Dokumentation zum SnapCenter Plug-in für VMware vSphere

SnapCenter Plug-in for VMware vSphere 6.2

NetApp
December 09, 2025

Inhalt

Dokumentation zum SnapCenter Plug-in für VMware vSphere

Versionshinweise

Versionshinweise zum SnapCenter Plug-in für VMware vSphere

Informieren Sie sich über die neuen und verbesserten Funktionen des SnapCenter Plug-in for VMware vSphere 6.2.

Einzelheiten zu bekannten Problemen, Einschränkungen und behobenen Problemen finden Sie unter "Versionshinweise zum SnapCenter Plug-in for VMware vSphere 6.2" . Sie müssen sich mit Ihrem NetApp -Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zugreifen zu können.

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

Was ist neu im SnapCenter Plug-in for VMware vSphere 6.2

Informieren Sie sich über die neuen Funktionen des SnapCenter Plug-in for VMware vSphere 6.2.

Das SnapCenter Plug-in for VMware vSphere 6.2 bietet Unterstützung für die Sicherung und Wiederherstellung virtueller Maschinen (VMs) auf VMFS-Datenspeichern für ASA r2-Systeme mit ONTAP 9.17.1 oder höher. Mit dieser Version können Sie die folgenden Vorgänge für VMs, Datenspeicher und das Virtual Machine Disk (VMDK)-Format auf ASA r2-Systemen durchführen:

- Bereitstellen von Konsistenzgruppen für den primären Schutz
- Durchführen von Konsistenzgruppen-basierten Backups
- Verwenden Sie hierarchische Konsistenzgruppen (verfügbar mit ONTAP 9.17.1 und späteren Versionen)
- Ausführen von Klon-Workflows
- Ausführen von Wiederherstellungsworkflows
- Stellen Sie beim Erstellen oder Ändern von Ressourcengruppen einen sekundären Schutz bereit (verfügbar mit ONTAP 9.16.1 und späteren Versionen)

Ab dieser Version unterstützt das SnapCenter Plug-in for VMware vSphere Amazon FSxN für NetApp ONTAP -Speichersysteme ab Version 9.10.

Upgrade-Pfade

Die Version des SnapCenter-Plug-ins für VMware vSphere (SCV), auf die Sie aktualisieren können, hängt von der aktuellen Version ab.

Das Upgrade auf das SnapCenter-Plug-in für VMware vSphere (SCV) 4.8 und höher wird nur auf VMware vCenter Server 7 Update 1 und höheren Versionen unterstützt. Für VMware vCenter-Server vor Version 7 Update 1 sollten Sie SCV 4.7 weiterhin verwenden.

Wenn Sie die SCV-Version… verwenden	Sie können SCV direkt auf… aktualisieren
SCV 6,1	SCV 6,2
SCV 6,0	SCV 6.1 und SCV 6.2
SCV 5,0	SCV 6.0 und SCV 6.1
SCV 4.9	SCV 5.0 und SCV 6.0

Bei virtualisierten Datenbanken und Filesystemen, die mit SnapCenter integriert sind, handelt es sich um einen Upgrade-Pfad:

Wenn Sie verwenden	Wenn Ihr VMware Plug-in… lautet	Sie können direkt auf… upgraden
SnapCenter 6.2	SCV 6,1	SCV 6,2
SnapCenter 6.1	SCV 6,0	SCV 6,1
SnapCenter 6.0	SCV 5,0	SCV 6,0
SnapCenter 5.0	SCV 4.9	SCV 5,0
SnapCenter 4.9	SCV 4.8	SCV 4.9
SnapCenter 4.8	SCV 4.7	SCV 4.8

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" (IMT).

Konzepte

Produktübersicht

Das SnapCenter Plug-in für VMware vSphere wird als virtuelle Linux-basierte Appliance bereitgestellt.

Das SnapCenter Plug-in für VMware vSphere erweitert Ihre Umgebung um folgende Funktionen:

- Unterstützung von VM-konsistenten und absturzkonsistenten Datensicherungsvorgängen

  Sie können die VMware vSphere-Client-Benutzeroberfläche in vCenter für alle Sicherungs- und Wiederherstellungsvorgänge von virtuellen VMware-Maschinen (herkömmliche VMs und vVol-VMs), VMDKs und Datenspeichern verwenden. Für vVol-VMs (VMs in vVol-Datenspeichern) werden nur absturzkonsistente Backups unterstützt. Sie können auch VMs und VMDKs wiederherstellen und Dateien und Ordner wiederherstellen, die sich auf einem Gastbetriebssystem befinden.

  Beim Backup von VMs, VMDKs und Datastores unterstützt das Plug-in keine RDMs. Backup-Jobs für VMs ignorieren RDMs. Wenn Sie RDMs sichern müssen, müssen Sie ein SnapCenter-Applikations-basiertes Plug-in.

  Das SnapCenter Plug-in für VMware vSphere umfasst eine MySQL Datenbank mit dem SnapCenter Plug-in für VMware vSphere Metadaten. Für die VM-konsistente und absturzkonsistente Datensicherung müssen Sie den SnapCenter Server nicht installieren.

- Unterstützung für applikationskonsistente(Applikations-over VMDK/RDM) Datensicherungsvorgänge

  Sie können die SnapCenter Benutzeroberfläche und die entsprechenden SnapCenter -Anwendungs-Plug -Ins für alle Sicherungs- und Wiederherstellungsvorgänge von Datenbanken und Dateisystemen auf primären und sekundären Speichern auf VMs verwenden.

  SnapCenter nutzt das SnapCenter Plug-in für VMware vSphere nativ für alle Datensicherungsvorgänge auf VMDKs, Raw Device Mappings (RDMs) und NFS-Datastores. Nach der Implementierung der virtuellen Appliance ist das Plug-in für alle Interaktionen mit vCenter zuständig. Das SnapCenter Plug-in für VMware vSphere unterstützt alle applikationsbasierten SnapCenter Plug-ins.

  SnapCenter unterstützt keine einzelnen Snapshots von Datenbanken und VMs zusammen. Backups für VMs und Datenbanken müssen unabhängig voneinander geplant und ausgeführt werden, wodurch separate Snapshots erstellt werden, selbst wenn die Datenbanken und VMs auf demselben Volume gehostet werden. Planen Sie die Datenbankanwendungssicherungen mithilfe der SnapCenter -Benutzeroberfläche; planen Sie die VM- und Datenspeichersicherungen mithilfe der VMware vSphere-Client-Benutzeroberfläche.

- Für VM-konsistente Snapshots sind VMware Tools erforderlich

  Wenn die VMware Tools nicht installiert sind und ausgeführt werden, wird das Filesystem nicht stillgelegt und ein Crash-konsistenter Snapshot erstellt.

- VMware Storage vMotion ist für die Wiederherstellung von SAN-Umgebungen (VMFS) erforderlich

  Der Wiederherstellungsworkflow für das VMware Filesystem (VMFS) verwendet die VMware Storage vMotion Funktion. Storage vMotion ist Teil der vSphere Standard Lizenz, ist jedoch nicht mit den Lizenzen vSphere Essentials oder Essentials Plus erhältlich.

  Die meisten Restore-Vorgänge in NFS-Umgebungen verwenden native ONTAP-Funktionen (z. B. Single

File SnapRestore) und erfordern kein VMware Storage vMotion.

- Für die Konfiguration von VMware vVol VMs sind ONTAP Tools für VMware vSphere erforderlich.

  Mit ONTAP-Tools können Sie Storage für VVols in ONTAP und im VMware Web-Client bereitstellen und konfigurieren.

  Weitere Informationen finden Sie in der Dokumentation zu den ONTAP tools for VMware vSphere . Weitere Informationen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" für aktuelle Informationen zu den unterstützten Versionen der ONTAP Tools.

- Das SnapCenter Plug-in für VMware vSphere wird als virtuelle Appliance in einer Linux VM bereitgestellt

  Obwohl die virtuelle Appliance als Linux VM installiert werden muss, unterstützt das SnapCenter Plug-in für VMware vSphere sowohl Windows-basierte als auch Linux-basierte vCenter. SnapCenter verwendet dieses Plug-in nativ ohne Eingreifen des Benutzers, um mit Ihrem vCenter zu kommunizieren und auf SnapCenter basierende Plug-ins zu unterstützen, die Datensicherungsvorgänge für virtualisierte Windows und Linux Applikationen durchführen.

Neben diesen wichtigen Funktionen bietet das SnapCenter Plug-in für VMware vSphere auch Unterstützung für iSCSI, Fibre Channel, FCoE, NFS 3.0/4.1, VMFS 5.0/6.0, NVMe over FC und NVMe over TCP.

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" (IMT).

Informationen zu NFS-Protokollen und ESXi-Host finden Sie in der vSphere Storage-Dokumentation, die von VMware bereitgestellt wird.

Weitere Informationen zum SnapCenter Datenschutz finden Sie in den Datenschutzinformationen zu Ihrem SnapCenter-Plug-in in der "SnapCenter-Dokumentation".

Informationen zu unterstützten Upgrade- und Migrationspfaden finden Sie unter "SnapCenter Plug-in für VMware vSphere – Versionsinformationen".

Übersicht über die verschiedenen SnapCenter -Benutzeroberflächen

In Ihrer SnapCenter -Umgebung müssen Sie die entsprechende Benutzeroberfläche verwenden, um Datenschutz- und Verwaltungsvorgänge durchzuführen.

Das SnapCenter Plug-in for VMware vSphere ist ein eigenständiges Plug-in, das sich von anderen SnapCenter -Plug-ins unterscheidet. Sie müssen die VMware vSphere-Client-Benutzeroberfläche in vCenter für alle Sicherungs- und Wiederherstellungsvorgänge für VMs, VMDKs und Datenspeicher verwenden. Sie verwenden auch das Dashboard der Webclient-Benutzeroberfläche, um die Liste der geschützten und ungeschützten VMs zu überwachen. Für alle anderen SnapCenter -Plug-In-Vorgänge (anwendungsbasierte Plug-Ins) wie Backup und Wiederherstellung sowie Auftragsüberwachung verwenden Sie die SnapCenter Benutzeroberfläche.

Zum Schutz von VMs und Datenspeichern verwenden Sie die VMware vSphere-Clientschnittstelle. Die Benutzeroberfläche des Webclients lässt sich in die NetApp Snapshot-Technologie auf dem Speichersystem integrieren. Auf diese Weise können Sie VMs und Datenspeicher in Sekundenschnelle sichern und VMs wiederherstellen, ohne einen ESXi-Host offline zu nehmen.

Es gibt auch eine Verwaltungsbenutzeroberfläche zum Durchführen administrativer Vorgänge am SnapCenter Plug-in for VMware vSphere.

Die folgende Tabelle zeigt die Vorgänge, die die SnapCenter Benutzeroberfläche ausführt.

Verwenden Sie diese Benutzeroberfläche…	Zur Ausführung dieser Vorgänge…	Und für den Zugriff auf diese Backups…
SnapCenter vSphere-Client-Benutzeroberfläche	VM- und Datastore-Backup VMDK-Anbindung und -Trennung Datastore-Mount und unmounten Sie VM und VMDK Restore der Gastdatei und Ordner	Sicherungen von VMs und Datenspeichern mithilfe der VMware vSphere-Client-Benutzeroberfläche.
SnapCenter -Benutzeroberfläche	Backup und Restore von Datenbanken und Applikationen auf VMs, einschließlich der Sicherung von Datenbanken für Microsoft SQL Server, Microsoft Exchange und Oracle. Datenbankklone	Mithilfe der SnapCenter Benutzeroberfläche durchgeführte Sicherungen.
SnapCenter Plug-in for VMware vSphere Verwaltungsbenutzeroberfläche	Ändern der Netzwerkkonfiguration Erstellen Sie ein Supportpaket Ändern der NTP-Servereinstellungen Deaktivieren/Aktivieren des Plug-ins	N.A.
vCenter-Benutzeroberfläche	Hinzufügen von SCV-Rollen zu vCenter Active Directory-Benutzern Hinzufügen von Ressourcenzugriff für Benutzer oder Gruppen	N.A.

Für VM-konsistente Sicherungs- und Wiederherstellungsvorgänge müssen Sie die Benutzeroberfläche des VMware vSphere-Clients verwenden. Obwohl es möglich ist, einige Vorgänge mithilfe von VMware-Tools auszuführen, beispielsweise das Mounten oder Umbenennen eines Datenspeichers, werden diese Vorgänge nicht im SnapCenter -Repository registriert und nicht erkannt.

SnapCenter unterstützt keine einzelnen Snapshots von Datenbanken und VMs zusammen. Sicherungen für VMs und Datenbanken müssen unabhängig voneinander geplant und ausgeführt werden, wodurch separate Snapshots erstellt werden, selbst wenn die Datenbanken und VMs auf demselben Volume gehostet werden. Anwendungsbasierte Sicherungen müssen über die SnapCenter -Benutzeroberfläche geplant werden; VM-konsistente Sicherungen müssen über die VMware vSphere-Client-Benutzeroberfläche geplant werden.

Lizenzierung

Das SnapCenter Plug-in für VMware vSphere ist ein kostenloses Produkt, wenn Sie die folgenden Storage-Systeme verwenden:

- Lokale ONTAP Cluster (FAS, AFF und ASA Systeme)
- Cloud Volumes ONTAP
- ONTAP Select

Es wird empfohlen, aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen

hinzufügen. Wenn SnapCenter Standardlizenzen nicht auf sekundären Systemen aktiviert sind, können Sie SnapCenter nach einem Failover-Vorgang nicht verwenden. Allerdings ist eine FlexClone Lizenz auf sekundärem Storage erforderlich, um Mount- und Attached-Vorgänge durchzuführen. Zur Durchführung von Restore-Vorgängen ist eine SnapRestore Lizenz erforderlich.

Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)

Das SnapCenter Plug-in für VMware vSphere bietet zusätzliche RBAC-Funktionen für das Management virtualisierter Ressourcen. Das Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC.

Die rollenbasierte Zugriffssteuerung von SnapCenter und ONTAP gilt nur für applikationskonsistente Aufgaben des SnapCenter Servers (Applikation über VMDK). Wenn Sie das SnapCenter-Plug-in für VMware vSphere zur Unterstützung von anwendungskonsistenten SnapCenter-Jobs verwenden, müssen Sie die SnapCenterAdmin-Rolle zuweisen. Sie können die Berechtigungen der SnapCenterAdmin-Rolle nicht ändern.

Das SnapCenter Plug-in for VMware vSphere wird mit vordefinierten vCenter-Rollen geliefert. Sie müssen die vCenter-Benutzeroberfläche verwenden, um diese Rollen vCenter Active Directory-Benutzern hinzuzufügen, damit Sie SnapCenter Vorgänge ausführen können.

Sie können jederzeit Rollen erstellen und ändern und Benutzern Zugriff auf Ressourcen hinzufügen. Wenn Sie jedoch das SnapCenter-Plug-in für VMware vSphere zum ersten Mal einrichten, sollten Sie mindestens Active Directory-Benutzer oder -Gruppen zu Rollen hinzufügen und diesen Benutzern oder Gruppen dann Ressourcenzugriff hinzufügen.

RBAC-Typen für SnapCenter Plug-in für VMware vSphere Benutzer

Wenn Sie das SnapCenter Plug-in für VMware vSphere nutzen, bietet der vCenter Server zusätzliche RBAC-Funktionen. Das Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC.

RBAC für vCenter Server

Dieser Sicherheitsmechanismus gilt für alle Jobs, die vom SnapCenter-Plug-in für VMware vSphere ausgeführt werden. Zu diesen Aufgaben gehören VM-konsistente, absturzkonsistente VM- und SnapCenter-Server-Jobs (Applikation über VMDK). Diese RBAC-Ebene schränkt die Möglichkeiten von vSphere Benutzern ein, SnapCenter Plug-ins für VMware vSphere Aufgaben an vSphere Objekten wie beispielsweise Virtual Machines (VMs) und Datastores auszuführen.

Das SnapCenter Plug-in für die Bereitstellung von VMware vSphere erstellt für SnapCenter Operations on vCenter die folgenden Rollen:

```
SCV Administrator
SCV Backup
SCV Guest File Restore
SCV Restore
SCV View
```

Der vSphere Administrator richtet die RBAC für vCenter Server folgendermaßen ein:

- Sie können Benutzern unter globalen Berechtigungen vordefinierte Rollen zuordnen.
- Legen Sie die vCenter Server-Berechtigungen auf dem Root-Objekt (auch als Stammordner bekannt) fest. Sie können dann die Sicherheit verbessern, indem Sie untergeordnete Entitäten, die diese Berechtigungen nicht benötigen, einschränken.
- Zuweisen der SCV-Rollen zu Active Directory-Benutzern.

  Alle Benutzer müssen mindestens in der Lage sein, vCenter-Objekte anzuzeigen. Ohne diese Berechtigung können Benutzer nicht auf die Benutzeroberfläche des VMware vSphere-Clients zugreifen.

ONTAP RBAC

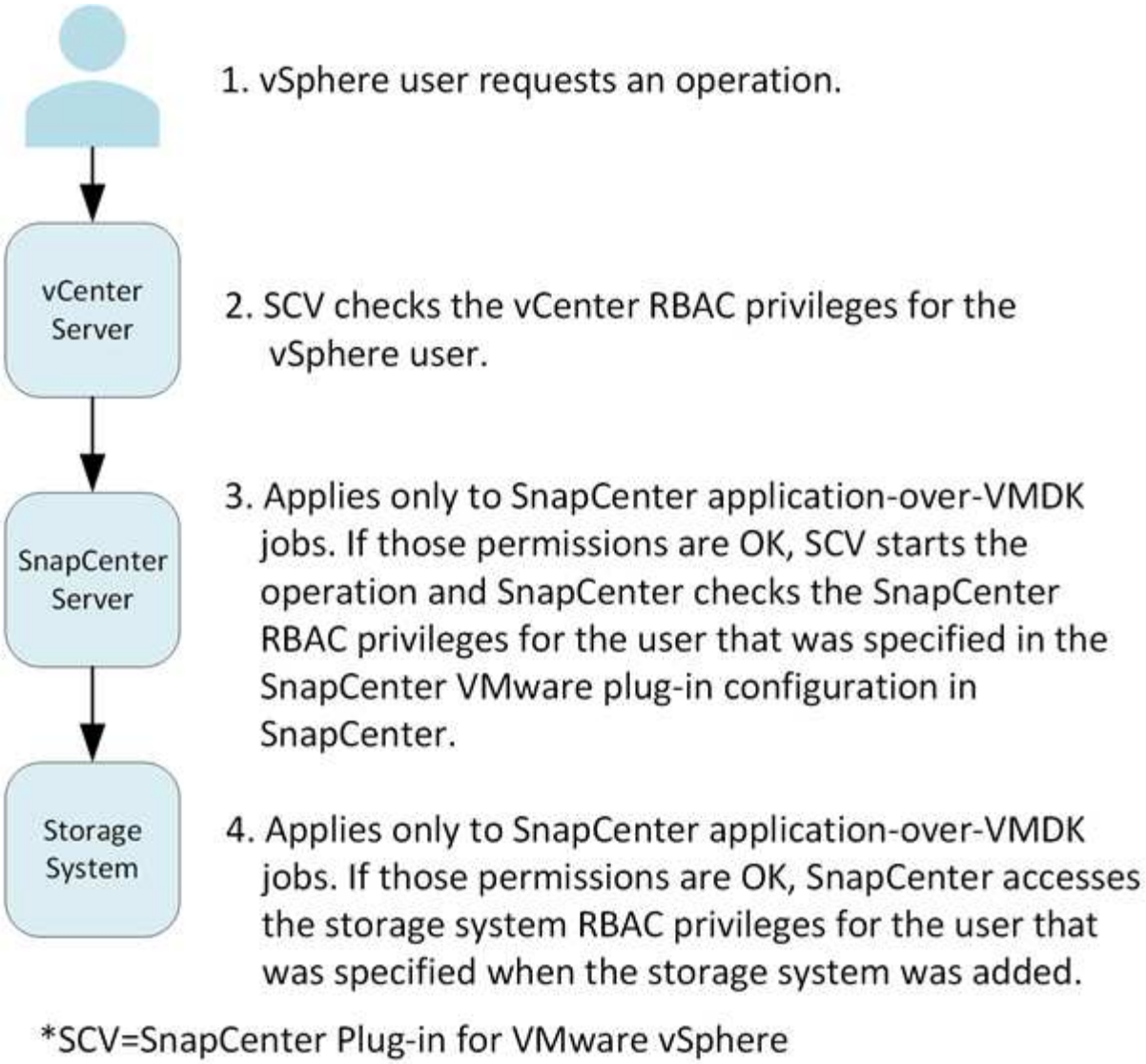
Dieser Sicherheitsmechanismus gilt nur für applikationskonsistente Aufgaben des SnapCenter Servers (Applikation über VMDK). Diese Ebene schränkt die Fähigkeit von SnapCenter ein, bestimmte Storage-Vorgänge, beispielsweise Backups für Datenspeicher, auf einem bestimmten Storage-System durchzuführen.

Nutzen Sie den folgenden Workflow, um die RBAC für ONTAP und SnapCenter einzurichten:

1. Der Storage-Administrator erstellt eine Rolle auf der Storage-VM mit den erforderlichen Berechtigungen.
2. Dann weist der Speicheradministrator die Rolle einem Speicherbenutzer zu.
3. Der SnapCenter-Administrator fügt mit diesem Storage-Benutzernamen die Storage-VM zum SnapCenter-Server hinzu.
4. Anschließend weist der SnapCenter-Administrator SnapCenter-Benutzern Rollen zu.

Validierungs-Workflow für RBAC-Berechtigungen

Die folgende Abbildung bietet einen Überblick über den Validierungs-Workflow für RBAC-Berechtigungen (vCenter und ONTAP):



ONTAP RBAC-Funktionen im SnapCenter Plug-in für VMware vSphere

ONTAP RBAC ist nur für applikationskonsistente (Applikations-Over VMDK) Jobs des SnapCenter Servers gültig.

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von ONTAP können Sie den Zugriff auf bestimmte Storage-Systeme steuern und die Aktionen ausführen, die ein Benutzer auf diesen Storage-Systemen durchführen kann. Das SnapCenter Plug-in für VMware vSphere funktioniert mit RBAC für vCenter Server, RBAC für SnapCenter (bei Bedarf zur Unterstützung applikationsbasierter Vorgänge) und RBAC für ONTAP, um festzulegen, welche SnapCenter Aufgaben ein bestimmter Benutzer an Objekten eines spezifischen Storage-Systems ausführen kann.

SnapCenter verwendet die von Ihnen festgelegten Anmeldedaten (Benutzername und Passwort) zur Authentifizierung jedes Storage-Systems und zur Bestimmung, welche Vorgänge auf diesem Storage-System ausgeführt werden können. Das SnapCenter Plug-in für VMware vSphere verwendet für jedes Storage-System

einen Satz von Anmeldeinformationen. Diese Anmeldedaten bestimmen alle Aufgaben, die auf dem Storage-System ausgeführt werden können. Das heißt, die Anmeldedaten gelten für SnapCenter, nicht für einen einzelnen SnapCenter-Benutzer.

ONTAP RBAC gilt nur für den Zugriff auf Storage-Systeme und zur Durchführung von SnapCenter Aufgaben, beispielsweise für das Backup von VMs. Wenn Sie nicht über die entsprechenden ONTAP RBAC-Berechtigungen für ein bestimmtes Storage-System verfügen, können Sie keine Aufgaben auf einem vSphere Objekt ausführen, das auf diesem Storage-System gehostet wird.

Jedem Speichersystem ist ein Satz von ONTAP-Berechtigungen zugeordnet.

Die Nutzung der ONTAP RBAC und der vCenter Server RBAC bietet folgende Vorteile:

- Sicherheit

  Der Administrator kann steuern, welche Benutzer Aufgaben sowohl auf feingranularen vCenter Server-Objektebene als auch auf Storage-System-Ebene ausführen können.

- Audit-Informationen

  In vielen Fällen erstellt SnapCenter ein Audit-Trail im Storage-System, über das Sie Ereignisse zurück an den vCenter Benutzer nachverfolgen können, der die Storage-Änderungen durchgeführt hat.

- Benutzerfreundlichkeit

  Sie können die Controller-Anmeldedaten an einer Stelle beibehalten.

Vordefinierte Rollen in Paketen mit SnapCenter Plug-in für VMware vSphere

Das SnapCenter Plug-in für VMware vSphere bietet eine Reihe vordefinierter Rollen, mit denen Benutzer SnapCenter-Aufgaben ausführen können, um die Arbeit mit RBAC für vCenter Server zu vereinfachen. Es gibt auch eine schreibgeschützte Rolle, mit der Benutzer SnapCenter-Informationen anzeigen, aber keine Aufgaben ausführen können.

Die vordefinierten Rollen verfügen sowohl über die erforderlichen SnapCenter-spezifischen Berechtigungen als auch über die nativen vCenter Server-Berechtigungen, um sicherzustellen, dass Aufgaben korrekt ausgeführt werden. Darüber hinaus sind die Rollen so eingerichtet, dass sie über die erforderlichen Berechtigungen für alle unterstützten Versionen von vCenter Server verfügen.

Als Administrator können Sie diese Rollen den entsprechenden Benutzern zuweisen.

Das SnapCenter-Plug-in für VMware vSphere setzt diese Rollen bei jedem Neustart des vCenter-Webclient-Dienstes oder bei der Änderung der Installation auf die Standardwerte (anfängliche Berechtigungseinstellung) zurück. Wenn Sie das SnapCenter-Plug-in für VMware vSphere aktualisieren, werden die vordefinierten Rollen automatisch aktualisiert, um mit dieser Version des Plug-ins zu arbeiten.

Sie können die vordefinierten Rollen in der vCenter-Benutzeroberfläche sehen, indem Sie **Menü > Verwaltung > Rollen** auswählen, wie in der folgenden Tabelle gezeigt.

Rolle	Beschreibung
SCV-Administrator	Bietet alle nativen vCenter Server und SnapCenter-spezifischen Berechtigungen, die zur Ausführung aller SnapCenter Plug-ins für VMware vSphere Aufgaben erforderlich sind Ab Version SCV 6.1 wird dieser Rolle eine neue Berechtigung zum Erstellen eines sekundären Schutzes hinzugefügt.
SCV-Backup	Bereitstellung aller nativen vCenter Server und SnapCenter-spezifischen Berechtigungen, die für das Backup von vSphere Objekten (Virtual Machines und Datastores) erforderlich sind Der Benutzer hat auch Zugriff auf die Konfigurationsberechtigung. Der Benutzer kann Backups nicht wiederherstellen. Ab Version SCV 6.1 wird dieser Rolle eine neue Berechtigung zum Erstellen eines sekundären Schutzes hinzugefügt.
Wiederherstellung der SCV-Gastdatei	Bietet alle nativen vCenter Server und SnapCenter-spezifischen Berechtigungen, die für die Wiederherstellung von Gastdateien und Ordnern erforderlich sind Der Benutzer kann keine VMs oder VMDKs wiederherstellen.
SCV-Wiederherstellung	Bietet alle nativen vCenter Server- und SnapCenter-spezifischen Berechtigungen, die erforderlich sind, um vSphere Objekte wiederherzustellen, die mit dem SnapCenter Plug-in für VMware vSphere gesichert wurden, und um Gastdateien und -Ordner wiederherzustellen. Der Benutzer hat auch Zugriff auf die Konfigurationsberechtigung. Der Benutzer kann vSphere-Objekte nicht sichern.
SCV-Ansicht	Bietet schreibgeschützten Zugriff auf alle SnapCenter Plug-in für VMware vSphere-Backups, Ressourcengruppen und Richtlinien.

So konfigurieren Sie ONTAP RBAC für SnapCenter Plug-in für VMware vSphere

ONTAP RBAC ist nur für applikationskonsistente (Applikations-Over VMDK) Jobs des SnapCenter Servers gültig.

> Ab dem SnapCenter Plug-in für VMware (SCV) 5.0 müssen Sie Applikationen des Typs HTTP und ONTAPI als Benutzeranmeldemethoden für alle ONTAP-Benutzer mit benutzerdefiniertem rollenbasiertem Zugriff auf das SCV hinzufügen. Ohne Zugriff auf diese Applikationen können Backups fehlschlagen. Sie müssen den SCV-Dienst neu starten, um Änderungen an den ONTAP-Benutzeranmeldemethoden zu erkennen. Informationen zum Erstellen oder Ändern von Anmeldekonten finden Sie unter "Arbeitsblätter für die Administratorauthentifizierung und die RBAC-Konfiguration".

Sie müssen die ONTAP RBAC auf dem Storage-System konfigurieren, wenn Sie sie mit dem SnapCenter Plug-in für VMware vSphere verwenden möchten. In ONTAP müssen Sie die folgenden Aufgaben ausführen:

- Erstellen einer einzelnen Rolle.

  "Administratorauthentifizierung und RBAC"

- Erstellen Sie in ONTAP einen Benutzernamen und ein Kennwort (Anmeldeinformationen des Speichersystems) für die Rolle.

  Diese Anmeldeinformationen für das Speichersystem werden benötigt, um die Konfiguration der Speichersysteme für das SnapCenter-Plug-in für VMware vSphere zu ermöglichen. Dazu geben Sie die Anmeldeinformationen in das Plug-in ein. Jedes Mal, wenn Sie sich mit diesen Zugangsdaten bei einem Storage-System anmelden, werden Ihnen die SnapCenter-Funktionen angezeigt, die Sie beim Erstellen der Zugangsdaten in ONTAP eingerichtet haben.

Sie können den Administrator oder die Root-Anmeldung verwenden, um auf alle SnapCenter Aufgaben zuzugreifen. Es empfiehlt sich jedoch, die RBAC-Funktion von ONTAP zu nutzen, um ein oder mehrere benutzerdefinierte Konten mit eingeschränkten Zugriffsrechten zu erstellen.

Weitere Informationen finden Sie unter "Mindestberechtigungen für ONTAP erforderlich".

Los geht’s

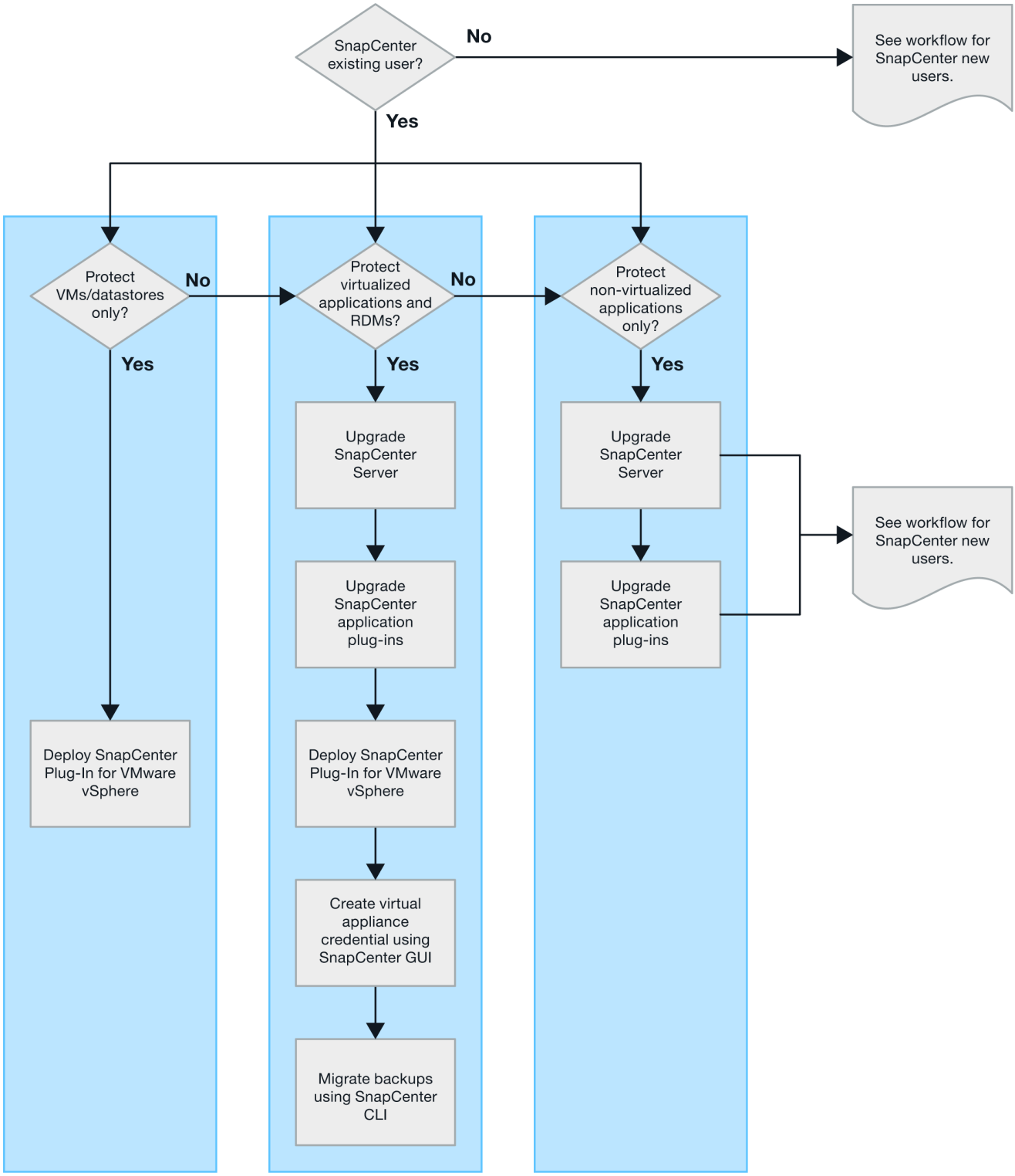
Implementierungsübersicht

Um SnapCenter VMs, Datastores und applikationskonsistente Datenbanken auf virtualisierten Maschinen zu sichern, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren.

Vorhandene SnapCenter Benutzer müssen einen anderen Implementierungs-Workflow als neue SnapCenter Benutzer verwenden.

Implementierungs-Workflow für vorhandene Benutzer

Wenn Sie SnapCenter Benutzer sind und über SnapCenter-Backups verfügen, können Sie mit dem folgenden Workflow beginnen.



Anforderungen für die Bereitstellung von SCV

Implementierungsplanung und -Anforderungen

Sie sollten mit den folgenden Anforderungen vertraut sein, bevor Sie mit der Bereitstellung des SnapCenter Plug-ins für VMware vSphere (SCV) beginnen.

Host-Anforderungen erfüllt

Bevor Sie mit der Bereitstellung des SnapCenter Plug-ins für VMware vSphere (SCV) beginnen, sollten Sie mit den Host-Anforderungen vertraut sein.

- Das SnapCenter Plug-in für VMware vSphere wird als Linux VM implementiert, unabhängig davon, ob es zum Schutz von Daten auf Windows- oder Linux-Systemen verwendet wird.
- Sie sollten das SnapCenter-Plug-in für VMware vSphere auf dem vCenter-Server bereitstellen.

  Backup-Zeitpläne werden in der Zeitzone ausgeführt, in der das SnapCenter-Plug-in für VMware vSphere bereitgestellt wird, und vCenter meldet Daten in der Zeitzone, in der sich das Plug-in befindet. Wenn sich das SnapCenter-Plug-in für VMware vSphere und vCenter daher in unterschiedlichen Zeitzonen befinden, sind die Daten im SnapCenter-Plug-in für VMware vSphere Dashboard möglicherweise nicht mit den Daten in den Berichten identisch.

- Sie dürfen das SnapCenter-Plug-in für VMware vSphere nicht in einem Ordner mit einem Namen bereitstellen, der Sonderzeichen enthält.

  Der Ordnername darf die folgenden Sonderzeichen nicht enthalten: €!@#%^&()_+{}';.,*?"<>

- Sie müssen für jeden vCenter Server eine separate, eindeutige Instanz des SnapCenter Plug-ins für VMware vSphere bereitstellen und registrieren.
  - Jeder vCenter-Server, ob im verknüpften Modus oder nicht, muss mit einer separaten Instanz des SnapCenter-Plug-ins für VMware vSphere gekoppelt werden.
  - Jede Instanz des SnapCenter Plug-ins für VMware vSphere muss als separate Linux VM implementiert werden.

    Nehmen wir beispielsweise an, Sie möchten Backups von sechs verschiedenen Instanzen des vCenter Servers durchführen. In diesem Fall müssen Sie das SnapCenter-Plug-in für VMware vSphere auf sechs Hosts bereitstellen, und jeder vCenter-Server muss mit einer eindeutigen Instanz des SnapCenter-Plug-ins für VMware vSphere gekoppelt werden.

- Zur Sicherung von vVol VMs (VMs auf VMware vVol Datastores) müssen Sie zuerst ONTAP Tools für VMware vSphere einsetzen. Durch die ONTAP Tools wird Storage für VVols auf ONTAP und auf dem VMware Web-Client bereitgestellt und konfiguriert.

  Weitere Informationen finden Sie in der Dokumentation zu den ONTAP tools for VMware vSphere . Weitere Informationen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" für aktuelle Informationen zu den unterstützten Versionen der ONTAP Tools.

- Das SnapCenter Plug-in für VMware vSphere bietet eingeschränkte Unterstützung gemeinsam genutzter PCI- oder PCIe-Geräte (z. B. NVIDIA Grid GPU), da die Virtual Machines bei der Unterstützung von Storage vMotion beschränkt sind. Weitere Informationen finden Sie im Dokument Deployment Guide for VMware des Bieters.
  - Was unterstützt wird:

    Erstellen von Ressourcengruppen

    Erstellen von Backups ohne konsistente VMs

    Die Wiederherstellung einer vollständigen VM, wenn sich alle VMDKs auf einem NFS-Datastore befinden und das Plug-in nicht Storage vMotion verwenden muss

Anschließen und Trennen von VMDKs

Montage und EntMounten von Datenspeichern

Wiederherstellung von Gastdateien

- Was nicht unterstützt wird:

  Erstellen von Backups mit der Konsistenz von VMs

Wiederherstellung einer vollständigen VM, wenn eine oder mehrere VMDKs auf einem VMFS-Datastore vorhanden sind.

- Eine detaillierte Liste der Einschränkungen des SnapCenter-Plug-in für VMware vSphere finden Sie unter "SnapCenter Plug-in für VMware vSphere – Versionsinformationen".

Lizenzanforderungen

Sie müssen Lizenzen für… bereitstellen	Lizenzanforderungen
ONTAP	Eine dieser Optionen: SnapMirror oder SnapVault (für sekundäre Datensicherung unabhängig von der Art der Beziehung)
Zusätzliche Produkte	VSphere Standard, Enterprise oder Enterprise Plus Eine vSphere-Lizenz ist erforderlich, um Wiederherstellungsvorgänge mit Storage vMotion auszuführen. VSphere Essentials- oder Essentials Plus-Lizenzen enthalten kein Storage vMotion.
Primäre Ziele	SnapCenter Standard: Erforderlich zur Durchführung applikationsbasierter Sicherung über VMware SnapRestore: Erforderlich zur Durchführung von Restore-Vorgängen für VMware VMs und Datenspeicher nur FlexClone: Wird nur für die Mounten und Anbindung von VMware VMs und Datastores verwendet
Sekundäre Ziele	SnapCenter Standard: Wird für Failover-Vorgänge für applikationsbasierten Schutz über VMware FlexClone verwendet: Nur für Mount- und Attached-Vorgänge auf VMware VMs und Datastores

Softwaresupport

Element	Unterstützte Versionen
VCenter vSphere	7.0U1 und höher.
ESXi-Server	7.0U1 und höher.
IP-Adressen	IPv4, IPv6
VMware TLS	1.2, 1.3

Element	Unterstützte Versionen
TLS auf dem SnapCenter-Server	1.2, 1.3 der SnapCenter-Server kommuniziert damit mit dem SnapCenter-Plug-in für VMware vSphere für Anwendungen über VMDK-Datensicherungsvorgänge.
VMware Application vStorage API für Array Integration (VAAI)	Das SnapCenter Plug-in für VMware vSphere nutzt diese Technologie zur Verbesserung der Performance von Restore-Vorgängen. Außerdem verbessert es die Performance in NFS Umgebungen.
ONTAP Tools für VMware	Das SnapCenter Plug-in for VMware vSphere verwendet dies zum Verwalten von vVol-Datenspeichern (virtuelle VMware-Volumes). Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" .
Amazon FSxN für NetApp ONTAP -Speicher	9.10 und höher

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

Anforderungen für NVMe-over-TCP und NVMe-over-FC-Protokolle

Die Mindestanforderungen an die Software für die Unterstützung von NVMe over TCP und NVMe over FC-Protokollen sind:

- VCenter vSphere 7.0U3
- ESXi 7.0U3
- ONTAP 9.10.1

Platz-, Dimensionierungs- und Skalierungsanforderungen

Element	Anforderungen
Empfohlene CPU-Anzahl	8 Kerne
Empfohlener RAM	24GB
Minimaler Festplattenspeicher für das SnapCenter Plug-in für VMware vSphere, Logs und MySQL Datenbank	100 GB

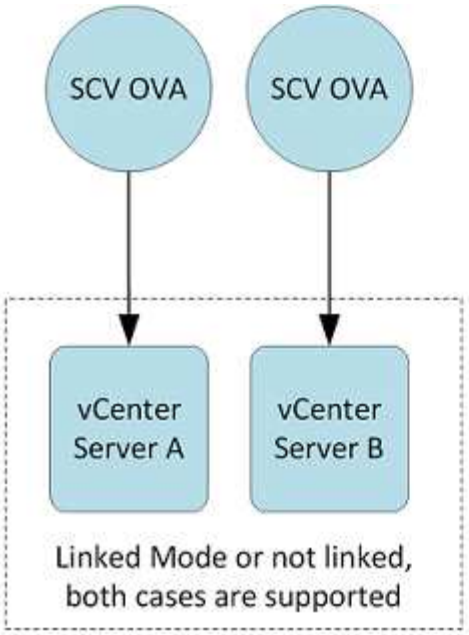
Verbindungs- und Portanforderungen

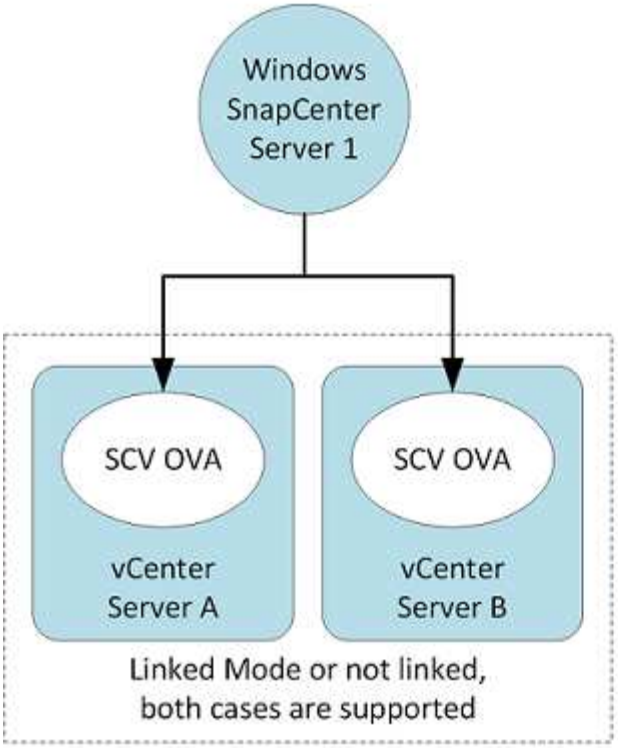
Typ des Ports	Vorkonfigurierter Port
VMware ESXi Server-Port	443 (HTTPS), bidirektional die Funktion „Wiederherstellung von Gastdateien“ verwendet diesen Port.

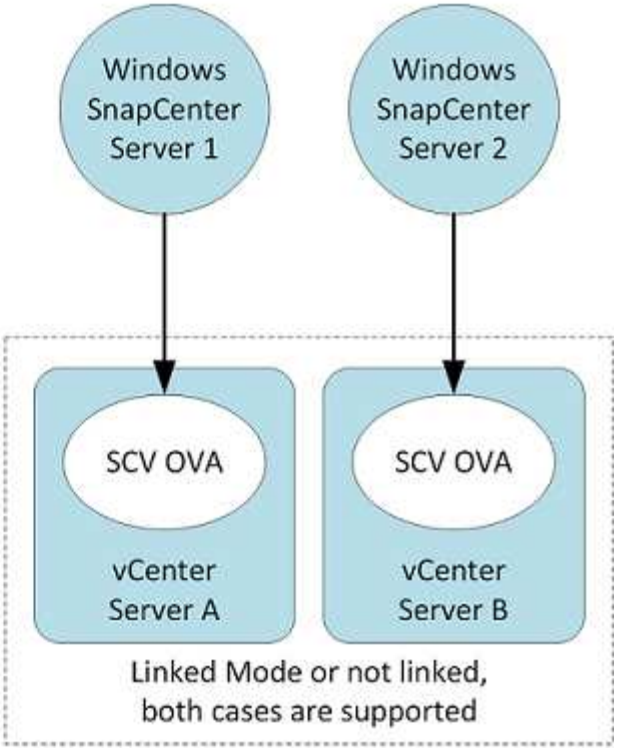
Typ des Ports	Vorkonfigurierter Port
SnapCenter Plug-in für VMware vSphere Port	8144 (HTTPS), bidirektional der Port wird für die Kommunikation vom VMware vSphere-Client und dem SnapCenter-Server verwendet. 8080 bidirektional dieser Port wird zur Verwaltung virtueller Appliances verwendet. Hinweis: Es wird ein benutzerdefinierter Port zum Hinzufügen des SCV-Hosts zu SnapCenter unterstützt.
VMware vSphere vCenter Server Port	Sie müssen Port 443 verwenden, wenn Sie vVol VMs schützen.
Storage-Cluster oder Storage-VM-Port	443 (HTTPS), bidirektional 80 (HTTP), bidirektional der Port wird zur Kommunikation zwischen der virtuellen Appliance und der Storage-VM oder dem Cluster mit der Storage-VM verwendet.

Unterstützte Konfigurationen

Jede Plug-in-Instanz unterstützt nur einen vCenter Server, der sich im verknüpften Modus befindet. Mehrere Plug-in-Instanzen können jedoch denselben SnapCenter Server unterstützen, wie in der folgenden Abbildung dargestellt.







RBAC-Berechtigungen erforderlich

Für das vCenter-Administratorkonto muss die erforderliche vCenter-Privileges in der folgenden Tabelle angegeben sein.

So führen Sie diese Operation aus…	Sie müssen über diese vCenter-Berechtigungen verfügen…
Implementieren und registrieren Sie das SnapCenter Plug-in für VMware vSphere in vCenter	Erweiterung: Verlängerung registrieren

So führen Sie diese Operation aus…	Sie müssen über diese vCenter-Berechtigungen verfügen…
Aktualisieren oder entfernen Sie das SnapCenter Plug-in für VMware vSphere	Erweiterung • Erweiterung aktualisieren • Erweiterung wird aufgehoben
Lassen Sie das in SnapCenter registrierte vCenter Credential-Benutzerkonto zu, um den Benutzerzugriff auf das SnapCenter Plug-in für VMware vSphere zu validieren	sessions.validate.session
Benutzern den Zugriff auf das SnapCenter Plug-in für VMware vSphere ermöglichen	SCV Administrator SCV Backup SCV Gastdateiwiederherstellung SCV Wiederherstellung SCV SCV Ansicht die Berechtigung muss im vCenter Root zugewiesen werden.

AutoSupport

Das SnapCenter Plug-in für VMware vSphere enthält mindestens Informationen zur Nachverfolgung seiner Nutzung, einschließlich der Plug-in-URL. AutoSupport enthält eine Tabelle installierter Plug-ins, die vom AutoSupport Viewer angezeigt werden.

ONTAP-Berechtigungen erforderlich

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

Ab dem SnapCenter Plug-in für VMware (SCV) 5.0 müssen Sie Applikationen des Typs HTTP und ONTAPI als Benutzeranmeldemethoden für alle ONTAP-Benutzer mit benutzerdefiniertem rollenbasiertem Zugriff auf das SCV hinzufügen. Ohne Zugriff auf diese Applikationen können Backups fehlschlagen. Sie müssen den SCV-Dienst neu starten, um Änderungen an den ONTAP-Benutzeranmeldemethoden zu erkennen.

Mindestberechtigungen für ONTAP erforderlich

Für alle SnapCenter Plug-ins sind die folgenden Mindestberechtigungen erforderlich.

Alle Befehle: Minimale ONTAP Privileges.
Event Generate-AutoSupport-log
Job-Verlauf wird angezeigt Jobanzeigen Job beenden
lun lun create lun delete lun igroup hinzufügen lun igroup erstellen lun igroup löschen lun igroup umbenennen lun igroup anzeigen lun Mapping add-Reporting-Nodes lun Mapping erstellen lun Mapping delete lun Mapping remove-Reporting-Nodes lun Mapping show lun modify lun move-in-Volume lun offline lun online lun persistent-reservat clear lun resize lun serial lun anzeigen

snapmirror list-Ziele snapmirror Policy add-rule snapmirror Policy modify-rule snapmirror Policy remove-rule snapmirror Policy show snapmirror restore SnapMirror show SnapMirror show-history snapmirror Update-ls-set snapmirror Update-ls-set
Version
Volume-Klon erstellen Volume-Klon zeigen Volume-Klon teilen starten Volume-Klon-Split-Status Volume-Clone-Split-Volume stoppen Volume erstellen Volume löschen Volume löschen Datei-Klon erstellen Volume-Datei zeigen-Disk-Nutzung Volume offline Volume online Volume-Volume verwalten Volume-Volume ändern Volume-qtree Volume erstellen qtree Volume löschen Volume-Volume ändern Volume-Snapshot Volume erstellen Volume löschen Snapshot Volume ändern Volume-SnapLock-Ablauf-Zeit Volume-Snapshot umbenennen Volume-Snapshot wiederherstellen-Datei-Volume-Snapshot wiederherstellen-Laufwerk zeigen Delta zeigen
vserver cifs vServer cifs Freigabe vserver erstellen cifs Freigabe vserver löschen vserver cifs shadowcopy vServer zeigen cifs share vserver zeigen vserver Export-Policy vServer Export-Policy vServer Export-Policy erstellen vServer Export-Policy löschen vServer NVMe-Subsystem vserver NVMe-Subsystem wserver vserver nvme-Subsystem abbilden vserver Export-Policy-Regel zeigen vserver Export-Policy zeigen vserver zeigen vserver iscsi vserver iscsi-Verbindung zeigen vserver zeigen vserver

Schreibgeschützte Befehle: Minimale ONTAP Privileges
Cluster Identity show Network Interface show vserver vserver Peer vserver show

Alle Befehle: Minimale ONTAP Privileges
Zeigt die Storage-Einheit der Konsistenzgruppe an

Sie können den Befehl *Cluster Identity show* Cluster Level ignorieren, wenn Sie eine Rolle erstellen, die dem Daten-Vserver zugeordnet werden soll.

Sie können die Warnmeldungen zu den nicht unterstützten vServer-Befehlen ignorieren.

Weitere ONTAP-Informationen

- Zur Verwendung der SnapMirror Active Sync Funktion benötigen Sie ONTAP 9.12.1 oder höher.
- So verwenden Sie die tamperproof Snapshot (TPS)-Funktion:
  - Für SAN benötigen Sie ONTAP 9.13.1 und höher
  - Für NFS benötigen Sie ONTAP 9.12.1 und höher
- Für das NVMe over TCP- und NVMe over FC-Protokoll benötigen Sie ONTAP 9.10.1 und höher.

Ab ONTAP Version 9.11.1 erfolgt die Kommunikation mit dem ONTAP Cluster über REST-APIs. Der ONTAP -Benutzer sollte die HTTP-Anwendung aktiviert haben. Wenn jedoch Probleme mit ONTAP REST-APIs auftreten, hilft der Konfigurationsschlüssel „FORCE_ZAPI“ bei der Umstellung auf den herkömmlichen ZAPI-Workflow. Möglicherweise müssen Sie diesen Schlüssel mithilfe der Konfigurations-APIs hinzufügen oder aktualisieren und auf „true“ setzen. Siehe KB-Artikel, "So bearbeiten Sie Konfigurationsparameter in SCV mithilfe der RestAPI" für weitere Informationen.

Minimale vCenter-Berechtigungen erforderlich

Bevor Sie mit der Implementierung des SnapCenter Plug-ins für VMware vSphere beginnen, sollten Sie sicherstellen, dass die erforderlichen Mindestberechtigungen für vCenter vorhanden sind.

Erforderliche Berechtigungen für vCenter Admin-Rolle

Datastore.AllocateSpace Datastore.Browse Datastore.Delete Datastore.FileManagement Datastore.Move Datastore.Rename Extension.Register Extension.Unregister Extension.Update Host.Config.AdvancedConfig Host.Config.Resources Host.Config.Settings Host.Config.Storage Host.Local.CreateVM Host.Local.DeleteVM Network.Local.ReconfigVM Resource.ApplyMachine.Assign.Assignate Virtual Machine.NewVM Resource HostConfig.RemigralConfig.VM

Erforderliche Berechtigungen für SnapCenter Plug-in für VMware vCenter

Privilegien	Etikett
NetappSCV.Guest.RestoreDatei	Wiederherstellung Von Gastdateien
NetappSCV.Recovery.MountUnMount	Montieren/Entfernen
NetappSCV.Backup.DeleteBackupJob	Ressourcengruppe/Sicherung Löschen
NetappSCV.Configure.ConfigureStorageSystems.Delete	Storage-Systeme Entfernen
NetappSCV.View	Anzeigen
NetappSCV.Recovery.RecoverVM	Wiederherstellung von VM
NetappSCV.Configure.ConfigureStorageSystems.AddUpdate	Storage-Systeme Hinzufügen/Ändern
NetappSCV.Backup.BackupJetzt	Jetzt Sichern
NetappSCV.Guest.Configure	Gastkonfiguration
NetappSCV.Configure.ConfigureSnapCenterServer	Konfigurieren Sie den SnapCenter-Server
NetappSCV.Backup.BackupScheduled	Ressourcengruppe Erstellen

Open Virtual Appliance (OVA) herunterladen

Fügen Sie vor der Installation der Open Virtual Appliance (OVA) das Zertifikat in vCenter hinzu. Die .tar-Datei enthält die OVA und die Root- und Intermediate-Zertifikate. Die Zertifikate finden Sie im Ordner Zertifikate. Die OVA-Implementierung wird in VMware vCenter 7u1 und höher unterstützt.

In VMware vCenter 7.0.3 Versionen und höher ist die OVA, die vom Vertrauenzertifikat unterzeichnet wurde, nicht mehr vertrauenswürdig. Zur Behebung des Problems müssen Sie das folgende Verfahren durchführen.

Schritte

1. So laden Sie das SnapCenter Plug-in für VMware herunter:
    - Loggen Sie sich auf der NetApp Support Site ein (

"https://mysupport.netapp.com/products/index.html").

- Wählen Sie aus der Liste der Produkte **SnapCenter Plug-in für VMware vSphere** aus und klicken Sie dann auf die Schaltfläche **Neueste Version herunterladen**.
- Laden Sie das SnapCenter Plug-in für VMware vSphere herunter `.tar` Datei an jedem Speicherort.

2. Extrahieren Sie den Inhalt der tar-Datei. Die tar-Datei enthält den Ordner OVA und certs. Der Ordner „Zertifikaten“ enthält die Zertifikate „Stammanvertrauen“ und „Intermediate“.
3. Melden Sie sich mit dem vSphere Client am vCenter Server an.
4. Navigieren Sie zu **Administration > Zertifikate > Zertifikatverwaltung**.
5. Wählen Sie neben **Trusted Root Certificates Add**
   - Wechseln Sie zum Ordner *certs*.
   - Wählen Sie Root- und Intermediate-Zertifikate anvertrauen aus.
   - Installieren Sie jedes Zertifikat einzeln.
6. Die Zertifikate werden zu einem Panel unter **Trusted Root Certificates** hinzugefügt. Sobald die Zertifikate installiert sind, kann OVA überprüft und bereitgestellt werden.

Wenn das heruntergeladene OVA nicht manipuliert wird, wird in der Spalte **Publisher Trusted Certificate** *angezeigt.

Implementieren Sie das SnapCenter Plug-in für VMware vSphere

Um SnapCenter VMs, Datastores und applikationskonsistente Datenbanken auf virtualisierten Maschinen zu sichern, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren.

Bevor Sie beginnen

In diesem Abschnitt werden alle erforderlichen Aktionen aufgeführt, die Sie vor Beginn der Bereitstellung durchführen sollten.

Die OVA-Implementierung wird in VMware vCenter 7u1 und höher unterstützt.

- Stellen Sie sicher, dass Sie die Bereitstellungsanforderungen überprüft haben.
- Stellen Sie sicher, dass Sie eine unterstützte Version von vCenter Server ausführen.
- Bestätigen Sie, dass Ihre vCenter Server-Umgebung konfiguriert und eingerichtet ist.
- Bereiten Sie einen ESXi-Host für das SnapCenter Plug-in for VMware vSphere VM vor.
- Laden Sie die TAR-Datei des SnapCenter Plug-in for VMware vSphere herunter.
- Besorgen Sie sich die Anmeldeinformationen für Ihre vCenter Server-Instanz.
- Erwerben Sie ein Zertifikat mit gültigen öffentlichen und privaten Schlüsseldateien. Einzelheiten finden Sie in den Artikeln im "Storage-Zertifikatmanagement" Abschnitt.
- Melden Sie sich ab, schließen Sie alle Browsersitzungen des vSphere-Clients und leeren Sie den Browser-Cache, um Probleme während der Bereitstellung zu vermeiden.
- Aktivieren Sie Transport Layer Security (TLS) in vCenter. Weitere Informationen finden Sie in der VMware-Dokumentation.

- Wenn Sie Sicherungen in anderen vCentern als dem durchführen möchten, in dem das SnapCenter Plug-in for VMware vSphere bereitgestellt ist, stellen Sie sicher, dass der ESXi-Server, das SnapCenter Plug-in for VMware vSphere und jedes vCenter auf die gleiche Zeit synchronisiert sind.
- Um VMs auf vVol-Datenspeichern zu schützen, stellen Sie zuerst ONTAP tools for VMware vSphere bereit. Informationen zu unterstützten ONTAP Toolversionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool" . ONTAP -Tools stellen Speicher auf ONTAP und dem VMware-Webclient bereit und konfigurieren ihn.

Stellen Sie das SnapCenter-Plug-in für VMware vSphere in derselben Zeitzone wie vCenter bereit. Backup-Zeitpläne werden in der Zeitzone ausgeführt, in der das SnapCenter Plug-in für VMware vSphere bereitgestellt wird. VCenter meldet Daten in der Zeitzone, in der sich vCenter befindet. Wenn sich das SnapCenter-Plug-in für VMware vSphere und vCenter daher in unterschiedlichen Zeitzonen befinden, sind die Daten im SnapCenter-Plug-in für VMware vSphere Dashboard möglicherweise nicht mit den Daten in den Berichten identisch.

Schritte

1. Befolgen Sie für VMware vCenter 7.0.3 und neuere Versionen die Schritte unter "Open Virtual Appliance (OVA) herunterladen" So importieren Sie die Zertifikate in vCenter.
2. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.

   Für IPv6-Adressen-HTML-Web-Clients müssen Sie entweder Chrome oder Firefox verwenden.

3. Melden Sie sich auf der Seite **VMware vCenter Single Sign-On** an.
4. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf ein Inventarobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Rechenzentrum, Cluster oder Host, und wählen Sie **Deploy OVF Template** aus, um den VMware Deploy Wizard zu starten.
5. Extrahieren Sie die .tar-Datei, die die .ova-Datei auf Ihr lokales System enthält. Geben Sie auf der Seite **Wählen Sie eine OVF-Vorlage** den Speicherort des an `.ova` Datei im extrahierten Ordner .tar.
6. Wählen Sie **Weiter**.
7. Geben Sie auf der Seite **Namen und Ordner auswählen** einen eindeutigen Namen für die VM oder vApp ein, wählen Sie einen Bereitstellungsort aus und wählen Sie dann **Weiter** aus.

   In diesem Schritt wird festgelegt, wo der importiert werden soll `.tar` Datei in vCenter. Der Standardname für die VM entspricht dem Namen der ausgewählten `.ova` Datei: Wenn Sie den Standardnamen ändern, wählen Sie einen Namen aus, der in jedem vCenter Server VM-Ordner eindeutig ist.

   Der Standardbereitstellungs-Speicherort für die VM ist das Inventurobjekt, an dem Sie den Assistenten gestartet haben.

8. Wählen Sie auf der Seite **Select a Resource** die Ressource aus, auf der Sie die bereitgestellte VM-Vorlage ausführen möchten, und wählen Sie **Next** aus.
9. Überprüfen Sie auf der Seite **Details überprüfen** die `.tar` Vorlagendetails und wählen Sie **Weiter** aus.
10. Aktivieren Sie auf der Seite **Lizenzvereinbarungen** das Kontrollkästchen für **Ich akzeptiere alle Lizenzvereinbarungen**.
11. Legen Sie auf der Seite * Storage auswählen* fest, wo und wie die Dateien für die bereitgestellte OVF-Vorlage gespeichert werden sollen.

    a. Wählen Sie das Festplattenformat für die VMDKs aus.

    b. Wählen Sie eine VM-Speicherrichtlinie aus.

Diese Option ist nur verfügbar, wenn Storage-Richtlinien auf der Zielressource aktiviert sind.

c. Wählen Sie einen Datenspeicher aus, um die implementierte OVA-Vorlage zu speichern.

Die Konfigurationsdatei und die Dateien virtueller Laufwerke werden auf dem Datastore gespeichert.

Wählen Sie einen Datenspeicher aus, der ausreichend groß ist, um die virtuelle Maschine oder vApp und alle zugehörigen virtuellen Festplattendateien aufzunehmen.

12. Gehen Sie auf der Seite **Netzwerke auswählen** wie folgt vor:

a. Wählen Sie ein Quellnetzwerk aus, und ordnen Sie es einem Zielnetzwerk zu.

In der Spalte Source Network werden alle Netzwerke aufgelistet, die in der OVA-Vorlage definiert sind.

b. Wählen Sie im Abschnitt **IP Allocation Settings** das gewünschte IP-Adressenprotokoll aus und wählen Sie dann **Next** aus.

Das SnapCenter Plug-in für VMware vSphere unterstützt eine Netzwerkschnittstelle. Wenn Sie mehrere Netzwerkadapter benötigen, müssen Sie diese manuell einrichten. Siehe "KB-Artikel: So erstellen Sie zusätzliche Netzwerkadapter".

13. Gehen Sie auf der Seite **Vorlage anpassen** wie folgt vor:

a. Geben Sie im Abschnitt **Registrieren bei vorhandenem vCenter** den vCenter-Namen und die vCenter-Anmeldedaten der virtuellen Appliance ein.

Geben Sie im Feld **vCenter Benutzername** den Benutzernamen in das Format ein `domain\username`.

b. Geben Sie im Abschnitt **SCV-Anmeldeinformationen erstellen** die lokalen Anmeldeinformationen ein.

Geben Sie im Feld **Benutzername** den lokalen Benutzernamen ein; fügen Sie keine Domain-Details ein.

Notieren Sie sich den Benutzernamen und das Kennwort, den Sie angeben. Sie müssen diese Anmeldeinformationen verwenden, wenn Sie die Konfiguration des SnapCenter-Plug-ins für VMware vSphere später ändern möchten.

c. Geben Sie die Anmeldeinformationen für den Benutzer von maint ein.

d. Geben Sie im Abschnitt **Netzwerkeigenschaften einrichten** den Hostnamen ein.

i. Geben Sie im Abschnitt **Setup IPv4 Network Properties** die Netzwerkinformationen wie IPv4-Adresse, IPv4-Netzmaske, IPv4-Gateway, primärer IPv4-DNS, sekundärer IPv4-DNS, und IPv4-Suchdomänen.

ii. Geben Sie im Abschnitt **IPv6-Netzwerkeigenschaften einrichten** die Netzwerkinformationen ein, z. B. IPv6-Adresse, IPv6-Netzmaske, IPv6-Gateway, IPv6-Primärer DNS, IPv6-SekundärDNS, und IPv6-Suchdomänen.

Wählen Sie die IPv4- oder IPv6-Adressfelder oder beide aus. Wenn Sie sowohl IPv4- als auch IPv6-Adressen verwenden, müssen Sie den primären DNS nur für eine dieser Adressen angeben.

Sie können diese Schritte überspringen und die Einträge im Abschnitt **Setup Network Properties** leer lassen, wenn Sie DHCP als Netzwerkkonfiguration verwenden möchten.

a. Wählen Sie unter **Setup Datum und Uhrzeit** die Zeitzone aus, in der sich das vCenter befindet.

14. Überprüfen Sie die Seite auf der Seite **Ready to Complete**, und wählen Sie **Finish**.

    Alle Hosts müssen mit IP-Adressen konfiguriert sein (FQDN-Hostnamen werden nicht unterstützt). Der Bereitstellungsvorgang überprüft Ihre Eingaben vor der Bereitstellung nicht.

    Sie können den Fortschritt der Bereitstellung im Fenster „Letzte Aufgaben“ anzeigen, während Sie warten, bis die OVF-Import- und Bereitstellungsaufgaben abgeschlossen sind.

    Wenn das SnapCenter-Plug-in für VMware vSphere erfolgreich bereitgestellt wurde, wird es als Linux-VM bereitgestellt, bei vCenter registriert und ein VMware vSphere-Client installiert.

15. Navigieren Sie zu der VM, auf der das SnapCenter-Plug-in für VMware vSphere bereitgestellt wurde, wählen Sie dann die Registerkarte **Zusammenfassung** aus, und wählen Sie dann das Feld **Einschalten** aus, um die virtuelle Appliance zu starten.
16. Während das SnapCenter-Plug-in für VMware vSphere eingeschaltet ist, klicken Sie mit der rechten Maustaste auf das bereitgestellte SnapCenter-Plug-in für VMware vSphere, wählen Sie **Gastbetriebssystem** aus und wählen Sie dann **VMware-Tools installieren** aus.

    Die VMware-Tools werden auf der VM installiert, auf der das SnapCenter-Plug-in für VMware vSphere bereitgestellt wird. Weitere Informationen zum Installieren von VMware-Tools finden Sie in der VMware-Dokumentation.

    Die Implementierung kann einige Minuten dauern. Die erfolgreiche Bereitstellung wird angezeigt, wenn das SnapCenter-Plug-in für VMware vSphere eingeschaltet ist, die VMware-Tools installiert sind und Sie auf dem Bildschirm aufgefordert werden, sich beim SnapCenter-Plug-in für VMware vSphere anzumelden. Sie können die Netzwerkkonfiguration während des ersten Neustarts von DHCP auf statisch umschalten. Der Wechsel von statischem zu DHCP wird jedoch nicht unterstützt.

    Auf dem Bildschirm wird die IP-Adresse angezeigt, unter der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. Notieren Sie sich die IP-Adresse. Sie müssen sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere anmelden, wenn Sie Änderungen an der Konfiguration des SnapCenter Plug-in for VMware vSphere vornehmen möchten.

17. Melden Sie sich mit der auf dem Bereitstellungsbildschirm angezeigten IP-Adresse und den Anmeldeinformationen, die Sie im Bereitstellungsassistenten angegeben haben, bei der SnapCenter Plug-in for VMware vSphere für VMware vSphere an. Überprüfen Sie dann auf dem Dashboard, ob das SnapCenter Plug-in for VMware vSphere erfolgreich mit vCenter verbunden und aktiviert ist.

    Verwenden Sie das Format `https://<appliance-IP-address>:8080` um auf die Verwaltungsbenutzeroberfläche zuzugreifen.

    Melden Sie sich bei der Implementierung mit dem Admin-Benutzernamen und -Passwort an, und verwenden Sie das MFA-Token, das über die Wartungskonsole generiert wurde.

    Wenn das SnapCenter-Plug-in für VMware vSphere nicht aktiviert ist, finden Sie weitere Informationen unter "Starten Sie den VMware vSphere-Client-Service neu".

    Wenn der Hostname 'UnifiedVSC/SCV' lautet, starten Sie das Gerät neu. Wenn beim Neustart des Geräts der Hostname nicht in den angegebenen Hostnamen geändert wird, müssen Sie das Gerät neu installieren.

Nachdem Sie fertig sind

Sie müssen die erforderlichen Daten ausfüllen "Vorgänge nach der Implementierung".

Nach der Implementierung erforderliche Betriebsabläufe und Probleme

Nach der Bereitstellung des SnapCenter Plug-ins für VMware vSphere müssen Sie die Installation abschließen.

Erforderliche Vorgänge nach der Implementierung

Als neuer SnapCenter Benutzer müssen Sie SnapCenter Storage-VMs hinzufügen, bevor Sie Datensicherungsvorgänge durchführen können. Geben Sie beim Hinzufügen von Storage VMs die Management-LIF an. Sie können auch ein Cluster hinzufügen und die Cluster-Management-LIF angeben. Informationen zum Hinzufügen von Speicher finden Sie unter "Erweitern Sie Ihren Storage".

Möglicherweise treten Bereitstellungsprobleme auf

- Nach der Bereitstellung der virtuellen Appliance wird die Registerkarte * Sicherungsjobs* auf dem Dashboard möglicherweise in den folgenden Szenarien nicht geladen:
  - Sie führen eine IPv4-Adresse aus und haben zwei IP-Adressen für den SnapCenter VMware vSphere-Host. Daher wird die Jobanforderung an eine IP-Adresse gesendet, die vom SnapCenter-Server nicht erkannt wird. Um dieses Problem zu vermeiden, fügen Sie die IP-Adresse, die Sie verwenden möchten, wie folgt hinzu:
    i. Navigieren Sie zu dem Speicherort, an dem das SnapCenter-Plug-in für VMware vSphere bereitgestellt wird: `/opt/netapp/scvservice/standalone_aegis/etc`
    ii. Öffnen Sie das Dateinetzwerk- interface.properties.
    iii. Im `network.interface=10.10.10.10` Geben Sie die IP-Adresse ein, die Sie verwenden möchten.
  - Sie haben zwei NICs.
- Nach der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere zeigt der MOB-Eintrag in vCenter für SnapCenter Plug-in für VMware vSphere möglicherweise immer noch die alte Versionsnummer an. Dies kann auftreten, wenn andere Jobs im vCenter ausgeführt werden. VCenter wird schließlich den Eintrag aktualisieren.

Gehen Sie wie folgt vor, um eine dieser Probleme zu beheben:

1. Leeren Sie den Browser-Cache und prüfen Sie anschließend, ob die Benutzeroberfläche ordnungsgemäß funktioniert.

   Wenn das Problem weiterhin besteht, starten Sie den VMware vSphere-Client-Service neu

2. Melden Sie sich bei vCenter an, wählen Sie dann in der Symbolleiste **Menü** aus und wählen Sie dann **SnapCenter-Plug-in für VMware vSphere** aus.

Management von Authentifizierungsfehlern

Wenn Sie die Administratoranmeldeinformationen nicht verwenden, wird möglicherweise nach der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder nach der Migration ein Authentifizierungsfehler angezeigt. Wenn ein Authentifizierungsfehler auftritt, müssen Sie den Dienst neu starten.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungsbenutzeroberfläche mit dem Format `https://<appliance-IP-address>:8080` . Verwenden Sie zur Anmeldung den Administratorbenutzernamen, das Kennwort und die MFA-Token-Details. MFA-Token können über die Wartungskonsole generiert werden.
2. Starten Sie den Dienst neu.

Registrieren Sie das SnapCenter Plug-in für VMware vSphere mit SnapCenter Server

Wenn Sie Applikations-Over-VMDK-Workflows in SnapCenter ausführen möchten (applikationsbasierte Sicherungs-Workflows für virtualisierte Datenbanken und Filesysteme), müssen Sie das SnapCenter Plug-in für VMware vSphere mit dem SnapCenter Server registrieren.

Bevor Sie beginnen

- Sie müssen SnapCenter Server 4.2 oder höher ausführen.
- Sie müssen das SnapCenter Plug-in für VMware vSphere implementieren und aktivieren.

Über diese Aufgabe

- Sie registrieren das SnapCenter Plug-in for VMware vSphere beim SnapCenter -Server, indem Sie über die SnapCenter Benutzeroberfläche einen Host vom Typ „vsphere“ hinzufügen.

  Port 8144 ist vordefiniert für die Kommunikation innerhalb des SnapCenter Plug-ins für VMware vSphere.

  Sie können mehrere Instanzen des SnapCenter-Plug-ins für VMware vSphere auf demselben SnapCenter-Server registrieren, um applikationsbasierte Datensicherungsvorgänge auf VMs zu unterstützen. Sie können nicht dasselbe SnapCenter Plug-in für VMware vSphere auf mehreren SnapCenter Servern registrieren.

- Bei vCenters im Linked Mode müssen Sie das SnapCenter Plug-in für VMware vSphere für jedes vCenter registrieren.

Schritte

1. Wählen Sie im linken Navigationsbereich der SnapCenter Benutzeroberfläche **Hosts** aus.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist. Suchen Sie anschließend den Host-Namen der virtuellen Appliance und überprüfen Sie, ob diese vom SnapCenter-Server aufgelöst wird.
3. Wählen Sie **Hinzufügen**, um den Assistenten zu starten.
4. Geben Sie im Dialogfeld **Hosts hinzufügen** den Host an, den Sie dem SnapCenter-Server hinzufügen möchten, wie in der folgenden Tabelle aufgeführt:

Für dieses Feld…	Do this…
Host-Typ	Wählen Sie **vSphere** als Host-Typ aus.
Host-Name	Überprüfen Sie die IP-Adresse der virtuellen Appliance.
Anmeldedaten	Geben Sie den Benutzernamen und das Kennwort für das SnapCenter-Plug-in für VMware vSphere ein, das während der Bereitstellung bereitgestellt wurde.

5. Wählen Sie **Senden**.

   Wenn der VM-Host erfolgreich hinzugefügt wurde, wird er auf der Registerkarte Managed Hosts angezeigt.

6. Wählen Sie im linken Navigationsbereich **Einstellungen**, dann die Registerkarte **Credential** und wählen Sie dann **Add**, um Anmeldeinformationen für die virtuelle Appliance hinzuzufügen.
7. Geben Sie die Anmeldeinformationen an, die während der Bereitstellung des SnapCenter Plug-ins für VMware vSphere angegeben wurden.

   Sie müssen Linux für das Feld Authentifizierung auswählen.

Nachdem Sie fertig sind

Wenn das SnapCenter-Plug-in für VMware vSphere-Anmeldedaten geändert werden, müssen Sie die Registrierung im SnapCenter-Server über die Seite SnapCenter Managed Hosts aktualisieren.

Melden Sie sich beim SnapCenter VMware vSphere-Client an

Wenn das SnapCenter Plug-in für VMware vSphere implementiert wird, wird ein VMware vSphere Client in vCenter installiert, der auf dem vCenter Bildschirm mit anderen vSphere Clients angezeigt wird.

Bevor Sie beginnen

Transport Layer Security (TLS) muss in vCenter aktiviert sein. Lesen Sie die VMware-Dokumentation.

Schritte

1. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.
2. Melden Sie sich auf der Seite **VMware vCenter Single Sign-On** an.

   Klicken Sie auf die Schaltfläche **Login**. Aufgrund eines bekannten VMware-Problems, verwenden Sie nicht den EINGABETASTE, um sich anzumelden. Weitere Informationen finden Sie in der VMware-Dokumentation zu Problemen mit dem ESXi Embedded Host Client.

3. Wählen Sie auf der Seite **VMware vSphere Client** die Option Menü in der Symbolleiste und dann **SnapCenter Plug-in für VMware vSphere**.

Schnellstart

Überblick

Die Schnellstartdokumentation enthält einen Satz von Anweisungen, mit denen das SnapCenter Plug-in für virtuelle VMware vSphere Appliance implementiert und das SnapCenter Plug-in für VMware vSphere ermöglicht wird. Diese Anweisungen richten sich an Kunden, die noch nicht über SnapCenter verfügen und nur VMs und Datastores schützen möchten.

Bevor Sie beginnen, lesen Sie bitte "Implementierungsplanung und -Anforderungen".

Implementieren Sie das SnapCenter Plug-in für VMware vSphere

Um SnapCenter VMs, Datastores und applikationskonsistente Datenbanken auf virtualisierten Maschinen zu sichern, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren.
Der "Open Virtual Appliance (OVA) herunterladen" Seite enthält Anweisungen zum Herunterladen der OVA-Dateien.

1. Befolgen Sie für VMware vCenter 7.0.3 und neuere Versionen die Schritte unter "Open Virtual Appliance (OVA) herunterladen" So importieren Sie die Zertifikate in vCenter.
2. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.

   Für IPv6-Adressen-HTML-Web-Clients müssen Sie entweder Chrome oder Firefox verwenden.

3. Melden Sie sich auf der Seite **VMware vCenter Single Sign-On an**.
4. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf ein beliebiges Inventurobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Rechenzentrum, einen Ordner, einen Cluster oder einen Host, und wählen Sie **OVF-Vorlage bereitstellen** aus, um den VMware-Bereitstellungsassistenten zu starten.
5. Geben Sie auf der Seite **Wählen Sie eine OVF-Vorlage** den Speicherort der Datei an `.ova` (wie in der folgenden Tabelle aufgeführt), und wählen Sie **Weiter**.

Auf dieser Assistentenseite…	Do this…
Wählen Sie einen Namen und einen Ordner aus	Geben Sie einen eindeutigen Namen für die VM oder vApp ein, und wählen Sie einen Speicherort für die Bereitstellung aus.
Wählen Sie eine Ressource aus	Wählen Sie eine Ressource aus, in der Sie die implementierte VM-Vorlage ausführen möchten.
Lesen Sie die Details durch	Überprüfen Sie die `.ova` Vorlagendetails:
Lizenzvereinbarungen	Aktivieren Sie das Kontrollkästchen für **Ich akzeptiere alle Lizenzvereinbarungen**.

Auf dieser Assistentenseite…	Do this…
Wählen Sie Storage aus	Legen Sie fest, wo und wie die Dateien für die bereitgestellte OVF-Vorlage gespeichert werden.
Wählen Sie Netzwerke aus	Wählen Sie ein Quellnetzwerk aus, und ordnen Sie es einem Zielnetzwerk zu.
Vorlage anpassen	Geben Sie unter **Registrieren Sie sich bei vorhandenem vCenter** die vCenter-Anmeldedaten ein. Geben Sie in **Create SnapCenter Plug-in for VMware vSphere Credentials** das SnapCenter Plug-in für VMware vSphere ein. Notieren Sie sich den Benutzernamen und das Kennwort, den Sie angeben. Sie müssen diese Anmeldedaten verwenden, wenn Sie die Konfiguration des SnapCenter Plug-ins für VMware vSphere zu einem späteren Zeitpunkt ändern möchten. Geben Sie im Abschnitt **Netzwerkeigenschaften einrichten** die Netzwerkinformationen ein. Wählen Sie im Abschnitt **Setup-Datum und -Uhrzeit** die Zeitzone aus, in der sich das vCenter befindet.
Fertig	Überprüfen Sie die Seite und wählen Sie **Fertig stellen**.

Alle Hosts müssen mit IP-Adressen konfiguriert sein (FQDN-Hostnamen werden nicht unterstützt). Der Bereitstellungsvorgang überprüft Ihre Eingaben vor der Bereitstellung nicht.

6. Navigieren Sie zu der VM, auf der das SnapCenter-Plug-in für VMware vSphere bereitgestellt wurde, wählen Sie dann die Registerkarte **Zusammenfassung** aus, und wählen Sie dann das Feld **Einschalten** aus, um das SnapCenter-Plug-in für VMware vSphere zu starten.
7. Während das SnapCenter-Plug-in für VMware vSphere eingeschaltet ist, klicken Sie mit der rechten Maustaste auf das bereitgestellte SnapCenter-Plug-in für VMware vSphere, wählen Sie **Gastbetriebssystem** aus und wählen Sie dann **VMware-Tools installieren** aus.

   Die Implementierung kann einige Minuten dauern. Die erfolgreiche Bereitstellung wird angezeigt, wenn das SnapCenter-Plug-in für VMware vSphere eingeschaltet ist, die VMware-Tools installiert sind und Sie auf dem Bildschirm aufgefordert werden, sich beim SnapCenter-Plug-in für VMware vSphere anzumelden.

   Auf dem Bildschirm wird die IP-Adresse angezeigt, unter der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. Notieren Sie sich die IP-Adresse. Sie müssen sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere anmelden, wenn Sie Änderungen an der Konfiguration des SnapCenter Plug-in for VMware vSphere vornehmen möchten.

8. Melden Sie sich mit der auf dem Bereitstellungsbildschirm angezeigten IP-Adresse und den Anmeldeinformationen, die Sie im Bereitstellungsassistenten angegeben haben, bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere für VMware vSphere an.

Überprüfen Sie dann auf dem Dashboard, ob das SnapCenter Plug-in for VMware vSphere erfolgreich mit vCenter verbunden und aktiviert ist.

Verwenden Sie das Format `https://<appliance-IP-address>:8080` um auf die Verwaltungsbenutzeroberfläche zuzugreifen.

Melden Sie sich bei der Implementierung mit dem Admin-Benutzernamen und -Passwort an, und verwenden Sie das MFA-Token, das über die Wartungskonsole generiert wurde.

9. Melden Sie sich beim vCenter HTML5 Client an, wählen Sie dann **Menü** in der Symbolleiste und dann **SnapCenter Plug-in für VMware vSphere**

Erweitern Sie Ihren Storage

Führen Sie die Schritte in diesem Abschnitt aus, um Speicher hinzuzufügen.

1. Wählen Sie im linken Navigationsfenster des SCV-Plug-ins **Storage Systems** aus und wählen Sie dann **Add** aus.
2. Geben Sie im Dialogfeld Speichersystem hinzufügen die grundlegenden SVM- oder Cluster-Informationen ein, und wählen Sie **Hinzufügen** aus.

Backup-Richtlinien erstellen

Befolgen Sie die unten angegebenen Anweisungen, um Backup-Richtlinien zu erstellen

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Richtlinien** aus, und wählen Sie dann **Neue Richtlinie** aus.
2. Geben Sie auf der Seite **New Backup Policy** die Konfigurationsinformationen für die Richtlinie ein, und wählen Sie dann **Add** aus.

Erstellen von Ressourcengruppen

Führen Sie die folgenden Schritte aus, um Ressourcengruppen zu erstellen.

1. Wählen Sie im linken Navigationsfenster des SCV-Plug-ins **Ressourcengruppen** aus, und wählen Sie dann **Erstellen** aus.
2. Geben Sie auf jeder Seite des Assistenten „Ressourcengruppe erstellen“ die erforderlichen Informationen ein, wählen Sie die VMs und Datastores aus, die in die Ressourcengruppe aufgenommen werden sollen, und wählen Sie dann die Backup-Richtlinien aus, die auf die Ressourcengruppe angewendet werden sollen. Fügen Sie die Details zum sekundären Remote-Schutz hinzu, und geben Sie den Backup-Zeitplan an.

Backups werden gemäß den für die Ressourcengruppe konfigurierten Backup-Richtlinien durchgeführt.

Sie können auf der Seite **Ressourcengruppen** nach Bedarf ein Backup durchführen, indem Sie auswählen **Jetzt Laufen**.

Monitoring und Reporting

Zeigt Statusinformationen an

Sie können Statusinformationen im vSphere-Client-Dashboard anzeigen. Die Statusinformationen werden einmal pro Stunde aktualisiert.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard** > **Status**.
3. Zeigen Sie Statusinformationen für die Übersicht an, oder wählen Sie einen Link für weitere Details aus, wie in der folgenden Tabelle aufgeführt.

Dieses Dashboard-Feld…	Zeigt die folgenden Informationen an…
Zuletzt verwendete Job-Aktivitäten	Die drei bis fünf letzten Backup-, Restore- und Mount-Aufgaben. • Wählen Sie auf einer Job-ID aus, um weitere Details zu diesem Job anzuzeigen. • Wählen Sie **Alle anzeigen**, um auf die Registerkarte Job Monitor zu gelangen, um weitere Details zu allen Jobs zu erhalten.
Jobs	Eine Anzahl von Jobs (Backup, Restore und Mount), die innerhalb des ausgewählten Zeitfensters ausgeführt werden. Bewegen Sie den Cursor über einen Abschnitt des Diagramms, um weitere Details zu dieser Kategorie anzuzeigen.

Dieses Dashboard-Feld…	Zeigt die folgenden Informationen an…
Aktuelle Zusammenfassung Des Schutzes	Zusammenfassungen des Datensicherungsstatus von primären und sekundären VMs oder Datastores im ausgewählten Zeitfenster. • Wählen Sie das Dropdown-Menü aus, um **VMs** oder **Datastores** auszuwählen. • Wählen Sie als Sekundärspeicher **SnapVault** oder **SnapMirror** aus. • Bewegen Sie den Mauszeiger über einen Abschnitt eines Diagramms, um die Anzahl der VMs oder Datastores in dieser Kategorie anzuzeigen. In der Kategorie erfolgreich wird für jede Ressource das aktuellste Backup aufgeführt. • Sie können das Zeitfenster ändern, indem Sie die Konfigurationsdatei bearbeiten. Der Standardwert ist 7 Tage. Weitere Informationen finden Sie unter "Passen Sie Ihre Konfiguration an". • Interne Zähler werden nach jedem primären oder sekundären Backup aktualisiert. Die Dashboard-Kachel wird alle sechs Stunden aktualisiert. Die Aktualisierungszeit kann nicht geändert werden. Hinweis: Wenn Sie eine Mirror-Vault-Schutzrichtlinie verwenden, werden die Zähler für die Sicherungszusammenfassung im SnapVault-Übersichtsdiagramm und nicht im SnapMirror Diagramm angezeigt.
Konfiguration	Gesamtzahl der jeden Objekttyp, die vom SnapCenter Plug-in für VMware vSphere gemanagt wird

Dieses Dashboard-Feld…	Zeigt die folgenden Informationen an…
Storage	Die Gesamtzahl der erstellten Snapshots, SnapVault- und SnapMirror-Snapshots sowie die Menge des für primäre und sekundäre Snapshots verwendeten Speichers. Das Liniendiagramm stellt den primären und sekundären Speicherverbrauch über einen laufenden Zeitraum von 90 Tagen täglich separat dar. Storage-Informationen werden alle 24 Stunden um 1:08 UHR aktualisiert. Storage Savings ist das Verhältnis der logischen Kapazität (Snapshot-Einsparungen plus verbrauchter Storage) zur physischen Kapazität des primären Storage. Das Balkendiagramm zeigt die Storage-Einsparungen. Bewegen Sie den Cursor über eine Linie auf der Karte, um detaillierte Ergebnisse für Tag anzuzeigen.

Überwachen von Jobs

Nachdem Sie mit dem VMware vSphere-Client einen Datensicherungsvorgang durchgeführt haben, können Sie den Job-Status über die Registerkarte Job Monitor im Dashboard überwachen und Jobdetails anzeigen.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard**.
3. Wenn zwei oder mehr vCenter im verknüpften Modus konfiguriert sind, wählen Sie die SCV-Plug-in-Instanz aus und wählen Sie die Registerkarte **Job Monitor** aus. Auf der Registerkarte Job Monitor werden die einzelnen Jobs sowie deren Status, die Startzeit und die Endzeit aufgelistet. Wenn die Jobnamen lang sind, müssen Sie möglicherweise nach rechts blättern, um die Start- und Endzeiten anzuzeigen. Das Display wird alle 30 Sekunden aktualisiert.
    - Wählen Sie das Symbol Aktualisieren in der Symbolleiste aus, um die Anzeige bei Bedarf zu aktualisieren.
    - Wählen Sie das Filtersymbol aus, um den Zeitraum, den Typ, das Tag und den Status der Jobs auszuwählen, die angezeigt werden sollen. Der Filter ist Groß-/Kleinschreibung beachten.
    - Wählen Sie das Symbol Aktualisieren im Fenster Job-Details aus, um die Anzeige während der Ausführung des Jobs zu aktualisieren.

Wenn im Dashboard keine Jobinformationen angezeigt werden, lesen Sie "KB-Artikel: SnapCenter vSphere-Client-Dashboard zeigt keine Jobs an".

Job-Protokolle herunterladen

Sie können die Jobprotokolle von der Registerkarte Job Monitor auf dem Dashboard des

SnapCenter VMware vSphere Clients herunterladen.

Wenn bei der Verwendung des VMware vSphere-Clients ein unerwartetes Verhalten auftritt, können Sie mithilfe der Protokolldateien die Ursache identifizieren und das Problem lösen.

> Der Standardwert für die Aufbewahrung von Jobprotokollen beträgt 30 Tage; der Standardwert für die Beibehaltung von Jobs beträgt 90 Tage. Job-Protokolle und Jobs, die älter als die konfigurierte Aufbewahrung sind, werden alle sechs Stunden gelöscht. Sie können die Konfiguration verwenden `jobs/cleanup` REST-APIs ändern, wie lange Jobs und Job-Logs aufbewahrt werden. Der Spülzeitplan kann nicht geändert werden.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard** > **Job Monitor**.
3. Wählen Sie in der Titelleiste des Job Monitors das Download-Symbol aus.

   Möglicherweise müssen Sie nach rechts blättern, um das Symbol zu sehen.

   Sie können auch auf einen Job doppelklicken, um das Fenster Job-Details aufzurufen, und dann **Job-Protokolle herunterladen** auswählen.

Ergebnis

Job-Protokolle befinden sich auf dem Linux VM-Host, auf dem das SnapCenter Plug-in für VMware vSphere bereitgestellt wird. Der Standardspeicherort für das Jobprotokoll ist `/var/log/netapp`.

Wenn Sie versucht haben, Jobprotokolle herunterzuladen, aber die Protokolldatei mit dem Namen in der Fehlermeldung gelöscht wurde, kann es zu folgendem Fehler kommen: `HTTP ERROR 500 Problem accessing /export-scv-logs`. Um diesen Fehler zu beheben, überprüfen Sie den Zugriffsstatus und die Berechtigungen für die Datei mit dem Namen in der Fehlermeldung und beheben Sie das Zugriffsproblem.

Aufrufen von Berichten

Sie können über das Dashboard Berichte für einen oder mehrere Jobs anfordern.

Die Registerkarte Berichte enthält Informationen zu den Jobs, die auf der Seite Jobs im Dashboard ausgewählt wurden. Wenn keine Jobs ausgewählt sind, ist die Registerkarte Berichte leer.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard** > **Reports**.
3. Für Backup-Berichte können Sie Folgendes tun:
   a. Ändern Sie den Bericht

      Wählen Sie das Filtersymbol aus, um den Zeitbereich, den Jobstatustyp, die Ressourcengruppen und die Richtlinien zu ändern, die in den Bericht aufgenommen werden sollen.

   b. Erstellen eines detaillierten Berichts

Doppelklicken Sie auf einen Job, um einen detaillierten Bericht für diesen Job zu erstellen.

4. Optional: Wählen Sie auf der Registerkarte Berichte **Download** und wählen Sie das Format (HTML oder CSV) aus.

   Sie können das Download-Symbol auswählen, um Plug-In-Protokolle herunterzuladen.

Berichtstypen vom VMware vSphere Client

Der VMware vSphere Client für SnapCenter bietet anpassbare Berichtsoptionen, die Ihnen Details zu Ihren Datensicherungsaufgaben und zum Plug-in-Ressourcenstatus liefern. Sie können Berichte nur für den Primärschutz erstellen.

> Backup-Zeitpläne werden in der Zeitzone ausgeführt, in der das SnapCenter Plug-in für VMware vSphere bereitgestellt wird. VCenter meldet Daten in der Zeitzone, in der sich vCenter befindet. Wenn sich das SnapCenter-Plug-in für VMware vSphere und vCenter daher in unterschiedlichen Zeitzonen befinden, sind die Daten im VMware vSphere Client-Dashboard möglicherweise nicht mit den Daten in den Berichten identisch.

Das Dashboard zeigt Informationen zu migrierten Backups nur an, nachdem Backups nach der Migration durchgeführt wurden.

Berichtstyp	Beschreibung
Backup-Bericht	Zeigt Übersichtsdaten zu Sicherungsaufträgen an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um eine Liste der Jobs mit diesem Status auf der Registerkarte **Reports** anzuzeigen. Für jeden Job werden im Bericht die Job-ID, die entsprechende Ressourcengruppe, die Backup-Richtlinie, die Startzeit und -Dauer, der Status und die Jobdetails aufgeführt, die den Jobnamen (Snapshot-Name), wenn der Job abgeschlossen ist, sowie alle Warn- oder Fehlermeldungen enthalten. Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht). Gelöschte Backups sind nicht im Bericht enthalten.
Mount-Bericht	Zeigt Übersichtsdaten zu Mount-Jobs an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um eine Liste der Jobs mit diesem Status auf der Registerkarte Berichte anzuzeigen. Für jeden Job werden die Job-ID, der Job-Status, der Job-Name sowie die Start- und Endzeiten des Jobs im Bericht aufgelistet. Der Jobname enthält den Snapshot-Namen. Zum Beispiel: `Mount Backup <snapshot-copy-name>` Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht).

Berichtstyp	Beschreibung
Bericht Wiederherstellen	Zeigt Überblicksinformationen zu wiederherstellenden Jobs an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um eine Liste der Jobs mit diesem Status auf der Registerkarte Berichte anzuzeigen. Für jeden Job werden die Job-ID, der Job-Status, der Job-Name sowie die Start- und Endzeiten des Jobs im Bericht aufgelistet. Der Jobname enthält den Snapshot-Namen. Zum Beispiel: `Restore Backup <snapshot-copy-name>` Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht).
Letzter Sicherungsstatus von VMs oder Datastores	Zeigt eine Übersicht über den Schutzstatus während der konfigurierten Anzahl von Tagen für VMs und Datastores an, die vom SnapCenter-Plug-in für VMware vSphere verwaltet werden. Der Standardwert ist 7 Tage. Informationen zum Ändern des Werts in der Eigenschaftendatei finden Sie unter "Ändern Sie die Standardwerte der Konfiguration". Wählen Sie im primären Schutzdiagramm einen Abschnitt/Status aus, um eine Liste der VMs oder Datastores mit diesem Status auf der Registerkarte **Reports** anzuzeigen. Der Bericht zum Schutz der VMs oder Datastores für geschützte VMs und Datastores zeigt die Namen der VMs oder Datenspeicher an, die während der konfigurierten Anzahl von Tagen gesichert wurden, den Namen des letzten Snapshots sowie die Start- und Endzeiten der letzten Backup-Ausführung. In der VM- oder Datastores-Sicherungsstatusbericht für ungesicherte VMs oder Datastores werden die Namen von VMs oder Datastores angezeigt, die während der konfigurierten Anzahl von Tagen keine erfolgreichen Backups aufweisen. Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht). Dieser Bericht wird jede Stunde aktualisiert, wenn der Plug-in-Cache aktualisiert wird. Daher zeigt der Bericht möglicherweise keine VMs oder Datenspeicher an, die kürzlich gesichert wurden.

Generieren Sie ein Support-Paket aus der SnapCenter Plug-in for VMware vSphere Benutzeroberfläche

Bevor Sie beginnen

Um sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere anzumelden, müssen Sie die IP-Adresse und die Anmeldeinformationen

kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

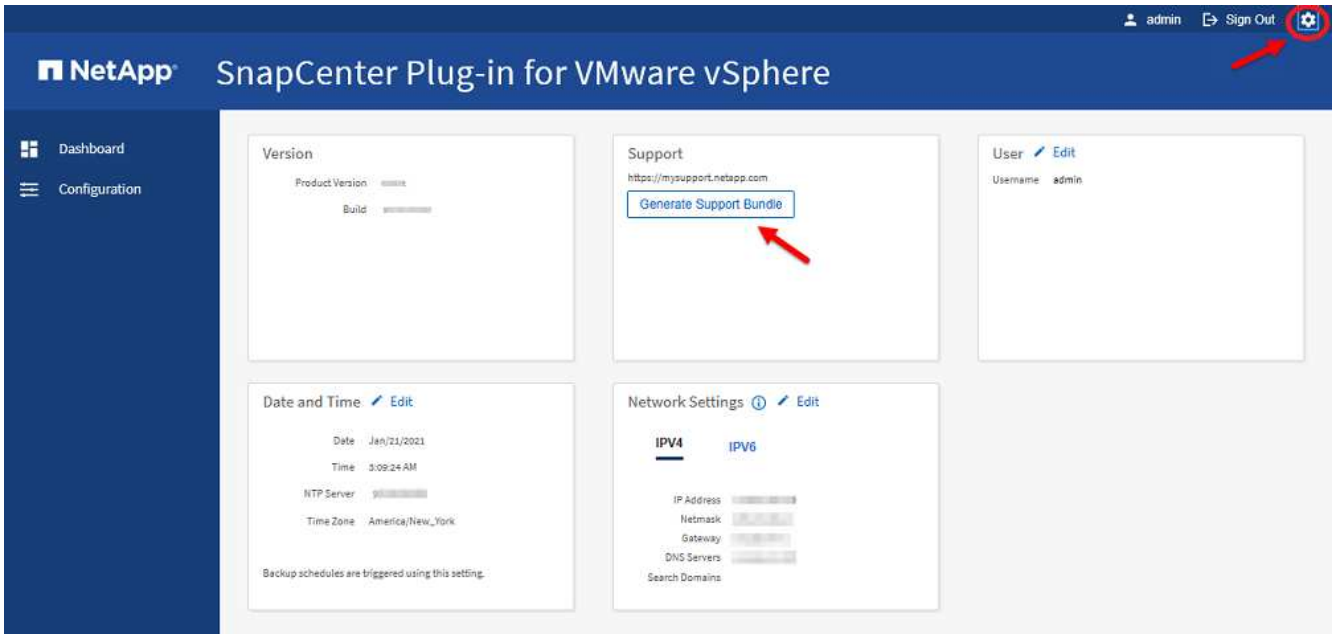
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere angezeigt.
- Verwenden Sie die Anmeldeinformationen, die während der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder später geändert wurden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

Schritte

1. Melden Sie sich bei der Benutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

   Verwenden Sie das Format `https://<OVA-IP-address>:8080`.

2. Wählen Sie das Symbol Einstellungen in der oberen Symbolleiste.



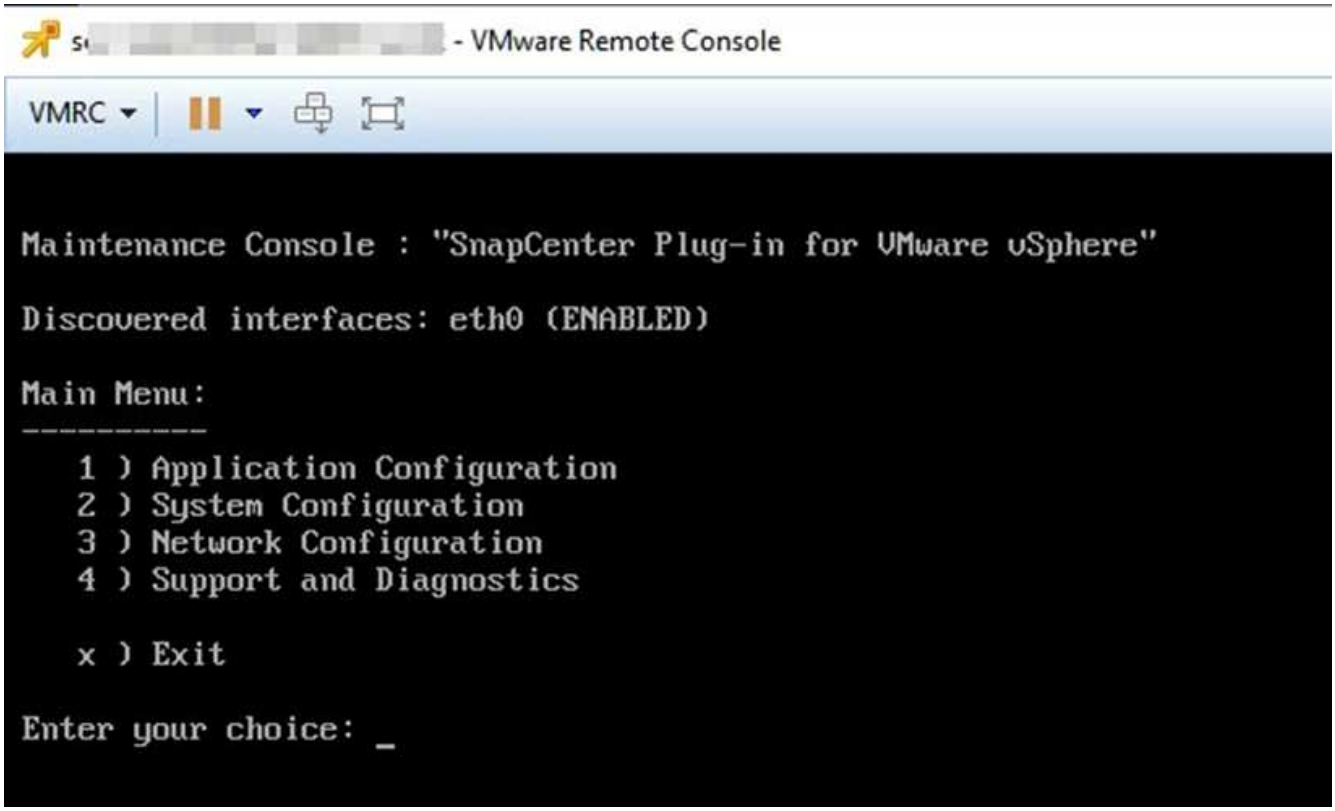
3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Support** die Option **Support** Bundle generieren.
4. Wählen Sie nach dem Generieren des Support-Bundles den Link aus, über den das Bundle auf NetApp heruntergeladen werden kann.

Generieren Sie ein Support-Bundle über die Wartungskonsole

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter-Plug-in für VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remote Console starten oder Web Console starten** aus, um ein Fenster der Wartungskonsole zu öffnen, und melden Sie sich dann an.

   Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter "Öffnen Sie die Wartungskonsole".



3. Geben Sie im Hauptmenü die Option **4) Support und Diagnose** ein.
4. Geben Sie im Menü Support und Diagnose die Option **1) Supportpaket generieren** ein.

Um auf das Support-Paket zuzugreifen, geben Sie im Menü Support und Diagnose die Option **2) Zugriff auf Diagnose Shell** ein. Navigieren Sie in der Konsole zu `/support/support/<bundle_name>.tar.gz`.

Prüfprotokolle

Ein Audit-Protokoll ist eine Sammlung von Ereignissen in chronologischer Reihenfolge, die in eine Datei innerhalb der Appliance geschrieben wird. Die Audit-Log-Dateien werden am Speicherort generiert `/var/log/netapp/audit` , und die Dateinamen folgen einer der folgenden Namenskonventionen:

- Audit.log: Aktive Audit-Log-Datei, die verwendet wird.
- Audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz: Gerollt über Audit-Log-Datei. Das Datum und die Uhrzeit im Dateinamen geben an, wann die Datei erstellt wurde, z. B. Audit-2022-12-15-16-28-01.log.gz.

In der SCV-Plug-in-Benutzeroberfläche können Sie die Audit-Log-Details über **Dashboard** > **Einstellungen** > **Audit-Protokolle**-Registerkarte anzeigen und exportieren. Die Prüfprotokolle werden mit dem Support Bundle heruntergeladen.

Wenn E-Mail-Einstellungen konfiguriert sind, sendet SCV eine E-Mail-Benachrichtigung im Falle eines Fehlers bei der Integritätsprüfung des Überwachungsprotokolls. Ein Fehler bei der Überprüfung der Integrität des Überwachungsprotokolls kann auftreten, wenn eine der Dateien manipuliert oder gelöscht wird.

Die Standardkonfigurationen der Audit-Dateien sind:

- Die verwendete Audit-Log-Datei kann auf maximal 10 MB anwachsen
- Es werden maximal 10 Audit-Log-Dateien aufbewahrt

Gerollte über Audit-Protokolle werden regelmäßig auf ihre Integrität überprüft. SCV stellt REST-APIs zur Verfügung, um Protokolle anzuzeigen und deren Integrität zu überprüfen. Ein integrierter Zeitplan löst und weist einen der folgenden Integritätsstatus zu.

Status	Beschreibung
MANIPULIERT	Der Inhalt der Audit-Log-Datei wird geändert
NORMAL	Audit-Log-Datei wurde nicht geändert
ROLLOVER LÖSCHEN	- Audit-Log-Datei wird auf Basis der Aufbewahrung gelöscht - Standardmäßig bleiben nur 10 Dateien erhalten
UNERWARTETES LÖSCHEN	Audit-Log-Datei wird gelöscht
AKTIV	- Audit Log Datei wird verwendet - Gilt nur für audit.log

Die Ereignisse lassen sich in drei Hauptkategorien einteilen:

- Ereignisse Auf Der Datensicherung
- Ereignisse Der Wartungskonsole
- Ereignisse Der Admin-Konsole

Ereignisse Auf Der Datensicherung

Die Ressourcen in SCV sind:

- Storage-System
- Ressourcengruppe
- Richtlinie
- Backup
- Abonnement
- Konto

In der folgenden Tabelle sind die Vorgänge aufgeführt, die für jede Ressource durchgeführt werden können:

Ressourcen	**Betrieb**
Storage-System	Erstellt, Geändert, Gelöscht
Abonnement	Erstellt, Geändert, Gelöscht
Konto	Erstellt, Geändert, Gelöscht
Ressourcengruppe	Erstellt, Geändert, Gelöscht, Unterbrochen, Fortgesetzt
Richtlinie	Erstellt, Geändert, Gelöscht

Backup	Erstellt, Umbenannt, Gelöscht, Angehängt, Abgehängt, VMDK wiederhergestellt, VM wiederhergestellt, VMDK anhängen, VMDK trennen, Gastdatei wiederherstellen

Ereignisse Der Wartungskonsole

Der administrative Betrieb in der Wartungskonsole wird geprüft. Folgende Optionen für die Wartungskonsole sind verfügbar:

1. Dienste starten/stoppen
2. Benutzername und Passwort ändern
3. MySQL-Kennwort ändern
4. Konfigurieren Sie MySQL Backup
5. MySQL Backup wiederherstellen
6. Ändern Sie das Benutzerpasswort „Wartung“
7. Zeitzone ändern
8. Ändern Sie den NTP-Server
9. Deaktivieren Sie den SSH-Zugriff
10. Erhöhen Sie die Größe der Jail-Festplatte
11. Upgrade
12. VMware Tools installieren (Wir arbeiten daran, dies durch Open-vm-Tools zu ersetzen)
13. Ändern Sie die IP-Adresseinstellungen
14. Ändern Sie die Einstellungen für die DNS-Suche
15. Ändern Sie statische Routen
16. Zugriff auf die Diagnoseschale
17. Remote-Diagnosezugriff aktivieren

Ereignisse Der Admin-Konsole

Die folgenden Vorgänge in der Admin Console-UI werden geprüft:

- Einstellungen
  - Ändern Sie die Anmeldedaten des Administrators
  - Ändern Sie die Zeitzone
  - Ändern Sie den NTP-Server
  - Ändern Sie die IPv4/IPv6-Adresseinstellungen
- Konfiguration
  - Ändern Sie die vCenter Credentials
  - Plug-in-Aktivierung/Deaktivierung

Konfigurieren Sie Syslog-Server

Prüfprotokolle werden in der Appliance gespeichert und regelmäßig auf ihre Integrität überprüft. Mit der Ereignisweiterleitung können Sie Ereignisse vom Quell- oder Weiterleitungscomputer abrufen und auf einem zentralen Computer, dem Syslog-Server, speichern. Die Daten werden während der Übertragung zwischen Quelle und Ziel verschlüsselt.

Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

Über diese Aufgabe

Diese Aufgabe unterstützt Sie bei der Konfiguration des Syslog-Servers.

Schritte

1. Melden Sie sich beim SnapCenter-Plug-in für VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen** > **Audit-Protokolle** > **Einstellungen**.
3. Wählen Sie im Bereich **Audit Log Settings** die Option **Send Audit Logs to Syslog Server** aus
4. Geben Sie die folgenden Details ein:
   - Syslog-Server-IP
   - Syslog-Server-Port
   - RFC-Format
   - Syslog-Serverzertifikat
5. Wählen Sie **SAVE**, um die Syslog-Server-Einstellungen zu speichern.

Ändern Sie die Einstellungen des Überwachungsprotokolls

Sie können die Standardkonfigurationen der Protokolleinstellungen ändern.

Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

Über diese Aufgabe

Mit dieser Aufgabe können Sie die standardmäßigen Einstellungen des Überwachungsprotokolls ändern.

Schritte

1. Melden Sie sich beim SnapCenter-Plug-in für VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen** > **Audit-Protokolle** > **Einstellungen**.
3. Geben Sie im Bereich **Audit Log Settings** die maximale Anzahl an Audit Log Files und die maximale Größe der Audit Log Files ein.
4. Wählen Sie die Option **Überwachungsprotokolle an Syslog-Server senden** aus, wenn Sie die Protokolle an Syslog-Server senden möchten. Geben Sie die Details des Servers ein.
5. Speichern Sie die Einstellungen.

Storage-Management

Erweitern Sie Ihren Storage

Bevor Sie VMs sichern oder wiederherstellen können, müssen Sie Storage-Cluster oder Storage-VMs hinzufügen. Durch Hinzufügen von Storage kann das SnapCenter Plug-in für VMware vSphere Backup- und Restore-Vorgänge in vCenter erkennen und managen.

- Welche Benutzeroberfläche soll verwendet werden?

  Verwenden Sie den VMware vSphere Client, um Storage hinzuzufügen.

- Große LUNs

  Das SnapCenter Plug-in für VMware vSphere 4.5 und höher unterstützt Datastores mit großen LUN-Größen bis zu 128 TB auf ASA Aggregaten. Bei großen LUNs unterstützt SnapCenter nur über Thick Provisioning bereitgestellte LUNs, um Latenz zu vermeiden.

- VMware Virtual Volumes (VVols)

  Sie müssen Storage-Cluster zum SnapCenter-Plug-in für VMware vSphere und ONTAP-Tools für VMware vSphere für vVol Data Protection hinzufügen, um arbeiten zu können.

  Weitere Informationen finden Sie in der Dokumentation zu den ONTAP tools for VMware vSphere . Weitere Informationen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" für aktuelle Informationen zu den unterstützten Versionen der ONTAP Tools.

Bevor Sie beginnen

Der ESXi-Server, das SnapCenter-Plug-in für VMware vSphere und jedes vCenter müssen zur gleichen Zeit synchronisiert werden. Wenn Sie versuchen, Speicher hinzuzufügen, aber die Zeiteinstellungen für Ihre vCenters nicht synchronisiert sind, schlägt der Vorgang möglicherweise mit einem Java-Zertifikatfehler fehl.

Über diese Aufgabe

Das SnapCenter Plug-in für VMware vSphere führt Backup- und Restore-Vorgänge auf direkt verbundenen Storage-VMs und Storage-VMs in einem Storage-Cluster durch.

> Wenn Sie das SnapCenter Plug-in for VMware vSphere verwenden, um anwendungsbasierte Backups auf VMDKs zu unterstützen, müssen Sie die SnapCenter Benutzeroberfläche verwenden, um Speicherauthentifizierungsdetails einzugeben und Speichersysteme zu registrieren.

- Bei vCenters im Linked-Modus müssen Sie jedem vCenter separat Storage-Systeme hinzufügen.
- Wenn Sie SVMs hinzufügen, müssen die Namen von Storage-VMs den Management-LIFs zugewiesen werden.

  Wenn Sie in SnapCenter Einträge zur Datei „*etc\Hosts*“ für Storage-VM-Namen hinzugefügt haben, müssen Sie sicherstellen, dass diese auch von der virtuellen Appliance aufgelöst werden können. Wenn dies nicht der Fall ist, sollten Sie ähnliche Einträge zur *etc/Hosts*-Datei innerhalb der Appliance hinzufügen.

  Wenn Sie eine Storage-VM mit einem Namen hinzufügen, der nicht zur Management-LIF auflöst, schlagen geplante Backup-Jobs fehl, da das Plug-in keine Datenspeicher oder Volumes auf dieser Storage-VM

finden kann. Falls dies der Fall ist, fügen Sie entweder die Storage VM zur SnapCenter hinzu und geben Sie die Management-LIF an, oder fügen Sie einen Cluster hinzu, der die Storage-VM enthält, und geben Sie die Cluster-Management-LIF an.

- Details zur Storage-Authentifizierung werden nicht von mehreren Instanzen des SnapCenter Plug-ins für VMware vSphere oder zwischen Windows SnapCenter Server und dem SnapCenter Plug-in in in vCenter gemeinsam genutzt.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard** > **Storage Systems**.
3. Wählen Sie auf der Seite Speichersysteme die Option **Hinzufügen** aus.
4. Geben Sie im Assistenten * Storage System* die grundlegenden Speicher-VM oder Cluster-Informationen ein, wie in der folgenden Tabelle aufgeführt:

Für dieses Feld…	Do this…
Storage-System	Geben Sie die IP-Adresse eines Storage-Clusters oder einer Storage-VM des FQDN oder Management LIF ein. Das SnapCenter Plug-in für VMware vSphere unterstützt nicht mehrere Storage-VMs mit demselben Namen in verschiedenen Clustern.
Authentifizierungsmethode	Wählen Sie entweder Anmeldeinformationen oder Zertifikat aus. Es werden zwei Arten von Zertifikaten unterstützt: - "Selbstsigniertes Zertifikat" - "KANN signiertes Zertifikat".
Benutzername	Dieses Feld wird angezeigt, wenn Sie Anmeldeinformationen als Authentifizierungsmethode auswählen. Geben Sie den ONTAP-Benutzernamen ein, mit dem Sie sich bei der Storage-VM oder beim Cluster anmelden.
Passwort	Dieses Feld wird angezeigt, wenn Sie Anmeldeinformationen als Authentifizierungsmethode auswählen. Geben Sie das Passwort für die Storage-VM oder das Cluster-Login ein.
Zertifikat	Dieses Feld wird angezeigt, wenn Sie Zertifikat als Authentifizierungsmethode auswählen. Wählen Sie die Zertifikatdatei aus.
Privater Schlüssel	Dieses Feld wird angezeigt, wenn Sie Zertifikat als Authentifizierungsmethode auswählen. Wählen Sie die Datei mit dem privaten Schlüssel aus.
Protokoll	Wählen Sie das Storage-Protokoll aus.
Port	Port, den das Speichersystem akzeptiert. - 443 für HTTPS-Verbindung - 80 für HTTP-Verbindung

Für dieses Feld…	Do this…
Zeitüberschreitung	Geben Sie die Anzahl der Sekunden ein, die das SnapCenter-Plug-in für VMware vSphere warten sollte, bevor Sie den Vorgang absetzen. Die Standardeinstellung ist 60 Sekunden.
Bevorzugte IP-Adresse	Wenn die Speicher-VM über mehr als eine Management-IP-Adresse verfügt, aktivieren Sie dieses Kontrollkästchen, und geben Sie die IP-Adresse ein, die das SnapCenter-Plug-in für VMware vSphere verwenden soll. **Hinweis:** Verwenden Sie keine eckigen Klammern ([]), wenn Sie die IP-Adresse eingeben.
Einstellungen für Ereignismanagement-System (EMS) und AutoSupport	Wenn Sie EMS-Meldungen an das Syslog-Speichersystem senden möchten oder wenn Sie AutoSupport-Meldungen für den angewendeten Schutz, abgeschlossene Wiederherstellungsvorgänge oder fehlgeschlagene Vorgänge an das Speichersystem senden möchten, aktivieren Sie das entsprechende Kontrollkästchen. Aktivieren Sie das Kontrollkästchen **AutoSupport-Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden** und das Kontrollkästchen * SnapCenter-Serverereignisse in syslog*, um AutoSupport-Benachrichtigungen zu aktivieren.
Protokollieren von SnapCenter-Serverereignissen im Syslog	Aktivieren Sie das Kontrollkästchen, um Ereignisse für das SnapCenter-Plug-in für VMware vSphere zu protokollieren.
AutoSupport-Benachrichtigung für fehlgeschlagenen Vorgang an das Speichersystem senden	Aktivieren Sie das Kontrollkästchen, wenn AutoSupport-Benachrichtigungen für fehlgeschlagene Datensicherungsaufträge angezeigt werden sollen. Sie müssen auch AutoSupport auf der Storage VM aktivieren und die AutoSupport E-Mail-Einstellungen konfigurieren.

5. Wählen Sie **Hinzufügen**.

   Wenn Sie ein Storage-Cluster hinzugefügt haben, werden alle Storage-VMs in diesem Cluster automatisch hinzugefügt. Automatisch hinzugefügte Speicher-VMs (manchmal auch „implizite“ Speicher-VMs genannt) werden auf der Cluster-Übersichtsseite mit einem Bindestrich (-) anstelle eines Benutzernamens angezeigt. Benutzernamen werden nur für explizite Speichereinheiten angezeigt.

Management von Storage-Systemen

Bevor Sie VMs oder Datastores mithilfe des VMware vSphere Clients sichern oder wiederherstellen können, müssen Sie den Storage hinzufügen.

Ändern Sie Storage-VMs

Mit dem VMware vSphere Client können Sie die Konfigurationen der Cluster und Storage-VMs, die im SnapCenter Plug-in für VMware vSphere registriert und für VM-Datensicherungsvorgänge verwendet werden, ändern.

Wenn Sie eine Storage-VM ändern, die automatisch als Teil eines Clusters hinzugefügt wurde (manchmal auch als implizite Storage-VM bezeichnet), dann ändert sich diese Storage-VM in eine explizite Storage-VM und kann separat gelöscht werden, ohne die restlichen Storage-VMs in diesem Cluster zu ändern. Auf der Seite Storage Systems wird der Benutzername als N/A angezeigt, wenn die Authentifizierungsmethode über das Zertifikat erfolgt. Benutzernamen werden nur für explizite Speicher-VMs in der Cluster-Liste angezeigt und lassen das ExplicitSVM-Flag auf true gesetzt. Alle Storage-VMs werden immer unter dem zugehörigen Cluster aufgeführt.

Wenn Sie Speicher-VMs für anwendungsbasierte Datenschutzvorgänge über die SnapCenter -Benutzeroberfläche hinzugefügt haben, müssen Sie zum Ändern dieser Speicher-VMs dieselbe Benutzeroberfläche verwenden.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Storage Systems** aus.
2. Wählen Sie auf der Seite **Speichersysteme** die zu ändernde Speicher-VM aus und wählen Sie dann **Bearbeiten**.
3. Geben Sie im Fenster **Speichersystem bearbeiten** die neuen Werte ein, und wählen Sie dann **Update**, um die Änderungen anzuwenden.

Storage-VMs entfernen

Sie können den VMware vSphere-Client verwenden, um Storage-VMs aus dem Inventar in vCenter zu entfernen.

Wenn Sie Speicher-VMs für anwendungsbasierte Datenschutzvorgänge über die SnapCenter -Benutzeroberfläche hinzugefügt haben, müssen Sie zum Ändern dieser Speicher-VMs dieselbe Benutzeroberfläche verwenden.

Bevor Sie beginnen

Sie müssen alle Datenspeicher in der Storage-VM unmounten, bevor Sie die Storage-VM entfernen können.

Über diese Aufgabe

Wenn eine Ressourcengruppe Backups enthält, die sich auf einer Speicher-VM befinden, die Sie entfernen, dann schlagen nachfolgende Backups für diese Ressourcengruppe fehl.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Storage Systems** aus.
2. Wählen Sie auf der Seite **Storage Systems** die zu entfernende Speicher-VM aus und wählen Sie dann **Delete** aus.
3. Aktivieren Sie im Bestätigungsfeld **Speichersystem entfernen** das Kontrollkästchen **Speichersystem(e) löschen** und wählen Sie dann **Ja** zur Bestätigung aus. **Hinweis:** nur ESXi-Host 7.0U1 und neuere Versionen werden unterstützt.

   "Starten Sie den VMware vSphere-Client-Service neu".

Ändern Sie die konfigurierte Storage-Zeitüberschreitung

Obwohl Backups in der Vergangenheit erfolgreich ausgeführt wurden, können sie zu dem Zeitpunkt fehlschlagen, zu dem das SnapCenter-Plug-in für VMware vSphere warten muss, bis das Speichersystem den konfigurierten Timeout-Zeitraum überschreitet. Wenn diese Bedingung eintritt, können Sie die konfigurierte Zeitüberschreitung erhöhen.

Möglicherweise tritt der Fehler auf `Unable to discover resources on SCV: Unable to get storage details for datastore <xxx>…`

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Storage Systems** aus.
2. Wählen Sie auf der Seite Speichersysteme das zu ändernde Speichersystem aus und wählen Sie **Bearbeiten**.
3. Erhöhen Sie im Feld Timeout die Anzahl der Sekunden.

   Für große Umgebungen wird 180 Sekunden empfohlen.

Sichern von Daten

Datensicherungs-Workflow

Nutzen Sie den SnapCenter vSphere Client, um Datensicherungsvorgänge für VMs, VMDKs und Datastores durchzuführen. Alle Backup-Vorgänge werden von Ressourcengruppen durchgeführt, die eine oder mehrere VMs und Datastores beliebig kombinieren können. Sie können Backups nach Bedarf oder gemäß einem definierten Schutzzeitplan erstellen.

Wenn Sie einen Datenspeicher sichern, sichern Sie alle VMs in diesem Datenspeicher.

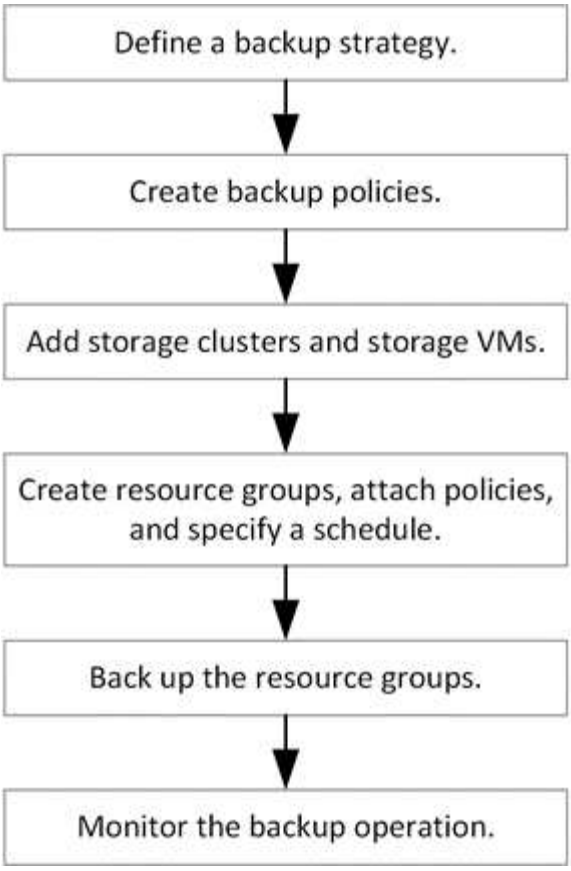
Backup- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressourcengruppe durchgeführt werden.

Sehen Sie sich die Informationen zu Funktionen an, die das SnapCenter Plug-in für VMware vSphere unterstützt und nicht. "Implementierungsplanung und -Anforderungen"

In MetroCluster Konfigurationen:

- Das SnapCenter Plug-in für VMware vSphere kann nach einem Failover möglicherweise keine Sicherungsbeziehung erkennen. Weitere Informationen finden Sie unter "KB-Artikel: Kann die SnapMirror oder SnapVault-Beziehung nach dem MetroCluster Failover nicht erkennen" .
- Wenn Backups mit dem Fehler fehlschlagen `Unable to discover resources on SCV: <xxx>…` Starten Sie bei NFS und VMFS VMs nach Umschaltung/Switch wieder die SnapCenter VMware Services von der Wartungskonsole aus neu.

Die folgende Workflow-Abbildung zeigt die Reihenfolge, in der Sie Sicherungsvorgänge ausführen müssen:



Zeigen Sie VM- und Datastore-Backups an

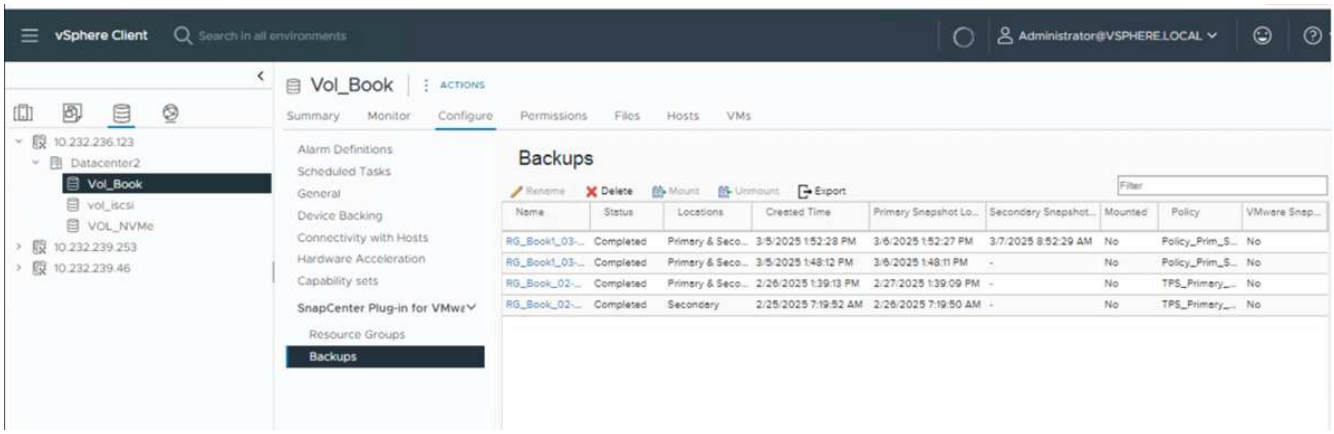
Bei der Vorbereitung der Sicherung oder Wiederherstellung einer VM oder eines Datastore sollten Sie möglicherweise alle für diese Ressource verfügbaren Backups anzeigen und die Details dieser Backups anzeigen.

Über diese Aufgabe

Das Durchsuchen großer Dateiordner, wie etwa 10k-Dateiordner, kann beim ersten Mal eine oder mehrere Minuten dauern. Nachfolgende Browsersitzungen nehmen weniger Zeit in Anspruch.

Schritte

1. Melden Sie sich beim vCenter Server an.
2. Navigieren Sie zur Seite **Inventar** und wählen Sie einen Datastore oder eine VM aus.
3. Wählen Sie im rechten Fensterbereich **Konfigurieren** > **SnapCenter-Plug-in für VMware vSphere** > **Backups**.



Wenn die Option **Enable Secondary Snapshot Locking** während der Richtlinienerstellung nicht ausgewählt ist, wird standardmäßig der für die Option **Enable Primary Snapshot Locking** festgelegte Wert verwendet. In der Liste Backups zeigt der Bindestrich im Feld **Secondary Snapshot Lock Expiration** an, dass sowohl primäre als auch sekundäre Sperrfristen identisch sind.

4. Wählen Sie das Backup aus, das Sie anzeigen möchten.

Erstellen von Backup-Richtlinien für VMs und Datastores

Sie müssen Backup-Richtlinien erstellen, bevor Sie das SnapCenter Plug-in für VMware vSphere zum Backup von VMs und Datastores verwenden.

Bevor Sie beginnen

- Sie müssen die Voraussetzungen gelesen haben.
- Sie müssen sekundäre Storage-Beziehungen konfiguriert haben.
  - Wenn Sie Snapshots auf einen sekundären Spiegel- oder Vault-Speicher replizieren, müssen die Beziehungen konfiguriert werden. Der SnapCenter-Administrator muss Ihnen die Storage-VMs sowohl für die Quell- als auch für die Ziel-Volumes zugewiesen haben.
  - Um Snapshots für Versionen-FlexibleMirror-Beziehungen auf einem NFS- oder VMFS-Datastore erfolgreich in den sekundären Speicher zu übertragen, stellen Sie sicher, dass der Richtlinientyp SnapMirror „asynchrone Spiegelung“ ist und dass die Option „all_source_Snapshots“ aktiviert ist.
  - Wenn die Anzahl der Snapshots auf dem sekundären Speicher (Mirror-Vault) das maximale Limit erreicht, schlägt die Aktivität zur Registrierung von Backups und Anwendung der Aufbewahrung im Backup-Vorgang mit folgender Fehlermeldung fehl: `This snapshot is currently used as a reference snapshot by one or more SnapMirror relationships. Deleting the snapshot can cause future SnapMirror operations to fail.`

    Um dieses Problem zu beheben, konfigurieren Sie die SnapMirror-Aufbewahrungsrichtlinie für sekundären Speicher, um zu vermeiden, dass die maximale Snapshot-Grenze erreicht wird.

  Informationen dazu, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie unter "SnapCenter-Informationen zur Nutzung der rollenbasierten Zugriffssteuerung" .

- Wenn Sie VM-konsistente Backups wünschen, müssen VMware Tools installiert und ausgeführt werden. Um VMs stillzulegen, sind VMware Tools erforderlich. VM-konsistente Backups werden für vVol VMs nicht unterstützt.
- SnapMirror Active Sync ermöglicht Business Services auch bei einem vollständigen Standortausfall den

Betrieb weiter und unterstützt Applikationen bei einem transparenten Failover mithilfe einer sekundären Kopie.

SnapMirror Active Sync wird nur für VMFS Datastores unterstützt.

Zum Schutz eines VMFS-Datenspeichers in einer Implementierung mit aktiver SnapMirror Synchronisierung müssen Sie als SnapCenter-Administrator Folgendes tun:

- Konfigurieren Sie Cluster und Mediator wie im technischen Bericht beschrieben: "Konfigurieren Sie den ONTAP Mediator und die Cluster für SnapMirror Active Sync".
- Fügen Sie das dem VMFS-Datastore zugeordnete Volume zur Konsistenzgruppe hinzu und erstellen Sie mithilfe der *AutomatedFailOver*- oder *AutomatedFailOverDuplex*-Schutzrichtlinie zwischen zwei ONTAP-Speichersystemen eine Datensicherungsbeziehung. *AutomaticatedFailOverDuplex*-Richtlinie wird ab ONTAP 9.15.1 unterstützt.

In der Fan-out-Konfiguration wird die Konsistenzgruppe für einen tertiären Standort nicht unterstützt.

Über diese Aufgabe

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. In den folgenden Informationen werden einige der Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Richtlinien** aus.
2. Wählen Sie auf der Seite **Policies Create** aus, um den Assistenten zu starten.
3. Geben Sie auf der Seite **New Backup Policy** den Richtliniennamen und eine Beschreibung ein.

   - Verknüpfter Modus

     Im Linked-Modus besitzt jedes vCenter eine separate virtuelle Appliance. Daher können Sie doppelte Namen in allen vCenters verwenden. Sie müssen die Richtlinie jedoch im selben vCenter wie die Ressourcengruppe erstellen.

   - Nicht unterstützte Zeichen

     Verwenden Sie nicht die folgenden Sonderzeichen in VMs, Datenspeicher, Cluster, Richtlinien, Backups, Oder Ressourcengruppennamen: % & * € # @ ! \ / : * ? " < > - | ; ' und Leerzeichen.

   Ein Unterstrich (_) ist zulässig.

4. Geben Sie die Frequenzeinstellungen an.

   Die Richtlinie gibt nur die Backup-Häufigkeit an. Der spezifische Schutzzeitplan für das Sichern ist in der Ressourcengruppe festgelegt. Daher können zwei oder mehr Ressourcengruppen dieselbe Richtlinien- und Backup-Häufigkeit teilen, jedoch unterschiedliche Backup-Pläne haben.

5. Aktivieren Sie das Kontrollkästchen **Sperrfrist**, um die Snapshot-Sperrung zu aktivieren. Sie können die Sperrzeiten für primäre und sekundäre Snapshots als Tage/Monate/Jahre auswählen.

   Unabhängig vom in der ONTAP SnapMirror-Richtlinie festgelegten Aufbewahrungswert wird die sekundäre Snapshot-Kopie vor der angegebenen sekundären Snapshot-Sperrfrist nicht gelöscht.

6. Legen Sie die Aufbewahrungseinstellungen fest.

> Sie sollten den Aufbewahrungswert auf 2 Backups oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 Backup gesetzt haben, kann der Aufbewahrungsvorgang fehlschlagen. Das liegt daran, dass der erste Snapshot der Referenz-Snapshot für die SnapVault-Beziehung ist, bis der neuere Snapshot auf das Ziel repliziert wird.

> Der maximale Aufbewahrungswert beträgt 1018 Backups. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Das gilt auch für das Spanning von Datenspeichern.

7. Geben Sie in den Feldern **Replikation** den Replikationstyp auf sekundären Speicher an, wie in der folgenden Tabelle dargestellt:

Für dieses Feld…	Do this…
Aktualisierung von SnapMirror nach dem Backup	Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen, das über eine SnapMirror Beziehung zum primären Backup Volume verfügt. Wenn ein Volume mit einer Mirror-Vault-Beziehung konfiguriert ist, müssen Sie nur die Option **Update SnapVault after Backup** auswählen, wenn Sie Backups auf die Mirror-Vault Ziele kopieren möchten. Diese Option wird für Datastores in FlexGroup Volumes im SnapCenter Plug-in für VMware vSphere 4.5 und höher unterstützt. Zum Schutz des VMFS-Datastore auf der Bereitstellung von SnapMirror Active Sync müssen Sie die im Abschnitt *before you begin* genannten Voraussetzungen erfüllen und **Update SnapMirror after Backup** aktivieren.

Für dieses Feld…	Do this…
SnapVault nach Backup aktualisieren	Wählen Sie diese Option aus, um Disk-to-Disk Backup-Replikation auf einem anderen Volume mit einer SnapVault-Beziehung zum primären Backup Volume durchzuführen. Wenn ein Volume mit einer Mirror-Vault-Beziehung konfiguriert ist, müssen Sie nur diese Option auswählen, wenn Sie Backups auf die Mirror-Vault Ziele kopieren möchten. Diese Option wird für Datastores in FlexGroup Volumes im SnapCenter Plug-in für VMware vSphere 4.5 und höher unterstützt.
Snapshot-Etikett	Geben Sie ein optionales, benutzerdefiniertes Etikett ein, das zu SnapVault- und SnapMirror-Snapshots, die mit dieser Richtlinie erstellt wurden, hinzugefügt werden soll. Das Snapshot-Label hilft, mit dieser Richtlinie erstellte Snapshots von anderen Snapshots auf dem sekundären Storage-System zu unterscheiden. Für Snapshot-Beschriftungen sind maximal 31 Zeichen zulässig.

8. Optional: Wählen Sie in den Feldern **Erweitert** die gewünschten Felder aus. In der folgenden Tabelle sind die Details zum Advanced Field Portal aufgeführt.

Für dieses Feld…	Do this…
VM-Konsistenz	Aktivieren Sie dieses Kontrollkästchen, um die VMs stillzulegen und jedes Mal, wenn der Backup-Job ausgeführt wird, einen VMware-Snapshot zu erstellen. Diese Option wird für VVols nicht unterstützt. Bei vVol VMs werden nur absturzkonsistente Backups durchgeführt. Sie müssen VMware Tools auf der VM ausführen, um VM-konsistente Backups durchzuführen. Wenn VMware-Tools nicht ausgeführt werden, wird stattdessen ein Crash-konsistentes Backup durchgeführt. Wenn Sie das Kontrollkästchen für die Konsistenz der VM aktivieren, können Backup-Vorgänge länger dauern und mehr Speicherplatz benötigen. In diesem Szenario werden die VMs zuerst stillgelegt, dann führt VMware einen VM-konsistenten Snapshot durch, dann führt SnapCenter seinen Backup-Vorgang durch und anschließend werden die VM-Vorgänge wieder aufgenommen. Der VM-Gastspeicher ist nicht in VM Consistency Snapshots enthalten.
Einbeziehen von Datastores mit unabhängigen Festplatten	Aktivieren Sie dieses Kontrollkästchen, um alle Datenspeicher mit unabhängigen Festplatten, die temporäre Daten enthalten, in das Backup einzubeziehen.

Für dieses Feld…	Do this…
Skripte	Geben Sie den vollständig qualifizierten Pfad des Prescript oder Postscripts ein, das das SnapCenter-Plug-in für VMware vSphere vor oder nach Sicherungsvorgängen ausführen soll. Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren und Protokolle zu senden. Der Skriptpfad wird zum Zeitpunkt der Ausführung des Skripts validiert. Prescripts und Postscripts müssen auf der VM der virtuellen Appliance liegen. Um mehrere Skripte einzugeben, drücken Sie nach jedem Skriptpfad **Enter**, um jedes Skript in einer eigenen Zeile aufzulisten. Das Zeichen „;“ ist nicht zulässig.

9. Wählen Sie **Hinzufügen**

   Sie können die Erstellung der Richtlinie überprüfen und die Richtlinienkonfiguration überprüfen, indem Sie die Richtlinie auf der Seite Richtlinien auswählen.

Erstellen von Ressourcengruppen

Eine Ressourcengruppe ist der Container für VMs, Datastores, vSphere Tags und vSphere VM-Ordner, den Sie schützen möchten.

Eine Ressourcengruppe kann Folgendes enthalten:

- Beliebige Kombination aus herkömmlichen VMs, herkömmlichen SAN-Datenspeichern und herkömmlichen NAS-Datastores Herkömmliche VMs können nicht mit vVol VMs kombiniert werden.
- Ein einzelner FlexGroup Datenspeicher. SCV unterstützt keine übergreifenden FlexGroup Datenspeicher. Ein FlexGroup -Datenspeicher kann nicht mit herkömmlichen VMs oder Datenspeichern kombiniert werden.
- Ein oder mehrere FlexVol Datastores. Spanning-Datenspeicher werden unterstützt.
- Ein oder mehrere vVol VMs. VVol VMs können nicht mit herkömmlichen VMs oder Datastores kombiniert werden.
- Alle VMs und Datastores, ausgenommen vVol Datastores, die das angegebene vSphere-Tag haben.
- Alle VVols in einem einzelnen, angegebenen vVol Ordner. Wenn der Ordner eine Kombination aus vVol VMs und herkömmlichen VMs enthält, sichert das SnapCenter Plug-in für VMware vSphere die vVol VMs und überspringt die herkömmlichen VMs.
- VMs und Datenspeicher auf ASA R2-Speichersystemen. Sie können ASA R2-VMs und -Datenspeicher nicht mit anderen VMs und Datenspeichern kombinieren.

Wenn Sie VMware vSphere Cluster Service (vCLS) verwenden, fügen Sie dem SnapCenter Plug-in for VMware vSphere Ressourcengruppen keine von vCLS verwalteten VMs hinzu.

Weitere Informationen finden Sie unter "SCV kann VCLS-VMs nicht sichern, nachdem vCenter auf 7.0.x aktualisiert wurde"

Das SnapCenter Plug-in für VMware vSphere 4.5 und höher unterstützt Datastores auf großen LUNs und Dateien bis zu 128 TB mit Volumen von bis zu 300 TB. Wenn Sie große LUNs schützen, verwenden Sie nur per Thick Provisioning bereitgestellte LUNs, um Latenz zu vermeiden.

Fügen Sie keine VMs hinzu, die sich in einem nicht zugänglichen Zustand befinden. Obwohl es möglich ist, eine Ressourcengruppe zu erstellen, die nicht zugängliche VMs enthält, schlägt die Erstellung von Backups für diese Ressourcengruppe fehl.

Bevor Sie beginnen

ONTAP Tools für VMware müssen bereitgestellt werden, bevor Sie eine Ressourcengruppe erstellen, die vVol VMs enthält.

Weitere Informationen finden Sie in der Dokumentation zu den ONTAP tools for VMware vSphere . Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" .

Über diese Aufgabe

- Sie können einer Ressourcengruppe jederzeit Ressourcen hinzufügen oder daraus entfernen.
- Um eine einzelne Ressource, beispielsweise eine VM, zu sichern, erstellen Sie eine Ressourcengruppe, die nur diese Ressource enthält.
- Um mehrere Ressourcen zu sichern, erstellen Sie eine Ressourcengruppe, die alle Ressourcen enthält, die Sie schützen möchten.
- Wenn Sie für FlexGroup -Volumes in MetroCluster Umgebungen ONTAP 9.8 oder 9.9 verwenden, starten Sie das SnapCenter Plug-in for VMware vSphere Dienst neu und synchronisieren Sie die SnapMirror -Beziehungen nach einem Switchover oder Switchback neu, bevor Sie Ressourcengruppen sichern. In ONTAP 9.8 können Backups nach einem Switchback hängen bleiben. Dieses Problem wurde in ONTAP 9.9 behoben.
- Um eine optimale Snapshot-Leistung zu erzielen, gruppieren Sie VMs und Datenspeicher auf demselben Volume in einer einzigen Ressourcengruppe.
- Sie können eine Ressourcengruppe ohne Sicherungsrichtlinie erstellen, für den Datenschutz ist jedoch mindestens eine Richtlinie erforderlich. Wählen Sie eine vorhandene Richtlinie aus oder erstellen Sie während der Erstellung der Ressourcengruppe eine neue.

  Wenn Sie eine Backup-Richtlinie mit Snapshot-Sperrfrist auswählen, müssen Sie ONTAP 9.12.1 oder höher auswählen.

- Beim Erstellen einer Ressourcengruppe führt SnapCenter Kompatibilitätsprüfungen durch.

  Managen Sie Fehler bei der Kompatibilitätsprüfung

- Erstellen Sie einen sekundären Schutz für eine Ressourcengruppe

  Der sekundäre Schutz ermöglicht die Replikation für die Ressourcen in der Ressourcengruppe. Um den sekundären Schutz zu verwenden, erstellen Sie mithilfe einer angegebenen Richtlinie eine auf einer

Konsistenzgruppe basierende SnapMirror -Beziehung vom primären zum bevorzugten Cluster und SVM. Diese Funktion wird nur für auf dem ASA R2-System basierende Datenspeicher und virtuelle Maschinen unterstützt. Stellen Sie sicher, dass Cluster- und SVM-Peering im Voraus konfiguriert sind. Es werden nur asynchrone SnapMirror Richtlinien unterstützt. Beim Konfigurieren des sekundären Schutzes müssen Sie ein Konsistenzgruppensuffix angeben.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Ressourcengruppen** und dann **Erstellen** aus, um den Assistenten zu starten. Alternativ können Sie eine Ressourcengruppe für eine einzelne Ressource erstellen, indem Sie einen der folgenden Schritte ausführen:
   - Um eine Ressourcengruppe für eine VM zu erstellen, wählen Sie auf der Seite Verknüpfungen **Hosts und Cluster** aus, klicken Sie mit der rechten Maustaste auf eine VM und wählen Sie **SnapCenter-Plug-in für VMware vSphere** > **Ressourcengruppe erstellen** aus.
   - Um eine Ressourcengruppe für einen Datastore zu erstellen, wählen Sie auf der Shortcuts-Seite **Hosts und Cluster** aus, klicken Sie mit der rechten Maustaste auf einen Datastore, wählen Sie **SnapCenter-Plug-in für VMware vSphere** > **Ressourcengruppe erstellen** aus.
2. Gehen Sie auf der Seite **Allgemeine Informationen & Benachrichtigungen** im Assistenten wie folgt vor:

Für dieses Feld…	**Do this…**
VCenter Server	Wählen Sie einen vCenter-Server aus.
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Verwenden Sie die folgenden Sonderzeichen nicht in VM-, Datenspeicher-, Richtlinien-, Sicherungs- oder Ressourcengruppennamen: % & * $ # @ ! \ / : * ? " < > - [vertikaler Strich] ; ' und Leerzeichen. Ein Unterstrich (_) ist zulässig. VM- oder Datenspeichernamen mit Sonderzeichen werden abgeschnitten, was die Suche nach einem bestimmten Backup erschwert. Im verknüpften Modus verwaltet jedes vCenter sein eigenes SnapCenter Plug-in for VMware vSphere Repository. Dadurch können Sie dieselben Ressourcengruppennamen in verschiedenen vCentern verwenden.
Beschreibung	Geben Sie eine Beschreibung der Ressourcengruppe ein.
Benachrichtigung	Wählen Sie aus, wann Sie Benachrichtigungen über Vorgänge dieser Ressourcengruppe erhalten möchten: Fehler oder Warnungen: Nur Fehler und Warnungen senden: Nur Benachrichtigungen für Fehler senden immer nur senden: Benachrichtigung für alle Nachrichtentypen senden nie: Keine Benachrichtigung senden
E-Mail senden von	Geben Sie die E-Mail-Adresse ein, von der die Benachrichtigung gesendet werden soll.

Für dieses Feld…	Do this…
E-Mail senden an	Geben Sie die E-Mail-Adresse der Person ein, die Sie erhalten möchten. Verwenden Sie für mehrere Empfänger ein Komma, um die E-Mail-Adressen zu trennen.
E-Mail-Betreff	Geben Sie den gewünschten Betreff für die Benachrichtigungs-E-Mails ein.
Letzter Snapshot-Name	Wenn Sie das Suffix „_recent“ zum letzten Snapshot hinzufügen möchten, aktivieren Sie dieses Kontrollkästchen. Das Suffix „_recent“ ersetzt Datum und Zeitstempel. A `_recent` Für jede Richtlinie, die einer Ressourcengruppe zugeordnet ist, wird ein Backup erstellt. Daher wird eine Ressourcengruppe mit mehreren Richtlinien über mehrere Ressourcen verfügen `_recent` Backups: Nicht manuell umbenennen `_recent` Backups: Das ASA r2-Speichersystem unterstützt das Umbenennen von Snapshots nicht und daher werden die Umbenennungsfunktionen von SCV und die letzten Snapshot-Benennungsfunktionen nicht unterstützt.

Für dieses Feld…	Do this…
Benutzerdefiniertes Snapshot-Format	Wenn Sie ein benutzerdefiniertes Format für die Snapshot-Namen verwenden möchten, aktivieren Sie dieses Kontrollkästchen, und geben Sie das Namensformat ein. • Diese Funktion ist standardmäßig deaktiviert. • Standardmäßig folgen Snapshot-Namen dem Format `<ResourceGroup>_<Date-TimeStamp>` . Sie können den Snapshot-Namen mithilfe von Variablen wie $ResourceGroup, $Policy, $HostName, $ScheduleType und $CustomText anpassen. Wählen Sie die gewünschten Variablen und deren Reihenfolge aus der Dropdown-Liste im Feld „Benutzerdefinierter Name“ aus. Wenn Sie $CustomText einschließen, wird das Format `<CustomName>_<Date-TimeStamp>` . Geben Sie Ihren benutzerdefinierten Text in das bereitgestellte Feld ein. [HINWEIS]: Wenn Sie das Suffix „_recent“ auswählen, stellen Sie sicher, dass Ihre benutzerdefinierten Snapshot-Namen innerhalb des Datenspeichers eindeutig sind, indem Sie die Variablen $ResourceGroup und $Policy in den Namen aufnehmen. • Sonderzeichen für Sonderzeichen in Namen, befolgen Sie die gleichen Richtlinien für das Namensfeld.

3. Gehen Sie auf der Seite **Ressourcen** wie folgt vor:

Für dieses Feld…	Do this…
Umfang	Wählen Sie den zu schützenden Ressourcentyp aus: * Datenspeicher (alle traditionellen VMs in einem oder mehreren angegebenen Datastores). Sie können keinen vVol Datastore auswählen. * Virtual Machines (einzelne traditionelle oder vVol VMs; im Feld müssen Sie zu dem Datenspeicher navigieren, der die VMs oder vVol VMs enthält). Sie können keine einzelnen VMs in einem FlexGroup Datastore auswählen. * Tags Der Tag-basierte Datastore-Schutz wird nur für NFS- und VMFS-Datastores sowie für Virtual Machines und vVol Virtual Machines unterstützt. * VM-Ordner (alle vVol-VMs in einem angegebenen Ordner; im Popup-Feld müssen Sie zu dem Rechenzentrum navigieren, in dem sich der Ordner befindet)

Für dieses Feld…	Do this…
Rechenzentrum	Navigieren Sie zu den VMs, Datastores oder Ordnern, die Sie hinzufügen möchten. Namen von VMs und Datenspeichern in einer Ressourcengruppe müssen eindeutig sein.
Verfügbare Einheiten	Wählen Sie die Ressourcen aus, die Sie schützen möchten, und wählen Sie dann **>**, um Ihre Auswahl in die Liste Ausgewählte Elemente zu verschieben.

Wenn Sie **Weiter** auswählen, prüft das System zunächst, ob SnapCenter den Speicher verwaltet und mit dem Speicher kompatibel ist, auf dem sich die ausgewählten Ressourcen befinden.

Wenn die Meldung `Selected <resource-name> is not SnapCenter compatible` angezeigt wird, ist eine ausgewählte Ressource nicht mit SnapCenter kompatibel.

Um einen oder mehrere Datastores global von Backups auszuschließen, müssen Sie den/die Datastore-Namen in der Eigenschaft in der Konfigurationsdatei angeben `global.ds.exclusion.pattern scbr.override` . Siehe "Eigenschaften, die Sie überschreiben können".

4. Wählen Sie auf der Seite **Spanning Disks** eine Option für VMs mit mehreren VMDKs über mehrere Datastores aus:
   - Schließen Sie immer alle Spanning Datastores aus (dies ist der Standard für Datastores.)
   - Berücksichtigen Sie immer alle spannenden Datenspeicher (dies ist der Standard für VMs).
   - Wählen Sie manuell die Spanning-Datenspeicher aus, die einbezogen werden sollen

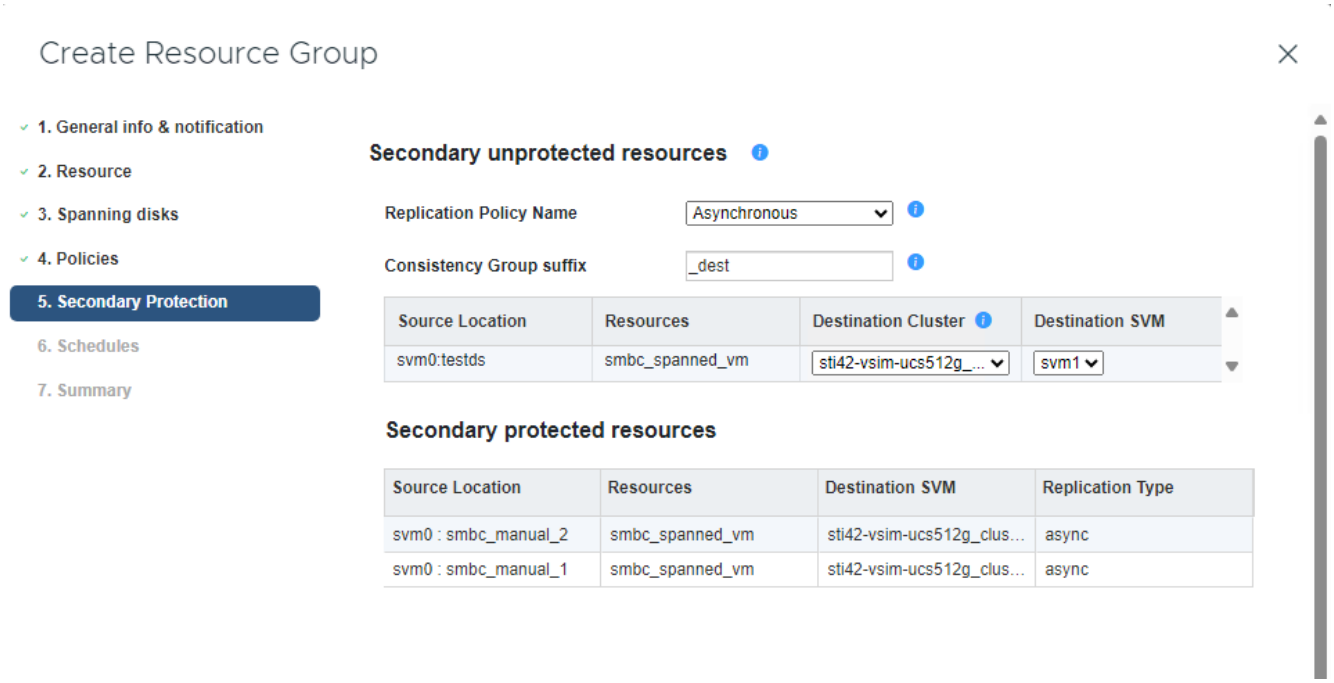
     Spanning-VMs werden für FlexGroup- und vVol-Datenspeicher nicht unterstützt.
5. Wählen oder erstellen Sie auf der Seite **Richtlinien** eine oder mehrere Backup-Richtlinien, wie in der folgenden Tabelle dargestellt:

Um… zu verwenden	Do this…
Eine vorhandene Richtlinie	Wählen Sie eine oder mehrere Richtlinien aus der Liste aus. Der sekundäre Schutz gilt für vorhandene und neue Richtlinien, bei denen Sie sowohl SnapMirror als auch SnapVault Updates ausgewählt haben.
Eine neue Richtlinie	a. Wählen Sie **Erstellen**. b. Schließen Sie den Assistenten für neue Backup-Richtlinien ab, um zum Assistenten „Ressourcengruppe erstellen“ zurückzukehren.

Im verknüpften Modus enthält die Liste Richtlinien in allen verknüpften vCenters. Sie müssen eine Richtlinie auswählen, die sich im selben vCenter befindet wie die Ressourcengruppe.

6. Auf der Seite **Sekundärer Schutz** sehen Sie die ausgewählten Ressourcen zusammen mit ihrem aktuellen Schutzstatus. Um den Schutz für alle ungeschützten Ressourcen zu aktivieren, wählen Sie den Replikationsrichtlinientyp, geben Sie ein Konsistenzgruppensuffix ein und wählen Sie den Zielcluster und die Ziel-SVM aus den Dropdown-Menüs aus. Wenn die Ressourcengruppe erstellt wird, startet SCV einen separaten Job für den sekundären Schutz. Sie können diesen Job im Job-Monitor-Fenster überwachen.

Felder	Beschreibung
Name der Replikationsrichtlinie	Name der SnapMirror-Richtlinie Es werden nur die sekundären Richtlinien **Asynchronous** und **Mirror und Vault** unterstützt.
Suffix für Konsistenzgruppen	Geben Sie beim Erstellen der Zielkonsistenzgruppe ein Suffix ein, das an den Namen der primären Konsistenzgruppe angehängt werden soll. Wenn der Name der primären Konsistenzgruppe beispielsweise `sccg_2024-11-28_120918` und du gehst hinein `_dest` als Suffix wird die sekundäre Konsistenzgruppe benannt `sccg_2024-11-28_120918_dest` . Dieses Suffix wird nur für ungeschützte Konsistenzgruppen verwendet.
Ziel-Cluster	Für alle ungeschützten Speichereinheiten zeigt SCV die Namen der Peering-Cluster im Dropdown-Menü an. Wenn der Speicher mit SVM-Bereich zu SCV hinzugefügt wird, wird aufgrund von ONTAP Einschränkungen die Cluster-ID anstelle des Clusternamens angezeigt.
Ziel-SVM	Für alle ungeschützten Speichereinheiten zeigt SCV die Namen der per Peering verbundenen SVMs an. Wenn Sie eine Speichereinheit auswählen, die Teil einer Konsistenzgruppe ist, werden der entsprechende Cluster und die SVM automatisch für alle anderen Speichereinheiten in dieser Konsistenzgruppe ausgewählt.
Sekundäre geschützte Ressourcen	Für alle geschützten Storage-Einheiten der Ressourcen, die auf der Seite Ressourcen hinzugefügt werden, werden die Details der sekundären Beziehung angezeigt, einschließlich Cluster, SVM und Replizierungstyp.



7. Richten Sie auf der Seite **Zeitpläne** den Sicherungszeitplan für jede ausgewählte Richtlinie ein.

   Geben Sie im Feld Startzeit ein Datum und eine andere Zeit als null ein. Das Datum muss das Format haben `day/month/year`.

   Wenn Sie im Feld **Alle** einen Wert auswählen (z. B. **Alle 2 Tage**), werden die Sicherungen am ersten Tag des Monats ausgeführt und dann für den Rest des Monats im angegebenen Intervall (Tag 1, 3, 5, 7 usw.) wiederholt, unabhängig davon, ob das Startdatum gerade oder ungerade ist.

   Alle Felder sind Pflichtfelder. Das SnapCenter Plug-in for VMware vSphere erstellt Sicherungspläne basierend auf der Zeitzone, in der es bereitgestellt wird. Um die Zeitzone zu ändern, verwenden Sie die Benutzeroberfläche des SnapCenter Plug-in for VMware vSphere .

   "Ändern der Zeitzonen für Backups".

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig stellen**. Ab SCV 6.1 sind sekundäre Schutzfunktionen für ASA r2-Systeme auf der Übersichtsseite sichtbar.

   Bevor Sie **Fertig stellen** auswählen, können Sie zu einer beliebigen Seite des Assistenten zurückkehren und die Informationen ändern.

   Nachdem Sie **Fertig stellen** ausgewählt haben, wird die neue Ressourcengruppe zur Liste der Ressourcengruppen hinzugefügt.

   Wenn der Stilllegungsvorgang für eine der VMs im Backup fehlschlägt, markiert SCV das Backup als nicht VM-konsistent, auch wenn Sie eine Richtlinie mit VM-Konsistenz ausgewählt haben. In diesem Fall ist es möglich, dass einige der VMs erfolgreich stillgelegt wurden.

Managen Sie Fehler bei der Kompatibilitätsprüfung

SnapCenter führt Kompatibilitätsprüfungen durch, wenn Sie versuchen, eine Ressourcengruppe zu erstellen. Beziehen Sie sich immer auf "NetApp Interoperabilitäts-Matrix-Tool (IMT)" für die neuesten Informationen zum

SnapCenter Support. Gründe für Inkompatibilität können sein:

- Ein gemeinsam genutztes PCI-Gerät ist mit einer VM verbunden.
- Die bevorzugte IP-Adresse ist in SnapCenter nicht konfiguriert.
- Sie haben SnapCenter keine Management-IP-Adresse für die Storage VM (SVM) hinzugefügt.
- Die Storage-VM ist ausgefallen.

Um einen Kompatibilitätsfehler zu beheben, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die Storage-VM ausgeführt wird.
2. Stellen Sie sicher, dass das Speichersystem, auf dem sich die VMs befinden, zum SnapCenter-Plug-in für den VMware vSphere-Bestand hinzugefügt wurde.
3. Stellen Sie sicher, dass die Speicher-VM zu SnapCenter hinzugefügt wird. Verwenden Sie die Option „Speichersystem hinzufügen“ auf der Benutzeroberfläche des VMware vSphere-Clients.
4. Wenn VMs über VMDKs sowohl auf NetApp als auch auf Datastores anderer Anbieter verfügen, verschieben Sie die VMDKs zu NetApp Datastores.

Vorschriften und Postskripte

Im Rahmen Ihrer Datensicherungsabläufe können Sie benutzerdefinierte Prescripts und Postskripte verwenden. Diese Skripte ermöglichen die Automatisierung entweder vor oder nach Ihrem Datensicherungsauftrag. Sie können z. B. ein Skript einschließen, das Sie automatisch über Fehler oder Warnungen bei Datenschutzaufstellungsfehlern benachrichtigt. Bevor Sie Ihre Prescripts und Postscripts einrichten, sollten Sie einige der Anforderungen zur Erstellung dieser Skripte kennen.

Unterstützte Skripttypen

Perl- und Shell-Skripte werden unterstützt. Shell-Skripte müssen mit beginnen `!/bin/bash`. (`!/bin/sh` Wird nicht unterstützt.)

Speicherort des Skriptpfads

Prescripts und Postscripts werden vom SnapCenter Plug-in für VMware vSphere ausgeführt. Daher müssen die Skripte im SnapCenter Plug-in für VMware vSphere OVA mit ausführbaren Berechtigungen zu finden sein.

Beispiel:

- Ein PERL-Skriptpfad könnte sein `/support/support/script.pl`
- Ein Shell-Skriptpfad könnte sein `/support/support/script.sh`

Der Skriptpfad wird zum Zeitpunkt der Ausführung des Skripts validiert.

Angeben von Skripten

Skripte werden in den Backup-Richtlinien angegeben. Wenn ein Sicherungsauftrag gestartet wird, ordnet die Richtlinie das Skript automatisch den gesicherten Ressourcen zu.

Um mehrere Skripte festzulegen, drücken Sie nach jedem Skriptpfad **Enter**, um jedes Skript in einer eigenen

Zeile aufzulisten. Semikolons (;) sind nicht zulässig. Sie können mehrere Vorschriften und mehrere Postskripte angeben. Ein einziges Skript kann sowohl als Vorskript als auch als Postscript codiert werden und kann andere Skripte aufrufen.

Wenn Skripte ausgeführt werden

Skripte werden gemäß dem für BACKUP_PHASE eingestellten Wert ausgeführt.

- BACKUP_PHASE=PRE_BACKUP

  In DER PHASE PRE_BACKUP des Vorgangs werden Prescripts ausgeführt.

> Wenn ein Prescript fehlschlägt, wird die Sicherung erfolgreich abgeschlossen und eine Warnmeldung gesendet.

- BACKUP_PHASE=POST_BACKUP ODER BACKUP_PHASE=FAILED_BACKUP

  Postscripts werden in DER PHASE POST_BACKUP des Vorgangs ausgeführt, nachdem das Backup erfolgreich abgeschlossen wurde, oder in DER PHASE FAILED_BACKUP, wenn das Backup nicht erfolgreich abgeschlossen wurde.

> Wenn ein Postscript fehlschlägt, wird das Backup erfolgreich abgeschlossen und eine Warnmeldung gesendet.

Überprüfen Sie Folgendes, um sicherzustellen, dass die Skriptwerte ausgefüllt sind:

- Für PERL-Skripte: `/support/support/log_env.log`
- Für Shell-Skripte: `/support/support/log_file.log`

Umgebungsvariablen an Skripte übergeben

Sie können die in der folgenden Tabelle aufgeführten Umgebungsvariablen in Skripten verwenden.

Umgebungsvariable	Beschreibung
`BACKUP_NAME`	Name des Backups. Variable nur in Postskripten übergeben.
`BACKUP_DATE`	Datum des Backups, im Format `yyyymmdd`Variable nur in Postskripten übergeben.
`BACKUP_TIME`	Zeit des Backups, im Format `hhmmss`Variable nur in Postskripten übergeben.
`BACKUP_PHASE`	Die Phase des Backups, in der das Skript ausgeführt werden soll. Gültige Werte sind: `PRE_BACKUP, POST_BACKUP, and FAILED_BACKUP`. Variable in Vorschriften und Postskripten übergeben.
`STORAGE_SNAPSHOTS`	Die Anzahl der Speicher-Snapshots im Backup. Variable nur in Postskripten übergeben.

Umgebungsvariable	Beschreibung
`STORAGE_SNAPSHOT.#`	Einer der definierten Speicher-Snapshots im folgenden Format: `<filer>:/vol/<volume>:<ONTAP-snapshot-name>`Variable nur in Postskripten übergeben.
`VIRTUAL_MACHINES`	Die Anzahl der VMs im Backup. Variable in Vorschriften und Postskripten übergeben.
`VIRTUAL_MACHINE.#`	Eine der definierten virtuellen Maschinen im folgenden Format: `<VM name>[vertical bar]<VM UUID>[vertical bar]<power-state>[vertical bar]<VM snapshot>[vertical bar]<ip-addresses>` `<power-state> has the values POWERED_ON, POWERED_OFF, or SUSPENDED` `<VM snapshot>` Verfügt über die Werte `true` Oder `false`Variable in Vorschriften und Postskripten übergeben.

Skript-Timeouts

Das Timeout für Backup-Skripts beträgt 15 Minuten und kann nicht geändert werden.

Beispiel FÜR PERL-Skript #1

Das folgende Beispiel PERL-Skript druckt die Umgebungsvariablen, wenn ein Backup ausgeführt wird.

```
#!/usr/bin/perl
use warnings;
use strict;
my $argnum;
my $logfile = '/support/support/log_env.log';
open (FH, '>>', $logfile) or die $!;
foreach (sort keys %ENV) {
print FH "$_ = $ENV{$_}\n";
}
print FH "=========\n";
close (FH);
```

Beispiel FÜR PERL-Skript #2

Im folgenden Beispiel werden Informationen zum Backup gedruckt.

```
#!/usr/bin/perl
use warnings;
use strict;

my $argnum;
my $logfile = '/support/support/log_env.log';
```

```
open (FH, '>>', $logfile) or die $!;

print FH "BACKUP_PHASE is $ENV{'BACKUP_PHASE'}\n";
print FH "Backup name $ENV{'BACKUP_NAME'}\n";
print FH "Virtual Machine $ENV{'VIRTUAL_MACHINES'}\n";
print FH "VIRTUAL_MACHINE # is $ENV{'VIRTUAL_MACHINE.1'}\n";
print FH "BACKUP_DATE is $ENV{'BACKUP_DATE'}\n";
print FH "BACKUP_TIME is $ENV{'BACKUP_TIME'}\n";
print FH "STORAGE_SNAPSHOTS is $ENV{'STORAGE_SNAPSHOTS'}\n";
print FH "STORAGE_SNAPSHOT # is $ENV{'STORAGE_SNAPSHOT.1'}\n";

print FH "PWD is $ENV{'PWD'}\n";
print FH "INVOCATION_ID is $ENV{'INVOCATION_ID'}\n";

print FH "=========\n";
close (FH);
```

Beispiel für Shell-Skript

```
============================================
#!/bin/bash
echo Stage $BACKUP_NAME >> /support/support/log_file.log
env >> /support/support/log_file.log
============================================
```

Fügen Sie eine einzelne VM oder einen Datenspeicher zu einer Ressourcengruppe hinzu

Sie können schnell eine einzelne VM oder einen Datastore zu einer beliebigen vorhandenen Ressourcengruppe hinzufügen, die über das SnapCenter Plug-in für VMware vSphere gemanagt wird.

Über diese Aufgabe

Fügen Sie SAN- und NAS-Datastores hinzu, aber nicht VSAN oder VVOL Datastores.

Schritte

1. Wählen Sie in der Benutzeroberfläche des vSphere-Clients in der Symbolleiste **Menü** aus und navigieren Sie zu der VM oder dem Datenspeicher, den Sie hinzufügen möchten.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf die VM oder den Datastore, und wählen Sie in der sekundären Dropdown-Liste **SnapCenter-Plug-in für VMware vSphere** > **zu Ressourcengruppe hinzufügen** aus.

   Das System überprüft zunächst, ob SnapCenter verwaltet und mit dem Speichersystem kompatibel ist, auf dem sich die ausgewählte VM befindet, und zeigt dann die Seite **zur Ressourcengruppe hinzufügen** an. Wenn die Meldung angezeigt wird `SnapCenter Compatibility Error` Wird angezeigt, dann ist die ausgewählte VM nicht mit SnapCenter kompatibel und Sie müssen zuerst die entsprechende Storage-VM zu SnapCenter hinzufügen.

3. Wählen Sie auf der Seite **zu Ressourcengruppe hinzufügen** eine Ressourcengruppe aus, und wählen Sie dann **OK** aus.

Wenn Sie **OK** auswählen, prüft das System zunächst, ob SnapCenter den Speicher verwaltet und kompatibel ist, auf dem sich die ausgewählten VMs oder Datastores befinden.

Wenn die Meldung `Selected <resource-name> is not SnapCenter compatible` angezeigt wird, ist eine ausgewählte VM oder ein ausgewählter Datastore nicht mit SnapCenter kompatibel. Weitere Informationen finden Sie unter "Managen Sie Fehler bei der Kompatibilitätsprüfung" .

Fügen Sie mehrere VMs und Datenspeicher einer Ressourcengruppe hinzu

Mit dem Assistenten zum Bearbeiten von Ressourcengruppen für SnapCenter vSphere-Clients können Sie einer vorhandenen Ressourcengruppe mehrere Ressourcen hinzufügen.

Eine Ressourcengruppe kann eine der folgenden Elemente enthalten:

- Beliebige Kombination aus herkömmlichen VMs sowie SAN- und NAS-Datenspeichern (vVol Datastores werden nicht unterstützt)
- Ein FlexGroup Datastore (Spanning VMs werden nicht unterstützt).
- Ein oder mehrere FlexVol Datastores (Spanning VMs werden unterstützt).
- Ein oder mehrere vVol VMs.
- Alle vVol VMs mit einem angegebenen vSphere Tag.
- Alle vVol VMs in einem angegebenen Ordner.

VVol VMs, die mehrere vVol Datastores umfassen, werden nicht unterstützt, da SnapCenter nur VVols im primären, ausgewählten vVol Datastore sichert.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Ressourcengruppen** aus, wählen Sie dann eine Ressourcengruppe aus und wählen Sie dann **Ressourcengruppe bearbeiten** aus, um den Assistenten zu starten.
2. Gehen Sie auf der Seite **Ressource** wie folgt vor:
   a. Navigieren Sie im Feld Datastores zu den VMs oder Datastores, die Sie hinzufügen möchten.
   b. Wählen Sie in der Liste Verfügbare Entitäten eine oder mehrere VMs oder Datastores aus, die Sie der Ressourcengruppe hinzufügen möchten, und wählen Sie dann **>** aus, um Ihre Auswahl in die Liste Ausgewählte Entitäten zu verschieben. Wählen Sie **>>**, um alle verfügbaren Entitäten zu verschieben.

      Standardmäßig wird das Datacenter-Objekt in der Liste Verfügbare Entitäten angezeigt. Sie können einen Datenspeicher auswählen, um die VMs im Datastore anzuzeigen und dieser Ressourcengruppe hinzuzufügen.

   Wenn Sie **Weiter** auswählen, prüft das System zunächst, ob SnapCenter den Speicher verwaltet und kompatibel ist, auf dem sich die ausgewählten VMs oder Datastores befinden. Wenn die Meldung `Some entities are not SnapCenter compatible` angezeigt wird, ist eine ausgewählte VM oder ein ausgewählter Datastore nicht mit SnapCenter kompatibel. Weitere Informationen finden Sie unter "Managen Sie Fehler bei der Kompatibilitätsprüfung" .

3. Wiederholen Sie Schritt 2 für jede VM oder jeden Datenspeicher, den Sie hinzufügen möchten.
4. Wählen Sie **Weiter**, bis Sie die Seite **Zusammenfassung** erreichen, überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**.

Backup des umbenannten Speichers wiederherstellen

Wenn der Speicher umbenannt wird, fehlschlagen Workflows, die vor der Umbenennung mithilfe von Backups durchgeführt wurden. Mit der Einführung der Funktion zum Umbenennen von Backups, auf die ausschließlich über die REST-API zugegriffen werden kann, ist es nun möglich, die Backups zu verwenden, die vor der Umbenennung des Speichers erstellt wurden. Im Folgenden werden der Workflow und die Verwendung der REST-API beschrieben.

Das ASA r2-Speichersystem unterstützt die Funktion „Letzte Snapshot-Benennung“ nicht.

Schritte

1. Fügen Sie die neue Speicherverbindung hinzu oder aktualisieren Sie sie, um sicherzustellen, dass der neue Cluster- oder SVM-Name in SCV angezeigt wird.
2. Starten Sie den Service neu, um die Caches zu aktualisieren, wie im KB-Artikel beschrieben: "SCV-Backups schlagen nach dem Umbenennen der SVM fehl"
3. Erstellen Sie ein neues Backup.
4. Verwenden Sie die Sicherungsdetails, um die alten und neuen Speichernamen zu finden.
5. Wählen Sie im Fenster **Backups** des vSphere-Clients das Backup aus, um die Details anzuzeigen.
6. Greifen Sie über die URL auf Swagger zu: `https://<SCV-IP>:8144/api/swagger-ui/index.html`

   Verwenden Sie die folgende API, um den Speicher umzubenennen:

   PATCH
   /4.1/Storage-System

   Beispiel:
   {
   „ExistingSVM“: {
   „Name“: „String“
   },
   „NewSVM“: {
   „Name“: „String“
   }
   }

   Antwort:

   {
   „Statusmeldung“: „OK“,
   „Statuscode“: 200,
   "ResponseMessage": [
   „Speichersystem erfolgreich umbenannt.“
   ]
   }

Nachdem Sie diese API ausgeführt haben, können Sie alle Workflows ausführen, einschließlich des Wiederherstellungsvorgangs aus dem alten Backup.

Bei Bedarf das Sichern von Ressourcengruppen sichern

Backup-Vorgänge werden für alle in einer Ressourcengruppe definierten Ressourcen durchgeführt. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

ASA r2 Backup erstellt Snapshots von Konsistenzgruppen und stellt eine primäre Konsistenzgruppe bereit, wenn die angegebene Ressource sie nicht bereits hat.

Bevor Sie beginnen

Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

Starten Sie keinen On-Demand-Backup-Job, wenn bereits ein Job zum Sichern der SnapCenter-Plug-in für VMware vSphere MySQL-Datenbank ausgeführt wird. Verwenden Sie die Wartungskonsole, um den konfigurierten Backup-Zeitplan für die MySQL-Datenbank anzuzeigen.

Über diese Aufgabe

In früheren Versionen der Virtual Storage Console (VSC) können Sie ein On-Demand-Backup durchführen, ohne einen Backup-Job für eine VM oder einen Datastore konfigurieren zu müssen. Für das SnapCenter-Plug-in für VMware vSphere müssen sich VMs und Datastores jedoch in einer Ressourcengruppe befinden, bevor Sie Backups durchführen können.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Ressourcengruppen** aus, wählen Sie dann eine Ressourcengruppe aus und wählen Sie dann **Jetzt ausführen** aus, um das Backup zu starten.
2. Wenn die Ressourcengruppe mehrere Richtlinien konfiguriert hat, wählen Sie im Dialogfeld **Jetzt sichern** die Richtlinie aus, die Sie für diesen Sicherungsvorgang verwenden möchten.
3. Wählen Sie **OK**, um die Sicherung zu starten.
4. Optional: Überwachen Sie den Vorgangsfortschritt, indem Sie im unteren Bereich des Fensters **Letzte Aufgaben** oder im Dashboard **Job Monitor** für weitere Details auswählen. .Result

Wenn der Quiesce-Vorgang für eine der VMs im Backup fehlschlägt, dann wird der Backup mit einer Warnung abgeschlossen und als nicht VM konsistent markiert, auch wenn für die ausgewählte Richtlinie die VM-Konsistenz ausgewählt ist. In diesem Fall ist es möglich, dass einige der VMs erfolgreich stillgelegt wurden. In der Job-Überwachung zeigt die Detailbeschreibung für fehlgeschlagene VM das Quiesce als fehlgeschlagen an.

Sichern Sie das SnapCenter Plug-in für VMware vSphere MySQL Datenbank

Das SnapCenter Plug-in für VMware vSphere umfasst eine MySQL Datenbank (auch NSM-Datenbank genannt), die Metadaten für alle vom Plug-in ausgeführten Jobs enthält. Sie sollten dieses Repository regelmäßig sichern.

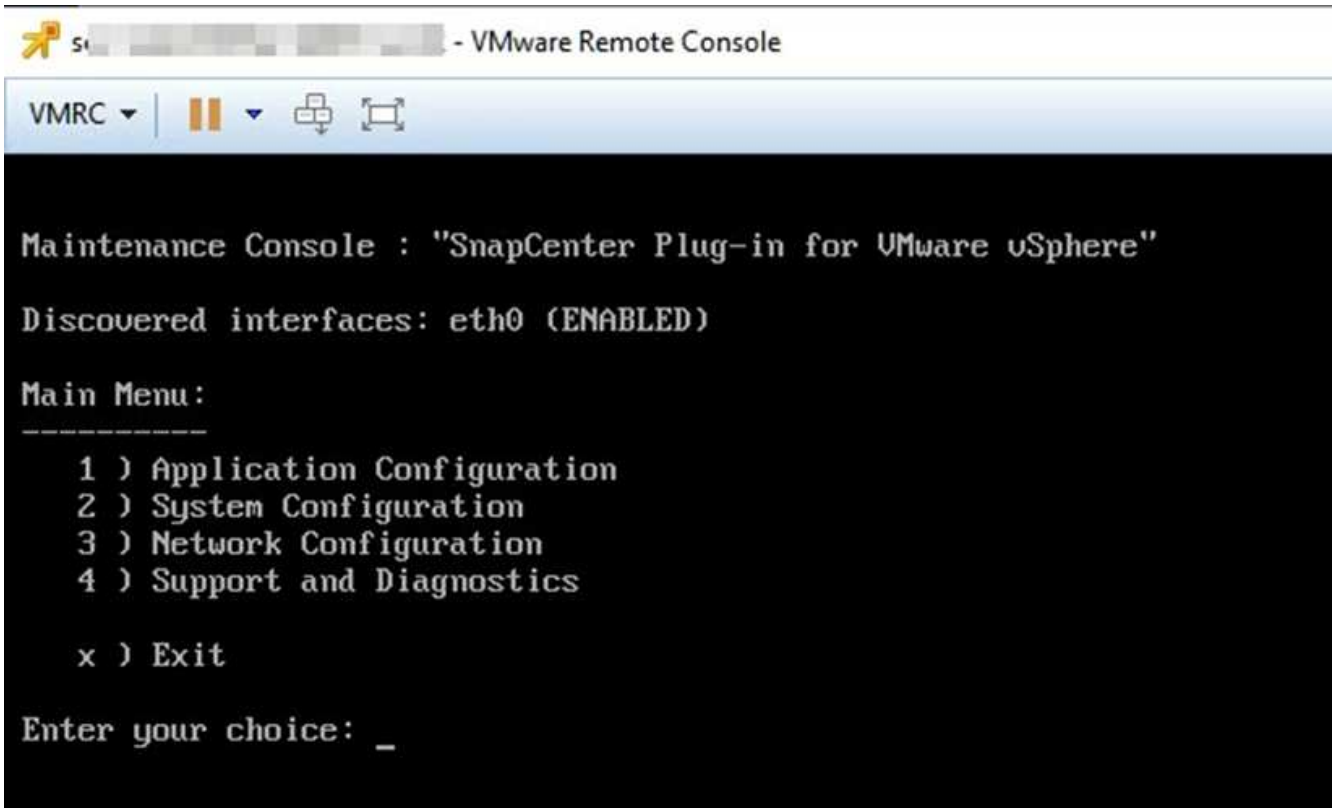
Sie sollten zudem ein Backup des Repositorys vor Migrationen oder Upgrades durchführen.

Bevor Sie beginnen

Starten Sie keinen Job zum Backup der MySQL Datenbank, wenn bereits ein On-Demand-Backup ausgeführt wird.

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter-Plug-in für VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remote Console starten oder Web Console starten** aus, um ein Fenster der Wartungskonsole zu öffnen.



3. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration ein.**
4. Geben Sie im Menü Anwendungskonfiguration die Option **6) MySQL-Sicherung und -Wiederherstellung ein.**
5. Geben Sie im Menü MySQL Backup and Restore Configuration die Option **1) MySQL Backup konfigurieren** ein.
6. Geben Sie an der Eingabeaufforderung den Backup-Speicherort für das Repository ein, die Anzahl der zu bewahrenden Backups und die Zeit, zu der das Backup gestartet werden soll.

   Alle Eingaben werden gespeichert, wenn Sie sie eingeben. Wenn die Nummer der Backup-Aufbewahrung erreicht ist, werden ältere Backups gelöscht, wenn neue Backups durchgeführt werden.

   Repository-Backups werden mit dem Namen „Backup-<date>“ benannt. Da die Repository-Wiederherstellungsfunktion nach dem Präfix „Backup“ sucht, sollten Sie es nicht ändern.

Verwalten von Ressourcengruppen

Sie können Backup-Ressourcengruppen erstellen, ändern und löschen und Backup-Vorgänge für Ressourcengruppen durchführen.

Ressourcengruppen werden als Backup-Jobs in der Virtual Storage Console (VSC) bezeichnet.

Unterbrechen und Fortsetzen des Betriebs von Ressourcengruppen

Unterbrechen Sie geplante Vorgänge für eine Ressourcengruppe. Aktivieren Sie sie bei Bedarf erneut.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Ressourcengruppen**, wählen Sie eine Ressourcengruppe aus und wählen Sie **Unterbrechen** (oder wählen Sie **Fortsetzen**) aus.
2. Wählen Sie im Bestätigungsfeld zur Bestätigung **OK** aus.

Nachdem Sie fertig sind

Auf der Seite Ressourcengruppen lautet der Job-Status für die gesperrte Ressource `Under_Maintenance`. Möglicherweise müssen Sie nach rechts in der Tabelle blättern, um die Spalte Job Status anzuzeigen.

Nachdem die Sicherungsvorgänge wieder aufgenommen wurden, ändert sich der Job-Status in `Production`.

Ressourcengruppen ändern

Ressourcen in Ressourcengruppen in vCenter können entfernt oder hinzugefügt, Richtlinien abgetrennt oder zugewiesen, Zeitpläne geändert oder andere Optionen für Ressourcengruppen geändert werden.

Über diese Aufgabe

Wenn Sie den Namen einer Ressourcengruppe ändern möchten, verwenden Sie die folgenden Sonderzeichen nicht in VM-, Datastore-, Richtlinien-, Backup- oder Ressourcengruppennamen:

% & * # @ ! \ / : * ? " < > - | ; ' und Leerzeichen. Ein Unterstrich (_) ist zulässig.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und wählen Sie **Bearbeiten** aus.
2. Wählen Sie in der linken Liste im Assistenten **Ressourcengruppe bearbeiten** die Kategorie aus, die Sie ändern möchten, und geben Sie Ihre Änderungen ein.

   Sie können Änderungen in mehreren Kategorien vornehmen. Mit dieser Option können Sie auch sekundäre geschützte Ressourcen bearbeiten.

3. Wählen Sie **Weiter**, bis die Übersichtsseite angezeigt wird, und wählen Sie dann **Fertig stellen**.

Löschen von Ressourcengruppen

Löschen Sie eine Ressourcengruppe in vCenter, wenn Sie die Ressourcen nicht schützen müssen. Löschen Sie alle Ressourcengruppen, bevor Sie das SnapCenter Plug-in for VMware vSphere entfernen.

Über diese Aufgabe

Alle Löschvorgänge für Ressourcengruppen werden als erzwungene Löschungen ausgeführt. Wenn Sie eine Ressourcengruppe löschen, trennt das System alle Richtlinien von der vCenter-Ressourcengruppe, entfernt die Ressourcengruppe aus dem SnapCenter Plug-in for VMware vSphere und löscht alle Sicherungen und Snapshots der Ressourcengruppe.

> In einer SnapVault -Beziehung können Sie den letzten Snapshot nicht löschen und daher auch nicht die Ressourcengruppe. Bevor Sie eine Ressourcengruppe in einer SnapVault -Beziehung löschen, entfernen Sie die Beziehung mit System Manager oder ONTAP CLI und löschen Sie dann den letzten Snapshot.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und wählen Sie **Löschen** aus.
2. Wählen Sie im Bestätigungsdialogfeld **Ressourcengruppe löschen** zur Bestätigung **OK** aus. Durch das Löschen einer Ressourcengruppe wird der sekundäre Schutz nicht entfernt. Verwenden Sie bei Bedarf den System Manager, um den sekundären Schutz zu löschen. Für die Ressourcengruppe erstellte Konsistenzgruppen werden nicht automatisch entfernt. Sie müssen sie manuell mithilfe von System Manager oder einer anderen unterstützten Schnittstelle aus ONTAP löschen.

Management von Richtlinien

Backup-Richtlinien für das SnapCenter Plug-in für VMware vSphere lassen sich erstellen, ändern, anzeigen, trennen und löschen. Zur Durchführung von Datensicherungsvorgängen sind Richtlinien erforderlich.

Richtlinien trennen

Sie können Richtlinien aus einer SnapCenter Plug-in für VMware vSphere Ressourcengruppe entfernen, wenn diese Richtlinien die Datensicherung für die Ressourcen nicht mehr regeln sollen. Sie müssen eine Richtlinie trennen, bevor Sie sie entfernen können oder bevor Sie die Zeitplanfrequenz ändern.

Über diese Aufgabe

Die Richtlinien zum Trennen von Richtlinien aus den Ressourcengruppen des SnapCenter Plug-in für VMware vSphere unterscheiden sich von den Richtlinien für SnapCenter-Ressourcengruppen. Bei einer VMware vSphere-Client-Ressourcengruppe können alle Richtlinien getrennt werden, sodass die Ressourcengruppe keine Richtlinie bleibt. Um jedoch Datensicherungsvorgänge an dieser Ressourcengruppe durchzuführen, müssen Sie mindestens eine Richtlinie anhängen.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und wählen Sie **Bearbeiten** aus.
2. Deaktivieren Sie auf der Seite **Richtlinien** des Assistenten * Ressourcengruppe bearbeiten* das Häkchen neben den Richtlinien, die Sie entfernen möchten.

   Sie können der Ressourcengruppe auch eine Richtlinie hinzufügen, indem Sie die Richtlinie prüfen.

3. Nehmen Sie im Rest des Assistenten weitere Änderungen an der Ressourcengruppe vor, und wählen Sie dann **Fertig stellen**.

Richtlinien ändern

Sie können Richtlinien für ein SnapCenter Plug-in für eine VMware vSphere Ressourcengruppe ändern. Sie können die Häufigkeit, die Replikationsoptionen, die Einstellungen für die Snapshot-Aufbewahrung oder die Skriptinformationen ändern, während eine Richtlinie an eine Ressourcengruppe angehängt ist.

Über diese Aufgabe

Durch das Ändern von SnapCenter Plug-in für VMware vSphere-Backup-Richtlinien unterscheiden sich die Backup-Richtlinien für applikationsbasierte SnapCenter Plug-ins nicht. Wenn Sie die Plug-in-Richtlinien ändern, müssen Sie keine Richtlinien von Ressourcengruppen trennen.

Bevor Sie die Replizierungs- oder Aufbewahrungseinstellungen ändern, sollten Sie die möglichen Folgen berücksichtigen.

- Erhöhen der Replizierungs- oder Aufbewahrungseinstellungen

  Backups sammeln sich weiter an, bis sie die neue Einstellung erreichen.

- Verringerung der Replizierungs- oder Aufbewahrungseinstellungen

  Backups, die über die neue Einstellung hinausgehen, werden bei der Durchführung des nächsten Backups gelöscht.

Zum Ändern eines SnapCenter-Plug-ins für VMware vSphere-Richtlinienplans müssen Sie den Zeitplan in der Plug-in-Ressourcengruppe ändern.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Richtlinien**, wählen Sie dann eine Richtlinie aus und wählen Sie **Bearbeiten** aus.
2. Ändern Sie die Richtlinienfelder.
3. Wenn Sie fertig sind, wählen Sie **Update**.

Die Änderungen werden wirksam, wenn das nächste geplante Backup durchgeführt wird.

Richtlinien löschen

Wenn Sie keine konfigurierte Backup-Richtlinie mehr für das SnapCenter Plug-in für VMware vSphere benötigen, möchten Sie sie möglicherweise löschen.

Bevor Sie beginnen

Sie müssen die Richtlinie von allen Ressourcengruppen in der virtuellen Appliance für SnapCenter getrennt haben, bevor Sie sie löschen können.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-ins **Richtlinien**, wählen Sie dann eine Richtlinie aus und wählen Sie **Entfernen** aus.
2. Wählen Sie im Bestätigungsdialogfeld **OK**.

Backup-Management

Sie können Backups umbenennen und löschen, die vom SnapCenter Plug-in für VMware vSphere durchgeführt wurden. Sie können auch mehrere Backups gleichzeitig löschen.

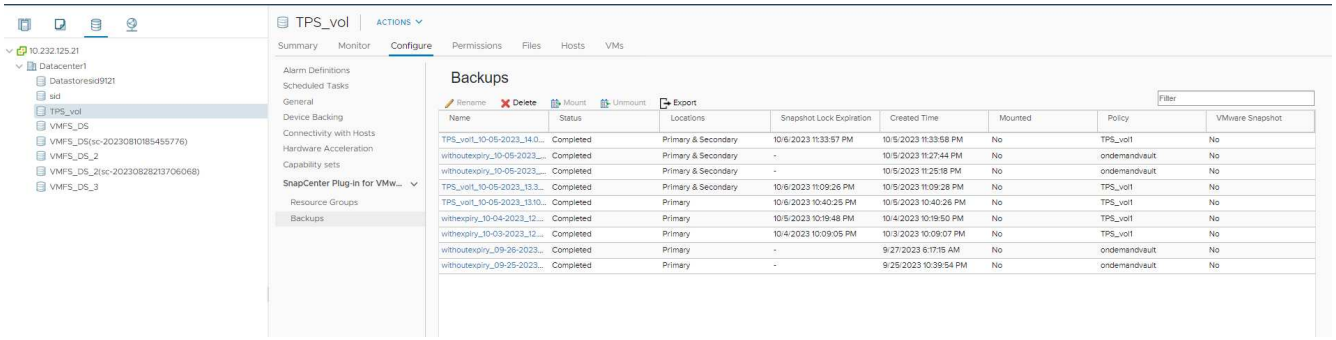
Backups umbenennen

Sie können das SnapCenter Plug-in für VMware vSphere Backups umbenennen, wenn Sie einen besseren Namen geben möchten, um die Suchbarkeit zu verbessern.

Das ASA r2-Speichersystem unterstützt das Umbenennen von Backups nicht.

Schritte

1. Wählen Sie **Menü** und wählen Sie die Menüoption **Hosts und Cluster** aus, wählen Sie dann eine VM aus, wählen Sie dann die Registerkarte **Konfigurieren** aus und wählen Sie dann **Backups** im Abschnitt **SnapCenter Plug-in für VMware vSphere** aus.



2. Wählen Sie auf der Registerkarte Konfigurieren ein Backup aus, und wählen Sie **Umbenennen** aus.
3. Geben Sie im Dialogfeld **Backup umbenennen** den neuen Namen ein und wählen Sie **OK**.

   Verwenden Sie die folgenden Sonderzeichen nicht in VM-, Datastore-, Richtlinien-, Backup- oder Ressourcengruppennamen: & * € # @ ! \ / : * ? " < > - | ; ' und Leerzeichen. Ein Unterstrich (_) ist zulässig.

Backups löschen

Das SnapCenter Plug-in für VMware vSphere Backups kann gelöscht werden, wenn das Backup für andere Datensicherungsvorgänge nicht mehr benötigt wird. Sie können ein Backup löschen oder mehrere Backups gleichzeitig löschen.

Bevor Sie beginnen

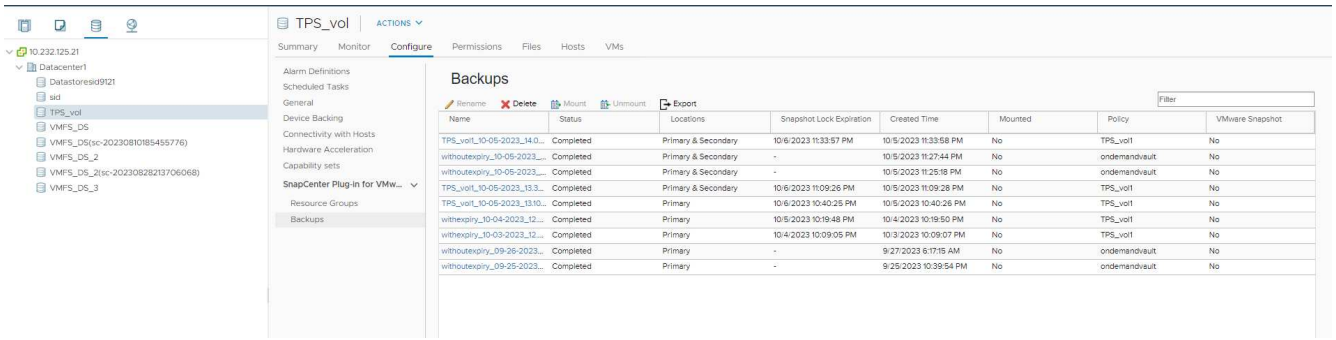
Sie können keine Backups löschen, die angehängt sind. Sie müssen die Bereitstellung einer Sicherung aufheben, bevor Sie sie löschen können.

Über diese Aufgabe

Snapshots auf dem Sekundärspeicher werden über Ihre ONTAP Aufbewahrungseinstellungen gemanagt, nicht durch das SnapCenter Plug-in für VMware vSphere. Wenn Sie das SnapCenter-Plug-in für VMware vSphere zum Löschen eines Backups verwenden, werden Snapshots auf dem primären Speicher gelöscht, Snapshots auf dem sekundären Speicher jedoch nicht gelöscht. Wenn ein Snapshot noch auf dem sekundären Speicher vorhanden ist, behält das SnapCenter-Plug-in für VMware vSphere die mit dem Backup verbundenen Metadaten zur Unterstützung von Wiederherstellungsanforderungen bei. Wenn der ONTAP-

Aufbewahrungsvorgang den sekundären Snapshot löscht, löscht das SnapCenter-Plug-in für VMware vSphere die Metadaten mithilfe eines Löschauftrags, der in regelmäßigen Abständen ausgeführt wird.

1. Wählen Sie **Menü** und wählen Sie die Menüoption **Hosts und Cluster** aus, wählen Sie dann eine VM aus, wählen Sie dann die Registerkarte **Konfigurieren** aus und wählen Sie dann **Backups** im Abschnitt **SnapCenter Plug-in für VMware vSphere** aus.



2. Wählen Sie ein oder mehrere Backups aus und wählen Sie **Löschen**.

   Sie können maximal 40 Backups zum Löschen auswählen.

3. Wählen Sie **OK**, um den Löschvorgang zu bestätigen.
4. Aktualisieren Sie die Backup-Liste, indem Sie in der linken vSphere-Menüleiste das Aktualisierungssymbol auswählen.

Mounten und Unmounten von Datastores

Mounten Sie ein Backup

Sie können einen herkömmlichen Datenspeicher aus einem Backup einbinden, wenn Sie auf die Dateien im Backup zugreifen möchten. Sie können das Backup entweder auf demselben ESXi Host mounten, auf dem das Backup erstellt wurde, oder auf einem alternativen ESXi Host, der denselben Typ von VM- und Host-Konfigurationen hat. Sie können einen Datastore mehrmals auf einem Host mounten.

Sie können einen vVol Datastore nicht mounten.

Bevor Sie beginnen

- Stellen Sie sicher, dass sich der alternative ESXi Host mit dem Speicher verbinden kann

  Wenn Sie einen alternativen ESXi-Host mounten möchten, müssen Sie sicherstellen, dass der alternative ESXi-Host eine Verbindung zum Speicher herstellen kann und Folgendes hat:

  - Dieselbe UID und dieselbe GID wie beim ursprünglichen Host
  - Dieselbe virtuelle Appliance für das SnapCenter Plug-in für VMware vSphere-Version wie die des ursprünglichen Hosts
- Stellen Sie bei Verwendung des iSCSI-Protokolls sicher, dass die Initiatoren für das Speichersystem dem ESXi-Host zugeordnet sind. Wenn Sie das NVMe-Protokoll verwenden, fügen Sie Controller hinzu, um das erforderliche Subsystem dem ESXi-Host zuzuordnen.
- Bereinigen Sie veraltete LUN/Namespace

  Da der ESXi-Host nur eine eindeutige LUN/einen eindeutigen Namespace pro Datastore erkennen kann, schlägt der Vorgang fehl, wenn mehr als einer gefunden wird. Dies kann auftreten, wenn Sie einen Mount-Vorgang starten, bevor ein vorheriger Mount-Vorgang abgeschlossen ist, oder wenn Sie LUN/Namespace manuell klonen oder wenn Klone während eines Unmounting-Vorgangs nicht aus dem Speicher gelöscht werden. Um das Erkennen mehrerer Klone zu vermeiden, sollten Sie alle veralteten LUNs/Namespaces auf dem Storage bereinigen.

Über diese Aufgabe

Der Mount-Vorgang kann fehlschlagen, wenn die Storage-Tier der FabricPool, auf der sich der Datastore befindet, nicht verfügbar ist.

Schritte

1. Wählen Sie auf der Seite VMware vSphere Client Shortcuts **Storage** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Datastore, und wählen Sie **SnapCenter Plug-in für VMware vSphere** > **Mount Backup**.
3. Wählen Sie auf der Seite **Mount Datastore** ein Backup und einen Backup-Speicherort (primär oder sekundär) aus, und wählen Sie dann **Finish** aus.
4. Optional: Gehen Sie wie folgt vor, um zu überprüfen, ob der Datenspeicher angehängt ist:
   a. Wählen Sie in der Symbolleiste **Menü** aus, und wählen Sie dann **Speicher** aus der Dropdown-Liste aus.
   b. Im linken Navigationsbereich wird der Datastore angezeigt, den Sie oben in der Liste gemountet

haben.

Um zu verhindern, dass beim Klonen des Volumes neue Snapshots erstellt werden, deaktivieren Sie den ONTAP-Zeitplan für das SnapVault Volume. Zuvor vorhandene Snapshots werden nicht gelöscht.

Heben Sie die Bereitstellung eines Backups auf

Sie können die Bereitstellung eines Backups aufheben, wenn Sie nicht mehr auf die Dateien im Datastore zugreifen müssen.

Wenn ein Backup in der Benutzeroberfläche des VMware vSphere-Clients als gemountet aufgeführt ist, es aber nicht im Bildschirm zum Unmounten von Backups aufgeführt ist, müssen Sie die REST-API verwenden. `/backup/{backup-Id}/cleanup` um die Out-of-Bound-Datenspeicher zu bereinigen und dann den Unmount-Vorgang erneut zu versuchen.

Wenn Sie versuchen, eine Sicherungskopie eines NFS-Datenspeichers auf einer Speicher-VM (SVM) mit dem Stammvolume in einer Lastenteilungs-Spiegelbeziehung zu mounten, tritt möglicherweise der Fehler `You might have reached the maximum number of NFS volumes configured in the vCenter. Check the vSphere Client for any error messages.` Um dieses Problem zu vermeiden, ändern Sie die Einstellung für die maximalen Volumes, indem Sie zu **ESX** > **Verwalten** > **Einstellungen** > **Erweiterte Systemeinstellungen** navigieren und den Wert NFS.MaxVolumes ändern. Der Maximalwert ist 256.

Schritte

1. Wählen Sie auf der Seite VMware vSphere Client Shortcuts **Storage** aus.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf einen Datastore, wählen Sie dann **SnapCenter Plug-in für VMware vSphere** in der Dropdown-Liste aus, und wählen Sie dann **Unmount** in der sekundären Dropdown-Liste aus.

   Stellen Sie sicher, dass Sie den richtigen Datastore zum Aufheben der Bereitstellung auswählen. Andernfalls können Sie Auswirkungen auf die Produktionsarbeit haben.

3. Wählen Sie im Dialogfeld **Unmounten geklonter Datastore** einen Datastore aus, aktivieren Sie das Kontrollkästchen **Unmounten des geklonten Datastore** und wählen Sie dann **Unmounten** aus.

Restore von Backups

Restore-Übersicht

Sie können VMs, VMDKs, Dateien und Ordner von primären oder sekundären Backups wiederherstellen.

- VM-Wiederherstellungsziele

  Sie können herkömmliche VMs auf dem ursprünglichen Host, auf einem alternativen Host im selben vCenter Server oder auf einem alternativen ESXi Host wiederherstellen, der von demselben vCenter oder einem beliebigen vCenter im verknüpften Modus gemanagt wird.

  Sie können vVol VMs zum ursprünglichen Host wiederherstellen.

- VMDK-Wiederherstellungsziele

  Sie können VMDKs in herkömmlichen VMs entweder auf dem Original oder in einem alternativen Datastore wiederherstellen.

  Sie können VMDKs in vVol VMs auch im ursprünglichen Datastore wiederherstellen.

Sie können auch einzelne Dateien und Ordner in einer Gastdatei-Wiederherstellungssitzung wiederherstellen, die eine Sicherungskopie eines virtuellen Laufwerks anhängt und die ausgewählten Dateien oder Ordner wiederherstellt.

Sie können Folgendes nicht wiederherstellen:

- Datenspeicher

  Sie können das SnapCenter Plug-in für VMware vSphere nicht zur Wiederherstellung eines Datenspeichers verwenden, sondern nur für die einzelnen VMs im Datastore.

- Backups entfernter VMs

  Sie können keine Backups von entfernten Storage-VMs wiederherstellen. Wenn Sie beispielsweise eine Storage VM mithilfe der Management-LIF hinzufügen und dann ein Backup erstellen, entfernen Sie diese Storage VM und fügen einen Cluster hinzu, der die gleiche Storage VM enthält. Der Wiederherstellungsvorgang für das Backup schlägt fehl.

Durchführen von Restore-Vorgängen

Für VMFS Umgebungen verwendet das SnapCenter Plug-in für VMware vSphere Klon- und Mount-Vorgänge mit Storage VMotion, um Restore-Vorgänge durchzuführen. Für NFS-Umgebungen verwendet das Plug-in natives ONTAP Single File SnapRestore (SFSR), um die Effizienz für die meisten Wiederherstellungsvorgänge zu steigern. Für vVol VMs verwendet das Plug-in zur Wiederherstellung ONTAP Single File Snapshot Restore (ONTAP SFSR) und SnapMirror Restore. Die folgende Tabelle zeigt, wie Wiederherstellungsvorgänge durchgeführt werden.

Restore-Vorgänge	Von	Durchgeführt mit
VMs und VMDKs	Primäre Backups	NFS-Umgebungen: ONTAP Single File SnapRestore VMFS-Umgebungen: Klonen und Mounten mit Storage VMotion
VMs und VMDKs	Sekundäre Backups	NFS-Umgebungen: ONTAP Single File SnapRestore VMFS-Umgebungen: Klonen und Mounten mit Storage VMotion
Gelöschte VMs und VMDKs	Primäre Backups	NFS-Umgebungen: ONTAP Single File SnapRestore VMFS-Umgebungen: Klonen und Mounten mit Storage VMotion
Gelöschte VMs und VMDKs	Sekundäre Backups	NFS-Umgebungen: Klonen und Mounten mit Storage VMotion VMFS-Umgebungen: Klonen und Mounten mit Storage VMotion
VMs und VMDKs	VM-konsistente primäre Backups	NFS-Umgebungen: ONTAP Single File SnapRestore VMFS-Umgebungen: Klonen und Mounten mit Storage VMotion
VMs und VMDKs	VM-konsistente sekundäre Backups	NFS-Umgebungen: ONTAP SnapMirror Restore VMFS-Umgebungen: Klonen und Mounten mit Storage VMotion
VVol VMs	Absturzkonsistente primäre Backups	Single File SnapRestore von ONTAP für alle Protokolle
VVol VMs	Absturzkonsistente sekundäre Backups	ONTAP SnapMirror Restore für alle Protokolle
FlexGroup-VMs	Primäre Backups	NFS-Umgebungen: * ONTAP Single File SnapRestore, wenn Sie ONTAP Version 9.10.1 und höher verwenden * Klonen und Mounten mit Storage VMotion auf früheren Versionen von ONTAP VMFS-Umgebungen: Nicht unterstützt für FlexGroups

Restore-Vorgänge	Von	Durchgeführt mit
FlexGroup-VMs	Sekundäre Backups	NFS-Umgebungen: • ONTAP SnapMirror Wiederherstellen, wenn Sie ONTAP Version 9.10.1 und höher verwenden • Klonen und Mounten mit Storage VMotion für ONTAP vorherige Versionen VMFS-Umgebungen: Nicht unterstützt für FlexGroups

Nach dem Ausgleich von vVol Containern können Sie keine vVol VM wiederherstellen.

Die Wiederherstellung von Gastdateien erfolgt sowohl mit Klon- als auch Mount-Vorgängen (nicht Storage VMotion) in NFS- und VMFS-Umgebungen.

Während eines Wiederherstellungsvorgangs kann der Fehler auftreten, oder dieser tritt auf `Host unresolved volumes is null Exception while calling pre-restore on SCV….Error mounting cloned LUN as datastore…` , wenn das SnapCenter-Plug-in für VMware vSphere versucht, den Klon neu zu signieren. Aufgrund von VMware-Einschränkungen kann das SnapCenter-Plug-in für VMware vSphere den Wert für die automatische Neusignatur in erweiterten ESXi-Hostkonfigurationen nicht steuern. Für NVMe over TCP und NVMe over FC Storage kann SCV keine Controller dynamisch hinzufügen, wenn ein neues Subsystem hinzugefügt wird. Sie sollten die erforderliche Zuordnung vor dem Mount-Vorgang vornehmen.

Weitere Informationen zum Fehler finden Sie unter "KB-Artikel: SCV-Clone oder Wiederherstellung schlagen mit Fehler 'Host ungelöste Volumes ist Null" .

Unterstützung für Amazon FSx for NetApp ONTAP Speichersysteme ist ab der SCV-Version 6.2 verfügbar.

Suche nach Backups

Mit dem Restore-Assistenten können Sie nach einem bestimmten Backup einer VM oder eines Datenspeichers suchen. Nachdem Sie ein Backup gefunden haben, können Sie es dann wiederherstellen.

Schritte

1. Wählen Sie in der Benutzeroberfläche des VMware vSphere-Clients in der Symbolleiste **Menü** aus und führen Sie dann einen der folgenden Schritte aus:

So zeigen Sie Backups für… an	Gehen Sie wie folgt vor…
VMs	Wählen Sie die Menüoption **Hosts und Cluster** aus, wählen Sie dann eine VM aus, wählen Sie dann die Registerkarte **Configure** aus und wählen Sie dann **Backups** im Abschnitt **SnapCenter Plug-in für VMware vSphere** aus.
Datenspeicher	Wählen Sie die Menüoption **Speicher** aus, wählen Sie dann einen Datastore aus, wählen Sie dann die Registerkarte **Konfigurieren** aus und wählen Sie dann **Backups** im Abschnitt **SnapCenter Plug-in für VMware vSphere** aus.

2. Erweitern Sie im linken Navigationsbereich das Rechenzentrum, das die VM oder den Datenspeicher enthält.
3. Optional: Klicken Sie mit der rechten Maustaste auf eine VM oder einen Datastore, wählen Sie dann **SnapCenter Plug-in für VMware vSphere** in der Dropdown-Liste aus und wählen Sie dann **Wiederherstellen** in der sekundären Dropdown-Liste aus.
4. Geben Sie im **Restore**-Assistenten einen Suchnamen ein und wählen Sie **Suche**.

   Sie können die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie dann aus, ob Backups mit VMware-Snapshots, gemountete Backups und den Speicherort enthalten sollen. Wählen Sie **OK**.

Wiederherstellung von VMs aus Backups

Wenn Sie eine VM wiederherstellen, können Sie den vorhandenen Inhalt mit der von Ihnen ausgewählten Backup-Kopie überschreiben oder eine Kopie der VM erstellen.

Sie können VMs an folgenden Orten wiederherstellen:

- Wiederherstellung am ursprünglichen Speicherort
  - In den ursprünglichen Datastore, der auf dem ursprünglichen ESXi-Host gemountet wird (dadurch wird die ursprüngliche VM überschrieben)
- Wiederherstellung an einem alternativen Speicherort
  - Auf einem anderen Datastore, der auf dem ursprünglichen ESXi-Host gemountet wird
  - Auf den ursprünglichen Datastore, der auf einem anderen ESXi-Host gemountet wird und von demselben vCenter gemanagt wird
  - In einem anderen Datastore, der auf einem anderen ESXi-Host gemountet wird und von demselben vCenter gemanagt wird
  - Auf einem anderen Datastore, der auf einem anderen ESXi Host gemountet wird und von einem anderen vCenter im verknüpften Modus verwaltet wird

Sie können vVol VMs nicht auf einem alternativen Host wiederherstellen.

Der folgende Wiederherstellungs-Workflow wird nicht unterstützt: Fügen Sie eine Storage-VM hinzu, führen Sie ein Backup dieser VM aus, löschen Sie dann die Storage-VM, fügen Sie einen Cluster hinzu, der die gleiche Storage-VM enthält, und versuchen Sie dann, das ursprüngliche Backup wiederherzustellen.

Um die Performance von Restore-Vorgängen in NFS-Umgebungen zu verbessern, aktivieren Sie vStorage API for Array Integration (VAAI) für VMware Applikation.

Bevor Sie beginnen

- Ein Backup muss vorhanden sein.

  Sie müssen ein Backup der VM mithilfe des SnapCenter-Plug-ins für VMware vSphere erstellt haben, bevor Sie die VM wiederherstellen können.

  Die Wiederherstellungsvorgänge können nicht erfolgreich abgeschlossen werden, wenn Snapshots der VM vorhanden sind, die von einer anderen Software als dem SnapCenter-Plug-in für VMware vSphere ausgeführt wurden.

- Der Ziel-Datastore muss bereit sein.
  - Der Ziel-Datastore für den Wiederherstellungsvorgang muss über genügend Speicherplatz für eine Kopie aller VM-Dateien (z. B. vmdk, vmx, vmsd) verfügen.
  - Der Ziel-Datastore darf keine veralteten VM-Dateien nach dem Ausfall des vorherigen Wiederherstellungsvorgangs enthalten. Veraltete Dateien haben das Namensformat `restore_xxx_xxxxxx_<filename>`.
- Die VM darf nicht während der Übertragung sein.

  Die VM, die Sie wiederherstellen möchten, darf sich nicht in einem Zustand von vMotion oder Storage vMotion befinden.

- FEHLER bei DER HA-Konfiguration

  Stellen Sie sicher, dass auf dem Bildschirm vCenter ESXi Host Summary keine HA-Konfigurationsfehler angezeigt werden, bevor Sie Backups an einen anderen Ort wiederherstellen.

- Wiederherstellung an einem anderen Speicherort
  - Beim Wiederherstellen an einem anderen Standort muss das SnapCenter Plug-in für VMware vSphere in vCenter ausgeführt werden, das Ziel für den Restore-Vorgang ist. Der Ziel-Datastore muss über ausreichend Speicherplatz verfügen.
  - Das Ziel-vCenter im Feld Wiederherstellen zu einem alternativen Speicherort muss DNS resolable sein.

Über diese Aufgabe

- VM ist nicht registriert und erneut registriert

  Durch den Wiederherstellungsvorgang für VMs wird die ursprüngliche VM aufgehoben, die VM wird aus einem Backup-Snapshot wiederhergestellt und die wiederhergestellte VM mit demselben Namen und derselben Konfiguration auf demselben ESXi-Server registriert. Nach der Wiederherstellung müssen Sie die VMs manuell den Ressourcengruppen hinzufügen.

- Wiederherstellen von Datenspeichern

Sie können zwar keine Datenspeicher wiederherstellen, aber Sie können jede VM im Datastore wiederherstellen.

- Wiederherstellung von vVol VMs
  - VVol Datastores, die über VMs verfügen, werden nicht unterstützt. Da angeschlossene VMDKs in einem VM-Spanning-VVol Datastore nicht gesichert werden, enthalten die wiederhergestellten VMs nur teilweise VMDKs.
  - Sie können ein vVol nicht auf einem alternativen Host wiederherstellen.
  - Der automatische Lastausgleich von vVol wird nicht unterstützt.
- VMware Konsistenz Snapshot-Fehler bei einer VM

  Auch wenn ein VMware Konsistenz-Snapshot für eine VM ausfällt, wird die VM trotzdem gesichert. Sie können die Einheiten, die in der Backup-Kopie im Wiederherstellungsassistenten enthalten sind, anzeigen und für Wiederherstellungsvorgänge verwenden.
- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn der Storage Tier der FabricPool, auf dem sich die VM befindet, nicht verfügbar ist.

Schritte

1. Wählen Sie in der Benutzeroberfläche des VMware vSphere-Clients in der Symbolleiste **Menü** und dann **VMs und Vorlagen** aus der Dropdown-Liste.

   Wenn Sie eine gelöschte VM wiederherstellen, müssen die Anmeldeinformationen der Speicher-VM, die zum SnapCenter-Plug-in für VMware vSphere hinzugefügt wurden, ein Benutzerkonto oder sein `vsadmin` , das über alle gleichen Berechtigungen wie verfügt `vsadmin`.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM, wählen Sie dann **SnapCenter Plug-in für VMware vSphere** in der Dropdown-Liste aus, und wählen Sie dann **Wiederherstellen** in der sekundären Dropdown-Liste aus, um den Assistenten zu starten.
3. Wählen Sie im **Restore**-Assistenten auf der Seite **Backup auswählen** den Backup-Snapshot aus, den Sie wiederherstellen möchten.

   Sie können nach einem bestimmten Backup-Namen oder einem partiellen Backup-Namen suchen, oder Sie können die Backup-Liste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie dabei aus, ob Sie Backups mit VMware-Snapshots erstellen möchten, ob Sie Backups mounten möchten, und wählen Sie den Speicherort aus. Wählen Sie **OK**, um zum Assistenten zurückzukehren.
4. Wählen Sie auf der Seite **Bereich auswählen** im Feld **Umfang wiederherstellen gesamte virtuelle Maschine** aus, wählen Sie dann den Speicherort für die Wiederherstellung aus, und geben Sie dann die Zielinformationen ein, auf denen das Backup gemountet werden soll.

   Wenn im Feld **VM Name** derselbe VM-Name existiert, dann ist das neue VM-Namensformat `<vm_name>_<timestamp>`.

   Bei der Wiederherstellung von Teilersicherungen wird die Seite **Bereich auswählen** mit dem Wiederherstellungsvorgang übersprungen.
5. Wählen Sie auf der Seite **Standort auswählen** den Speicherort für den wiederhergestellten Datastore aus.

   Im SnapCenter Plug-in für VMware vSphere 4.5 und höher können Sie sekundären Storage für FlexGroup

Volumes auswählen.

6. Überprüfen Sie die Übersichtsseite und wählen Sie dann **Fertig stellen**.
7. Optional: Überwachen Sie den Vorgangsfortschritt, indem Sie am unteren Bildschirmrand die Option **Letzte Aufgaben** auswählen.

   Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

Nachdem Sie fertig sind

- IP-Adresse ändern

  Wenn Sie an einem anderen Standort wiederhergestellt haben, müssen Sie die IP-Adresse der neu erstellten VM ändern, um einen IP-Adressenkonflikt zu vermeiden, wenn statische IP-Adressen konfiguriert werden.

- Fügen Sie wiederhergestellte VMs zu Ressourcengruppen hinzu

  Die VMs werden zwar wiederhergestellt, können aber nicht automatisch zu ihren ehemaligen Ressourcengruppen hinzugefügt werden. Daher müssen Sie die wiederhergestellten VMs manuell den entsprechenden Ressourcengruppen hinzufügen.

Gelöschte VMs aus Backups wiederherstellen

Sie können eine gelöschte VM aus einem primären oder sekundären Datastore-Backup auf einem von Ihnen ausgewählten ESXi Host wiederherstellen.

Sie können VMs an folgenden Orten wiederherstellen:

- Wiederherstellung am ursprünglichen Speicherort
  - Auf den ursprünglichen Datastore, der auf dem ursprünglichen ESXi-Host gemountet wird (dadurch wird eine Kopie der VM erstellt).
- Wiederherstellung an einem alternativen Speicherort
  - Auf einem anderen Datastore, der auf dem ursprünglichen ESXi-Host gemountet wird
  - Auf den ursprünglichen Datastore, der auf einem anderen ESXi-Host gemountet wird und von demselben vCenter gemanagt wird
  - In einem anderen Datastore, der auf einem anderen ESXi-Host gemountet wird und von demselben vCenter gemanagt wird
  - Auf einem anderen Datastore, der auf einem anderen ESXi Host gemountet wird und von einem anderen vCenter im verknüpften Modus verwaltet wird

Beim Wiederherstellen an einem anderen Standort muss das SnapCenter Plug-in für VMware vSphere in dem verknüpften vCenter ausgeführt werden, das Ziel für den Restore-Vorgang ist. Der Ziel-Datastore muss über ausreichend Speicherplatz verfügen.

Sie können vVol VMs nicht an einem anderen Speicherort wiederherstellen.

Beim Wiederherstellen einer gelöschten VM werden alle Tags oder Ordner, die ursprünglich der VM zugewiesen wurden, nicht wiederhergestellt.

Bevor Sie beginnen

- Das Benutzerkonto für das Speichersystem muss auf der Seite Speichersysteme im VMware vSphere-Client über die verfügen "Mindestberechtigungen für ONTAP für ONTAP erforderlich".
- Das Benutzerkonto in vCenter muss über den verfügen "Minimale vCenter-Berechtigungen, die für das SnapCenter Plug-in für VMware vSphere erforderlich sind".
- Ein Backup muss vorhanden sein.

  Bevor Sie die VMDKs auf dieser VM wiederherstellen können, müssen Sie ein Backup der VM mit dem SnapCenter Plug-in für VMware vSphere erstellt haben.

Um die Performance von Restore-Vorgängen in NFS-Umgebungen zu verbessern, aktivieren Sie vStorage API for Array Integration (VAAI) für VMware Applikation.

Über diese Aufgabe

Sie können zwar keine Datenspeicher wiederherstellen, aber Sie können jede VM im Datastore wiederherstellen.

Ein Wiederherstellungsvorgang kann fehlschlagen, wenn der Storage Tier der FabricPool, auf dem sich die VM befindet, nicht verfügbar ist.

Schritte

1. Navigieren Sie im vCenter Server zu **Inventar** > **Datastores** und wählen Sie einen Datenspeicher aus.
2. Wählen Sie im Abschnitt SnapCenter Plug-in für VMware vSphere die Option **Configure** > **Backups** aus.
3. Durch Doppelklicken auf ein Backup wird eine Liste aller VMs angezeigt, die im Backup enthalten sind.
4. Wählen Sie die gelöschte VM aus der Backup-Liste aus und wählen Sie **Restore**.
5. Wählen Sie im Assistenten * Wiederherstellen* auf der Seite **Sicherung auswählen** die Sicherungskopie aus, die Sie wiederherstellen möchten.

   Sie können nach einem bestimmten Backup-Namen oder einem partiellen Backup-Namen suchen, oder Sie können die Backup-Liste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie dabei aus, ob Sie Backups mit VMware-Snapshots erstellen möchten, ob Sie Backups mounten möchten, und wählen Sie den Speicherort aus. Wählen Sie **OK**, um zum Assistenten zurückzukehren.

6. Wählen Sie auf der Seite **Bereich auswählen** im Feld **Bereich wiederherstellen** die Option **gesamte virtuelle Maschine** aus, wählen Sie dann den Speicherort für die Wiederherstellung aus und geben Sie dann die Ziel-ESXi-Hostinformationen ein, in die das Backup eingebunden werden soll.

   Das Wiederherstellungsziel kann jeder beliebige ESXi Host sein, der SnapCenter hinzugefügt wurde. Diese Option stellt den Inhalt des ausgewählten Backups wieder her, in dem die VM zu dem angegebenen Zeitpunkt und Datum aus einem Snapshot residierte. Das Kontrollkästchen **VM neu starten** ist aktiviert, wenn Sie diese Option auswählen und die VM eingeschaltet wird.

   Wenn Sie eine VM in einem NFS-Datenspeicher auf einem anderen ESXi Host wiederherstellen, der sich in einem ESXi Cluster befindet, wird sie nach der Wiederherstellung der VM auf dem alternativen Host registriert.

7. Wählen Sie auf der Seite **Standort auswählen** den Speicherort des Backups aus, von dem Sie das Backup wiederherstellen möchten (primäre oder sekundäre).
8. Überprüfen Sie die Übersichtsseite und wählen Sie dann **Fertig stellen**.

Wiederherstellung von VMDKs aus Backups

Sie können vorhandene VMDKs, gelöschte oder abgetrennte VMDKs, entweder von einem primären oder sekundären Backup herkömmlicher VMs oder vVol VMs wiederherstellen.

Sie können eine oder mehrere Virtual Machine-Festplatten (VMDKs) auf einer VM im selben Datenspeicher wiederherstellen.

Um die Performance von Restore-Vorgängen in NFS-Umgebungen zu verbessern, aktivieren Sie vStorage API for Array Integration (VAAI) für VMware Applikation.

Bevor Sie beginnen

- Ein Backup muss vorhanden sein.

  Sie müssen mit dem SnapCenter Plug-in für VMware vSphere eine Sicherung der VM erstellt haben.

- Die VM darf nicht während der Übertragung sein.

  Die VM, die Sie wiederherstellen möchten, darf sich nicht in einem Zustand von vMotion oder Storage vMotion befinden.

Über diese Aufgabe

- Wenn die VMDK gelöscht oder von der VM getrennt wird, wird die VMDK durch den Wiederherstellungsvorgang an die VM angeschlossen.
- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn der Storage Tier der FabricPool, auf dem sich die VM befindet, nicht verfügbar ist.
- Verbinden Sie VMDKs über den Standard-SCSI-Controller und stellen Sie Wiederherstellungsvorgänge her. Wenn jedoch VMDKs gesichert werden, die an eine VM mit NVMe-Festplatte angeschlossen sind, verwenden die Anschluss- und Wiederherstellungsvorgänge, sofern verfügbar, den NVMe-Controller.

Schritte

1. Wählen Sie in der Benutzeroberfläche des VMware vSphere-Clients in der Symbolleiste **Menü** und dann **VMs und Vorlagen** aus der Dropdown-Liste.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM, wählen Sie dann **SnapCenter Plug-in für VMware vSphere** in der Dropdown-Liste aus, und wählen Sie dann **Wiederherstellen** in der sekundären Dropdown-Liste aus.
3. Wählen Sie im Assistenten **Wiederherstellen** auf der Seite Sicherung auswählen die Sicherungskopie aus, aus der Sie die Sicherungskopie wiederherstellen möchten.

   Sie können nach einem bestimmten Backup-Namen oder einem partiellen Backup-Namen suchen, oder Sie können die Backup-Liste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie aus, ob Backups mit VMware-Snapshots erstellt werden sollen, ob Backups gemountet werden sollen, und wählen Sie den primären oder sekundären Speicherort aus. Wählen Sie **OK**, um zum Assistenten zurückzukehren.

4. Wählen Sie auf der Seite **Bereich auswählen** das Wiederherstellungsziel aus.

Wiederherstellen auf…	Geben Sie das Wiederherstellungsziel… an
Den ursprünglichen Datenspeicher verwendet	Wählen Sie aus der Dropdown-Liste **particular Disk** aus und wählen Sie dann **Next** aus. In der Tabelle Datastore Selection können Sie beliebige VMDKs auswählen oder deren Auswahl aufheben.
Einen alternativen Datenspeicher an einem alternativen Speicherort	Wählen Sie den Ziel-Datastore aus und wählen Sie einen anderen Datastore aus der Liste aus.

5. Wählen Sie auf der Seite **Speicherort auswählen** den Snapshot aus, den Sie wiederherstellen möchten (primär oder sekundär).
6. Überprüfen Sie die Übersichtsseite und wählen Sie dann **Fertig stellen**.
7. Optional: Überwachen Sie den Vorgangsfortschritt, indem Sie am unteren Bildschirmrand die Option **Letzte Aufgaben** auswählen.
8. Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

Stellen Sie das neueste Backup der MySQL-Datenbank wieder her

Sie können die Wartungskonsole verwenden, um das aktuellste Backup der MySQL-Datenbank (auch NSM-Datenbank genannt) für das SnapCenter-Plug-in für VMware vSphere wiederherzustellen.

Schritte

1. Öffnen Sie ein Fenster der Wartungskonsole.

   "Öffnen Sie die Wartungskonsole".

2. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration** ein.
3. Geben Sie im Menü Anwendungskonfiguration die Option **6) MySQL-Sicherung und -Wiederherstellung** ein.
4. Geben Sie im Menü MySQL Backup and Restore Configuration die Option **4) MySQL Backup wiederherstellen** ein.
5. Geben Sie an der Eingabeaufforderung „Wiederherstellen mit dem neuesten Backup“ **y** ein, und drücken Sie dann **Enter**.

   Die MySQL Backup Datenbank wird an ihren ursprünglichen Speicherort wiederhergestellt.

Stellen Sie ein bestimmtes Backup der MySQL-Datenbank wieder her

Mit der Wartungskonsole können Sie ein bestimmtes Backup der MySQL-Datenbank (auch als NSM-Datenbank bezeichnet) für das SnapCenter Plug-in für die virtuelle Appliance VMware vSphere wiederherstellen.

Schritte

1. Öffnen Sie ein Fenster der Wartungskonsole.

   "Öffnen Sie die Wartungskonsole".

2. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration** ein.
3. Geben Sie im Menü Anwendungskonfiguration die Option **6) MySQL-Sicherung und -Wiederherstellung** ein.
4. Geben Sie im Menü MySQL Backup and Restore Configuration die Option **2) MySQL-Backups** ein und notieren Sie sich dann das Backup, das Sie wiederherstellen möchten.
5. Geben Sie im Menü MySQL Backup and Restore Configuration die Option **4) MySQL Backup wiederherstellen** ein.
6. Geben Sie an der Eingabeaufforderung „Wiederherstellen mit dem neuesten Backup“ **n** ein.
7. Geben Sie an der Eingabeaufforderung „Backup to restore from“ den Sicherungsnamen ein, und drücken Sie dann **Enter**.

   Die ausgewählte MySQL-Backup-Datenbank wird an ihren ursprünglichen Speicherort wiederhergestellt.

Anschließen und Trennen von VMDKs

Weisen Sie VMDKs an eine VM oder vVol VM zu

Sie können eine oder mehrere VMDKs aus einem Backup an die übergeordnete VM oder an eine alternative VM auf demselben ESXi Host oder an eine alternative VM auf einem alternativen ESXi Host anschließen, der im verknüpften Modus von demselben vCenter oder einem anderen vCenter gemanagt wird. VMs in herkömmlichen Datenspeichern und in vVol Datastores werden unterstützt.

Somit ist es einfacher, eine oder mehrere einzelne Dateien von einem Laufwerk wiederherzustellen, anstatt das gesamte Laufwerk wiederherzustellen. Sie können die VMDK trennen, nachdem Sie die Dateien wiederhergestellt haben oder auf die Sie zugreifen möchten.

Über diese Aufgabe

Sie haben die folgenden Zusatzoptionen:

- Sie können virtuelle Laufwerke von einem primären oder einem sekundären Backup hinzufügen.
- Sie können virtuelle Laufwerke an die übergeordnete VM (die gleiche VM, mit der die virtuelle Festplatte ursprünglich verknüpft war) oder an eine andere VM auf demselben ESXi-Host anschließen.

Die folgenden Einschränkungen gelten für das Anbinden virtueller Laufwerke:

- Vorgänge zum Verbinden und Trennen werden für VM-Vorlagen nicht unterstützt.
- Sind mehr als 15 VMDKs an einen iSCSI-Controller angeschlossen, kann die Virtual Machine für das SnapCenter Plug-in für VMware vSphere aufgrund der Einschränkungen von VMware keine VMDK-Gerätenummern über 15 finden.

  Fügen Sie in diesem Fall die SCSI-Controller manuell hinzu, und versuchen Sie es erneut.
- Sie können keine virtuelle Festplatte manuell anschließen, die als Teil eines Wiederherstellungsvorgangs für die Gastdatei angehängt oder angehängt wurde.
- Verbinden Sie VMDKs über den Standard-SCSI-Controller und stellen Sie Wiederherstellungsvorgänge her. Wenn jedoch VMDKs gesichert werden, die an eine VM mit NVMe-Festplatte angeschlossen sind, verwenden die Anschluss- und Wiederherstellungsvorgänge, sofern verfügbar, den NVMe-Controller.

Bevor Sie beginnen

Gehen Sie wie folgt vor, um NVMe Controller zur Festplatte hinzuzufügen.

1. Melden Sie sich beim vCenter Client an
2. Wählen Sie die VM aus dem VMFS-Datastore aus
3. Klicken Sie mit der rechten Maustaste auf die VM und gehen Sie zu **Einstellungen bearbeiten**
4. Wählen Sie im Fenster Einstellungen bearbeiten die Option **Neues Gerät hinzufügen** > **NVMe Controller**

Schritte

1. Wählen Sie in der Benutzeroberfläche des VMware vSphere-Clients in der Symbolleiste **Menü** und dann **Hosts und Cluster** aus der Dropdown-Liste.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM, und wählen Sie dann

SnapCenter Plug-in für VMware vSphere > **Virtuelle Festplatte(n) anhängen** aus.

3. Wählen Sie im Fenster **Virtuelles Laufwerk anhängen** im Abschnitt **Sicherung** ein Backup aus.

   Sie können die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie dann aus, ob Backups mit VMware-Snapshots, gemountete Backups und den Speicherort enthalten sollen. Wählen Sie **OK**.

4. Wählen Sie im Abschnitt **Select Disks** ein oder mehrere Festplatten aus, die Sie verbinden möchten, und den Speicherort, an den Sie anschließen möchten (primäre oder sekundäre).

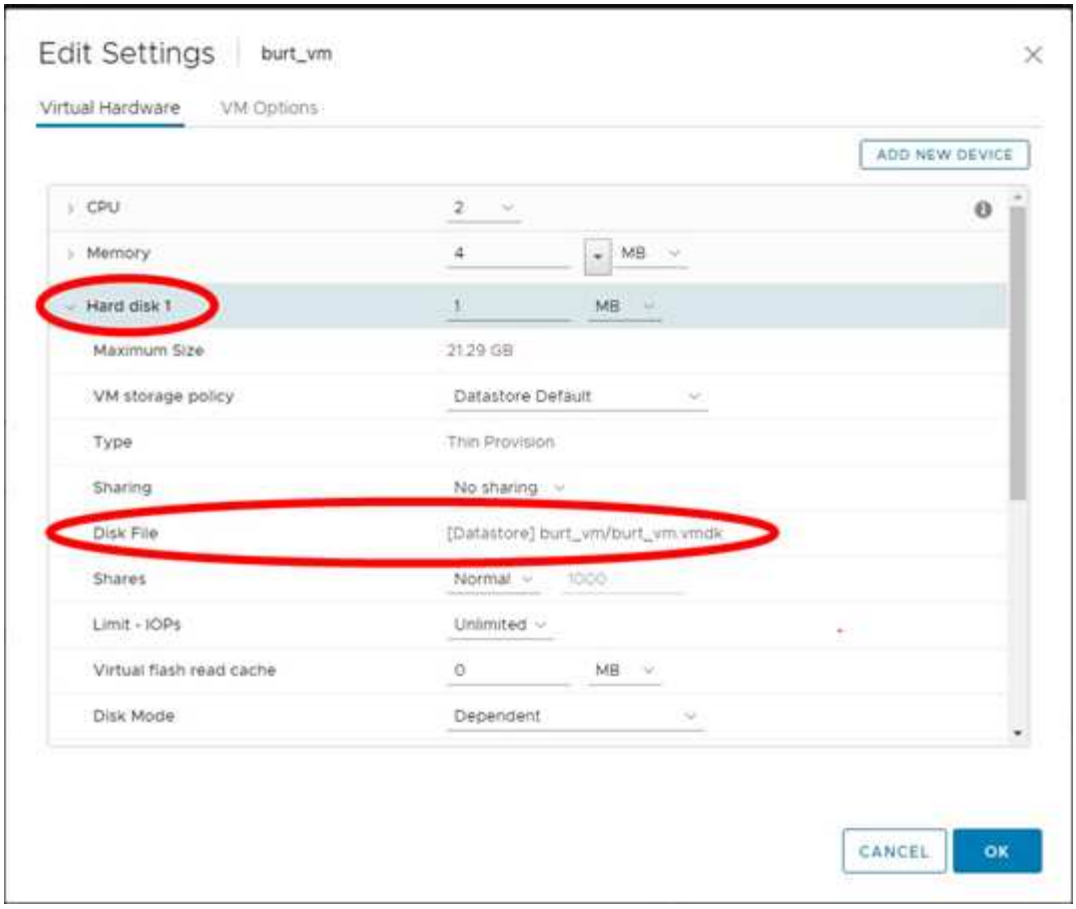
   Sie können den Filter so ändern, dass primäre und sekundäre Standorte angezeigt werden.

5. Standardmäßig sind die ausgewählten virtuellen Laufwerke an die übergeordnete VM angeschlossen. Um die ausgewählten virtuellen Laufwerke an eine alternative VM im selben ESXi-Host anzubinden, wählen Sie **Klicken Sie hier, um sie an eine alternative VM anzuhängen** und geben Sie die alternative VM an.
6. Wählen Sie **Anhängen**.
7. Optional: Überwachen Sie den Arbeitsfortschritt im Abschnitt * Letzte Aufgaben*.

   Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

8. Stellen Sie sicher, dass das virtuelle Laufwerk angeschlossen ist, indem Sie Folgendes durchführen:

   a. Wählen Sie in der Symbolleiste **Menu** aus, und wählen Sie dann **VMs und Vorlagen** aus der Dropdown-Liste aus.
   b. Klicken Sie im linken Navigationsfenster mit der rechten Maustaste auf eine VM, und wählen Sie dann in der Dropdown-Liste **Einstellungen bearbeiten** aus.
   c. Erweitern Sie im Fenster **Einstellungen bearbeiten** die Liste für jede Festplatte, um die Liste der Festplattendateien anzuzeigen.



Auf der Seite „Einstellungen bearbeiten“ werden die Festplatten auf der VM aufgeführt. Sie können die Details für jede Festplatte erweitern, um die Liste der verbundenen virtuellen Laufwerke anzuzeigen.

Ergebnis

Sie können vom Host-Betriebssystem auf die angeschlossenen Laufwerke zugreifen und die erforderlichen Informationen von den Festplatten abrufen.

Trennen Sie eine virtuelle Festplatte

Nachdem Sie ein virtuelles Laufwerk zur Wiederherstellung einzelner Dateien angeschlossen haben, können Sie das virtuelle Laufwerk von der übergeordneten VM trennen.

Schritte

1. Wählen Sie in der Benutzeroberfläche des VMware vSphere-Clients in der Symbolleiste **Menü** und dann **VMs und Vorlagen** aus der Dropdown-Liste.
2. Wählen Sie im linken Navigationsbereich eine VM aus.
3. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf die VM, wählen Sie dann **SnapCenter Plug-in für VMware vSphere** in der Dropdown-Liste aus, und wählen Sie dann **virtuelles Laufwerk trennen** in der sekundären Dropdown-Liste aus.
4. Wählen Sie auf dem Bildschirm **Virtuelles Laufwerk trennen** eine oder mehrere Laufwerke aus, die Sie trennen möchten, und aktivieren Sie dann das Kontrollkästchen **Ausgewählte Datenträger trennen**, und wählen Sie **TRENNEN**.

Stellen Sie sicher, dass Sie das richtige virtuelle Laufwerk auswählen. Die Auswahl der falschen Festplatte kann die Produktionsarbeit beeinträchtigen.

5. Optional: Überwachen Sie den Arbeitsfortschritt im Abschnitt * Letzte Aufgaben*.

   Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

6. Stellen Sie sicher, dass das virtuelle Laufwerk getrennt ist, indem Sie Folgendes durchführen:
   a. Wählen Sie in der Symbolleiste **Menu** aus, und wählen Sie dann **VMs und Vorlagen** aus der Dropdown-Liste aus.
   b. Klicken Sie im linken Navigationsfenster mit der rechten Maustaste auf eine VM, und wählen Sie dann in der Dropdown-Liste **Einstellungen bearbeiten** aus.
   c. Erweitern Sie im Fenster **Einstellungen bearbeiten** die Liste für jede Festplatte, um die Liste der Festplattendateien anzuzeigen.

      Auf der Seite **Edit Settings** werden die Festplatten auf der VM aufgelistet. Sie können die Details für jede Festplatte erweitern, um die Liste der verbundenen virtuellen Laufwerke anzuzeigen.

Wiederherstellung von Gastdateien und Ordnern

Workflow, Voraussetzungen und Einschränkungen

Sie können Dateien oder Ordner von einem Virtual Machine-Laufwerk (VMDK) auf einem Windows-Gastbetriebssystem wiederherstellen.

Workflow zur Wiederherstellung von Gastspielen

Zur Wiederherstellung von Gastbetriebssystemen gehören die folgenden Schritte:

1. Anhängen

   Schließen Sie ein virtuelles Laufwerk an eine Gast-VM oder Proxy-VM an, und starten Sie eine Wiederherstellungssitzung für die Gastdatei.

2. Warten

   Warten Sie, bis der Attach abgeschlossen ist, bevor Sie die Daten durchsuchen und wiederherstellen können. Wenn der Anschluss

   Der Vorgang ist abgeschlossen, eine Sitzung zur Wiederherstellung der Gastdatei wird automatisch erstellt und eine E-Mail-Benachrichtigung wird erstellt

   Gesendet.

3. Wählen Sie Dateien oder Ordner aus

   Durchsuchen Sie die VMDK in der Sitzung „Wiederherstellung von Gastdateien“ und wählen Sie eine oder mehrere Dateien oder Ordner aus, die wiederhergestellt werden sollen.

4. Wiederherstellen

   Stellen Sie die ausgewählten Dateien oder Ordner an einem bestimmten Speicherort wieder her.

Voraussetzungen für die Wiederherstellung von Gastdateien und -Ordnern

Bevor Sie eine oder mehrere Dateien oder Ordner von einer VMDK auf einem Windows-Gastbetriebssystem wiederherstellen, müssen Sie alle Anforderungen kennen.

- VMware-Tools müssen installiert und ausgeführt werden.

  SnapCenter verwendet Informationen aus VMware Tools, um eine Verbindung zum VMware Gastbetriebssystem herzustellen.

- Das Windows Gastbetriebssystem muss Windows Server 2008 R2 oder höher ausgeführt werden.

  Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

- Anmeldedaten für die Ziel-VM müssen das integrierte Domain-Administratorkonto oder das integrierte lokale Administratorkonto angeben. Der Benutzername muss „Administrator“ sein. Bevor Sie mit dem Wiederherstellungsvorgang beginnen, müssen die Anmeldeinformationen für die VM konfiguriert werden,

der Sie das virtuelle Laufwerk anschließen möchten. Die Anmeldeinformationen sind sowohl für den Attach-Vorgang als auch für den nachfolgenden Wiederherstellungsvorgang erforderlich. Workgroup-Benutzer können das integrierte lokale Administratorkonto verwenden.

> Wenn Sie ein Konto verwenden müssen, das nicht das integrierte Administratorkonto ist, aber über Administratorrechte innerhalb der VM verfügt, müssen Sie UAC auf der Gast-VM deaktivieren.

- Sie müssen den Backup-Snapshot und die VMDK kennen, von der aus Sie wiederherstellen möchten.

  Das SnapCenter Plug-in für VMware vSphere unterstützt nicht das Suchen der wiederherzustellenden Dateien oder Ordner. Daher müssen Sie vor dem Start den Speicherort der Dateien oder Ordner in Bezug auf den Snapshot und die entsprechende VMDK kennen.

- Das zu verbundene virtuelle Laufwerk muss in einem SnapCenter-Backup enthalten sein.

  Das virtuelle Laufwerk, das die wiederherzustellende Datei oder den Ordner enthält, muss sich in einem VM-Backup befinden, das mit der virtuellen Appliance für SnapCenter Plug-in für VMware vSphere durchgeführt wurde.

- Um eine Proxy-VM zu verwenden, muss die Proxy-VM konfiguriert werden.

  Wenn Sie eine virtuelle Festplatte an eine Proxy-VM anschließen möchten, muss die Proxy-VM konfiguriert werden, bevor der Vorgang zum Verbinden und Wiederherstellen beginnt.

- Bei Dateien mit nicht-englischen Alphabet-Namen müssen Sie sie in einem Verzeichnis und nicht als einzelne Datei wiederherstellen.

  Sie können Dateien mit nicht alphabetischen Namen, wie z. B. japanischen Kanji, wiederherstellen, indem Sie das Verzeichnis wiederherstellen, in dem die Dateien gespeichert sind.

- Die Wiederherstellung von einem Linux-Gastbetriebssystem wird nicht unterstützt

  Sie können keine Dateien und Ordner von einer VM wiederherstellen, auf der ein Linux-Gastbetriebssystem ausgeführt wird. Sie können jedoch ein VMDK anhängen und die Dateien und Ordner dann manuell wiederherstellen. Aktuelle Informationen zu unterstützten Gastbetriebssystemen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

Einschränkungen bei der Wiederherstellung von Gastdateien

Bevor Sie eine Datei oder einen Ordner von einem Gastbetriebssystem wiederherstellen, sollten Sie wissen, was die Funktion nicht unterstützt.

- Sie können keine dynamischen Festplattentypen innerhalb eines Gastbetriebssystems wiederherstellen.
- Wenn Sie eine verschlüsselte Datei oder einen verschlüsselten Ordner wiederherstellen, wird das Verschlüsselungsattribut nicht beibehalten. Dateien oder Ordner können nicht in einem verschlüsselten Ordner wiederhergestellt werden.
- Auf der Seite „Durchsuchen der Gastdatei“ werden die ausgeblendeten Dateien und Ordner angezeigt, die nicht gefiltert werden können.
- Sie können die Wiederherstellung nicht aus einem Linux Gast-Betriebssystem durchführen.

  Sie können keine Dateien und Ordner von einer VM wiederherstellen, auf der ein Linux-Gastbetriebssystem ausgeführt wird. Sie können jedoch ein VMDK anhängen und die Dateien und Ordner

dann manuell wiederherstellen. Aktuelle Informationen zu unterstützten Gastbetriebssystemen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

- Sie können von einem NTFS-Dateisystem nicht in ein FAT-Dateisystem wiederherstellen.

  Wenn Sie versuchen, vom NTFS-Format in DAS FAT-Format wiederherzustellen, wird der NTFS-Sicherheitsdeskriptor nicht kopiert, da das FAT-Dateisystem Windows-Sicherheitsattribute nicht unterstützt.

- Sie können Gastdateien nicht aus einer geklonten VMDK oder einer nicht initialisierten VMDK wiederherstellen.
- Sie können die Verzeichnisstruktur für eine Datei nicht wiederherstellen.

  Wenn eine Datei in einem verschachtelten Verzeichnis zur Wiederherstellung ausgewählt ist, wird die Datei nicht mit derselben Verzeichnisstruktur wiederhergestellt. Der Verzeichnisbaum wird nicht wiederhergestellt, nur die Datei. Wenn Sie eine Verzeichnisstruktur wiederherstellen möchten, können Sie das Verzeichnis selbst oben in der Struktur kopieren.

- Sie können keine Gastdateien von einer vVol VM zu einem anderen Host wiederherstellen.
- Verschlüsselte Gastdateien können nicht wiederhergestellt werden.

Wiederherstellung von Gastdateien und Ordnern über VMDKs

Sie können eine oder mehrere Dateien oder Ordner von einer VMDK auf einem Windows Gastbetriebssystem wiederherstellen.

Über diese Aufgabe

Standardmäßig ist das verbundene virtuelle Laufwerk 24 Stunden lang verfügbar und wird automatisch getrennt. Sie können im Assistenten wählen, ob die Sitzung automatisch gelöscht wird, wenn der Wiederherstellungsvorgang abgeschlossen ist, oder Sie können die Gastdateiwiederherstellungssitzung jederzeit manuell löschen oder die Zeit auf der Seite **Gastkonfiguration** verlängern.

Die Performance der Wiederherstellung von Gastdateien oder Ordnern hängt von zwei Faktoren ab: Der Größe der wiederherzustellenden Dateien oder Ordner und der Anzahl der wiederherzustellenden Dateien oder Ordner. Das Wiederherstellen einer großen Anzahl von kleinen Dateien kann sehr viel Zeit in Anspruch nehmen als erwartet, im Vergleich zur Wiederherstellung einer kleinen Anzahl großer Dateien, wenn der wiederherzustellende Datensatz von derselben Größe entspricht.

Auf einer VM kann nur ein Attach- oder Restore-Vorgang gleichzeitig ausgeführt werden. Sie können auf derselben VM keine parallelen Attached- oder Restore-Vorgänge ausführen.

Mit der Gastwiederherstellungsfunktion können Sie System- und verborgene Dateien anzeigen und wiederherstellen sowie verschlüsselte Dateien anzeigen. Versuchen Sie nicht, eine vorhandene Systemdatei zu überschreiben oder verschlüsselte Dateien in einem verschlüsselten Ordner wiederherzustellen. Während der Wiederherstellung bleiben die verborgenen, System- und verschlüsselten Attribute von Gastdateien nicht in der wiederhergestellten Datei erhalten. Das Anzeigen oder Durchsuchen von reservierten Partitionen kann zu einem Fehler führen.

Schritte

1. Wählen Sie im Fenster vSphere Client Shortcuts die Option **Hosts and Clusters** aus, und wählen Sie eine

VM aus.

2. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **SnapCenter Plug-in für VMware vSphere** > **Gastdateiwiederherstellung**.
3. Geben Sie auf der Seite **Wiederherstellungsumfang** das Backup an, das das virtuelle Laufwerk enthält, das Sie anhängen möchten, indem Sie wie folgt vorgehen:
   a. Wählen Sie in der Tabelle **Backup Name** das Backup aus, das das virtuelle Laufwerk enthält, das Sie anhängen möchten.
   b. Wählen Sie in der Tabelle **VMDK** das virtuelle Laufwerk aus, das die Dateien oder Ordner enthält, die Sie wiederherstellen möchten.
   c. Wählen Sie in der Tabelle **Locations** den primären oder sekundären Speicherort des virtuellen Laufwerks aus, das Sie verbinden möchten.
4. Gehen Sie auf der Seite **Gästedetails** wie folgt vor.
   a. Wählen Sie, wo das virtuelle Laufwerk angeschlossen werden soll:

Wählen Sie diese Option…	Wenn…
Verwenden Sie die Gast-VM	Sie möchten das virtuelle Laufwerk an die VM anhängen, auf die Sie vor dem Start des Assistenten mit der rechten Maustaste geklickt haben, und dann die Anmeldedaten für die VM auswählen, auf die Sie mit der rechten Maustaste geklickt haben. Für die VM müssen bereits Anmeldedaten erstellt werden.
Verwenden Sie die Proxy-VM zur Wiederherstellung der Gastdatei	Sie möchten das virtuelle Laufwerk mit einer Proxy-VM verbinden und dann die Proxy-VM auswählen. Die Proxy-VM muss konfiguriert werden, bevor der Anfügen- und Wiederherstellungsvorgang beginnt.

   b. Wählen Sie die Option **E-Mail-Benachrichtigung senden** aus.

      Diese Option ist erforderlich, wenn Sie benachrichtigt werden möchten, wenn der Anhängevorgang abgeschlossen ist, und das virtuelle Laufwerk verfügbar ist. Die Benachrichtigungs-E-Mail enthält den Namen des virtuellen Laufwerks, den VM-Namen und den neu zugewiesenen Laufwerksbuchstaben für die VMDK.

      Aktivieren Sie diese Option, da es sich bei der Wiederherstellung einer Gastdatei um einen asynchronen Vorgang handelt, und es kann zu einer Verzögerung bei der Festlegung einer Gastsitzung für Sie kommen.

Diese Option verwendet die E-Mail-Einstellungen, die beim Einrichten des VMware vSphere Clients in vCenter konfiguriert sind.

5. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig stellen**.

   Bevor Sie **Fertig stellen** auswählen, können Sie zu einer beliebigen Seite des Assistenten zurückkehren und die Informationen ändern.

6. Warten Sie, bis der Attach-Vorgang abgeschlossen ist.

   Sie können den Fortschritt des Vorgangs in der Job-Überwachung des Dashboards anzeigen oder auf die E-Mail-Benachrichtigung warten.

7. Um die Dateien zu finden, die Sie von der angeschlossenen virtuellen Festplatte wiederherstellen möchten, wählen Sie **SnapCenter Plug-in für VMware vSphere** aus dem Fenster vSphere Client Shortcuts.
8. Wählen Sie im linken Navigationsbereich **Gastdateiwiederherstellung** > **Gastkonfiguration**.

   In der Tabelle Guest Session Monitor können Sie zusätzliche Informationen zu einer Sitzung anzeigen, indem Sie *… *In der rechten Spalte.

9. Wählen Sie die Wiederherstellungssitzung der Gastdatei für das virtuelle Laufwerk aus, das in der Benachrichtigungs-E-Mail aufgeführt wurde.

   Allen Partitionen wird ein Laufwerksbuchstabe zugewiesen, einschließlich systemreservierter Partitionen. Wenn eine VMDK über mehrere Partitionen verfügt, können Sie ein bestimmtes Laufwerk auswählen, indem Sie das Laufwerk in der Dropdown-Liste im Laufwerkfeld oben auf der Seite „Durchsuchen der Gastdatei“ auswählen.

10. Wählen Sie das Symbol **Dateien durchsuchen**, um eine Liste der Dateien und Ordner auf dem virtuellen Laufwerk anzuzeigen.

    Wenn Sie einen Ordner zum Durchsuchen und Auswählen einzelner Dateien doppelt auswählen, kann es beim Abrufen der Dateiliste zu einer Zeitlatenz kommen, da der Abrufvorgang zur Laufzeit ausgeführt wird.

    Um das Durchsuchen zu vereinfachen, können Sie Filter in Ihrer Suchzeichenfolge verwenden. Bei den Filtern handelt es sich um Groß- und Kleinschreibung-Perlausdrücke ohne Leerzeichen. Der standardmäßige Suchstring lautet `.*`. Die folgende Tabelle zeigt ein Beispiel für Perl-Suchausdrücke.

Dieser Ausdruck…	**Sucht nach…**
.	Alle Zeichen außer einem neuen Zeichen.
.*	Beliebige Zeichenfolge. Dies ist die Standardeinstellung.
A	Das Zeichen a.
ab	Der String ab.
Ein [vertikaler Balken] b	Das Zeichen A oder B.
A*	Null oder mehr Instanzen des Zeichens a.
A+	Ein oder mehrere Instanzen des Zeichens a.
A?	Null oder eine Instanz des Zeichens a.
A{x}	Genau x Anzahl der Instanzen des Zeichens a.
A{x,}	Mindestens x Anzahl der Instanzen des Zeichens a.

Dieser Ausdruck…	Sucht nach…
A{x,y}	Mindestens x Anzahl der Instanzen des Zeichens A und höchstens y Zahl.
\	Entgeht einem besonderen Charakter.

Auf der Seite „Durchsuchen der Gastdatei“ werden alle verborgenen Dateien und Ordner sowie alle anderen Dateien und Ordner angezeigt.

11. Wählen Sie eine oder mehrere Dateien oder Ordner aus, die Sie wiederherstellen möchten, und wählen Sie dann **Speicherort für Wiederherstellung auswählen**.

    Die wiederherzustellenden Dateien und Ordner sind in der Tabelle Ausgewählte Dateien aufgeführt.

12. Geben Sie auf der Seite **Speicherort wiederherstellen** Folgendes an:

Option	Beschreibung
Wiederherstellen des Pfads	Geben Sie den UNC-Freigabepfad zum Gast ein, auf dem die ausgewählten Dateien wiederhergestellt werden. Beispiel für IPv4-Adresse `\\10.60.136.65\c$`: IPv6-Adresse Beispiel: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`
Wenn Originaldatei(en) vorhanden ist	Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die wiederherzustellende Datei oder der wiederherzustellende Ordner bereits auf dem Wiederherstellungsziel vorhanden ist: Immer überschreiben oder immer überspringen. Wenn der Ordner bereits vorhanden ist, wird der Inhalt des Ordners mit dem vorhandenen Ordner zusammengeführt.
Trennen Sie die Gastsitzung nach erfolgreicher Wiederherstellung	Wählen Sie diese Option aus, wenn die Wiederherstellungssitzung der Gastdatei gelöscht werden soll, wenn der Wiederherstellungsvorgang abgeschlossen ist.

13. Wählen Sie **Wiederherstellen**.

    Sie können den Fortschritt des Wiederherstellungsvorgangs in der Job-Überwachung des Dashboards anzeigen oder auf die E-Mail-Benachrichtigung warten. Die Zeit, die benötigt wird, bis die E-Mail-Benachrichtigung gesendet wird, hängt von der Dauer ab, die der Wiederherstellungsvorgang dauert.

    Die Benachrichtigungs-E-Mail enthält einen Anhang mit der Ausgabe aus dem Wiederherstellungsvorgang. Wenn der Wiederherstellungsvorgang fehlschlägt, öffnen Sie den Anhang, um weitere Informationen zu erhalten.

Einrichten von Proxy-VMs für Wiederherstellungsvorgänge

Wenn Sie eine Proxy-VM zum Anschließen einer virtuellen Festplatte für die Wiederherstellung von Gastdateien verwenden möchten, müssen Sie die Proxy-VM einrichten, bevor Sie mit der Wiederherstellung beginnen. Sie können zwar jederzeit eine Proxy-VM einrichten, jedoch ist es unter Umständen günstiger, sie sofort nach Abschluss der Plug-in-Bereitstellung einzurichten.

Schritte

1. Wählen Sie im Fenster vSphere Client Shortcuts unter Plug-ins **SnapCenter Plug-in für VMware vSphere** aus.
2. Wählen Sie in der linken Navigation **Guest File Restore**.
3. Führen Sie im Abschnitt * Ausführen als Anmeldeinformationen* einen der folgenden Schritte aus:

Um dies zu tun…	Do this…
Verwenden Sie vorhandene Anmeldedaten	Wählen Sie eine der konfigurierten Anmeldeinformationen aus.
Neue Anmeldedaten hinzufügen	a. Wählen Sie **Hinzufügen**. b. Geben Sie im Dialogfeld **Ausführen als Anmeldeinformationen** die Anmeldeinformationen ein. c. Wählen Sie **Select VM** aus, und wählen Sie dann im Dialogfeld **Proxy VM** eine VM aus. Wählen Sie **Speichern**, um zum Dialogfeld **Run As Credentials** zurückzukehren. d. Geben Sie die Anmeldeinformationen ein. Für den Benutzernamen müssen Sie „Administrator“ eingeben.

   Das SnapCenter Plug-in für VMware vSphere verwendet die ausgewählten Anmeldeinformationen, um sich bei der ausgewählten Proxy-VM anzumelden.

   Die Anmeldeinformationen „Ausführen als“ müssen der standardmäßige Domänenadministrator sein, der von Windows oder dem integrierten lokalen Administrator bereitgestellt wird. Workgroup-Benutzer können das integrierte lokale Administratorkonto verwenden.

4. Wählen Sie im Abschnitt **Proxy Credentials Hinzufügen** aus, um eine VM hinzuzufügen, die als Proxy verwendet werden soll.
5. Füllen Sie im Dialogfeld **Proxy VM** die Informationen aus, und wählen Sie dann **Speichern**.

Sie müssen die Proxy-VM aus dem SnapCenter-Plug-in für VMware vSphere-UI löschen, bevor Sie sie vom ESXi-Host löschen können.

Konfigurieren Sie die Anmeldedaten für die Wiederherstellung von VM-Gastdateien

Wenn Sie ein virtuelles Laufwerk zur Wiederherstellung von Gastdateien oder Ordnern anschließen, muss die Ziel-VM für die Anbindung die Anmeldeinformationen konfiguriert haben, bevor Sie die Wiederherstellung durchführen.

Über diese Aufgabe

In der folgenden Tabelle sind die Anforderungen an Anmeldeinformationen für Wiederherstellungen von Gastspielen aufgeführt.

	Benutzerzugriffssteuerung aktiviert	**Die Benutzerzugriffssteuerung ist deaktiviert**
Domain-Benutzer	Ein Domain-User mit „Administrator“ als Benutzername funktioniert. Zum Beispiel „NetApp\Administrator“. Ein Domain-Benutzer mit „xyz“ als Benutzername, der zu einer lokalen Administratorgruppe gehört, funktioniert jedoch nicht. Beispielsweise kann man nicht „NetApp\xyz“ verwenden.	Entweder funktioniert ein Domain-User mit „Administrator“ als Benutzername oder ein Domain-User mit „xyz“ als Benutzername, der zu einer lokalen Administratorgruppe gehört. Zum Beispiel „NetApp\Administrator“ oder „NetApp\xyz“.
Workgroup-Benutzer	Ein lokaler Benutzer mit „Administrator“, wie der Benutzername funktioniert. Ein lokaler Benutzer mit „xyz“ als Benutzername, der zu einer lokalen Administratorgruppe gehört, funktioniert jedoch nicht.	Entweder ein lokaler Benutzer mit „Administrator“ als Benutzername oder ein lokaler Benutzer mit „xyz“ als Benutzername, der zu einer lokalen Administratorgruppe gehört, funktioniert gut. Ein lokaler Benutzer mit „xyz“ als Benutzername, der nicht zur lokalen Administratorgruppe gehört, funktioniert jedoch nicht.

In den vorhergehenden Beispielen ist „NetApp“ der Dummy-Domain-Name und „xyz“ der dumme lokale Benutzername

Schritte

1. Wählen Sie im Fenster vSphere Client Shortcuts unter Plug-ins **SnapCenter Plug-in für VMware vSphere** aus.
2. Wählen Sie in der linken Navigation **Guest File Restore**.
3. Führen Sie im Abschnitt * Ausführen als Anmeldeinformationen* einen der folgenden Schritte aus:

Um dies zu tun…	**Do this…**
Verwenden Sie vorhandene Anmeldedaten	Wählen Sie eine der konfigurierten Anmeldeinformationen aus.

Um dies zu tun…	Do this…
Neue Anmeldedaten hinzufügen	a. Wählen Sie **Hinzufügen**. b. Geben Sie im Dialogfeld **Ausführen als Anmeldeinformationen** die Anmeldeinformationen ein. Für den Benutzernamen müssen Sie „Administrator“ eingeben. c. Wählen Sie **Select VM** aus, und wählen Sie dann im Dialogfeld **Proxy VM** eine VM aus. Wählen Sie **Speichern**, um zum Dialogfeld **Run As Credentials** zurückzukehren. Wählen Sie die VM aus, die zur Authentifizierung der Anmeldedaten verwendet werden soll.

Das SnapCenter Plug-in für VMware vSphere verwendet die ausgewählten Anmeldeinformationen zur Anmeldung an der ausgewählten VM.

4. Wählen Sie **Speichern**.

Verlängern Sie die Zeit für die Wiederherstellung von Gastdateien

Standardmäßig ist eine angeschlossene Gastdatei-Wiederherstellung VMDK für 24 Stunden verfügbar und wird automatisch getrennt. Sie können die Zeit auf der Seite **Gastkonfiguration** verlängern.

Über diese Aufgabe

Es ist vielleicht möglich, eine Wiederherstellungssitzung für Gastdateien zu erweitern, wenn Sie zu einem späteren Zeitpunkt zusätzliche Dateien oder Ordner aus der beigefügten VMDK wiederherstellen möchten. Da allerdings für die Wiederherstellung von Gastdateien viele Ressourcen verwendet werden, sollte die Sitzungsdauer nur gelegentlich verlängert werden.

Schritte

1. Wählen Sie im VMware vSphere-Client **Guest File Restore** aus.
2. Wählen Sie eine Sitzung zur Wiederherstellung einer Gastdatei aus, und klicken Sie dann in der Titelleiste des Gast-Sitzungsmonitors auf das Symbol Ausgewählte Gastsitzung erweitern.

   Die Sitzung wird um weitere 24 Stunden verlängert.

Szenario zur Wiederherstellung von Gastdateien, in denen Sie möglicherweise auftreten können

Beim Versuch, eine Gastdatei wiederherzustellen, kann es zu einem der folgenden Szenarien kommen.

Die Sitzung zur Wiederherstellung der Gastdatei ist leer

Dieses Problem tritt auf, wenn Sie eine Gastdateiwiederherstellungssitzung erstellen und während diese Sitzung aktiv war, wird das Gastbetriebssystem neu gestartet. Wenn diese Funktion eintritt, bleiben VMDKs im Gastbetriebssystem möglicherweise offline. Wenn Sie versuchen, die Sitzung zur Wiederherstellung der Gastdatei zu durchsuchen, ist die Liste leer.

Um das Problem zu beheben, legen Sie die VMDKs manuell wieder im Gastbetriebssystem online. Wenn die VMDKs online sind, wird in der Wiederherstellungssitzung der Gastdatei der korrekte Inhalt angezeigt.

Der Vorgang zum Wiederherstellen der Gastdatei schlägt fehl

Dieses Problem tritt auf, wenn Sie eine Wiederherstellung von Gastdateien starten, aber der Vorgang zum Anbinden der Festplatte schlägt fehl, obwohl VMware-Tools ausgeführt werden und die Zugangsdaten für das Gastbetriebssystem korrekt sind. In diesem Fall wird der folgende Fehler zurückgegeben:

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

Um das Problem zu beheben, starten Sie den Windows-Dienst für VMware-Tools auf dem Gastbetriebssystem neu, und wiederholen Sie dann den Wiederherstellungsvorgang für die Gastdatei.

Gast-E-Mail zeigt ???? Für den Dateinamen

Dieses Problem tritt auf, wenn Sie die Funktion zum Wiederherstellen von Gastdateien verwenden, um Dateien oder Ordner mit nicht-englischen Zeichen in den Namen wiederherzustellen und die E-Mail-Benachrichtigung „???????“ anzeigt. " Für die wiederhergestellten Dateinamen. Der E-Mail-Anhang enthält die Namen der wiederhergestellten Dateien und Ordner korrekt.

Backups werden nach dem Abbruch der Sitzung zur Wiederherstellung von Gastdateien nicht mehr getrennt

Dieses Problem tritt auf, wenn Sie eine Gastdatei über ein VM-konsistentes Backup wiederherstellen. Während die Wiederherstellungssitzung für die Gastdatei aktiv ist, wird ein weiteres VM-konsistentes Backup für dieselbe VM durchgeführt. Wenn die Sitzung zur Wiederherstellung der Gastdatei getrennt wird, entweder manuell oder automatisch nach 24 Stunden, werden die Backups für die Sitzung nicht getrennt.

Um das Problem zu beheben, trennen Sie die VMDKs, die an die aktive Gastdateiwiederherstellungssitzung angeschlossen wurden, manuell.

Managen Sie das SnapCenter Plug-in für VMware vSphere Appliance

Starten Sie den VMware vSphere-Client-Service neu

Wenn sich der SnapCenter VMware vSphere Client falsch verhält, müssen Sie möglicherweise den Browser-Cache löschen. Wenn das Problem weiterhin besteht, starten Sie den Web-Client-Service neu.

Starten Sie den VMware vSphere-Client-Service in einem Linux-vCenter

Bevor Sie beginnen

Sie müssen vCenter 7.0U1 oder höher ausführen.

Schritte

1. Verwenden Sie SSH, um sich bei der vCenter Server Appliance als Root anzumelden.
2. Greifen Sie mit dem folgenden Befehl auf die Appliance-Shell oder DIE BASH-Shell zu:

   ```
   shell
   ```

3. Beenden Sie den Web-Client-Service mit dem folgenden HTML5-Befehl:

   ```
   service-control --stop vsphere-ui
   ```

4. Löschen Sie alle veralteten HTML5-Scvm-Pakete auf vCenter mithilfe des folgenden Shell-Befehls:

   ```
   etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/

   rm -rf com.netapp.scv.client-<version_number>
   ```

   Entfernen Sie die Pakete VASA oder vCenter 7.x und höher nicht.

5. Starten Sie den Web-Client-Dienst mit dem folgenden HTML5-Befehl:

   ```
   service-control --start vsphere-ui
   ```

Öffnen Sie die Wartungskonsole

Die Wartungskonsole für das SnapCenter Plug-in für VMware vSphere ermöglicht das Management Ihrer Applikations-, System- und Netzwerkkonfigurationen. Sie können Ihr Administratorpasswort, das Wartungspasswort, das Generieren von Support Bundles und das Starten der Remote Diagnostics ändern.

Bevor Sie beginnen

Bevor Sie das SnapCenter-Plug-in für den VMware vSphere-Dienst beenden und neu starten, sollten Sie alle Zeitpläne unterbrechen.

Über diese Aufgabe

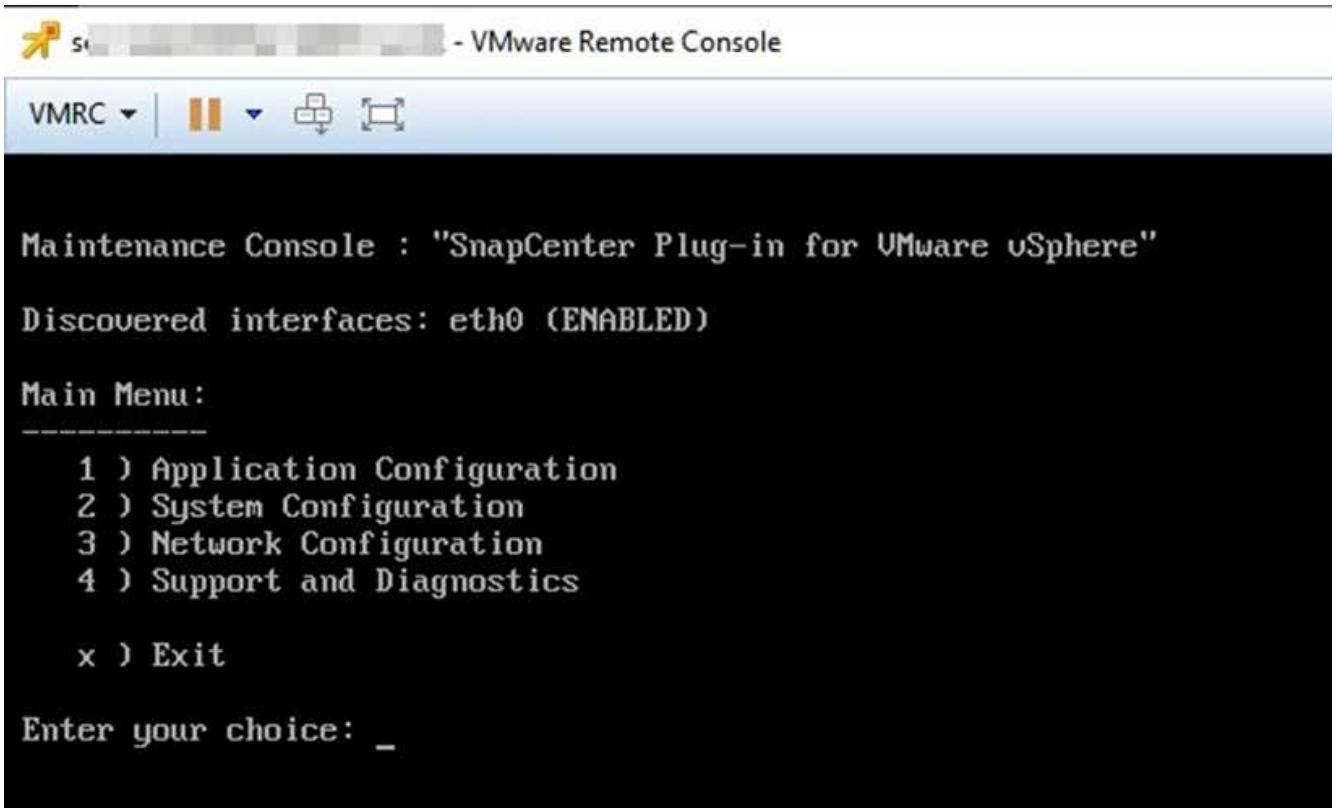
- Im SnapCenter-Plug-in für VMware vSphere 4.6P1 müssen Sie beim ersten Installieren des SnapCenter-Plug-ins für VMware vSphere ein Passwort angeben. Wenn Sie von Version 4.6 oder früher auf Version 4.6P1 oder höher aktualisieren, wird das frühere Standardpasswort akzeptiert.
- Sie müssen ein Passwort für den Benutzer „diag“ festlegen, während Sie die Ferndiagnose aktivieren.

  Um die Root-Benutzerberechtigung zum Ausführen des Befehls zu erhalten, verwenden Sie sudo <command>.

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter-Plug-in für VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remote Console starten** aus, um ein Fenster der Wartungskonsole zu öffnen.

   Melden Sie sich mit dem standardmäßigen Benutzernamen für die Wartungskonsole an `maint` Und das Passwort, das Sie bei der Installation festgelegt haben.



3. Sie können folgende Vorgänge durchführen:

   - Option 1: Anwendungskonfiguration

     Zusammenfassung des SnapCenter-Plug-ins für VMware vSphere anzeigen Starten oder Stoppen des SnapCenter-Plug-ins für VMware vSphere-Service Anmeldenamen oder Kennwort für SnapCenter-Plug-in für VMware vSphere ändern MySQL-Kennwort sichern und wiederherstellen, MySQL-Backups konfigurieren und auflisten

   - Option 2: Systemkonfiguration

Starten Sie die virtuelle Maschine neu
Fahren Sie die virtuelle Maschine herunter
Ändern Sie das Benutzerpasswort „Wartung“
Zeitzone ändern
NTP-Server ändern
Aktivieren Sie den SSH-Zugriff
Erhöhen der Größe der Jail-Festplatte (/jail)
Upgrade
Installation der VMware Tools
MFA-Token generieren

MFA ist immer aktiviert, Sie können MFA nicht deaktivieren.

- Option 3: Netzwerkkonfiguration

  Anzeigen oder Ändern von IP-Adresseinstellungen Anzeigen oder Ändern von Einstellungen für die Suche nach Domänennamen Anzeigen oder Ändern statischer Routen Übergeben von Änderungen Ping a Host

- Option 4: Support und Diagnose

  Support Bundle generieren Access Diagnostic Shell Remote-Zugriff für Diagnosezugriff erzeugen Core Dump Bundle generieren

Ändern Sie das Kennwort des SnapCenter-Plug-ins für VMware vSphere über die Wartungskonsole

Wenn Sie das Administratorkennwort für die Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere nicht kennen, können Sie über die Wartungskonsole ein neues Kennwort festlegen.

Bevor Sie beginnen

Bevor Sie das SnapCenter-Plug-in für VMware vSphere anhalten und neu starten, sollten Sie alle Zeitpläne unterbrechen.

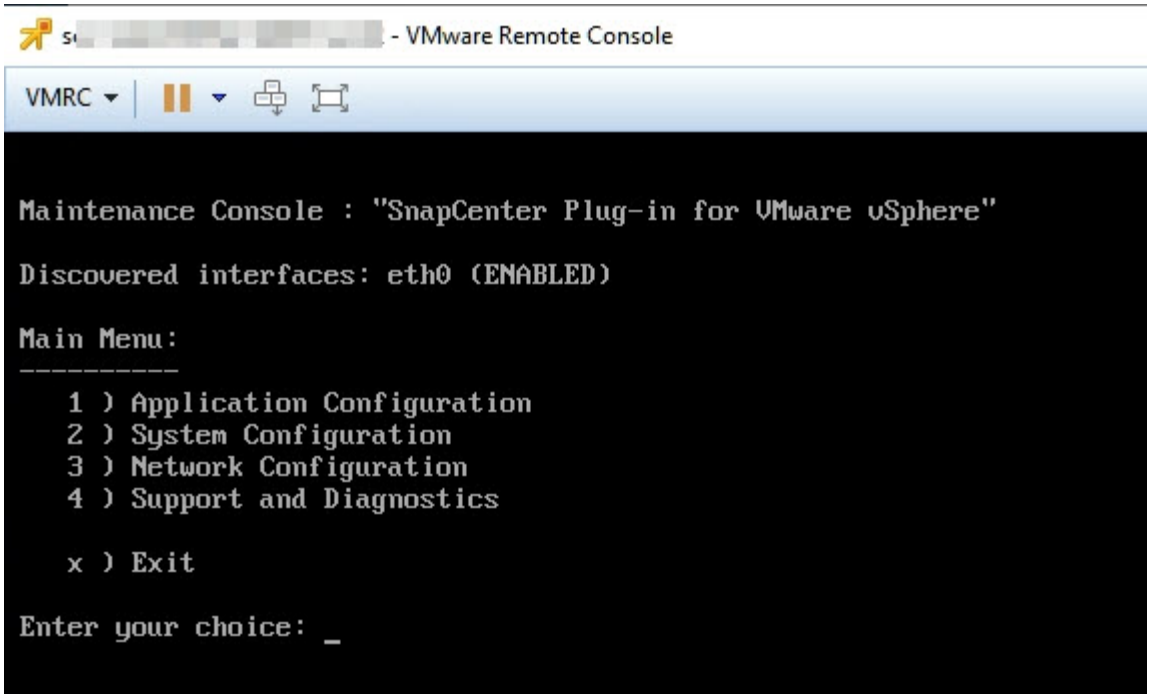
Über diese Aufgabe

Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter "Öffnen Sie die Wartungskonsole".

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter-Plug-in für VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remote Console starten** aus, um ein Fenster der Wartungskonsole zu öffnen, und melden Sie sich dann an.

   Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter "Öffnen Sie die Wartungskonsole".



3. Geben Sie „**1**“ für die Anwendungskonfiguration ein.
4. Geben Sie „**4**“ ein, um den Benutzernamen oder das Kennwort zu ändern.
5. Geben Sie das neue Passwort ein.

   Der Service der virtuellen SnapCenter VMware Appliance wird angehalten und gestartet.

Erstellen und Importieren von Zertifikaten

Das SnapCenter Plug-in für VMware vSphere verwendet SSL-Verschlüsselung zur sicheren Kommunikation mit dem Client-Browser. Während dies verschlüsselte Daten über das Netzwerk, die Erstellung eines neuen selbst signiertes Zertifikat, oder mit Ihrer eigenen Certificate Authority (CA) Infrastruktur oder eine Drittanbieter-CA ermöglicht, stellt sicher, dass das Zertifikat ist einzigartig für Ihre Umgebung.

Weitere Informationen finden Sie unter "KB-Artikel: Erstellen und/oder importieren Sie ein SSL-Zertifikat in SnapCenter Plug-in für VMware vSphere" .

Heben Sie das SnapCenter Plug-in für VMware vSphere vom vCenter ab

Wenn Sie den SnapCenter-Plug-in für VMware vSphere-Dienst in einem vCenter im verknüpften Modus beenden, sind Ressourcengruppen nicht in allen verknüpften vCenter verfügbar, selbst wenn der SnapCenter-Plug-in für VMware vSphere-Dienst in den anderen verknüpften vCenter ausgeführt wird.

Sie müssen die Registrierung des SnapCenter-Plug-ins für VMware vSphere-Erweiterungen manuell aufheben.

Schritte

1. Navigieren Sie auf dem Linked vCenter, bei dem der SnapCenter-Plug-in für VMware vSphere-Dienst angehalten ist, zum Manager Managed Object Reference (MOB).
2. Wählen Sie in der Option Eigenschaften in der Spalte Wert die Option **Inhalt** aus, und wählen Sie dann im nächsten Bildschirm in der Spalte Wert die Option **ExtensionManager** aus, um eine Liste der registrierten Erweiterungen anzuzeigen.
3. Deaktivieren Sie die Registrierung der Erweiterungen `com.netapp.scv.client` Und `com.netapp.aegis`.

Deaktivieren und aktivieren Sie das SnapCenter Plug-in für VMware vSphere

Wenn Sie die SnapCenter Datensicherungsfunktionen nicht mehr benötigen, müssen Sie die Konfiguration des SnapCenter-Plug-ins für VMware vSphere ändern. Wenn Sie beispielsweise das Plug-in in einer Testumgebung implementiert haben, müssen Sie die SnapCenter-Funktionen in dieser Umgebung möglicherweise deaktivieren und in einer Produktionsumgebung aktivieren.

Bevor Sie beginnen

- Sie müssen über Administratorrechte verfügen.
- Stellen Sie sicher, dass keine SnapCenter-Jobs ausgeführt werden.

Über diese Aufgabe

Wenn Sie das SnapCenter-Plug-in für VMware vSphere deaktivieren, werden alle Ressourcengruppen angehalten, und das Plug-in wird als Erweiterung in vCenter aufgehoben.

Wenn Sie das SnapCenter-Plug-in für VMware vSphere aktivieren, wird das Plug-in als Erweiterung in vCenter registriert, alle Ressourcengruppen befinden sich im Produktionsmodus und alle Zeitpläne sind aktiviert.

Schritte

1. Optional: Sichern Sie das SnapCenter Plug-in für VMware vSphere MySQL Repository, falls Sie es in einer neuen virtuellen Appliance wiederherstellen möchten.

   "Sichern Sie das SnapCenter Plug-in für VMware vSphere MySQL Datenbank".

2. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungsbenutzeroberfläche im Format `https://<OVA-IP-address>:8080` . Melden Sie sich mit dem zum Zeitpunkt der Bereitstellung festgelegten Administratorbenutzernamen und -kennwort sowie dem mithilfe der Wartungskonsole generierten MFA-Token an.

   Die IP-Adresse des SnapCenter-Plug-ins für VMware vSphere wird angezeigt, wenn Sie das Plug-in bereitstellen.

3. Wählen Sie im linken Navigationsbereich **Configuration** aus, und deaktivieren Sie dann die Option Service im Abschnitt **Plug-in Details**, um das Plug-in zu deaktivieren.
4. Bestätigen Sie Ihre Auswahl.
   - Wenn Sie das SnapCenter-Plug-in für VMware vSphere nur zum Durchführen von VM-konsistenten Backups verwendet haben

Das Plug-in ist deaktiviert, und es ist keine weitere Aktion erforderlich.

- Wenn Sie das SnapCenter Plug-in für VMware vSphere verwendet haben, um applikationskonsistente Backups durchzuführen

  Das Plug-in ist deaktiviert und eine weitere Bereinigung erforderlich.

  i. Melden Sie sich bei VMware vSphere an.
  ii. Schalten Sie die VM aus.
  iii. Klicken Sie im linken Navigationsbildschirm mit der rechten Maustaste auf die Instanz des SnapCenter-Plug-ins für VMware vSphere (den Namen der Datei, die bei der Bereitstellung der `.ova` virtuellen Appliance verwendet wurde), und wählen Sie **von Festplatte löschen** aus.
  iv. Melden Sie sich bei SnapCenter an und entfernen Sie den vSphere-Host.

Entfernen Sie das SnapCenter Plug-in für VMware vSphere

Wenn Sie die SnapCenter-Datenschutzfunktionen nicht mehr verwenden müssen, müssen Sie das SnapCenter-Plug-in für VMware vSphere deaktivieren, um die Registrierung von vCenter aufzuheben, dann das SnapCenter-Plug-in für VMware vSphere aus vCenter entfernen und die übrig gebliebenen Dateien manuell löschen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte verfügen.
- Stellen Sie sicher, dass keine SnapCenter-Jobs ausgeführt werden.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungsbenutzeroberfläche im Format `https://<OVA-IP-address>:8080`.

   Die IP-Adresse des SnapCenter-Plug-ins für VMware vSphere wird angezeigt, wenn Sie das Plug-in bereitstellen.

2. Wählen Sie im linken Navigationsbereich **Configuration** aus, und deaktivieren Sie dann die Option Service im Abschnitt **Plug-in Details**, um das Plug-in zu deaktivieren.
3. Melden Sie sich bei VMware vSphere an.
4. Klicken Sie im linken Navigationsbildschirm mit der rechten Maustaste auf die Instanz des SnapCenter-Plug-ins für VMware vSphere (den Namen der Datei, die bei der Bereitstellung der `.tar` virtuellen Appliance verwendet wurde), und wählen Sie **von Festplatte löschen** aus.
5. Wenn Sie mit dem SnapCenter Plug-in für VMware vSphere andere SnapCenter-Plug-ins für applikationskonsistente Backups unterstützt haben, melden Sie sich bei SnapCenter an, und entfernen Sie den vSphere-Host.

Nachdem Sie fertig sind

Die virtuelle Appliance wird weiterhin bereitgestellt, aber das SnapCenter Plug-in für VMware vSphere wird entfernt.

Nach dem Entfernen der Host-VM für das SnapCenter-Plug-in für VMware vSphere bleibt das Plug-in möglicherweise in vCenter aufgeführt, bis der lokale vCenter Cache aktualisiert wird. Da das Plug-in entfernt wurde, können auf diesem Host jedoch keine SnapCenter VMware vSphere Vorgänge durchgeführt werden.

Wenn Sie den lokalen vCenter-Cache aktualisieren möchten, stellen Sie zunächst sicher, dass sich die Appliance auf der Seite SnapCenter-Plug-in für VMware vSphere-Konfiguration in einem deaktivierten Zustand befindet, und starten Sie dann den vCenter-Webclientdienst neu.

Managen Sie Ihre Konfiguration

Ändern der Zeitzonen für Backups

Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldeinformationen für das SnapCenter Plug-in for VMware vSphere Verwaltungsbenutzeroberfläche kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

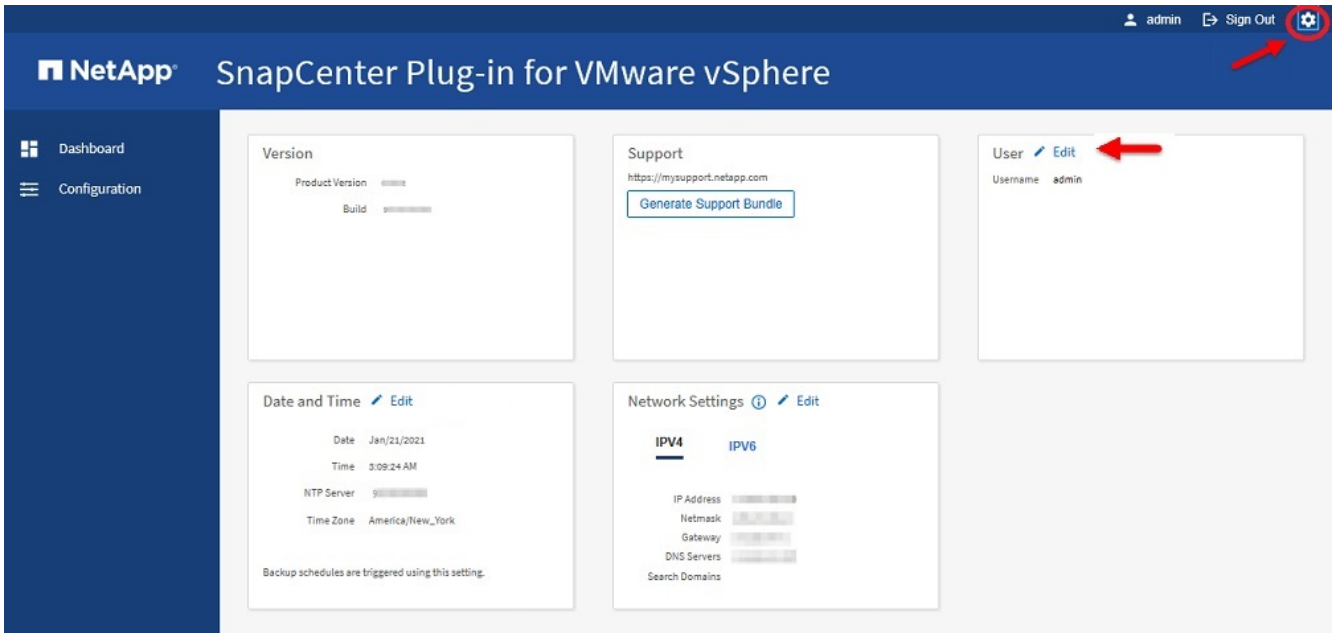
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere angezeigt.
- Verwenden Sie die Anmeldeinformationen, die während der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder später geändert wurden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

Schritte

1. Melden Sie sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

   Verwenden Sie das Format `https://<appliance-IP-address>:8080`

2. Wählen Sie das Symbol Einstellungen in der oberen Symbolleiste.



3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Datum und Uhrzeit Bearbeiten**.
4. Wählen Sie die neue Zeitzone aus und wählen Sie **Speichern**.

   Die neue Zeitzone wird für alle Backups verwendet, die vom SnapCenter-Plug-in für VMware vSphere durchgeführt werden.

Ändern der Anmeldeinformationen

Sie können die Anmeldeinformationen für die Verwaltungsbenutzeroberfläche des

SnapCenter Plug-in for VMware vSphere ändern.

Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldeinformationen für die Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

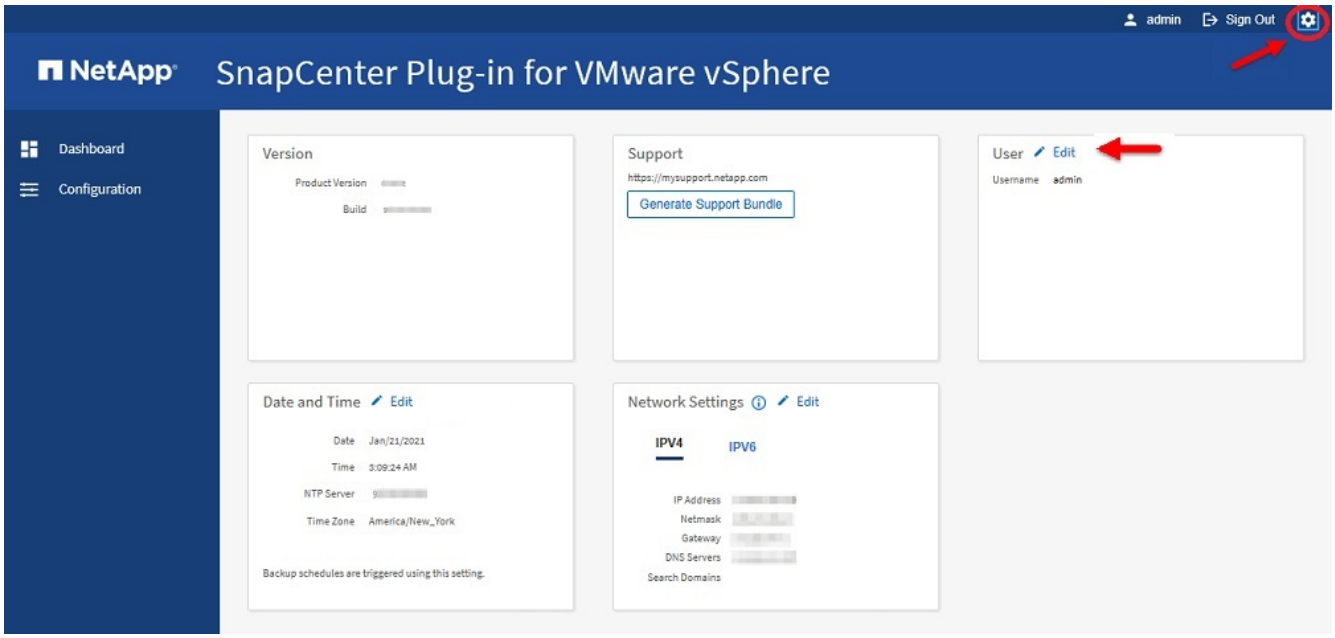
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere angezeigt.
- Verwenden Sie die Anmeldeinformationen, die während der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder später geändert wurden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

Schritte

1. Melden Sie sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

   Verwenden Sie das Format `https://<appliance-IP-address>:8080`

2. Wählen Sie das Symbol Einstellungen in der oberen Symbolleiste.



3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Benutzer Bearbeiten** aus.
4. Geben Sie das neue Passwort ein und wählen Sie **Speichern**.

   Es kann einige Minuten dauern, bis alle Dienste wieder verfügbar sind.

Ändern Sie die Anmeldedaten für vCenter-Anmeldung

Sie können die im SnapCenter-Plug-in für VMware vSphere konfigurierten Anmeldedaten für vCenter ändern. Diese Einstellungen werden vom Plug-in für den Zugriff auf vCenter genutzt.
Wenn Sie das vCenter-Passwort ändern, müssen Sie die Registrierung der ONTAP-Tools für VMware vSphere aufheben und es mit dem neuen Passwort erneut registrieren, damit

die vVol-Backups reibungslos funktionieren.

Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldeinformationen für die Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

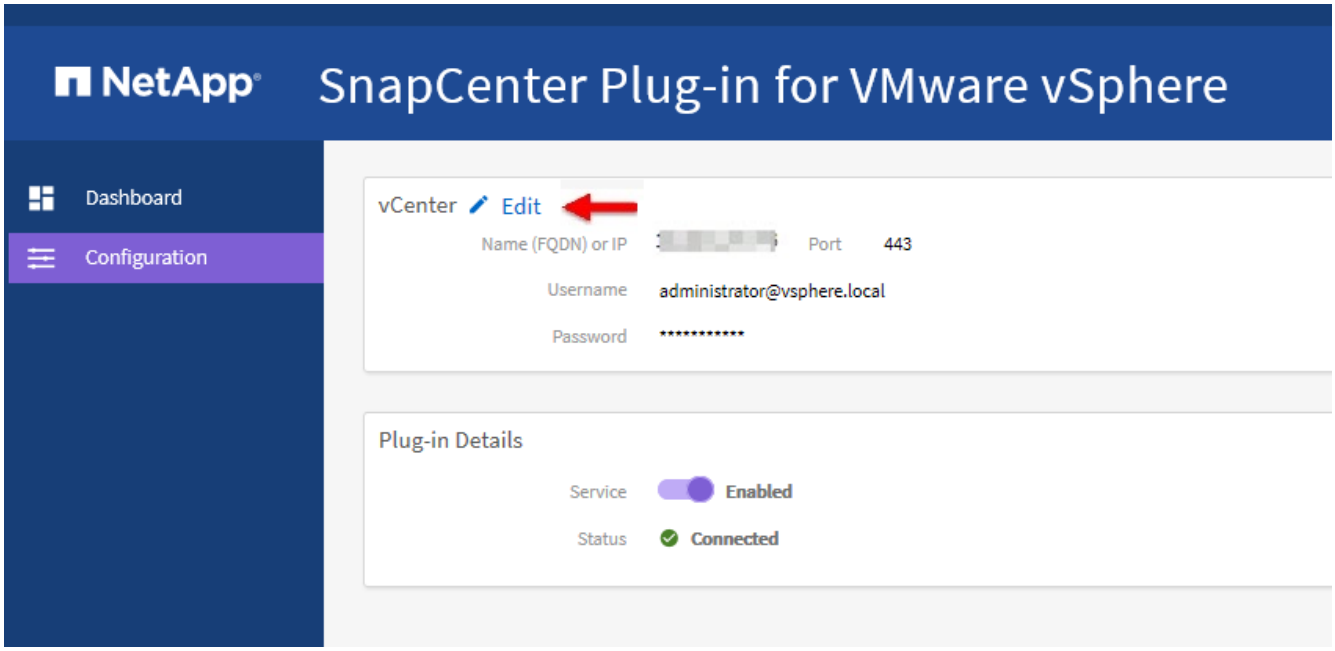
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere angezeigt.
- Verwenden Sie die Anmeldeinformationen, die während der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder später geändert wurden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

Schritte

1. Melden Sie sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

   Verwenden Sie das Format `https://<appliance-IP-address>:8080`

2. Wählen Sie im linken Navigationsbereich **Konfiguration** aus.



3. Wählen Sie auf der Seite **Konfiguration** im Abschnitt **vCenter Bearbeiten** aus.
4. Geben Sie das neue Passwort ein und wählen Sie dann **Speichern**.

   Ändern Sie die Portnummer nicht.

Ändern Sie die Netzwerkeinstellungen

Sie können die Netzwerkeinstellungen ändern, die im SnapCenter Plug-in für VMware vSphere konfiguriert sind. Diese Einstellungen werden vom Plug-in für den Zugriff auf vCenter genutzt.

Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldeinformationen für die Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

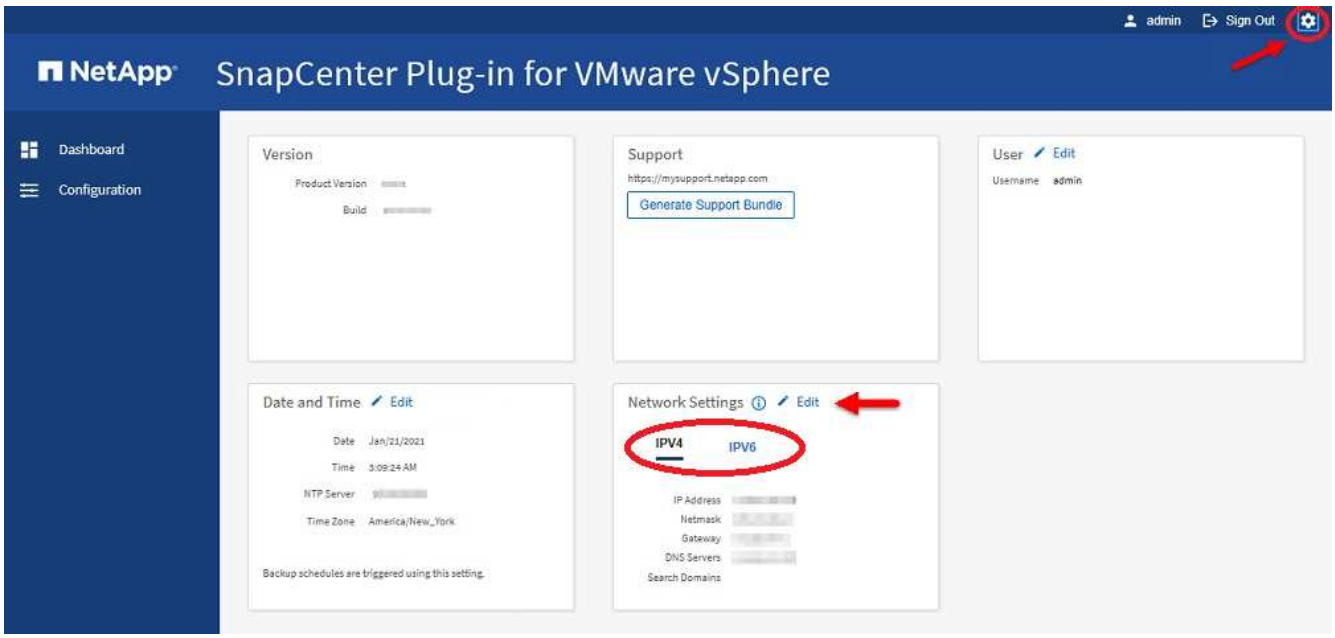
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere angezeigt.
- Verwenden Sie die Anmeldeinformationen, die während der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder später geändert wurden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

Schritte

1. Melden Sie sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

   Verwenden Sie das Format `https://<appliance-IP-address>:8080`

2. Wählen Sie das Symbol Einstellungen in der oberen Symbolleiste.



3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Netzwerkeinstellungen** die Option **IPv4** oder **IPv6** -Adresse aus und wählen Sie dann **Bearbeiten**.

   Geben Sie die neuen Informationen ein und wählen Sie **Speichern**.

4. Wenn Sie eine Netzwerkeinstellung entfernen, gehen Sie wie folgt vor:
   - IPv4: Geben Sie im Feld **IP-Adresse** ein `0.0.0.0` und wählen Sie dann **Speichern**.
   - IPv6: Geben Sie im Feld **IP-Adresse** ein `: :0`, und wählen Sie dann **Speichern**.

> Wenn Sie sowohl IPv4- als auch IPv6-Adressen verwenden, können Sie nicht beide Netzwerkeinstellungen entfernen. Das restliche Netzwerk muss die Felder DNS-Server und Suchdomänen angeben.

Ändern Sie die Standardwerte der Konfiguration

Zur Verbesserung der betrieblichen Effizienz können Sie die anpassen `scbr.override` Konfigurationsdatei zum Ändern der Standardwerte. Diese Werte steuern Einstellungen wie die Anzahl der während eines Backups erstellten oder gelöschten VMware Snapshots oder die Zeit, bis ein Backup-Skript nicht mehr ausgeführt wird.

Der `scbr.override` Das SnapCenter-Plug-in für VMware vSphere wird mit der Konfigurationsdatei in Umgebungen verwendet, die applikationsbasierte Datensicherungsvorgänge von SnapCenter unterstützen. Wenn diese Datei nicht vorhanden ist, müssen Sie sie aus der Vorlagendatei erstellen.

Erstellen Sie die Konfigurationsdatei scbr.override

Der `scbr.override` Das SnapCenter-Plug-in für VMware vSphere wird mit der Konfigurationsdatei in Umgebungen verwendet, die applikationsbasierte Datensicherungsvorgänge von SnapCenter unterstützen.

1. Gehen Sie zu `/opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.override-template`.
2. Kopieren Sie die `scbr.override-template` Datei zu einer neuen Datei namens `scbr.override` Im `\opt\netapp\scvservice\standalone_aegis\etc\scbr` Verzeichnis.

Eigenschaften, die Sie überschreiben können

Sie können Eigenschaften verwenden, die im aufgeführt sind `scbr.override` Konfigurationsdatei zum Ändern der Standardwerte.

- Standardmäßig verwendet die Vorlage Hash-Symbol, um die Konfigurationseigenschaften zu kommentieren. Um einen Konfigurationswert mit einer Eigenschaft zu ändern, müssen Sie den entfernen `#` Zeichen.
- Sie müssen den Service auf dem SnapCenter Plug-in für VMware vSphere Host neu starten, damit die Änderungen wirksam werden.

Sie können die folgenden Eigenschaften verwenden, die in aufgeführt sind `scbr.override` Konfigurationsdatei zum Ändern der Standardwerte.

- **dashboard.protected.vm.count.interval=7**

  Gibt die Anzahl der Tage an, für die das Dashboard den VM-Schutzstatus anzeigt.

  Der Standardwert ist "7".

- **Deaktivier.schwächCiphers=true**

  Deaktiviert die folgenden Schwächler für den Kommunikationskanal zwischen SnapCenter Plug-in für VMware vSphere und SnapCenter, und alle weiteren Schwächler, die in aufgeführt sind `include.weakCiphers`: TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_HA256 TLS_DHE_RSA_HA256_MIT AES_128 128_CBC_SHA256 TLS_ECE_MIT RSA_HA256_AES_HA256

TLS_BCBC_HA256_MIT RSA_HA256_HABCBC_HA256_256 256 TLS_HA256_BCBC_HA256_AES_BCBC_HA256_HA256_128_AES_BCBC_BCBC_AES_B6_B6_B6_B6_BCBC_B6_B6_B6_B

- **Global.ds.exclusion.pattern**

  Gibt einen oder mehrere herkömmliche oder vVol Datastores an, die von Backup-Vorgängen ausgeschlossen werden sollen. Sie können die Datenspeicher mit jedem gültigen Java-regulären Ausdruck angeben.

  Beispiel 1: Der Ausdruck `global.ds.exclusion.pattern=.*21` Schließt Datenspeicher mit einem gemeinsamen Muster aus, z. B. `datastore21` Und `dstest21` Ausgeschlossen werden.

  Beispiel 2: Der Ausdruck `global.ds.exclusion.pattern=ds-.*|^vol123` Schließt alle Datenspeicher aus, die enthalten sind `ds-` (Beispiel `scvds-test`) Oder beginnen Sie mit `vol123`.

- **guestFileRestore.guest.operation.interval=5**

  Gibt das Zeitintervall in Sekunden an, das SnapCenter Plug-in für VMware vSphere zum Abschluss von Gastoperationen auf dem Gastsystem überwacht (Online-Festplatte und Restore-Dateien). Die gesamte Wartezeit wird von eingestellt `guestFileRestore.online.disk.timeout` Und `guestFileRestore.restore.files.timeout`.

  Der Standardwert ist "5".

- **GuestFileRestore.MonitorIntervall=30**

  Gibt das Zeitintervall in Minuten an, das das SnapCenter Plug-in für VMware vSphere für die Wiederherstellung abgelaufener Gastdateien überwacht. Jede Sitzung, die über die konfigurierte Sitzungszeit hinaus ausgeführt wird, wird getrennt.

  Der Standardwert ist "30".

- **GuestFileRestore.online.Disk.Timeout=100**

  Gibt die Zeit in Sekunden an, die das SnapCenter-Plug-in für VMware vSphere auf den Abschluss eines Online-Festplattenvorgangs auf einer Gast-VM wartet. Beachten Sie, dass es eine weitere 30-Sekunden-Wartezeit gibt, bevor das Plug-in abfragt, um den Online-Festplattenvorgang abgeschlossen zu haben.

  Der Standardwert ist "100".

- **GuestFileRestore.restore.files.Timeout=3600**

  Gibt die Zeit in Sekunden an, die das SnapCenter-Plug-in für VMware vSphere auf den Abschluss eines Wiederherstellungsvorgangs auf einer Gast-VM wartet. Wenn die Zeit überschritten wird, wird der Prozess beendet und der Job als fehlgeschlagen markiert.

  Der Standardwert ist "3600" (1 Stunde).

- **GuestFileRestore.robotcopy.Directory.Flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP**

  Gibt die zusätzlichen robocopy-Flags an, die beim Kopieren von Verzeichnissen während der Wiederherstellung von Gastdateien verwendet werden sollen.

Nicht entfernen `/NJH` Oder hinzufügen `/NJS` Weil dies das Parsen der Wiederherstellungsausgabe bricht.

Lassen Sie keine unbegrenzten Wiederholungen zu (durch Entfernen der `/R` Flag) weil dies zu endlosen Wiederholungen für fehlgeschlagene Kopien führen kann.

Die Standardwerte sind `"/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP"`.

- **GuestFileRestore.robotcopy.file.Flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP**

  Gibt die zusätzlichen robocopy-Flags an, die beim Kopieren einzelner Dateien während der Wiederherstellung von Gastdateien verwendet werden sollen.

  Nicht entfernen `/NJH` Oder hinzufügen `/NJS` Weil dies das Parsen der Wiederherstellungsausgabe bricht.

  Lassen Sie keine unbegrenzten Wiederholungen zu (durch Entfernen der `/R` Flag) weil dies zu endlosen Wiederholungen für fehlgeschlagene Kopien führen kann.

  Die Standardwerte sind `"/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP"`.

- **guestFileRestore.sessionTime=1440**

  Gibt die Zeit in Minuten an, zu der das SnapCenter Plug-in für VMware vSphere eine Wiederherstellungssitzung für Gastdateien aktiv hält.

  Der Standardwert ist "1440" (24 Stunden).

- **guestFileRestore.use.custom.online.disk.script=true**

  Gibt an, ob beim Erstellen von Sitzungen zur Wiederherstellung von Gastdateien ein benutzerdefiniertes Skript zum Einlegen von Datenträgern und Abrufen von Laufwerksbuchstaben verwendet werden soll. Das Skript muss sich unter befinden `[Install Path] \etc\guestFileRestore_onlineDisk.ps1`. Bei der Installation wird ein Standardskript bereitgestellt. Der Werte `[Disk_Serial_Number]`, `[Online_Disk_Output]`, und `[Drive_Output]` Werden im Skript während des Begleitprozesses ersetzt.

  Der Standardwert ist „false“.

- **include.esx.initiator.id.from.cluster=true**

  Gibt an, dass das SnapCenter-Plug-in für VMware vSphere iSCSI- und FCP-Initiator-IDs von allen ESXi-Hosts im Cluster in der Anwendung über VMDK-Workflows enthalten sollte.

  Der Standardwert ist „false“.

- **Include.schwächCiphers**

  Wenn `disable.weakCiphers` Ist auf festgelegt `true`, Gibt die schwachen Chiffren an, die Sie neben den schwachen Chiffren deaktivieren möchten `disable.weakCiphers` Deaktiviert standardmäßig.

- **Max.Concurrent.ds.Storage.query.count=15**

  Gibt die maximale Anzahl gleichzeitiger Anrufe an, die das SnapCenter-Plug-in für VMware vSphere am SnapCenter-Server durchführen kann, um den Speicherplatzbedarf für die Datastores zu ermitteln. Das Plug-in führt diese Aufrufe aus, wenn Sie den Linux-Dienst auf dem SnapCenter-Plug-in für VMware vSphere VM-Host neu starten.

- **nfs.Datastore.Mount.retry.count=3**

  Gibt die maximale Anzahl der Versuche an, die das SnapCenter-Plug-in für VMware vSphere versucht, ein Volume als NFS-Datastore in vCenter zu mounten.

  Der Standardwert ist "3".

- **nfs.datastore.mount.retry.delay=60000**

  Gibt die Zeit in Millisekunden an, die das SnapCenter-Plug-in für VMware vSphere zwischen den Versuchen wartet, ein Volume als NFS-Datastore in vCenter zu mounten.

  Der Standardwert ist "60000" (60 Sekunden).

- **script.virtual.machine.count.variable.name= VIRTUELLE_MASCHINEN**

  Gibt den Namen der Umgebungsvariable an, der die Anzahl der virtuellen Maschinen enthält. Sie müssen die Variable definieren, bevor Sie während eines Backup-Jobs benutzerdefinierte Skripte ausführen.

  BEISPIELSWEISE bedeutet VIRTUAL_MACHINES=2, dass zwei virtuelle Maschinen gesichert werden.

- **script.virtual.machine.info.variable.name=VIRTUAL_MACHINE.%s**

  Gibt den Namen der Umgebungsvariable an, die Informationen über die n. Virtuelle Maschine im Backup enthält. Sie müssen diese Variable festlegen, bevor Sie während einer Sicherung benutzerdefinierte Skripts ausführen.

  Beispielsweise liefert die Umgebungsvariable VIRTUAL_MACHINE.2 Informationen über die zweite virtuelle Maschine im Backup.

- * script.virtual.machine.info.format= %s *

  Stellt Informationen zur virtuellen Maschine bereit. Das Format für diese Informationen, das in der Umgebungsvariable festgelegt ist, ist Folgendes: `VM name|VM UUID| VM power state (on|off)|VM snapshot taken (true|false)|IP address(es)`

  Im Folgenden finden Sie ein Beispiel für die Informationen, die Sie bereitstellen können:

  ```
  VIRTUAL_MACHINE.2=VM 1|564d6769-f07d-6e3b-
  68b1f3c29ba03a9a|POWERED_ON||true|10.0.4.2
  ```

- **Storage.connection.Timeout=600000**

  Gibt den Zeitraum in Millisekunden an, den der SnapCenter-Server auf eine Antwort des Storage-Systems wartet.

  Der Standardwert ist "600000" (10 Minuten).

- **vmware.esx.ip.kernel.ip.map**

  Es gibt keinen Standardwert. Sie verwenden diesen Wert, um die ESXi-Host-IP-Adresse der VMkernel-IP-Adresse zuzuordnen. Standardmäßig verwendet das SnapCenter-Plug-in für VMware vSphere die Management-VMkernel-Adapter-IP-Adresse des ESXi-Hosts. Wenn das SnapCenter-Plug-in für VMware vSphere eine andere VMkernel-Adapter-IP-Adresse verwenden soll, müssen Sie einen Überschreibungswert angeben.

Im folgenden Beispiel ist die IP-Adresse des Management-VMkernel-Adapters 10.225.10.56. Das SnapCenter-Plug-in für VMware vSphere verwendet jedoch die angegebene Adresse 10.225.11.57 und 10.225.11.58. Und wenn die Management-VMkernel-Adapter-IP-Adresse 10.225.10.60 ist, verwendet das Plug-in die Adresse 10.225.11.61.

```
vmware.esx.ip.kernel.ip.map=10.225.10.56:10.225.11.57,10.225.11.58;
10.225.10.60:10.225.11.61
```

- **vmware.max.Concurrent.Snapshots=30**

  Gibt die maximale Anzahl gleichzeitiger VMware-Snapshots an, die das SnapCenter-Plug-in für VMware vSphere auf dem Server durchführt.

  Diese Zahl wird pro Datenspeicher geprüft und nur dann aktiviert, wenn für die Richtlinie „VM-konsistent“ ausgewählt ist. Wenn Sie absturzkonsistente Backups durchführen, gilt diese Einstellung nicht.

  Der Standardwert ist "30".

- **vmware.max.concurrent.snapshots.delete=30**

  Gibt die maximale Anzahl gleichzeitiger VMware-Snapshot-Löschvorgänge pro Datastore an, die das SnapCenter-Plug-in für VMware vSphere auf dem Server ausführt.

  Diese Nummer wird pro Datenspeicher geprüft.

  Der Standardwert ist "30".

- **vmware.query.unresolved.retry.count=10**

  Gibt die maximale Anzahl von Versuchen an, die das SnapCenter-Plug-in für VMware vSphere wiederholt versucht, eine Abfrage über nicht aufgelöste Volumes zu senden, weil „…Zeitlimit für das Abhalten von I/O…“ Fehler.

  Der Standardwert ist "10".

- **vmware.quiesce.retry.count=0**

  Gibt die maximale Anzahl von Versuchen an, die das SnapCenter-Plug-in für VMware vSphere wiederholt versucht, eine Abfrage über VMware-Snapshots zu senden, weil „…Zeitlimit für I/O-Zurückhaltung…“ Fehler während einer Sicherung.

  Der Standardwert ist „0“.

- **vmware.quiesce.retry.interval=5**

  Gibt die Zeitdauer in Sekunden an, die das SnapCenter-Plug-in für VMware vSphere zwischen dem Senden der Abfragen zum VMware-Snapshot „…Zeitlimit für das Abhalten von I/O…“ wartet. Fehler während einer Sicherung.

  Der Standardwert ist "5".

- **vmware.query.unresolved.retry.delay= 60000**

  Gibt die Zeit in Millisekunden an, die das SnapCenter-Plug-in für VMware vSphere zwischen dem Senden der Abfragen zu nicht aufgelösten Volumes wartet, da „…Zeitlimit für das Abhalten von I/O…“ Fehler. Dieser Fehler tritt auf, wenn ein VMFS-Datastore geklont wird.

Der Standardwert ist "60000" (60 Sekunden).

- **vmware.reconfig.vm.retry.count=10**

  Gibt die maximale Anzahl von Wiederholungen an, die das SnapCenter-Plug-in für VMware vSphere wiederholt versucht, eine Abfrage zur Neukonfiguration einer VM zu senden, da „…Zeitlimit für das Abhalten von I/O…“ Fehler.

  Der Standardwert ist "10".

- **vmware.reconfig.vm.retry.delay=30000**

  Gibt die maximale Zeit in Millisekunden an, die das SnapCenter-Plug-in für VMware vSphere zwischen dem Senden von Abfragen zur Neukonfiguration einer VM wartet, da „…Zeitlimit für die Einschränkung von I/O…“ Fehler.

  Der Standardwert ist "30000" (30 Sekunden).

- **vmware.Rescan.hba.retry.count=3**

  Gibt die Zeit in Millisekunden an, die das SnapCenter-Plug-in für VMware vSphere zwischen dem Senden der Abfragen zum erneuten Scannen des Host-Bus-Adapters wartet, da „…Zeitlimit für das Halten von I/O…“ Fehler.

  Der Standardwert ist "3".

- **vmware.rescan.hba.retry.delay=30000**

  Gibt die maximale Anzahl von Wiederholungen an, die das SnapCenter-Plug-in für VMware vSphere zum erneuten Scannen des Host-Bus-Adapters verwendet.

  Der Standardwert ist "30000".

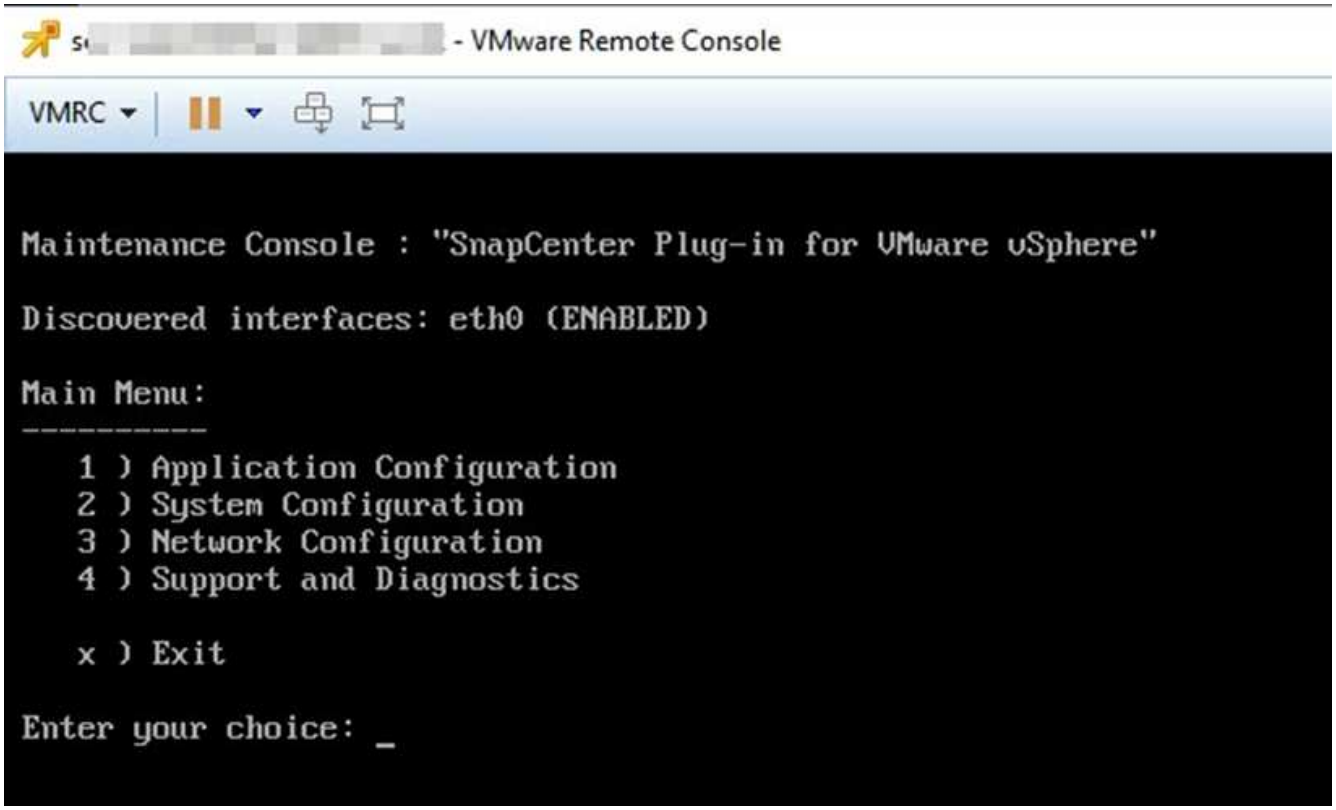
Aktivieren Sie das SSH for SnapCenter Plug-in für VMware vSphere

Wenn das SnapCenter-Plug-in für VMware vSphere bereitgestellt wird, ist SSH standardmäßig deaktiviert.

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter-Plug-in für VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remote Console starten** aus, um ein Fenster der Wartungskonsole zu öffnen, und melden Sie sich dann an.

   Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter "Öffnen Sie die Wartungskonsole".



3. Wählen Sie im Hauptmenü die Menüoption **2) Systemkonfiguration**.
4. Wählen Sie im Menü Systemkonfiguration die Menüoption **6) SSH-Zugriff aktivieren** und geben Sie dann an der Bestätigungsaufforderung „**y**“ ein.
5. Warten Sie auf die Meldung „SSH Access aktivieren…“ Drücken Sie dann **Enter**, um fortzufahren, und geben Sie dann **X** an der Eingabeaufforderung ein, um den Wartungsmodus zu beenden.

Rest-APIs

Überblick

Sie können das SnapCenter Plug-in für VMware vSphere REST-APIs verwenden, um allgemeine Datensicherungsvorgänge auszuführen. Das Plug-in hat verschiedene Swagger-Webseiten von den Windows SnapCenter-Swagger-Webseiten.

- REST-API-Workflows werden für folgende Operationen auf VMs und Datastores dokumentiert. Dazu verwendet die REST-APIs für VMware vSphere:
  - Fügen Sie Storage-VMs und -Cluster hinzu, ändern oder löschen Sie sie
  - Ressourcengruppen erstellen, ändern und löschen
  - Backup von geplanten und On-Demand-VMs
  - Wiederherstellung vorhandener VMs und gelöschter VMs
  - Wiederherstellung von VMDKs
  - Anschließen und Trennen von VMDKs
  - Mounten und Unmounten von Datastores
  - Laden Sie Jobs herunter und erstellen Sie Berichte
  - Integrierte Zeitpläne ändern
  - Konfigurieren Sie den sekundären Schutz für ASA r2
- Operationen, die von DEN REST-APIs für VMware vSphere nicht unterstützt werden
  - Wiederherstellung von Gastdateien
  - Installation und Konfiguration des SnapCenter Plug-ins für VMware vSphere
  - Weisen Sie Benutzern RBAC-Rollen oder -Zugriff zu
- `uri` Parameter

  Der `uri` Parameter gibt immer einen Wert von „Null“ zurück.

- Zeitüberschreitung bei der Anmeldung

  Die standardmäßige Zeitüberschreitung beträgt 120 Minuten (2 Stunden). In den vCenter-Einstellungen können Sie einen anderen Timeout-Wert konfigurieren.

- Token-Management

  REST-APIs verwenden aus Sicherheitsgründen ein obligatorisches Token, das mit jeder Anforderung übergeben wird und in allen API-Aufrufen zur Client-Validierung verwendet wird. DIE REST-APIs für VMware vSphere erhalten das Token mithilfe der VMware-Authentifizierungs-API. VMware stellt das Token-Management bereit.

  Um das Token zu erhalten, verwenden Sie `/4.1/auth/login` REST API und Bereitstellung der vCenter Anmeldedaten.

- API-Versionsbezeichnungen

  Jeder REST-API-Name enthält die SnapCenter-Versionsnummer, in der die REST-API zum ersten Mal

freigegeben wurde. Zum Beispiel die REST API `/4.1/datastores/{moref}/backups` Wurde erstmals im SnapCenter 4.1 veröffentlicht.

REST-APIs in zukünftigen Versionen werden in der Regel abwärtskompatibel sein und je nach Bedarf an neuen Funktionen angepasst werden.

Greifen Sie über die Swagger API-Webseite auf REST-APIs zu

REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um entweder den SnapCenter-Server oder das SnapCenter-Plug-in für VMware vSphere REST-APIs anzuzeigen und einen API-Aufruf manuell auszuführen. Verwenden Sie das SnapCenter Plug-in für VMware vSphere REST-APIs, um VMs und Datastores zu steuern.

Das Plug-in hat verschiedene Swagger-Webseiten von den SnapCenter-Serverdolch-Webseiten.

Bevor Sie beginnen

Um auf das SnapCenter Plug-in for VMware vSphere REST-APIs zuzugreifen, stellen Sie sicher, dass Sie über die IP-Adresse oder den Hostnamen des SnapCenter Plug-in for VMware vSphere verfügen.

Das Plug-in unterstützt nur REST APIs zur Integration mit Applikationen anderer Anbieter. PowerShell Commandlets oder CLI werden nicht unterstützt.

Schritte

1. Geben Sie in einem Browser die URL ein, um auf die Plug-in Swagger Webseite zuzugreifen:

   `https://<SCV_IP>:8144/api/swagger-ui/index.html`

   Verwenden Sie nicht die folgenden Zeichen in DER REST-API-URL: +, . , % Und &.

   Beispiel

   Access SnapCenter Plug-in für VMware vSphere REST-APIs:

   `https://<SCV_IP>:8144/api/swagger-ui/index.html`

   `https://OVAhost:8144/api/swagger-ui/index.html`

   Melden Sie sich mit dem vCenter-Authentifizierungsmechanismus an, um das Token zu generieren.

2. Wählen Sie einen API-Ressourcentyp aus, um die APIs in diesem Ressourcentyp anzuzeigen.

REST-API-Workflows zum Hinzufügen und Ändern von Storage-VMs

Zum Hinzufügen und Ändern von Storage-VM-Vorgängen mit dem SnapCenter Plug-in für VMware vSphere REST-APIs müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

So fügen Sie Storage-VM-Vorgänge hinzu:

Schritt	REST API	Kommentare
1	`/4.1/storage-system`	`Add Storage System` Fügt die angegebene Storage-VM zum SnapCenter-Plug-in für VMware vSphere hinzu.

Führen Sie den folgenden Workflow aus, um Vorgänge für Storage-VMs zu ändern:

Schritt	REST API	Kommentare
1	`/4.1/storage-system`	`getSvmAll` Ruft die Liste aller verfügbaren Storage VMs ab. Beachten Sie den **Namen** der Speicher-VM, die Sie ändern möchten.
2	`/4.1/storage-system`	`Modify Storage System` Ändert die angegebene Storage-VM. Übergeben Sie den **Name** aus Schritt 1 zusätzlich zu allen anderen erforderlichen Attributen.

REST-API-Workflows zum Erstellen und Ändern von Ressourcengruppen

Zum Erstellen und Ändern von Gruppenoperationen über das SnapCenter Plug-in für VMware vSphere REST-APIs müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Gehen Sie zum Erstellen von Ressourcengruppen wie folgt vor:

Schritt	REST API	Kommentare
1	`/4.1/policies`	`Get Policies` Ruft die Liste der VMware vSphere Client-Richtlinien ab. Beachten Sie die **RichtlinieID**, die Sie beim Erstellen der Ressourcengruppe und der Richtlinie **Frequency** verwenden möchten. Wenn keine Richtlinien aufgeführt sind, verwenden Sie das `Create Policy` REST API zur Erstellung einer neuen Richtlinie

Schritt	REST API	Kommentare
2	`/4.1/resource-groups`	`Create a Resource Group` Erstellt eine Ressourcengruppe mit der angegebenen Richtlinie. Geben Sie die **RichtlinieID** aus Schritt 1 ein und geben Sie zusätzlich zu allen anderen erforderlichen Attributen die Richtlinie **Frequenz** -Details ein. Sie können den sekundären Schutz mit dieser REST-API aktivieren.

Gehen Sie wie folgt vor, um Ressourcengruppen zu ändern:

Schritt	REST API	Kommentare
1	`/4.1/resource-groups`	`Get List of Resource Groups` Ruft die Liste der VMware vSphere Client Ressourcengruppen ab. Beachten Sie die **resourceGroupID**, die Sie ändern möchten.
2	`/4.1/policies`	Wenn Sie die zugewiesenen Richtlinien ändern möchten, `Get Policies` Ruft die Liste der VMware vSphere Client-Richtlinien ab. Beachten Sie die **Policy ID**, die Sie beim Ändern der Ressourcengruppe und der Richtlinie **Frequency** verwenden möchten.
3	`/4.1/resource-groups/{resouceGroupId}`	`Update a Resource Group` Ändert die angegebene Ressourcengruppe. Übergeben Sie die **resourceGroupID** von Schritt 1. Übergeben Sie optional die **policyID** aus Schritt 2 und geben Sie zusätzlich zu allen anderen erforderlichen Attributen die **Frequency**-Details ein.

REST-API-Workflow für Backup nach Bedarf

Um Backup-Vorgänge On-Demand mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Schritt	REST API	Kommentare
1	`/4.1/resource-groups`	`Get List of Resource Groups` Ruft die Liste der VMware vSphere Client Ressourcengruppen ab. Beachten Sie die **resourceGroupID** und die **Policy ID** für die Ressourcengruppe, die Sie sichern möchten.
2	`/4.1/resource-groups/backupnow`	`Run a backup on a Resource Group` Sichert die Ressourcengruppe nach Bedarf. Übergeben Sie die **resourceGroupID** und die **policyId** aus Schritt 1.

REST-API-Workflow zur Wiederherstellung von VMs

Um VM-Backups mit dem SnapCenter Plug-in for VMware vSphere REST-APIs wiederherzustellen, befolgen Sie die erforderliche Abfolge von REST-API-Aufrufen, wie unten beschrieben.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Schritt	REST API	Kommentare
1	Gehen Sie zu `http://<vCenter-IP>/mob`	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den **moref** für die VM, die Sie wiederherstellen möchten.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` Ruft eine Liste von Backups für die angegebene VM ab. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **Backupid** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations` Ruft den Speicherort des Snapshots für das angegebene Backup ab. Übergeben Sie die **Backupid** aus Schritt 2. Beachten Sie die **snapshotStandorteList** Informationen.

Schritt	REST API	Kommentare
4	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts` Ruft die Informationen für den Host ab, auf dem das Backup gespeichert ist. Beachten Sie die **verfügbarEsxHostsList** Informationen.
5	`/4.1/vm/{moref}/backups/{backupId}/restore`	`Restore a VM from a backup` Stellt das angegebene Backup wieder her. Geben Sie die Informationen aus den Schritten 3 und 4 im Attribut **restoreLocations** weiter. Wenn es sich bei der VM-Sicherung um ein partielles Backup handelt, legen Sie den fest `restartVM` Parameter auf „false“. Sie können keine VM wiederherstellen, die eine Vorlage ist.

REST-API-Workflow zur Wiederherstellung gelöschter VMs

Um die Restore-Vorgänge für VM-Backups mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Schritt	REST API	Kommentare
1	Gehen Sie zu `http://<vCenter-IP>/mob`	Suchen Sie die VM-UUID aus der URL der von VMware gemanagten Objekte. Beachten Sie die **UUID** für die VM, die Sie wiederherstellen möchten.

Schritt	REST API	Kommentare
2	`/4.1/vm/{uuid}/backups`	`Get VM Backups` Ruft eine Liste von Backups für die angegebene VM ab. Geben Sie die **UUID** von Schritt 1. Beachten Sie die **Backupid** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations` Ruft den Speicherort des Snapshots für das angegebene Backup ab. Übergeben Sie die **Backupid** aus Schritt 2. Beachten Sie die **snapshotStandorteList** Informationen.
4	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts` Ruft die Informationen für den Host ab, auf dem das Backup gespeichert ist. Beachten Sie die **verfügbarEsxHostsList** Informationen.
5	`/4.1/vm/{uuid}/backups/{backupId}/restore`	`Restore VM from a backup using uuid or restore a deleted VM` Stellt das angegebene Backup wieder her. Geben Sie die **UUID** von Schritt 1. Übergeben Sie die **Backupid** aus Schritt 2. Geben Sie die Informationen aus den Schritten 3 und 4 im Attribut **restoreLocations** weiter. Wenn es sich bei der VM-Sicherung um ein partielles Backup handelt, legen Sie den fest `restartVM` Parameter auf „false“. **Hinweis:** eine VM, die eine Vorlage ist, kann nicht wiederhergestellt werden.

REST-API-Workflow zur Wiederherstellung von VMDKs

Um Restore-Vorgänge für VMDKs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Schritt	REST API	Kommentare
1	Gehen Sie zu `http://<vCenter-IP>/mob`	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den **moref** für die VM, in der sich die VMDK befindet.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` Ruft eine Liste von Backups für die angegebene VM ab. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **Backupid** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations` Ruft den Speicherort des Snapshots für das angegebene Backup ab. Übergeben Sie die **Backupid** aus Schritt 2. Beachten Sie die **snapshotStandorteList** Informationen.
4	`/4.1/vm/{moref}/backups/vmdklocations`	`Get Vmdk Locations` Ruft eine Liste von VMDKs für die angegebene VM ab. Beachten Sie die **vmdk-StandorteList** -Informationen.
5	`/4.1/vm/{ moref}/backups/{backupId}/availabledatastores`	`Get Available Datastores` Ruft eine Liste von Datenspeichern ab, die für den Wiederherstellungsvorgang verfügbar sind. Übergeben Sie den **moref** von Schritt 1. Übergeben Sie die **Backupid** aus Schritt 2. Beachten Sie die **DatastoreNameList**-Informationen.
6	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts` Ruft die Informationen für den Host ab, auf dem das Backup gespeichert ist. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **verfügbarEsxHostsList** Informationen.

Schritt	REST API	Kommentare
7	`/4.1/vm/{moref}/backups/{backupId}/restorevmdks`	`Restore a VMDK from a backup` Stellt die angegebene VMDK aus dem angegebenen Backup wieder her. Geben Sie im Attribut **esxHost** die Informationen aus **availEsxHostsList** in Schritt 6 weiter. Geben Sie die Informationen von den Schritten 3 bis 5 an das Attribut **VMDKs RestoreLocations** weiter: • Geben Sie im Attribut RestoresFromLocation die Informationen aus snapshotStandorteList in Schritt 3 weiter. • Geben Sie im Attribut VMDKs-ToRestore die Informationen aus VMDKs-StandorteList in Schritt 4 weiter. • Geben Sie im Attribut restoreToDatastore die Informationen aus DatastoreNameList in Schritt 5 weiter.

REST-API-Workflows zum Verbinden und Trennen von VMDKs

Um mithilfe des SnapCenter Plug-ins für VMware vSphere REST-APIs Verbindungen zu und Abtrennen von VMDKs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Gehen Sie wie folgt vor, um VMDKs anzuhängen:

Schritt	REST API	Kommentare
1	Gehen Sie zu `http://<vCenter-IP>/mob`	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den **moref** für die VM, an die Sie eine VMDK anhängen möchten.

Schritt	REST API	Kommentare
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` Ruft eine Liste von Backups für die angegebene VM ab. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **Backupid** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/{moref}/backups/{backupId}/vmdklocations`	`Get VMDK Locations` Ruft eine Liste von VMDKs für die angegebene VM ab. Bestehen Sie die **Backupid** aus Schritt 2 und den **moref** aus Schritt 1. Beachten Sie die **vmdk-StandorteList** -Informationen.
4	`/4.1/vm/{moref}/attachvmdks`	`Attach VMDKs` Fügt die angegebene VMDK an die ursprüngliche VM an. Bestehen Sie die **Backupid** aus Schritt 2 und den **moref** aus Schritt 1. Geben Sie die **VMDKs StandorteListe** von Schritt 3 bis zum Attribut **VMDKs Locations** weiter. Um eine VMDK an eine andere VM anzuhängen, übergeben Sie den moref der Ziel-VM im altersVmMoref Attribut.

Gehen Sie zum Trennen von VMDKs wie folgt vor:

Schritt	REST API	Kommentare
1	Gehen Sie zu `http://<vCenter-IP>/mob`	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den **moref** für die VM, auf der Sie eine VMDK abtrennen möchten.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` Ruft eine Liste von Backups für die angegebene VM ab. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **Backupid** des Backups, das Sie wiederherstellen möchten.

Schritt	REST API	Kommentare
3	`/4.1/vm/{moref}/backups/{backupId}/vmdklocations`	`Get VMDK Locations` Ruft eine Liste von VMDKs für die angegebene VM ab. Bestehen Sie die **Backupid** aus Schritt 2 und den **moref** aus Schritt 1. Beachten Sie die **vmdk-StandorteList** -Informationen.
4	`/4.1/vm/{moref}/detachvmdks`	`Detach VMDKs` Trennt die angegebene VMDK. Übergeben Sie den **moref** von Schritt 1. Geben Sie die VMDK **vmdk-StandorteListe** Details von Schritt 3 bis zum **VMDKs ToDetach** -Attribut.

REST-API-Workflows zum Mounten und Unmounten von Datastores

Um Mount- und Unmount-Vorgänge für Datastore-Backups mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Folgen Sie zum Mounten von Datastores diesem Workflow:

Schritt	REST API	Kommentare
1	Gehen Sie zu `http://<vCenter-IP>/mob`	Suchen Sie den Datastore-moref aus der URL von VMware Managed Objects. Beachten Sie den **moref** für den Datastore, den Sie mounten möchten.
2	`/4.1/datastores/{moref}/backups`	`Get the list of backups for a datastore` Ruft eine Liste von Backups für den angegebenen Datastore ab. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **Backupid**, die Sie montieren möchten.

Schritt	REST API	Kommentare
3	`/4.1/datastores/backups/{backupId}/snapshotlocators`	`Get the list of Snapshot Locations` Ruft Details zum Speicherort des angegebenen Backups ab. Übergeben Sie die **Backupid** aus Schritt 2. Beachten Sie den **Datastore** und den Standort aus der Liste **snapshotStandorteList**.
4	`/4.1/datastores/{moref}/availableEsxHosts`	`Get the list of Available Esxi Hosts` Ruft die Liste der ESXi Hosts ab, die für Mount-Vorgänge verfügbar sind. Übergeben Sie den **moref** von Schritt 1. Beachten Sie die **verfügbarEsxHostsList** Informationen.
5	`/4.1/datastores/backups/{backupId}/mount`	`Mount datastores for a backup` Bindet das angegebene Datastore-Backup ein. Übergeben Sie die **Backupid** aus Schritt 2. Geben Sie die Informationen in den Attributen **Datastore** und **location** an `snapshotLocationsList` In Schritt 3. Geben Sie im Attribut **esxHostName** die Informationen aus **availEsxHostsList** in Schritt 4 weiter.

Folgen Sie zum Unmounten von Datastores diesem Workflow:

Schritt	REST API	Kommentare
1	`/4.1/datastores/backups/{backupId}/mounted`	`Get the list of mounted datastores`. Beachten Sie den Datenspeicher **moref**(s), den Sie unmounten möchten.
2	`/4.1/datastores/unmount`	`UnMount datastores for a backup` Hängt das angegebene Datastore-Backup ab. Übergeben Sie den Datenspeicher **moref**(s) aus Schritt 1.

REST-APIs zum Herunterladen von Jobs und zum Generieren von Berichten

Zum Generieren von Berichten und Herunterladen von Protokollen für VMware vSphere Client-Jobs mithilfe des SnapCenter Plug-ins für VMware vSphere REST-APIs müssen SIE DIE REST-API-Aufrufe für VMware vSphere verwenden.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Verwenden Sie die folgenden REST-APIs im Abschnitt Jobs, um detaillierte Informationen über Jobs zu erhalten:

REST API	Kommentare
`/4.1/jobs`	`Get all jobs` Ruft die Job-Details für mehrere Jobs ab. Sie können den Umfang der Anforderung eingrenzen, indem Sie einen Jobtyp angeben, z. B. `backup`, `mountBackup`, Oder `restore`.
`/4.1/jobs/{id}`	`Get job details` Ruft detaillierte Informationen für den angegebenen Job ab.

Verwenden Sie die folgende REST-API im Abschnitt Jobs zum Herunterladen von Jobprotokollen:

REST API	Kommentare
`/4.1/jobs/{id}/logs`	`getJobLogsById` lädt die Protokolle für den angegebenen Job herunter.

Verwenden Sie die folgenden REST-APIs im Abschnitt Berichte zum Generieren von Berichten:

REST API	Kommentare
`4.1/reports/protectedVM`	`Get Protected VM List` Erhalten Sie in den letzten sieben Tagen eine Liste der geschützten VMs.
`/4.1/reports/unProtectedVM`	`Get Unprotected VM List` Erhalten eine Liste der ungeschützten VMs in den letzten sieben Tagen.

REST-API-Workflow zum Ändern integrierter Zeitpläne

Um integrierte Zeitpläne für VMware vSphere Client-Jobs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs zu ändern, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Integrierte Zeitpläne sind die Zeitpläne, die als Teil des Produkts bereitgestellt werden, z. B. der Zeitplan für den MySQL-Datenbank-Dump. Sie können die folgenden Zeitpläne ändern:
`Schedule-DatabaseDump`
`Schedule-PurgeBackups`
`Schedule-AsupDataCollection`
`Schedule-ComputeStorageSaving`
`Schedule-PurgeJobs`

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Schritt	REST API	Kommentare
1	`/4.1/schedules`	`Get all built-in` Zeitpläne erhalten eine Liste der Jobpläne, die ursprünglich im Produkt bereitgestellt wurden. Notieren Sie sich den Planungsnamen, den Sie ändern möchten, und den zugeordneten cron-Ausdruck.
2	`/4.1/schedules`	`Modify any built-in schedule` Ändert den benannten Zeitplan. Übergeben Sie den Planungsnamen aus Schritt 1 und erstellen Sie einen neuen cron-Ausdruck für den Zeitplan.

REST-API zum Markieren von eingeklemmten Jobs als fehlgeschlagen

Um Job-IDs für VMware vSphere-Client-Jobs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs zu finden, müssen DIE REST-API-Aufrufe für VMware vSphere verwendet werden. Diese REST-APIs wurden im SnapCenter Plug-in für VMware vSphere 4.4 hinzugefügt.

Fügen Sie für jede REST-API https://<server>:<port>` an der Vorderseite der REST-API hinzu, um einen vollständigen Endpunkt zu bilden.

Verwenden Sie die folgende REST-API im Abschnitt Jobs, um Jobs zu ändern, die sich in einem laufenden Zustand befinden, in einen fehlgeschlagenen Status:

REST API	Kommentare
`/4.1/jobs/{id}/failJobs`	Wenn Sie die IDs von Jobs übergeben, die im laufenden Zustand hängen bleiben, `failJobs` markiert diese Jobs als fehlgeschlagen. Um Jobs zu identifizieren, die im laufenden Status hängen geblieben sind, verwenden Sie die Benutzeroberfläche des Job-Monitors, um den Status jedes Jobs und die Job-ID anzuzeigen.

REST-APIs zur Erstellung von Prüfprotokollen

Sie können die Audit-Log-Details von Swagger Rest APIs sowie die SCV Plugin-Benutzeroberfläche sammeln.

Unten sind die Swagger Rest APIs angegeben:

1. ERHALTEN Sie 4.1/Audit/Logs: Erhalten Sie Audit-Daten für alle Protokolle
2. GET 4.1/Audit/logs/{filename}: Get Audit-Daten für eine bestimmte Protokolldatei

3. NACH 4.1/Audit/Verify: Prüfung des Prüfprotokolls auslösen
4. GET 4.1/Audit/config: Get the Audit and syslog Server config
5. PUT 4.1/Audit/config: Aktualisieren Sie die Audit- und syslog-Server-Konfiguration

Um Prüfprotokolle für VMware vSphere Client-Jobs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs zu generieren, müssen REST-API-Aufrufe für VMware vSphere verwendet werden.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>/api` An der Vorderseite der REST-API zu einem vollständigen Endpunkt

Verwenden Sie die folgenden REST-APIs im Abschnitt Jobs, um detaillierte Informationen über Jobs zu erhalten:

REST API	Kommentare
`4.1/audit/logs`	Gibt Audit-Log-Dateien mit Integritätsdaten zurück
`4.1/audit/logs/{filename}`	Erhalten Sie eine spezifische Audit-Log-Datei mit Integritätsdaten
`4.1/audit/verify`	Löst die Überprüfung des Audits aus
`4.1/audit/syslogcert`	Aktualisiert das Syslog-Serverzertifikat

Upgrade

Upgrade von einer früheren Version des SnapCenter Plug-ins für VMware vSphere

Das Upgrade auf SCV 6.2 wird nur auf VMware vCenter Server 7 Update 1 und späteren Versionen unterstützt. Für VMware vCenter Server vor Version 7 Update 1 sollten Sie weiterhin SCV 4.7 verwenden. Das Upgrade führt bei nicht unterstützten Versionen des VMware vCenter-Servers zu Unterbrechungen.

Wenn Sie das SnapCenter Plug-in für virtuelle VMware vSphere Appliance verwenden, können Sie ein Upgrade auf eine neuere Version durchführen. Beim Upgrade-Prozess wird das bestehende Plug-in wieder registriert und ein Plug-in wird implementiert, das nur mit vSphere 7.0U1 und höheren Versionen kompatibel ist.

Upgrade-Pfade

Wenn Sie ein SnapCenter-Plug-in für VMware vSphere (SCV)-Version verwenden…	Sie können das SnapCenter Plug-in für VMware vSphere direkt auf folgende Weise aktualisieren:
SCV 6,1	Upgrade auf SCV 6.2
SCV 6,0	Upgrade auf SCV 6.1 und SCV 6.2
SCV 5,0	Upgrade auf SCV 6.0 und SCV 6.1
SCV 4.9	Upgrade auf SCV 5.0 und SCV 6.0
SCV 4.8	Upgrade auf SCV 4.9 und SCV 5.0
SCV 4.7	Upgrade auf SCV 4.8 und SCV 4.9
SCV 4.6	Upgrade auf SCV 4.7 und SCV 4.8

Sichern Sie das SnapCenter Plug-in für VMware vSphere OVA, bevor Sie ein Upgrade starten.

Das Umschalten der Netzwerkkonfiguration von statisch auf DHCP wird nicht unterstützt.

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" (IMT).

Schritte

1. Bereiten Sie sich auf das Upgrade vor, indem Sie das SnapCenter Plug-in für VMware vSphere deaktivieren.
   a. Melden Sie sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere an. Die IP-Adresse wird angezeigt, wenn Sie das SnapCenter Plug-in for VMware vSphere bereitstellen.
   b. Wählen Sie im linken Navigationsbereich **Configuration** aus, und wählen Sie dann im Abschnitt Plug-in Details die Option **Service** aus, um das Plug-in zu deaktivieren.
2. Laden Sie das Upgrade herunter `.iso` Datei:

a. Loggen Sie sich auf der NetApp Support Site ein .

b. Wählen Sie aus der Liste der Produkte **SnapCenter Plug-in für VMware vSphere**, und klicken Sie dann auf die Schaltfläche **NEUESTES RELEASE HERUNTERLADEN**.

c. Laden Sie das Upgrade zum SnapCenter Plug-in für VMware vSphere herunter `.iso` Datei an jedem Speicherort.

3. Installieren Sie das Upgrade.

a. Navigieren Sie im Browser zu VMware vSphere vCenter.

b. Wählen Sie auf der vCenter-Benutzeroberfläche **vSphere-Client (HTML)** aus.

c. Melden Sie sich auf der Seite **VMware vCenter Single Sign-On** an.

d. Wählen Sie im Navigationsfenster die VM aus, die Sie aktualisieren möchten, und wählen Sie dann die Registerkarte **Zusammenfassung** aus.

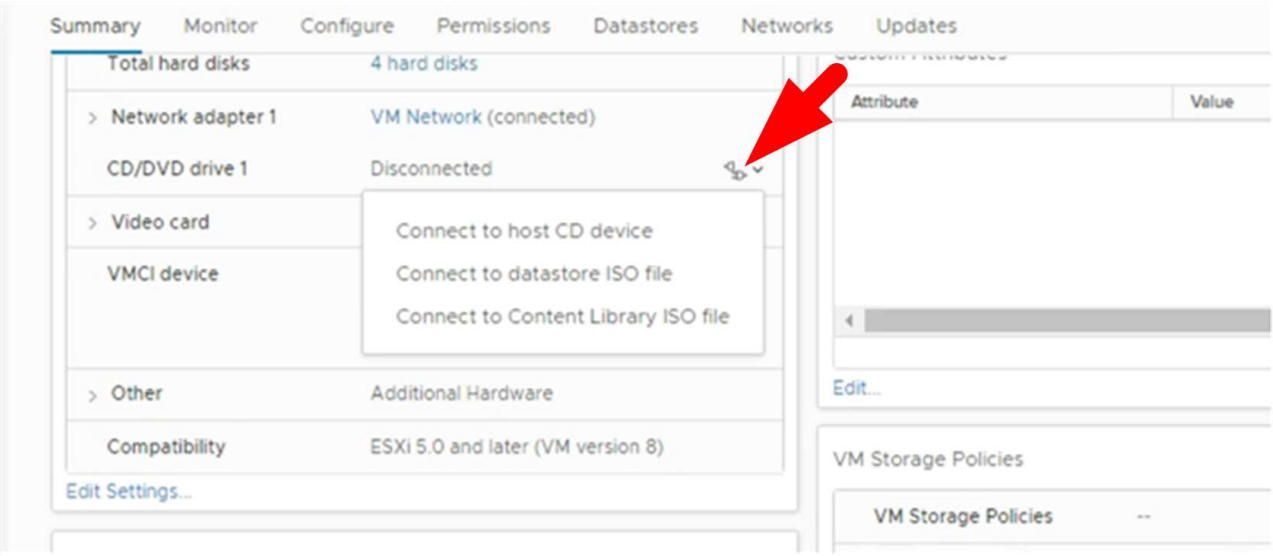
e. Wählen Sie im Bereich **Related Objects** einen beliebigen Datastore in der Liste aus und wählen Sie dann die Registerkarte **Summary** aus.

f. Wählen Sie auf der Registerkarte **Dateien** für den ausgewählten Datastore einen beliebigen Ordner in der Liste aus, und wählen Sie dann **Dateien hochladen**.

g. Navigieren Sie im Popup-Fenster „Hochladen“ zu dem Speicherort, an dem Sie die Datei heruntergeladen `.iso` haben, wählen Sie dann auf dem Dateibild aus `.iso`, und wählen Sie dann **Öffnen**. Die Datei wird in den Datastore hochgeladen.

h. Navigieren Sie zurück zu der VM, die Sie aktualisieren möchten, und wählen Sie die Registerkarte **Zusammenfassung**. Im Fenster **VM Hardware** im Feld CD/DVD sollte der Wert „getrennt“ sein.

i. Wählen Sie im Feld CD/DVD das Verbindungssymbol aus und wählen Sie **mit CD/DVD-Image auf einem Datenspeicher verbinden**.



j. Gehen Sie im Assistenten wie folgt vor:

i. Wählen Sie in der Spalte Datastores den Datenspeicher aus, auf den Sie den hochgeladen haben `.iso` Datei:

ii. Navigieren Sie in der Spalte Inhalt zu der `.iso` hochgeladenen Datei, stellen Sie sicher, dass im Feld Dateityp „ISO-Image“ ausgewählt ist, und wählen Sie dann **OK**. Warten Sie, bis der Status „verbunden“ angezeigt wird.

k. Melden Sie sich bei der Wartungskonsole an, indem Sie auf die Registerkarte **Zusammenfassung** der

virtuellen Appliance zugreifen und dann den grünen Run-Pfeil auswählen, um die Wartungskonsole zu starten.

l. Geben Sie **2** für die Systemkonfiguration ein, und geben Sie dann **8** für die Aktualisierung ein.

m. Geben Sie **y** ein, um mit dem Upgrade fortzufahren und zu starten.

Upgraden Sie auf einen neuen Patch derselben Version des SnapCenter Plug-ins für VMware vSphere

Wenn Sie ein Upgrade auf einen neuen Patch derselben Version durchführen, müssen Sie das SnapCenter Plug-in für VMware vSphere Cache auf dem vCenter Webserver löschen und den Server vor dem Upgrade oder der Registrierung neu starten.

Wenn der Plug-in-Cache nicht gelöscht wird, werden die letzten Jobs in den folgenden Szenarien nicht im Dashboard und auf der Jobüberwachung angezeigt:

- Das SnapCenter Plug-in für VMware vSphere wurde mithilfe von vCenter bereitgestellt und später auf ein Patch in derselben Version aktualisiert.
- Die virtuelle SnapCenter VMware Appliance wurde in vCenter 1 implementiert. Später wurde dieses SnapCenter Plug-in für VMware vSphere in einem neuen vCenter2 registriert. Eine neue Instanz des SnapCenter Plug-ins für VMware vSphere wird mit einem Patch erstellt und in vCenter1 registriert. Da vCenter1 jedoch noch das Cache-Plug-in des ersten SnapCenter Plug-ins für VMware vSphere ohne Patch hat, muss der Cache gelöscht werden.

Schritte zum Löschen des Caches

1. Suchen Sie das `vsphere-client-serenity` Ordner, und suchen Sie anschließend das `com.netapp.scv.client-<release-number>` Ordner und löschen.

   Der Ordnername ändert sich für jedes Release.

   Informationen zum Speicherort des Ordners für Ihr Betriebssystem finden Sie in der VMware-Dokumentation `vsphere-client-serenity` .

2. Starten Sie vCenter Server neu.

   Anschließend können Sie das SnapCenter-Plug-in für VMware vSphere aktualisieren.

Informationen, die nach dem Upgrade auf einen neuen Patch derselben Version nicht angezeigt werden

Nach dem Upgrade des SnapCenter Plug-ins für VMware vSphere auf einen neuen Patch derselben Version werden aktuelle Jobs oder andere Informationen möglicherweise nicht im Dashboard und auf der Jobüberwachung angezeigt.

Wenn Sie ein Upgrade auf einen neuen Patch derselben Version durchführen, müssen Sie das SnapCenter Plug-in für VMware vSphere Cache auf dem vCenter Webserver löschen und den Server vor dem Upgrade oder der Registrierung neu starten.

Wenn der Plug-in-Cache nicht gelöscht wird, werden die letzten Jobs in den folgenden Szenarien nicht im

Dashboard und auf der Jobüberwachung angezeigt:

- Das SnapCenter Plug-in für VMware vSphere wurde mithilfe von vCenter bereitgestellt und später auf ein Patch in derselben Version aktualisiert.
- Die virtuelle SnapCenter VMware Appliance wurde in vCenter 1 implementiert. Später wurde dieses SnapCenter Plug-in für VMware vSphere in einem neuen vCenter2 registriert. Eine neue Instanz des SnapCenter Plug-ins für VMware vSphere wird mit einem Patch erstellt und in vCenter1 registriert. Da vCenter1 jedoch noch das Cache-Plug-in des ersten SnapCenter Plug-ins für VMware vSphere ohne Patch hat, muss der Cache gelöscht werden.

Der Cache befindet sich an den folgenden Orten, abhängig vom Typ des Serverbetriebssystems:

- VCenter Server Linux Appliance

  `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/`

- Windows OS

  `%PROGRAMFILES%/VMware/vSphere client/vc-packages/vsphere-client-serenity/`

Problemumgehung, wenn Sie bereits vor dem Löschen des Caches aktualisiert haben

1. Melden Sie sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

   Die IP-Adresse wird angezeigt, wenn Sie das SnapCenter-Plug-in für VMware vSphere bereitstellen.

2. Wählen Sie im linken Navigationsbereich **Configuration** aus, und wählen Sie dann im Abschnitt **Plug-in Details** die Option Service aus, um das Plug-in zu deaktivieren.

   SnapCenter-Plug-in für VMware vSphere ist deaktiviert, und die Erweiterung wird in vCenter nicht registriert.

3. Suchen Sie das `vsphere-client-serenity` Ordner, und suchen Sie anschließend das `com.netapp.scv.client-<release-number>` Ordner und löschen.

   Der Ordnername ändert sich für jedes Release.

4. Starten Sie vCenter Server neu.
5. Melden Sie sich beim VMware vSphere-Client an.
6. Wählen Sie im linken Navigationsbereich **Configuration** aus, und wählen Sie dann im Abschnitt **Plug-in Details** die Option Service aus, um das Plug-in zu aktivieren.

   Der Service SnapCenter Plug-in für VMware vSphere ist aktiviert, und die Erweiterung wird in vCenter registriert.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis zum SnapCenter Plug-in for VMware vSphere 6.2"