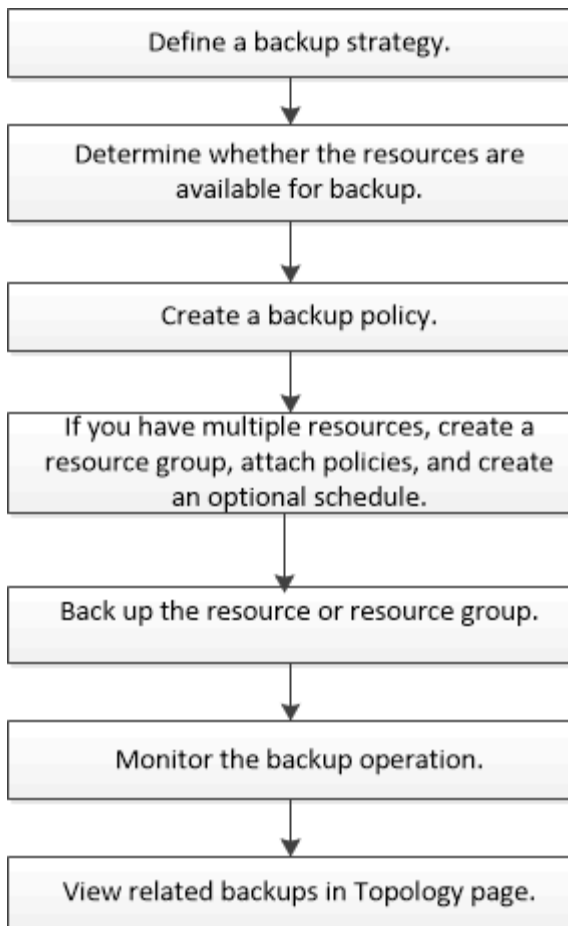
Sichern von Exchange-Ressourcen

Sicherungsworkflow

Wenn Sie das SnapCenter -Plug-in für Microsoft Exchange Server in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern von Exchange-Ressourcen verwenden.

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden. Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden. Aktive und passive Sicherungskopien auf demselben Volume werden nicht unterstützt.

Der folgende Arbeitsablauf 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 Sicherungsüberprüfung. Sie können jedoch das mit Exchange bereitgestellte Tool „Eseutil“ verwenden, um Exchange-Datenbanken und -Sicherungen zu überprüfen.

Das Microsoft Exchange Eseutil-Tool ist ein Befehlszeilenprogramm, das in Ihrem Exchange-Server enthalten ist. Mit dem Dienstprogramm können Sie Konsistenzprüfungen durchführen, um die Integrität von Exchange-Datenbanken und -Sicherungen zu überprüfen.

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

Weitere Informationen finden Sie unter ["Microsoft Exchange Server-Dokumentation"](#).

Ermitteln, ob Exchange-Ressourcen für die Sicherung verfügbar sind

Ressourcen sind die Datenbanken und Exchange Database Availability Groups, die von den von Ihnen installierten Plug-Ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzaufgaben auszuführen. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Ihnen zur Verfügung stehen. Durch die Ermittlung der verfügbaren Ressourcen wird auch überprüft, ob die Plug-In-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen, das Hinzufügen von Anmeldeinformationen und die Installation des Plug-ins für Exchange abgeschlossen haben.
- Um die Funktionen der Single Mailbox Recovery-Software nutzen zu können, müssen Sie Ihre aktive Datenbank auf dem Exchange-Server lokalisiert haben, auf dem die Single Mailbox Recovery-Software installiert ist.
- Wenn sich Datenbanken auf VMware RDM LUNs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Der "[SnapCenter Plug-in for VMware vSphere Dokumentation](#)" hat weitere Informationen.

Informationen zu diesem Vorgang

- Sie können keine Datenbanken sichern, wenn die Option **Gesamtstatus** auf der Seite „Details“ auf „Nicht für Sicherung verfügbar“ eingestellt ist. Die Option **Gesamtstatus** wird auf „Nicht für Sicherung verfügbar“ gesetzt, wenn eine der folgenden Bedingungen zutrifft:
 - Datenbanken befinden sich nicht auf einer NetApp LUN.
 - Die Datenbanken befinden sich nicht im Normalzustand.

Datenbanken befinden sich nicht im Normalzustand, wenn sie sich im Status „Mounten“, „Unmounten“, „Reseed“ oder „Wiederherstellung ausstehend“ befinden.

- Wenn Sie über eine Database Availability Group (DAG) verfügen, können Sie alle Datenbanken in der Gruppe sichern, indem Sie den Sicherungsauftrag von der DAG aus ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **Microsoft Exchange Server** aus der Plug-In-Dropdownliste in der oberen linken Ecke der Ressourcenseite aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdownliste „Anzeigen“ die Option „**Datenbank**“, „**Datenbankverfügbarkeitsgruppe**“ 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  und wählen Sie den Hostnamen und den Exchange-Server aus, um die Ressourcen zu filtern. Sie können dann auf , um den Filterbereich zu schließen.

3. Klicken Sie auf **Ressourcen aktualisieren**.

Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden im SnapCenter Server-Inventar 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 die Datenbank derzeit aktiv ist, Server mit Kopien, Zeitpunkt der letzten Sicherung und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem Nicht- NetApp -Speicher befindet, wird in der Spalte „Gesamtstatus“ „Nicht für Sicherung verfügbar“ angezeigt.

Wenn sich in einer DAG die aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und sich mindestens eine passive Datenbankkopie auf einem NetApp -Speicher befindet, wird in der Spalte **Gesamtstatus** „Nicht geschützt“ angezeigt.

Sie können keine Datenschutzvorgänge für eine Datenbank durchführen, die sich auf einem anderen Speichertyp als NetApp befindet.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte **Gesamtstatus** „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte **Gesamtstatus** die Meldung „Sicherung nicht ausgeführt“ an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist und die Sicherung für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche in der Spalte **Gesamtstatus** die Meldung „Sicherung erfolgreich“ an.

Erstellen von Sicherungsrichtlinien für Exchange Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Exchange-Ressourcen oder für die Ressourcengruppen erstellen, bevor Sie SnapCenter zum Sichern von Microsoft Exchange Server-Ressourcen verwenden, oder Sie können eine Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine einzelne Ressource sichern.

Bevor Sie beginnen

- Sie müssen Ihre Datenschutzstrategie definiert haben.

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

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Sie müssen die Exchange Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss der SnapCenter Administrator Ihnen die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des `usePowershellProcessforScripts` Parameter auf `true` im `web.config` Datei.

Der Standardwert ist „false“.

- Überprüfen Sie die spezifischen Voraussetzungen und Einschränkungen der SnapMirror Active Sync. Weitere Informationen finden Sie unter ["Objektlimits für SnapMirror Active Sync"](#).

Informationen zu diesem Vorgang

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten und aufbewahren und wie häufig die Ressource oder Ressourcengruppe gesichert wird. Darüber hinaus können Sie Skripteinstellungen festlegen. Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.
- Die vollständige Aufbewahrung von Backups ist an eine bestimmte Richtlinie gebunden. Eine Datenbank

oder Ressource, die Richtlinie A mit einer vollständigen Sicherungsaufbewahrung von 4 verwendet, behält 4 vollständige Sicherungen bei und hat keine Auswirkungen auf Richtlinie B für dieselbe Datenbank oder Ressource, die möglicherweise eine Aufbewahrung von 3 hat, um 3 vollständige Sicherungen beizubehalten.

- Die Aufbewahrung von Protokollsicherungen ist richtlinienübergreifend wirksam und gilt für alle Protokollsicherungen einer Datenbank oder Ressource. Wenn also eine vollständige Sicherung mit Richtlinie B durchgeführt wird, wirkt sich die Protokollaufbewahrungseinstellung auf Protokollsicherungen aus, die mit Richtlinie A auf derselben Datenbank oder Ressource erstellt wurden. Ebenso wirkt sich die Protokollaufbewahrungseinstellung für Richtlinie A auf Protokollsicherungen aus, die von Richtlinie B in derselben Datenbank erstellt wurden.
- Der `SCRIPTS_PATH` wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad 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 des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

Best Practice: Am besten konfigurieren Sie die sekundäre Aufbewahrungsrichtlinie basierend auf der Anzahl der vollständigen und Protokollsicherungen, die Sie insgesamt aufbewahren möchten. Wenn Sie sekundäre Aufbewahrungsrichtlinien konfigurieren, bedenken Sie, dass bei Datenbanken und Protokollen, die sich auf unterschiedlichen Volumes befinden, jede Sicherung drei Snapshots haben kann, und dass bei Datenbanken und Protokollen, die sich auf demselben Volume befinden, jede Sicherung zwei Snapshots haben kann.

- SnapLock
 - Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.

Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Sicherungstyp und Replikation“ die folgenden Schritte aus:
 - a. Wählen Sie den Sicherungstyp:

Wenn Sie wollen...	Machen Sie Folgendes...
Sichern Sie die Datenbankdateien und die erforderlichen Transaktionsprotokolle	Wählen Sie Vollständige Sicherung und Protokollsicherung. Datenbanken werden mit Protokollkürzung gesichert und alle Protokolle werden gesichert, einschließlich der gekürzten Protokolle.  Dies ist der empfohlene Sicherungstyp.
Sichern Sie die Datenbankdateien und die nicht festgeschriebenen Transaktionsprotokolle	Wählen Sie Vollständige Sicherung. Datenbanken werden mit Protokollkürzung gesichert, gekürzte Protokolle werden nicht gesichert.
Sichern Sie alle Transaktionsprotokolle	Wählen Sie Protokollsicherung. Alle Transaktionsprotokolle auf dem aktiven Dateisystem werden gesichert und es erfolgt keine Protokollkürzung. Auf derselben Festplatte wie das Live-Protokoll wird ein <i>scebackupinfo</i>-Verzeichnis erstellt. Dieses Verzeichnis enthält den Zeiger auf die inkrementellen Änderungen für die Exchange-Datenbank und ist nicht gleichbedeutend mit den vollständigen Protokolldateien.
Sichern Sie alle Datenbankdateien und Transaktionsprotokolle, ohne die Transaktionsprotokolldateien zu kürzen	Wählen Sie Backup kopieren. Alle Datenbanken und alle Protokolle werden gesichert und es erfolgt keine Protokollkürzung. Normalerweise verwenden Sie diesen Sicherungstyp zum erneuten Seeding eines Replikats oder zum Testen oder Diagnostizieren eines Problems.



Sie sollten den für Protokollsicherungen erforderlichen Speicherplatz auf Grundlage der vollständigen Sicherungsaufbewahrung und nicht auf Grundlage der minutengenauen (UTM) Aufbewahrung definieren.



Erstellen Sie beim Umgang mit Exchange-Volumes (LUNs) separate Tresorrichtlinien für Protokolle und Datenbanken und legen Sie die Aufbewahrungsdauer (Keep) für die Protokollrichtlinie für jedes Label auf die doppelte Zahl fest wie für die Datenbankrichtlinie, wobei Sie dieselben Labels verwenden. Weitere Informationen finden Sie unter ["SnapCenter für Exchange-Backups speichert nur die Hälfte der Snapshots auf dem Vault-Zielprotokollvolume"](#)

b. Wählen Sie im Abschnitt „Einstellungen der Datenbankverfügbarkeitsgruppe“ eine Aktion aus:

Für dieses Feld...	Machen Sie Folgendes...
Sichern aktiver Kopien	Wählen Sie diese Option, um nur die aktiven Kopien der ausgewählten Datenbank zu sichern. Bei Datenbankverfügbarkeitsgruppen (DAGs) sichert diese Option nur aktive Kopien aller Datenbanken in der DAG. Passive Kopien werden nicht gesichert.
Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen	Wählen Sie diese Option, um alle Kopien der Datenbanken auf den ausgewählten Servern (aktiv und passiv) zu sichern. Bei DAGs sichert diese Option sowohl aktive als auch passive Kopien aller Datenbanken auf den ausgewählten Servern.



In Clusterkonfigurationen werden die Sicherungen gemäß den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Knoten des Clusters aufbewahrt. Wenn sich der Besitzerknoten des Clusters ändert, bleiben die Sicherungen des vorherigen Besitzerknotens erhalten. Die Aufbewahrung gilt nur auf Knotenebene.

c. Wählen Sie im Abschnitt „Häufigkeit planen“ einen oder mehrere der Häufigkeitstypen aus: **Auf Anfrage, Stündlich, Täglich, Wöchentlich** und **Monatlich**.



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



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

a. Wählen Sie die Richtlinienbezeichnung aus.



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

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

Für dieses Feld...	Machen Sie Folgendes...
Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) aufzubewahren. Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.  Die Nur-Primär-Richtlinie kann nicht verwendet werden, wenn SnapMirror Active Sync für Exchange ONTAP -Volumes eingerichtet ist. SnapCenter lässt dies nicht zu. Sie sollten die Option „Spiegeln“ aktivieren. Durch Klicken auf die Schaltfläche Aktualisieren auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden. Sehen "Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“" .
Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen.
Fehleranzahl der Wiederholungsversuche	Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird.



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

6. Konfigurieren Sie auf der Seite „Aufbewahrung“ die Aufbewahrungseinstellungen.

Die angezeigten Optionen hängen vom Sicherungstyp und der Häufigkeit ab, die Sie zuvor ausgewählt haben.



Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden ONTAP Version unterstützt wird.



Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

- a. Wählen Sie im Abschnitt „Aufbewahrungseinstellungen für Protokollsicherungen“ eine der folgenden Optionen aus:

Wenn Sie wollen...	Machen Sie Folgendes...
Behalten Sie nur eine bestimmte Anzahl von Protokollsicherungen	Wählen Sie Anzahl der vollständigen Sicherungen, für die Protokolle aufbewahrt werden und geben Sie die Anzahl der vollständigen Sicherungen an, für die Sie eine minutengenaue Wiederherstellung wünschen. Die minutengenaue Aufbewahrung (UTM) gilt für Protokollsicherungen, die über eine vollständige oder Protokollsicherung erstellt wurden. Wenn beispielsweise die UTM-Aufbewahrungseinstellungen so konfiguriert sind, dass die Protokollsicherungen der letzten 5 vollständigen Sicherungen aufbewahrt werden, werden die Protokollsicherungen der letzten 5 vollständigen Sicherungen aufbewahrt. Die im Rahmen von Voll- und Log-Backups erstellten Log-Ordner werden im Rahmen von UTM automatisch gelöscht. Sie können die Protokollordner nicht manuell löschen. Wenn beispielsweise die Aufbewahrungseinstellung für die vollständige oder vollständige und Protokollsicherung auf 1 Monat und die UTM-Aufbewahrung auf 10 Tage eingestellt ist, wird der im Rahmen dieser Sicherungen erstellte Protokollordner gemäß UTM gelöscht. Infolgedessen sind nur 10-Tage-Protokollordner vorhanden und alle anderen Sicherungen sind für die Wiederherstellung zu einem bestimmten Zeitpunkt markiert. Sie können den UTM-Aufbewahrungswert auf 0 setzen, wenn Sie keine minutengenaue Wiederherstellung durchführen möchten. Dadurch wird die Wiederherstellung zu einem bestimmten Zeitpunkt ermöglicht. Best Practice: Es ist am besten, wenn die Einstellung der Einstellung für „Gesamtanzahl der Snapshots (vollständige Sicherungen)“ im Abschnitt „Einstellungen für die Aufbewahrung vollständiger Sicherungen“ entspricht. Dadurch wird sichergestellt, dass die Protokolldateien für jede vollständige Sicherung erhalten bleiben.

Wenn Sie wollen...	Machen Sie Folgendes...
Bewahren Sie die Sicherungskopien für eine bestimmte Anzahl von Tagen auf	Wählen Sie die Option Protokollsicherungen bis zuletzt aufbewahren und geben Sie die Anzahl der Tage an, für die die Protokollsicherungskopien aufbewahrt werden sollen. Die Protokollsicherungen werden bis zur Anzahl der Tage der vollständigen Sicherungen aufbewahrt.
Snapshot-Sperrzeitraum	Wählen Sie Sperrzeitraum für Snapshot-Kopie und wählen Sie Tage, Monate oder Jahre aus. Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.

Wenn Sie als Sicherungstyp **Protokollsicherung** ausgewählt haben, werden Protokollsicherungen als Teil der aktuellen Aufbewahrungseinstellungen für vollständige Sicherungen aufbewahrt.

- b. Wählen Sie im Abschnitt „Aufbewahrungseinstellungen für vollständige Sicherungen“ eine der folgenden Optionen für On-Demand-Sicherungen und dann eine für vollständige Sicherungen aus:

Für dieses Feld...	Machen Sie Folgendes...
Behalten Sie nur eine bestimmte Anzahl von Snapshots	Wenn Sie die Anzahl der aufzubewahrenden Vollsicherungen angeben möchten, wählen Sie die Option Gesamtzahl der aufzubewahrenden Snapshot-Kopien und geben Sie die Anzahl der aufzubewahrenden Snapshots (Vollsicherungen) an. Wenn die Anzahl der vollständigen Sicherungen die angegebene Zahl überschreitet, werden die vollständigen Sicherungen, die die angegebene Zahl überschreiten, gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.
Vollständige Backups für eine bestimmte Anzahl von Tagen aufbewahren	Wählen Sie die Option Snapshot-Kopien aufbewahren für und geben Sie die Anzahl der Tage an, die Snapshots (vollständige Backups) aufbewahrt werden sollen.
Sperrzeitraum für primäre Snapshots	Wählen Sie Sperrzeitraum für primäre Snapshot-Kopie und wählen Sie Tage, Monate oder Jahre aus. Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.

Für dieses Feld...	Machen Sie Folgendes...
Sperrzeitraum für sekundäre Snapshots	Wählen Sie Sperrzeitraum für sekundäre Snapshot-Kopie und wählen Sie Tage, Monate oder Jahre aus.

Wenn Sie auf einem Host in einer DAG-Konfiguration eine Datenbank mit nur Protokollsicherungen und ohne vollständige Sicherungen haben, werden die Protokollsicherungen auf folgende Weise aufbewahrt:

- Standardmäßig sucht SnapCenter die älteste vollständige Sicherung für diese Datenbank auf allen anderen Hosts im DAG und löscht alle Protokollsicherungen auf diesem Host, die vor der vollständigen Sicherung erstellt wurden.
- Sie können das oben genannte Standardaufbewahrungsverhalten für eine Datenbank auf einem Host in einem DAG mit ausschließlich Protokollsicherungen überschreiben, indem Sie den Schlüssel **MaxLogBackupOnlyCountWithoutFullBackup** in der Datei *C:\Program Files\NetApp\SnapCenter\WebApp\web.config* hinzufügen.

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

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

7. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Sicherungsvorgang ausgeführt werden soll.

- Zu den Prescript-Sicherungsargumenten gehören „\$Database“ und „\$ServerInstance“.
- Zu den Postscript-Sicherungsargumenten gehören „\$Database“, „\$ServerInstance“, „\$BackupName“, „\$LogDirectory“ und „\$LogSnapshot“.

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



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Exchange-Server hinzu

Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzauftrags, den Sie ausführen möchten, und den Schutzzeitplan zu definieren.

Informationen zu diesem Vorgang

- Der SCRIPTS_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad 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 des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.
- Das Hinzufügen neuer Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Zustand Ressourcen hinzufügen.

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 SnapCenter kürzlich eine Ressource 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 aus:

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie den Namen der Ressourcengruppe ein.  Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

Für dieses Feld...	Machen Sie Folgendes...
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: <code>customtext_resourcegroup_policy_hostname</code> oder <code>resourcegroup_hostname</code>. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

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

- a. Wählen Sie den Ressourcentyp und die Datenbankverfügbarkeitsgruppe aus Dropdown-Listen aus, um die Liste der verfügbaren Ressourcen zu filtern.



Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

In den Abschnitten „Verfügbare Ressourcen“ und „Ausgewählte Ressourcen“ wird der Datenbankname mit dem FQDN des Hosts angezeigt. Dieser FQDN zeigt nur an, dass die Datenbank auf diesem bestimmten Host aktiv ist und möglicherweise keine Sicherung auf diesem Host durchführt. Sie sollten aus der Serverauswahloption einen oder mehrere Sicherungsserver auswählen, auf denen Sie eine Sicherung durchführen möchten, falls Sie in der Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben.

- b. Geben Sie den Namen der Ressource in das Suchtextfeld ein oder scrollen Sie, um eine Ressource zu finden.
- c. Um Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben, führen Sie einen der folgenden Schritte aus:
 - Wählen Sie **Alle Ressourcen auf demselben Speichervolume automatisch auswählen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
 - Wählen Sie die Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.

Ressourcengruppen von SnapCenter für Microsoft Exchange Server können nicht mehr als 30 Datenbanken pro Snapshot haben. Wenn in einer Ressourcengruppe mehr als 30 Datenbanken vorhanden sind, wird für die zusätzlichen Datenbanken ein zweiter Snapshot erstellt. Daher werden unter dem Hauptsicherungsjob zwei Unterjobs erstellt. Bei Sicherungen mit sekundärer Replikation kann es während der Ausführung einer SnapMirror oder SnapVault -Aktualisierung zu Szenarien kommen, in denen sich die Aktualisierung für beide Unteraufträge überschneidet. Der Hauptsicherungsauftrag wird für immer weiter ausgeführt, auch wenn die Protokolle anzeigen, dass der Auftrag abgeschlossen ist.

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

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



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



Wenn eine Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** enthält, wird eine Serverauswahloption angezeigt, um einen oder mehrere Server auszuwählen. Die Serverauswahloption listet nur den Server auf, auf dem sich die ausgewählte Datenbank im NetApp -Speicher befindet.

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

- b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf  * **in der Spalte *Zeitpläne konfigurieren** für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **OK**.

Sie müssen dies für jede in der Richtlinie aufgeführte Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte **Angewandte Zeitpläne** im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

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

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

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

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

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

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

Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für Exchange Server

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

Bevor Sie beginnen

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

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen

ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

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

Schritte

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

Dieses Beispiel öffnet eine PowerShell-Sitzung:

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

2. Erstellen Sie eine neue Verbindung zum Speichersystem, indem Sie das `Add-SmStorageConnection` Cmdlet.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

3. Erstellen Sie ein neues Ausführen-als-Konto mithilfe des `Add-Credential` Cmdlet.

In diesem Beispiel wird ein neues „Ausführen als“-Konto mit dem Namen „ExchangeAdmin“ und Windows-Anmeldeinformationen erstellt:

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

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

Sichern Sie 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 vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten SVM zugewiesen haben.

- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn Sie eine Sicherung einer Datenbank oder einer Datenbankverfügbarkeitsgruppe durchführen möchten, die über eine aktive/passive Datenbankkopie auf einem NetApp und Nicht- NetApp -Speicher verfügt, und Sie in der Richtlinie die Option **Aktive Kopien sichern** oder **Kopien auf Servern sichern, die während der Erstellungszeit des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben, wechseln die Sicherungsaufträge in den Warnzustand. Die Sicherung ist für die aktive/passive Datenbankkopie auf NetApp -Speicher erfolgreich, für die aktive/passive Datenbankkopie auf Nicht-NetApp -Speicher schlägt die Sicherung fehl.

Best Practice: Führen Sie nicht gleichzeitig Backups von aktiven und passiven Datenbanken durch. Es kann zu einem Race Condition kommen und eine der Sicherungen kann fehlschlagen.

SnapCenter -Benutzeroberfläche

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 „Datenbankverfügbarkeitsgruppe“ aus der Liste „Anzeigen“ aus.

Auf der Seite „Ressourcen“ wird  Das Symbol zeigt an, dass sich die Datenbank auf einem Nicht-NetApp -Speicher befindet.



Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und mindestens eine passive Datenbankkopie auf einem NetApp -Speicher liegt, 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 auf * klicken.  *, um den Filterbereich zu schließen.

- Wenn Sie eine Datenbank sichern möchten, klicken Sie auf den Datenbanknamen.
 - i. Wenn die Topologieansicht angezeigt wird, klicken Sie auf **Schützen**.
 - ii. Wenn der Assistent „Datenbank – Ressource schützen“ angezeigt wird, fahren Sie mit Schritt 3 fort.
 - Wenn Sie eine Datenbankverfügbarkeitsgruppe sichern möchten, klicken Sie auf den Namen der Datenbankverfügbarkeitsgruppe.
3. 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: *customtext_policy_hostname* oder *resource_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

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

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



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



Wenn eine Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** enthält, wird eine Serverauswahloption angezeigt, um einen oder mehrere Server auszuwählen. Die Serverauswahloption listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf einem NetApp -Speicher befindet.

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

- b.

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

Zeitplan konfigurieren möchten.

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

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

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

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

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



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

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

Die Seite „Datenbanktopologie“ wird angezeigt.

7. Klicken Sie auf **Jetzt sichern**.

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

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

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

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

9. Überwachen Sie den Fortschritt der Sicherung, indem Sie im Aktivitätsbereich unten auf der Seite auf den Auftrag doppelklicken, um die Seite mit den Auftragsdetails anzuzeigen.

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

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

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

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

PowerShell-Cmdlets

Schritte

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

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

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

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

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit einem vollständigen Backup und einem Protokoll-Backup vom Exchange-Sicherungstyp erstellt:

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

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit einem stündlichen vollständigen Backup und einem Protokoll-Backup vom Exchange-Sicherungstyp erstellt:

```
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 Sicherungsrichtlinie erstellt, um nur Exchange-Protokolle zu sichern:

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

3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „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 SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

In diesem Beispiel wird eine neue Exchange Server-Datenbanksicherungsressourcengruppe 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_bkp_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'}
```

In diesem Beispiel wird eine neue Backup-Ressourcengruppe für die Exchange Database Availability Group (DAG) mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
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_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

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

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

In diesem Beispiel wird eine neue Sicherung auf einem sekundären Speicher erstellt:

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

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

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

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

In diesem Beispiel wird ein Auftragszusammenfassungsbericht für eine bestimmte Auftrags-ID angezeigt:

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie

durch Ausführen von *Get-Help command_name*. Alternativ siehe ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

Sichern von Exchange-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG und die Ressourcengruppe kann entweder einen ganzen DAG oder einzelne Datenbanken umfassen. Sie können die Ressourcengruppen von der Seite „Ressourcen“ aus sichern.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet beginnt. Sie sollten den Wert von konfigurieren `MaxRetryForUninitializedHosts` In `web.config` mithilfe der `Set-SmConfigSettings` PowerShell-Cmdlet.
- Wenn Sie in einer Ressourcengruppe eine Datenbank oder Datenbankverfügbarkeitsgruppe einschließen, die über eine aktive/passive Datenbankkopie auf einem NetApp und Nicht- NetApp -Speicher verfügt, und Sie in der Richtlinie die Option **Aktive Kopien sichern** oder **Kopien auf Servern sichern, die während der Erstellungszeit des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben, wechseln die Sicherungsaufträge in den Warnzustand.

Die Sicherung ist für die aktive/passive Datenbankkopie auf NetApp -Speicher erfolgreich, für die aktive/passive Datenbankkopie auf Nicht- NetApp -Speicher schlägt die Sicherung fehl.

Informationen zu diesem Vorgang

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

Schritte

1. 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 „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf * klicken.  * und wählen Sie dann das Tag aus. Sie können dann auf * klicken.  *, um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

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

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

- b. Klicken Sie auf **Sichern**.
5. Überwachen Sie den Fortschritt der Sicherung, indem Sie im Aktivitätsbereich unten auf der Seite auf den Auftrag doppelklicken, um die Seite mit den Auftragsdetails anzuzeigen.

Überwachen von Sicherungsvorgängen

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

Informationen zu diesem Vorgang

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Jobs**.
3. Führen Sie auf der Seite „Jobs“ die folgenden Schritte aus:
 - a. Klicken  um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
 - b. Geben Sie das Start- und Enddatum an.
 - c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
 - d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
 - e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.



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

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

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

Überwachen von Vorgängen im Aktivitätsbereich

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

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

Schritte

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

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

Abbrechen von Sicherungsvorgängen für die Exchange-Datenbank

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

Was Sie brauchen

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“

Wenn Sie die Sicherung einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen auf dem primären und sekundären Speicher anzuzeigen.

Informationen zu diesem Vorgang

Auf der Seite „Topologie“ können Sie alle Sicherungen sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

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

-  zeigt die Anzahl der Sicherungen an, die auf dem primären Speicher verfügbar sind.
-  zeigt die Anzahl der Sicherungen an, die mithilfe der SnapMirror -Technologie auf dem sekundären Speicher gespiegelt werden.
-  zeigt die Anzahl der Sicherungen an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.
 - Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups.

Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.

Best Practice: Um sicherzustellen, dass die richtige Anzahl replizierter Sicherungen angezeigt wird, empfehlen wir Ihnen, die Topologie zu aktualisieren.

Wenn Sie eine sekundäre Beziehung als SnapMirror Active Sync haben (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), können Sie die folgenden zusätzlichen Symbole sehen:

-  Die Replikationssite ist aktiv.
-  Die Replikationssite ist ausgefallen.
-  Die sekundäre Spiegel- oder Tresorbeziehung wurde nicht wiederhergestellt.

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

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

4. Im Abschnitt „Zusammenfassungskarte“ finden Sie eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen.

Im Abschnitt „Zusammenfassungskarte“ werden die Gesamtzahl der Sicherungen und die Gesamtzahl der Protokollsicherungen angezeigt.

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

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

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

Bei der aktiven Synchronisierung von SnapMirror wird durch Klicken auf die Schaltfläche **Aktualisieren** das SnapCenter -Sicherungsinventar aktualisiert, indem ONTAP sowohl nach primären als auch nach Replikationsstandorten abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken aus, die eine aktive Synchronisierungsbeziehung mit SnapMirror enthalten.

- Für SnapMirror Active Sync und nur für ONTAP 9.14.1 sollten Async Mirror- oder Async MirrorVault-Beziehungen zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault nach dem Failover automatisch auf das neue primäre Ziel konfiguriert.
- Nach dem Failover sollte ein Backup für SnapCenter erstellt werden, um über das Failover informiert

zu sein. Sie können erst auf **Aktualisieren** klicken, nachdem eine Sicherung erstellt wurde.

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

Die Details der Sicherungen werden in einem Tabellenformat angezeigt.

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



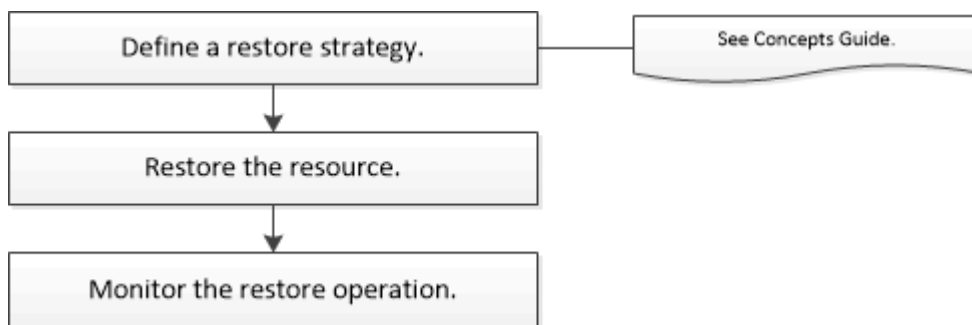
Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch löschen. Das Löschen von Snapshots wird durch die ONTAP Aufbewahrungseinstellungen geregelt.

Wiederherstellen von Exchange-Ressourcen

Wiederherstellungs-Workflow

Sie können SnapCenter verwenden, um Exchange-Datenbanken wiederherzustellen, indem Sie eine oder mehrere Sicherungen in Ihrem aktiven Dateisystem wiederherstellen.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Wiederherstellungsvorgänge für die Exchange-Datenbank durchführen müssen:



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

Voraussetzungen 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 den SnapCenter Server als auch das SnapCenter -Plug-in für die Exchange-Datenbank auf 4.6 aktualisieren.

- Der Exchange-Server muss online und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.

- Die Datenbanken müssen auf dem Exchange-Server vorhanden sein.



Das Wiederherstellen gelöschter Datenbanken wird nicht unterstützt.

- SnapCenter -Zeitpläne für die Datenbank müssen ausgesetzt werden.
- Der SnapCenter -Server und das SnapCenter -Plug-in für den Microsoft Exchange Server-Host müssen mit dem primären und sekundären Speicher verbunden sein, der die wiederherzustellenden Sicherungen enthält.

Wiederherstellen von Exchange-Datenbanken

Sie können SnapCenter verwenden, um gesicherte Exchange-Datenbanken wiederherzustellen.

Bevor Sie beginnen

- Sie müssen die Ressourcengruppen, Datenbanken oder Datenbankverfügbarkeitsgruppen (DAGs) gesichert haben.
- Wenn die Exchange-Datenbank an einen anderen Speicherort migriert wird, funktioniert der Wiederherstellungsvorgang für alte Sicherungen nicht.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und Sie eine Wiederherstellung aus der Sicherung der passiven Datenbankkopie durchführen möchten, die sich auf einem NetApp -Speicher befindet, machen Sie die passive Kopie (NetApp -Speicher) zur aktiven Kopie, aktualisieren Sie die Ressourcen und führen Sie den Wiederherstellungsvorgang durch.

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

Der "[Microsoft-Dokumentation](#)" enthält Informationen zu diesem Befehl.

Informationen zu diesem Vorgang

- Wenn ein Wiederherstellungsvorgang für eine Datenbank ausgeführt wird, wird die Datenbank wieder auf demselben Host bereitgestellt und es wird kein neues Volume erstellt.
- Sicherungen auf DAG-Ebene müssen aus einzelnen Datenbanken wiederhergestellt werden.
- Die vollständige Datenträgerwiederherstellung wird nicht unterstützt, wenn andere Dateien als die Exchange-Datenbankdatei (.edb) vorhanden sind.

Das Plug-in für Exchange führt keine vollständige Wiederherstellung einer Festplatte durch, wenn die Festplatte Exchange-Dateien enthält, wie sie beispielsweise für die Replikation verwendet werden. Wenn eine vollständige Wiederherstellung die Exchange-Funktionalität beeinträchtigen könnte, führt das Plug-in für Exchange einen einzelnen Dateiwiederherstellungsvorgang durch.

- Das Plug-in für Exchange kann mit BitLocker verschlüsselte Laufwerke nicht wiederherstellen.
- Der `SCRIPTS_PATH` wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad 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 des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.
- Für den Wiederherstellungsvorgang mit SnapMirror Active Sync müssen Sie die Sicherung vom primären Speicherort auswählen.

SnapCenter -Benutzeroberfläche

Schritte

1. Klicken Sie im linken Navigationsbereich oben links auf der Ressourcenseite 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 „Kopien verwalten“ in der Tabelle „Primäre Sicherungen“ die Option „Sicherungen“ aus und klicken Sie dann auf „*“ .
6. Wählen Sie auf der Seite „Optionen“ eine der folgenden Protokollsicherungsoptionen aus:

Option	Beschreibung
Alle Protokollsicherungen	Wählen Sie Alle Protokollsicherungen , um einen minutengenauen Sicherungswiederherstellungsvorgang durchzuführen und alle verfügbaren Protokollsicherungen nach der vollständigen Sicherung wiederherzustellen.
Durch Log-Backups bis	Wählen Sie Nach Protokollsicherungen bis, um eine zeitpunktbezogene Wiederherstellung durchzuführen, bei der die Datenbank basierend auf Protokollsicherungen bis zum ausgewählten Protokoll wiederhergestellt wird.  Die Anzahl der in der Dropdown-Liste angezeigten Protokolle basiert auf UTM. Wenn beispielsweise die vollständige Sicherungsaufbewahrung 5 und die UTM-Aufbewahrung 3 beträgt, ist die Anzahl der verfügbaren Protokollsicherungen 5, aber in der Dropdown-Liste werden nur 3 Protokolle aufgelistet, um den Wiederherstellungsvorgang durchzuführen.
Nach einem bestimmten Datum bis	Wählen Sie Nach bestimmtem Datum bis , um das Datum und die Uhrzeit anzugeben, bis zu der Transaktionsprotokolle auf die wiederhergestellte Datenbank angewendet werden. Dieser Point-in-Time-Wiederherstellungsvorgang stellt Transaktionsprotokolleinträge wieder her, die bis zur letzten Sicherung am angegebenen Datum und zur angegebenen Uhrzeit aufgezeichnet wurden.

Option	Beschreibung
Keine	Wählen Sie Keine , wenn Sie nur die vollständige Sicherung ohne Protokollsicherungen wiederherstellen müssen.

Sie können eine der folgenden Aktionen ausführen:

- **Datenbank nach der Wiederherstellung wiederherstellen und mounten** – Diese Option ist standardmäßig ausgewählt.
- **Überprüfen Sie vor der Wiederherstellung nicht die Integrität der Transaktionsprotokolle im Backup.** – Standardmäßig überprüft SnapCenter die Integrität der Transaktionsprotokolle in einem Backup, bevor ein Wiederherstellungsvorgang durchgeführt wird.

Best Practice: Sie sollten diese Option nicht auswählen.

7. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Wiederherstellungsvorgang ausgeführt werden soll.

Zu den Argumenten des Wiederherstellungsvorskripts gehören \$Database und \$ServerInstance.

Zu den Postscript-Argumenten für die Wiederherstellung gehören \$Database, \$ServerInstance, \$BackupName, \$LogDirectory und \$TargetServerInstance.

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



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

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

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

10. Sie können den Status des Wiederherstellungsauftrags anzeigen, indem Sie das Aktivitätsfenster unten auf der Seite erweitern.

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

Wenn Sie eine aktive Datenbank aus einer Sicherung wiederherstellen, kann die passive Datenbank in den Zustand „Angehalten“ oder „Fehler“ wechseln, wenn zwischen dem Replikat und der aktiven Datenbank eine Verzögerung auftritt.

Die Statusänderung kann auftreten, wenn sich die Protokollkette der aktiven Datenbank verzweigt und einen neuen Zweig beginnt, der die Replikation unterbricht. Exchange Server versucht, das Replikat zu reparieren. Wenn dies jedoch nicht gelingt, sollten Sie nach der Wiederherstellung eine neue Sicherung erstellen und dann das Replikat erneut initialisieren.

PowerShell-Cmdlets

Schritte

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

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

2. Rufen Sie die Informationen zu den Backups ab, die Sie wiederherstellen möchten, indem Sie die `Get-SmBackup Cmdlet`.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
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 der Sicherung wieder her, indem Sie das `Restore-SmBackup Cmdlet`.

In diesem Beispiel wird eine aktuelle Sicherung 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 eine zeitpunktbezogene Sicherung 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 eine Sicherung auf dem sekundären Speicher im primären Speicher wiederhergestellt:

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

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

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

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

Granulare Wiederherstellung von E-Mails und Postfächern

Mit der Single Mailbox Recovery (SMBR)-Software können Sie E-Mails oder Postfächer anstelle der gesamten Exchange-Datenbank wiederherstellen.

Das Wiederherstellen einer kompletten Datenbank, nur um eine einzelne E-Mail wiederherzustellen, kostet viel Zeit und Ressourcen. SMBR hilft bei der schnellen Wiederherstellung der E-Mails, indem es eine Klonkopie des Snapshots erstellt und dann Microsoft-APIs verwendet, um das Postfach in SMBR zu mounten. Informationen zur Verwendung von SMBR finden Sie unter ["SMBR-Administrationshandbuch"](#) .

Weitere Informationen zu SMBR finden Sie hier:

- ["So stellen Sie ein einzelnes Element manuell mit SMBR wieder her \(gilt auch für Ontrack Power Control-Wiederherstellungen\)"](#)
- ["So stellen Sie mit SnapCenter vom sekundären Speicher in SMBR wieder her"](#)
- ["Wiederherstellen von Microsoft Exchange-E-Mails aus SnapVault mithilfe von SMBR"](#)

Wiederherstellen einer Exchange Server-Datenbank aus einem sekundären Speicher

Sie können eine gesicherte Exchange Server-Datenbank aus einem sekundären Speicher (Spiegel oder Tresor) wiederherstellen.

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

Informationen zu diesem Vorgang

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.
- Für den Wiederherstellungsvorgang mit SnapMirror Active Sync müssen Sie die Sicherung vom primären Speicherort auswählen.

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“ aus der Dropdownliste „Anzeigen“ die Option „Datenbank“ oder „Ressourcengruppe“ aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus.

Die Seite mit der Datenbank- oder Ressourcengruppentopologie wird angezeigt.

4. Wählen Sie im Abschnitt „Kopien verwalten“ **Backups** aus dem sekundären Speichersystem (Spiegel oder Tresor) aus.
5. Wählen Sie das Backup aus der Liste aus und klicken Sie dann auf  .
6. Wählen Sie auf der Seite „Speicherort“ das Zielvolume für die Wiederherstellung der ausgewählten Ressource aus.
7. Schließen Sie den Wiederherstellungsassistenten ab, überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Reseed einer passiven Exchange-Knotenreplik

Wenn Sie eine Replikatkopie neu initialisieren müssen, beispielsweise wenn eine Kopie beschädigt ist, können Sie mithilfe der Reseed-Funktion in SnapCenter ein Reseed auf die neueste Sicherung durchführen.

Bevor Sie beginnen

Sie müssen eine Sicherungskopie der Datenbank erstellt haben, die Sie neu befüllen möchten.

+ Um Verzögerungen zwischen Knoten zu vermeiden, können Sie entweder vor der Durchführung eines Reseed-Vorgangs ein neues Backup erstellen oder den Host mit dem neuesten Backup auswählen.

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 „Anzeigen“ aus:

Option	Beschreibung
So führen Sie ein erneutes Seeding für eine einzelne Datenbank durch	Wählen Sie Datenbank aus der Ansichtsliste.
So führen Sie ein erneutes Seeding von Datenbanken in einer DAG durch	Wählen Sie Datenbankverfügbarkeitsgruppe aus der Liste „Anzeigen“ aus.

3. Wählen Sie die Ressource aus, die Sie neu säen möchten.
4. Klicken Sie auf der Seite „Kopien verwalten“ auf **Neu säen**.
5. Wählen Sie im Reseed-Assistenten aus der Liste der fehlerhaften Datenbankkopien diejenige aus, für die Sie ein Reseed durchführen möchten, und klicken Sie dann auf **Weiter**.
6. Wählen Sie im Host-Fenster den Host mit dem Backup aus, von dem Sie ein Reseed durchführen möchten, und klicken Sie dann auf **Weiter**.

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

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

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



Der Reseed-Vorgang wird nicht unterstützt, wenn sich die passive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet.

Führen Sie mithilfe von PowerShell-Cmdlets für die Exchange-Datenbank ein erneutes Seeding eines Replikats durch

Sie können PowerShell-Cmdlets verwenden, um ein fehlerhaftes Replikat wiederherzustellen, indem Sie entweder die neueste Kopie auf demselben Host oder die neueste Kopie von einem anderen Host verwenden.

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

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer mithilfe der *Open-SmConnection* Cmdlet.

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

2. Führen Sie ein erneutes Seeding der Datenbank durch, indem Sie *reseed-SmDagReplicaCopy* Cmdlet.

In diesem Beispiel wird die fehlgeschlagene Kopie der Datenbank mit dem Namen „execdb“ auf dem Host „mva-rx200.netapp.com“ mithilfe der neuesten Sicherung auf diesem Host neu gestartet.

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

In diesem Beispiel wird für die fehlgeschlagene Kopie der Datenbank mit dem Namen „execdb“ ein neues Seeding durchgeführt. Dabei wird die neueste Sicherung der Datenbank (Produktion/Kopie) auf einem alternativen Host „mva-rx201.netapp.com“ verwendet.

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

Überwachen von Wiederherstellungsvorgängen

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

Informationen zu diesem Vorgang

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

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

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

Schritte

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

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

Abbrechen von Wiederherstellungsvorgängen für die Exchange-Datenbank

Sie können in der Warteschlange befindliche Wiederherstellungsaufträge abbrechen.

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

Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Wiederherstellungsvorgang entweder auf der Seite

Überwachen oder im Bereich **Aktivität** abbrechen.

- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der...	Aktion
Monitorseite	1. Klicken Sie im linken Navigationsbereich auf Monitor > Jobs. 2. Wählen Sie den Auftrag aus und klicken Sie auf Auftrag abbrechen.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite „Auftragsdetails“ auf Auftrag 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 IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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