SnapCenter Plug-in for VMware vSphere Dokumentation

SnapCenter Plug-in for VMware vSphere

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/de-de/sc-plugin-vmware-vsphere-61/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

Inhalt

SnapCenter Plug-in for VMware vSphere Dokumentation . . . 1
Versionshinweise . . . 2
- Versionshinweise zum SnapCenter Plug-in for VMware vSphere . . . 2
- Was ist neu im SnapCenter Plug-in for VMware vSphere 6.1 . . . 2
- Upgrade-Pfade . . . 2

Konzepte . . . 4
- Produktübersicht . . . 4
- Übersicht über die verschiedenen SnapCenter -GUIs . . . 5
- Lizenzierung . . . 6
- Rollenbasierte Zugriffskontrolle (RBAC) . . . 7
- Arten von RBAC für SnapCenter Plug-in for VMware vSphere Benutzer . . . 7
  - vCenter Server RBAC . . . 7
  - ONTAP RBAC . . . 8
  - Validierungsworkflow für RBAC-Berechtigungen . . . 8
- ONTAP RBAC-Funktionen im SnapCenter Plug-in for VMware vSphere . . . 9
- Vordefinierte Rollen im SnapCenter Plug-in for VMware vSphere . . . 10
- So konfigurieren Sie ONTAP RBAC für das SnapCenter Plug-in for VMware vSphere . . . 11

Erste Schritte . . . 13
- Bereitstellungsübersicht . . . 13
- Bereitstellungsworkflow für vorhandene Benutzer . . . 13
- Voraussetzungen für die Bereitstellung von SCV . . . 14
  - Bereitstellungsplanung und -anforderungen . . . 14
  - ONTAP -Berechtigungen erforderlich . . . 20
  - Mindestens erforderliche vCenter-Berechtigungen . . . 22
- Laden Sie die Open Virtual Appliance (OVA) herunter . . . 23
- Bereitstellen des SnapCenter Plug-in for VMware vSphere . . . 23
- Nach der Bereitstellung erforderliche Vorgänge und Probleme . . . 27
  - Erforderliche Vorgänge nach der Bereitstellung . . . 27
  - Mögliche Bereitstellungsprobleme . . . 27
  - Verwalten von Authentifizierungsfehlern . . . 28
  - Registrieren Sie das SnapCenter Plug-in for VMware vSphere beim SnapCenter -Server . . . 28
- Melden Sie sich beim SnapCenter VMware vSphere-Client an . . . 29

Schnellstart . . . 31
- Überblick . . . 31
- Bereitstellen des SnapCenter Plug-in for VMware vSphere . . . 31
- Speicher hinzufügen . . . 33
- Erstellen von Sicherungsrichtlinien . . . 33
- Erstellen von Ressourcengruppen . . . 33

Überwachen und berichten . . . 34
- Statusinformationen anzeigen . . . 34
- Überwachen von Jobs . . . 36
- Jobprotokolle herunterladen . . . 36
- Zugriffsberichte . . . 37

Berichtstypen vom VMware vSphere-Client . . . 37
Generieren Sie ein Support-Paket aus dem SnapCenter Plug-in for VMware vSphere GUI . . . 39
Generieren Sie ein Support-Paket aus der Wartungskonsole . . . 40
Überwachungsprotokolle . . . 41
Datenschutzereignisse . . . 42
Ereignisse der Wartungskonsole . . . 43
Ereignisse in der Admin-Konsole . . . 43
Konfigurieren von Syslog-Servern . . . 44
Ändern der Überwachungsprotokolleinstellungen . . . 44
Speicher verwalten . . . 45
Speicher hinzufügen . . . 45
Speichersysteme verwalten . . . 47
Ändern von Speicher-VMs . . . 48
Entfernen von Speicher-VMs . . . 48
Ändern Sie das konfigurierte Speicher-Timeout . . . 49
Daten schützen . . . 50
Datenschutz-Workflow . . . 50
Anzeigen von VM- und Datenspeichersicherungen . . . 51
Erstellen Sie Sicherungsrichtlinien für VMs und Datenspeicher . . . 52
Erstellen von Ressourcengruppen . . . 57
Verwalten von Fehlern bei der Kompatibilitätsprüfung . . . 66
Präskripte und Postskripte . . . 66
Unterstützte Skripttypen . . . 66
Speicherort des Skriptpfads . . . 66
Wo Skripte angegeben werden . . . 67
Wenn Skripte ausgeführt werden . . . 67
An Skripte übergebene Umgebungsvariablen . . . 67
Skript-Timeouts . . . 68
Beispiel-PERL-Skript Nr. 1 . . . 68
Beispiel-PERL-Skript Nr. 2 . . . 68
Beispiel-Shell-Skript . . . 69
Hinzufügen einer einzelnen VM oder eines Datenspeichers zu einer Ressourcengruppe . . . 69
Hinzufügen mehrerer VMs und Datenspeicher zu einer Ressourcengruppe . . . 70
Wiederherstellen der Sicherung des umbenannten Speichers . . . 71
Sichern Sie Ressourcengruppen bei Bedarf . . . 72
Sichern Sie das SnapCenter Plug-in for VMware vSphere MySQL-Datenbank . . . 72
Verwalten von Ressourcengruppen . . . 73
Anhalten und Fortsetzen von Vorgängen für Ressourcengruppen . . . 74
Ändern von Ressourcengruppen . . . 74
Ressourcengruppen löschen . . . 74
Richtlinien verwalten . . . 75
Richtlinien trennen . . . 75
Richtlinien ändern . . . 75
Richtlinien löschen . . . 76
Backups verwalten . . . 76

Backups umbenennen . . . 76
Backups löschen . . . 77
Mounten und Unmounten von Datenspeichern . . . 79
Mounten Sie ein Backup . . . 79
Ein Backup aushängen . . . 80
Sicherungen wiederherstellen . . . 81
Übersicht wiederherstellen . . . 81
So werden Wiederherstellungsvorgänge ausgeführt . . . 81
Suche nach Backups . . . 83
Wiederherstellen von VMs aus Backups . . . 84
Wiederherstellen gelöschter VMs aus Backups . . . 87
Wiederherstellen von VMDKs aus Backups . . . 88
Stellen Sie die neueste Sicherung der MySQL-Datenbank wieder her . . . 90
Stellen Sie eine bestimmte Sicherung der MySQL-Datenbank wieder her . . . 90
Anhängen und Trennen von VMDKs . . . 92
VMDKs an eine VM oder vVol-VM anhängen . . . 92
Trennen einer virtuellen Festplatte . . . 94
Wiederherstellen von Gastdateien und -ordnern . . . 96
Arbeitsablauf, Voraussetzungen und Einschränkungen . . . 96
Workflow zur Gastwiederherstellung . . . 96
Voraussetzungen für die Wiederherstellung von Gastdateien und -ordnern . . . 96
Einschränkungen bei der Wiederherstellung von Gastdateien . . . 97
Wiederherstellen von Gastdateien und -ordnern aus VMDKs . . . 98
Einrichten von Proxy-VMs für Wiederherstellungsvorgänge . . . 102
Konfigurieren Sie Anmeldeinformationen für die Wiederherstellung von VM-Gastdateien . . . 103
Verlängern Sie die Dauer einer Gastdateiwiederherstellungssitzung . . . 104
Mögliche Szenarien zur Wiederherstellung von Gastdateien . . . 104
Die Gastdateiwiederherstellungssitzung ist leer . . . 105
Der Vorgang zum Anhängen der Festplatte beim Wiederherstellen der Gastdatei schlägt fehl . . . 105
Gast-E-Mail zeigt ?????? als Dateinamen . . . 105
Sicherungen werden nicht getrennt, nachdem die Gastdateiwiederherstellungssitzung abgebrochen wurde . . . 105
Verwalten des SnapCenter Plug-in for VMware vSphere -Geräte . . . 106
Starten Sie den VMware vSphere-Clientdienst neu . . . 106
Starten Sie den VMware vSphere-Clientdienst in einem Linux vCenter neu . . . 106
Zugriff auf die Wartungskonsole . . . 106
Ändern Sie das Kennwort des SnapCenter Plug-in for VMware vSphere über die Wartungskonsole. . . . 108
Zertifikate erstellen und importieren . . . 109
Aufheben der Registrierung des SnapCenter Plug-in for VMware vSphere bei vCenter . . . 109
Deaktivieren und Aktivieren des SnapCenter Plug-in for VMware vSphere . . . 110
Entfernen Sie das SnapCenter Plug-in for VMware vSphere . . . 111
Verwalten Sie Ihre Konfiguration . . . 113
Ändern der Zeitzonen für Backups . . . 113
Ändern der Anmeldeinformationen . . . 113
Ändern der vCenter-Anmeldeinformationen . . . 114

Ändern Sie die Netzwerkeinstellungen . . . 115
Ändern der Konfigurationsstandardwerte . . . 116
Erstellen Sie die Konfigurationsdatei scbr.override . . . 117
Eigenschaften, die Sie überschreiben können . . . 117
Aktivieren Sie SSH für das SnapCenter Plug-in for VMware vSphere . . . 122
REST-APIs . . . 124
Überblick . . . 124
Greifen Sie über die Swagger-API-Webseite auf REST-APIs zu . . . 125
REST-API-Workflows zum Hinzufügen und Ändern von Speicher-VMs . . . 125
REST-API-Workflows zum Erstellen und Ändern von Ressourcengruppen . . . 126
REST-API-Workflow zum Sichern auf Anfrage . . . 128
REST-API-Workflow zum Wiederherstellen von VMs . . . 128
REST-API-Workflow zum Wiederherstellen gelöschter VMs . . . 129
REST-API-Workflow zum Wiederherstellen von VMDKs . . . 131
REST-API-Workflows zum Anhängen und Trennen von VMDKs . . . 132
Um VMDKs anzuhängen, folgen Sie diesem Workflow: . . . 132
Um VMDKs zu trennen, folgen Sie diesem Workflow: . . . 133
REST-API-Workflows zum Mounten und Unmounten von Datenspeichern . . . 134
Um Datenspeicher zu mounten, folgen Sie diesem Workflow: . . . 134
Um die Bereitstellung von Datenspeichern aufzuheben, folgen Sie diesem Arbeitsablauf: . . . 135
REST-APIs zum Herunterladen von Jobs und Generieren von Berichten . . . 135
Verwenden Sie die folgenden REST-APIs im Abschnitt „Jobs“, um detaillierte Informationen zu Jobs zu erhalten: . . . 136
Verwenden Sie die folgende REST-API im Abschnitt „Jobs“, um Jobprotokolle herunterzuladen: . . . 136
Verwenden Sie die folgenden REST-APIs im Abschnitt „Berichte“, um Berichte zu generieren: . . . 136
REST-API-Workflow zum Ändern integrierter Zeitpläne . . . 136
REST-API zum Markieren feststeckender Jobs als fehlgeschlagen . . . 137
REST-APIs zum Generieren von Audit-Protokollen . . . 137
Upgrade . . . 139
Upgrade von einer früheren Version des SnapCenter Plug-in for VMware vSphere . . . 139
Upgrade-Pfade . . . 139
Upgrade auf einen neuen Patch der gleichen Version des SnapCenter Plug-in for VMware vSphere . . . 141
Schritte zum Leeren des Caches . . . 141
Nach dem Upgrade auf einen neuen Patch derselben Version werden keine Informationen angezeigt . . . 141
Problemumgehung, wenn Sie bereits vor dem Leeren des Caches ein Upgrade durchgeführt haben . . . 142
Rechtliche Hinweise . . . 143
Copyright . . . 143
Marken . . . 143
Patente . . . 143
Datenschutzrichtlinie . . . 143
Open Source . . . 143

SnapCenter Plug-in for VMware vSphere Dokumentation

Versionshinweise

Versionshinweise zum SnapCenter Plug-in for VMware vSphere

Informieren Sie sich über die neuen und verbesserten Funktionen des SnapCenter Plug-in for VMware vSphere 6.1.

Einzelheiten zu bekannten Problemen, Einschränkungen und behobenen Problemen finden Sie unter "Versionshinweise zum SnapCenter Plug-in for VMware vSphere 6.1" . Sie müssen sich mit Ihrem NetApp -Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zugreifen zu können.

> Die neuesten Informationen zu unterstützten Versionen finden Sie im NetApp Interoperability Matrix Tool("IMT").

Was ist neu im SnapCenter Plug-in for VMware vSphere 6.1

Unterstützung für VMs und VMFS-Datenspeicher auf ASA r2-Systemen

Das SnapCenter -Plug-in für VMware vSphere 6.1 unterstützt die Bereitstellung von virtuellen Maschinen (VMs) und VMFS-Datenspeichern auf ASA r2-Systemen. ASA r2-Systeme bieten eine einheitliche Hardware- und Softwarelösung, die ein vereinfachtes Erlebnis bietet, das speziell auf die Anforderungen von reinen SAN-Kunden zugeschnitten ist. Zu den vom SnapCenter Plug-in for VMware vSphere 6.1 unterstützten Funktionen für VMs, Datenspeicher und Virtual Machine Disk Format (VMDK) auf ASA r2-Systemen gehören:

- Bereitstellung von Konsistenzgruppen für primären Schutz
- Konsistenzgruppenbasierte Sicherung
- Klonen von Workflows
- Wiederherstellungsworkflows
- Bereitstellung eines sekundären Schutzes beim Erstellen oder Ändern der Ressourcengruppe.

> Der sekundäre Schutz wird nur auf ONTAP 9.16.1 und späteren Versionen unterstützt

Unterstützung für sekundäre manipulationssichere Snapshots (TPS)

Das SnapCenter Plug-in for VMware vSphere bietet Unterstützung für sekundäre TPS und stellt so sicher, dass sekundäre Snapshot-Kopien vor Löschung oder Veränderung durch Ransomware-Angreifer oder betrügerische Administratoren geschützt sind und auch nach einem Angriff verfügbar bleiben.

Upgrade-Pfade

Auf welche Version des SnapCenter Plug-in for VMware vSphere (SCV) Sie aktualisieren können, hängt von der Version ab, die Sie derzeit ausführen.

Das Upgrade auf das SnapCenter Plug-in for VMware vSphere (SCV) 4.8 und höher 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.

Wenn Sie die SCV-Version verwenden …	Sie können SCV direkt aktualisieren auf …
SCV 6,0	SCV 6,1
SCV 5,0	SCV 6.0 und SCV 6.1
SCV 4,9	SCV 5.0 und SCV 6.0
SCV 4,8	SCV 4.9 und SCV 5.0
SCV 4,7	SCV 4.8 und SCV 4.9

Für virtualisierte Datenbanken und Dateisysteme, die in SnapCenter integriert sind, ist dies der Upgradepfad:

Wenn Sie	Wenn Ihr VMware-Plug-In … ist	Sie können direkt upgraden auf…
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 Interoperabilitätsmatrix-Tool" (IMT).

Konzepte

Produktübersicht

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

Das SnapCenter Plug-in for VMware vSphere fügt Ihrer Umgebung die folgenden Funktionen hinzu:

- Unterstützung für VM-konsistente und absturzkonsistente Datenschutzvorgänge.

  Sie können die GUI des VMware vSphere-Clients 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 Sichern von VMs, VMDKs und Datenspeichern unterstützt das Plug-In keine RDMs. Sicherungsaufträge für VMs ignorieren RDMs. Wenn Sie RDMs sichern müssen, müssen Sie ein anwendungsbasiertes SnapCenter -Plug-In verwenden.

  Das SnapCenter Plug-in for VMware vSphere enthält eine MySQL-Datenbank, die die Metadaten des SnapCenter Plug-in for VMware vSphere enthält. Für VM-konsistenten und absturzkonsistenten Datenschutz müssen Sie SnapCenter Server nicht installieren.

- Unterstützung für anwendungskonsistente (Anwendung über VMDK/RDM) Datenschutzvorgänge.

  Sie können die SnapCenter GUI 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 for VMware vSphere nativ für alle Datenschutzvorgänge auf VMDKs, Raw Device Mappings (RDMs) und NFS-Datenspeichern. Nachdem die virtuelle Appliance bereitgestellt wurde, übernimmt das Plug-In alle Interaktionen mit vCenter. Das SnapCenter Plug-in for VMware vSphere unterstützt alle anwendungsbasierten 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 -GUI; planen Sie die VM- und Datenspeichersicherungen mithilfe der VMware vSphere-Client-GUI.

- VMware-Tools sind für VM-konsistente Snapshots erforderlich

  Wenn VMware Tools nicht installiert und ausgeführt wird, wird das Dateisystem nicht stillgelegt und ein absturzkonsistenter Snapshot erstellt.

- VMware Storage vMotion ist für Wiederherstellungsvorgänge in SAN-Umgebungen (VMFS) erforderlich

  Der Wiederherstellungs-Workflow für das VMware-Dateisystem (VMFS) nutzt die VMware Storage vMotion-Funktion. Storage vMotion ist Teil der vSphere Standard-Lizenz, aber nicht mit den Lizenzen vSphere Essentials oder Essentials Plus verfügbar.

  Die meisten Wiederherstellungsvorgänge in NFS-Umgebungen verwenden native ONTAP -Funktionen (z. B. Single File SnapRestore) und erfordern kein VMware Storage vMotion.

- Zum Konfigurieren von VMware vVol-VMs sind ONTAP tools for VMware vSphere erforderlich.

  Sie verwenden ONTAP Tools, um Speicher für vVols in ONTAP und im VMware-Webclient bereitzustellen und zu konfigurieren.

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

- SnapCenter Plug-in for 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 for VMware vSphere sowohl Windows-basierte als auch Linux-basierte vCenter. SnapCenter verwendet dieses Plug-In nativ und ohne Benutzereingriff, um mit Ihrem vCenter zu kommunizieren und anwendungsbasierte Plug-Ins von SnapCenter zu unterstützen, die Datenschutzvorgänge auf virtualisierten Windows- und Linux-Anwendungen durchführen.

Zusätzlich zu diesen Hauptfunktionen bietet das SnapCenter Plug-in for VMware vSphere auch Unterstützung für iSCSI, Fiber Channel, FCoE, NFS 3.0/4.1, VMFS 5.0/6.0, NVMe über FC und NVMe über TCP.

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

Informationen zu NFS-Protokollen und ESXi-Hosts finden Sie in der von VMware bereitgestellten vSphere Storage-Dokumentation.

Informationen zum SnapCenter -Datenschutz finden Sie in den Datenschutzinformationen für Ihr SnapCenter -Plugin im "SnapCenter -Dokumentation" .

Informationen zu unterstützten Upgrade- und Migrationspfaden finden Sie unter"Versionshinweise zum SnapCenter Plug-in for VMware vSphere" .

Übersicht über die verschiedenen SnapCenter -GUIs

In Ihrer SnapCenter -Umgebung müssen Sie die entsprechende GUI 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-GUI in vCenter für alle Sicherungs- und Wiederherstellungsvorgänge für VMs, VMDKs und Datenspeicher verwenden. Sie verwenden auch das GUI-Dashboard des Webclients, 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 GUI.

Zum Schutz von VMs und Datenspeichern verwenden Sie die VMware vSphere-Clientschnittstelle. Die GUI des Webclients lässt sich in die Snapshot-Technologie von NetApp 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 Verwaltungs-GUI zum Durchführen administrativer Vorgänge am SnapCenter Plug-in for VMware vSphere.

Die folgende Tabelle zeigt die Vorgänge, die die SnapCenter -GUI ausführt.

Verwenden Sie diese GUI…	So führen Sie diese Vorgänge aus:	Und um auf diese Backups zuzugreifen …
SnapCenter vSphere-Client-GUI	VM- und Datenspeichersicherung, VMDK anhängen und trennen, Datenspeicher mounten und unmounten, VM- und VMDK-Wiederherstellung, Gastdatei- und -ordnerwiederherstellung	Sicherungen von VMs und Datenspeichern mithilfe der VMware vSphere-Client-GUI.
SnapCenter -Benutzeroberfläche	Sicherung und Wiederherstellung von Datenbanken und Anwendungen auf VMs, einschließlich Schutz von Datenbanken für Microsoft SQL Server, Microsoft Exchange und Oracle. Datenbankklon	Mit der SnapCenter -GUI durchgeführte Sicherungen.
SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI	Ändern Sie die Netzwerkkonfiguration. Generieren Sie ein Support-Paket. Ändern Sie die NTP-Servereinstellungen. Deaktivieren/Aktivieren Sie das Plug-In.	N / A
vCenter-GUI	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 GUI 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 mithilfe der SnapCenter -GUI geplant werden; VM-konsistente Sicherungen müssen mithilfe der VMware vSphere-Client-GUI geplant werden.

Lizenzierung

Das SnapCenter Plug-in for VMware vSphere ist ein kostenloses Produkt, wenn Sie die folgenden Speichersysteme verwenden:

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

Es wird empfohlen, ist aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standardlizenzen auf sekundären Systemen nicht aktiviert sind, können Sie SnapCenter nach der Durchführung eines Failover-Vorgangs nicht verwenden. Zum Durchführen von Mount- und Attach-Vorgängen ist jedoch eine FlexClone -Lizenz auf dem Sekundärspeicher erforderlich. Zum

Durchführen von Wiederherstellungsvorgängen ist eine SnapRestore -Lizenz erforderlich.

Rollenbasierte Zugriffskontrolle (RBAC)

Das SnapCenter Plug-in for VMware vSphere bietet eine zusätzliche RBAC-Ebene für die Verwaltung virtualisierter Ressourcen. Das Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC.

SnapCenter und ONTAP RBAC gelten nur für anwendungskonsistente SnapCenter Server-Jobs (Anwendung über VMDK). Wenn Sie das SnapCenter Plug-in for VMware vSphere verwenden, um anwendungskonsistente SnapCenter -Jobs zu unterstützen, müssen Sie die Rolle SnapCenterAdmin zuweisen. Sie können die Berechtigungen der Rolle SnapCenterAdmin nicht ändern.

Das SnapCenter Plug-in for VMware vSphere wird mit vordefinierten vCenter-Rollen geliefert. Sie müssen diese Rollen über die vCenter-GUI zu vCenter Active Directory-Benutzern hinzufügen, um SnapCenter -Vorgänge auszuführen.

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

Arten von RBAC für SnapCenter Plug-in for VMware vSphere Benutzer

Wenn Sie das SnapCenter Plug-in for VMware vSphere verwenden, bietet der vCenter Server eine zusätzliche RBAC-Ebene. Das Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC.

vCenter Server RBAC

Dieser Sicherheitsmechanismus gilt für alle Jobs, die vom SnapCenter Plug-in for VMware vSphere ausgeführt werden, einschließlich VM-konsistenter, VM-absturzkonsistenter und SnapCenter Server-anwendungskonsistenter (Anwendung über VMDK) Jobs. Diese RBAC-Ebene schränkt die Möglichkeit von vSphere-Benutzern ein, SnapCenter Plug-in for VMware vSphere Aufgaben auf vSphere-Objekten wie virtuellen Maschinen (VMs) und Datenspeichern auszuführen.

Das SnapCenter Plug-in for VMware vSphere Bereitstellung erstellt die folgenden Rollen für SnapCenter -Vorgänge auf vCenter:

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

Der vSphere-Administrator richtet vCenter Server RBAC wie folgt ein:

- Festlegen der vCenter Server-Berechtigungen für das Stammobjekt (auch als Stammordner bezeichnet). Sie können die Sicherheit dann verfeinern, indem Sie untergeordnete Entitäten einschränken, die diese Berechtigungen nicht benötigen.

- 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 GUI des VMware vSphere-Clients zugreifen.

ONTAP RBAC

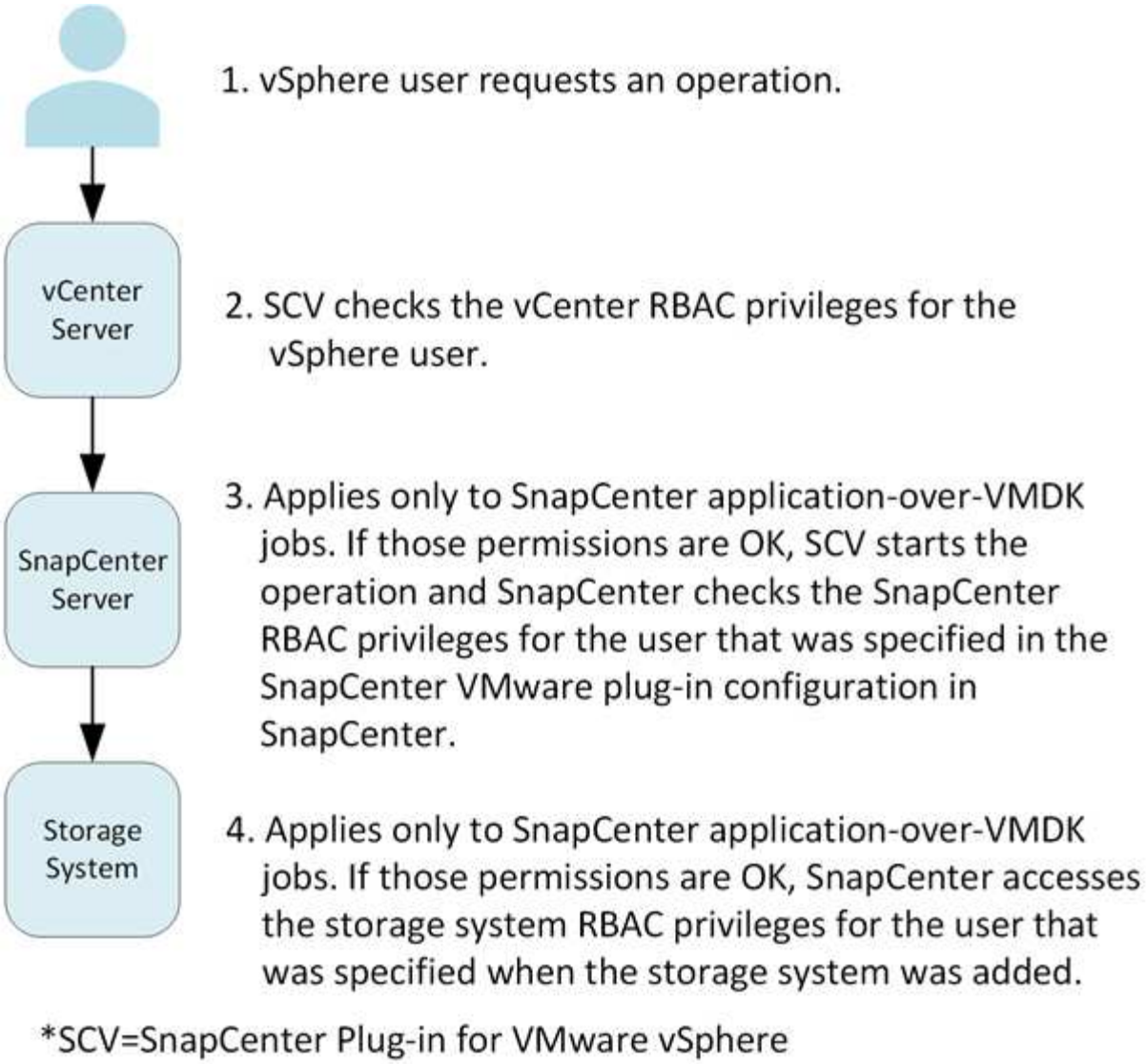
Dieser Sicherheitsmechanismus gilt nur für anwendungskonsistente SnapCenter Server-Jobs (Anwendung über VMDK). Diese Ebene schränkt die Fähigkeit von SnapCenter ein, bestimmte Speichervorgänge, wie z. B. das Sichern von Speicher für Datenspeicher, auf einem bestimmten Speichersystem durchzuführen.

Verwenden Sie den folgenden Workflow, um ONTAP und SnapCenter RBAC einzurichten:

1. Der Speicheradministrator erstellt auf der Speicher-VM eine Rolle mit den erforderlichen Berechtigungen.
2. Anschließend weist der Speicheradministrator die Rolle einem Speicherbenutzer zu.
3. Der SnapCenter Administrator fügt die Speicher-VM unter Verwendung dieses Speicherbenutzernamens zum SnapCenter Server hinzu.
4. Anschließend weist der SnapCenter Administrator den SnapCenter Benutzern Rollen zu.

Validierungsworkflow für RBAC-Berechtigungen

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



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

> ONTAP RBAC gilt nur für anwendungskonsistente SnapCenter Server-Jobs (Anwendung über VMDK).

Mit der rollenbasierten Zugriffskontrolle (RBAC) von ONTAP können Sie den Zugriff auf bestimmte Speichersysteme und die Aktionen steuern, die ein Benutzer auf diesen Speichersystemen ausführen kann. Das SnapCenter Plug-in for VMware vSphere arbeitet mit vCenter Server RBAC, SnapCenter RBAC (bei Bedarf zur Unterstützung anwendungsbasierter Vorgänge) und ONTAP RBAC, um zu bestimmen, welche SnapCenter -Aufgaben ein bestimmter Benutzer an Objekten auf einem bestimmten Speichersystem ausführen kann.

SnapCenter verwendet die von Ihnen eingerichteten Anmeldeinformationen (Benutzername und Kennwort), um jedes Speichersystem zu authentifizieren und zu bestimmen, welche Vorgänge auf diesem Speichersystem ausgeführt werden können. Das SnapCenter Plug-in for VMware vSphere verwendet einen Satz

Anmeldeinformationen für jedes Speichersystem. Diese Anmeldeinformationen bestimmen alle Aufgaben, die auf diesem Speichersystem ausgeführt werden können. Mit anderen Worten: Die Anmeldeinformationen gelten für SnapCenter und nicht für einen einzelnen SnapCenter -Benutzer.

ONTAP RBAC gilt nur für den Zugriff auf Speichersysteme und die Durchführung von SnapCenter -Aufgaben im Zusammenhang mit dem Speicher, wie etwa das Sichern von VMs. Wenn Sie nicht über die entsprechenden ONTAP RBAC-Berechtigungen für ein bestimmtes Speichersystem verfügen, können Sie keine Aufgaben an einem auf diesem Speichersystem gehosteten vSphere-Objekt ausführen.

Jedem Speichersystem ist ein Satz ONTAP Berechtigungen zugeordnet.

Die Verwendung von ONTAP RBAC und vCenter Server RBAC bietet die folgenden Vorteile:

- Sicherheit

  Der Administrator kann steuern, welche Benutzer welche Aufgaben sowohl auf der feinkörnigen vCenter Server-Objektebene als auch auf der Speichersystemebene ausführen können.

- Audit-Informationen

  In vielen Fällen stellt SnapCenter einen Prüfpfad auf dem Speichersystem bereit, mit dem Sie Ereignisse bis zum vCenter-Benutzer zurückverfolgen können, der die Speicheränderungen vorgenommen hat.

- Benutzerfreundlichkeit

  Sie können die Controller-Anmeldeinformationen an einem Ort verwalten.

Vordefinierte Rollen im SnapCenter Plug-in for VMware vSphere

Um die Arbeit mit vCenter Server RBAC zu vereinfachen, bietet das SnapCenter Plug-in for VMware vSphere eine Reihe vordefinierter Rollen, mit denen Benutzer SnapCenter -Aufgaben ausführen können. Es gibt auch eine schreibgeschützte Rolle, die es Benutzern ermöglicht, SnapCenter -Informationen anzuzeigen, aber keine Aufgaben auszuführen.

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 for VMware vSphere setzt diese Rollen jedes Mal auf ihre Standardwerte (anfänglicher Satz von Berechtigungen) zurück, wenn Sie den vCenter-Webclientdienst neu starten oder Ihre Installation ändern. Wenn Sie das SnapCenter Plug-in for VMware vSphere aktualisieren, werden die vordefinierten Rollen automatisch aktualisiert, damit sie mit dieser Version des Plug-ins funktionieren.

Sie können die vordefinierten Rollen in der vCenter-GUI 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 zum Ausführen aller SnapCenter Plug-in for VMware vSphere erforderlich sind. Ab der SCV-Version 6.1 wird dieser Rolle ein neues Privileg zum Erstellen eines sekundären Schutzes hinzugefügt.
SCV-Sicherung	Bietet alle nativen vCenter Server- und SnapCenter-spezifischen Berechtigungen, die zum Sichern von vSphere-Objekten (virtuelle Maschinen und Datenspeicher) erforderlich sind. Der Benutzer hat auch Zugriff auf die Konfigurationsberechtigung. Der Benutzer kann keine Sicherungen wiederherstellen. Ab der SCV-Version 6.1 wird dieser Rolle ein neues Privileg zum Erstellen eines sekundären Schutzes hinzugefügt.
SCV-Gastdateiwiederherstellung	Bietet alle nativen vCenter Server- und SnapCenter-spezifischen Berechtigungen, die zum Wiederherstellen 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 zum Wiederherstellen von vSphere-Objekten erforderlich sind, die mit dem SnapCenter Plug-in for VMware vSphere gesichert wurden, sowie zum Wiederherstellen von Gastdateien und -ordnern. Der Benutzer hat auch Zugriff auf die Konfigurationsberechtigung. Der Benutzer kann keine vSphere-Objekte sichern.
SCV-Ansicht	Bietet schreibgeschützten Zugriff auf alle SnapCenter Plug-in for VMware vSphere Backups, Ressourcengruppen und Richtlinien.

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

ONTAP RBAC gilt nur für anwendungskonsistente SnapCenter Server-Jobs (Anwendung über VMDK).

> Ab SnapCenter Plug-in für VMware (SCV) 5.0 müssen Sie Anwendungen vom Typ HTTP und ONTAPI als Benutzeranmeldemethoden für alle ONTAP Benutzer mit benutzerdefiniertem rollenbasierten Zugriff auf das SCV hinzufügen. Ohne Zugriff auf diese Anwendungen schlagen Backups fehl. Sie müssen den SCV-Dienst neu starten, um Änderungen an den Anmeldemethoden für ONTAP Benutzer zu erkennen. Informationen zum Erstellen oder Ändern von Anmeldekonten finden Sie unter "Arbeitsblätter zur Administratorauthentifizierung und RBAC-Konfiguration" .

Sie müssen ONTAP RBAC auf dem Speichersystem konfigurieren, wenn Sie es mit dem SnapCenter Plug-in

for VMware vSphere verwenden möchten. Innerhalb von ONTAP müssen Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine einzelne Rolle.

  "Administratorauthentifizierung und RBAC"

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

  Diese Speichersystem-Anmeldeinformationen sind erforderlich, damit Sie die Speichersysteme für das SnapCenter Plug-in for VMware vSphere konfigurieren können. Geben Sie dazu die Anmeldeinformationen in das Plug-in ein. Bei jeder Anmeldung an einem Speichersystem mit diesen Anmeldeinformationen werden Ihnen die SnapCenter -Funktionen angezeigt, die Sie beim Erstellen der Anmeldeinformationen in ONTAP eingerichtet haben.

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

Weitere Informationen finden Sie unter "Mindestens erforderliche ONTAP -Berechtigungen" .

Erste Schritte

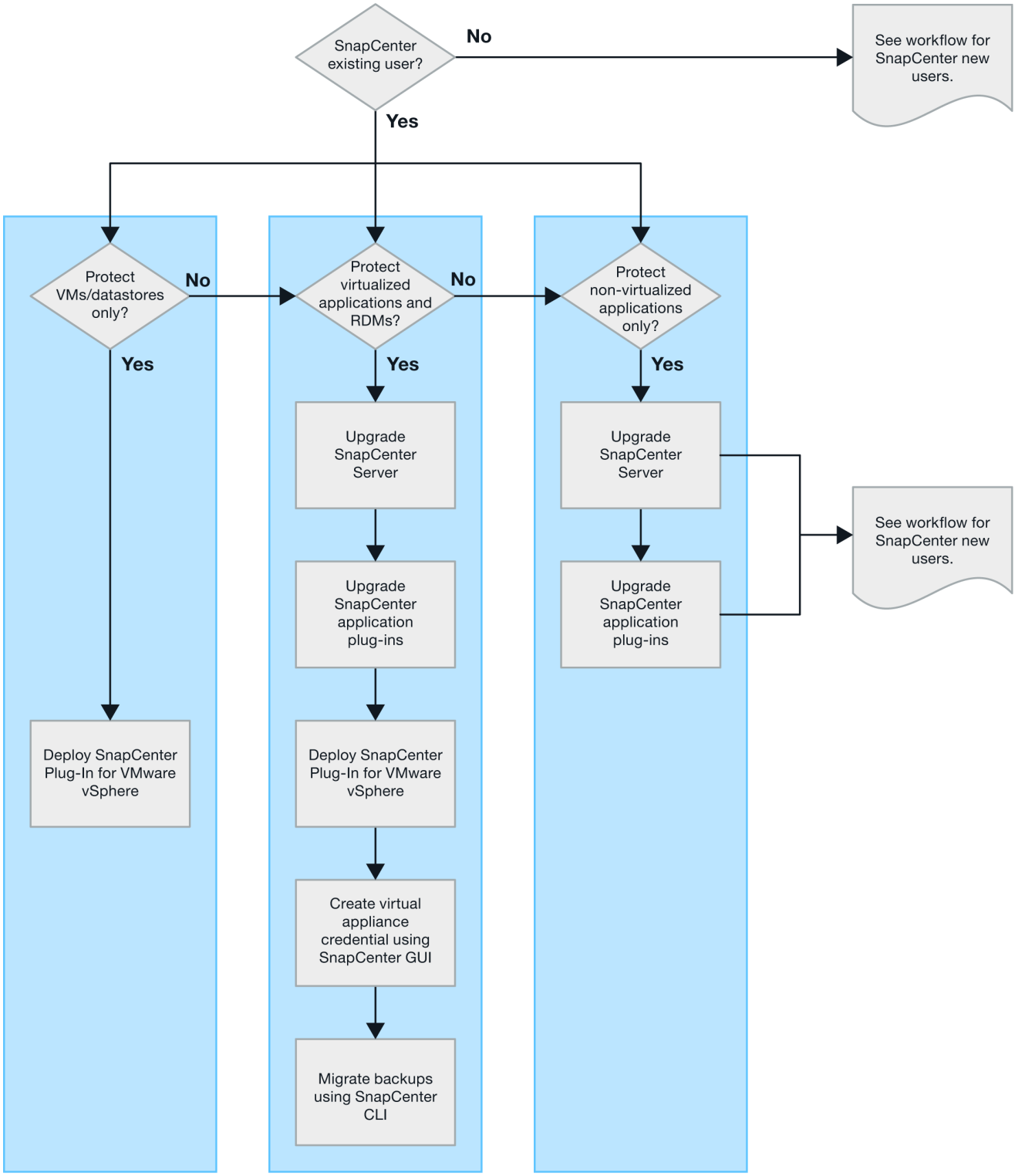
Bereitstellungsübersicht

Um SnapCenter -Funktionen zum Schutz von VMs, Datenspeichern und anwendungskonsistenten Datenbanken auf virtualisierten Maschinen zu verwenden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen.

Vorhandene SnapCenter Benutzer müssen einen anderen Bereitstellungsworkflow verwenden als neue SnapCenter Benutzer.

Bereitstellungsworkflow für vorhandene Benutzer

Wenn Sie ein SnapCenter -Benutzer sind und über SnapCenter -Backups verfügen, verwenden Sie für den Einstieg den folgenden Workflow.



Voraussetzungen für die Bereitstellung von SCV

Bereitstellungsplanung und -anforderungen

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

Host-Anforderungen

Bevor Sie mit der Bereitstellung des SnapCenter Plug-in for VMware vSphere (SCV) beginnen, sollten Sie mit den Hostanforderungen vertraut sein.

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

  Sicherungspläne werden in der Zeitzone ausgeführt, in der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird, und vCenter meldet Daten in der Zeitzone, in der es sich befindet. Wenn sich das SnapCenter Plug-in for VMware vSphere und vCenter in unterschiedlichen Zeitzonen befinden, stimmen die Daten im SnapCenter Plug-in for VMware vSphere Dashboard möglicherweise nicht mit den Daten in den Berichten überein.

- Sie dürfen das SnapCenter Plug-in for VMware vSphere nicht in einem Ordner bereitstellen, dessen Name Sonderzeichen enthält.

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

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

    Angenommen, Sie möchten Sicherungen von sechs verschiedenen Instanzen des vCenter Servers durchführen. In diesem Fall müssen Sie das SnapCenter Plug-in for VMware vSphere auf sechs Hosts bereitstellen und jeder vCenter-Server muss mit einer eindeutigen Instanz des SnapCenter Plug-in for VMware vSphere gekoppelt werden.

- Um vVol-VMs (VMs auf VMware vVol-Datenspeichern) zu schützen, müssen Sie zunächst ONTAP tools for VMware vSphere bereitstellen. ONTAP -Tools stellen Speicher für vVols auf ONTAP und auf dem VMware-Webclient bereit und konfigurieren ihn.

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

- Das SnapCenter Plug-in for VMware vSphere bietet aufgrund einer Einschränkung der virtuellen Maschinen bei der Unterstützung von Storage vMotion eingeschränkte Unterstützung für gemeinsam genutzte PCI- oder PCIe-Geräte (z. B. NVIDIA Grid GPU). Weitere Informationen finden Sie im Dokument „Bereitstellungshandbuch für VMware“ des Anbieters.
  - Was wird unterstützt:

    Erstellen von Ressourcengruppen

    Erstellen von Backups ohne VM-Konsistenz

    Wiederherstellen einer vollständigen VM, wenn sich alle VMDKs auf einem NFS-Datenspeicher befinden und das Plug-In Storage vMotion nicht verwenden muss

Anhängen und Trennen von VMDKs

Einbinden und Ausbinden von Datenspeichern

Wiederherstellung von Gastdateien

- Was nicht unterstützt wird:

  Erstellen von Backups mit VM-Konsistenz

Wiederherstellen einer vollständigen VM, wenn sich ein oder mehrere VMDKs auf einem VMFS-Datenspeicher befinden.

- Eine detaillierte Liste der Einschränkungen des SnapCenter Plug-in for VMware vSphere finden Sie unter"Versionshinweise zum SnapCenter Plug-in for VMware vSphere" .

Lizenzanforderungen

Sie müssen Lizenzen bereitstellen für…	Lizenzanforderung
ONTAP	Eines davon: SnapMirror oder SnapVault (für sekundären Datenschutz unabhängig von der Art der Beziehung)
Ergänzende Produkte	vSphere Standard, Enterprise oder Enterprise Plus: Für die Durchführung von Wiederherstellungsvorgängen mit Storage vMotion ist eine vSphere-Lizenz erforderlich. vSphere Essentials- oder Essentials Plus-Lizenzen beinhalten kein Storage vMotion.
Primäre Ziele	SnapCenter Standard: erforderlich, um anwendungsbasierten Schutz über VMware durchzuführen. SnapRestore: erforderlich, um Wiederherstellungsvorgänge nur für VMware-VMs und -Datenspeicher durchzuführen. FlexClone: wird nur für Mount- und Attach-Vorgänge auf VMware-VMs und -Datenspeichern verwendet.
Sekundärziele	SnapCenter Standard: wird für Failover-Vorgänge für anwendungsbasierten Schutz über VMware FlexClone verwendet: wird nur für Mount- und Attach-Vorgänge auf VMware-VMs und -Datenspeichern verwendet

Softwareunterstützung

Artikel	Unterstützte Versionen
vCenter vSphere	7.0U1 und höher.
ESXi-Server	7.0U1 und höher.
IP-Adressen	IPv4, IPv6
VMware TLS	1,2, 1,3

Artikel	Unterstützte Versionen
TLS auf dem SnapCenter -Server	1.2, 1.3 Der SnapCenter Server verwendet dies zur Kommunikation mit dem SnapCenter Plug-in for VMware vSphere für Anwendungen über VMDK-Datenschutzvorgänge.
VMware-Anwendung vStorage API für Array-Integration (VAAI)	Das SnapCenter Plug-in for VMware vSphere verwendet dies, um die Leistung bei Wiederherstellungsvorgängen zu verbessern. Es verbessert auch die Leistung 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 Interoperabilitätsmatrix-Tool" .

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

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

Die Mindestsoftwareanforderungen für die Unterstützung der Protokolle NVMe over TCP und NVMe over FC sind:

- vCenter vSphere 7.0U3
- ESXi 7.0U3
- ONTAP 9.10.1

Platz-, Größen- und Skalierungsanforderungen

Artikel	Anforderungen
Empfohlene CPU-Anzahl	8 Kerne
Empfohlener RAM	24 GB
Mindestfestplattenspeicherplatz für das SnapCenter Plug-in for VMware vSphere, Protokolle und MySQL-Datenbank	100 GB
Maximale Heap-Größe des vmcontrol-Dienstes in der Appliance	8 GB

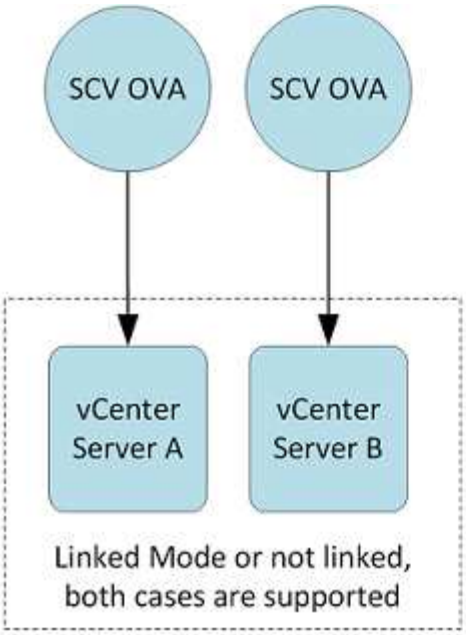
Verbindungs- und Portanforderungen

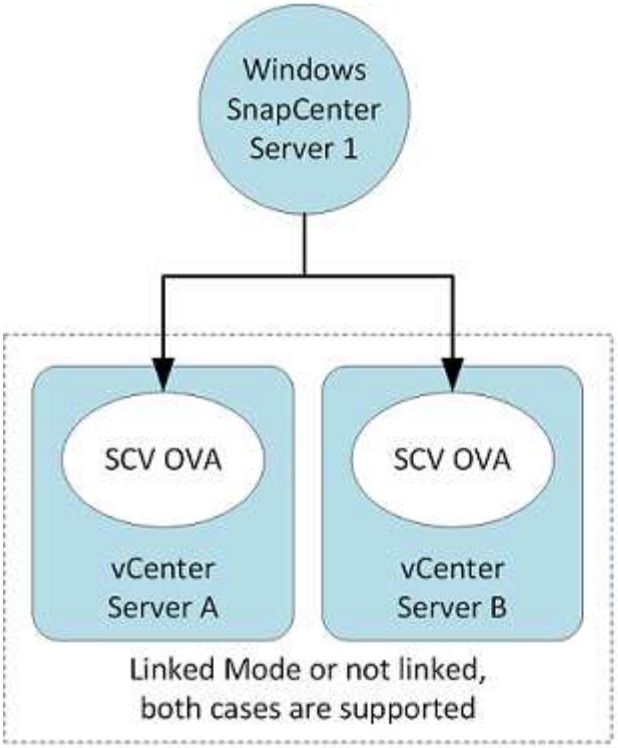
Art des Anschlusses	Vorkonfigurierter Port
VMware ESXi-Server-Port	443 (HTTPS), bidirektional. Die Funktion zur Wiederherstellung von Gastdateien verwendet diesen Port.

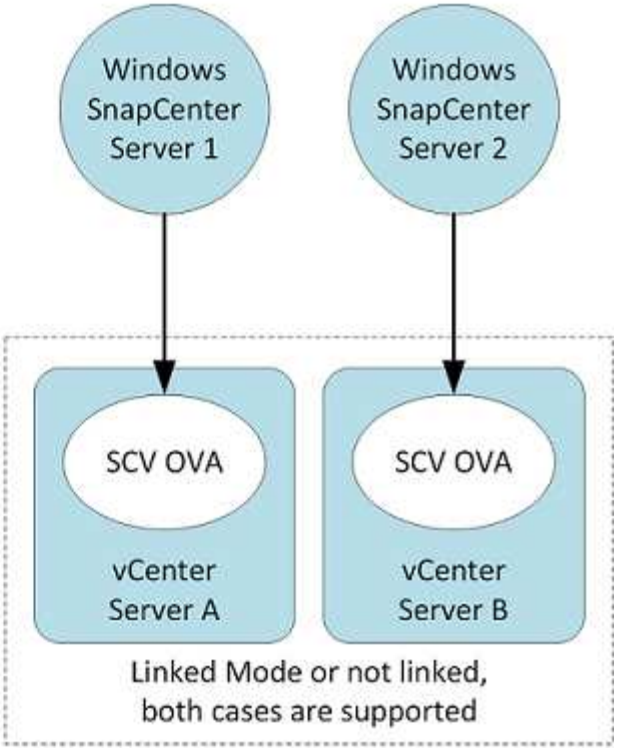
Art des Anschlusses	Vorkonfigurierter Port
SnapCenter Plug-in for VMware vSphere Port	8144 (HTTPS), bidirektional. Der Port wird für die Kommunikation zwischen dem VMware vSphere-Client und dem SnapCenter -Server verwendet. 8080 bidirektional. Dieser Port wird zum Verwalten virtueller Appliances verwendet. Hinweis: Ein benutzerdefinierter Port zum Hinzufügen eines SCV-Hosts zu SnapCenter wird unterstützt.
VMware vSphere vCenter Server-Port	Sie müssen Port 443 verwenden, wenn Sie vVol-VMs schützen.
Speichercluster oder Speicher-VM-Port	443 (HTTPS), bidirektional 80 (HTTP), bidirektional Der Port wird für die Kommunikation zwischen der virtuellen Appliance und der Speicher-VM oder dem Cluster, der die Speicher-VM enthält, verwendet.

Unterstützte Konfigurationen

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







RBAC-Berechtigungen erforderlich

Das vCenter-Administratorkonto muss über die in der folgenden Tabelle aufgeführten erforderlichen vCenter-Berechtigungen verfügen.

So führen Sie diesen Vorgang aus:	Sie müssen über diese vCenter-Berechtigungen verfügen …
Bereitstellen und Registrieren des SnapCenter Plug-in for VMware vSphere in vCenter	Erweiterung: Registererweiterung

So führen Sie diesen Vorgang aus:	Sie müssen über diese vCenter-Berechtigungen verfügen …
Aktualisieren oder entfernen Sie das SnapCenter Plug-in for VMware vSphere	Verlängerung • Update-Erweiterung • Aufheben der Registrierung der Erweiterung
Erlauben Sie dem in SnapCenter registrierten vCenter Credential-Benutzerkonto, den Benutzerzugriff auf das SnapCenter Plug-in for VMware vSphere zu validieren.	Sitzungen.validieren.Sitzung
Benutzern den Zugriff auf das SnapCenter Plug-in for VMware vSphere ermöglichen	SCV-Administrator, SCV-Sicherung, SCV-Gastdateiwiederherstellung, SCV-Wiederherstellung, SCV-Ansicht. Das Recht muss am vCenter-Stamm zugewiesen werden.

AutoSupport

Das SnapCenter Plug-in for VMware vSphere bietet ein Minimum an Informationen zur Verfolgung seiner Nutzung, einschließlich der Plug-in-URL. AutoSupport enthält eine Tabelle mit installierten Plug-Ins, die vom AutoSupport Viewer angezeigt wird.

ONTAP -Berechtigungen erforderlich

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

> Ab SnapCenter Plug-in für VMware (SCV) 5.0 müssen Sie Anwendungen vom Typ HTTP und ONTAPI als Benutzeranmeldemethoden für alle ONTAP Benutzer mit benutzerdefiniertem rollenbasierten Zugriff auf das SCV hinzufügen. Ohne Zugriff auf diese Anwendungen schlagen Backups fehl. Sie müssen den SCV-Dienst neu starten, um Änderungen an den Anmeldemethoden für ONTAP Benutzer zu erkennen.

Mindestens erforderliche ONTAP -Berechtigungen

Alle SnapCenter Plug-Ins erfordern die folgenden Mindestberechtigungen.

Befehle mit vollem Zugriff: Mindestberechtigungen für ONTAP .
Ereignis generieren-Autosupport-Protokoll
Jobverlauf Job anzeigen Job anzeigen Stopp
lun lun erstellen lun löschen lun igroup lun igroup hinzufügen lun igroup erstellen lun igroup löschen lun igroup umbenennen lun igroup anzeigen lun-Mapping Reporting-Nodes hinzufügen lun-Mapping Lun-Mapping erstellen Lun-Mapping löschen Reporting-Nodes entfernen lun-Mapping anzeigen lun ändern lun Volume verschieben lun offline lun online lun persistente Reservierung lun löschen Größe ändern lun seriell lun anzeigen

Snapmirror-Listenziele Snapmirror-Richtlinie Regel hinzufügen Snapmirror-Richtlinie Regel ändern Snapmirror-Richtlinie Regel entfernen Snapmirror-Richtlinie Snapmirror anzeigen Snapmirror wiederherstellen Snapmirror anzeigen Snapmirror-Verlauf anzeigen Snapmirror aktualisieren Snapmirror Update-LS-Set
Version
Volume klonen Volume klonen Volume anzeigen Klonaufteilung starten Volume klonen Aufteilungsstatus Volume klonen Aufteilung stoppen Volume erstellen Volume löschen Volume zerstören Datei klonen Volume erstellen Datei anzeigen Datenträgernutzung anzeigen Volume offline Volume online Volume verwaltete Funktion Volume ändern Volume Qtree Volume erstellen Qtree Volume löschen Qtree Volume ändern Qtree Volume anzeigen Volume einschränken Volume anzeigen Volume-Snapshot erstellen Volume-Snapshot löschen Volume-Snapshot ändern Ablaufzeit der Snaplock ändern Volume-Snapshot umbenennen Volume-Snapshot wiederherstellen Datei wiederherstellen Volume-Snapshot Volume-Snapshot anzeigen Volume-Delta anzeigen aushängen
vserver cifs vserver cifs share erstellen vserver cifs share löschen vserver cifs shadowcopy anzeigen vserver cifs share anzeigen vserver cifs anzeigen vserver export-policy anzeigen vserver export-policy erstellen vserver export-policy löschen vserver export-policy rule erstellen vserver export-policy rule anzeigen vserver export-policy anzeigen vserver iscsi vserver iscsi connection anzeigen vserver nvme subsystem controller vserver nvme subsystem controller anzeigen vserver nvme subsystem erstellen vserver nvme subsystem löschen vserver nvme subsystem host vserver nvme subsystem host anzeigen vserver nvme subsystem host hinzufügen vserver nvme subsystem host entfernen vserver nvme subsystem map vserver nvme subsystem map anzeigen vserver nvme subsystem map hinzufügen vserver nvme subsystem map entfernen vserver nvme subsystem ändern vserver nvme subsystem anzeigen vserver nvme namespace erstellen vserver nvme namespace löschen vServer NVMe-Namespace ändern vServer NVMe-Namespace Netzwerkschnittstelle anzeigen Netzwerkschnittstelle Failover-Gruppen

Schreibgeschützte Befehle: Privileges für ONTAP
Clusteridentität anzeigen Netzwerkschnittstelle anzeigen VServer VServer-Peer VServer anzeigen

All-Access-Befehle: Mindestberechtigungen für ONTAP
Konsistenzgruppen-Speichereinheit anzeigen

Sie können den Befehl *cluster identity show* auf Clusterebene ignorieren, wenn Sie eine Rolle erstellen, die dem Daten-vServer zugeordnet werden soll.

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

Zusätzliche ONTAP -Informationen

- Sie benötigen ONTAP 9.12.1 oder eine spätere Version, um die SnapMirror Active Sync-Funktion zu verwenden.
- So verwenden Sie die TamperProof Snapshot (TPS)-Funktion:
  - Sie benötigen ONTAP 9.13.1 und spätere Versionen für SAN
  - Sie benötigen ONTAP 9.12.1 und spätere Versionen für NFS
- Für NVMe über TCP und NVMe über 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 verwenden Sie RestAPI zum Bearbeiten von Konfigurationsparametern in SCV" für weitere Informationen.

Mindestens erforderliche vCenter-Berechtigungen

Bevor Sie mit der Bereitstellung des SnapCenter Plug-in for VMware vSphere beginnen, sollten Sie sicherstellen, dass Sie über die erforderlichen Mindestberechtigungen für vCenter verfügen.

Erforderliche Berechtigungen für die vCenter-Administratorrolle

Datastore.Platz zuweisen Datastore.Durchsuchen Datastore.Löschen Datastore.Dateiverwaltung Datastore.Verschieben Datastore.Umbenennen Erweiterung.Registrieren Erweiterung.Registrierung aufheben Erweiterung.Aktualisieren Host.Konfiguration.ErweiterteKonfiguration Host.Konfiguration.Ressourcen Host.Konfiguration.Einstellungen Host.Konfiguration.Speicher Host.Lokal.VM erstellen Host.Lokal.VM löschen Host.Lokal.VM neu konfigurieren Netzwerk.Zuweisen Ressource.Empfehlung anwenden Ressource.VM einem Pool zuweisen Ressource.Kaltmigration Ressource.Hotmigration Ressource.VM abfragen System.Anonym System.Lesen System.Anzeigen Task.Erstellen Task.Aktualisieren VirtualMachine.Konfiguration.VorhandeneDisk hinzufügen VirtualMachine.Konfiguration.NeueDisk hinzufügen VirtualMachine.Konfiguration.ErweiterteKonfiguration VirtualMachine.Konfiguration.VomPfad neu laden VirtualMachine.Konfiguration.Disk entfernen VirtualMachine.Konfiguration.Ressource VirtualMachine.GuestOperations.Ausführen VirtualMachine.GuestOperations.Modify VirtualMachine.GuestOperations.Query VirtualMachine.Interact.PowerOff VirtualMachine.Interact.PowerOn VirtualMachine.Inventory.Create VirtualMachine.Inventory.CreateFromExisting VirtualMachine.Inventory.Delete VirtualMachine.Inventory.Move VirtualMachine.Inventory.Register VirtualMachine.Inventory.Unregister VirtualMachine.State.CreateSnapshot VirtualMachine.State.RemoveSnapshot VirtualMachine.State.RevertToSnapshot

Erforderliche Berechtigungen speziell für das SnapCenter Plug-in für VMware vCenter

* Privileges*	**Etikett**
netappSCV.Guest.RestoreFile	Wiederherstellung der Gastdatei
netappSCV.Recovery.MountUnMount	Einhängen/Aushängen
netappSCV.Backup.DeleteBackupJob	Ressourcengruppe/Backup löschen
netappSCV.Configure.ConfigureStorageSystems.Delete	Speichersysteme entfernen
netappSCV.View	Anzeigen
netappSCV.Recovery.RecoverVM	VM wiederherstellen
netappSCV.Configure.ConfigureStorageSystems.AddUpdate	Speichersysteme hinzufügen/ändern
netappSCV.Backup.BackupNow	Jetzt sichern
netappSCV.Guest.Configure	Gastkonfiguration

netappSCV.Configure.ConfigureSnapCenterServer	SnapCenter Server konfigurieren
netappSCV.Backup.BackupScheduled	Ressourcengruppe erstellen

Laden Sie die Open Virtual Appliance (OVA) herunter

Fügen Sie vor der Installation der Open Virtual Appliance (OVA) das Zertifikat zum vCenter hinzu. Die TAR-Datei enthält die OVA- und Entrust-Stamm- und Zwischenzertifikate. Die Zertifikate befinden sich im Zertifikatsordner. Die OVA-Bereitstellung wird in VMware vCenter 7u1 und höher unterstützt.

In VMware vCenter-Versionen ab 7.0.3 wird der mit dem Entrust-Zertifikat signierten OVA nicht mehr vertraut. Sie müssen das folgende Verfahren durchführen, um das Problem zu beheben.

Schritte

1. So laden Sie das SnapCenter -Plug-in für VMware herunter:
   - Melden Sie sich bei der NetApp Support Site an ("https://mysupport.netapp.com/products/index.html").
   - Wählen Sie aus der Produktliste * SnapCenter Plug-in for VMware vSphere* und dann die Schaltfläche **Neueste Version herunterladen**.
   - Laden Sie das SnapCenter Plug-in for VMware vSphere herunter `.tar` Datei an einen beliebigen Ort.
2. Extrahieren Sie den Inhalt der TAR-Datei. Die TAR-Datei enthält den OVA- und Zertifikatsordner. Der Ordner „Certs“ enthält die Stamm- und Zwischenzertifikate von Entrust.
3. Melden Sie sich mit dem vSphere-Client beim vCenter Server an.
4. Navigieren Sie zu **Administration > Zertifikate > Zertifikatsverwaltung**.
5. Wählen Sie neben **Vertrauenswürdige Stammzertifikate** die Option **Hinzufügen**
   - Gehen Sie zum Ordner *certs*.
   - Wählen Sie die Entrust-Stamm- und Zwischenzertifikate aus.
   - Installieren Sie jedes Zertifikat einzeln.
6. Die Zertifikate werden einem Panel unter **Vertrauenswürdige Stammzertifikate** hinzugefügt. Sobald die Zertifikate installiert sind, kann OVA überprüft und bereitgestellt werden.

> Wenn die heruntergeladene OVA-Datei nicht manipuliert wurde, wird in der Spalte **Herausgeber Vertrauenswürdiges Zertifikat** angezeigt.

Bereitstellen des SnapCenter Plug-in for VMware vSphere

Um SnapCenter -Funktionen zum Schutz von VMs, Datenspeichern und anwendungskonsistenten Datenbanken auf virtualisierten Maschinen zu verwenden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen.

Bevor Sie beginnen

In diesem Abschnitt sind alle erforderlichen Aktionen aufgeführt, die Sie ausführen sollten, bevor Sie mit der Bereitstellung beginnen.

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

- Sie müssen die Bereitstellungsanforderungen gelesen haben.
- Sie müssen eine unterstützte Version von vCenter Server ausführen.
- Sie müssen Ihre vCenter Server-Umgebung konfiguriert und eingerichtet haben.
- Sie müssen einen ESXi-Host für das SnapCenter Plug-in for VMware vSphere VM eingerichtet haben.
- Sie müssen die TAR-Datei des SnapCenter Plug-in for VMware vSphere heruntergeladen haben.
- Sie müssen über die Anmeldeauthentifizierungsdaten für Ihre vCenter Server-Instanz verfügen.
- Sie müssen über ein Zertifikat mit gültigen öffentlichen und privaten Schlüsseldateien verfügen. Weitere Informationen finden Sie in den Artikeln unter "Speicherzertifikatsverwaltung" Abschnitt.
- Sie müssen sich abgemeldet und alle Browsersitzungen des vSphere-Clients geschlossen und den Browser-Cache gelöscht haben, um Probleme mit dem Browser-Cache während der Bereitstellung des SnapCenter Plug-in for VMware vSphere zu vermeiden.
- Sie müssen Transport Layer Security (TLS) in vCenter aktiviert haben. 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, müssen der ESXi-Server, das SnapCenter Plug-in for VMware vSphere und jedes vCenter auf dieselbe Zeit synchronisiert werden.
- Um VMs auf vVol-Datenspeichern zu schützen, müssen Sie zunächst ONTAP tools for VMware vSphere bereitstellen. Die neuesten Informationen zu unterstützten Versionen der ONTAP Tools finden Sie unter "NetApp Interoperabilitätsmatrix-Tool" . ONTAP -Tools stellen Speicher auf ONTAP und auf dem VMware-Webclient bereit und konfigurieren ihn.

Stellen Sie das SnapCenter Plug-in for VMware vSphere in derselben Zeitzone wie das vCenter bereit. Sicherungspläne werden in der Zeitzone ausgeführt, in der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. vCenter meldet Daten in der Zeitzone, in der sich das vCenter befindet. Wenn sich das SnapCenter Plug-in for VMware vSphere und vCenter in unterschiedlichen Zeitzonen befinden, stimmen die Daten im SnapCenter Plug-in for VMware vSphere Dashboard möglicherweise nicht mit den Daten in den Berichten überein.

Schritte

1. Für VMware vCenter 7.0.3 und spätere Versionen folgen Sie den Schritten in"Laden Sie die Open Virtual Appliance (OVA) herunter" um die Zertifikate in vCenter zu importieren.
2. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.

   Für HTML-Webclients mit IPv6-Adressen 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 Inventarobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Rechenzentrum, ein Cluster oder ein Host, und wählen Sie **OVF-Vorlage bereitstellen** aus, um den VMware-Bereitstellungsassistenten zu starten.
5. Extrahieren Sie die TAR-Datei, die die OVA-Datei enthält, auf Ihr lokales System. Geben Sie auf der Seite **Wählen Sie eine OVF-Vorlage** den Speicherort der `.ova` Datei im extrahierten .tar-Ordner.
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 klicken Sie dann auf **Weiter**.

   Dieser Schritt gibt an, wohin die `.tar` Datei in vCenter. Der Standardname für die VM ist derselbe wie der Name der ausgewählten `.ova` Datei. Wenn Sie den Standardnamen ändern, wählen Sie einen Namen, der innerhalb jedes vCenter Server-VM-Ordners eindeutig ist.

   Der Standardbereitstellungsort für die VM ist das Inventarobjekt, bei dem Sie den Assistenten gestartet haben.

8. Wählen Sie auf der Seite **Ressource auswählen** die Ressource aus, auf der Sie die bereitgestellte VM-Vorlage ausführen möchten, und wählen Sie **Weiter**.
9. Überprüfen Sie auf der Seite **Details überprüfen** die `.tar` Vorlagendetails und wählen Sie **Weiter**.
10. Aktivieren Sie auf der Seite **Lizenzvereinbarungen** das Kontrollkästchen **Ich akzeptiere alle Lizenzvereinbarungen**.
11. Definieren Sie auf der Seite **Speicher auswählen**, 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 auf der Zielressource Speicherrichtlinien aktiviert sind.

    c. Wählen Sie einen Datenspeicher zum Speichern der bereitgestellten OVA-Vorlage aus.

       Die Konfigurationsdatei und die virtuellen Festplattendateien werden im Datenspeicher gespeichert.

    Wählen Sie einen Datenspeicher aus, der groß genug 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 „Quellnetzwerk“ werden alle Netzwerke aufgelistet, die in der OVA-Vorlage definiert sind.

    b. Wählen Sie im Abschnitt **IP-Zuweisungseinstellungen** das gewünschte IP-Adressprotokoll aus und klicken Sie dann auf **Weiter**.

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

13. Führen Sie auf der Seite **Vorlage anpassen** die folgenden Schritte aus:

    a. Geben Sie im Abschnitt **Bei vorhandenem vCenter registrieren** den vCenter-Namen und die vCenter-Anmeldeinformationen der virtuellen Appliance ein.

       Geben Sie im Feld **vCenter-Benutzername** den Benutzernamen im Format `domain\username` .

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

       Geben Sie im Feld **Benutzername** den lokalen Benutzernamen ein. Geben Sie die Domänendetails nicht an.

> Notieren Sie sich den Benutzernamen und das Passwort, die Sie angeben. Sie müssen diese Anmeldeinformationen verwenden, wenn Sie die Konfiguration des SnapCenter Plug-in for VMware vSphere später ändern möchten.

c. Geben Sie die Anmeldeinformationen für den Wartungsbenutzer ein.

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

   i. Geben Sie im Abschnitt **IPv4-Netzwerkeigenschaften einrichten** die Netzwerkinformationen ein, z. B. 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, primären IPv6-DNS, sekundären IPv6-DNS und IPv6-Suchdomänen.

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

> Sie können diese Schritte überspringen und die Einträge im Abschnitt **Netzwerkeigenschaften einrichten** leer lassen, wenn Sie mit DHCP als Netzwerkkonfiguration fortfahren möchten.

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

14. Überprüfen Sie die Seite **Bereit zum Abschließen** und wählen Sie **Fertig**.

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

    Sie können den Fortschritt der Bereitstellung im Fenster „Letzte Aufgaben“ anzeigen, während Sie auf den Abschluss der OVF-Import- und Bereitstellungsaufgaben warten.

    Wenn das SnapCenter Plug-in for 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 for VMware vSphere bereitgestellt wurde, wählen Sie dann die Registerkarte **Zusammenfassung** und anschließend das Feld **Einschalten** aus, um die virtuelle Appliance zu starten.

16. Klicken Sie beim Einschalten des SnapCenter Plug-in for VMware vSphere mit der rechten Maustaste auf das bereitgestellte SnapCenter Plug-in for VMware vSphere, wählen Sie **Gastbetriebssystem** und dann **VMware-Tools installieren**.

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

    Die Bereitstellung kann einige Minuten dauern. Eine erfolgreiche Bereitstellung wird angezeigt, wenn das SnapCenter Plug-in for VMware vSphere eingeschaltet ist, die VMware-Tools installiert sind und Sie auf dem Bildschirm aufgefordert werden, sich beim SnapCenter Plug-in for VMware vSphere anzumelden. Sie können Ihre Netzwerkkonfiguration beim ersten Neustart von DHCP auf statisch umstellen. Das Umschalten von statisch auf 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 Verwaltungs-GUI 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 im Bereitstellungsassistenten angegebenen Anmeldeinformationen bei der Verwaltungs-GUI des SnapCenter Plug-in for 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 Verwaltungs-GUI zuzugreifen.

    Melden Sie sich mit dem zum Zeitpunkt der Bereitstellung festgelegten Administratorbenutzernamen und -kennwort sowie dem mithilfe der Wartungskonsole generierten MFA-Token an.

    Wenn das SnapCenter Plug-in for VMware vSphere nicht aktiviert ist, lesen Sie"Starten Sie den VMware vSphere-Clientdienst neu" .

    Wenn der Hostname „UnifiedVSC/SCV“ lautet, starten Sie das Gerät neu. Wenn der Neustart der Appliance den Hostnamen nicht in den angegebenen Hostnamen ändert, müssen Sie die Appliance neu installieren.

Nach Abschluss

Sie sollten die erforderlichen"Vorgänge nach der Bereitstellung" .

Nach der Bereitstellung erforderliche Vorgänge und Probleme

Nach der Bereitstellung des SnapCenter Plug-in for VMware vSphere müssen Sie die Installation abschließen.

Erforderliche Vorgänge nach der Bereitstellung

Wenn Sie ein neuer SnapCenter Benutzer sind, müssen Sie SnapCenter Speicher-VMs hinzufügen, bevor Sie Datenschutzvorgänge durchführen können. Geben Sie beim Hinzufügen von Speicher-VMs das Verwaltungs-LIF an. Sie können auch einen Cluster hinzufügen und das LIF für die Clusterverwaltung angeben. Informationen zum Hinzufügen von Speicher finden Sie unter"Speicher hinzufügen" .

Mögliche Bereitstellungsprobleme

- Nach der Bereitstellung der virtuellen Appliance wird die Registerkarte **Sicherungsaufträge** im Dashboard in den folgenden Szenarien möglicherweise nicht geladen:
  - Sie verwenden eine IPv4-Adresse und haben zwei IP-Adressen für den SnapCenter VMware vSphere-Host. Infolgedessen 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 for VMware vSphere bereitgestellt wird: `/opt/netapp/scvservice/standalone_aegis/etc`
    ii. Öffnen Sie die Datei network-interface.properties.
    iii. Im `network.interface=10.10.10.10` Fügen Sie im Feld die IP-Adresse hinzu, die Sie verwenden möchten.

    - Sie haben zwei Netzwerkkarten.
- Nach der Bereitstellung des SnapCenter Plug-in for VMware vSphere zeigt der MOB-Eintrag in vCenter für das SnapCenter Plug-in for VMware vSphere möglicherweise noch die alte Versionsnummer an. Dies kann auftreten, wenn andere Jobs im vCenter ausgeführt werden. vCenter aktualisiert den Eintrag schließlich.

Um eines dieser Probleme zu beheben, gehen Sie wie folgt vor:

1. Leeren Sie den Browser-Cache und prüfen Sie dann, ob die GUI ordnungsgemäß funktioniert.

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

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

Verwalten von Authentifizierungsfehlern

Wenn Sie die Administratoranmeldeinformationen nicht verwenden, wird nach der Bereitstellung des SnapCenter Plug-in for VMware vSphere oder nach der Migration möglicherweise 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 Management GUI 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 for VMware vSphere beim SnapCenter -Server

Wenn Sie Application-over-VMDK-Workflows in SnapCenter ausführen möchten (anwendungsbasierte Schutz-Workflows für virtualisierte Datenbanken und Dateisysteme), müssen Sie das SnapCenter Plug-in for VMware vSphere beim SnapCenter Server registrieren.

Bevor Sie beginnen

- Sie müssen SnapCenter Server 4.2 oder höher ausführen.
- Sie müssen das SnapCenter Plug-in for VMware vSphere bereitgestellt und aktiviert haben.

Informationen zu diesem Vorgang

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

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

  Sie können mehrere Instanzen des SnapCenter Plug-in for VMware vSphere auf demselben SnapCenter -Server registrieren, um anwendungsbasierte Datenschutzvorgänge auf VMs zu unterstützen. Sie können dasselbe SnapCenter Plug-in for VMware vSphere nicht auf mehreren SnapCenter Servern registrieren.

- Für vCenter im verknüpften Modus müssen Sie das SnapCenter Plug-in for VMware vSphere für jedes vCenter registrieren.

Schritte

1. Wählen Sie im linken Navigationsbereich der SnapCenter -GUI **Hosts** aus.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist, suchen Sie dann den Hostnamen der virtuellen Appliance und stellen Sie sicher, dass er 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…	Mach das…
Hosttyp	Wählen Sie **vSphere** als Hosttyp aus.
Hostname	Überprüfen Sie die IP-Adresse der virtuellen Appliance.
Anmeldeinformationen	Geben Sie den Benutzernamen und das Kennwort für das SnapCenter Plug-in for 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 „Verwaltete Hosts“ angezeigt.

6. Wählen Sie im linken Navigationsbereich **Einstellungen**, dann die Registerkarte **Anmeldeinformationen** und anschließend **Hinzufügen** aus, um Anmeldeinformationen für die virtuelle Appliance hinzuzufügen.
7. Geben Sie die Anmeldeinformationen an, die während der Bereitstellung des SnapCenter Plug-in for VMware vSphere angegeben wurden.

   Sie müssen im Feld „Authentifizierung“ Linux auswählen.

Nach Abschluss

Wenn die Anmeldeinformationen des SnapCenter Plug-in for VMware vSphere 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 for VMware vSphere bereitgestellt wird, installiert es einen VMware vSphere-Client auf vCenter, der zusammen mit anderen vSphere-Clients auf dem vCenter-Bildschirm angezeigt wird.

Bevor Sie beginnen

Transport Layer Security (TLS) muss in vCenter aktiviert sein. Weitere Informationen finden Sie in der 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.

Wählen Sie die Schaltfläche **Anmelden**. Aufgrund eines bekannten VMware-Problems verwenden Sie zur Anmeldung nicht die Eingabetaste. 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** in der Symbolleiste „Menü“ und dann „SnapCenter Plug-in for VMware vSphere“ aus.

Schnellstart

Überblick

Die Schnellstartdokumentation enthält eine komprimierte Anleitung zum Bereitstellen des SnapCenter Plug-in for VMware vSphere Appliance und zum Aktivieren des SnapCenter Plug-in for VMware vSphere. Diese Anweisungen richten sich an Kunden, die SnapCenter noch nicht installiert haben und nur VMs und Datenspeicher schützen möchten.

Bevor Sie beginnen, lesen Sie"Bereitstellungsplanung und -anforderungen" .

Bereitstellen des SnapCenter Plug-in for VMware vSphere

Um SnapCenter -Funktionen zum Schutz von VMs, Datenspeichern und anwendungskonsistenten Datenbanken auf virtualisierten Maschinen zu verwenden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen. Der"Laden Sie die Open Virtual Appliance (OVA) herunter" Seite enthält Anweisungen zum Herunterladen der OVA-Dateien.

1. Für VMware vCenter 7.0.3 und spätere Versionen folgen Sie den Schritten in"Laden Sie die Open Virtual Appliance (OVA) herunter" um die Zertifikate in vCenter zu importieren.
2. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.

   Für HTML-Webclients mit IPv6-Adressen müssen Sie entweder Chrome oder Firefox verwenden.

3. Melden Sie sich auf der **VMware vCenter Single Sign-On-Seite** an.
4. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf ein beliebiges Bestandsobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Rechenzentrum, Ordner, Cluster oder 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 `.ova` Datei (wie in der folgenden Tabelle aufgeführt) und wählen Sie **Weiter**.

Auf dieser Assistentenseite …	Mach das…
Wählen Sie einen Namen und einen Ordner	Geben Sie einen eindeutigen Namen für die VM oder vApp ein und wählen Sie einen Bereitstellungsort aus.
Wählen Sie eine Ressource aus	Wählen Sie eine Ressource aus, auf der Sie die bereitgestellte VM-Vorlage ausführen möchten.
Bewertungsdetails	Überprüfen Sie die `.ova` Vorlagendetails.
Lizenzvereinbarungen	Aktivieren Sie das Kontrollkästchen **Ich akzeptiere alle Lizenzvereinbarungen**.

Auf dieser Assistentenseite …	Mach das…
Speicher auswählen	Definieren Sie, wo und wie die Dateien für die bereitgestellte OVF-Vorlage gespeichert werden sollen.
Netzwerke auswählen	Wählen Sie ein Quellnetzwerk aus und ordnen Sie es einem Zielnetzwerk zu.
Vorlage anpassen	Geben Sie unter **Bei vorhandenem vCenter registrieren** die vCenter-Anmeldeinformationen ein. Geben Sie unter **Anmeldeinformationen für SnapCenter Plug-in for VMware vSphere erstellen** die Anmeldeinformationen für SnapCenter Plug-in for VMware vSphere ein. Notieren Sie sich den Benutzernamen und das Passwort, die Sie angeben. Sie müssen diese Anmeldeinformationen 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 **Datum und Uhrzeit einrichten** die Zeitzone aus, in der sich das vCenter befindet.
Bereit zum Abschließen	Überprüfen Sie die Seite und wählen Sie **Fertig**.

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

6. Navigieren Sie zu der VM, auf der das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde, wählen Sie dann die Registerkarte **Zusammenfassung** und anschließend das Feld **Einschalten** aus, um das SnapCenter Plug-in for VMware vSphere zu starten.
7. Klicken Sie beim Einschalten des SnapCenter Plug-in for VMware vSphere mit der rechten Maustaste auf das bereitgestellte SnapCenter Plug-in for VMware vSphere, wählen Sie **Gastbetriebssystem** und dann **VMware-Tools installieren**.

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

des SnapCenter Plug-in for VMware vSphere für 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 Verwaltungs-GUI zuzugreifen.

Melden Sie sich mit dem zum Zeitpunkt der Bereitstellung festgelegten Administratorbenutzernamen und -kennwort sowie dem mithilfe der Wartungskonsole generierten MFA-Token an.

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

Speicher hinzufügen

Befolgen Sie die Schritte in diesem Abschnitt, um Speicher hinzuzufügen.

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Speichersysteme** und dann die Option **Hinzufügen** aus.
2. Geben Sie im Dialogfeld „Speichersystem hinzufügen“ die grundlegenden SVM- oder Clusterinformationen ein und wählen Sie **Hinzufügen**.

Erstellen von Sicherungsrichtlinien

Befolgen Sie die unten stehenden Anweisungen, um Sicherungsrichtlinien zu erstellen

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins „Richtlinien“ und dann „Neue Richtlinie“ aus.
2. Geben Sie auf der Seite **Neue Sicherungsrichtlinie** die Richtlinienkonfigurationsinformationen ein und wählen Sie dann **Hinzufügen** aus.

Erstellen von Ressourcengruppen

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

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Ressourcengruppen** und dann **Erstellen** aus.
2. Geben Sie auf jeder Seite des Assistenten „Ressourcengruppe erstellen“ die erforderlichen Informationen ein, wählen Sie VMs und Datenspeicher aus, die in die Ressourcengruppe aufgenommen werden sollen, und wählen Sie dann die Sicherungsrichtlinien aus, die auf die Ressourcengruppe angewendet werden sollen. Fügen Sie die Details zum sekundären Remoteschutz hinzu und geben Sie den Sicherungszeitplan an.

Sicherungen werden gemäß den für die Ressourcengruppe konfigurierten Sicherungsrichtlinien durchgeführt.

Sie können auf der Seite **Ressourcengruppen** eine Sicherung nach Bedarf durchführen, indem Sie **Jetzt ausführen**.

Überwachen und berichten

Statusinformationen anzeigen

Sie können Statusinformationen auf dem Dashboard des vSphere-Clients anzeigen. Die Statusinformationen werden stündlich aktualisiert.

Schritte

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

Diese Dashboard-Kachel …	Zeigt die folgenden Informationen an …
Aktuelle berufliche Tätigkeiten	Die drei bis fünf aktuellsten Sicherungs-, Wiederherstellungs- und Bereitstellungsaufträge. • Wählen Sie eine Job-ID aus, um weitere Details zu diesem Job anzuzeigen. • Wählen Sie **Alle anzeigen**, um zur Registerkarte „Job-Monitor“ zu gelangen und weitere Details zu allen Jobs anzuzeigen.
Jobs	Eine Zählung aller Auftragstypen (Sicherung, Wiederherstellung und Bereitstellung), die innerhalb des ausgewählten Zeitfensters ausgeführt wurden. Bewegen Sie den Cursor über einen Abschnitt des Diagramms, um weitere Details zu dieser Kategorie anzuzeigen.

Diese Dashboard-Kachel …	Zeigt die folgenden Informationen an …
Neueste Schutzzusammenfassung	Zusammenfassungen des Datenschutzstatus primärer und sekundärer VMs oder Datenspeicher innerhalb des ausgewählten Zeitfensters. • Wählen Sie im Dropdown-Menü **VMs** oder **Datastores** aus. • Wählen Sie als sekundären Speicher * SnapVault* oder * SnapMirror*. • Bewegen Sie den Cursor über einen Abschnitt eines Diagramms, um die Anzahl der VMs oder Datenspeicher in dieser Kategorie anzuzeigen. In der Kategorie „Erfolgreich“ wird für jede Ressource das aktuellste Backup aufgelistet. • Sie können das Zeitfenster ändern, indem Sie die Konfigurationsdatei bearbeiten. Der Standardwert beträgt 7 Tage. Weitere Informationen finden Sie unter "Passen Sie Ihre Konfiguration an" . • Interne Zähler werden nach jeder primären oder sekundären Sicherung 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 Schutzzusammenfassung im SnapVault Zusammenfassungsdiagramm und nicht im SnapMirror Diagramm angezeigt.
Konfiguration	Die Gesamtzahl aller Objekttypen, die vom SnapCenter Plug-in for VMware vSphere verwaltet werden.
Storage	Die Gesamtzahl der generierten Snapshots, SnapVault und SnapMirror -Snapshots und die für primäre und sekundäre Snapshots verwendete Speichermenge. Das Liniendiagramm stellt den Primär- und Sekundärspeicherverbrauch über einen rollierenden 90-Tage-Zeitraum hinweg getrennt auf Tagesbasis dar. Die Speicherinformationen werden alle 24 Stunden um 1:08 Uhr aktualisiert. Die Speichereinsparungen sind das Verhältnis der logischen Kapazität (Snapshot-Einsparungen plus verbrauchter Speicher) zur physischen Kapazität des Primärspeichers. Das Balkendiagramm veranschaulicht die Speichereinsparungen. Bewegen Sie den Cursor über eine Linie im Diagramm, um detaillierte Tagesergebnisse anzuzeigen.

Überwachen von Jobs

Nachdem Sie mit dem VMware vSphere-Client einen Datenschutzvorgang durchgeführt haben, können Sie den Jobstatus auf der Registerkarte „Job Monitor“ im Dashboard überwachen und Jobdetails anzeigen.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV **Dashboard** aus.
3. Wenn zwei oder mehr vCenter im verknüpften Modus konfiguriert sind, wählen Sie die SCV-Plug-In-Instanz und wählen Sie die Registerkarte **Job Monitor**. Auf der Registerkarte „Job Monitor“ werden alle Jobs und ihr Status sowie ihre Start- und Endzeit aufgelistet. Wenn die Jobnamen lang sind, müssen Sie möglicherweise nach rechts scrollen, um die Start- und Endzeiten anzuzeigen. Die Anzeige wird alle 30 Sekunden aktualisiert.
   - Wählen Sie das Aktualisierungssymbol in der Symbolleiste, 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 berücksichtigt die Groß- und Kleinschreibung.
   - Wählen Sie das Aktualisierungssymbol im Fenster „Auftragsdetails“ aus, um die Anzeige während der Ausführung des Auftrags zu aktualisieren.

Wenn das Dashboard keine Jobinformationen anzeigt, lesen Sie "KB-Artikel: SnapCenter vSphere-Client-Dashboard zeigt keine Jobs an" .

Jobprotokolle herunterladen

Sie können die Jobprotokolle von der Registerkarte „Job Monitor“ im Dashboard des SnapCenter VMware vSphere-Clients herunterladen.

Wenn bei der Verwendung des VMware vSphere-Clients unerwartetes Verhalten auftritt, können Sie die Protokolldateien verwenden, um die Ursache zu ermitteln und das Problem zu beheben.

> Der Standardwert für die Aufbewahrung von Jobprotokollen beträgt 30 Tage; der Standardwert für die Aufbewahrung von Jobs beträgt 90 Tage. Jobprotokolle und Jobs, die älter als die konfigurierte Aufbewahrungsdauer sind, werden alle sechs Stunden gelöscht. Sie können die Konfiguration verwenden `jobs/cleanup` REST-APIs zum Ändern der Aufbewahrungsdauer von Jobs und Jobprotokollen. Sie können den Bereinigungszeitplan nicht ändern.

Schritte

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

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

   Sie können auch auf einen Job doppelklicken, um auf das Fenster „Jobdetails“ zuzugreifen, und dann

„Jobprotokolle herunterladen“ auswählen.

Ergebnis

Jobprotokolle befinden sich auf dem Linux-VM-Host, auf dem das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. Der Standardspeicherort des Jobprotokolls ist `/var/log/netapp` .

Wenn Sie versucht haben, Jobprotokolle herunterzuladen, die in der Fehlermeldung genannte Protokolldatei jedoch gelöscht wurde, tritt möglicherweise der folgende Fehler auf: `HTTP ERROR 500 Problem accessing /export-scv-logs` . Um diesen Fehler zu beheben, überprüfen Sie den Dateizugriffsstatus und die Berechtigungen für die in der Fehlermeldung genannte Datei und beheben Sie das Zugriffsproblem.

Zugriffsberichte

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 sind. Wenn keine Jobs ausgewählt sind, ist die Registerkarte „Berichte“ leer.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV die Registerkarte **Dashboard** > **Berichte** aus.
3. Für Sicherungsberichte können Sie Folgendes tun:
   a. Ändern des Berichts

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

   b. Erstellen Sie einen detaillierten Bericht

      Doppelklicken Sie auf einen beliebigen Job, um einen ausführlichen Bericht für diesen Job zu erstellen.
4. Optional: Wählen Sie auf der Registerkarte „Berichte“ die Option „Herunterladen“ und wählen Sie das Format (HTML oder CSV).

   Sie können auch 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 Datenschutzaufträgen und dem Status der Plug-In-Ressourcen liefern. Sie können nur Berichte zum primären Schutz erstellen.

> Sicherungspläne werden in der Zeitzone ausgeführt, in der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. vCenter meldet Daten in der Zeitzone, in der sich das vCenter befindet. Wenn sich das SnapCenter Plug-in for VMware vSphere und das vCenter in unterschiedlichen Zeitzonen befinden, stimmen die Daten im Dashboard des VMware vSphere-Clients möglicherweise nicht mit den Daten in den Berichten überein.

Das Dashboard zeigt Informationen zu migrierten Sicherungen erst an, nachdem Sicherungen nach der Migration durchgeführt wurden.

Berichtstyp	Beschreibung
Sicherungsbericht	Zeigt Übersichtsdaten zu Sicherungsaufträgen an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um auf der Registerkarte **Berichte** eine Liste der Jobs mit diesem Status anzuzeigen. Für jeden Job listet der Bericht die Job-ID, die entsprechende Ressourcengruppe, die Sicherungsrichtlinie, Startzeit und Dauer, den Status und die Jobdetails auf, einschließlich des Jobnamens (Snapshot-Namens), wenn der Job abgeschlossen ist, sowie etwaige Warn- oder Fehlermeldungen. Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Jobprotokolle für alle Jobs herunterladen (nicht nur für 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 auf der Registerkarte „Berichte“ eine Liste der Jobs mit diesem Status anzuzeigen. Für jeden Auftrag listet der Bericht die Auftrags-ID, den Auftragsstatus, den Auftragsnamen sowie die Start- und Endzeiten des Auftrags auf. 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-Jobprotokolle für alle Jobs herunterladen (nicht nur für die Jobs im Bericht).
Wiederherstellungsbericht	Zeigt eine Übersicht über Statusinformationen zu Wiederherstellungsaufträgen an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um auf der Registerkarte „Berichte“ eine Liste der Jobs mit diesem Status anzuzeigen. Für jeden Auftrag listet der Bericht die Auftrags-ID, den Auftragsstatus, den Auftragsnamen sowie die Start- und Endzeiten des Auftrags auf. 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-Jobprotokolle für alle Jobs herunterladen (nicht nur für die Jobs im Bericht).

Berichtstyp	Beschreibung
Bericht zum letzten Schutzstatus von VMs oder Datenspeichern	Zeigt Übersichtsinformationen zum Schutzstatus für die konfigurierte Anzahl von Tagen für VMs und Datenspeicher an, die vom SnapCenter Plug-in for VMware vSphere verwaltet werden. Der Standardwert beträgt 7 Tage. Informationen zum Ändern des Werts in der Eigenschaftendatei finden Sie unter"Ändern der Konfigurationsstandardwerte" . Wählen Sie einen Abschnitt/Status im primären Schutzdiagramm aus, um auf der Registerkarte **Berichte** eine Liste der VMs oder Datenspeicher mit diesem Status anzuzeigen. Der VM- oder Datastore-Schutzstatusbericht für geschützte VMs und Datastores zeigt die Namen der VMs oder Datastores an, die während der konfigurierten Anzahl von Tagen gesichert wurden, den Namen des letzten Snapshots sowie die Start- und Endzeiten für den letzten Sicherungslauf. Der VM- oder Datenspeicher-Schutzstatusbericht für ungeschützte VMs oder Datenspeicher zeigt die Namen der VMs oder Datenspeicher an, für die während der konfigurierten Anzahl von Tagen keine erfolgreichen Sicherungen durchgeführt wurden. Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Jobprotokolle für alle Jobs herunterladen (nicht nur für die Jobs im Bericht). Dieser Bericht wird stündlich aktualisiert, wenn der Plug-In-Cache aktualisiert wird. Daher werden im Bericht möglicherweise keine VMs oder Datenspeicher angezeigt, die kürzlich gesichert wurden.

Generieren Sie ein Support-Paket aus dem SnapCenter Plug-in for VMware vSphere GUI

Bevor Sie beginnen

Um sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI anzumelden, müssen Sie die IP-Adresse und die Anmeldeinformationen kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

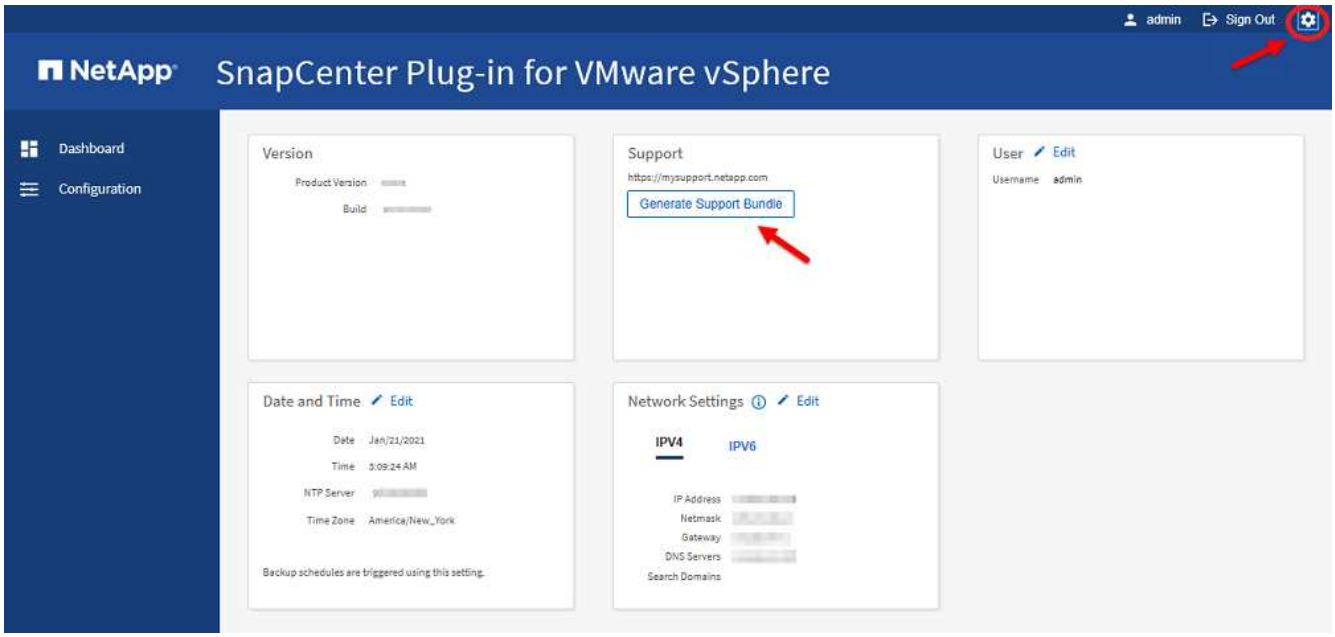
- Die IP-Adresse wurde angezeigt, als das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde.
- Verwenden Sie die Anmeldeinformationen, die Sie während der Bereitstellung des SnapCenter Plug-in for VMware vSphere erhalten haben oder die später geändert wurden.
- Generieren Sie mithilfe der Systemkonfigurationsoptionen der Wartungskonsole ein 6-stelliges MFA-Token.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere GUI an.

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

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



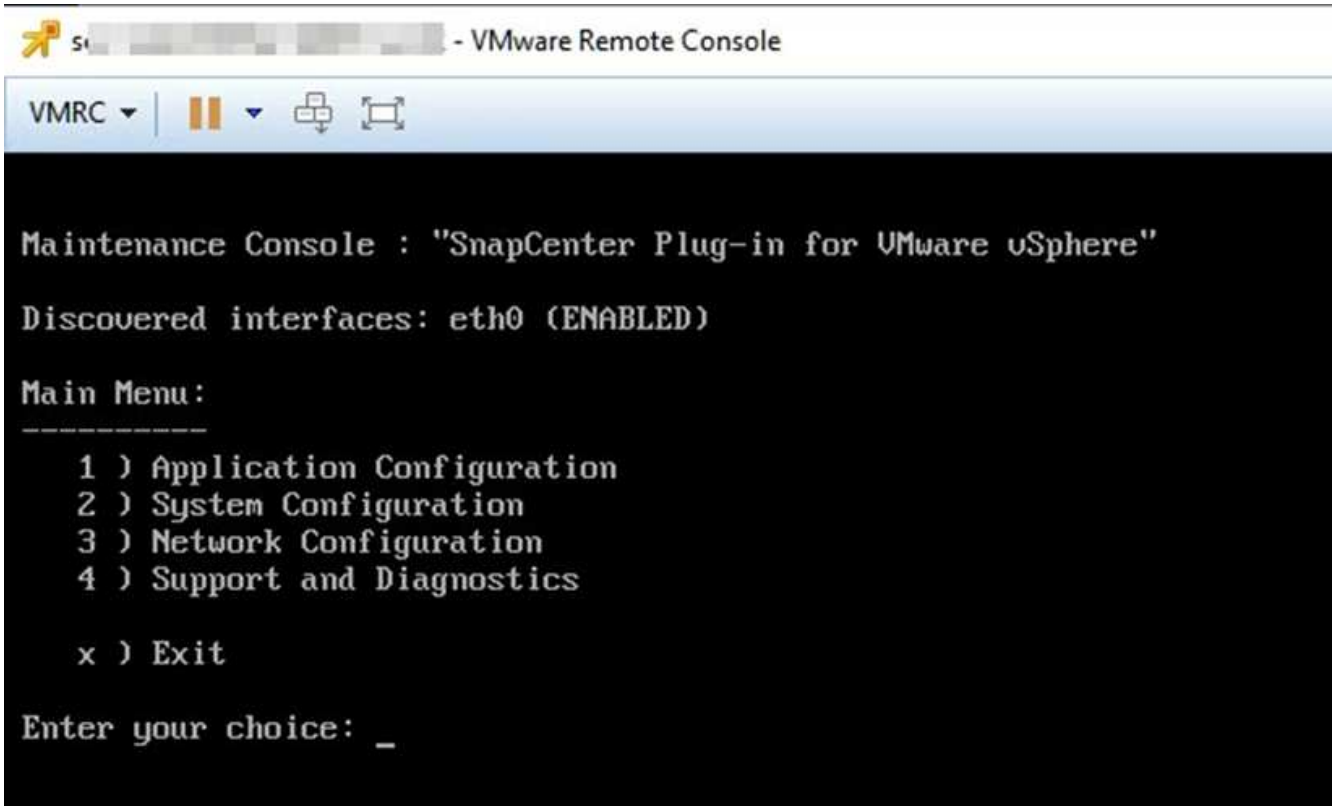
3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Support** die Option **Support-Paket generieren** aus.
4. Nachdem das Support-Paket generiert wurde, wählen Sie den bereitgestellten Link aus, um das Paket auf NetApp herunterzuladen.

Generieren Sie ein Support-Paket aus der Wartungskonsole

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter Plug-in for VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remotekonsole starten oder Webkonsole starten** aus, um ein Wartungskonsolenfenster zu öffnen, und melden Sie sich dann an.

   Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter"Zugriff auf 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) Support-Paket generieren** ein.

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

Überwachungsprotokolle

Ein Prüfprotokoll ist eine Sammlung von Ereignissen in chronologischer Reihenfolge, die in eine Datei innerhalb des Geräts geschrieben wird. Die Audit-Logdateien werden generiert unter `/var/log/netapp/audit` Speicherort und die Dateinamen folgen einer der folgenden Namenskonventionen:

- audit.log: Aktive Audit-Protokolldatei, die verwendet wird.
- audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz: Audit-Protokolldatei übertragen. Datum und Uhrzeit im Dateinamen geben an, wann die Datei erstellt wurde, zum Beispiel: audit-2022-12-15-16-28-01.log.gz.

In der Benutzeroberfläche des SCV-Plug-ins können Sie die Details des Prüfprotokolls unter **Dashboard** > **Einstellungen** > Registerkarte **Prüfprotokolle** anzeigen und exportieren. Sie können die Betriebsprüfung in den Prüfprotokollen anzeigen. Die Prüfprotokolle werden mit dem Support-Paket heruntergeladen.

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

Die Standardkonfigurationen der Auditdateien sind:

- Die verwendete Audit-Protokolldatei kann auf maximal 10 MB anwachsen
- Es werden maximal 10 Audit-Logdateien aufbewahrt

Übertragene Prüfprotokolle werden regelmäßig auf Integrität überprüft. SCV bietet REST-APIs zum Anzeigen von Protokollen und Überprüfen ihrer Integrität. Ein integrierter Zeitplan löst einen der folgenden Integritätsstatus aus und weist ihn zu.

Status	Beschreibung
MANIPULIERT	Der Inhalt der Überwachungsprotokolldatei wurde geändert
NORMAL	Die Audit-Protokolldatei ist unverändert
ROLLOVER-LÖSCHEN	- Die Prüfprotokolldatei wird basierend auf der Aufbewahrung gelöscht. - Standardmäßig werden nur 10 Dateien aufbewahrt
UNERWARTETES LÖSCHEN	Die Audit-Protokolldatei wird gelöscht
AKTIV	- Audit-Protokolldatei wird verwendet - Gilt nur für audit.log

Ereignisse werden in drei Hauptkategorien eingeteilt:

- Datenschutzereignisse
- Ereignisse der Wartungskonsole
- Ereignisse in der Admin-Konsole

Datenschutzereignisse

Die Ressourcen in SCV sind:

- Speichersystem
- Ressourcengruppe
- Politik
- Sicherung
- Abonnement
- Konto

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

Ressourcen	**Operationen**
Speichersystem	Erstellt, geändert, gelöscht
Abonnement	Erstellt, geändert, gelöscht
Konto	Erstellt, geändert, gelöscht
Ressourcengruppe	Erstellt, geändert, gelöscht, ausgesetzt, fortgesetzt
Politik	Erstellt, geändert, gelöscht

Sicherung	Erstellt, umbenannt, gelöscht, gemountet, unmountet, VMDK wiederhergestellt, VM wiederhergestellt, VMDK anhängen, VMDK trennen, Gastdatei wiederherstellen

Ereignisse der Wartungskonsole

Die Verwaltungsvorgänge in der Wartungskonsole werden geprüft. Verfügbare Optionen für die Wartungskonsole sind:

1. Dienste starten/stoppen
2. Benutzernamen und Passwort ändern
3. MySQL-Passwort ändern
4. Konfigurieren der MySQL-Sicherung
5. MySQL-Backup wiederherstellen
6. Ändern Sie das Benutzerkennwort „maint“.
7. Zeitzone ändern
8. NTP-Server ändern
9. SSH-Zugriff deaktivieren
10. Erhöhen Sie die Größe der Jail-Festplatte
11. Upgrade
12. Installieren Sie VMware Tools (wir arbeiten daran, diese durch Open-VM-Tools zu ersetzen)
13. IP-Adresseinstellungen ändern
14. Sucheinstellungen für Domänennamen ändern
15. Statische Routen ändern
16. Zugriff auf die Diagnose-Shell
17. Aktivieren Sie den Ferndiagnosezugriff

Ereignisse in der Admin-Konsole

Die folgenden Vorgänge in der Benutzeroberfläche der Admin-Konsole werden überwacht:

- Einstellungen
  - Administratoranmeldeinformationen ändern
  - Zeitzone ändern
  - NTP-Server ändern
  - IPv4/IPv6-Adresseinstellungen ändern
- Konfiguration
  - Ändern der vCenter-Anmeldeinformationen
  - Plug-in aktivieren/deaktivieren

Konfigurieren von Syslog-Servern

Prüfprotokolle werden innerhalb der Appliance gespeichert und regelmäßig auf Integrität überprüft. Durch die 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.

Informationen zu diesem Vorgang

Diese Aufgabe hilft Ihnen bei der Konfiguration des Syslog-Servers.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen** > **Überwachungsprotokolle** > **Einstellungen**.
3. Wählen Sie im Bereich **Audit-Protokolleinstellungen** die Option **Audit-Protokolle an Syslog-Server senden**
4. Geben Sie die folgenden Details ein:
   - Syslog-Server-IP
   - Syslog-Server-Port
   - RFC-Format
   - Syslog-Server-Zertifikat
5. Wählen Sie **SPEICHERN**, um die Syslog-Servereinstellungen zu speichern.

Ändern der Überwachungsprotokolleinstellungen

Sie können die Standardkonfigurationen der Protokolleinstellungen ändern.

Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

Informationen zu diesem Vorgang

Diese Aufgabe hilft Ihnen, die Standardeinstellungen des Überwachungsprotokolls zu ändern.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen** > **Überwachungsprotokolle** > **Einstellungen**.
3. Geben Sie im Bereich **Audit-Protokolleinstellungen** die maximale Anzahl von Audit-Protokolldateien und die Größenbeschränkung für Audit-Protokolldateien ein.
4. Wählen Sie die Option **Auditprotokolle an Syslog-Server senden**, wenn Sie die Protokolle an den Syslog-Server senden möchten. Geben Sie die Details des Servers ein.
5. Speichern Sie die Einstellungen.

Speicher verwalten

Speicher hinzufügen

Bevor Sie VMs sichern oder wiederherstellen können, müssen Sie Speichercluster oder Speicher-VMs hinzufügen. Durch das Hinzufügen von Speicher kann das SnapCenter Plug-in for VMware vSphere Sicherungs- und Wiederherstellungsvorgänge in vCenter erkennen und verwalten.

- Welche GUI soll verwendet werden?

  Verwenden Sie den VMware vSphere-Client, um Speicher hinzuzufügen.

- Große LUNs

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

- Virtuelle VMware-Volumes (vVols)

  Sie müssen Speichercluster zum SnapCenter Plug-in for VMware vSphere und ONTAP tools for VMware vSphere hinzufügen, damit vVol DataProtection funktioniert.

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Das SnapCenter Plug-in for VMware vSphere führt Sicherungs- und Wiederherstellungsvorgänge auf direkt verbundenen Speicher-VMs und auf Speicher-VMs in einem Speichercluster durch.

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

- Für vCenter im verknüpften Modus müssen Sie jedem vCenter separat Speichersysteme hinzufügen.
- Wenn Sie SVM hinzufügen, müssen die Namen der Speicher-VMs in Verwaltungs-LIFs aufgelöst werden.

  Wenn Sie in SnapCenter Einträge zur Datei *etc\hosts* für Speicher-VM-Namen hinzugefügt haben, müssen Sie sicherstellen, dass diese auch von der virtuellen Appliance auflösbar sind. Wenn dies nicht der Fall ist, sollten Sie ähnliche Einträge zur Datei *etc/hosts* innerhalb der Appliance hinzufügen.

  Wenn Sie eine Speicher-VM mit einem Namen hinzufügen, der nicht in das Verwaltungs-LIF aufgelöst werden kann, schlagen geplante Sicherungsaufträge fehl, da das Plug-In keine Datenspeicher oder Volumes auf dieser Speicher-VM erkennen kann. Wenn dies eintritt, fügen Sie entweder die Speicher-VM

zu SnapCenter hinzu und geben Sie das Verwaltungs-LIF an oder fügen Sie einen Cluster hinzu, der die Speicher-VM enthält, und geben Sie das Cluster-Verwaltungs-LIF an.

- Speicherauthentifizierungsdetails werden nicht zwischen mehreren Instanzen des SnapCenter Plug-in for VMware vSphere oder zwischen Windows SnapCenter Server und dem SnapCenter -Plug-In auf vCenter geteilt.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV **Dashboard** > **Speichersysteme**.
3. Wählen Sie auf der Seite „Speichersysteme“ die Option **Hinzufügen**.
4. Geben Sie im Assistenten **Speichersystem hinzufügen** die grundlegenden Speicher-VM- oder Clusterinformationen ein, wie in der folgenden Tabelle aufgeführt:

Für dieses Feld…	Mach das…
Speichersystem	Geben Sie den FQDN oder die IP-Adresse des Management-LIF eines Speicherclusters oder einer Speicher-VM ein. Das SnapCenter Plug-in for VMware vSphere unterstützt nicht mehrere Speicher-VMs mit demselben Namen auf verschiedenen Clustern.
Authentifizierungsmethode	Wählen Sie entweder Anmeldeinformationen oder Zertifikat aus. Es werden zwei Arten von Zertifikaten unterstützt: - "Selbstsigniertes Zertifikat" - "CA-signiertes Zertifikat" .
Benutzername	Dieses Feld ist sichtbar, wenn Sie „Anmeldeinformationen“ als Authentifizierungsmethode auswählen. Geben Sie den ONTAP -Benutzernamen ein, der für die Anmeldung bei der Speicher-VM oder dem Cluster verwendet wird.
Passwort	Dieses Feld ist sichtbar, wenn Sie „Anmeldeinformationen“ als Authentifizierungsmethode auswählen. Geben Sie das Anmeldekennwort für die Speicher-VM oder den Cluster ein.
Zertifikat	Dieses Feld ist sichtbar, wenn Sie „Zertifikat“ als Authentifizierungsmethode auswählen. Durchsuchen Sie die Datei, um die Zertifikatsdatei auszuwählen.
Privater Schlüssel	Dieses Feld ist sichtbar, wenn Sie „Zertifikat“ als Authentifizierungsmethode auswählen. Durchsuchen Sie die Datei, um sie mit dem privaten Schlüssel auszuwählen.
Protokoll	Wählen Sie das Speicherprotokoll aus.
Hafen	Port, den das Speichersystem akzeptiert. - 443 für HTTPS-Verbindung - 80 für HTTP-Verbindung

Für dieses Feld…	Mach das…
Time-out	Geben Sie die Anzahl der Sekunden ein , die das SnapCenter Plug-in for VMware vSphere warten soll, bevor der Vorgang abgebrochen wird. Der Standardwert beträgt 60 Sekunden.
Bevorzugte IP-Adresse	Wenn die Speicher-VM über mehr als eine Verwaltungs-IP-Adresse verfügt, aktivieren Sie dieses Kontrollkästchen und geben Sie die IP-Adresse ein, die das SnapCenter Plug-in for VMware vSphere verwenden soll. **Hinweis:** Verwenden Sie bei der Eingabe der IP-Adresse keine eckigen Klammern ([]).
Event Management System (EMS) und AutoSupport -Einstellungen	Wenn Sie EMS-Nachrichten an das Syslog des Speichersystems senden möchten oder wenn Sie möchten, dass AutoSupport Nachrichten zum angewendeten Schutz, zu abgeschlossenen Wiederherstellungsvorgängen oder zu fehlgeschlagenen Vorgängen an das Speichersystem gesendet werden, aktivieren Sie das entsprechende Kontrollkästchen. Aktivieren Sie das Kontrollkästchen * AutoSupport -Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden* und das Kontrollkästchen * SnapCenter -Server-Ereignisse in Syslog protokollieren*, um AutoSupport Benachrichtigungen zu aktivieren.
SnapCenter Server-Ereignisse im Syslog protokollieren	Aktivieren Sie das Kontrollkästchen, um Ereignisse für das SnapCenter Plug-in for VMware vSphere zu protokollieren.
Senden Sie eine AutoSupport -Benachrichtigung für einen fehlgeschlagenen Vorgang an das Speichersystem	Aktivieren Sie das Kontrollkästchen, wenn Sie eine AutoSupport Benachrichtigung für fehlgeschlagene Datenschutzaufträge erhalten möchten. Sie müssen AutoSupport auch auf der Speicher-VM aktivieren und die E-Mail-Einstellungen von AutoSupport konfigurieren.

5. Wählen Sie **Hinzufügen**.

   Wenn Sie einen Speichercluster hinzugefügt haben, werden alle Speicher-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.

Speichersysteme verwalten

Bevor Sie VMs oder Datenspeicher mit dem VMware vSphere-Client sichern oder wiederherstellen können, müssen Sie den Speicher hinzufügen.

Ändern von Speicher-VMs

Sie können den VMware vSphere-Client verwenden, um die Konfigurationen von Clustern und Speicher-VMs zu ändern, die im SnapCenter Plug-in for VMware vSphere registriert sind und für VM-Datenschutzvorgänge verwendet werden.

Wenn Sie eine Speicher-VM ändern, die automatisch als Teil eines Clusters hinzugefügt wurde (manchmal auch als implizite Speicher-VM bezeichnet), wird diese Speicher-VM zu einer expliziten Speicher-VM und kann separat gelöscht werden, ohne dass die restlichen Speicher-VMs in diesem Cluster geändert werden. Auf der Seite „Speichersysteme“ wird der Benutzername als N/A angezeigt, wenn die Authentifizierungsmethode über das Zertifikat erfolgt. Benutzernamen werden nur für explizite Speicher-VMs in der Clusterliste angezeigt und haben das Flag „ExplicitSVM“ auf „true“ gesetzt. Alle Storage-VMs werden immer unter dem zugehörigen Cluster aufgelistet.

> Wenn Sie Speicher-VMs für anwendungsbasierte Datenschutzvorgänge mithilfe der SnapCenter -GUI hinzugefügt haben, müssen Sie dieselbe GUI verwenden, um diese Speicher-VMs zu ändern.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Speichersysteme** 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 **Aktualisieren**, um die Änderungen anzuwenden.

Entfernen von Speicher-VMs

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

> Wenn Sie Speicher-VMs für anwendungsbasierte Datenschutzvorgänge mithilfe der SnapCenter -GUI hinzugefügt haben, müssen Sie dieselbe GUI verwenden, um diese Speicher-VMs zu ändern.

Bevor Sie beginnen

Sie müssen alle Datenspeicher in der Speicher-VM aushängen, bevor Sie die Speicher-VM entfernen können.

Informationen zu diesem Vorgang

Wenn eine Ressourcengruppe über Sicherungen verfügt, die sich auf einer Speicher-VM befinden, die Sie entfernen, schlagen nachfolgende Sicherungen für diese Ressourcengruppe fehl.

Schritte

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

   "Starten Sie den VMware vSphere-Clientdienst neu" .

Ändern Sie das konfigurierte Speicher-Timeout

Auch wenn Sicherungen in der Vergangenheit erfolgreich ausgeführt wurden, können sie während der Zeit, in der das SnapCenter Plug-in for VMware vSphere warten muss, bis das Speichersystem den konfigurierten Timeout-Zeitraum überschreitet, fehlschlagen. Wenn dieser Zustand eintritt, können Sie das konfigurierte Timeout erhöhen.

Möglicherweise tritt der Fehler `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 **Speichersysteme** 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 werden 180 Sekunden empfohlen.

Daten schützen

Datenschutz-Workflow

Verwenden Sie den SnapCenter vSphere-Client, um Datenschutzvorgänge für VMs, VMDKs und Datenspeicher durchzuführen. Alle Sicherungsvorgänge werden auf Ressourcengruppen ausgeführt, die eine beliebige Kombination aus einer oder mehreren VMs und Datenspeichern enthalten können. Sie können Backups nach Bedarf oder gemäß einem festgelegten Schutzzeitplan durchführen.

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

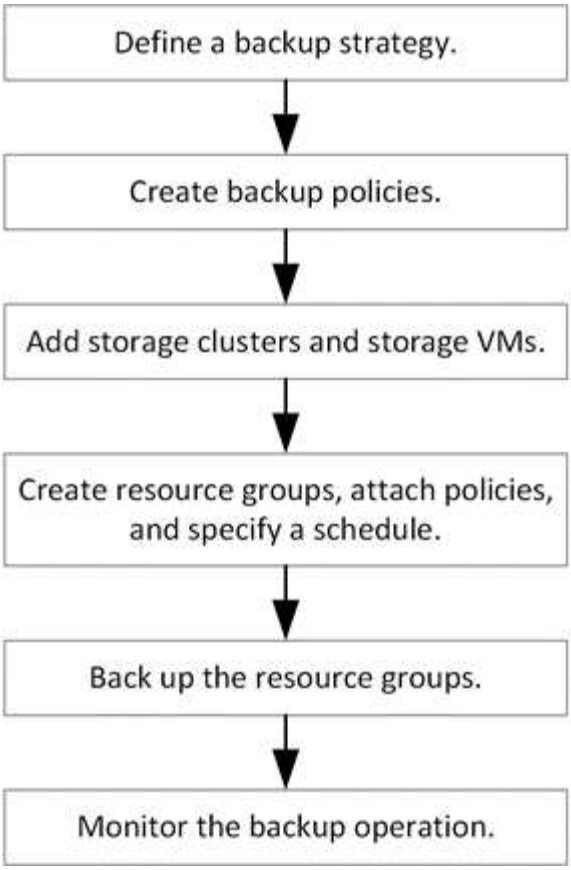
Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig für dieselbe Ressourcengruppe ausgeführt werden.

Sie sollten die Informationen darüber lesen, was das SnapCenter Plug-in for VMware vSphere unterstützt und was nicht."Bereitstellungsplanung und -anforderungen"

In MetroCluster -Konfigurationen:

- Das SnapCenter Plug-in for VMware vSphere kann nach einem Failover möglicherweise keine Schutzbeziehung erkennen. Siehe "KB-Artikel: SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden" für weitere Informationen.
- Wenn die Sicherung mit dem Fehler fehlschlägt `Unable to discover resources on SCV: <xxx>…` Starten Sie für NFS- und VMFS-VMs nach dem Umschalten/Zurückschalten die SnapCenter VMware-Dienste von der Wartungskonsole aus neu.

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



Anzeigen von VM- und Datenspeichersicherungen

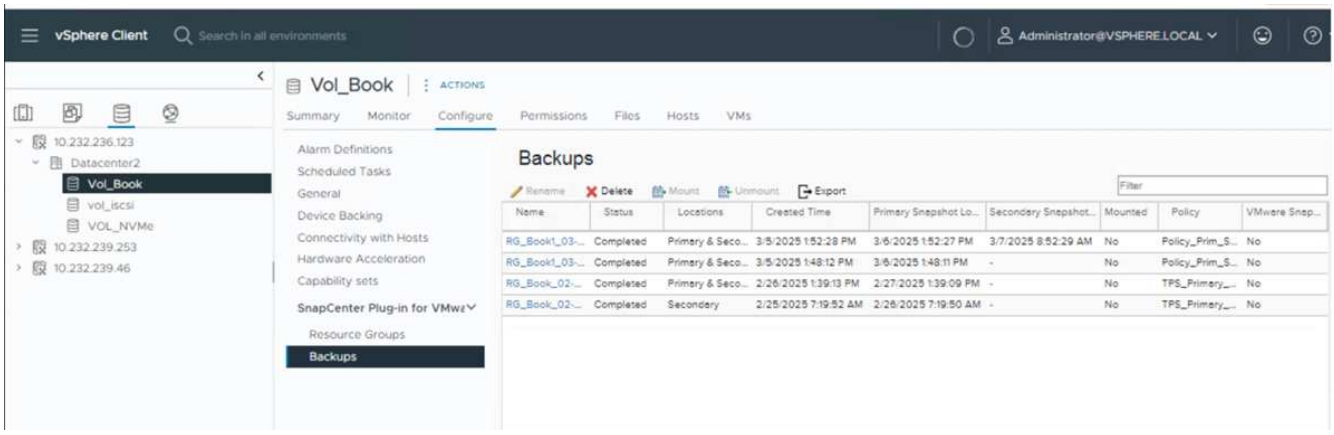
Wenn Sie die Sicherung oder Wiederherstellung einer VM oder eines Datenspeichers vorbereiten, möchten Sie möglicherweise alle für diese Ressource verfügbaren Sicherungen anzeigen und die Details dieser Sicherungen ansehen.

Informationen zu diesem Vorgang

Das Durchsuchen großer Dateiordner, beispielsweise 10.000-Dateiordner, kann beim ersten Mal eine oder mehrere Minuten dauern. Nachfolgende Browsersitzungen dauern weniger lang.

Schritte

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



Wenn die Option **Sekundäre Snapshot-Sperre aktivieren** während der Richtlinienerstellungsphase nicht ausgewählt wird, wird standardmäßig der für die Option **Primäre Snapshot-Sperre aktivieren** festgelegte Wert verwendet. In der Sicherungsliste zeigt der Bindestrich im Feld **Ablauf der sekundären Snapshot-Sperre** an, dass die Sperrzeiträume für die primäre und sekundäre Sperre identisch sind.

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

Erstellen Sie Sicherungsrichtlinien für VMs und Datenspeicher

Sie müssen Sicherungsrichtlinien erstellen, bevor Sie das SnapCenter Plug-in for VMware vSphere zum Sichern von VMs und Datenspeichern verwenden.

Bevor Sie beginnen

- Sie müssen die Voraussetzungen gelesen haben.
- Sie müssen sekundäre Speicherbeziehungen konfiguriert haben.
  - Wenn Sie Snapshots auf einen Spiegel- oder Tresor-Sekundärspeicher replizieren, müssen die Beziehungen konfiguriert werden und der SnapCenter Administrator muss Ihnen die Speicher-VMs sowohl für das Quell- als auch für das Zielvolume zugewiesen haben.
  - Um Snapshots für Version-FlexibleMirror-Beziehungen auf einem NFS- oder VMFS-Datenspeicher erfolgreich auf den sekundären Speicher zu übertragen, stellen Sie sicher, dass der SnapMirror Richtlinientyp „Asynchronous Mirror“ ist und dass die Option „all_source_snapshots“ aktiviert ist.
  - Wenn die Anzahl der Snapshots auf dem sekundären Speicher (Mirror-Vault) die maximale Grenze erreicht, schlägt die Aktivität zum Registrieren der Sicherung und Anwenden der Aufbewahrung im Sicherungsvorgang mit dem folgenden Fehler 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 den sekundären Speicher, um zu vermeiden, dass die maximale Anzahl an Snapshots erreicht wird.

  Informationen dazu, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie unter "SnapCenter Informationen zur Verwendung der rollenbasierten Zugriffskontrolle" .

- Wenn Sie VM-konsistente Backups wünschen, müssen Sie VMware-Tools installiert und ausgeführt haben. Zum Stilllegen von VMs werden VMware-Tools benötigt. VM-konsistente Sicherungen werden für vVol-VMs nicht unterstützt.

- SnapMirror Active Sync ermöglicht die Weiterführung des Betriebs von Geschäftsdiensten auch bei einem vollständigen Site-Ausfall und unterstützt Anwendungen bei einem transparenten Failover mithilfe einer sekundären Kopie.

  > SnapMirror Active Sync wird nur für VMFS-Datenspeicher unterstützt.

  Um einen VMFS-Datenspeicher auf einer SnapMirror Active Sync-Bereitstellung zu schützen, 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 mit dem VMFS-Datenspeicher verknüpfte Volume der Konsistenzgruppe hinzu und erstellen Sie mithilfe der Schutzrichtlinie *AutomatedFailOver* oder *AutomatedFailOverDuplex* eine Datenschutzbeziehung zwischen zwei ONTAP Speichersystemen. Die Richtlinie *AutomatedFailOverDuplex* wird ab der ONTAP Version 9.15.1 unterstützt.

> In der Fan-Out-Konfiguration wird die Konsistenzgruppe für den tertiären Standort nicht unterstützt.

Informationen zu diesem Vorgang

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. Die folgenden Informationen beschreiben einige der Felder, für die Sie möglicherweise Anleitungen benötigen.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Richtlinien** aus.
2. Wählen Sie auf der Seite **Richtlinien** die Option **Erstellen** aus, um den Assistenten zu starten.
3. Geben Sie auf der Seite **Neue Sicherungsrichtlinie** den Richtliniennamen und eine Beschreibung ein.

   - Verknüpfter Modus

     Im verknüpften Modus verfügt jedes vCenter über eine separate virtuelle Appliance. Daher können Sie in allen vCentern doppelte Namen verwenden. Sie müssen die Richtlinie jedoch im selben vCenter wie die Ressourcengruppe erstellen.

   - Nicht unterstützte Zeichen

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

   Ein Unterstrich (_) ist zulässig.

4. Geben Sie die Frequenzeinstellungen an.

   Die Richtlinie gibt nur die Sicherungshäufigkeit an. Der spezifische Schutzzeitplan für die Sicherung wird in der Ressourcengruppe definiert. Daher können zwei oder mehr Ressourcengruppen dieselbe Richtlinie und Sicherungshäufigkeit verwenden, jedoch unterschiedliche Sicherungspläne haben.

5. Aktivieren Sie das Kontrollkästchen **Sperrzeitraum**, um die Snapshot-Sperre zu aktivieren. Sie können die Sperrzeiträume für den primären und sekundären Snapshot in Tagen/Monaten/Jahren auswählen.

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

6. Geben Sie die Aufbewahrungseinstellungen an.

Sie sollten die Aufbewahrungsanzahl auf 2 Backups oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Anzahl der aufzubewahrenden Sicherungen auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen. Dies 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. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden ONTAP Version unterstützt wird. Dies gilt auch für übergreifende Datenspeicher.

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

Für dieses Feld…	Mach das…
SnapMirror nach der Sicherung aktualisieren	Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, das über eine SnapMirror -Beziehung zum primären Sicherungsvolume verfügt. Wenn ein Volume mit einer Mirror-Vault-Beziehung konfiguriert ist, müssen Sie nur die Option * SnapVault nach Sicherung aktualisieren* auswählen, wenn Sie möchten, dass Sicherungen an die Mirror-Vault-Ziele kopiert werden. Diese Option wird für Datenspeicher in FlexGroup -Volumes im SnapCenter Plug-in for VMware vSphere 4.5 und höher unterstützt. Um den VMFS-Datenspeicher bei der Bereitstellung von SnapMirror Active Sync zu schützen, müssen Sie die im Abschnitt „Bevor Sie beginnen“ genannten Voraussetzungen erfüllen und „ SnapMirror nach der Sicherung aktualisieren“ aktivieren.

Für dieses Feld…	Mach das…
SnapVault nach der Sicherung aktualisieren	Wählen Sie diese Option, um eine Disk-to-Disk-Sicherungsreplikation auf einem anderen Volume durchzuführen, das über eine SnapVault -Beziehung zum primären Sicherungsvolume verfügt. Wenn ein Volume mit einer Mirror-Vault-Beziehung konfiguriert ist, müssen Sie diese Option nur auswählen, wenn Sie möchten, dass Sicherungen an die Mirror-Vault-Ziele kopiert werden. Diese Option wird für Datenspeicher in FlexGroup -Volumes im SnapCenter Plug-in for VMware vSphere 4.5 und höher unterstützt.
Snapshot-Bezeichnung	Geben Sie eine optionale, benutzerdefinierte Bezeichnung ein, die den mit dieser Richtlinie erstellten SnapVault und SnapMirror -Snapshots hinzugefügt werden soll. Die Snapshot-Bezeichnung hilft dabei, mit dieser Richtlinie erstellte Snapshots von anderen Snapshots auf dem sekundären Speichersystem zu unterscheiden. Für Snapshot-Beschriftungen sind maximal 31 Zeichen zulässig.

8. Optional: Wählen Sie in den **Erweiterten** Feldern die benötigten Felder aus. Die erweiterten Felddetails sind in der folgenden Tabelle aufgeführt.

Für dieses Feld…	Mach das…
VM-Konsistenz	Aktivieren Sie dieses Kontrollkästchen, um die VMs stillzulegen und bei jeder Ausführung des Sicherungsjobs einen VMware-Snapshot zu erstellen. Diese Option wird für vVols nicht unterstützt. Für vVol-VMs werden nur absturzkonsistente Sicherungen durchgeführt. Um VM-konsistente Sicherungen durchführen zu können, müssen auf der VM VMware-Tools ausgeführt werden. Wenn VMware Tools nicht ausgeführt wird, wird stattdessen eine absturzkonsistente Sicherung durchgeführt. Wenn Sie das Kontrollkästchen „VM-Konsistenz“ aktivieren, können Sicherungsvorgänge länger dauern und mehr Speicherplatz erfordern. In diesem Szenario werden die VMs zunächst stillgelegt, dann führt VMware einen VM-konsistenten Snapshot durch, anschließend führt SnapCenter seinen Sicherungsvorgang durch und anschließend werden die VM-Vorgänge wieder aufgenommen. Der VM-Gastspeicher ist nicht in den VM-Konsistenz-Snapshots enthalten.
Datenspeicher mit unabhängigen Datenträgern einbeziehen	Aktivieren Sie dieses Kontrollkästchen, um alle Datenspeicher mit unabhängigen Festplatten, die temporäre Daten enthalten, in die Sicherung einzubeziehen.

Für dieses Feld…	Mach das…
Skripte	Geben Sie den vollqualifizierten Pfad des Präskripts oder Postskripts ein, das das SnapCenter Plug-in for VMware vSphere vor oder nach Sicherungsvorgängen ausführen soll. Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren und Protokolle zu senden. Der Skriptpfad wird zum Zeitpunkt der Skriptausführung validiert. Prescripts und Postscripts müssen sich auf der virtuellen Appliance-VM befinden. Um mehrere Skripte einzugeben, drücken Sie nach jedem Skriptpfad die Eingabetaste, um jedes Skript in einer separaten Zeile aufzulisten. Das Zeichen „;“ ist nicht zulässig.

9. Wählen Sie **Hinzufügen**.

   Sie können überprüfen, ob die Richtlinie erstellt wurde, und die Richtlinienkonfiguration prüfen, indem Sie die Richtlinie auf der Seite „Richtlinien“ auswählen.

Erstellen von Ressourcengruppen

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

Eine Ressourcengruppe kann Folgendes enthalten:

- Herkömmliche VMs und Datenspeicher

  Jede Kombination aus herkömmlichen VMs, herkömmlichen SAN-Datenspeichern und herkömmlichen NAS-Datenspeichern. Herkömmliche VMs können nicht mit vVol-VMs kombiniert werden.

- Flexgroup-Datenspeicher

  Ein einzelner FlexGroup Datenspeicher. Spanning Flexgroup-Datenspeicher werden nicht unterstützt. Ein FlexGroup -Datenspeicher kann nicht mit herkömmlichen VMs oder Datenspeichern kombiniert werden.

- FlexVol -Datenspeicher

  Ein oder mehrere FlexVol -Datenspeicher. Spanning-Datastores werden unterstützt.

- vVol-VMs

  Eine oder mehrere vVol-VMs. vVol-VMs können nicht mit herkömmlichen VMs oder Datenspeichern kombiniert werden.

- vSphere-Tag

  Alle VMs und Datastores, ausgenommen vVol-Datastores, die über das angegebene vSphere-Tag verfügen.

- vVol-VMs in einem Ordner

  Alle vVols in einem einzigen, angegebenen vVol-Ordner. Wenn der Ordner eine Mischung aus vVol-VMs und herkömmlichen VMs enthält, sichert das SnapCenter Plug-in for VMware vSphere die vVol-VMs und überspringt die herkömmlichen VMs.

- VMs und Datenspeicher auf ASA r2

  Sie können ASA R2-VMs und -Datenspeicher nicht mit anderen VMs und Datenspeichern kombinieren.

Für alle Ressourcengruppen:

> Wenn Sie VMware vSphere Cluster Service (vCLS) verwenden, schließen Sie keine von vCLS verwalteten VMs in das SnapCenter Plug-in for VMware vSphere Ressourcengruppen ein.

Weitere Informationen finden Sie unter "SCV kann vCLS-VMs nach der Aktualisierung von vCenter auf 7.0.x nicht sichern"

> Das SnapCenter Plug-in for VMware vSphere 4.5 und höher unterstützt Datenspeicher auf großen LUNs und Dateien bis zu 128 TB mit Volumes bis zu 300 TB. Wenn Sie große LUNs schützen, verwenden Sie nur Thick Provisioning-LUNs, um Latenz zu vermeiden.

> Fügen Sie keine VMs hinzu, die sich in einem unzugänglichen Zustand befinden. Obwohl es möglich ist, eine Ressourcengruppe zu erstellen, die nicht zugängliche VMs enthält, schlagen Sicherungen 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 . Weitere Informationen finden Sie unter "NetApp Interoperabilitätsmatrix-Tool" für aktuelle Informationen zu den unterstützten Versionen der ONTAP Tools.

Informationen zu diesem Vorgang

Sie können einer Ressourcengruppe jederzeit Ressourcen hinzufügen oder daraus entfernen.

- Sichern einer einzelnen Ressource

  Um eine einzelne Ressource (z. B. eine einzelne VM) zu sichern, müssen Sie eine Ressourcengruppe erstellen, die diese einzelne Ressource enthält.

- Sichern mehrerer Ressourcen

  Um mehrere Ressourcen zu sichern, müssen Sie eine Ressourcengruppe erstellen, die mehrere Ressourcen enthält.

- Ressourcengruppen, die FlexGroup Volumes in MetroCluster -Umgebungen enthalten

Wenn Sie ONTAP 9.8 oder ONTAP 9.9 verwenden, müssen Sie nach einem Switchover oder Switchback das SnapCenter Plug-in for VMware vSphere Dienst neu starten und die SnapMirror -Beziehungen neu synchronisieren, bevor Sie Ressourcengruppen in MetroCluster Umgebungen sichern.

Bei ONTAP 9.8 bleiben die Backups nach dem Switchback hängen. Dieses Problem wurde in ONTAP 9.9 behoben.

- Optimieren von Snapshots

  Um Snapshots zu optimieren, sollten Sie die VMs und Datenspeicher, die demselben Volume zugeordnet sind, in einer Ressourcengruppe zusammenfassen.

- Sicherungsrichtlinien

  Sie können zwar eine Ressourcengruppe ohne Sicherungsrichtlinie erstellen, Datenschutzvorgänge sind jedoch nur möglich, wenn der Ressourcengruppe mindestens eine Richtlinie zugeordnet ist. Sie haben die Möglichkeit, während des Erstellungsprozesses der Ressourcengruppe eine vorhandene Richtlinie zu verwenden oder eine neue zu erstellen.

  > Wenn Sie eine Sicherungsrichtlinie mit Snapshot-Sperrzeitraum auswählen, müssen Sie ONTAP 9.12.1 oder eine höhere Version auswählen.

- Kompatibilitätsprüfungen

  SnapCenter führt Kompatibilitätsprüfungen durch, wenn Sie eine Ressourcengruppe erstellen.

  Verwalten von Fehlern bei der Kompatibilitätsprüfung

- Erstellen eines sekundären Schutzes für eine Ressourcengruppe

  Der sekundäre Schutz kümmert sich um die Erstellung einer Replikationsbeziehung für die in der Ressourcengruppe hinzugefügten Ressourcen. Sie müssen eine auf einer Konsistenzgruppe basierende SnapMirror Beziehung im bevorzugten Cluster und SVM mithilfe einer angegebenen Richtlinie vom Primärserver erstellen. Der sekundäre Schutz wird nur für Datenspeicher und virtuelle Maschinen auf Basis des ASA R2-Systems unterstützt. Das Cluster-Peering und das SVM-Peering sollten vorkonfiguriert sein. Der sekundäre Schutz erlaubt nur asynchrone SnapMirror Richtlinien. Sie müssen beim Erstellen des sekundären Schutzes ein Konsistenzgruppensuffix angeben.

Der sekundäre Schutz kümmert sich um die Erstellung einer Replikationsbeziehung für die in der Ressourcengruppe hinzugefügten Ressourcen.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Ressourcengruppen** und dann **Erstellen** aus, um den Assistenten zu starten.

Dies ist die einfachste Möglichkeit, eine Ressourcengruppe zu erstellen. Sie können jedoch auch eine Ressourcengruppe mit einer Ressource erstellen, indem Sie einen der folgenden Schritte ausführen:

- Um eine Ressourcengruppe für eine VM zu erstellen, wählen Sie auf der Verknüpfungsseite **Hosts und Cluster** aus, klicken Sie dann mit der rechten Maustaste auf eine VM und wählen Sie * SnapCenter Plug-in for VMware vSphere* > **Ressourcengruppe erstellen**.
- Um eine Ressourcengruppe für einen Datenspeicher zu erstellen, wählen Sie auf der Verknüpfungsseite **Hosts und Cluster** aus, klicken Sie dann mit der rechten Maustaste auf einen Datenspeicher und wählen Sie * SnapCenter Plug-in for VMware vSphere* > **Ressourcengruppe erstellen**.

a. Führen Sie auf der Seite **Allgemeine Informationen und Benachrichtigungen** im Assistenten die folgenden Schritte aus:

Für dieses Feld…	Mach das…
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 verfügt jedes vCenter über ein separates SnapCenter Plug-in for VMware vSphere Repository. Daher können Sie in allen vCentern doppelte Namen verwenden.
Beschreibung	Geben Sie eine Beschreibung der Ressourcengruppe ein.
Benachrichtigung	Wählen Sie aus, wann Sie Benachrichtigungen über Vorgänge in dieser Ressourcengruppe erhalten möchten: Fehler oder Warnungen: Benachrichtigung nur bei Fehlern und Warnungen senden Fehler: Benachrichtigung nur bei Fehlern senden Immer: Benachrichtigung für alle Nachrichtentypen senden Nie: Keine Benachrichtigung senden
E-Mail gesendet von	Geben Sie die E-Mail-Adresse ein, von der die Benachrichtigung gesendet werden soll.
E-Mail senden an	Geben Sie die E-Mail-Adresse der Person ein, die die Benachrichtigung erhalten soll. Bei mehreren Empfängern trennen Sie die E-Mail-Adressen durch Kommas.
E-Mail-Betreff	Geben Sie den gewünschten Betreff für die Benachrichtigungs-E-Mails ein.

Für dieses Feld…	Mach das…
Name des neuesten Snapshots	Wenn Sie möchten, dass dem neuesten Snapshot das Suffix „_recent“ hinzugefügt wird, aktivieren Sie dieses Kontrollkästchen. Das Suffix „_recent“ ersetzt Datum und Zeitstempel. A `_recent` Für jede Richtlinie, die einer Ressourcengruppe zugeordnet ist, wird eine Sicherung erstellt. Daher hat eine Ressourcengruppe mit mehreren Richtlinien mehrere `_recent` Sicherungen. Nicht manuell umbenennen `_recent` Sicherungen. Das ASA R2-Speichersystem unterstützt das Umbenennen von Snapshots nicht und daher werden die SCV-Funktionen zum Umbenennen von Backups und zur Benennung aktueller Snapshots nicht unterstützt.

Für dieses Feld…	Mach das…
Benutzerdefiniertes Snapshot-Format	Wenn Sie ein benutzerdefiniertes Format für die Snapshot-Namen verwenden möchten, aktivieren Sie dieses Kontrollkästchen und geben Sie das Namensformat ein. • Standardmäßig ist diese Funktion deaktiviert. • Die Standard-Snapshot-Namen verwenden das Format `<ResourceGroup>_<Date-TimeStamp>` Sie können jedoch mithilfe der Variablen $ResourceGroup, $Policy, $HostName, $ScheduleType und $CustomText ein benutzerdefiniertes Format angeben. Verwenden Sie die Dropdown-Liste im Feld „Benutzerdefinierter Name“, um auszuwählen, welche Variablen Sie verwenden möchten und in welcher Reihenfolge sie verwendet werden sollen. Wenn Sie $CustomText auswählen, ist das Namensformat `<CustomName>_<Date-TimeStamp>` . Geben Sie den benutzerdefinierten Text in das bereitgestellte zusätzliche Feld ein. [HINWEIS]: Wenn Sie auch das Suffix „_recent“ auswählen, müssen Sie sicherstellen, dass die benutzerdefinierten Snapshot-Namen im Datenspeicher eindeutig sind. Daher sollten Sie dem Namen die Variablen $ResourceGroup und $Policy hinzufügen. • Sonderzeichen: Befolgen Sie für Sonderzeichen in Namen die gleichen Richtlinien wie für das Feld „Name“.

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

Für dieses Feld…	Mach das…
Umfang	Wählen Sie den Ressourcentyp aus, den Sie schützen möchten: * Datenspeicher (alle herkömmlichen VMs in einem oder mehreren angegebenen Datenspeichern). Sie können keinen vVol-Datenspeicher auswählen. * Virtuelle Maschinen (einzelne herkömmliche oder vVol-VMs; im Feld müssen Sie zu dem Datenspeicher navigieren, der die VMs oder vVol-VMs enthält). Sie können in einem FlexGroup -Datenspeicher keine einzelnen VMs auswählen. * Tags Tag-basierter Datenspeicherschutz wird nur für NFS- und VMFS-Datenspeicher sowie für virtuelle Maschinen und vVol-virtuelle Maschinen 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)
Rechenzentrum	Navigieren Sie zu den VMs, Datenspeichern oder Ordnern, die Sie hinzufügen möchten. VM- und Datenspeichernamen in einer Ressourcengruppe müssen eindeutig sein.
Verfügbare Entitäten	Wählen Sie die Ressourcen aus, die Sie schützen möchten, und wählen Sie dann **>**, um Ihre Auswahl in die Liste „Ausgewählte Entitäten“ zu verschieben.

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

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

Um einen oder mehrere Datenspeicher global von Backups auszuschließen, müssen Sie den/die Datenspeichernamen in der `global.ds.exclusion.pattern` Eigentum in der `scbr.override` Konfigurationsdatei. Weitere Informationen finden Sie unter "Eigenschaften, die Sie überschreiben können" .

a. Wählen Sie auf der Seite **Spanning Disks** eine Option für VMs mit mehreren VMDKs über mehrere Datenspeicher hinweg aus:
   - Immer alle übergreifenden Datenspeicher ausschließen (Dies ist die Standardeinstellung für Datenspeicher.)
   - Immer alle übergreifenden Datenspeicher einschließen (Dies ist die Standardeinstellung für VMs.)
   - Wählen Sie manuell die einzuschließenden Spanning Datastores aus

     Spanning-VMs werden für FlexGroup und vVol-Datenspeicher nicht unterstützt.

b. Wählen oder erstellen Sie auf der Seite **Richtlinien** eine oder mehrere Sicherungsrichtlinien, wie in der folgenden Tabelle gezeigt:

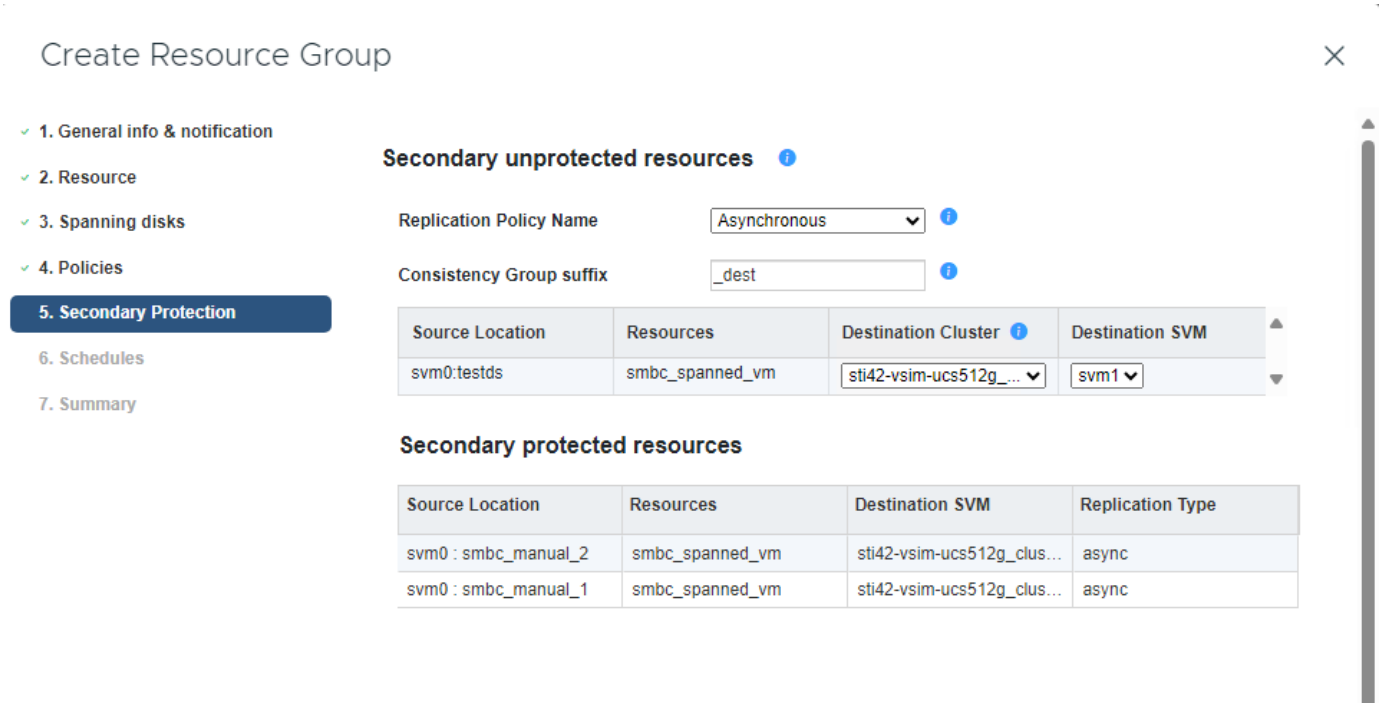
Zur Verwendung…	Mach das…
Eine bestehende Richtlinie	Wählen Sie eine oder mehrere Richtlinien aus der Liste aus. Der sekundäre Schutz gilt für bestehende und neue Richtlinien, bei denen Sie sowohl SnapMirror als auch SnapVault -Updates ausgewählt haben.
Eine neue Politik	i. Wählen Sie **Erstellen**. ii. Schließen Sie den Assistenten „Neue Sicherungsrichtlinie“ ab, um zum Assistenten „Ressourcengruppe erstellen“ zurückzukehren.

Im verknüpften Modus enthält die Liste Richtlinien in allen verknüpften vCentern. Sie müssen eine Richtlinie auswählen, die sich auf demselben vCenter wie die Ressourcengruppe befindet.

c. Auf der Seite **Sekundärer Schutz** wird die Liste der ausgewählten Ressourcen mit ihrem Schutzstatus angezeigt. Um die ungeschützten Ressourcen zu schützen, wählen Sie den Replikationsrichtlinientyp, das Konsistenzgruppensuffix, den Zielcluster und die Ziel-SVM aus der Dropdown-Liste aus. Beim Erstellen der Ressourcengruppe wird ein separater Job für den sekundären Schutz erstellt, den Sie im Job-Monitor-Fenster sehen können.

Felder	Beschreibung
Name der Replikationsrichtlinie	Name der SnapMirror -Richtlinie. Es werden nur die sekundären Richtlinien **Asynchronous** und **Mirror and Vault** unterstützt.
Konsistenzgruppensuffix	Eine Zieleinstellung, die zum Anhängen an die primäre Konsistenzgruppe verwendet wird, um den Namen der Zielkonsistenzgruppe zu bilden. Beispiel: Wenn der Name der primären Konsistenzgruppe „sccg_2024-11-28_120918“ lautet und Sie „_dest“ als Suffix eingeben, wird die sekundäre Konsistenzgruppe als „sccg_2024-11-28_120918_dest“ erstellt. Das Suffix ist nur für ungeschützte Konsistenzgruppen anwendbar.
Zielcluster	Für alle ungeschützten Speichereinheiten zeigt SCV die Namen der Peering-Cluster in der Dropdown-Liste an. Wenn sich der zu SCV hinzugefügte Speicher im SVM-Bereich befindet, wird aufgrund der ONTAP Beschränkung die Cluster-ID anstelle des Namens angezeigt.
Ziel-SVM	Für alle ungeschützten Speichereinheiten zeigt SCV die Namen der Peered-SVMs an. Cluster und SVM werden automatisch ausgewählt, wenn eine der Speichereinheiten ausgewählt wird, die Teil der Konsistenzgruppe ist. Dasselbe gilt für alle anderen Speichereinheiten in derselben Konsistenzgruppe.

Felder	Beschreibung
Sekundär geschützte Ressourcen	Für alle geschützten Speichereinheiten der Ressourcen, die auf der Ressourcenseite hinzugefügt werden, werden die sekundären Beziehungsdetails einschließlich Cluster, SVM und Replikationstyp angezeigt.



1. Konfigurieren Sie auf der Seite **Zeitpläne** den Sicherungszeitplan für jede ausgewählte Richtlinie.

   Geben Sie im Feld „Startstunde“ ein Datum und eine Uhrzeit ungleich Null ein. Das Datum muss im Format `day/month/year` .

   Wenn Sie im Feld „Alle“ eine Anzahl von Tagen auswählen, werden Sicherungen am ersten Tag des Monats und danach in jedem angegebenen Intervall durchgeführt. Wenn Sie beispielsweise die Option **Alle 2 Tage** auswählen, werden im Laufe des Monats an den Tagen 1, 3, 5, 7 usw. Sicherungen durchgeführt, unabhängig davon, ob das Startdatum gerade oder ungerade ist.

   Sie müssen jedes Feld ausfüllen. Das SnapCenter Plug-in for VMware vSphere erstellt Zeitpläne in der Zeitzone, in der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. Sie können die Zeitzone mithilfe der SnapCenter Plug-in for VMware vSphere ändern.

   "Ändern der Zeitzonen für Backups" .

2. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**. Ab SCV 6.1 ist der sekundäre Schutz für ASA R2-Systemressourcen auf der Übersichtsseite sichtbar.

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

   Nachdem Sie **Fertig** ausgewählt haben, wird die neue Ressourcengruppe zur Ressourcengruppenliste hinzugefügt.

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

Verwalten von Fehlern bei der Kompatibilitätsprüfung

SnapCenter führt Kompatibilitätsprüfungen durch, wenn Sie versuchen, eine Ressourcengruppe zu erstellen. Beziehen Sie sich immer auf "NetApp Interoperability Matrix Tool (IMT)" für die neuesten Informationen zum SnapCenter -Support. Gründe für Inkompatibilität können sein:

- Ein gemeinsam genutztes PCI-Gerät ist an eine VM angeschlossen.
- Die bevorzugte IP-Adresse ist in SnapCenter nicht konfiguriert.
- Sie haben die IP-Adresse zur Verwaltung der Storage-VM (SVM) nicht zu SnapCenter hinzugefügt.
- Die Speicher-VM ist ausgefallen.

Um einen Kompatibilitätsfehler zu beheben, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Speicher-VM ausgeführt wird.
2. Stellen Sie sicher, dass das Speichersystem, auf dem sich die VMs befinden, zum Inventar des SnapCenter Plug-in for VMware vSphere hinzugefügt wurde.
3. Stellen Sie sicher, dass die Speicher-VM zu SnapCenter hinzugefügt wird. Verwenden Sie die Option „Speichersystem hinzufügen“ in der GUI des VMware vSphere-Clients.
4. Wenn übergreifende VMs vorhanden sind, die VMDKs sowohl auf NetApp als auch auf Nicht- NetApp -Datenspeichern haben, verschieben Sie die VMDKs auf NetApp -Datenspeicher.

Präskripte und Postskripte

Sie können im Rahmen Ihrer Datenschutzmaßnahmen benutzerdefinierte Prescripts und Postscripts verwenden. Diese Skripte ermöglichen die Automatisierung entweder vor oder nach Ihrem Datenschutzjob. Sie können beispielsweise ein Skript einbinden, das Sie automatisch über Fehler oder Warnungen bei Datenschutzaufträgen benachrichtigt. Bevor Sie Ihre Präskripte und Postskripte einrichten, sollten Sie einige der Anforderungen zum Erstellen dieser Skripte verstehen.

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 for VMware vSphere ausgeführt. Daher müssen sich die Skripte mit Ausführungsberechtigungen im SnapCenter Plug-in for VMware vSphere OVA befinden.

Zum 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 Skriptausführung validiert.

Wo Skripte angegeben werden

Skripte werden in Sicherungsrichtlinien angegeben. Wenn ein Sicherungsauftrag gestartet wird, verknüpft die Richtlinie das Skript automatisch mit den zu sichernden Ressourcen.

Um mehrere Skripte anzugeben, drücken Sie nach jedem Skriptpfad die Eingabetaste, um jedes Skript in einer separaten Zeile aufzulisten. Semikolons (;) sind nicht zulässig. Sie können mehrere Präskripte und mehrere Postskripte angeben. Ein einzelnes Skript kann sowohl als Präskript als auch als Postskript codiert werden und andere Skripte aufrufen.

Wenn Skripte ausgeführt werden

Skripte werden entsprechend dem für BACKUP_PHASE festgelegten Wert ausgeführt.

- BACKUP_PHASE=PRE_BACKUP

  Prescripts werden in der PRE_BACKUP-Phase des Vorgangs 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 POST_BACKUP-Phase des Vorgangs ausgeführt, nachdem die Sicherung erfolgreich abgeschlossen wurde, oder in der FAILED_BACKUP-Phase, wenn die Sicherung nicht erfolgreich abgeschlossen wurde.

  > Wenn ein Postscript fehlschlägt, wird die Sicherung 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`

An Skripte übergebene Umgebungsvariablen

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

Umgebungsvariable	Beschreibung
`BACKUP_NAME`	Name der Sicherung. Variable wird nur in Postskripten übergeben.
`BACKUP_DATE`	Datum der Sicherung im Format `yyyymmdd` Variable wird nur in Postskripten übergeben.
`BACKUP_TIME`	Zeitpunkt der Sicherung im Format `hhmmss` Variable wird nur in Postskripten übergeben.

Umgebungsvariable	Beschreibung
BACKUP_PHASE	Die Phase der Sicherung, in der das Skript ausgeführt werden soll. Gültige Werte sind: PRE_BACKUP, POST_BACKUP, and FAILED_BACKUP . In Präskripten und Postskripten übergebene Variable.
STORAGE_SNAPSHOTS	Die Anzahl der Speicher-Snapshots im Backup. Variable wird nur in Postskripten übergeben.
STORAGE_SNAPSHOT.#	Einer der definierten Speicher-Snapshots im folgenden Format: <filer>:/vol/<volume>:<ONTAP-snapshot-name> Variable wird nur in Postskripten übergeben.
VIRTUAL_MACHINES	Die Anzahl der VMs im Backup. In Präskripten und Postskripten übergebene Variable.
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> hat die Werte true oder false In Präskripten und Postskripten übergebene Variable.

Skript-Timeouts

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

Beispiel-PERL-Skript Nr. 1

Das folgende Beispiel-PERL-Skript druckt die Umgebungsvariablen, wenn eine Sicherung 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-PERL-Skript Nr. 2

Das folgende Beispiel gibt Informationen zur Sicherung aus.

```
#!/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-Shell-Skript

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

Hinzufügen einer einzelnen VM oder eines Datenspeichers zu einer Ressourcengruppe

Sie können schnell eine einzelne VM oder einen einzelnen Datenspeicher zu jeder vorhandenen Ressourcengruppe hinzufügen, die vom SnapCenter Plug-in for VMware vSphere verwaltet wird.

Informationen zu diesem Vorgang

Sie können SAN- und NAS-Datenspeicher hinzufügen, jedoch keine VSAN- oder VVOL-Datenspeicher.

Schritte

1. Wählen Sie in der GUI des vSphere-Clients **Menü** in der Symbolleiste 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 Datenspeicher und wählen Sie aus der sekundären Dropdownliste „SnapCenter Plug-in for VMware vSphere“ > „Zur Ressourcengruppe hinzufügen“ aus.

   Das System prüft zunächst, ob SnapCenter das Speichersystem, auf dem sich die ausgewählte VM befindet, verwaltet und mit diesem kompatibel ist, und zeigt dann die Seite **Zur Ressourcengruppe**

hinzufügen an. Wenn die Nachricht `SnapCenter Compatibility Error` angezeigt wird, ist die ausgewählte VM nicht mit SnapCenter kompatibel und Sie müssen zuerst die entsprechende Speicher-VM zu SnapCenter hinzufügen.

3. Wählen Sie auf der Seite **Zur Ressourcengruppe hinzufügen** eine Ressourcengruppe aus und klicken Sie dann auf **OK**.

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

   Wenn die Nachricht `Selected <resource-name> is not SnapCenter compatible` angezeigt wird, ist eine ausgewählte VM oder ein ausgewählter Datenspeicher nicht mit SnapCenter kompatibel. Weitere Informationen finden Sie unter "Verwalten von Fehlern bei der Kompatibilitätsprüfung" für weitere Informationen.

Hinzufügen mehrerer VMs und Datenspeicher zu einer Ressourcengruppe

Mit dem Assistenten „Ressourcengruppe bearbeiten“ des SnapCenter VMware vSphere-Clients können Sie einer vorhandenen Ressourcengruppe mehrere Ressourcen hinzufügen.

Eine Ressourcengruppe kann eines der folgenden Elemente enthalten:

- Jede Kombination aus herkömmlichen VMs und SAN- und NAS-Datenspeichern (vVol-Datenspeicher werden nicht unterstützt).
- Ein FlexGroup -Datenspeicher (übergreifende VMs werden nicht unterstützt).
- Ein oder mehrere FlexVol -Datenspeicher (übergreifende VMs werden unterstützt).
- Eine oder mehrere vVol-VMs.
- Alle vVol-VMs mit einem angegebenen vSphere-Tag.
- Alle vVol-VMs in einem angegebenen Ordner.

> vVol-VMs, die sich über mehrere vVol-Datenspeicher erstrecken, werden nicht unterstützt, da SnapCenter vVols nur im primären, ausgewählten vVol-Datenspeicher sichert.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plugins **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und wählen Sie dann **Ressourcengruppe bearbeiten**, um den Assistenten zu starten.
2. Führen Sie auf der Seite **Ressource** die folgenden Schritte aus:

   a. Navigieren Sie im Feld „Datenspeicher“ zu den VMs oder Datenspeichern, die Sie hinzufügen möchten.

   b. Wählen Sie in der Liste „Verfügbare Entitäten“ eine oder mehrere VMs oder Datenspeicher 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 in der Liste „Verfügbare Entitäten“ das Datacenter-Objekt angezeigt. Sie können einen Datenspeicher auswählen, um die VMs im Datenspeicher anzuzeigen und sie der

Ressourcengruppe hinzuzufügen.

Wenn Sie **Weiter** auswählen, überprüft das System zunächst, ob SnapCenter den Speicher verwaltet und mit ihm kompatibel ist, auf dem sich die ausgewählten VMs oder Datenspeicher befinden. Wenn die Nachricht `Some entities are not SnapCenter compatible` angezeigt wird, ist eine ausgewählte VM oder ein ausgewählter Datenspeicher nicht mit SnapCenter kompatibel. Weitere Informationen finden Sie unter "Verwalten von Fehlern bei der Kompatibilitätsprüfung" für weitere Informationen.

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

Wiederherstellen der Sicherung des umbenannten Speichers

Wenn der Speicher umbenannt wird, schlugen Workflows, die vor der Umbenennung erstellte Sicherungen verwendeten, fehl. Mit der Einführung der Funktion zum Umbenennen von Backups, die ausschließlich über die REST-API zugänglich ist, ist es jetzt möglich, die Backups zu verwenden, die vor der Umbenennung des Speichers erstellt wurden. Der Arbeitsablauf und die Verwendung der REST-API werden unten beschrieben.

Das ASA R2-Speichersystem unterstützt die Funktion zur Benennung aktueller Snapshots nicht.

Schritte

1. Fügen Sie die neue Speicherverbindung hinzu oder aktualisieren Sie sie und stellen Sie sicher, dass der neue Cluster- oder SVM-Name in SCV angezeigt wird.
2. Starten Sie den Dienst neu, um die Caches wie im KB-Artikel beschrieben zu aktualisieren: "SCV-Sicherungen schlagen nach der SVM-Umbenennung fehl"
3. Erstellen Sie ein neues Backup.
4. Verwenden Sie die Sicherungsdetails, um die alten und neuen Speichernamen zu finden.
5. Wählen Sie im Bildschirm **Backups** des vSphere-Clients das Backup aus, um dessen 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/Speichersystem

   Beispiel: { "existingSVM": { "name": "string" }, "newSVM": { "name": "string" } }

   Antwort:

   { "statusMessage": "OK", "statusCode": 200, "responseMessage": ["Speichersystem erfolgreich umbenannt."] }

   Nach dem Ausführen dieser API können Sie alle Workflows ausführen, einschließlich des Wiederherstellungsvorgangs aus der alten Sicherung.

Sichern Sie Ressourcengruppen bei Bedarf

Sicherungsvorgänge werden für alle in einer Ressourcengruppe definierten Ressourcen ausgeführt. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

> ASA R2 Backup erstellt Snapshots der Konsistenzgruppe und stellt eine primäre Konsistenzgruppe bereit, wenn die angegebene Ressource noch nicht darüber verfügt.

Bevor Sie beginnen

Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

> Starten Sie keinen On-Demand-Sicherungsauftrag, wenn bereits ein Auftrag zum Sichern des SnapCenter Plug-in for VMware vSphere MySQL-Datenbank ausgeführt wird. Verwenden Sie die Wartungskonsole, um den konfigurierten Sicherungszeitplan für die MySQL-Datenbank anzuzeigen.

Informationen zu diesem Vorgang

In früheren Versionen der Virtual Storage Console (VSC) konnten Sie eine On-Demand-Sicherung durchführen, ohne dass ein Sicherungsauftrag für eine VM oder einen Datenspeicher konfiguriert war. Für das SnapCenter Plug-in for VMware vSphere müssen sich VMs und Datenspeicher jedoch in einer Ressourcengruppe befinden, bevor Sie Sicherungen durchführen können.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plugins **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und wählen Sie dann **Jetzt ausführen**, um die Sicherung zu starten.
2. Wenn für die Ressourcengruppe mehrere Richtlinien konfiguriert sind, 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 unten im Fenster **Letzte Aufgaben** auswählen oder im Dashboard **Job Monitor** für weitere Details. .Ergebnis

Wenn der Stilllegungsvorgang für eine der VMs im Backup fehlschlägt, wird das Backup mit einer Warnung abgeschlossen und als nicht VM-konsistent gekennzeichnet, auch wenn in der ausgewählten Richtlinie VM-Konsistenz ausgewählt ist. In diesem Fall ist es möglich, dass einige der VMs erfolgreich stillgelegt wurden. Im Job-Monitor wird in den Details der fehlgeschlagenen VM die Stilllegung als fehlgeschlagen angezeigt.

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

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

Sie sollten das Repository auch sichern, bevor Sie Migrationen oder Upgrades durchführen.

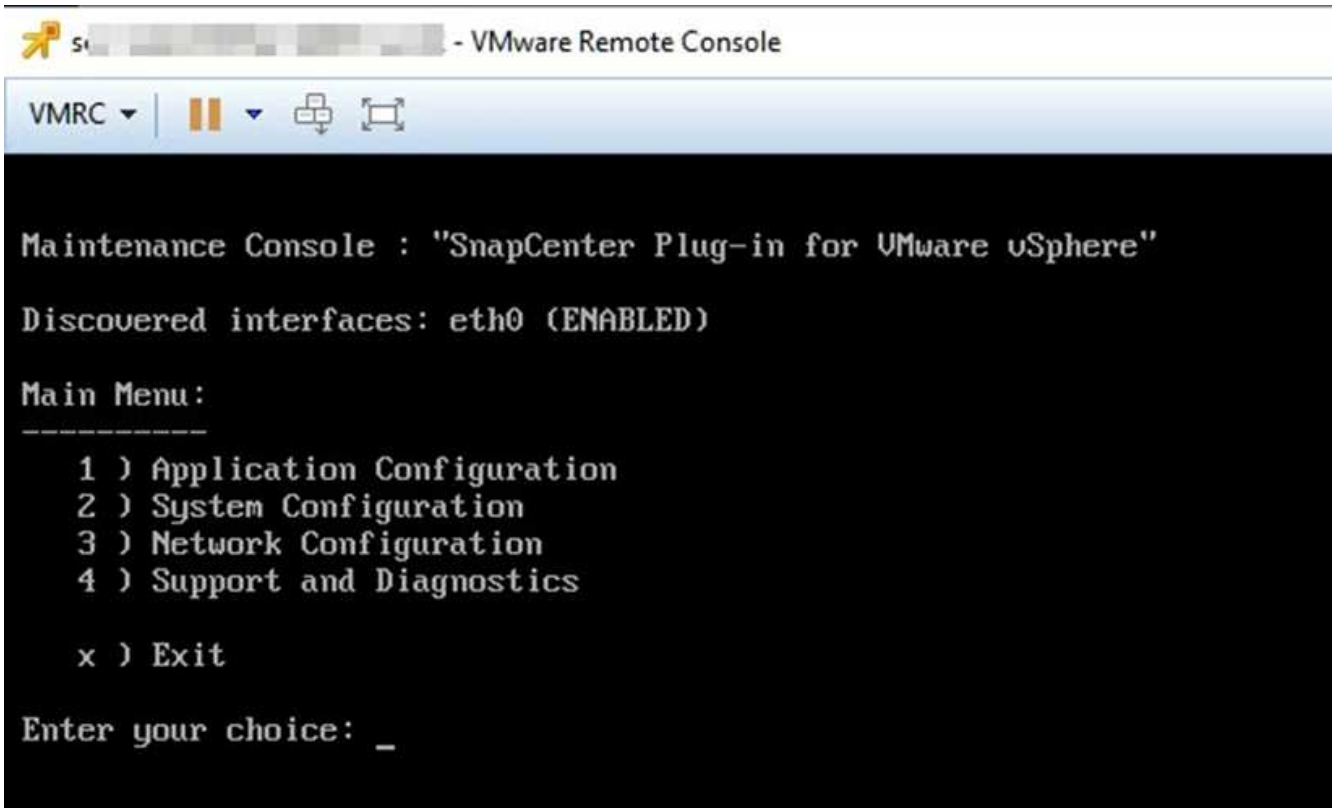
Bevor Sie beginnen

Starten Sie keinen Job zum Sichern der MySQL-Datenbank, wenn bereits ein On-Demand-Sicherungsjob

ausgeführt wird.

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter Plug-in for VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remotekonsole starten oder Webkonsole starten** aus, um ein Wartungskonsolenfenster zu öffnen.



3. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration** ein.
4. Geben Sie im Anwendungskonfigurationsmenü die Option **6) MySQL-Sicherung und -Wiederherstellung** ein.
5. Geben Sie im Konfigurationsmenü für MySQL-Backup und -Wiederherstellung die Option **1) MySQL-Backup konfigurieren** ein.
6. Geben Sie bei der Eingabeaufforderung den Sicherungsspeicherort für das Repository, die Anzahl der aufzubewahrenden Sicherungen und die Uhrzeit ein, zu der die Sicherung beginnen soll.

   Alle Eingaben werden beim Eingeben gespeichert. Wenn die Sicherungsaufbewahrungsnummer erreicht ist, werden ältere Sicherungen gelöscht, wenn neue Sicherungen durchgeführt werden.

   Repository-Backups werden „backup-<Datum>“ genannt. Da die Repository-Wiederherstellungsfunktion nach dem Präfix „Backup“ sucht, sollten Sie es nicht ändern.

Verwalten von Ressourcengruppen

Sie können Sicherungsressourcengruppen erstellen, ändern und löschen sowie Sicherungsvorgänge für Ressourcengruppen durchführen.

Ressourcengruppen werden in der Virtual Storage Console (VSC) als Sicherungsjobs bezeichnet.

Anhalten und Fortsetzen von Vorgängen für Ressourcengruppen

Sie können den Start geplanter Vorgänge für eine Ressourcengruppe vorübergehend deaktivieren. Sie können diese Vorgänge später bei Bedarf aktivieren.

Schritte

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

Nach Abschluss

Auf der Seite „Ressourcengruppen“ lautet der Auftragsstatus für die ausgesetzte Ressource `Under_Maintenance` . Möglicherweise müssen Sie in der Tabelle nach rechts scrollen, um die Spalte „Auftragsstatus“ anzuzeigen.

Nach der Wiederaufnahme der Sicherungsvorgänge ändert sich der Jobstatus in `Production` .

Ändern von Ressourcengruppen

Sie können Ressourcen in Ressourcengruppen in vCenter entfernen oder hinzufügen, Richtlinien trennen oder anhängen, Zeitpläne ändern oder jede andere Option der Ressourcengruppe ändern.

Informationen zu diesem Vorgang

Wenn Sie den Namen einer Ressourcengruppe ändern möchten, verwenden Sie in den Namen von VMs, Datenspeichern, Richtlinien, Backups oder Ressourcengruppen nicht die folgenden Sonderzeichen:

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

Schritte

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

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

3. Wählen Sie **Weiter**, bis die Seite „Zusammenfassung“ angezeigt wird, und wählen Sie dann **Fertig**.

Ressourcengruppen löschen

Sie können eine Ressourcengruppe in vCenter löschen, wenn Sie die Ressourcen in der Ressourcengruppe nicht mehr schützen müssen. Sie müssen sicherstellen, dass alle Ressourcengruppen gelöscht werden, bevor Sie das SnapCenter Plug-in for VMware vSphere aus vCenter entfernen.

Informationen zu diesem Vorgang

Alle Löschvorgänge für Ressourcengruppen werden als erzwungene Löschungen ausgeführt. Der Löschvorgang trennt 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 kann der letzte Snapshot nicht gelöscht werden. Daher kann die Ressourcengruppe nicht gelöscht werden. Bevor Sie eine Ressourcengruppe löschen, die Teil einer SnapVault -Beziehung ist, müssen Sie entweder den System Manager oder die ONTAP CLI verwenden, um die SnapVault -Beziehung zu entfernen. Anschließend müssen Sie den letzten Snapshot löschen.

Schritte

1. Wählen Sie im linken Navigationsbereich des SCV-Plug-Ins **Ressourcengruppen** aus, wählen Sie dann eine Ressourcengruppe aus und wählen Sie **Löschen**.
2. Wählen Sie im Bestätigungsfeld **Ressourcengruppe löschen** zur Bestätigung **OK** aus.

Richtlinien verwalten

Sie können Sicherungsrichtlinien für das SnapCenter Plug-in for VMware vSphere erstellen, ändern, anzeigen, trennen und löschen. Zur Durchführung von Datenschutzvorgängen sind Richtlinien erforderlich.

Richtlinien trennen

Sie können Richtlinien von einer SnapCenter Plug-in for VMware vSphere trennen, wenn diese Richtlinien den Datenschutz für die Ressourcen nicht mehr regeln sollen. Sie müssen eine Richtlinie trennen, bevor Sie sie entfernen oder die Zeitplanhäufigkeit ändern können.

Informationen zu diesem Vorgang

Die Richtlinien zum Trennen von Richtlinien vom SnapCenter Plug-in for VMware vSphere Ressourcengruppen unterscheiden sich von den Richtlinien für SnapCenter -Ressourcengruppen. Bei einer VMware vSphere-Client-Ressourcengruppe ist es möglich, alle Richtlinien zu trennen, sodass die Ressourcengruppe keine Richtlinie mehr hat. Um jedoch Datenschutzvorgänge für diese Ressourcengruppe durchführen zu können, müssen Sie mindestens eine Richtlinie anhängen.

Schritte

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

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

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

Informationen zu diesem Vorgang

Das Ändern der Sicherungsrichtlinien des SnapCenter Plug-in for VMware vSphere unterscheidet sich vom Ändern der Sicherungsrichtlinien für anwendungsbasierte SnapCenter -Plug-ins. Sie müssen Richtlinien nicht von Ressourcengruppen trennen, wenn Sie die Plug-In-Richtlinien ändern.

Bevor Sie die Replikations- oder Aufbewahrungseinstellungen ändern, sollten Sie die möglichen Konsequenzen bedenken.

- Erhöhen der Replikations- oder Aufbewahrungseinstellungen

  Es werden weiterhin Backups gesammelt, bis die neue Einstellung erreicht ist.

- Reduzieren der Replikations- oder Aufbewahrungseinstellungen

  Sicherungen, die über die neue Einstellung hinausgehen, werden bei der nächsten Sicherung gelöscht.

> Um einen Richtlinienplan für das SnapCenter Plug-in for VMware vSphere zu ändern, müssen Sie den Zeitplan in der Plug-in-Ressourcengruppe ändern.

Schritte

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

Die Änderungen werden wirksam, wenn die nächste geplante Sicherung durchgeführt wird.

Richtlinien löschen

Wenn Sie eine konfigurierte Sicherungsrichtlinie für das SnapCenter Plug-in for VMware vSphere nicht mehr 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“ aus, wählen Sie dann eine Richtlinie aus und wählen Sie „Entfernen“ aus.
2. Wählen Sie im Bestätigungsdialogfeld **OK**.

Backups verwalten

Sie können vom SnapCenter Plug-in for VMware vSphere durchgeführte Sicherungen umbenennen und löschen. Sie können auch mehrere Backups gleichzeitig löschen.

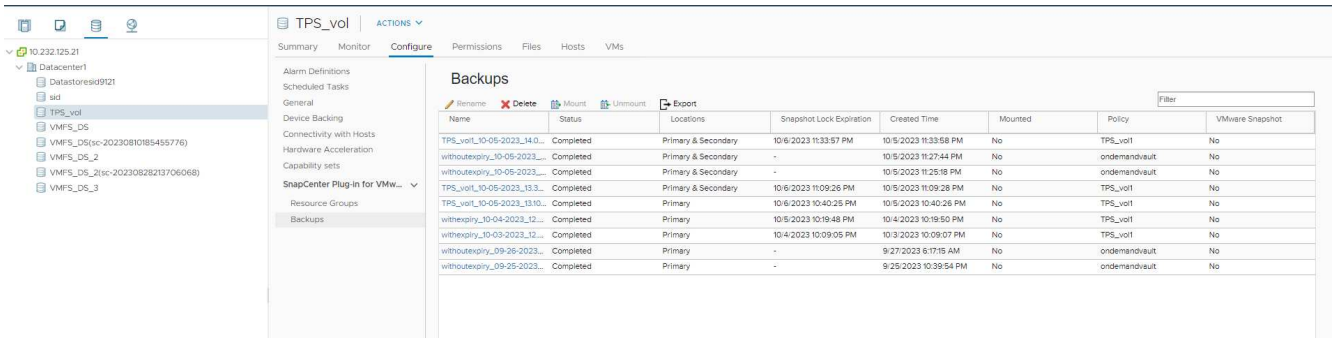
Backups umbenennen

Sie können das SnapCenter Plug-in for VMware vSphere Backups umbenennen, wenn Sie einen besseren Namen zur Verbesserung der Suchbarkeit angeben möchten.

Das ASA R2-Speichersystem unterstützt das Umbenennen von Backups nicht.

Schritte

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



2. Wählen Sie auf der Registerkarte „Konfigurieren“ eine Sicherung 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-, Datenspeicher-, Richtlinien-, Sicherungs- oder Ressourcengruppennamen: & * $ # @ ! \ / : * ? " < > - | ; ' und Leerzeichen. Ein Unterstrich (_) ist zulässig.

Backups löschen

Sie können das SnapCenter Plug-in for VMware vSphere -Backups löschen, wenn Sie das Backup nicht mehr für andere Datenschutzvorgänge benötigen. Sie können ein Backup oder mehrere Backups gleichzeitig löschen.

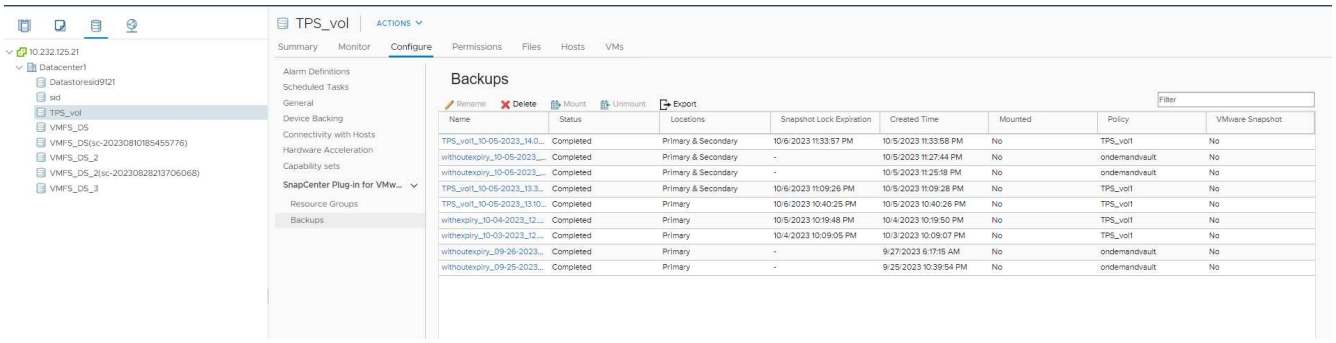
Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Snapshots auf sekundärem Speicher werden von Ihren ONTAP Aufbewahrungseinstellungen verwaltet, nicht vom SnapCenter Plug-in for VMware vSphere. Wenn Sie daher das SnapCenter Plug-in for VMware vSphere zum Löschen einer Sicherung verwenden, werden Snapshots auf dem primären Speicher gelöscht, Snapshots auf dem sekundären Speicher jedoch nicht. Wenn auf dem sekundären Speicher noch ein Snapshot vorhanden ist, behält das SnapCenter Plug-in for VMware vSphere die mit der Sicherung verknüpften Metadaten bei, um Wiederherstellungsanforderungen zu unterstützen. Wenn der ONTAP Aufbewahrungsprozess den sekundären Snapshot löscht, löscht das SnapCenter Plug-in for VMware vSphere die Metadaten mithilfe eines Bereinigungsjobs, der in regelmäßigen Abständen ausgeführt wird.

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



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 Sicherungsliste, indem Sie das Aktualisierungssymbol in der linken vSphere-Menüleiste auswählen.

Mounten und Unmounten von Datenspeichern

Mounten Sie ein Backup

Sie können einen herkömmlichen Datenspeicher aus einer Sicherung mounten, wenn Sie auf Dateien in der Sicherung 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 über denselben VM-Typ und dieselben Hostkonfigurationen verfügt. Sie können einen Datenspeicher mehrmals auf einem Host mounten.

Sie können keinen vVol-Datenspeicher mounten.

Bevor Sie beginnen

- Stellen Sie sicher, dass ein alternativer ESXi-Host eine Verbindung zum Speicher herstellen kann

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

  - Dieselbe UID und GID wie die des ursprünglichen Hosts
  - Dieselbe virtuelle Appliance für das SnapCenter Plug-in for 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 LUNs/Namespaces

  Da der ESXi-Host nur einen eindeutigen LUN/Namespace pro Datenspeicher erkennen kann, schlägt der Vorgang fehl, wenn mehr als einer gefunden wird. Dies kann passieren, 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 Unmount-Vorgangs nicht aus dem Speicher gelöscht werden. Um die Erkennung mehrerer Klone zu vermeiden, sollten Sie alle veralteten LUNs/Namespaces auf dem Speicher bereinigen.

Informationen zu diesem Vorgang

Ein Mount-Vorgang kann fehlschlagen, wenn die Speicherebene des FabricPool , in dem sich der Datenspeicher befindet, nicht verfügbar ist.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des VMware vSphere-Clients **Speicher** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Datenspeicher und wählen Sie * SnapCenter Plug-in for VMware vSphere* > **Backup mounten**.
3. Wählen Sie auf der Seite **Datenspeicher bereitstellen** eine Sicherung und einen Sicherungsspeicherort (primär oder sekundär) aus und wählen Sie dann **Fertig stellen**.
4. Optional: Um zu überprüfen, ob der Datenspeicher gemountet ist, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **Menü** in der Symbolleiste und wählen Sie dann **Speicher** aus der Dropdown-Liste.
   b. Im linken Navigationsbereich wird der von Ihnen gemountete Datenspeicher oben in der Liste angezeigt.

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

Ein Backup aushängen

Sie können die Bereitstellung einer Sicherung aufheben, wenn Sie nicht mehr auf die Dateien im Datenspeicher zugreifen müssen.

Wenn ein Backup in der VMware vSphere-Client-GUI als gemountet aufgeführt ist, 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 may 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 Verknüpfungsseite des VMware vSphere-Clients **Speicher** aus.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf einen Datenspeicher, wählen Sie dann in der Dropdownliste „SnapCenter Plug-in for VMware vSphere“ und anschließend in der sekundären Dropdownliste „Unmounten“ aus.

   Stellen Sie sicher, dass Sie den richtigen Datenspeicher zum Unmounten auswählen. Andernfalls kann es zu Beeinträchtigungen der Produktionsarbeit kommen.

3. Wählen Sie im Dialogfeld **Unmount Cloned Datastore** einen Datenspeicher aus, aktivieren Sie das Kontrollkästchen **Unmount the cloned datastore** und wählen Sie dann **Unmount**.

Sicherungen wiederherstellen

Übersicht wiederherstellen

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

- VM-Wiederherstellungsziele

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

  Sie können vVol-VMs auf dem ursprünglichen Host wiederherstellen.

- VMDK-Wiederherstellungsziele

  Sie können VMDKs in herkömmlichen VMs entweder im Original oder in einem alternativen Datenspeicher wiederherstellen.

  Sie können VMDKs in vVol-VMs im ursprünglichen Datenspeicher wiederherstellen.

Sie können auch einzelne Dateien und Ordner in einer Gastdateiwiederherstellungssitzung wiederherstellen, bei der eine Sicherungskopie einer virtuellen Festplatte angehängt und dann die ausgewählten Dateien oder Ordner wiederhergestellt werden.

Folgendes können Sie nicht wiederherstellen:

- Datenspeicher

  Sie können das SnapCenter Plug-in for VMware vSphere nicht zum Wiederherstellen eines Datenspeichers verwenden, sondern nur der einzelnen VMs im Datenspeicher.

- Backups entfernter VMs

  Sie können keine Sicherungen von entfernten Speicher-VMs wiederherstellen. Wenn Sie beispielsweise mithilfe des Management-LIF eine Speicher-VM hinzufügen und dann ein Backup erstellen und dann diese Speicher-VM entfernen und einen Cluster hinzufügen, der dieselbe Speicher-VM enthält, schlägt der Wiederherstellungsvorgang für das Backup fehl.

So werden Wiederherstellungsvorgänge ausgeführt

Für VMFS-Umgebungen verwendet das SnapCenter Plug-in for VMware vSphere Klon- und Mountvorgänge mit Storage VMotion, um Wiederherstellungsvorgänge durchzuführen. Für NFS-Umgebungen verwendet das Plug-in den nativen ONTAP Single File SnapRestore (SFSR), um bei den meisten Wiederherstellungsvorgängen eine höhere Effizienz zu gewährleisten. Für vVol-VMs verwendet das Plug-In ONTAP Single File Snapshot Restore (ONTAP SFSR) und SnapMirror Restore für Wiederherstellungsvorgänge. In der folgenden Tabelle ist aufgeführt, wie Wiederherstellungsvorgänge durchgeführt werden.

Wiederherstellungsvorgänge	Aus	Durchgeführt mit
VMs und VMDKs	Primäre Sicherungen	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 Sicherungen	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	ONTAP Single File SnapRestore für alle Protokolle
vVol-VMs	Absturzkonsistente sekundäre Backups	ONTAP SnapMirror Restore für alle Protokolle
FlexGroup -VMs	Primäre Sicherungen	NFS-Umgebungen: * ONTAP Single File SnapRestore, wenn Sie ONTAP Version 9.10.1 und höher verwenden * Klonen und Mounten mit Storage VMotion auf früheren ONTAP Versionen VMFS-Umgebungen: Nicht unterstützt für FlexGroups

Wiederherstellungsvorgänge	Aus	Durchgeführt mit
FlexGroup -VMs	Sekundäre Backups	NFS-Umgebungen: • ONTAP SnapMirror Restore, 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

Sie können eine vVol-VM nach einer Neuverteilung des vVol-Containers nicht wiederherstellen.

Gastdateiwiederherstellungsvorgänge werden mithilfe von Klon- und Mountvorgängen (nicht Storage VMotion) in NFS- und VMFS-Umgebungen durchgeführt.

Während einer Wiederherstellung kann der Fehler auftreten `Host unresolved volumes is null` oder `Exception while calling pre-restore on SCV….Error mounting cloned LUN as datastore…` Dies tritt auf, wenn das SnapCenter Plug-in for VMware vSphere versucht, den Klon neu zu signieren. Aufgrund von VMware-Einschränkungen kann das SnapCenter Plug-in for VMware vSphere den automatischen Neusignaturwert in erweiterten ESXi-Hostkonfigurationen nicht steuern. Bei NVMe-über-TCP- und NVMe-über-FC-Speicher kann SCV keine Controller dynamisch hinzufügen, wenn ein neues Subsystem hinzugefügt wird. Sie sollten die erforderliche Zuordnung vor dem Mount-Vorgang vornehmen.

Siehe "KB-Artikel: SCV-Klonen oder -Wiederherstellungen schlagen mit der Fehlermeldung „Host Unresolved volumes is null“ fehl." für weitere Informationen zum Fehler.

Suche nach Backups

Mit dem Wiederherstellungsassistenten können Sie nach einer bestimmten Sicherung einer VM oder eines Datenspeichers suchen und diese finden. Nachdem Sie eine Sicherungskopie gefunden haben, können Sie sie wiederherstellen.

Schritte

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

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

So zeigen Sie Sicherungen für … an	Gehen Sie wie folgt vor…
Datenspeicher	Wählen Sie die Menüoption **Speicher**, wählen Sie dann einen Datenspeicher aus, wählen Sie dann die Registerkarte **Konfigurieren** und wählen Sie dann **Backups** im Abschnitt * SnapCenter Plug-in for VMware vSphere*.

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 Datenspeicher, wählen Sie dann * SnapCenter Plug-in for VMware vSphere* in der Dropdown-Liste und wählen Sie dann * Wiederherstellen * in der sekundären Dropdown-Liste.
4. Geben Sie im Assistenten **Wiederherstellen** einen Suchnamen ein und wählen Sie **Suchen**.

   Sie können die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Außerdem können Sie auswählen, ob Sie Sicherungen mit VMware-Snapshots wünschen, ob Sie bereitgestellte Sicherungen wünschen und den Speicherort. Wählen Sie **OK**.

Wiederherstellen von VMs aus Backups

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

Sie können VMs an den folgenden Speicherorten wiederherstellen:

- Am ursprünglichen Speicherort wiederherstellen
  - Zum ursprünglichen Datenspeicher, der auf dem ursprünglichen ESXi-Host gemountet ist (dadurch wird die ursprüngliche VM überschrieben)
- An einem anderen Speicherort wiederherstellen
  - Zu einem anderen Datenspeicher, der auf dem ursprünglichen ESXi-Host gemountet ist
  - Zum ursprünglichen Datenspeicher, der auf einem anderen ESXi-Host bereitgestellt ist, der vom selben vCenter verwaltet wird
  - Zu einem anderen Datenspeicher, der auf einem anderen ESXi-Host bereitgestellt ist, der vom selben vCenter verwaltet wird
  - Zu einem anderen Datenspeicher, der auf einem anderen ESXi-Host bereitgestellt ist, der 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 Speicher-VM hinzu, führen Sie dann eine Sicherung dieser VM durch, löschen Sie dann die Speicher-VM und fügen Sie einen Cluster hinzu, der dieselbe Speicher-VM enthält, und versuchen Sie dann, die ursprüngliche Sicherung wiederherzustellen.

Aktivieren Sie die VMware-Anwendung vStorage API for Array Integration (VAAI), um die Leistung von Wiederherstellungsvorgängen in NFS-Umgebungen zu verbessern.

Bevor Sie beginnen

- Es muss ein Backup vorhanden sein.

  Sie müssen mit dem SnapCenter Plug-in for VMware vSphere eine Sicherung der VM erstellt haben, bevor Sie die VM wiederherstellen können.

  > Wiederherstellungsvorgänge können nicht erfolgreich abgeschlossen werden, wenn Snapshots der VM vorhanden sind, die mit anderer Software als dem SnapCenter Plug-in for VMware vSphere erstellt wurden.

- Der Zieldatenspeicher muss bereit sein.
  - Der Zieldatenspeicher für den Wiederherstellungsvorgang muss über genügend Speicherplatz verfügen, um eine Kopie aller VM-Dateien aufzunehmen (z. B. vmdk, vmx, vmsd).
  - Der Zieldatenspeicher darf keine veralteten VM-Dateien aus früheren fehlgeschlagenen Wiederherstellungsvorgängen enthalten. Veraltete Dateien haben das Namensformat `restore_xxx_xxxxxx_<filename>`.
- Die VM darf sich nicht im Transit befinden.

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

- HA-Konfigurationsfehler

  Stellen Sie sicher, dass auf dem Bildschirm „vCenter ESXi-Hostübersicht“ keine HA-Konfigurationsfehler angezeigt werden, bevor Sie Sicherungen an einem anderen Speicherort wiederherstellen.

- Wiederherstellen an einem anderen Ort
  - Bei der Wiederherstellung an einem anderen Speicherort muss das SnapCenter Plug-in for VMware vSphere im vCenter ausgeführt werden, das das Ziel für den Wiederherstellungsvorgang ist. Der Zieldatenspeicher muss über ausreichend Speicherplatz verfügen.
  - Das Ziel-vCenter im Feld „An alternativem Speicherort wiederherstellen“ muss per DNS auflösbar sein.

Informationen zu diesem Vorgang

- VM wird abgemeldet und erneut registriert

  Der Wiederherstellungsvorgang für VMs hebt die Registrierung der ursprünglichen VM auf, stellt die VM aus einem Sicherungs-Snapshot wieder her und registriert die wiederhergestellte VM mit demselben Namen und derselben Konfiguration auf demselben ESXi-Server. Sie müssen die VMs nach der Wiederherstellung manuell zu Ressourcengruppen hinzufügen.

- Wiederherstellen von Datenspeichern

  Sie können einen Datenspeicher nicht wiederherstellen, aber Sie können jede VM im Datenspeicher wiederherstellen.

- Wiederherstellen von vVol-VMs
  - vVol-Datenspeicher, die sich über mehrere VMs erstrecken, werden nicht unterstützt. Da angehängte VMDKs in einem VM-übergreifenden vVol-Datenspeicher nicht gesichert werden, enthalten die wiederhergestellten VMs nur teilweise VMDKs.
  - Sie können ein vVol nicht auf einem alternativen Host wiederherstellen.

    - Die automatische Neuverteilung von vVol wird nicht unterstützt.
- VMware-Konsistenz-Snapshot-Fehler für eine VM

  Selbst wenn ein VMware-Konsistenz-Snapshot für eine VM fehlschlägt, wird die VM dennoch gesichert. Sie können die in der Sicherungskopie enthaltenen Entitäten im Wiederherstellungsassistenten anzeigen und für Wiederherstellungsvorgänge verwenden.

- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn die Speicherebene des FabricPool , in dem sich die VM befindet, nicht verfügbar ist.

Schritte

1. Wählen Sie in der GUI 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 dem SnapCenter Plug-in for VMware vSphere hinzugefügt wurden, `vsadmin` oder ein Benutzerkonto, das über dieselben Berechtigungen verfügt wie `vsadmin` .

2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM, wählen Sie dann in der Dropdownliste „SnapCenter Plug-in for VMware vSphere“ und anschließend in der sekundären Dropdownliste „Wiederherstellen“ aus, um den Assistenten zu starten.
3. Wählen Sie im Assistenten **Wiederherstellen** auf der Seite **Sicherung auswählen** den Sicherungs-Snapshot aus, den Sie wiederherstellen möchten.

   Sie können nach einem bestimmten Sicherungsnamen oder einem Teil des Sicherungsnamens suchen oder die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Außerdem können Sie auswählen, ob Sie Sicherungen mit VMware-Snapshots wünschen, ob Sie bereitgestellte Sicherungen wünschen und den Speicherort. Wählen Sie **OK**, um zum Assistenten zurückzukehren.

4. Wählen Sie auf der Seite **Bereich auswählen** im Feld **Wiederherstellungsbereich** die Option **Gesamte virtuelle Maschine** aus, wählen Sie dann den Wiederherstellungsort aus und geben Sie dann die Zielinformationen ein, unter denen die Sicherung bereitgestellt werden soll.

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

   Beim Wiederherstellen von Teilsicherungen wird die Seite „Bereich auswählen“ beim Wiederherstellungsvorgang übersprungen.

5. Wählen Sie auf der Seite **Speicherort auswählen** den Speicherort für den wiederhergestellten Datenspeicher aus.

   Im SnapCenter Plug-in for VMware vSphere 4.5 und höher können Sie sekundären Speicher für FlexGroup -Volumes auswählen.

6. Überprüfen Sie die Seite „Zusammenfassung“ und wählen Sie dann **Fertig**.
7. Optional: Überwachen Sie den Vorgangsfortschritt, indem Sie unten auf dem Bildschirm **Letzte Aufgaben** auswählen.

   Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

Nach Abschluss

- IP-Adresse ändern

  Wenn Sie die Wiederherstellung an einem anderen Standort durchgeführt haben, müssen Sie die IP-Adresse der neu erstellten VM ändern, um einen IP-Adresskonflikt zu vermeiden, wenn statische IP-Adressen konfiguriert sind.

- Hinzufügen wiederhergestellter VMs zu Ressourcengruppen

  Obwohl die VMs wiederhergestellt werden, werden sie nicht automatisch zu ihren früheren Ressourcengruppen hinzugefügt. Daher müssen Sie die wiederhergestellten VMs manuell zu den entsprechenden Ressourcengruppen hinzufügen.

Wiederherstellen gelöschter VMs aus Backups

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

Sie können VMs an den folgenden Speicherorten wiederherstellen:

- Am ursprünglichen Speicherort wiederherstellen
  - Zum ursprünglichen Datenspeicher, der auf dem ursprünglichen ESXi-Host gemountet ist (dadurch wird eine Kopie der VM erstellt)
- An einem anderen Speicherort wiederherstellen
  - Zu einem anderen Datenspeicher, der auf dem ursprünglichen ESXi-Host gemountet ist
  - Zum ursprünglichen Datenspeicher, der auf einem anderen ESXi-Host bereitgestellt ist, der vom selben vCenter verwaltet wird
  - Zu einem anderen Datenspeicher, der auf einem anderen ESXi-Host bereitgestellt ist, der vom selben vCenter verwaltet wird
  - Zu einem anderen Datenspeicher, der auf einem anderen ESXi-Host bereitgestellt ist, der von einem anderen vCenter im verknüpften Modus verwaltet wird

> Bei der Wiederherstellung an einem anderen Speicherort muss das SnapCenter Plug-in for VMware vSphere im verknüpften vCenter ausgeführt werden, das das Ziel für den Wiederherstellungsvorgang ist. Der Zieldatenspeicher 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 der VM ursprünglich zugewiesen waren, nicht wiederhergestellt.

Bevor Sie beginnen

- Das Benutzerkonto für das Speichersystem auf der Seite „Speichersysteme“ im VMware vSphere-Client muss über die"Für ONTAP ONTAP Mindestberechtigungen" .
- Das Benutzerkonto in vCenter muss über die"Für das SnapCenter Plug-in for VMware vSphere sind mindestens vCenter-Berechtigungen erforderlich" .

- Es muss ein Backup vorhanden sein.

  Sie müssen mit dem SnapCenter Plug-in for VMware vSphere eine Sicherung der VM erstellt haben, bevor Sie die VMDKs auf dieser VM wiederherstellen können.

> Aktivieren Sie die VMware-Anwendung vStorage API for Array Integration (VAAI), um die Leistung von Wiederherstellungsvorgängen in NFS-Umgebungen zu verbessern.

Informationen zu diesem Vorgang

Sie können einen Datenspeicher nicht wiederherstellen, aber Sie können jede VM im Datenspeicher wiederherstellen.

Ein Wiederherstellungsvorgang kann fehlschlagen, wenn die Speicherebene des FabricPool , in dem sich die VM befindet, nicht verfügbar ist.

Schritte

1. Navigieren Sie im vCenter Server zu **Inventar** > **Datenspeicher** und wählen Sie einen Datenspeicher aus.
2. Wählen Sie im Abschnitt „SnapCenter Plug-in for VMware vSphere“ die Option „Konfigurieren“ > „Backups“ aus.
3. Doppelklicken Sie auf ein Backup, um eine Liste aller VMs anzuzeigen, die im Backup enthalten sind.
4. Wählen Sie die gelöschte VM aus der Sicherungsliste aus und wählen Sie **Wiederherstellen**.
5. Wählen Sie im Assistenten **Wiederherstellen** auf der Seite **Sicherung auswählen** die Sicherungskopie aus, von der Sie wiederherstellen möchten.

   Sie können nach einem bestimmten Backup-Namen oder einem Teil des Backup-Namens suchen oder die Backup-Liste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Außerdem können Sie auswählen, ob Sie Backups mit VMware-Snapshots wünschen, ob Sie gemountete Backups wünschen und den Speicherort. Wählen Sie **OK**, um zum Assistenten zurückzukehren.

6. Wählen Sie auf der Seite **Bereich auswählen** im Feld **Wiederherstellungsbereich** die Option **Gesamte virtuelle Maschine** aus, wählen Sie dann den Wiederherstellungsort aus und geben Sie dann die Informationen zum Ziel-ESXi-Host ein, auf dem die Sicherung bereitgestellt werden soll.

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

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

7. Wählen Sie auf der Seite **Speicherort auswählen** den Speicherort der Sicherung aus, von der Sie wiederherstellen möchten (primär oder sekundär).
8. Überprüfen Sie die Seite „Zusammenfassung“ und wählen Sie dann **Fertig**.

Wiederherstellen von VMDKs aus Backups

Sie können vorhandene VMDKs oder gelöschte oder getrennte VMDKs entweder aus einem primären oder sekundären Backup herkömmlicher VMs oder vVol-VMs

wiederherstellen.

Sie können eine oder mehrere virtuelle Maschinenfestplatten (VMDKs) auf einer VM im selben Datenspeicher wiederherstellen.

> Aktivieren Sie die VMware-Anwendung vStorage API for Array Integration (VAAI), um die Leistung von Wiederherstellungsvorgängen in NFS-Umgebungen zu verbessern.

Bevor Sie beginnen

- Es muss ein Backup vorhanden sein.

  Sie müssen mit dem SnapCenter Plug-in for VMware vSphere ein Backup der VM erstellt haben.

- Die VM darf sich nicht im Transit befinden.

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

Informationen zu diesem Vorgang

- Wenn das VMDK gelöscht oder von der VM getrennt wird, wird das VMDK beim Wiederherstellungsvorgang an die VM angehängt.
- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn die Speicherebene des FabricPool , in dem sich die VM befindet, nicht verfügbar ist.
- Anfügen- und Wiederherstellungsvorgänge verbinden VMDKs mithilfe des Standard-SCSi-Controllers. Wenn jedoch VMDKs gesichert werden, die an eine VM mit einer NVMe-Festplatte angeschlossen sind, verwenden die Anfüge- und Wiederherstellungsvorgänge den NVMe-Controller, sofern verfügbar.

Schritte

1. Wählen Sie in der GUI 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 in der Dropdownliste „SnapCenter Plug-in for VMware vSphere“ und anschließend in der sekundären Dropdownliste „Wiederherstellen“ aus.
3. Wählen Sie im Assistenten **Wiederherstellen** auf der Seite „Sicherung auswählen“ die Sicherungskopie aus, von der Sie wiederherstellen möchten.

   Sie können nach einem bestimmten Backup-Namen oder einem Teil des Backup-Namens suchen oder die Backup-Liste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie aus, ob Sie Backups mit VMware-Snapshots wünschen, ob Sie gemountete Backups wünschen und ob es sich um einen primären oder sekundären Speicherort handelt. 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…
Der ursprüngliche Datenspeicher	Wählen Sie **Bestimmte Festplatte** aus der Dropdown-Liste und wählen Sie dann **Weiter**. In der Datastore-Auswahltabelle können Sie beliebige VMDKs auswählen oder die Auswahl aufheben.

Wiederherstellen auf…	Geben Sie das Wiederherstellungsziel an…
Ein alternativer Datenspeicher an einem alternativen Standort	Wählen Sie den Zieldatenspeicher und wählen Sie einen anderen Datenspeicher 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 Seite „Zusammenfassung“ und wählen Sie dann **Fertig**.
7. Optional: Überwachen Sie den Vorgangsfortschritt, indem Sie unten auf dem Bildschirm **Letzte Aufgaben** auswählen.
8. Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

Stellen Sie die neueste Sicherung der MySQL-Datenbank wieder her

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

Schritte

1. Öffnen Sie ein Wartungskonsolenfenster.

   "Zugriff auf die Wartungskonsole" .

2. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration** ein.
3. Geben Sie im Anwendungskonfigurationsmenü die Option **6) MySQL-Sicherung und -Wiederherstellung** ein.
4. Geben Sie im Konfigurationsmenü für MySQL-Backup und -Wiederherstellung die Option **4) MySQL-Backup wiederherstellen** ein.
5. Geben Sie bei der Eingabeaufforderung „Mit der aktuellsten Sicherung wiederherstellen“ **y** ein und drücken Sie dann die **Eingabetaste**.

   Die MySQL-Datenbanksicherung wird an ihrem ursprünglichen Speicherort wiederhergestellt.

Stellen Sie eine bestimmte Sicherung der MySQL-Datenbank wieder her

Sie können die Wartungskonsole verwenden, um eine bestimmte Sicherung der MySQL-Datenbank (auch NSM-Datenbank genannt) für das SnapCenter Plug-in for VMware vSphere Appliance wiederherzustellen.

Schritte

1. Öffnen Sie ein Wartungskonsolenfenster.

   "Zugriff auf die Wartungskonsole" .

2. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration** ein.

3. Geben Sie im Anwendungskonfigurationsmenü die Option **6) MySQL-Sicherung und -Wiederherstellung** ein.
4. Geben Sie im Konfigurationsmenü „MySQL-Backup und -Wiederherstellung“ die Option **2) MySQL-Backups auflisten** ein und notieren Sie sich dann das Backup, das Sie wiederherstellen möchten.
5. Geben Sie im Konfigurationsmenü für MySQL-Backup und -Wiederherstellung die Option **4) MySQL-Backup wiederherstellen** ein.
6. Geben Sie bei der Eingabeaufforderung „Mit der aktuellsten Sicherung wiederherstellen“ **n** ein.
7. Geben Sie bei der Eingabeaufforderung „Backup zum Wiederherstellen von“ den Backup-Namen ein und drücken Sie dann die Eingabetaste.

   Die ausgewählte MySQL-Sicherungsdatenbank wird an ihrem ursprünglichen Speicherort wiederhergestellt.

Anhängen und Trennen von VMDKs

VMDKs an eine VM oder vVol-VM anhängen

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 anhängen, der vom selben vCenter oder einem anderen vCenter im verknüpften Modus verwaltet wird. VMs in herkömmlichen Datenspeichern und in vVol-Datenspeichern werden unterstützt.

Dadurch ist es einfacher, eine oder mehrere einzelne Dateien von einem Laufwerk wiederherzustellen, anstatt das gesamte Laufwerk wiederherzustellen. Sie können das VMDK trennen, nachdem Sie die benötigten Dateien wiederhergestellt oder darauf zugegriffen haben.

Informationen zu diesem Vorgang

Sie haben folgende Anhängemöglichkeiten:

- Sie können virtuelle Datenträger aus einem primären oder sekundären Backup anhängen.
- Sie können virtuelle Datenträger an die übergeordnete VM (dieselbe VM, mit der der virtuelle Datenträger ursprünglich verknüpft war) oder an eine alternative VM auf demselben ESXi-Host anhängen.

Für das Anschließen virtueller Datenträger gelten die folgenden Einschränkungen:

- Anfüge- und Trennvorgänge werden für Vorlagen virtueller Maschinen nicht unterstützt.
- Wenn mehr als 15 VMDKs an einen iSCSI-Controller angeschlossen sind, kann die virtuelle Maschine für das SnapCenter Plug-in for VMware vSphere aufgrund von VMware-Einschränkungen keine VMDK-Einheitennummern über 15 finden.

  Fügen Sie in diesem Fall die SCSi-Controller manuell hinzu und versuchen Sie den Anschlussvorgang erneut.

- Sie können eine virtuelle Festplatte, die im Rahmen einer Gastdateiwiederherstellung angeschlossen oder gemountet wurde, nicht manuell anschließen.
- Anfügen- und Wiederherstellungsvorgänge verbinden VMDKs mithilfe des Standard-SCSi-Controllers. Wenn jedoch VMDKs gesichert werden, die an eine VM mit einer NVMe-Festplatte angeschlossen sind, verwenden die Anfüge- und Wiederherstellungsvorgänge den NVMe-Controller, sofern verfügbar.

Bevor Sie beginnen

Führen Sie die folgenden Schritte aus, um der Festplatte einen NVMe-Controller hinzuzufügen.

1. Melden Sie sich beim vCenter-Client an
2. Wählen Sie die VM aus dem VMFS-Datenspeicher 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“ aus.

Schritte

1. Wählen Sie in der GUI 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 for VMware vSphere* > **Virtuelle Festplatte(n) anhängen**.
3. Wählen Sie im Fenster **Virtuelle Festplatte anhängen** im Abschnitt **Backup** ein Backup aus.

   Sie können die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Außerdem können Sie auswählen, ob Sie Sicherungen mit VMware-Snapshots wünschen, ob Sie gemountete Sicherungen wünschen und den Speicherort. Wählen Sie **OK**.

4. Wählen Sie im Abschnitt **Datenträger auswählen** einen oder mehrere Datenträger aus, die Sie anschließen möchten, und den Speicherort (primär oder sekundär), von dem aus Sie die Verbindung herstellen möchten.

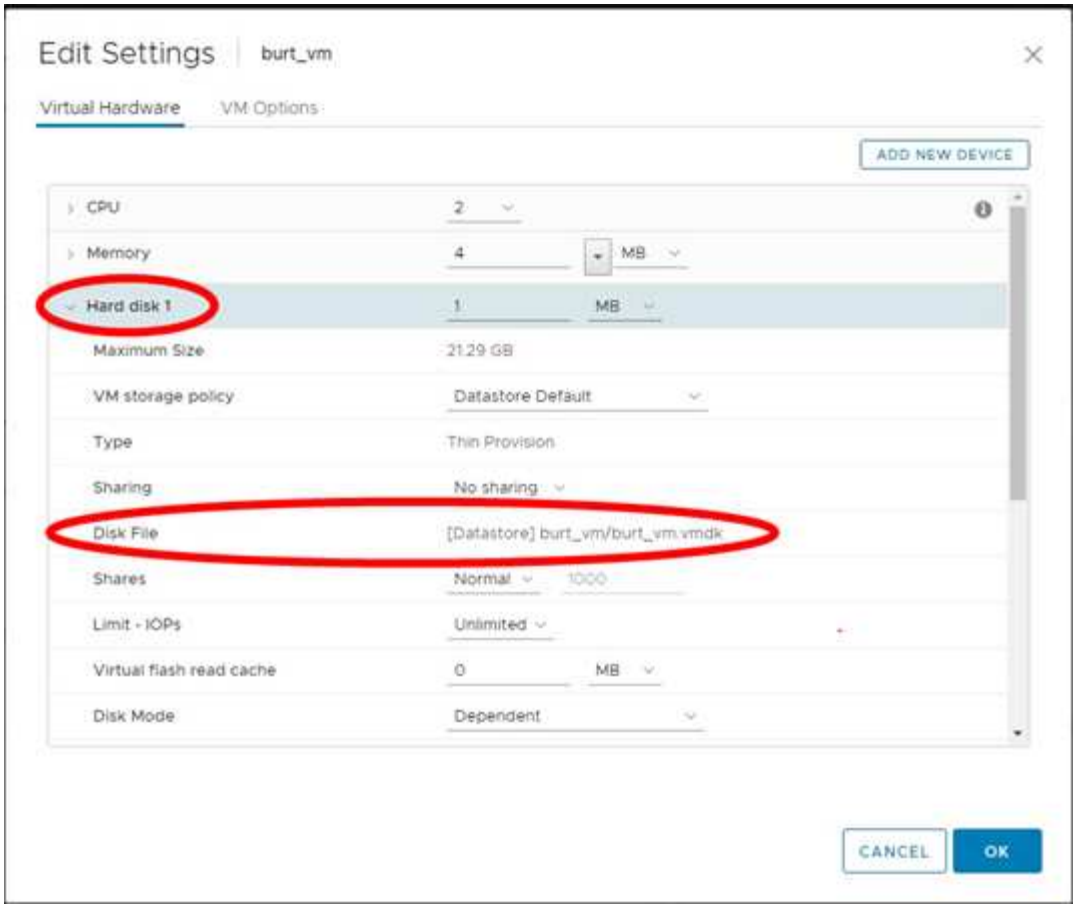
   Sie können den Filter ändern, um primäre und sekundäre Standorte anzuzeigen.

5. Standardmäßig werden die ausgewählten virtuellen Datenträger an die übergeordnete VM angeschlossen. Um die ausgewählten virtuellen Datenträger an eine alternative VM im selben ESXi-Host anzuhängen, wählen Sie **Klicken Sie hier, um eine Anbindung an eine alternative VM herzustellen** und geben Sie die alternative VM an.
6. Wählen Sie **Anhängen**.
7. Optional: Überwachen Sie den Vorgangsfortschritt im Abschnitt **Letzte Aufgaben**.

   Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

8. Überprüfen Sie, ob die virtuelle Festplatte angeschlossen ist, indem Sie die folgenden Schritte ausführen:

   a. Wählen Sie **Menü** in der Symbolleiste und wählen Sie dann **VMs und Vorlagen** aus der Dropdown-Liste.
   b. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM und wählen Sie dann in der Dropdownliste **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 aufgelistet. Sie können die Details für jede Festplatte erweitern, um die Liste der angeschlossenen virtuellen Festplatten anzuzeigen.

Ergebnis

Sie können vom Host-Betriebssystem aus auf die angeschlossenen Datenträger zugreifen und dann die benötigten Informationen von den Datenträgern abrufen.

Trennen einer virtuellen Festplatte

Nachdem Sie eine virtuelle Festplatte zum Wiederherstellen einzelner Dateien angeschlossen haben, können Sie die virtuelle Festplatte von der übergeordneten VM trennen.

Schritte

1. Wählen Sie in der GUI 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 in der Dropdownliste „SnapCenter Plug-in for VMware vSphere“ und dann in der sekundären Dropdownliste „Virtuelle Festplatte trennen“ aus.
4. Wählen Sie auf dem Bildschirm **Virtuelle Festplatte trennen** eine oder mehrere Festplatten aus, die Sie trennen möchten, aktivieren Sie dann das Kontrollkästchen **Ausgewählte Festplatte(n) trennen** und wählen Sie **TRENNEN**.

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

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

   Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

6. Überprüfen Sie, ob die virtuelle Festplatte getrennt ist, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie **Menü** in der Symbolleiste und wählen Sie dann **VMs und Vorlagen** aus der Dropdown-Liste.
   b. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM und wählen Sie dann in der Dropdownliste **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 aufgelistet. Sie können die Details für jede Festplatte erweitern, um die Liste der angeschlossenen virtuellen Festplatten anzuzeigen.

Wiederherstellen von Gastdateien und -ordnern

Arbeitsablauf, Voraussetzungen und Einschränkungen

Sie können Dateien oder Ordner von einer virtuellen Maschinenfestplatte (VMDK) auf einem Windows-Gastbetriebssystem wiederherstellen.

Workflow zur Gastwiederherstellung

Die Wiederherstellungsvorgänge des Gastbetriebssystems umfassen die folgenden Schritte:

1. Befestigen

   Schließen Sie eine virtuelle Festplatte an eine Gast-VM oder Proxy-VM an und starten Sie eine Gast-Dateiwiederherstellungssitzung.

2. Warten

   Warten Sie, bis der Anfügevorgang abgeschlossen ist, bevor Sie suchen und wiederherstellen können. Wenn der Anhang

   Der Vorgang wird abgeschlossen, eine Gastdatei-Wiederherstellungssitzung wird automatisch erstellt und eine E-Mail-Benachrichtigung wird

   gesendet.

3. Dateien oder Ordner auswählen

   Durchsuchen Sie das VMDK in der Gastdateiwiederherstellungssitzung und wählen Sie eine oder mehrere Dateien oder Ordner zur Wiederherstellung aus.

4. Wiederherstellen

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

Voraussetzungen für die Wiederherstellung von Gastdateien und -ordnern

Bevor Sie eine oder mehrere Dateien oder Ordner aus einem VMDK auf einem Windows-Gastbetriebssystem wiederherstellen, müssen Sie sich aller Anforderungen bewusst sein.

- VMware-Tools müssen installiert und ausgeführt werden.

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

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

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

- Die Anmeldeinformationen für die Ziel-VM müssen das integrierte Domänenadministratorkonto oder das integrierte lokale Administratorkonto angeben. Der Benutzername muss „Administrator“ sein. Bevor Sie den Wiederherstellungsvorgang starten, müssen die Anmeldeinformationen für die VM konfiguriert werden,

an die Sie die virtuelle Festplatte anschließen möchten. Die Anmeldeinformationen werden sowohl für den Anfügevorgang als auch für den nachfolgenden Wiederherstellungsvorgang benötigt. Arbeitsgruppenbenutzer 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 die Benutzerkontensteuerung auf der Gast-VM deaktivieren.

- Sie müssen den Sicherungs-Snapshot und das VMDK kennen, von dem die Wiederherstellung durchgeführt werden soll.

  Das SnapCenter Plug-in for VMware vSphere unterstützt nicht die Suche nach wiederherzustellenden Dateien oder Ordnern. Daher müssen Sie vor Beginn den Speicherort der Dateien oder Ordner in Bezug auf den Snapshot und das entsprechende VMDK kennen.

- Die anzuschließende virtuelle Festplatte muss sich in einem SnapCenter -Backup befinden.

  Die virtuelle Festplatte, die die Datei oder den Ordner enthält, die/den Sie wiederherstellen möchten, muss sich in einer VM-Sicherung befinden, die mit der virtuellen Appliance für das SnapCenter Plug-in for 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 anhängen möchten, muss die Proxy-VM konfiguriert werden, bevor der Anhänge- und Wiederherstellungsvorgang beginnt.

- Dateien mit Namen, die nicht aus dem englischen Alphabet stammen, müssen Sie in einem Verzeichnis und nicht als einzelne Datei wiederherstellen.

  Sie können Dateien mit nicht-alphabetischen Namen, wie etwa japanische Kanji, wiederherstellen, indem Sie das Verzeichnis wiederherstellen, in dem sich die Dateien befinden.

- 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 Interoperability Matrix Tool (IMT)" .

Einschränkungen bei der Wiederherstellung von Gastdateien

Bevor Sie eine Datei oder einen Ordner von einem Gastbetriebssystem wiederherstellen, sollten Sie sich darüber im Klaren sein, was die Funktion nicht unterstützt.

- Sie können dynamische Datenträgertypen nicht innerhalb eines Gastbetriebssystems wiederherstellen.
- Wenn Sie eine verschlüsselte Datei oder einen verschlüsselten Ordner wiederherstellen, bleibt das Verschlüsselungsattribut nicht erhalten. Sie können keine Dateien oder Ordner in einem verschlüsselten Ordner wiederherstellen.
- Auf der Seite „Gastdatei durchsuchen“ werden die versteckten Dateien und Ordner angezeigt, die Sie nicht filtern können.
- Eine Wiederherstellung von einem Linux-Gastbetriebssystem ist nicht möglich.

  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 Interoperability Matrix Tool (IMT)" .

- Sie können keine Wiederherstellung von einem NTFS-Dateisystem auf ein FAT-Dateisystem durchführen.

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

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

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

- Sie können keine Gastdateien von einer vVol-VM auf einem alternativen Host wiederherstellen.
- Sie können verschlüsselte Gastdateien nicht wiederherstellen.

Wiederherstellen von Gastdateien und -ordnern aus VMDKs

Sie können eine oder mehrere Dateien oder Ordner aus einem VMDK auf einem Windows-Gastbetriebssystem wiederherstellen.

Informationen zu diesem Vorgang

Standardmäßig ist die angeschlossene virtuelle Festplatte 24 Stunden lang verfügbar und wird dann automatisch getrennt. Sie können im Assistenten auswählen, dass die Sitzung nach Abschluss des Wiederherstellungsvorgangs automatisch gelöscht werden soll. Alternativ können Sie die Sitzung zur Wiederherstellung der Gastdatei jederzeit manuell löschen oder die Zeit auf der Seite **Gastkonfiguration** verlängern.

Die Leistung 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 kleiner Dateien kann im Vergleich zum Wiederherstellen einer kleinen Anzahl großer Dateien länger dauern als erwartet, wenn der wiederherzustellende Datensatz dieselbe Größe hat.

Auf einer VM kann gleichzeitig nur ein Anfüge- oder Wiederherstellungsvorgang ausgeführt werden. Sie können auf derselben VM keine parallelen Anfüge- oder Wiederherstellungsvorgänge ausführen.

Mit der Gastwiederherstellungsfunktion können Sie System- und versteckte 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 des Wiederherstellungsvorgangs bleiben die versteckten, System- und verschlüsselten Attribute von Gastdateien in der wiederhergestellten Datei nicht erhalten. Das Anzeigen oder Durchsuchen reservierter Partitionen kann zu einem Fehler führen.

Schritte

1. Wählen Sie im Verknüpfungsfenster des vSphere-Clients „Hosts und Cluster“ und wählen Sie eine VM aus.
2. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie * SnapCenter Plug-in for VMware vSphere* > **Guest File Restore**.
3. Geben Sie auf der Seite **Wiederherstellungsbereich** die Sicherung an, die die virtuelle Festplatte enthält, die Sie anhängen möchten, indem Sie wie folgt vorgehen:
   a. Wählen Sie in der Tabelle **Sicherungsname** die Sicherung aus, die die virtuelle Festplatte enthält, die Sie anhängen möchten.
   b. Wählen Sie in der **VMDK**-Tabelle die virtuelle Festplatte aus, die die Dateien oder Ordner enthält, die Sie wiederherstellen möchten.
   c. Wählen Sie in der Tabelle **Standorte** den primären oder sekundären Standort der virtuellen Festplatte aus, die Sie anschließen möchten.
4. Gehen Sie auf der Seite **Gästedetails** wie folgt vor.

   a. Wählen Sie, wo die virtuelle Festplatte angeschlossen werden soll:

Wählen Sie diese Option…	Wenn…
Gast-VM verwenden	Sie möchten die virtuelle Festplatte an die VM anhängen, auf die Sie vor dem Starten des Assistenten mit der rechten Maustaste geklickt haben, und dann die Anmeldeinformationen für die VM auswählen, auf die Sie mit der rechten Maustaste geklickt haben. Für die VM müssen bereits Anmeldeinformationen erstellt worden sein.
Verwenden Sie die Proxy-VM zur Gastdateiwiederherstellung	Sie möchten die virtuelle Festplatte an eine Proxy-VM anhängen und dann die Proxy-VM auswählen. Die Proxy-VM muss konfiguriert werden, bevor der Anfüge- und Wiederherstellungsvorgang beginnt.

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

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

   Aktivieren Sie diese Option, da die Wiederherstellung einer Gastdatei ein asynchroner Vorgang ist und es möglicherweise zu einer Zeitverzögerung kommt, bis eine Gastsitzung für Sie eingerichtet wird.

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

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

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

6. Warten Sie, bis der Anfügevorgang abgeschlossen ist.

   Sie können den Fortschritt des Vorgangs im Dashboard-Jobmonitor 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 for VMware vSphere* aus dem Verknüpfungsfenster des vSphere-Clients.
8. Wählen Sie im linken Navigationsbereich **Guest File Restore** > **Guest Configuration**.

   In der Tabelle „Gastsitzungsmonitor“ können Sie zusätzliche Informationen zu einer Sitzung anzeigen, indem Sie *… auswählen. *in der rechten Spalte.

9. Wählen Sie die Gastdateiwiederherstellungssitzung für die virtuelle Festplatte aus, die in der Benachrichtigungs-E-Mail aufgeführt war.

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

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

    Wenn Sie einen Ordner doppelt auswählen, um einzelne Dateien zu durchsuchen und auszuwählen, kann es beim Abrufen der Dateiliste zu einer Zeitverzögerung kommen, da der Abrufvorgang zur Laufzeit durchgeführt wird.

    Zum einfacheren Durchsuchen können Sie Filter in Ihrer Suchzeichenfolge verwenden. Die Filter sind case-sensitiv, Perl-Ausdrücke ohne Leerzeichen. Die Standardsuchzeichenfolge ist `.` *. Die folgende Tabelle zeigt einige Beispiele für Perl-Suchausdrücke.

Dieser Ausdruck…	Sucht nach…
.	Jedes Zeichen außer einem Zeilenumbruchzeichen.
.*	Beliebige Zeichenfolge. Dies ist die Standardeinstellung.
A	Das Zeichen a.
ab	Die Saite ab.
a [vertikaler Strich] b	Das Zeichen a oder b.
A*	Null oder mehr Instanzen des Zeichens a.
a+	Eine oder mehrere Instanzen des Zeichens a.
A?	Keine oder eine Instanz des Zeichens a.

Dieser Ausdruck…	Sucht nach…
Axt}	Genau x-maliges Vorkommen des Zeichens a.
Axt,}	Mindestens x Vorkommen des Zeichens a.
a{x,y}	Mindestens x Vorkommen des Zeichens a und höchstens y Vorkommen.
\	Entkommt einem Sonderzeichen.

Auf der Seite „Gastdatei durchsuchen“ werden neben allen anderen Dateien und Ordnern auch alle versteckten Dateien und Ordner angezeigt.

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

    Die wiederherzustellenden Dateien und Ordner werden in der Tabelle „Ausgewählte Datei(en)“ aufgelistet.

12. Geben Sie auf der Seite **Wiederherstellungsort auswählen** Folgendes an:

Option	Beschreibung
Auf Pfad wiederherstellen	Geben Sie den UNC-Freigabepfad zum Gast ein, auf dem die ausgewählten Dateien wiederhergestellt werden. Beispiel für eine IPv4-Adresse: `\\10.60.136.65\c$` Beispiel für eine IPv6-Adresse: `\\fd20-8b1e-b255-832e–61.ipv6-literal.net\C\restore`
Wenn Originaldatei(en) vorhanden sind	Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die wiederherzustellende Datei oder der wiederherzustellende Ordner bereits am 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, wenn die Gastdateiwiederherstellungssitzung nach Abschluss des Wiederherstellungsvorgangs gelöscht werden soll.

13. Wählen Sie **Wiederherstellen**.

    Sie können den Fortschritt des Wiederherstellungsvorgangs im Dashboard-Jobmonitor anzeigen oder auf die E-Mail-Benachrichtigung warten. Die Zeit, die zum Senden der E-Mail-Benachrichtigung benötigt wird, hängt von der Dauer des Wiederherstellungsvorgangs ab.

    Die Benachrichtigungs-E-Mail enthält einen Anhang mit der Ausgabe des Wiederherstellungsvorgangs. 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 Anhängen einer virtuellen Festplatte für Dateiwiederherstellungsvorgänge des Gasts verwenden möchten, müssen Sie die Proxy-VM einrichten, bevor Sie mit dem Wiederherstellungsvorgang beginnen. Obwohl Sie jederzeit eine Proxy-VM einrichten können, ist es möglicherweise bequemer, sie unmittelbar nach Abschluss der Plug-In-Bereitstellung einzurichten.

Schritte

1. Wählen Sie im Verknüpfungsfenster des vSphere-Clients unter Plug-Ins * SnapCenter Plug-in for VMware vSphere* aus.
2. Wählen Sie in der linken Navigation **Guest File Restore** aus.
3. Führen Sie im Abschnitt „Anmeldeinformationen für „Ausführen als““ einen der folgenden Schritte aus:

Um dies zu tun…	Mach das…
Vorhandene Anmeldeinformationen verwenden	Wählen Sie eine der konfigurierten Anmeldeinformationen aus.
Neue Anmeldeinformationen hinzufügen	a. Wählen Sie **Hinzufügen**. b. Geben Sie im Dialogfeld **Anmeldeinformationen für „Ausführen als“** die Anmeldeinformationen ein. c. Wählen Sie **VM auswählen** und wählen Sie dann im Dialogfeld **Proxy-VM** eine VM aus. Wählen Sie **Speichern**, um zum Dialogfeld **Anmeldeinformationen für „Ausführen als“** zurückzukehren. d. Geben Sie die Anmeldeinformationen ein. Als Benutzernamen müssen Sie „Administrator“ eingeben.

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

   Die Anmeldeinformationen für „Ausführen als“ müssen dem von Windows bereitgestellten Standarddomänenadministrator oder dem integrierten lokalen Administrator entsprechen. Arbeitsgruppenbenutzer können das integrierte lokale Administratorkonto verwenden.

4. Wählen Sie im Abschnitt **Proxy-Anmeldeinformationen** die Option **Hinzufügen** aus, um eine VM zur Verwendung als Proxy hinzuzufügen.
5. Vervollständigen Sie im Dialogfeld **Proxy-VM** die Informationen und wählen Sie dann **Speichern**.

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

Konfigurieren Sie Anmeldeinformationen für die Wiederherstellung von VM-Gastdateien

Wenn Sie eine virtuelle Festplatte für Datei- oder Ordnerwiederherstellungsvorgänge eines Gastes anhängen, müssen vor der Wiederherstellung die Anmeldeinformationen der Ziel-VM für den Anschluss konfiguriert sein.

Informationen zu diesem Vorgang

In der folgenden Tabelle sind die Anmeldeinformationsanforderungen für Gastwiederherstellungsvorgänge aufgeführt.

	Benutzerzugriffskontrolle aktiviert	**Benutzerzugriffskontrolle deaktiviert**
Domänenbenutzer	Ein Domänenbenutzer mit dem Benutzernamen „Administrator“ funktioniert einwandfrei. Beispiel: „NetApp\administrator“. Ein Domänenbenutzer mit dem Benutzernamen „xyz“, der zu einer lokalen Administratorgruppe gehört, funktioniert jedoch nicht. Beispielsweise können Sie „NetApp\xyz“ nicht verwenden.	Entweder ein Domänenbenutzer mit dem Benutzernamen „Administrator“ oder ein Domänenbenutzer mit dem Benutzernamen „xyz“, der zu einer lokalen Administratorgruppe gehört, funktioniert einwandfrei. Beispiel: „NetApp\administrator“ oder „NetApp\xyz“.
Arbeitsgruppenbenutzer	Ein lokaler Benutzer mit dem Benutzernamen „Administrator“ funktioniert einwandfrei. Ein lokaler Benutzer mit dem Benutzernamen „xyz“, der zu einer lokalen Administratorgruppe gehört, funktioniert jedoch nicht.	Entweder ein lokaler Benutzer mit dem Benutzernamen „Administrator“ oder ein lokaler Benutzer mit dem Benutzernamen „xyz“, der zu einer lokalen Administratorgruppe gehört, funktioniert einwandfrei. Ein lokaler Benutzer mit dem Benutzernamen „xyz“, der nicht zur lokalen Administratorgruppe gehört, funktioniert jedoch nicht.

In den vorhergehenden Beispielen ist „NetApp“ der Dummy-Domänenname und „xyz“ der Dummy-lokale Benutzername

Schritte

1. Wählen Sie im Verknüpfungsfenster des vSphere-Clients unter Plug-Ins * SnapCenter Plug-in for VMware vSphere* aus.
2. Wählen Sie in der linken Navigation **Guest File Restore** aus.
3. Führen Sie im Abschnitt „Anmeldeinformationen für „Ausführen als““ einen der folgenden Schritte aus:

Um dies zu tun…	**Mach das…**
Vorhandene Anmeldeinformationen verwenden	Wählen Sie eine der konfigurierten Anmeldeinformationen aus.

Um dies zu tun…	Mach das…
Neue Anmeldeinformationen hinzufügen	a. Wählen Sie **Hinzufügen**. b. Geben Sie im Dialogfeld **Anmeldeinformationen für „Ausführen als“** die Anmeldeinformationen ein. Als Benutzernamen müssen Sie „Administrator“ eingeben. c. Wählen Sie **VM auswählen** und wählen Sie dann im Dialogfeld **Proxy-VM** eine VM aus. Wählen Sie **Speichern**, um zum Dialogfeld **Anmeldeinformationen für „Ausführen als“** zurückzukehren. Wählen Sie die VM aus, die zur Authentifizierung der Anmeldeinformationen verwendet werden soll.

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

4. Wählen Sie **Speichern**.

Verlängern Sie die Dauer einer Gastdateiwiederherstellungssitzung

Standardmäßig ist eine angehängte Guest File Restore VMDK 24 Stunden lang verfügbar und wird dann automatisch getrennt. Sie können die Zeit auf der Seite **Gastkonfiguration** verlängern.

Informationen zu diesem Vorgang

Möglicherweise möchten Sie eine Gastdateiwiederherstellungssitzung verlängern, wenn Sie zu einem späteren Zeitpunkt zusätzliche Dateien oder Ordner aus dem angehängten VMDK wiederherstellen möchten. Da Gastdateiwiederherstellungssitzungen jedoch viele Ressourcen verbrauchen, sollte die Sitzungsdauer nur gelegentlich verlängert werden.

Schritte

1. Wählen Sie im VMware vSphere-Client **Guest File Restore** aus.
2. Wählen Sie eine Gastdateiwiederherstellungssitzung aus und wählen Sie dann das Symbol „Ausgewählte Gastsitzung erweitern“ in der Titelleiste des Gastsitzungsmonitors.

   Die Sitzung wird um weitere 24 Stunden verlängert.

Mögliche Szenarien zur Wiederherstellung von Gastdateien

Beim Versuch, eine Gastdatei wiederherzustellen, können die folgenden Szenarien auftreten.

Die Gastdateiwiederherstellungssitzung ist leer

Dieses Problem tritt auf, wenn Sie eine Gastdateiwiederherstellungssitzung erstellen und während diese Sitzung aktiv war, das Gastbetriebssystem neu gestartet wird. In diesem Fall bleiben VMDKs im Gastbetriebssystem möglicherweise offline. Wenn Sie versuchen, die Dateiwiederherstellungssitzung des Gasts zu durchsuchen, ist die Liste daher leer.

Um das Problem zu beheben, schalten Sie die VMDKs im Gastbetriebssystem manuell wieder online. Wenn die VMDKs online sind, zeigt die Dateiwiederherstellungssitzung des Gastes den richtigen Inhalt an.

Der Vorgang zum Anhängen der Festplatte beim Wiederherstellen der Gastdatei schlägt fehl

Dieses Problem tritt auf, wenn Sie einen Gastdateiwiederherstellungsvorgang starten, der Vorgang zum Anschließen der Festplatte jedoch fehlschlägt, obwohl VMware Tools ausgeführt wird und die Anmeldeinformationen des Gastbetriebssystems 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 VMware Tools-Windows-Dienst auf dem Gastbetriebssystem neu und versuchen Sie dann erneut, die Gastdatei wiederherzustellen.

Gast-E-Mail zeigt ?????? als Dateinamen

Dieses Problem tritt auf, wenn Sie die Funktion zur Dateiwiederherstellung des Gastes verwenden, um Dateien oder Ordner mit nicht-englischen Zeichen in den Namen wiederherzustellen, und in der E-Mail-Benachrichtigung „??????“ für die wiederhergestellten Dateinamen angezeigt wird. Im E-Mail-Anhang sind die Namen der wiederhergestellten Dateien und Ordner korrekt aufgeführt.

Sicherungen werden nicht getrennt, nachdem die Gastdateiwiederherstellungssitzung abgebrochen wurde

Dieses Problem tritt auf, wenn Sie einen Gastdateiwiederherstellungsvorgang aus einer VM-konsistenten Sicherung durchführen. Während die Gastdateiwiederherstellungssitzung aktiv ist, wird eine weitere VM-konsistente Sicherung für dieselbe VM durchgeführt. Wenn die Gastdateiwiederherstellungssitzung entweder manuell oder automatisch nach 24 Stunden getrennt wird, werden die Sicherungen für die Sitzung nicht getrennt.

Um das Problem zu beheben, trennen Sie die VMDKs, die an die aktive Gastdateiwiederherstellungssitzung angehängt waren, manuell.

Verwalten des SnapCenter Plug-in for VMware vSphere -Geräte

Starten Sie den VMware vSphere-Clientdienst neu

Wenn sich der SnapCenter VMware vSphere-Client nicht mehr richtig verhält, müssen Sie möglicherweise den Browser-Cache leeren. Wenn das Problem weiterhin besteht, starten Sie den Webclientdienst neu.

Starten Sie den VMware vSphere-Clientdienst in einem Linux vCenter neu

Bevor Sie beginnen

Sie müssen vCenter 7.0U1 oder höher ausführen.

Schritte

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

   ```
   shell
   ```

3. Stoppen Sie den Webclientdienst 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 nicht die Pakete VASA oder vCenter 7.x und höher.

5. Starten Sie den Webclientdienst mit dem folgenden HTML5-Befehl:

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

Zugriff auf die Wartungskonsole

Sie können Ihre Anwendungs-, System- und Netzwerkkonfigurationen mithilfe der Wartungskonsole für das SnapCenter Plug-in for VMware vSphere verwalten. Sie können Ihr Administratorkennwort und Ihr Wartungskennwort ändern, Supportpakete generieren und die Ferndiagnose starten.

Bevor Sie beginnen

Bevor Sie den SnapCenter Plug-in for VMware vSphere Dienst stoppen und neu starten, sollten Sie alle Zeitpläne aussetzen.

Informationen zu diesem Vorgang

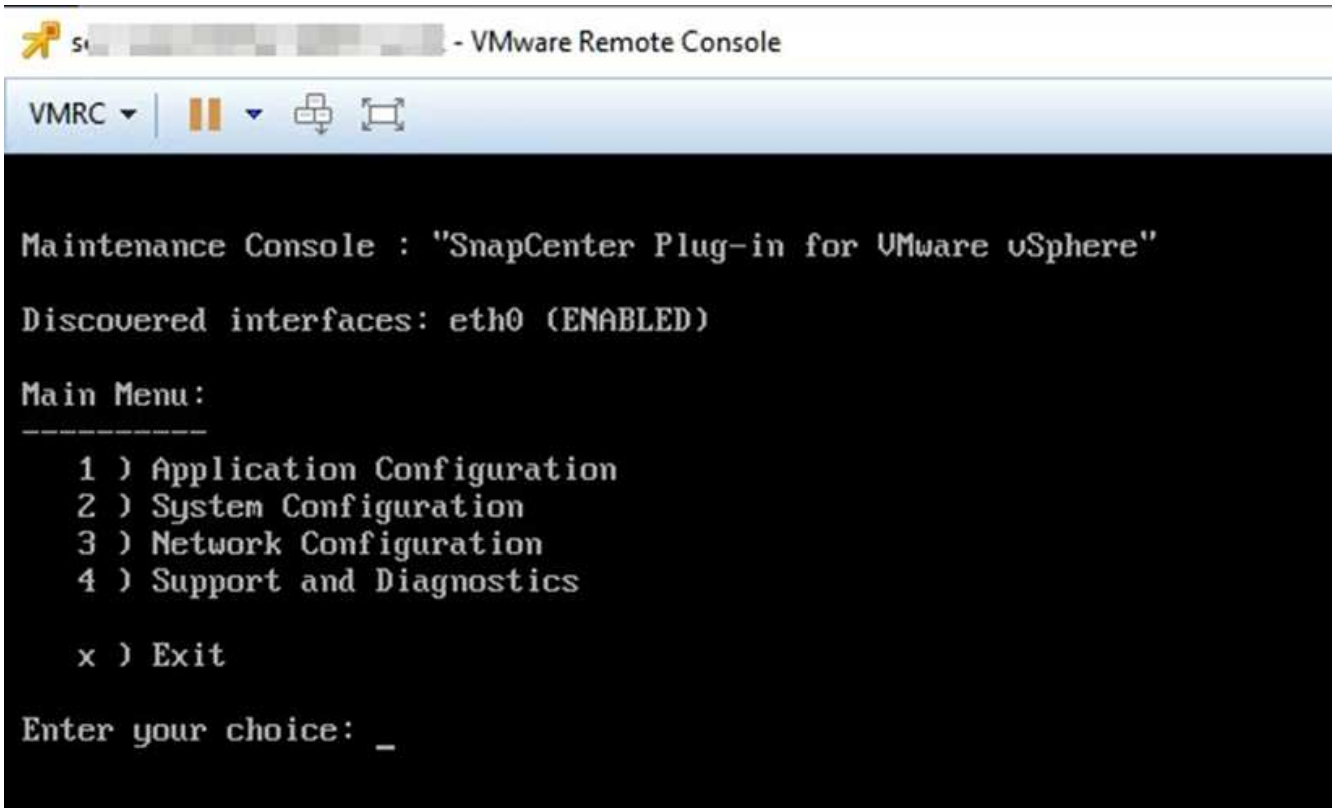
- Im SnapCenter Plug-in for VMware vSphere 4.6P1 müssen Sie bei der ersten Installation des SnapCenter Plug-in for VMware vSphere ein Kennwort angeben. Wenn Sie von Version 4.6 oder früher auf Version 4.6P1 oder höher aktualisieren, wird das frühere Standardkennwort akzeptiert.
- Sie müssen beim Aktivieren der Remotediagnose ein Kennwort für den Benutzer „diag“ festlegen.

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

Schritte

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

   Melden Sie sich mit dem Standardbenutzernamen der Wartungskonsole an `maint` und das Passwort, das Sie bei der Installation festgelegt haben.



3. Sie können die folgenden Vorgänge ausführen:

   - Option 1: Anwendungskonfiguration

     Eine Zusammenfassung des SnapCenter Plug-in for VMware vSphere anzeigen . SnapCenter Plug-in for VMware vSphere Dienst starten oder stoppen. Anmeldebenutzernamen oder -kennwort für SnapCenter Plug-in for VMware vSphere ändern. MySQL-Kennwort ändern. MySQL sichern und wiederherstellen, MySQL-Sicherungen konfigurieren und auflisten.

   - Option 2: Systemkonfiguration

Virtuelle Maschine neu starten Virtuelle Maschine herunterfahren Benutzerkennwort „maint“ ändern Zeitzone ändern NTP-Server ändern SSH-Zugriff aktivieren Jail-Festplattengröße erhöhen (/jail) Upgrade VMware Tools installieren MFA-Token generieren

> MFA ist immer aktiviert, Sie können MFA nicht deaktivieren.

- Option 3: Netzwerkkonfiguration

  IP-Adresseinstellungen anzeigen oder ändern Sucheinstellungen für Domänennamen anzeigen oder ändern Statische Routen anzeigen oder ändern Änderungen übernehmen Einen Host anpingen

- Option 4: Support und Diagnose

  Support-Paket generieren Auf Diagnose-Shell zugreifen Remote-Diagnosezugriff aktivieren Core-Dump-Paket generieren

Ändern Sie das Kennwort des SnapCenter Plug-in for VMware vSphere über die Wartungskonsole.

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

Bevor Sie beginnen

Bevor Sie den SnapCenter Plug-in for VMware vSphere stoppen und neu starten, sollten Sie alle Zeitpläne aussetzen.

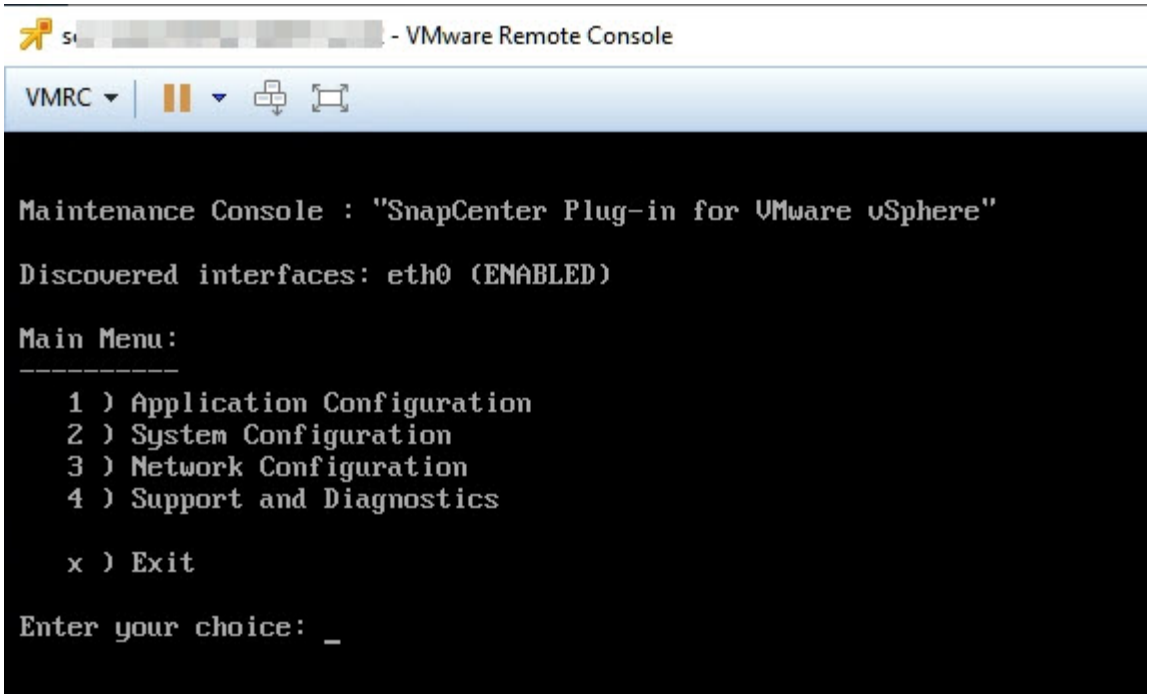
Informationen zu diesem Vorgang

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

Schritte

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

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



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

   Der virtuelle SnapCenter VMware-Appliance-Dienst wird gestoppt und neu gestartet.

Zertifikate erstellen und importieren

Das SnapCenter Plug-in for VMware vSphere verwendet SSL-Verschlüsselung für die sichere Kommunikation mit dem Client-Browser. Dadurch wird zwar die Verschlüsselung von Daten über die Leitung ermöglicht, durch die Erstellung eines neuen selbstsignierten Zertifikats oder die Verwendung Ihrer eigenen Zertifizierungsstelleninfrastruktur (CA) oder einer Zertifizierungsstelle eines Drittanbieters wird jedoch sichergestellt, dass das Zertifikat für Ihre Umgebung eindeutig ist.

Siehe "KB-Artikel: So erstellen und/oder importieren Sie ein SSL-Zertifikat in das SnapCenter Plug-in for VMware vSphere" für weitere Informationen.

Aufheben der Registrierung des SnapCenter Plug-in for VMware vSphere bei vCenter

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

Sie müssen die Registrierung des SnapCenter Plug-in for VMware vSphere Erweiterungen manuell aufheben.

Schritte

1. Navigieren Sie im verknüpften vCenter, bei dem der Dienst SnapCenter Plug-in for VMware vSphere gestoppt ist, zum Managed Object Reference (MOB)-Manager.
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**“, um eine Liste der registrierten Erweiterungen anzuzeigen.
3. Aufheben der Registrierung der Erweiterungen `com.netapp.scv.client` Und `com.netapp.aegis` .

Deaktivieren und Aktivieren des SnapCenter Plug-in for VMware vSphere

Wenn Sie die Datenschutzfunktionen von SnapCenter nicht mehr benötigen, müssen Sie die Konfiguration des SnapCenter Plug-in for VMware vSphere ändern. Wenn Sie das Plug-In beispielsweise in einer Testumgebung bereitgestellt haben, müssen Sie möglicherweise die SnapCenter -Funktionen in dieser Umgebung deaktivieren und in einer Produktionsumgebung aktivieren.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Wenn Sie das SnapCenter Plug-in for VMware vSphere deaktivieren, werden alle Ressourcengruppen angehalten und die Registrierung des Plug-ins als Erweiterung in vCenter aufgehoben.

Wenn Sie das SnapCenter Plug-in for 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 for VMware vSphere MySQL-Repository, falls Sie es auf einer neuen virtuellen Appliance wiederherstellen möchten.

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

2. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Management GUI mit dem 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-in for VMware vSphere wird angezeigt, wenn Sie das Plug-in bereitstellen.

3. Wählen Sie im linken Navigationsbereich **Konfiguration** aus und deaktivieren Sie dann die Option „Dienst“ im Abschnitt **Plug-in-Details**, um das Plug-in zu deaktivieren.
4. Bestätigen Sie Ihre Auswahl.
   - Wenn Sie nur das SnapCenter Plug-in for VMware vSphere verwendet haben, um VM-konsistente Backups durchzuführen

     Das Plug-In ist deaktiviert und es sind keine weiteren Maßnahmen erforderlich.

- Wenn Sie das SnapCenter Plug-in for VMware vSphere verwendet haben, um anwendungskonsistente Backups durchzuführen

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

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

Entfernen Sie das SnapCenter Plug-in for VMware vSphere

Wenn Sie die Datenschutzfunktionen von SnapCenter nicht mehr benötigen, müssen Sie das SnapCenter Plug-in for VMware vSphere deaktivieren, um es von vCenter abzumelden. Anschließend müssen Sie das SnapCenter Plug-in for VMware vSphere von vCenter entfernen und anschließend 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 Management GUI mit dem Format `https://<OVA-IP-address>:8080`.

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

2. Wählen Sie im linken Navigationsbereich **Konfiguration** aus und deaktivieren Sie dann die Option „Dienst“ im Abschnitt **Plug-in-Details**, um das Plug-in zu deaktivieren.
3. Melden Sie sich bei VMware vSphere an.
4. Klicken Sie im linken Navigator-Bildschirm mit der rechten Maustaste auf die Instanz des SnapCenter Plug-in for VMware vSphere (der Name des `.tar` Datei, die bei der Bereitstellung der virtuellen Appliance verwendet wurde) und wählen Sie **Von Festplatte löschen**.
5. Wenn Sie das SnapCenter Plug-in for VMware vSphere verwendet haben, um andere SnapCenter -Plug -ins für anwendungskonsistente Sicherungen zu unterstützen, melden Sie sich bei SnapCenter an und entfernen Sie den vSphere-Host.

Nach Abschluss

Die virtuelle Appliance ist weiterhin bereitgestellt, aber das SnapCenter Plug-in for VMware vSphere wurde entfernt.

Nach dem Entfernen der Host-VM für das SnapCenter Plug-in for VMware vSphere bleibt das Plug-In möglicherweise in vCenter aufgeführt, bis der lokale vCenter-Cache aktualisiert wird. Da das Plug-In jedoch entfernt wurde, können auf diesem Host keine SnapCenter VMware vSphere-Vorgänge ausgeführt werden. Wenn Sie den lokalen vCenter-Cache aktualisieren möchten, stellen Sie zunächst sicher, dass sich das Gerät auf der Konfigurationsseite des SnapCenter Plug-in for VMware vSphere im deaktivierten Zustand befindet,

und starten Sie dann den vCenter-Webclientdienst neu.

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

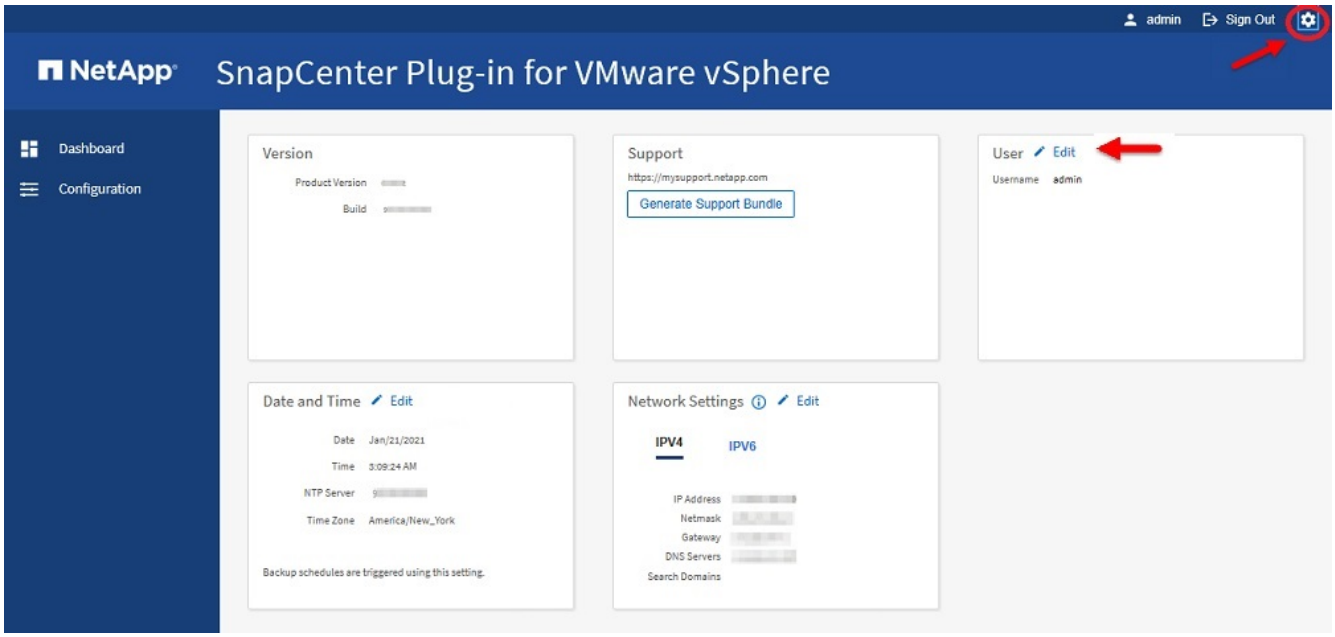
- Die IP-Adresse wurde angezeigt, als das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde.
- Verwenden Sie die Anmeldeinformationen, die Sie während der Bereitstellung des SnapCenter Plug-in for VMware vSphere erhalten haben oder die später geändert wurden.
- Generieren Sie mithilfe der Systemkonfigurationsoptionen der Wartungskonsole ein 6-stelliges MFA-Token.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI 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** die Option **Bearbeiten** aus.
4. Wählen Sie die neue Zeitzone aus und wählen Sie **Speichern**.

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

Ändern der Anmeldeinformationen

Sie können die Anmeldeinformationen für das SnapCenter Plug-in for VMware vSphere

Verwaltungs-GUI ändern.

Bevor Sie beginnen

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

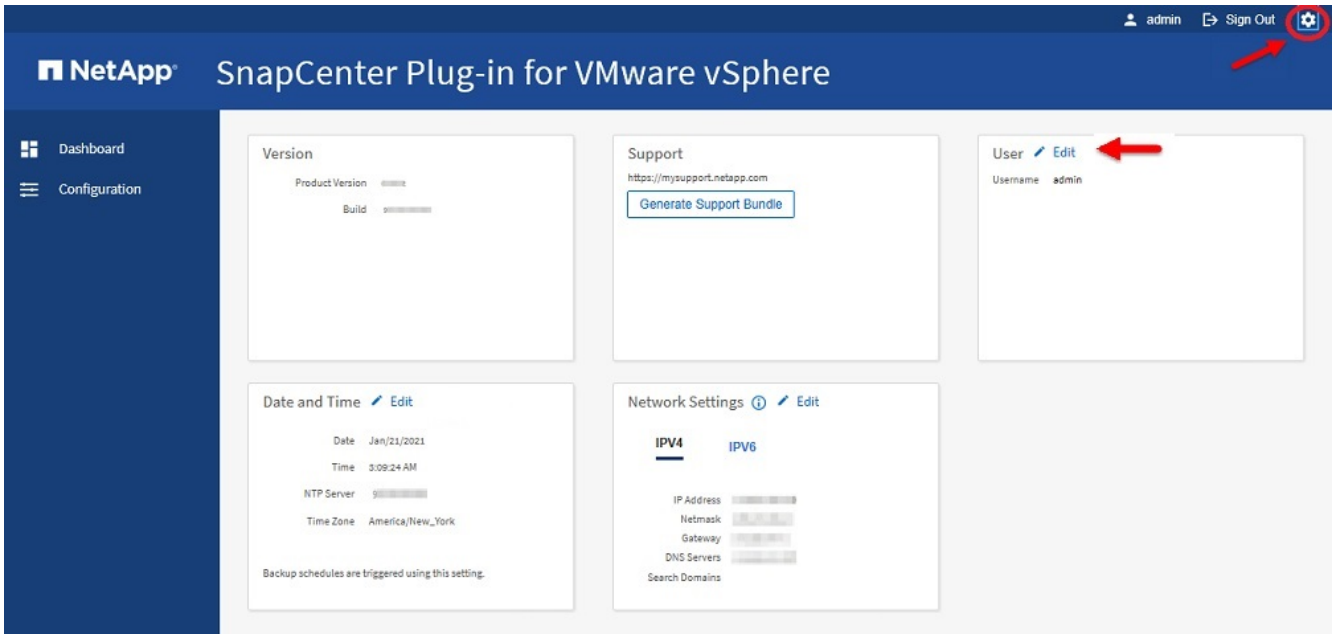
- Die IP-Adresse wurde angezeigt, als das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde.
- Verwenden Sie die Anmeldeinformationen, die Sie während der Bereitstellung des SnapCenter Plug-in for VMware vSphere erhalten haben oder die später geändert wurden.
- Generieren Sie mithilfe der Systemkonfigurationsoptionen der Wartungskonsole ein 6-stelliges MFA-Token.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI 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** die Option **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 der vCenter-Anmeldeinformationen

Sie können die vCenter-Anmeldeinformationen ändern, die im SnapCenter Plug-in for VMware vSphere konfiguriert sind. Diese Einstellungen werden vom Plug-In für den Zugriff auf vCenter verwendet. Wenn Sie das vCenter-Kennwort ändern, müssen Sie die Registrierung der ONTAP tools for VMware vSphere aufheben und sie mit dem neuen Kennwort erneut registrieren, damit die vVol-Backups reibungslos funktionieren.

Bevor Sie beginnen

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

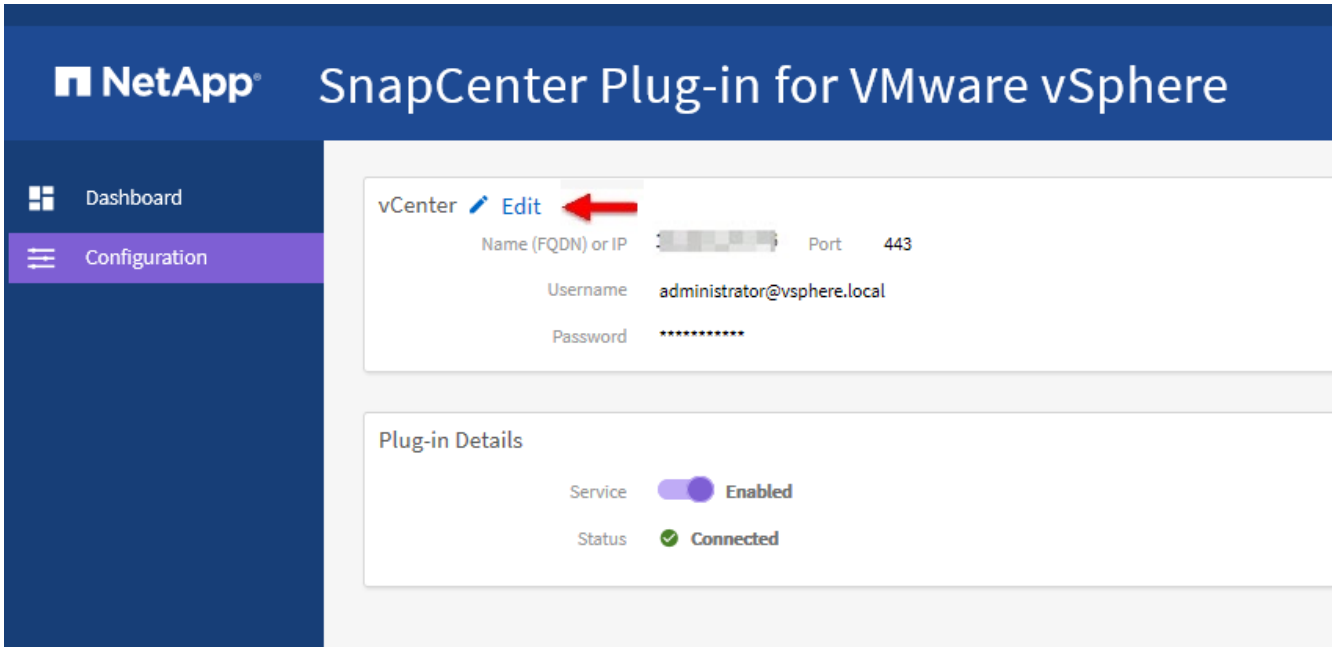
- Die IP-Adresse wurde angezeigt, als das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde.
- Verwenden Sie die Anmeldeinformationen, die Sie während der Bereitstellung des SnapCenter Plug-in for VMware vSphere erhalten haben oder die später geändert wurden.
- Generieren Sie mithilfe der Systemkonfigurationsoptionen der Wartungskonsole ein 6-stelliges MFA-Token.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI 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** die Option **Bearbeiten** aus.
4. Geben Sie das neue Passwort ein und wählen Sie anschließend **Speichern**.

   Ändern Sie die Portnummer nicht.

Ändern Sie die Netzwerkeinstellungen

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

Bevor Sie beginnen

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

notieren.

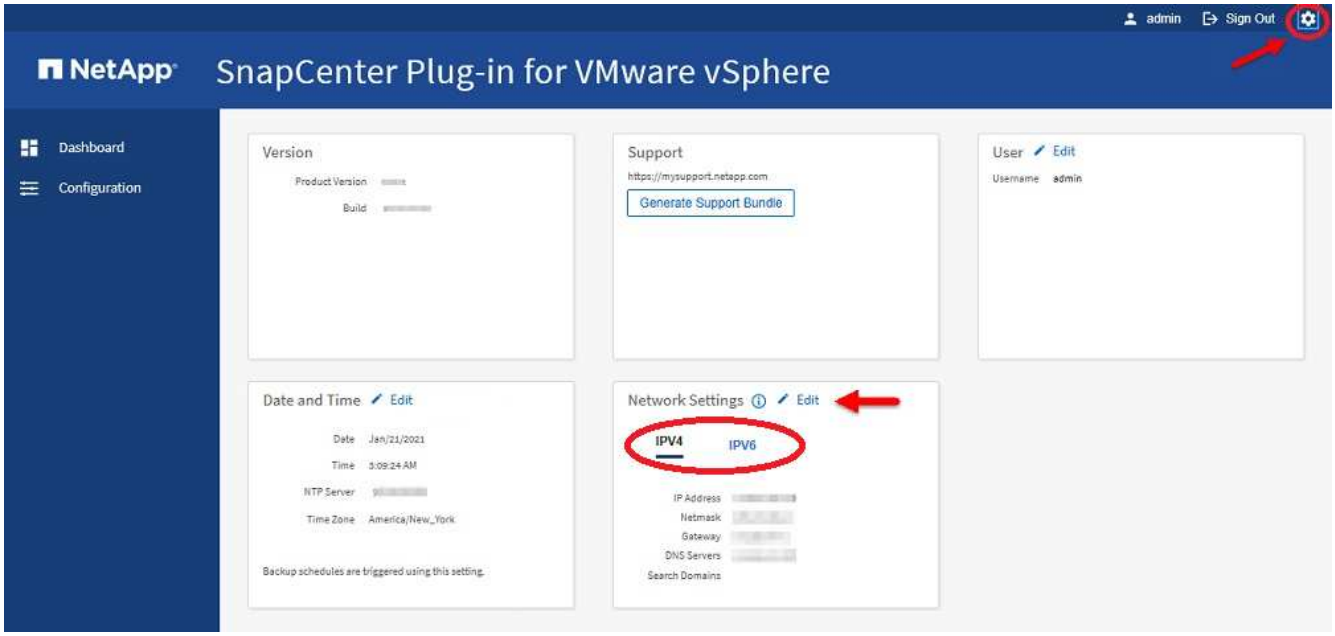
- Die IP-Adresse wurde angezeigt, als das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde.
- Verwenden Sie die Anmeldeinformationen, die Sie während der Bereitstellung des SnapCenter Plug-in for VMware vSphere erhalten haben oder die später geändert wurden.
- Generieren Sie mithilfe der Systemkonfigurationsoptionen der Wartungskonsole ein 6-stelliges MFA-Token.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI 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 **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** Folgendes ein: `: :0` und wählen Sie dann **Speichern**.

> Wenn Sie sowohl IPv4- als auch IPv6-Adressen verwenden, können Sie nicht beide Netzwerkeinstellungen entfernen. Das verbleibende Netzwerk muss die Felder „DNS-Server“ und „Suchdomänen“ angeben.

Ändern der Konfigurationsstandardwerte

Um die Betriebseffizienz zu verbessern, können Sie die `scbr.override` Konfigurationsdatei, um Standardwerte zu ändern. Diese Werte steuern Einstellungen

wie die Anzahl der VMware-Snapshots, die während einer Sicherung erstellt oder gelöscht werden, oder die Zeitspanne, bis die Ausführung eines Sicherungsskripts beendet wird.

Der `scbr.override` Die Konfigurationsdatei wird vom SnapCenter Plug-in for VMware vSphere in Umgebungen verwendet, die anwendungsbasierte Datenschutzvorgänge 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` Die Konfigurationsdatei wird vom SnapCenter Plug-in for VMware vSphere in Umgebungen verwendet, die anwendungsbasierte Datenschutzvorgänge von SnapCenter unterstützen.

1. Gehe zu `/opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.override-template` .
2. Kopieren Sie die `scbr.override-template` Datei in eine neue Datei mit dem Namen `scbr.override` im `\opt\netapp\scvservice\standalone_aegis\etc\scbr` Verzeichnis.

Eigenschaften, die Sie überschreiben können

Sie können Eigenschaften verwenden, die in der `scbr.override` Konfigurationsdatei, um Standardwerte zu ändern.

- Standardmäßig verwendet die Vorlage ein Rautesymbol, um die Konfigurationseigenschaften zu kommentieren. Um eine Eigenschaft zum Ändern eines Konfigurationswerts zu verwenden, müssen Sie die `#` Zeichen.
- Sie müssen den Dienst auf dem SnapCenter Plug-in for VMware vSphere Host neu starten, damit die Änderungen wirksam werden.

Sie können die folgenden Eigenschaften verwenden, die in der `scbr.override` Konfigurationsdatei, um Standardwerte zu ändern.

- **dashboard.protected.vm.count.interval=7**

  Gibt die Anzahl der Tage an, für die das Dashboard den VM-Schutzstatus anzeigt.

  Der Standardwert ist „7“.

- **disable.weakCiphers=true**

  Deaktiviert die folgenden schwachen Verschlüsselungen für den Kommunikationskanal zwischen SnapCenter Plug-in for VMware vSphere und SnapCenter sowie alle weiteren schwachen Verschlüsselungen, die in aufgeführt sind `include.weakCiphers` : TLS_RSA_MIT_AES_256_CBC_SHA256 TLS_DHE_RSA_MIT_AES_256_CBC_SHA256 TLS_RSA_MIT_AES_128_CBC_SHA256 TLS_DHE_RSA_MIT_AES_128_CBC_SHA256 TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384 TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256 TLS_RSA_MIT_AES_128_GCM_SHA256 TLS_RSA_MIT_AES_256_GCM_SHA384

- **global.ds.exclusion.pattern**

Gibt einen oder mehrere herkömmliche oder vVol-Datenspeicher an, die von Sicherungsvorgängen ausgeschlossen werden sollen. Sie können die Datenspeicher mit jedem gültigen regulären Java-Ausdruck angeben.

Beispiel 1: Der Ausdruck `global.ds.exclusion.pattern=.*21` schließt Datenspeicher aus, die ein gemeinsames Muster aufweisen; zum Beispiel `datastore21` Und `dstest21` wäre ausgeschlossen.

Beispiel 2: Der Ausdruck `global.ds.exclusion.pattern=ds-.*|^vol123` schließt alle Datenspeicher aus, die `ds-` (Zum Beispiel `scvds-test`) oder beginnen Sie mit `vol123` .

- **guestFileRestore.guest.operation.interval=5**

  Gibt das Zeitintervall in Sekunden an, in dem das SnapCenter Plug-in for VMware vSphere die Fertigstellung von Gastvorgängen auf dem Gast (Online-Datenträger und Wiederherstellungsdateien) überwacht. Die Gesamtwartezeit wird festgelegt durch `guestFileRestore.online.disk.timeout` Und `guestFileRestore.restore.files.timeout` .

  Der Standardwert ist „5“.

- **guestFileRestore.monitorInterval=30**

  Gibt das Zeitintervall in Minuten an, in dem das SnapCenter Plug-in for VMware vSphere auf abgelaufene Gastdateiwiederherstellungssitzungen überwacht. Jede Sitzung, die über die konfigurierte Sitzungszeit hinaus läuft, wird getrennt.

  Der Standardwert ist „30“.

- **guestFileRestore.online.disk.timeout=100**

  Gibt die Zeit in Sekunden an, die das SnapCenter Plug-in for VMware vSphere auf den Abschluss eines Online-Festplattenvorgangs auf einer Gast-VM wartet. Beachten Sie, dass eine zusätzliche Wartezeit von 30 Sekunden besteht, bevor das Plug-In die Fertigstellung des Online-Festplattenvorgangs abfragt.

  Der Standardwert ist „100“.

- **guestFileRestore.restore.files.timeout=3600**

  Gibt die Zeit in Sekunden an, die das SnapCenter Plug-in for VMware vSphere auf den Abschluss eines Vorgangs zum Wiederherstellen von Dateien auf einer Gast-VM wartet. Bei Überschreitung der Zeit wird der Vorgang beendet und der Auftrag als fehlgeschlagen markiert.

  Der Standardwert ist „3600“ (1 Stunde).

- **guestFileRestore.robocopy.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` da dies die Analyse der Wiederherstellungsausgabe unterbricht.

  Erlauben Sie keine unbegrenzten Wiederholungsversuche (durch Entfernen der `/R` Flag), da dies zu endlosen Wiederholungsversuchen für fehlgeschlagene Kopien führen kann.

  Die Standardwerte sind `"/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP"` .

- **guestFileRestore.robocopy.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 Dateiwiederherstellungsvorgängen des Gasts verwendet werden sollen.

  Nicht entfernen `/NJH` oder hinzufügen `/NJS` da dies die Analyse der Wiederherstellungsausgabe unterbricht.

  Erlauben Sie keine unbegrenzten Wiederholungsversuche (durch Entfernen der `/R` Flag), da dies zu endlosen Wiederholungsversuchen 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, die das SnapCenter Plug-in for VMware vSphere eine Gastdateiwiederherstellungssitzung aktiv hält.

  Der Standardwert ist „1440“ (24 Stunden).

- **guestFileRestore.use.custom.online.disk.script=true**

  Gibt an, ob beim Erstellen von Gastdateiwiederherstellungssitzungen ein benutzerdefiniertes Skript zum Online-Schalten von Datenträgern und Abrufen von Laufwerksbuchstaben verwendet werden soll. Das Skript muss sich unter folgendem Pfad befinden: `[Install Path] \etc\guestFileRestore_onlineDisk.ps1`. Mit der Installation wird ein Standardskript bereitgestellt. Die Werte `[Disk_Serial_Number]`, `[Online_Disk_Output]`, Und `[Drive_Output]` werden im Skript während des Anfügevorgangs ersetzt.

  Der Standardwert ist „false“.

- **include.esx.initiator.id.from.cluster=true**

  Gibt an, dass das SnapCenter Plug-in for VMware vSphere iSCSI- und FCP-Initiator-IDs von allen ESXi-Hosts im Cluster in die Anwendung über VMDK-Workflows einbeziehen soll.

  Der Standardwert ist „false“.

- **include.weakCiphers**

  Wann `disable.weakCiphers` ist eingestellt auf `true`, gibt die schwachen Chiffren an, die Sie deaktivieren möchten, zusätzlich zu den schwachen Chiffren, die `disable.weakCiphers` ist standardmäßig deaktiviert.

- **max.concurrent.ds.storage.query.count=15**

  Gibt die maximale Anzahl gleichzeitiger Aufrufe an, die das SnapCenter Plug-in for VMware vSphere an den SnapCenter -Server senden kann, um den Speicherbedarf für die Datenspeicher zu ermitteln. Das Plug-In führt diese Aufrufe durch, wenn Sie den Linux-Dienst auf dem SnapCenter Plug-in for VMware vSphere VM-Host neu starten.

- **nfs.datastore.mount.retry.count=3**

  Gibt die maximale Anzahl von Versuchen des SnapCenter Plug-in for VMware vSphere an, ein Volume als NFS-Datenspeicher in vCenter bereitzustellen.

Der Standardwert ist „3“.

- **nfs.datastore.mount.retry.delay=60000**

  Gibt die Zeit in Millisekunden an, die das SnapCenter Plug-in for VMware vSphere zwischen den Versuchen wartet, ein Volume als NFS-Datenspeicher in vCenter bereitzustellen.

  Der Standardwert ist „60000“ (60 Sekunden).

- **script.virtual.machine.count.variable.name= VIRTUELLE_MASCHINEN**

  Gibt den Namen der Umgebungsvariablen an, die die Anzahl der virtuellen Maschinen enthält. Sie müssen die Variable definieren, bevor Sie während eines Sicherungsauftrags benutzerdefinierte Skripts ausführen.

  Beispielsweise bedeutet VIRTUAL_MACHINES=2, dass zwei virtuelle Maschinen gesichert werden.

- **script.virtual.machine.info.variable.name=VIRTUELLE_MASCHINE.%s**

  Gibt den Namen der Umgebungsvariablen an, die Informationen zur n-ten virtuellen 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|%s|%s|%s|%s**

  Bietet Informationen zur virtuellen Maschine. Das Format für diese Informationen, das in der Umgebungsvariablen festgelegt wird, ist das folgende: `VM name|VM UUID| VM power state (on|off)|VM snapshot taken (true|false)|IP address(es)`

  Nachfolgend finden Sie ein Beispiel für die Informationen, die Sie angeben könnten:

  ```
  VIRTUAL_MACHINE.2=VM 1|564d6769-f07d-6e3b-
  68b1f3c29ba03a9a|POWERED_ON||true|10.0.4.2
  ```

- **storage.connection.timeout=600000**

  Gibt die Zeit in Millisekunden an, die der SnapCenter -Server auf eine Antwort vom Speichersystem wartet.

  Der Standardwert ist „600000“ (10 Minuten).

- **vmware.esx.ip.kernel.ip.map**

  Es gibt keinen Standardwert. Sie verwenden diesen Wert, um die IP-Adresse des ESXi-Hosts der IP-Adresse des VMkernels zuzuordnen. Standardmäßig verwendet das SnapCenter Plug-in for VMware vSphere die IP-Adresse des Verwaltungs-VMkernel-Adapters des ESXi-Hosts. Wenn das SnapCenter Plug-in for VMware vSphere eine andere IP-Adresse des VMkernel-Adapters verwenden soll, müssen Sie einen Überschreibungswert angeben.

  Im folgenden Beispiel lautet die IP-Adresse des Verwaltungsadapters für VMkernel 10.225.10.56. Das SnapCenter Plug-in for VMware vSphere verwendet jedoch die angegebenen Adressen 10.225.11.57 und 10.225.11.58. Und wenn die IP-Adresse des Verwaltungs-VMkernel-Adapters 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 for VMware vSphere auf dem Server ausführt.

  Diese Zahl wird pro Datenspeicher geprüft und nur, wenn in der Richtlinie „VM-konsistent“ ausgewählt ist. Wenn Sie absturzkonsistente Sicherungen durchführen, gilt diese Einstellung nicht.

  Der Standardwert ist „30“.

- **vmware.max.concurrent.snapshots.delete=30**

  Gibt die maximale Anzahl gleichzeitiger VMware-Snapshot-Löschvorgänge pro Datenspeicher an, die das SnapCenter Plug-in for VMware vSphere auf dem Server ausführt.

  Diese Zahl wird für jeden Datenspeicher einzeln überprüft.

  Der Standardwert ist „30“.

- **vmware.query.unresolved.retry.count=10**

  Gibt die maximale Anzahl von Wiederholungsversuchen des SnapCenter Plug-in for VMware vSphere an, eine Abfrage zu nicht aufgelösten Volumes aufgrund von „…Zeitlimit für das Zurückhalten von E/A…“-Fehlern zu senden.

  Der Standardwert ist „10“.

- **vmware.quiesce.retry.count=0**

  Gibt die maximale Anzahl von Wiederholungsversuchen des SnapCenter Plug-in for VMware vSphere an, eine Abfrage zu VMware-Snapshots zu senden, weil während einer Sicherung „…Zeitlimit für das Zurückhalten von E/A…“-Fehlern aufgetreten sind.

  Der Standardwert ist „0“.

- **vmware.quiesce.retry.interval=5**

  Gibt die Zeitspanne in Sekunden an, die das SnapCenter Plug-in for VMware vSphere zwischen dem Senden der Abfragen bezüglich VMware-Snapshot-Fehlern „…Zeitlimit für das Zurückhalten von E/A…“ während einer Sicherung wartet.

  Der Standardwert ist „5“.

- **vmware.query.unresolved.retry.delay= 60000**

  Gibt die Zeitspanne in Millisekunden an, die das SnapCenter Plug-in for VMware vSphere zwischen dem Senden der Abfragen bezüglich nicht aufgelöster Volumes aufgrund von „…Zeitlimit für das Zurückhalten von E/A…“-Fehlern wartet. Dieser Fehler tritt beim Klonen eines VMFS-Datenspeichers auf.

  Der Standardwert ist „60000“ (60 Sekunden).

- **vmware.reconfig.vm.retry.count=10**

Gibt die maximale Anzahl von Wiederholungsversuchen des SnapCenter Plug-in for VMware vSphere an, eine Abfrage zum Neukonfigurieren einer VM aufgrund von „…Zeitlimit für das Zurückhalten von E/A…“-Fehlern zu senden.

Der Standardwert ist „10“.

- **vmware.reconfig.vm.retry.delay=30000**

  Gibt die maximale Zeit in Millisekunden an, die das SnapCenter Plug-in for VMware vSphere zwischen dem Senden von Abfragen zur Neukonfiguration einer VM aufgrund von „…Zeitlimit für das Zurückhalten von E/A…“-Fehlern wartet.

  Der Standardwert ist „30000“ (30 Sekunden).

- **vmware.rescan.hba.retry.count=3**

  Gibt die Zeitspanne in Millisekunden an, die das SnapCenter Plug-in for VMware vSphere zwischen dem Senden der Abfragen zum erneuten Scannen des Hostbusadapters aufgrund von „…Zeitlimit für das Zurückhalten von E/A…“-Fehlern wartet.

  Der Standardwert ist „3“.

- **vmware.rescan.hba.retry.delay=30000**

  Gibt die maximale Anzahl von Wiederholungsversuchen des SnapCenter Plug-in for VMware vSphere zum erneuten Scannen des Hostbusadapters an.

  Der Standardwert ist „30000“.

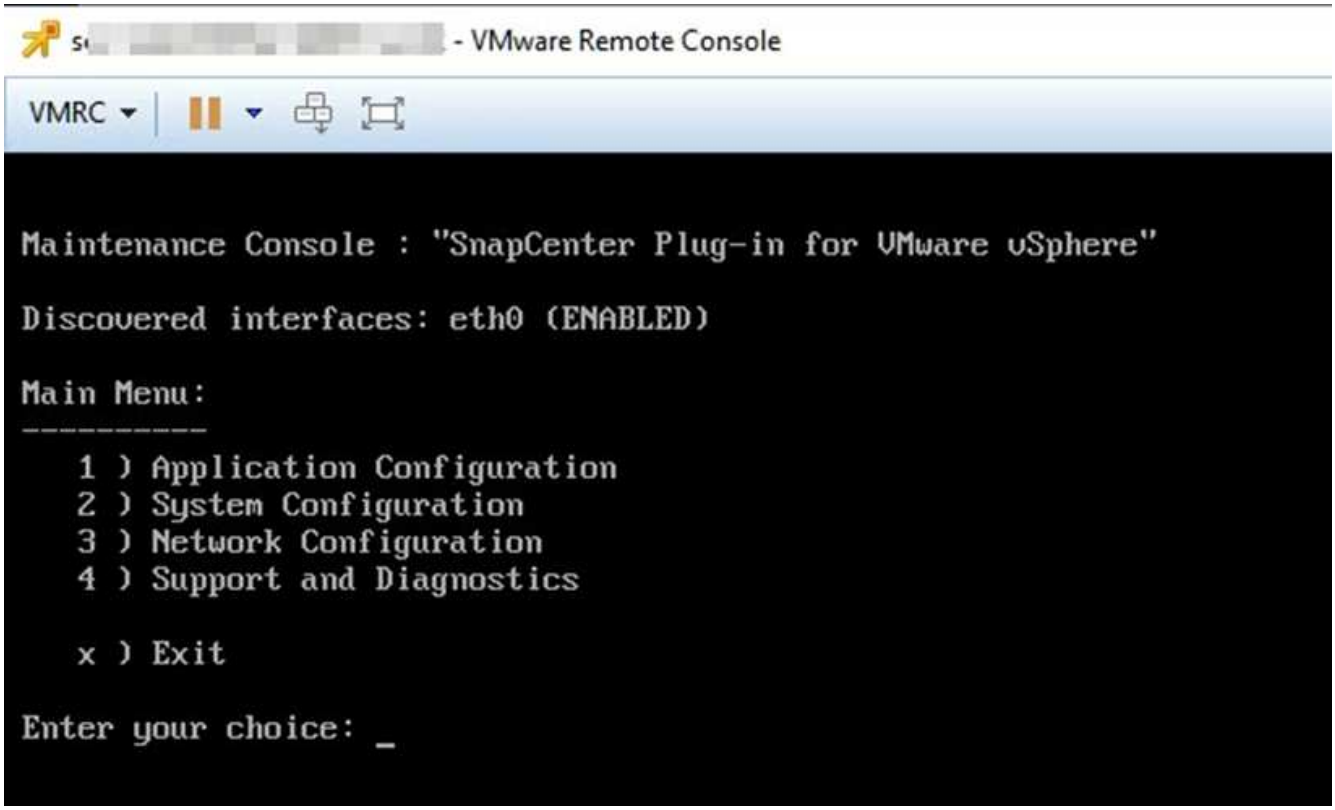
Aktivieren Sie SSH für das SnapCenter Plug-in for VMware vSphere

Wenn das SnapCenter Plug-in for 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 for VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remotekonsole starten** aus, um ein Wartungskonsolenfenster zu öffnen, und melden Sie sich dann an.

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



3. Wählen Sie im Hauptmenü die Menüoption **2) Systemkonfiguration**.
4. Wählen Sie im Systemkonfigurationsmenü die Menüoption **6) SSH-Zugriff aktivieren** und geben Sie dann bei der Bestätigungsaufforderung „**y**“ ein.
5. Warten Sie auf die Meldung „SSH-Zugriff aktivieren …“, drücken Sie dann die Eingabetaste, um fortzufahren, und geben Sie dann bei der Eingabeaufforderung **X** ein, um den Wartungsmodus zu beenden.

REST-APIs

Überblick

Sie können das SnapCenter Plug-in for VMware vSphere REST-APIs verwenden, um allgemeine Datenschutzvorgänge durchzuführen. Das Plug-In verfügt über andere Swagger-Webseiten als die Windows SnapCenter Swagger-Webseiten.

- REST-API-Workflows sind für die folgenden Vorgänge auf VMs und Datenspeichern unter Verwendung der REST-APIs für VMware vSphere dokumentiert:
  - Hinzufügen, Ändern und Löschen von Speicher-VMs und -Clustern
  - Erstellen, Ändern und Löschen von Ressourcengruppen
  - Backup-VMs, geplant und auf Abruf
  - Vorhandene und gelöschte VMs wiederherstellen
  - VMDKs wiederherstellen
  - Anhängen und Trennen von VMDKs
  - Mounten und Unmounten von Datenspeichern
  - Jobs herunterladen und Berichte erstellen
  - Integrierte Zeitpläne ändern
  - Konfigurieren Sie den sekundären Schutz für ASA r2
- Von den REST-APIs für VMware vSphere nicht unterstützte Vorgänge
  - Wiederherstellung der Gastdatei
  - Installation und Konfiguration des SnapCenter Plug-in for VMware vSphere
  - Zuweisen von RBAC-Rollen oder Zugriffsrechten an Benutzer
- `uri`Parameter

  Der `uri` Der Parameter gibt immer einen „Null“-Wert zurück.

- Anmeldezeitüberschreitung

  Das Standard-Timeout beträgt 120 Minuten (2 Stunden). Sie können in den vCenter-Einstellungen einen anderen Timeout-Wert konfigurieren.

- Token-Verwaltung

  Aus Sicherheitsgründen verwenden REST-APIs ein obligatorisches Token, das mit jeder Anforderung übergeben und in allen API-Aufrufen zur Clientvalidierung verwendet wird. Die REST-APIs für VMware vSphere verwenden die VMware-Authentifizierungs-API, um das Token zu erhalten. VMware stellt die Token-Verwaltung bereit.

  Um das Token zu erhalten, verwenden Sie `/4.1/auth/login` REST-API und geben Sie die vCenter-Anmeldeinformationen an.

- API-Versionsbezeichnungen

  Jeder REST-API-Name enthält die SnapCenter -Versionsnummer, in der die REST-API erstmals

veröffentlicht wurde. Zum Beispiel die REST-API `/4.1/datastores/{moref}/backups` wurde erstmals in SnapCenter 4.1 veröffentlicht.

REST-APIs in zukünftigen Versionen sind normalerweise abwärtskompatibel und werden bei Bedarf geändert, um neue Funktionen zu integrieren.

Greifen Sie über die Swagger-API-Webseite auf REST-APIs zu

REST-APIs werden über die Swagger-Webseite bereitgestellt. Sie können auf die Swagger-Webseite zugreifen, um entweder den SnapCenter -Server oder das SnapCenter Plug-in for VMware vSphere REST-APIs anzuzeigen und manuell einen API-Aufruf zu tätigen. Verwenden Sie das SnapCenter Plug-in for VMware vSphere REST-APIs, um Vorgänge auf VMs und Datenspeichern auszuführen.

Das Plug-in verfügt über andere Swagger-Webseiten als die Swagger-Webseiten des SnapCenter Servers.

Bevor Sie beginnen

Für SnapCenter Plug-in for VMware vSphere REST-APIs müssen Sie entweder die IP-Adresse oder den Hostnamen des SnapCenter Plug-in for VMware vSphere kennen.

> Das Plug-In unterstützt nur REST-APIs zum Zweck der Integration mit Anwendungen von Drittanbietern und unterstützt keine PowerShell-Cmdlets oder eine CLI.

Schritte

1. Geben Sie in einem Browser die URL ein, um auf die Swagger-Webseite des Plug-ins zuzugreifen:

   ```
   https://<SCV_IP>:8144/api/swagger-ui/index.html
   ```

   > Verwenden Sie die folgenden Zeichen nicht in der REST-API-URL: +, . , %, Und &.

   Beispiel

   Greifen Sie auf das SnapCenter Plug-in for VMware vSphere REST-APIs zu:

   ```
   https://<SCV_IP>:8144/api/swagger-ui/index.html
   ```

   ```
   https://OVAhost:8144/api/swagger-ui/index.html
   ```

   Melden Sie sich an und verwenden Sie den vCenter-Authentifizierungsmechanismus, 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 Speicher-VMs

Um Vorgänge zum Hinzufügen und Ändern von Speicher-VMs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene

Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Um Speicher-VM-Operationen hinzuzufügen, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	`/4.1/storage-system`	`Add Storage System`fügt die angegebene Speicher-VM zum SnapCenter Plug-in for VMware vSphere hinzu.

Um Speicher-VM-Vorgänge zu ändern, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	`/4.1/storage-system`	`getSvmAll`Ruft die Liste aller verfügbaren Speicher-VMs ab. Notieren Sie den **Namen** der Speicher-VM, die Sie ändern möchten.
2	`/4.1/storage-system`	`Modify Storage System`ändert die angegebene Speicher-VM. Übergeben Sie den **Namen** aus Schritt 1 zusätzlich zu allen anderen erforderlichen Attributen.

REST-API-Workflows zum Erstellen und Ändern von Ressourcengruppen

Um Vorgänge zum Erstellen und Ändern von Ressourcengruppen mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Um Ressourcengruppen zu erstellen, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	`/4.1/policies`	`Get Policies`Ruft die Liste der VMware vSphere-Clientrichtlinien ab. Notieren Sie sich die **policyId**, die Sie beim Erstellen der Ressourcengruppe und der Richtlinien-**Häufigkeit** verwenden möchten. Wenn keine Richtlinien aufgelistet sind, verwenden Sie die `Create Policy` REST-API zum Erstellen einer neuen Richtlinie.
2	`/4.1/resource-groups`	`Create a Resource Group`erstellt eine Ressourcengruppe mit der angegebenen Richtlinie. Übergeben Sie die **policyId** aus Schritt 1 und geben Sie zusätzlich zu allen anderen erforderlichen Attributen die Details zur **Häufigkeit** der Richtlinie ein. Sie können den sekundären Schutz mithilfe dieser REST-API aktivieren.

Um Ressourcengruppen zu ändern, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	`/4.1/resource-groups`	`Get List of Resource Groups`Ruft die Liste der VMware vSphere-Client-Ressourcengruppen ab. Notieren Sie sich 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-Clientrichtlinien ab. Notieren Sie sich die **policyId**, die Sie beim Ändern der Ressourcengruppe und der Richtlinien-**Häufigkeit** verwenden möchten.

Schritt	REST-API	Kommentare
3	`/4.1/resource-groups/{resouceGroupId}`	`Update a Resource Group`ändert die angegebene Ressourcengruppe. Übergeben Sie die **resourceGroupId** aus 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 zum Sichern auf Anfrage

Um Sicherungsvorgänge bei Bedarf mit dem SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Schritt	REST-API	Kommentare
1	`/4.1/resource-groups`	`Get List of Resource Groups`Ruft die Liste der VMware vSphere-Client-Ressourcengruppen ab. Notieren Sie sich die **resourceGroupId** und die **policyId** für die Ressourcengruppe, die Sie sichern möchten.
2	`/4.1/resource-groups/backupnow`	`Run a backup on a Resource Group`sichert die Ressourcengruppe bei Bedarf. Übergeben Sie die **resourceGroupId** und die **policyId** aus Schritt 1.

REST-API-Workflow zum Wiederherstellen von VMs

Um Wiederherstellungsvorgänge für VM-Backups mit dem SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Schritt	REST-API	Kommentare
1	Gehe zu `http://<vCenter-IP>/mob`	Suchen Sie das VM-Moref in der VMware Managed Objects-URL. Notieren Sie sich das **moref** für die VM, die Sie wiederherstellen möchten.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`Ruft eine Liste der Sicherungen für die angegebene VM ab. Übergeben Sie das **moref** aus Schritt 1. Notieren Sie sich die **Backup-ID** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations`Ruft den Speicherort des Snapshots für die angegebene Sicherung ab. Übergeben Sie die **Backup-ID** aus Schritt 2. Beachten Sie die Informationen **snapshotLocationsList**.
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 Informationen **availableEsxHostsList**.
5	`/4.1/vm/{moref}/backups/{backupId}/restore`	`Restore a VM from a backup`stellt die angegebene Sicherung wieder her. Übergeben Sie die Informationen aus den Schritten 3 und 4 im Attribut **restoreLocations**. Wenn es sich bei der VM-Sicherung um eine Teilsicherung handelt, legen Sie die `restartVM` Parameter auf „false“. Sie können eine VM, die eine Vorlage ist, nicht wiederherstellen.

REST-API-Workflow zum Wiederherstellen gelöschter VMs

Um Wiederherstellungsvorgänge für VM-Backups mit dem SnapCenter Plug-in for

VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Schritt	REST-API	Kommentare
1	Gehe zu `http://<vCenter-IP>/mob`	Suchen Sie die VM-UUID in der VMware Managed Objects-URL. Notieren Sie die **UUID** für die VM, die Sie wiederherstellen möchten.
2	`/4.1/vm/{uuid}/backups`	`Get VM Backups`Ruft eine Liste der Sicherungen für die angegebene VM ab. Übergeben Sie die **UUID** aus Schritt 1. Notieren Sie sich die **Backup-ID** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations`Ruft den Speicherort des Snapshots für die angegebene Sicherung ab. Übergeben Sie die **Backup-ID** aus Schritt 2. Beachten Sie die Informationen **snapshotLocationsList**.
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 Informationen **availableEsxHostsList**.
5	`/4.1/vm/{uuid}/backups/{backupId}/restore`	`Restore VM from a backup using uuid or restore a deleted VM`stellt die angegebene Sicherung wieder her. Übergeben Sie die **`UUID`** aus Schritt 1. Übergeben Sie die **`Backup-ID`** aus Schritt 2. Übergeben Sie die Informationen aus den Schritten 3 und 4 im Attribut **`restoreLocations`**. Wenn es sich bei der VM-Sicherung um eine Teilsicherung handelt, legen Sie die `restartVM` Parameter auf „false“. **Hinweis:** Sie können eine VM, die eine Vorlage ist, nicht wiederherstellen.

REST-API-Workflow zum Wiederherstellen von VMDKs

Um Wiederherstellungsvorgänge für VMDKs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Schritt	REST-API	Kommentare
1	Gehe zu `http://<vCenter-IP>/mob`	Suchen Sie das VM-Moref in der VMware Managed Objects-URL. Beachten Sie das **moref** für die VM, in der sich das VMDK befindet.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`Ruft eine Liste der Sicherungen für die angegebene VM ab. Übergeben Sie das **moref** aus Schritt 1. Notieren Sie sich die **Backup-ID** des Backups, das Sie wiederherstellen möchten.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations`Ruft den Speicherort des Snapshots für die angegebene Sicherung ab. Übergeben Sie die **Backup-ID** aus Schritt 2. Beachten Sie die Informationen **snapshotLocationsList**.
4	`/4.1/vm/{moref}/backups/vmdklocations`	`Get Vmdk Locations`Ruft eine Liste von VMDKs für die angegebene VM ab. Beachten Sie die Informationen **vmdkLocationsList**.
5	`/4.1/vm/{ moref}/backups/{backupId}/availabledatastores`	`Get Available Datastores`Ruft eine Liste der Datenspeicher ab, die für den Wiederherstellungsvorgang verfügbar sind. Übergeben Sie das **moref** aus Schritt 1. Übergeben Sie die **Backup-ID** aus Schritt 2. Beachten Sie die Informationen **DatastoreNameList**.
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 das **moref** aus Schritt 1. Beachten Sie die Informationen **availableEsxHostsList**.

Schritt	REST-API	Kommentare
7	`/4.1/vm/{moref}/backups/{backupId}/restorevmdks`	`Restore a VMDK from a backup`stellt das angegebene VMDK aus der angegebenen Sicherung wieder her. Übergeben Sie im Attribut **esxHost** die Informationen aus **availableEsxHostsList** in Schritt 6. Übergeben Sie die Informationen aus den Schritten 3 bis 5 an das Attribut **vmdkRestoreLocations**: • Übergeben Sie im Attribut „restoreFromLocation“ die Informationen aus „snapshotLocationsList“ in Schritt 3. • Übergeben Sie im Attribut „vmdkToRestore“ die Informationen aus „vmdkLocationsList“ in Schritt 4. • Übergeben Sie im Attribut „restoreToDatastore“ die Informationen aus „DatastoreNameList“ in Schritt 5.

REST-API-Workflows zum Anhängen und Trennen von VMDKs

Um Anfüge- und Trennvorgänge für VMDKs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Um VMDKs anzuhängen, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	Gehe zu `http://<vCenter-IP>/mob`	Suchen Sie das VM-Moref in der VMware Managed Objects-URL. Notieren Sie sich das **moref** für die VM, an die Sie ein VMDK anhängen möchten.

Schritt	REST-API	Kommentare
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`Ruft eine Liste der Sicherungen für die angegebene VM ab. Übergeben Sie das **moref** aus Schritt 1. Notieren Sie sich die **Backup-ID** 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. Übergeben Sie die **backupId** aus Schritt 2 und das **moref** aus Schritt 1. Beachten Sie die Informationen **vmdkLocationsList**.
4	`/4.1/vm/{moref}/attachvmdks`	`Attach VMDKs`hängt das angegebene VMDK an die ursprüngliche VM an. Übergeben Sie die **backupId** aus Schritt 2 und das **moref** aus Schritt 1. Übergeben Sie die **vmdkLocationsList** aus Schritt 3 an das Attribut **vmdkLocations**. Um ein VMDK an eine andere VM anzuhängen, übergeben Sie das Moref der Ziel-VM im Attribut alternateVmMoref.

Um VMDKs zu trennen, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	Gehe zu `http://<vCenter-IP>/mob`	Suchen Sie das VM-Moref in der VMware Managed Objects-URL. Beachten Sie das **moref** für die VM, von der Sie ein VMDK trennen möchten.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`Ruft eine Liste der Sicherungen für die angegebene VM ab. Übergeben Sie das **moref** aus Schritt 1. Notieren Sie sich die **Backup-ID** 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. Übergeben Sie die **backupId** aus Schritt 2 und das **moref** aus Schritt 1. Beachten Sie die Informationen **vmdkLocationsList**.
4	`/4.1/vm/{moref}/detachvmdks`	`Detach VMDKs`trennt das angegebene VMDK. Übergeben Sie das **moref** aus Schritt 1. Übergeben Sie die VMDK-Details **vmdkLocationsList** aus Schritt 3 an das Attribut **vmdksToDetach**.

REST-API-Workflows zum Mounten und Unmounten von Datenspeichern

Um Mount- und Unmount-Vorgänge für Datenspeichersicherungen mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Um Datenspeicher zu mounten, folgen Sie diesem Workflow:

Schritt	REST-API	Kommentare
1	Gehe zu `http://<vCenter-IP>/mob`	Suchen Sie den Datenspeicher moref über die VMware Managed Objects-URL. Notieren Sie sich das **moref** für den Datenspeicher, den Sie mounten möchten.
2	`/4.1/datastores/{moref}/backups`	`Get the list of backups for a datastore`Ruft eine Liste der Sicherungen für den angegebenen Datenspeicher ab. Übergeben Sie das **moref** aus Schritt 1. Notieren Sie sich die **Backup-ID**, die Sie mounten möchten.
3	`/4.1/datastores/backups/{backupId}/snapshotlocators`	`Get the list of Snapshot Locations`Ruft Details zum Speicherort der angegebenen Sicherung ab. Übergeben Sie die **Backup-ID** aus Schritt 2. Notieren Sie sich den **Datenspeicher** und den Speicherort aus der Liste **snapshotLocationsList**.

Schritt	REST-API	Kommentare
4	`/4.1/datastores/{moref}/availableEsxHosts`	`Get the list of Available Esxi Hosts`Ruft die Liste der ESXi-Hosts ab, die für Mountvorgänge verfügbar sind. Übergeben Sie das **moref** aus Schritt 1. Beachten Sie die Informationen **availableEsxHostsList**.
5	`/4.1/datastores/backups/{backupId}/mount`	`Mount datastores for a backup`mountet die angegebene Datenspeichersicherung. Übergeben Sie die **Backup-ID** aus Schritt 2. Übergeben Sie in den Attributen **datastore** und **location** die Informationen von `snapshotLocationsList` in Schritt 3. Übergeben Sie im Attribut **esxHostName** die Informationen aus **availableEsxHostsList** in Schritt 4.

Um die Bereitstellung von Datenspeichern aufzuheben, folgen Sie diesem Arbeitsablauf:

Schritt	REST-API	Kommentare
1	`/4.1/datastores/backups/{backupId}/mounted`	`Get the list of mounted datastores` . Notieren Sie sich die **moref**-Datenspeicher, die Sie aushängen möchten.
2	`/4.1/datastores/unmount`	`UnMount datastores for a backup`hebt die Bereitstellung der angegebenen Datenspeichersicherung auf. Übergeben Sie den/die Datenspeicher **moref** aus Schritt 1.

REST-APIs zum Herunterladen von Jobs und Generieren von Berichten

Um Berichte zu erstellen und Protokolle für VMware vSphere-Clientjobs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs herunterzuladen, 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, um einen vollständigen Endpunkt zu bilden.

Verwenden Sie die folgenden REST-APIs im Abschnitt „Jobs“, um detaillierte Informationen zu Jobs zu erhalten:

REST-API	Kommentare
`/4.1/jobs`	`Get all jobs`Ruft die Auftragsdetails für mehrere Aufträge ab. Sie können den Umfang der Anfrage einschränken, indem Sie einen Jobtyp angeben, wie zum Beispiel `backup`, `mountBackup`, oder `restore`.
`/4.1/jobs/{id}`	`Get job details`erhält detaillierte Informationen zum angegebenen Job.

Verwenden Sie die folgende REST-API im Abschnitt „Jobs“, um Jobprotokolle herunterzuladen:

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“, um Berichte zu generieren:

REST-API	Kommentare
`4.1/reports/protectedVM`	`Get Protected VM List`erhält eine Liste der geschützten VMs der letzten sieben Tage.
`/4.1/reports/unProtectedVM`	`Get Unprotected VM List`erhält eine Liste der ungeschützten VMs der letzten sieben Tage.

REST-API-Workflow zum Ändern integrierter Zeitpläne

Um integrierte Zeitpläne für VMware vSphere-Clientjobs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs zu ändern, müssen Sie die vorgeschriebene Reihenfolge der REST-API-Aufrufe einhalten.

Integrierte Zeitpläne sind die Zeitpläne, die als Teil des Produkts bereitgestellt werden, beispielsweise 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, um einen vollständigen Endpunkt zu bilden.

Schritt	REST-API	Kommentare
1	`/4.1/schedules`	`Get all built-in`schedules ruft eine Liste der Jobpläne ab, die ursprünglich im Produkt bereitgestellt wurden. Notieren Sie den Zeitplannamen, den Sie ändern möchten, und den zugehörigen Cron-Ausdruck.
2	`/4.1/schedules`	`Modify any built-in schedule`ändert den benannten Zeitplan. Übergeben Sie den Zeitplannamen aus Schritt 1 und erstellen Sie einen neuen Cron-Ausdruck für den Zeitplan.

REST-API zum Markieren feststeckender Jobs als fehlgeschlagen

Um Job-IDs für VMware vSphere-Clientjobs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs zu finden, müssen Sie die REST-API-Aufrufe für VMware vSphere verwenden. Diese REST-APIs wurden im SnapCenter Plug-in for VMware vSphere 4.4 hinzugefügt.

Fügen Sie für jede REST-API „\https://<Server>:<Port>“ am Anfang der REST-API hinzu, um einen vollständigen Endpunkt zu bilden.

Verwenden Sie die folgende REST-API im Abschnitt „Jobs“, um Jobs, die im laufenden Status feststecken, in einen fehlgeschlagenen Status zu ändern:

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 Zustand hängen geblieben sind, verwenden Sie die GUI des Job-Monitors, um den Status jedes Jobs und die Job-ID anzuzeigen.

REST-APIs zum Generieren von Audit-Protokollen

Sie können die Audit-Protokolldetails von Swagger-Rest-APIs sowie der Benutzeroberfläche des SCV-Plugins erfassen.

Nachfolgend sind die Swagger-Rest-APIs aufgeführt:

1. GET 4.1/audit/logs: Prüfdaten für alle Protokolle abrufen
2. GET 4.1/audit/logs/{filename}: Prüfdaten für eine bestimmte Protokolldatei abrufen

3. POST 4.1/audit/verify: Überprüfung des Audit-Protokolls auslösen.
4. GET 4.1/audit/config: Ruft die Konfiguration des Audit- und Syslog-Servers ab
5. PUT 4.1/audit/config: Aktualisieren Sie die Audit- und Syslog-Serverkonfiguration

Um Überwachungsprotokolle für VMware vSphere-Clientjobs mithilfe des SnapCenter Plug-in for VMware vSphere REST-APIs zu generieren, müssen Sie die REST-API-Aufrufe für VMware vSphere verwenden.

Fügen Sie für jede REST-API hinzu `https://<server>:<port>/api` an der Vorderseite der REST-API, um einen vollständigen Endpunkt zu bilden.

Verwenden Sie die folgenden REST-APIs im Abschnitt „Jobs“, um detaillierte Informationen zu Jobs zu erhalten:

REST-API	Kommentare
`4.1/audit/logs`	gibt Audit-Protokolldateien mit Integritätsdaten zurück
`4.1/audit/logs/{filename}`	Erhalten Sie eine spezifische Audit-Protokolldatei mit Integritätsdaten
`4.1/audit/verify`	löst Audit-Verifizierung aus
`4.1/audit/syslogcert`	aktualisiert das Syslog-Server-Zertifikat

Upgrade

Upgrade von einer früheren Version des SnapCenter Plug-in for VMware vSphere

> Das Upgrade auf SCV 6.1 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 for VMware vSphere Appliance verwenden, können Sie auf eine neuere Version aktualisieren. Der Upgrade-Prozess hebt die Registrierung des vorhandenen Plug-Ins auf und stellt ein Plug-In bereit, das nur mit vSphere 7.0U1 und späteren Versionen kompatibel ist.

Upgrade-Pfade

Wenn Sie die Version des SnapCenter Plug-in for VMware vSphere (SCV) verwenden …	Sie können das SnapCenter Plug-in for VMware vSphere direkt aktualisieren auf …
SCV 6,0	Upgrade auf SCV 6.1
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 for VMware vSphere OVA, bevor Sie ein Upgrade starten.

> Das Umstellen Ihrer Netzwerkkonfiguration von statisch auf DHCP wird nicht unterstützt.

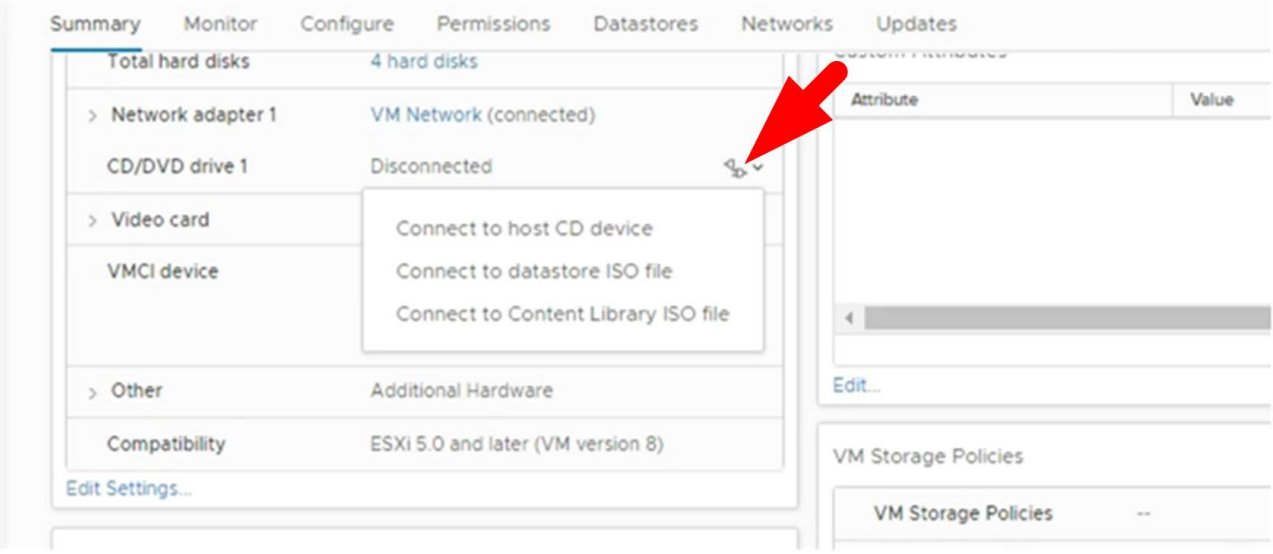
Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitätsmatrix-Tool" (IMT).

Schritte

1. Bereiten Sie das Upgrade vor, indem Sie das SnapCenter Plug-in for VMware vSphere deaktivieren.
   a. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI an. Die IP-Adresse wird angezeigt, wenn Sie das SnapCenter Plug-in for VMware vSphere bereitstellen.
   b. Wählen Sie im linken Navigationsbereich **Konfiguration** und dann im Abschnitt „Plug-in-Details“ die Option **Dienst**, um das Plug-in zu deaktivieren.
2. Herunterladen des Upgrades `.iso` Datei.
   a. Melden Sie sich bei der NetApp Support Site an(https://mysupport.netapp.com/products/index.html).
   b. Wählen Sie aus der Produktliste * SnapCenter Plug-in for VMware vSphere* und dann die Schaltfläche **NEUESTE VERSION HERUNTERLADEN**.
   c. Laden Sie das SnapCenter Plug-in for VMware vSphere Upgrade herunter `.iso` Datei an einen

beliebigen Ort.

3. Installieren Sie das Upgrade.
   a. Navigieren Sie in Ihrem Browser zum VMware vSphere vCenter.
   b. Wählen Sie in der vCenter-GUI **vSphere-Client (HTML)** aus.
   c. Melden Sie sich auf der Seite **VMware vCenter Single Sign-On** an.
   d. Wählen Sie im Navigationsbereich die VM aus, die Sie aktualisieren möchten, und wählen Sie dann die Registerkarte **Zusammenfassung** aus.
   e. Wählen Sie im Bereich **Verwandte Objekte** einen beliebigen Datenspeicher in der Liste aus und wählen Sie dann die Registerkarte **Zusammenfassung**.
   f. Wählen Sie auf der Registerkarte **Dateien** für den ausgewählten Datenspeicher einen beliebigen Ordner in der Liste aus und wählen Sie dann **Dateien hochladen**.
   g. Navigieren Sie im Upload-Popup-Bildschirm zu dem Speicherort, an dem Sie die `.iso` Datei, wählen Sie dann auf der `.iso` Dateibild und wählen Sie dann **Öffnen**. Die Datei wird in den Datenspeicher hochgeladen.
   h. Navigieren Sie zurück zur VM, die Sie aktualisieren möchten, und wählen Sie die Registerkarte **Zusammenfassung** aus. Im Bereich **VM-Hardware** sollte im Feld CD/DVD der Wert „Getrennt“ lauten.
   i. Wählen Sie das Verbindungssymbol im CD/DVD-Feld und wählen Sie **Mit CD/DVD-Image auf einem Datenspeicher verbinden**.



   j. Führen Sie im Assistenten die folgenden Schritte aus:
      i. Wählen Sie in der Spalte „Datenspeicher“ den Datenspeicher aus, in den Sie die `.iso` Datei.
      ii. Navigieren Sie in der Spalte Inhalt zu `.iso` Stellen Sie sicher, dass im Feld „Dateityp“ die Option „ISO-Image“ ausgewählt ist, und wählen Sie dann **OK** aus. Warten Sie, bis im Feld 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 Ausführungspfeil auswählen, um die Wartungskonsole zu starten.
   l. Geben Sie **2** für die Systemkonfiguration und dann **8** für das Upgrade ein.
   m. Geben Sie **y** ein, um fortzufahren und das Upgrade zu starten.

Upgrade auf einen neuen Patch der gleichen Version des SnapCenter Plug-in for VMware vSphere

Wenn Sie auf einen neuen Patch derselben Version aktualisieren, müssen Sie den Cache des SnapCenter Plug-in for VMware vSphere auf dem vCenter-Webserver löschen und den Server vor dem Upgrade oder der Registrierung neu starten.

Wenn der Plug-In-Cache nicht geleert wird, werden aktuelle Jobs in den folgenden Szenarien nicht im Dashboard und im Job-Monitor angezeigt:

- Das SnapCenter Plug-in for VMware vSphere wurde mithilfe von vCenter bereitgestellt und später auf einen Patch in derselben Version aktualisiert.
- Die virtuelle SnapCenter VMware-Appliance wurde in vCenter 1 bereitgestellt. Später wurde dieses SnapCenter Plug-in for VMware vSphere bei einem neuen vCenter2 registriert. Eine neue Instanz des SnapCenter Plug-in for VMware vSphere wird mit einem Patch erstellt und bei vCenter1 registriert. Da vCenter1 jedoch noch über das zwischengespeicherte Plug-In vom ersten SnapCenter Plug-in for VMware vSphere ohne Patch verfügt, muss der Cache geleert werden.

Schritte zum Leeren des Caches

1. Suchen Sie die `vsphere-client-serenity` Ordner, und suchen Sie dann die `com.netapp.scv.client-<release-number>` Ordner und löschen Sie ihn.

   Der Ordnername ändert sich für jede Version.

   Den Speicherort des `vsphere-client-serenity` Ordner für Ihr Betriebssystem.

2. Starten Sie den vCenter Server neu.

   Anschließend können Sie das SnapCenter Plug-in for VMware vSphere aktualisieren.

Nach dem Upgrade auf einen neuen Patch derselben Version werden keine Informationen angezeigt

Nach dem Upgrade des SnapCenter Plug-in for VMware vSphere auf einen neuen Patch derselben Version werden aktuelle Jobs oder andere Informationen möglicherweise nicht im Dashboard und im Job-Monitor angezeigt.

Wenn Sie auf einen neuen Patch derselben Version aktualisieren, müssen Sie den Cache des SnapCenter Plug-in for VMware vSphere auf dem vCenter-Webserver löschen und den Server vor dem Upgrade oder der Registrierung neu starten.

Wenn der Plug-In-Cache nicht geleert wird, werden aktuelle Jobs in den folgenden Szenarien nicht im Dashboard und im Job-Monitor angezeigt:

- Das SnapCenter Plug-in for VMware vSphere wurde mithilfe von vCenter bereitgestellt und später auf einen Patch in derselben Version aktualisiert.
- Die virtuelle SnapCenter VMware-Appliance wurde in vCenter 1 bereitgestellt. Später wurde dieses SnapCenter Plug-in for VMware vSphere bei einem neuen vCenter2 registriert. Eine neue Instanz des SnapCenter Plug-in for VMware vSphere wird mit einem Patch erstellt und bei vCenter1 registriert. Da

vCenter1 jedoch noch über das zwischengespeicherte Plug-In vom ersten SnapCenter Plug-in for VMware vSphere ohne Patch verfügt, muss der Cache geleert werden.

Der Cache befindet sich je nach Typ des Serverbetriebssystems an den folgenden Speicherorten:

- vCenter Server-Linux-Appliance

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

- Windows-Betriebssystem

  ```
  %PROGRAMFILES%/VMware/vSphere client/vc-packages/vsphere-client-serenity/
  ```

Problemumgehung, wenn Sie bereits vor dem Leeren des Caches ein Upgrade durchgeführt haben

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI an.

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

2. Wählen Sie im linken Navigationsbereich **Konfiguration** und dann im Abschnitt **Plug-in-Details** die Option „Dienst“, um das Plug-in zu deaktivieren.

   Das SnapCenter Plug-in for VMware vSphere Dienst ist deaktiviert und die Erweiterung ist in vCenter nicht registriert.

3. Suchen Sie die `vsphere-client-serenity` Ordner, und suchen Sie dann die `com.netapp.scv.client-<release-number>` Ordner und löschen Sie ihn.

   Der Ordnername ändert sich für jede Version.

4. Starten Sie den vCenter Server neu.
5. Melden Sie sich beim VMware vSphere-Client an.
6. Wählen Sie im linken Navigationsbereich **Konfiguration** und dann im Abschnitt **Plug-in-Details** die Option „Dienst“, um das Plug-in zu aktivieren.

   Das SnapCenter Plug-in for VMware vSphere Dienst ist aktiviert und die Erweiterung ist in vCenter registriert.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"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 ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp 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

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

"Hinweis zum SnapCenter Plug-in for VMware vSphere 6.1"

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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