



# **Dokumentation zum SnapCenter Plug-in für VMware vSphere**

SnapCenter Plug-in for VMware vSphere 5.0

NetApp  
July 18, 2024

# Inhalt

Dokumentation zum SnapCenter Plug-in für VMware vSphere	1
Versionshinweise	2
Konzepte	3
Produktübersicht	3
Überblick über die verschiedenen SnapCenter GUIs	4
Lizenzierung	5
Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)	6
RBAC-Typen für SnapCenter Plug-in für VMware vSphere Benutzer	6
ONTAP RBAC-Funktionen im SnapCenter Plug-in für VMware vSphere	8
Vordefinierte Rollen in Paketen mit SnapCenter Plug-in für VMware vSphere	9
So konfigurieren Sie ONTAP RBAC für SnapCenter Plug-in für VMware vSphere	10
Los geht's	12
Implementierungsübersicht	12
Implementierungs-Workflow für vorhandene Benutzer	12
Anforderungen für die Bereitstellung von SCV	13
Open Virtual Appliance (OVA) herunterladen	20
Implementieren Sie das SnapCenter Plug-in für VMware vSphere	21
Nach der Implementierung erforderliche Betriebsabläufe und Probleme	25
Melden Sie sich beim SnapCenter VMware vSphere-Client an	27
Schnellstart	28
Überblick	28
Implementieren Sie das SnapCenter Plug-in für VMware vSphere	28
Erweitern Sie Ihren Storage	30
Backup-Richtlinien erstellen	30
Erstellen von Ressourcengruppen	30
Monitoring und Reporting	31
Zeigt Statusinformationen an	31
Überwachen von Jobs	33
Job-Protokolle herunterladen	33
Aufrufen von Berichten	34
Generieren Sie ein Support Bundle aus dem SnapCenter Plug-in für VMware vSphere	36
Generieren Sie ein Support-Bundle über die Wartungskonsole	37
Prüfprotokolle	38
Storage-Management	42
Erweitern Sie Ihren Storage	42
Management von Storage-Systemen	44
Ändern Sie die konfigurierte Storage-Zeitüberschreitung	46
Sichern von Daten	47
Datensicherungs-Workflow	47
Zeigen Sie VM- und Datastore-Backups an	48
Erstellen von Backup-Richtlinien für VMs und Datastores	49
Erstellen von Ressourcengruppen	53
Vorschriften und Postskripte	60

Fügen Sie eine einzelne VM oder einen Datenspeicher zu einer Ressourcengruppe hinzu	63
Fügen Sie mehrere VMs und Datenspeicher einer Ressourcengruppe hinzu	64
Backup des umbenannten Speichers wiederherstellen	65
Bei Bedarf das Sichern von Ressourcengruppen sichern	66
Sichern Sie das SnapCenter Plug-in für VMware vSphere MySQL Datenbank	66
Verwalten von Ressourcengruppen	67
Management von Richtlinien	69
Backup-Management	70
Mounten und Unmounten von Datastores	73
Mounten Sie ein Backup	73
Heben Sie die Bereitstellung eines Backups auf	74
Restore aus Backups	75
Restore-Übersicht	75
Durchführen von Restore-Vorgängen	75
Suche nach Backups	77
Wiederherstellung von VMs aus Backups	78
Gelöschte VMs aus Backups wiederherstellen	81
Wiederherstellung von VMDKs aus Backups	82
Stellen Sie das neueste Backup der MySQL-Datenbank wieder her	84
Stellen Sie ein bestimmtes Backup der MySQL-Datenbank wieder her	84
Anschließen und Trennen von VMDKs	86
Weisen Sie VMDKs an eine VM oder vVol VM zu	86
Trennen Sie eine virtuelle Festplatte	88
Wiederherstellung von Gastdateien und Ordnern	89
Workflow, Voraussetzungen und Einschränkungen	89
Wiederherstellung von Gastdateien und Ordnern über VMDKs	91
Einrichten von Proxy-VMs für Wiederherstellungsvorgänge	95
Konfigurieren Sie die Anmeldedaten für die Wiederherstellung von VM-Gastdateien	95
Verlängern Sie die Zeit für die Wiederherstellung von Gastdateien	97
Szenario zur Wiederherstellung von Gastdateien, in denen Sie möglicherweise auftreten können	97
Managen Sie das SnapCenter Plug-in für VMware vSphere Appliance	99
Starten Sie den VMware vSphere-Client-Service neu	99
Öffnen Sie die Wartungskonsole	99
Ändern Sie das Passwort für das SnapCenter VMware Plug-in von der Wartungskonsole aus	101
Erstellen und Importieren von Zertifikaten	102
Heben Sie das SnapCenter Plug-in für VMware vSphere vom vCenter ab	102
Deaktivieren und aktivieren Sie das SnapCenter Plug-in für VMware vSphere	103
Entfernen Sie das SnapCenter Plug-in für VMware vSphere	104
Managen Sie Ihre Konfiguration	105
Ändern der Zeitzonen für Backups	105
Ändern der Anmeldeinformationen	105
Ändern Sie die Anmeldedaten für vCenter-Anmeldung	106
Ändern Sie die Netzwerkeinstellungen	107
Ändern Sie die Standardwerte der Konfiguration	108
Erstellen Sie die Konfigurationsdatei scbr.override	109

Eigenschaften, die Sie überschreiben können	109
Aktivieren Sie das SSH for SnapCenter Plug-in für VMware vSphere	114
Rest-APIs	116
Überblick	116
Greifen Sie über die Swagger API-Webseite auf REST-APIs zu	117
REST-API-Workflows zum Hinzufügen und Ändern von Storage-VMs	117
REST-API-Workflows zum Erstellen und Ändern von Ressourcengruppen	118
REST-API-Workflow für Backup nach Bedarf	119
REST-API-Workflow zur Wiederherstellung von VMs	120
REST-API-Workflow zur Wiederherstellung gelöschter VMs	121
REST-API-Workflow zur Wiederherstellung von VMDKs	122
REST-API-Workflows zum Verbinden und Trennen von VMDKs	124
REST-API-Workflows zum Mounten und Unmounten von Datastores	126
REST-APIs zum Herunterladen von Jobs und zum Generieren von Berichten	127
REST-API-Workflow zum Ändern integrierter Zeitpläne	128
REST-API zum Markieren von eingeklemmten Jobs als fehlgeschlagen	129
REST-APIs zur Erstellung von Prüfprotokollen	129
Upgrade	131
Upgrade von einer früheren Version des SnapCenter Plug-ins für VMware vSphere	131
Upgraden Sie auf einen neuen Patch derselben Version des SnapCenter Plug-ins für VMware vSphere	133
Informationen, die nach dem Upgrade auf einen neuen Patch derselben Version nicht angezeigt werden	133
Rechtliche Hinweise	135
Urheberrecht	135
Marken	135
Patente	135
Datenschutzrichtlinie	135
Open Source	135

# Dokumentation zum SnapCenter Plug-in für VMware vSphere

# Versionshinweise

In den Versionshinweisen finden Sie wichtige Informationen zu dieser Version des SnapCenter Plug-ins für VMware vSphere, einschließlich Lizenzierungsanforderungen, bekannten Problemen, Vorsichtsmaßnahmen, Einschränkungen, Und jegliche Aktualisierungen oder Korrekturen der Dokumentation. Weitere Informationen finden Sie unter "[Versionshinweise zum SnapCenter Plug-in für VMware vSphere 5.0](#)"

# Konzepte

## Produktübersicht

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

Das SnapCenter VMware Plug-in erweitert Ihre Umgebung um die folgenden Funktionen:

- Unterstützung von VM-konsistenten und absturzkonsistenten Datensicherungsvorgängen

Die VMware vSphere Client GUI in vCenter kann für alle Backup- und Restore-Vorgänge von VMware Virtual Machines (herkömmliche VMs und vVol VMs), VMDKs und Datastores genutzt werden. Für vVol VMs (VMs in vVol Datastores) werden nur absturzkonsistente Backups unterstützt. Sie haben auch die Möglichkeit, VMs und VMDKs wiederherzustellen sowie Dateien und Ordner auf dem Gastbetriebssystem wiederherzustellen.

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

Das SnapCenter VMware Plug-in beinhaltet eine MySQL Datenbank, die die SnapCenter VMware Plug-in-Metadaten enthält. Für die VM-konsistente und absturzkonsistente Datensicherung müssen Sie den SnapCenter Server nicht installieren.

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

Sie können die SnapCenter-Benutzeroberfläche und die entsprechenden SnapCenter-Applikations-Plug-ins für alle Backup- und Restore-Vorgänge von Datenbanken und Dateisystemen auf primärem und sekundärem Storage auf VMs verwenden.

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

SnapCenter unterstützt keine einzelnen Snapshots von Datenbanken und VMs zusammen. Backups für VMs und Datenbanken müssen unabhängig geplant und ausgeführt werden. Dadurch werden separate Snapshots erstellt, selbst wenn die Datenbanken und VMs im gleichen Volume gehostet werden. Planen Sie die Datenbank-Anwendungs-Backups mit der SnapCenter GUI. Planen Sie die VM- und Datenspeicher-Backups mit der VMware vSphere Client GUI.

- VMware Tools sind für VM-konsistente Snapshots erforderlich

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

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

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

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

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

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

Weitere Informationen finden Sie unter "[ONTAP Tools für VMware vSphere](#)"

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

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

Zusätzlich zu diesen wichtigen Funktionen unterstützt das SnapCenter Plug-in für VMware vSphere auch iSCSI, Fibre Channel, FCoE, VMDK über NFS 3.0 und 4.1 und VMDK über VMFS 5.0 und 6.0.

Die neuesten Informationen zu unterstützten Versionen finden Sie im <https://imt.netapp.com/matrix/imt.jsp?components=117018;&solution=1259&isHWU&src=IMT> [NetApp Interoperabilitäts-Matrix-Tool<sup>1</sup>] (IMT).

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

Weitere Informationen zum SnapCenter Datenschutz finden Sie in den Datenschutzzinformationen Ihres SnapCenter Plug-ins in der "[SnapCenter-Dokumentation](#)".

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

## Überblick über die verschiedenen SnapCenter GUIs

In Ihrer SnapCenter-Umgebung müssen die Datensicherung und das Management über die entsprechende GUI durchgeführt werden.

Das SnapCenter Plug-in für VMware vSphere ist ein Standalone-Plug-in, das sich von anderen SnapCenter-Plug-ins unterscheidet. Sie müssen die VMware vSphere Client GUI in vCenter für alle Backup- und Restore-Vorgänge für VMs, VMDKs und Datastores nutzen. Darüber hinaus verwenden Sie das Web-Client-GUI-Dashboard, um die Liste der geschützten und nicht geschützten VMs zu überwachen. Für alle anderen SnapCenter Plug-in-Vorgänge (applikationsbasierte Plug-ins) wie Backup und Restore sowie Job-Monitoring verwenden Sie die GUI von SnapCenter.

Zur Sicherung von VMs und Datastores nutzen Sie die Schnittstelle des VMware vSphere Clients. Die Web-Client-GUI ist in die NetApp Snapshot Technologie auf dem Storage-System integriert. So können Sie VMs und Datenspeicher in Sekundenschnelle sichern und VMs wiederherstellen, ohne einen ESXi Host offline zu schalten.

Es gibt auch eine Management-GUI zum Durchführen administrativer Vorgänge im SnapCenter VMware Plug-in.

Die folgende Tabelle zeigt die von der SnapCenter GUI durchgeführten Vorgänge.



Verwenden Sie diese GUI...	Zur Ausführung dieser Vorgänge...	Und für den Zugriff auf diese Backups...
SnapCenter vSphere Client-GUI	VM- und Datastore-Backup VMDK-Anbindung und -Trennung Datastore-Mount und unmounten Sie VM und VMDK Restore der Gastdatei und Ordner	Backups von VMs und Datastores mithilfe der VMware vSphere Client-GUI.
GUI von SnapCenter	Backup und Restore von Datenbanken und Applikationen auf VMs, einschließlich der Sicherung von Datenbanken für Microsoft SQL Server, Microsoft Exchange und Oracle. Datenbankklone	Backups werden über die GUI von SnapCenter durchgeführt.
SnapCenter Plug-in für Management-GUI von VMware vSphere	Ändern der Netzwerkkonfiguration Erstellen Sie ein Supportpaket Ändern der NTP-Servereinstellungen Deaktivieren/Aktivieren des Plug-ins	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 Backup- und Restore-Vorgänge müssen Sie die VMware vSphere Client GUI verwenden. Obwohl einige Vorgänge mithilfe von VMware Tools beispielsweise beim Mounten oder Umbenennen eines Datastores möglich sind, werden diese Vorgänge nicht im SnapCenter Repository registriert und werden nicht erkannt.

SnapCenter unterstützt keine einzelnen Snapshots von Datenbanken und VMs zusammen. Backups für VMs und Datenbanken müssen unabhängig geplant und ausgeführt werden. Dadurch werden separate Snapshots erstellt, selbst wenn die Datenbanken und VMs im gleichen Volume gehostet werden. Applikationskonsistente Backups müssen über die SnapCenter GUI geplant werden. VM-konsistente Backups müssen über die VMware vSphere Client GUI geplant werden.

## Lizenzierung

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

- FAS
- AFF
- Cloud Volumes ONTAP
- ONTAP Select
- ASA

Es wird empfohlen, aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standardlizenzen nicht auf sekundären Systemen aktiviert sind, können Sie SnapCenter nach einem Failover-Vorgang nicht verwenden. Allerdings ist eine FlexClone Lizenz auf

sekundärem Storage erforderlich, um Mount- und Attached-Vorgänge durchzuführen. Zur Durchführung von Restore-Vorgängen ist eine SnapRestore Lizenz erforderlich.

## **Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)**

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

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

Das SnapCenter VMware Plug-in wird mit vordefinierten vCenter Rollen ausgeliefert. 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 Zugriff auf Ressourcen hinzufügen. Wenn Sie jedoch das SnapCenter-VMware-Plug-in zum ersten Mal einrichten, sollten Sie den Rollen mindestens Active Directory-Benutzer oder -Gruppen hinzufügen und anschließend diesen Benutzern oder Gruppen Ressourcen-Zugriff hinzufügen.

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

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

### **RBAC für vCenter Server**

Dieser Sicherheitsmechanismus gilt für alle durch das SnapCenter Plug-in ausgeführten Aufgaben wie VM-konsistente, VM-Crash-konsistente und applikationskonsistente SnapCenter Server-Jobs (Applikation über VMDK). Durch diese Stufe der RBAC ist es möglich, vSphere Benutzer zur Durchführung von SnapCenter VMware Plug-in-Aufgaben auf vSphere Objekten wie Virtual Machines (VMs) und Datastores zu unterstützen.

Die Implementierung des SnapCenter VMware Plug-in erstellt folgende Rollen für SnapCenter Vorgänge in vCenter:

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

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

- Legen Sie die vCenter Server-Berechtigungen auf dem Root-Objekt (auch als Stammordner bekannt) fest. Sie können dann die Sicherheit verbessern, indem Sie untergeordnete Entitäten, die diese Berechtigungen

nicht benötigen, einschränken.

- Zuweisen der SCV-Rollen zu Active Directory-Benutzern.

Mindestens müssen alle Benutzer in der Lage sein, vCenter Objekte anzuzeigen. Ohne diese Berechtigung können Benutzer nicht auf die VMware vSphere Client GUI zugreifen.

## **ONTAP RBAC**

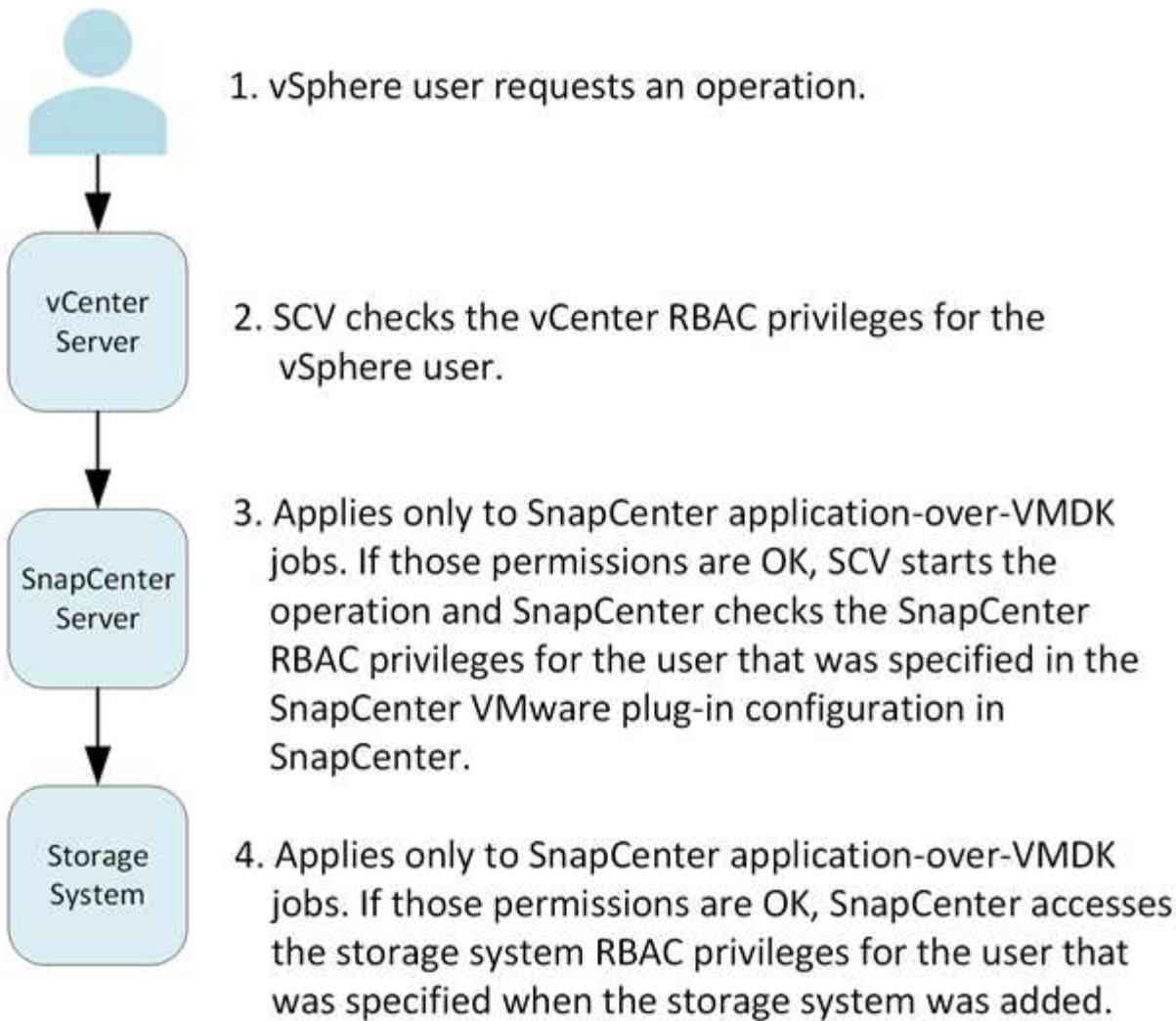
Dieser Sicherheitsmechanismus gilt nur für applikationskonsistente Aufgaben des SnapCenter Servers (Applikation über VMDK). Diese Ebene schränkt die Fähigkeit von SnapCenter ein, bestimmte Storage-Vorgänge, beispielsweise Backups für Datenspeicher, auf einem bestimmten Storage-System durchzuführen.

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

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

## **Validierungs-Workflow für RBAC-Berechtigungen**

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



\*SCV=SnapCenter Plug-in for VMware vSphere

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



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

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von ONTAP können Sie den Zugriff auf bestimmte Storage-Systeme steuern und die Aktionen ausführen, die ein Benutzer auf diesen Storage-Systemen durchführen kann. Das SnapCenter VMware Plug-in nutzt die rollenbasierte Zugriffssteuerung von vCenter Server, die SnapCenter RBAC (bei Bedarf zur Unterstützung applikationsbasierter Vorgänge) und die ONTAP RBAC. So können Sie festlegen, welche SnapCenter Aufgaben ein bestimmter Benutzer auf Objekten in einem bestimmten Storage-System ausführen kann.

SnapCenter verwendet die von Ihnen festgelegten Anmeldedaten (Benutzername und Passwort) zur Authentifizierung jedes Storage-Systems und zur Bestimmung, welche Vorgänge auf diesem Storage-System

ausgeführt werden können. Das SnapCenter VMware Plug-in verwendet einen Satz an Anmeldedaten für jedes Storage-System. Diese Anmeldedaten bestimmen alle Aufgaben, die auf dem Storage-System ausgeführt werden können. Das heißt, die Anmeldedaten gelten für SnapCenter, nicht für einen einzelnen SnapCenter-Benutzer.

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

Jedem Speichersystem ist ein Satz von ONTAP-Berechtigungen zugeordnet.

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

- Sicherheit

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

- Audit-Informationen

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

- Benutzerfreundlichkeit

Sie können die Controller-Anmeldedaten an einer Stelle beibehalten.

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

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

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

Als Administrator können Sie diese Rollen den entsprechenden Benutzern zuweisen.

Das SnapCenter-VMware-Plug-in gibt diese Rollen bei jedem Neustart des vCenter-Webclientdienstes oder bei der Änderung der Installation an die Standardwerte (anfängliche Privilegien) zurück. Wenn Sie das SnapCenter VMware Plug-in aktualisieren, werden die vordefinierten Rollen automatisch aktualisiert, um mit dieser Version des Plug-ins zu arbeiten.

Sie können die vordefinierten Rollen in der vCenter-GUI sehen, indem Sie wie in der folgenden Tabelle dargestellt auf **Menü > Administration > Rollen** klicken.

Rolle	Beschreibung
SCV Administrator	Bietet alle nativen vCenter Server und SnapCenter-spezifischen Berechtigungen, die zur Ausführung aller SnapCenter Plug-ins für VMware vSphere Aufgaben erforderlich sind
SCV-Backup	Bereitstellung aller nativen vCenter Server und SnapCenter-spezifischen Berechtigungen, die für das Backup von vSphere Objekten (Virtual Machines und Datastores) erforderlich sind Der Benutzer hat auch Zugriff auf die Konfigurationsberechtigung. Der Benutzer kann keine Sicherungskopien wiederherstellen.
Wiederherstellung der SCV-Gastdatei	Bietet alle nativen vCenter Server und SnapCenter-spezifischen Berechtigungen, die für die Wiederherstellung von Gastdateien und Ordnern erforderlich sind Der Benutzer kann keine VMs oder VMDKs wiederherstellen.
SCV-Wiederherstellung	Bietet alle nativen vCenter Server und SnapCenter spezifischen Berechtigungen, die erforderlich sind, um vSphere Objekte, die über das SnapCenter VMware Plug-in gesichert wurden, wiederherzustellen sowie Gastdateien und Ordner wiederherzustellen. Der Benutzer hat auch Zugriff auf die Konfigurationsberechtigung. Der Benutzer kann vSphere-Objekte nicht sichern.
SCV-Ansicht	Bietet schreibgeschützten Zugriff auf alle SnapCenter VMware Plug-in-Backups, Ressourcengruppen und Richtlinien.

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

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



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

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

- Erstellen einer einzelnen Rolle.

["Administratorauthentifizierung und RBAC"](#)

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

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

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

Weitere Informationen finden Sie unter ["Mindestberechtigungen für ONTAP erforderlich"](#).

# Los geht's

## Implementierungsübersicht

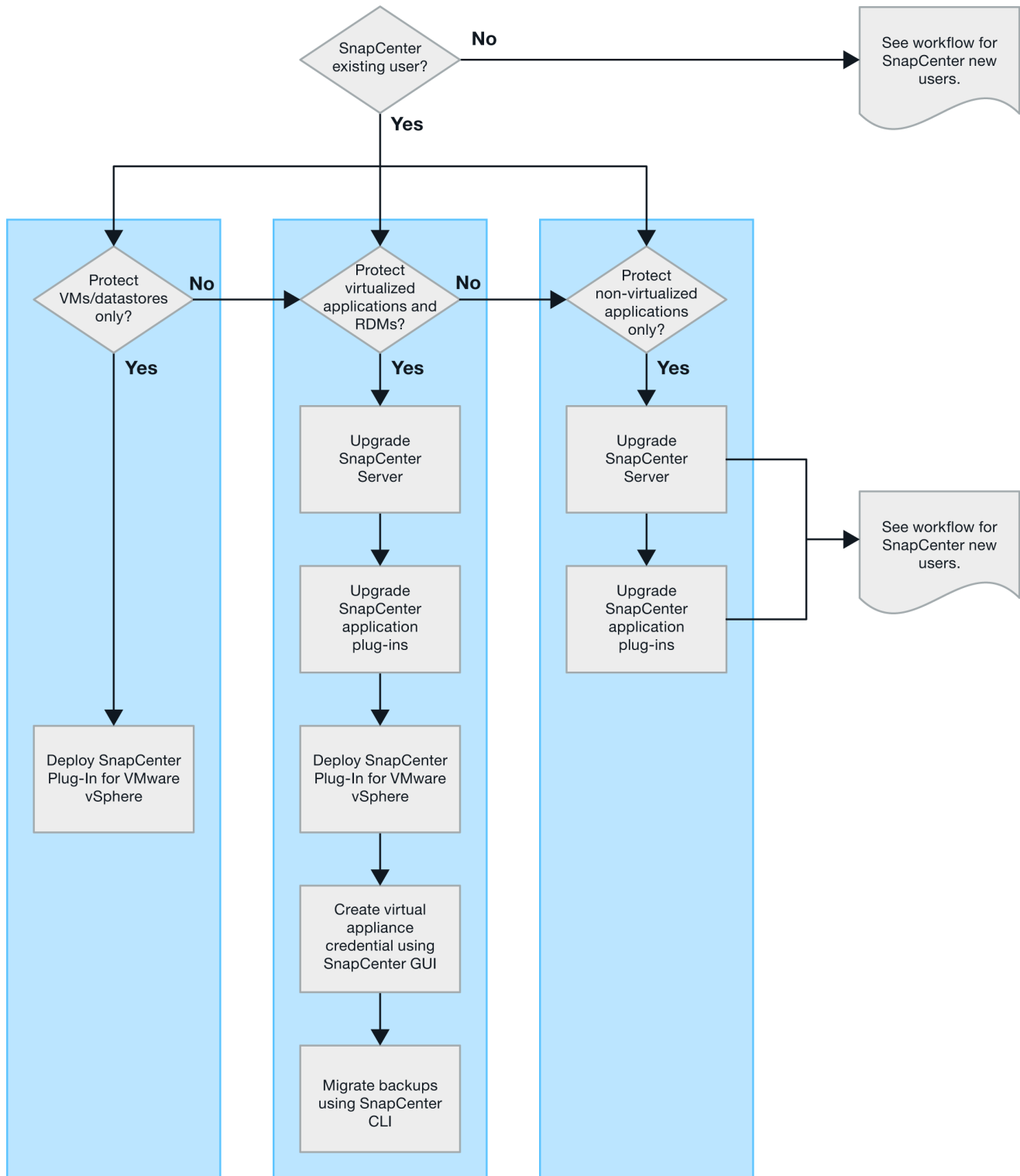
Um SnapCenter VMs, Datastores und applikationskonsistente Datenbanken auf virtualisierten Maschinen zu sichern, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren.

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

## Implementierungs-Workflow für vorhandene Benutzer

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





## Anforderungen für die Bereitstellung von SCV

### Implementierungsplanung und -Anforderungen

Vor der Bereitstellung der virtuellen Appliance sollten Sie die Implementierungsanforderungen kennen. Die Bereitstellungsanforderungen sind in den

folgenden Tabellen aufgeführt.

## Host-Anforderungen erfüllt

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

- Das SnapCenter VMware Plug-in wird als Linux VM implementiert, unabhängig davon, ob Sie das Plug-in verwenden, um Daten auf Windows-Systemen oder Linux-Systemen zu sichern.
- Sie sollten das SnapCenter VMware Plug-in auf dem vCenter Server bereitstellen.

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

- Das SnapCenter-VMware-Plug-in darf nicht in einem Ordner bereitgestellt werden, der einen Namen mit Sonderzeichen hat.

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

- Sie müssen für jeden vCenter Server eine separate, eindeutige Instanz des SnapCenter VMware Plug-ins implementieren und registrieren.
  - Jeder vCenter Server, ganz gleich, ob er sich im Linked-Modus befindet, muss mit einer separaten Instanz des SnapCenter VMware Plug-ins gekoppelt werden.
  - Jede Instanz des SnapCenter VMware Plug-ins muss als separate Linux VM implementiert werden.

Wenn Sie beispielsweise Backups von sechs verschiedenen Instanzen des vCenter Servers durchführen möchten, müssen Sie das SnapCenter VMware Plug-in auf sechs Hosts implementieren. Jeder vCenter Server muss mit einer eindeutigen Instanz des SnapCenter VMware Plug-ins gekoppelt werden.

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

Weitere Informationen finden Sie unter ["ONTAP Tools für VMware vSphere"](#)

Aktuelle Informationen zu unterstützten Versionen von ONTAP-Tools finden Sie unter ["NetApp Interoperabilitäts-Matrix-Tool"](#).

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

- Was unterstützt wird:

Erstellen von Ressourcengruppen

Erstellen von Backups ohne konsistente VMs

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

Anschließen und Trennen von VMDKs

Montage und Entmounten von Datenspeichern

Wiederherstellung von Gastdateien

- Was nicht unterstützt wird:

Erstellen von Backups mit der Konsistenz von VMs

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

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

## Lizenzanforderungen

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

## Softwaresupport

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

Element	Unterstützte Versionen
TLS auf dem SnapCenter-Server	1.2, 1.3 der SnapCenter-Server verwendet dies zur Kommunikation mit dem VMware Plug-in von SnapCenter für die Applikationssicherung über VMDK-Datensicherungsvorgänge.
VMware Application vStorage API für Array Integration (VAAI)	Das SnapCenter Plug-in für VMware vSphere nutzt diese Technologie zur Verbesserung der Performance von Restore-Vorgängen. Außerdem verbessert es die Performance in NFS Umgebungen.
ONTAP Tools für VMware	Das SnapCenter Plug-in für VMware vSphere verwendet dieses Tool zum Management von vVol Datastores (virtuelle VMware Volumes). Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitäts-Matrix-Tool"</a> .

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

### Platz- und Größenanforderungen

Element	Anforderungen
Betriebssystem	Linux
Minimale CPU-Anzahl	4 Kerne
Mind. RAM	Minimum: 12 GB empfohlen: 16 GB
Minimaler Festplattenspeicher für das SnapCenter Plug-in für VMware vSphere, Logs und MySQL Datenbank	100 GB

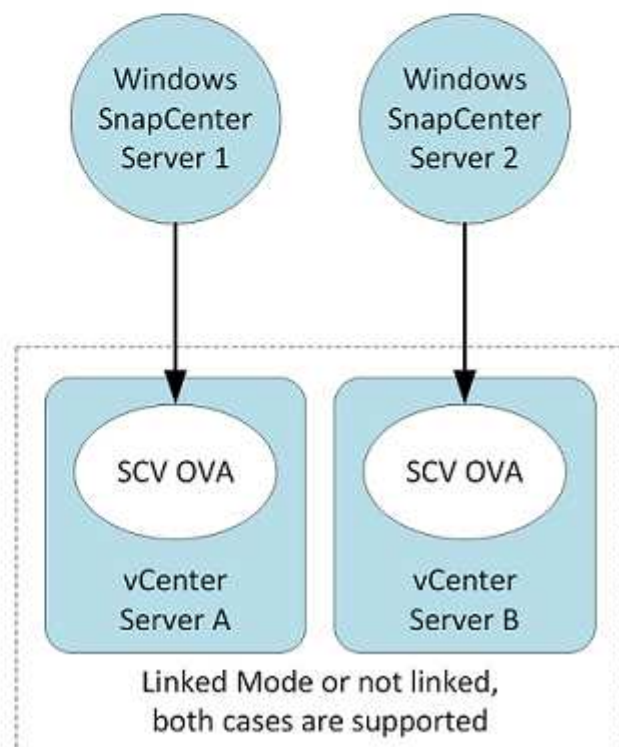
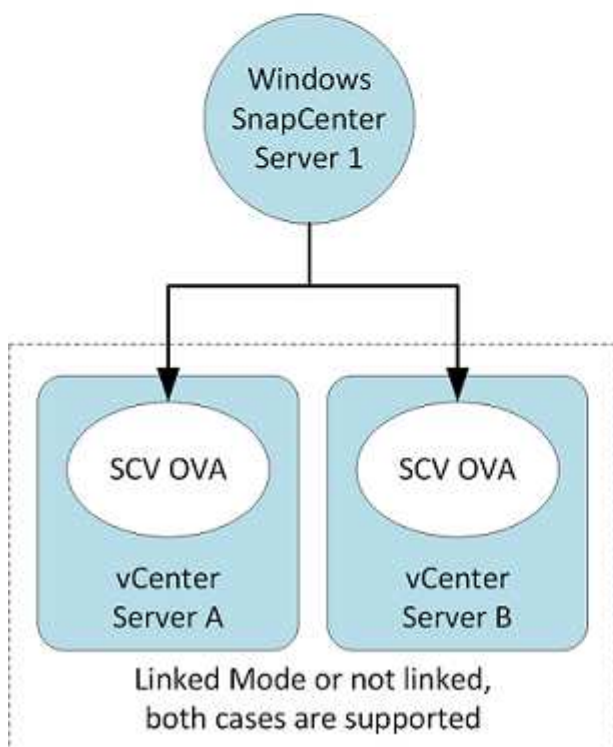
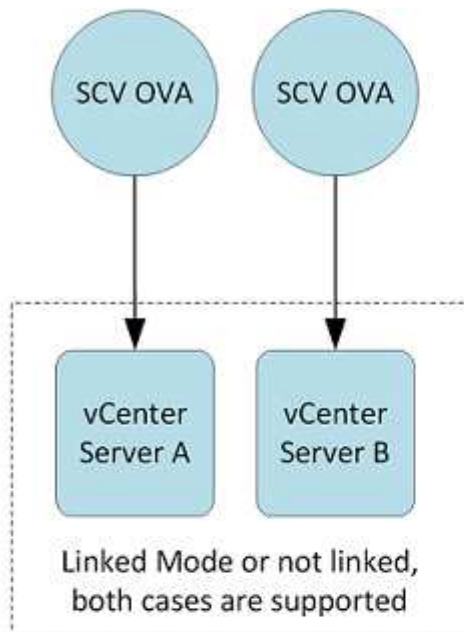
### Verbindungs- und Portanforderungen

Typ des Ports	Vorkonfigurierter Port
VMware ESXi Server-Port	443 (HTTPS), bidirektional die Funktion „Wiederherstellung von Gastdateien“ verwendet diesen Port.
SnapCenter Plug-in für VMware vSphere Port	8144 (HTTPS), der bidirektionale Port wird für die Kommunikation vom VMware vSphere Client und vom SnapCenter Server verwendet. 8080 bidirektional dieser Port wird zum Managen der virtuellen Appliance verwendet.  Hinweis: Es wird ein benutzerdefinierter Port zum Hinzufügen des SCV-Hosts zu SnapCenter unterstützt.
VMware vSphere vCenter Server Port	Sie müssen Port 443 verwenden, wenn Sie vVol VMs schützen.

Typ des Ports	Vorkonfigurierter Port
Storage-Cluster oder Storage-VM-Port	443 (HTTPS), bidirektional 80 (HTTP), bidirektional der Port wird für die Kommunikation zwischen der virtuellen Appliance und der Storage-VM oder dem Cluster, das die Storage-VM enthält, verwendet.

### Unterstützte Konfigurationen

Jede Plug-in-Instanz unterstützt nur einen vCenter Server. VCenter im verknüpften Modus werden unterstützt. Mehrere Plug-in-Instanzen können den gleichen SnapCenter-Server unterstützen, wie in der folgenden Abbildung dargestellt.



## RBAC-Berechtigungen erforderlich

Das vCenter-Administratorkonto muss über die erforderlichen vCenter-Berechtigungen verfügen, wie in der folgenden Tabelle aufgeführt.

So führen Sie diese Operation aus...	Sie müssen über diese vCenter-Berechtigungen verfügen...
Implementieren und registrieren Sie das SnapCenter Plug-in für VMware vSphere in vCenter	Erweiterung: Verlängerung registrieren
Aktualisieren oder entfernen Sie das SnapCenter Plug-in für VMware vSphere	Erweiterung <ul style="list-style-type: none"><li>• Erweiterung aktualisieren</li><li>• Erweiterung wird aufgehoben</li></ul>
Lassen Sie das in SnapCenter registrierte vCenter Credential-Benutzerkonto zu, um den Benutzerzugriff auf das SnapCenter Plug-in für VMware vSphere zu validieren	sessions.validate.session
Benutzern den Zugriff auf das SnapCenter Plug-in für VMware vSphere ermöglichen	SCV Administrator SCV Backup SCV Gastdateiwiederherstellung SCV Wiederherstellung SCV SCV Ansicht die Berechtigung muss im vCenter Root zugewiesen werden.

## AutoSupport

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

## ONTAP-Berechtigungen erforderlich

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



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

## Mindestberechtigungen für ONTAP erforderlich

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

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3 und höher
Cluster-ID wird angezeigt
Event Generate-AutoSupport-log
Jobverlauf zeigt Job Show Job Stop an

lun lun create lun delete lun igroup hinzufügen lun igroup erstellen lun igroup löschen lun igroup umbenennen  
lun igroup anzeigen lun Mapping add-Reporting-Nodes lun Mapping erstellen lun Mapping delete lun Mapping  
remove-Reporting-Nodes lun Mapping show lun modify lun move-in-Volume lun offline lun online lun  
persistent-reservat clear lun resize lun serial lun anzeigen

snapmirror list-Ziele snapmirror Policy add-rule snapmirror Policy modify-rule snapmirror Policy remove-rule  
snapmirror Policy show snapmirror restore SnapMirror show SnapMirror show-history snapmirror Update-Is-  
set snapmirror Update-Is-set

Version

Volume-Klon erstellen Volume-Klon zeigen Volume-Klon Teilung starten Volume-Klon-Teilung stoppen Volume  
erstellen Volume löschen Volume löschen Volume-Datei zerstören Volume-Datei Klon erstellen Volume-Datei  
zeigen-Nutzung Volume offline Volume online Volume ändern Volume-qtrees erstellen Volume qtrees löschen  
Volume-qtrees ändern Volume-qtrees zeigen Volume beschränken Volume zeigen Volume zeigen Volume  
zeigen Volume zeigen Volume beschränken Volume zeigen snapshot erstellen Volume Snapshot löschen  
Volume Snapshot ändern Volume Snapshot umbenennen Volume Snapshot wiederherstellen Volume  
Snapshot wiederherstellen Datei Volume Snapshot zeigen Volume unmounten

vserver cifs vserver cifs share vserver erstellen cifs share vserver löschen cifs shadowcopy show vserver cifs  
share show vserver cifs show vserver Export-Policy vserver Export-Policy vserver Export-Policy create  
vserver Export-Policy delete vserver Export-Policy rule create vserver Export-Policy rule show vserver Export-  
Policy show vserver iscsi vserver iscsi vserver iscsi Verbindung show vserver show Netzwerk Interface  
Netzwerkschnittstellen für Failover-Gruppen wird die Netzwerkschnittstelle angezeigt

### Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3 und höher erforderlich

vserver vServer Peer



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

### Weitere ONTAP-Informationen

- Wenn Sie ONTAP 8.2.x verwenden:

Sie müssen sich wie auf der Speicher-VM anmelden `vsadmin`, um über die entsprechenden Berechtigungen für das SnapCenter-Plug-in für VMware vSphere-Vorgänge zu verfügen.

- Wenn Sie ONTAP 8.3 und höher verwenden:

Sie müssen sich als oder mit einer Rolle anmelden `vsadmin`, die über die in den Tabellen oben aufgeführten Mindestberechtigungen verfügt.

- Sie müssen der Cluster-Administrator sein, um Benutzerrollen zu erstellen und zu managen. Sie können die Benutzer entweder der Cluster Storage VM oder der Storage VM zuordnen.
- Zur Verwendung der SnapMirror Business Continuity-Funktion (SM-BC) benötigen Sie ONTAP 9.12.1 oder höher.
- So verwenden Sie die tamperproof Snapshot (TPS)-Funktion:
  - Für SAN benötigen Sie ONTAP 9.13.1 und höher
  - Für NFS benötigen Sie ONTAP 9.12.1 und höher



Für ONTAP Version 9.11.1 und höher erfolgt die Kommunikation mit dem ONTAP Cluster über REST APIs. Für den ONTAP-Benutzer sollte die HTTP-Anwendung aktiviert sein. Falls jedoch Probleme mit ONTAP REST APIs auftreten, unterstützt der Konfigurationsschlüssel 'FORCE\_ZAPI' die Umschaltung auf den herkömmlichen ZAPI Workflow. Sie müssen möglicherweise diesen Schlüssel mit den Konfigurations-APIs hinzufügen oder aktualisieren und auf „wahr“ setzen. Siehe KB-Artikel, ["So bearbeiten Sie Konfigurationsparameter in SCV mithilfe der RestAPI"](#).

## Minimale vCenter-Berechtigungen erforderlich

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

### Erforderliche Berechtigungen für vCenter Admin-Rolle

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

### Erforderliche Berechtigungen für SnapCenter Plug-in für VMware vCenter

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

## Open Virtual Appliance (OVA) herunterladen

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



vCenter 7u1 und höher unterstützt.

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

### Schritte

1. So laden Sie das SnapCenter Plug-in für VMware herunter:
  - Melden Sie sich auf der NetApp Support-Website an (["https://mysupport.netapp.com/products/index.html"](https://mysupport.netapp.com/products/index.html)).
  - Wählen Sie aus der Liste der Produkte **SnapCenter Plug-in für VMware vSphere** und klicken Sie dann auf die Schaltfläche **Neueste Version herunterladen**.
  - Laden Sie das SnapCenter-Plug-in für VMware vSphere an einen beliebigen Speicherort herunter `.tar`.
2. Extrahieren Sie den Inhalt der tar-Datei. Die tar-Datei enthält den Ordner OVA und certs. Der Ordner „Zertifikaten“ enthält die Zertifikate „Stammanvertrauen“ und „Intermediate“.
3. Melden Sie sich mit dem vSphere Client am vCenter Server an.
4. Navigieren Sie zu **Administration > Zertifikate > Zertifikatverwaltung**.
5. Klicken Sie neben **Trusted Root Certificates** auf **Add**
  - Wechseln Sie zum Ordner *certs*.
  - Wählen Sie Root- und Intermediate-Zertifikate anvertrauen aus.
  - Installieren Sie jedes Zertifikat einzeln.
6. Die Zertifikate werden zu einem Panel unter **Trusted Root Certificates** hinzugefügt. Sobald die Zertifikate installiert sind, kann OVA überprüft und bereitgestellt werden.



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

## Implementieren Sie das SnapCenter Plug-in für VMware vSphere

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

### Bevor Sie beginnen

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



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

- Sie müssen die Implementierungsanforderungen 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 die SnapCenter-VMware-Plug-in-VM einrichten.

- Sie müssen das SnapCenter-Plug-in für die VMware vSphere .tar-Datei heruntergeladen haben.
- Sie benötigen die Anmeldedaten für Ihre vCenter Server-Instanz.
- Sie müssen über ein Zertifikat mit gültigen öffentlichen und privaten Schlüssel-Dateien verfügen. Weitere Informationen finden Sie in den Artikeln unter "[Storage-Zertifikatmanagement](#)" Abschnitt.
- Sie müssen alle Browser-Sitzungen des vSphere-Clients abgemeldet und geschlossen haben und den Browser-Cache gelöscht haben, um Probleme mit dem Browser-Cache während der Bereitstellung des SnapCenter-VMware-Plug-ins zu vermeiden.
- In vCenter müssen Sie Transport Layer Security (TLS) aktivieren. Lesen Sie die VMware-Dokumentation.
- Wenn Sie in anderen vCenter als in einem SnapCenter VMware Plug-in Backups durchführen möchten, müssen der ESXi Server, das SnapCenter VMware Plug-in und jedes vCenter mit derselben Zeit synchronisiert werden.
- Um VMs auf vVol Datastores zu schützen, müssen Sie zuerst ONTAP Tools für VMware vSphere implementieren. ONTAP Tools für VMware vSphere Version 9.10 und höher werden unterstützt. Durch die ONTAP Tools wird Storage auf ONTAP und im VMware Web-Client bereitgestellt und konfiguriert.

Implementieren Sie das SnapCenter VMware Plug-in in derselben Zeitzone wie vCenter. Die Backup-Zeitpläne werden in der Zeitzone ausgeführt, in der das SnapCenter VMware Plug-in implementiert wird. VCenter meldet Daten in der Zeitzone, in der sich vCenter befindet. Wenn sich das SnapCenter VMware Plug-in und vCenter in verschiedenen Zeitzonen befinden, sind die Daten im SnapCenter VMware Plug-in Dashboard möglicherweise nicht mit den Daten in den Berichten identisch.

### Schritte

1. Führen Sie für VMware vCenter 7.0.3 und neuere Versionen die Schritte in aus, um die Zertifikate in "[Open Virtual Appliance \(OVA\) herunterladen](#)" vCenter zu importieren.
2. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.



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

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

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

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

8. Wählen Sie auf der Seite **Select a Resource** die Ressource aus, auf der Sie die bereitgestellte VM-Vorlage ausführen möchten, und klicken Sie auf **Next**.
9. Überprüfen Sie auf der Seite **Details überprüfen** die .tar Vorlagendetails und klicken Sie auf **Weiter**.

10. Aktivieren Sie auf der Seite **Lizenzvereinbarungen** das Kontrollkästchen für **Ich akzeptiere alle Lizenzvereinbarungen**.
11. Legen Sie auf der Seite \* Storage auswählen\* fest, wo und wie die Dateien für die bereitgestellte OVF-Vorlage gespeichert werden sollen.
  - a. Wählen Sie das Festplattenformat für die VMDKs aus.
  - b. Wählen Sie eine VM-Speicherrichtlinie aus.

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

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

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

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

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

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

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

- b. Wählen Sie im Abschnitt **IP-Zuweisungs-Einstellungen** das erforderliche IP-Protokoll aus und klicken Sie dann auf **Weiter**.

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

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

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

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

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

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



Notieren Sie sich den Benutzernamen und das Kennwort, den Sie angeben. Sie müssen diese Anmeldedaten verwenden, wenn Sie die SnapCenter VMware Plug-in-Konfiguration später ändern möchten.

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

- d. Geben Sie unter **Setup-Netzwerkeigenschaften** den Hostnamen ein.

- i. Geben Sie im Abschnitt \* Setup IPv4 Network Properties\* die Netzwerkinformationen ein, z. B. IPv4-Adresse, IPv4-Netzmaske, IPv4-Gateway, IPv4 Primary DNS, IPv4 Secondary DNS, Und IPv4-Suchdomänen.

- ii. Geben Sie im Abschnitt \* IPv6-Netzwerkeigenschaften\* die Netzwerkinformationen ein, z. B. die IPv6-Adresse, IPv6-Netzmaske, IPv6 Gateway, IPv6 Primary DNS, IPv6 Secondary DNS, Und

IPv6-Suchdomänen.

Wählen Sie gegebenenfalls die IPv4- und/oder IPv6-Felder aus. Wenn Sie sowohl IPv4 als auch IPv6 verwenden, müssen Sie den primären DNS nur für eine von ihnen angeben.



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

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

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

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

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

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

15. Navigieren Sie zu der VM, auf der das SnapCenter-VMware-Plug-in bereitgestellt wurde, und klicken Sie dann auf die Registerkarte **Zusammenfassung** und dann auf das Feld **Einschalten**, um die virtuelle Appliance zu starten.

16. Während das SnapCenter VMware Plug-in eingeschaltet ist, klicken Sie mit der rechten Maustaste auf das implementierte SnapCenter VMware Plug-in, wählen Sie **Gastbetriebssystem** aus und klicken Sie dann auf **VMware Tools installieren**.

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

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

Auf dem Bildschirm wird die IP-Adresse angezeigt, an der das SnapCenter-VMware-Plug-in bereitgestellt wird. Notieren Sie sich die IP-Adresse. Sie müssen sich bei der Management-GUI des SnapCenter VMware Plug-ins anmelden, um Änderungen an der SnapCenter VMware Plug-in-Konfiguration vorzunehmen.

17. Melden Sie sich mithilfe der im Implementierungsbildschirm angezeigten IP-Adresse bei der Management-GUI des SnapCenter VMware-Plug-ins an und überprüfen Sie im Dashboard, ob das SnapCenter VMware-Plug-in erfolgreich mit vCenter verbunden und aktiviert ist.

Verwenden Sie das Format `https://<appliance-IP-address>:8080` für den Zugriff auf die Management-GUI.

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

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

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

### Nachdem Sie fertig sind

Sie sollten die erforderlichen "[Vorgänge nach der Implementierung](#)".

## Nach der Implementierung erforderliche Betriebsabläufe und Probleme

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

### Erforderliche Vorgänge nach der Implementierung

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

### Möglicherweise treten Bereitstellungsprobleme auf

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

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

1. Löschen Sie den Browser-Cache, und überprüfen Sie dann, ob die GUI ordnungsgemäß funktioniert.  
  
Wenn das Problem weiterhin besteht, starten Sie den VMware vSphere-Client-Service neu
2. Melden Sie sich bei vCenter an, klicken Sie dann in der Symbolleiste auf **Menü** und wählen Sie dann **SnapCenter Plug-in für VMware vSphere**.

## Management von Authentifizierungsfehlern

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

### Schritte

1. Melden Sie sich in der SnapCenter VMware Plug-in Management GUI mit dem Format `https://<appliance-IP-address>:8080` an. Verwenden Sie den Admin-Benutzernamen, das Passwort und die MFA-Token-Details für die Anmeldung. MFA-Token kann über die Wartungskonsole generiert werden.
2. Starten Sie den Dienst neu.

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

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

### Bevor Sie beginnen

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

### Über diese Aufgabe

- Sie registrieren SnapCenter-Plug-in für VMware vSphere mit SnapCenter-Server, indem Sie die SnapCenter-GUI verwenden, um einen Host vom Typ „vsphere“ hinzuzufügen.

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

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

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

### Schritte

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

Für dieses Feld...	Do this...
Host-Typ	Wählen Sie <b>vSphere</b> als Host-Typ aus.

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

5. Klicken Sie Auf **Absenden**.

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

6. Klicken Sie im linken Navigationsbereich auf **Einstellungen**, klicken Sie dann auf die Registerkarte **Credential** und wählen Sie dann **Hinzufügen**, um Anmeldeinformationen für die virtuelle Appliance hinzuzufügen.

7. Geben Sie die Anmeldeinformationen an, die während der Bereitstellung des SnapCenter Plug-ins für VMware vSphere angegeben wurden.



Sie müssen Linux für das Feld Authentifizierung auswählen.

#### Nachdem Sie fertig sind

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

## Melden Sie sich beim SnapCenter VMware vSphere-Client an

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

#### Bevor Sie beginnen

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

#### Schritte

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



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

3. Klicken Sie auf der Seite **VMware vSphere Client** in der Symbolleiste auf Menü und wählen Sie dann **SnapCenter Plug-in für VMware vSphere**.

# Schnellstart

## Überblick

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

Bevor Sie beginnen, siehe "[Implementierungsplanung und -Anforderungen](#)".

## Implementieren Sie das SnapCenter Plug-in für VMware vSphere

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

1. Führen Sie für VMware vCenter 7.0.3 und neuere Versionen die Schritte in aus, um die Zertifikate in "[Open Virtual Appliance \(OVA\) herunterladen](#)" vCenter zu importieren.
2. Navigieren Sie in Ihrem Browser zu VMware vSphere vCenter.




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

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

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



Auf dieser Assistentenseite...	Do this...
Wählen Sie Storage aus	Legen Sie fest, wo und wie die Dateien für die bereitgestellte OVF-Vorlage gespeichert werden.
Wählen Sie Netzwerke aus	Wählen Sie ein Quellnetzwerk aus, und ordnen Sie es einem Zielnetzwerk zu.
Vorlage anpassen	<p>Geben Sie unter <b>Registrieren Sie sich bei vorhandenem vCenter</b> die vCenter-Anmeldedaten ein. Geben Sie in <b>Create SnapCenter Plug-in for VMware vSphere Credentials</b> das SnapCenter Plug-in für VMware vSphere ein.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Notieren Sie sich den Benutzernamen und das Kennwort, den Sie angeben. Sie müssen diese Anmeldedaten verwenden, wenn Sie die Konfiguration des SnapCenter Plug-ins für VMware vSphere zu einem späteren Zeitpunkt ändern möchten.</p> </div> <p>Geben Sie unter * Netzwerkeigenschaften einrichten* die Netzwerkinformationen ein. Wählen Sie unter <b>Setup Datum und Uhrzeit</b> die Zeitzone aus, in der sich das vCenter befindet.</p>
Fertig	Überprüfen Sie die Seite und klicken Sie auf <b>Fertig stellen</b> .



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

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

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

Auf dem Bildschirm wird die IP-Adresse angezeigt, an der das SnapCenter-VMware-Plug-in bereitgestellt wird. Notieren Sie sich die IP-Adresse. Sie müssen sich bei der Management-GUI des SnapCenter VMware Plug-ins anmelden, um Änderungen an der SnapCenter VMware Plug-in-Konfiguration vorzunehmen.

8. Melden Sie sich über die im Implementierungsassistenten angegebene IP-Adresse bei der Management-GUI von SnapCenter VMware-Plug-in an. Überprüfen Sie anschließend im Dashboard, ob das SnapCenter VMware-Plug-in erfolgreich mit vCenter verbunden und aktiviert ist.

Verwenden Sie das Format `https://<appliance-IP-address>:8080` für den Zugriff auf die Management-GUI.

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

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

## Erweitern Sie Ihren Storage

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

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

## Backup-Richtlinien erstellen

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


1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Richtlinien** und wählen Sie dann **Neue Richtlinie** aus.
2. Geben Sie auf der Seite **Neue Sicherungsrichtlinie** die Konfigurationsdaten der Richtlinie ein und klicken Sie dann auf **Hinzufügen**.

## Erstellen von Ressourcengruppen

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

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Ressourcengruppen** und wählen Sie dann **Erstellen**.
2. Geben Sie auf jeder Seite des Assistenten zum Erstellen von Ressourcengruppen die erforderlichen Informationen ein, wählen Sie VMs und Datenspeicher aus, die in die Ressourcengruppe aufgenommen werden sollen, und wählen Sie dann die Backup-Richtlinien aus, die auf die Ressourcengruppe angewendet werden sollen, und geben Sie den Backup-Zeitplan an.

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

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

# Monitoring und Reporting

## Zeigt Statusinformationen an

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

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**, wählen Sie einen vCenter-Server aus, und klicken Sie dann im Dashboard auf die Registerkarte **Status**.
2. Zeigen Sie eine Übersicht Statusinformationen an, oder klicken Sie auf einen Link, um weitere Informationen zu erhalten, wie in der folgenden Tabelle aufgeführt.

Dieses Dashboard-Feld...	Zeigt die folgenden Informationen an...
Zuletzt verwendete Job-Aktivitäten	Die drei bis fünf letzten Backup-, Restore- und Mount-Aufgaben. <ul style="list-style-type: none"><li>• Klicken Sie auf eine Job-ID, um weitere Details zu diesem Job anzuzeigen.</li><li>• Klicken Sie auf <b>Alle anzeigen</b>, um zur Registerkarte Job Monitor zu gelangen, um weitere Details zu allen Jobs anzuzeigen.</li></ul>
Jobs	Eine Anzahl von Jobs (Backup, Restore und Mount), die innerhalb des ausgewählten Zeitfensters ausgeführt werden. Bewegen Sie den Cursor über einen Abschnitt des Diagramms, um weitere Details zu dieser Kategorie anzuzeigen.

Dieses Dashboard-Feld...	Zeigt die folgenden Informationen an...
Aktuelle Zusammenfassung Des Schutzes	<p>Zusammenfassungen des Datensicherungsstatus von primären und sekundären VMs oder Datastores im ausgewählten Zeitfenster.</p> <ul style="list-style-type: none"> <li>• Klicken Sie auf das Dropdown-Menü, um <b>VMs</b> oder <b>Datastores</b> auszuwählen.</li> <li>• Wählen Sie als Sekundärspeicher <b>SnapVault</b> oder <b>SnapMirror</b> aus.</li> <li>• Bewegen Sie den Mauszeiger über einen Abschnitt eines Diagramms, um die Anzahl der VMs oder Datastores in dieser Kategorie anzuzeigen. In der Kategorie erfolgreich wird für jede Ressource das aktuellste Backup aufgeführt.</li> <li>• Sie können das Zeitfenster ändern, indem Sie die Konfigurationsdatei bearbeiten. Der Standardwert ist 7 Tage. Weitere Informationen finden Sie unter "<a href="#">Passen Sie Ihre Konfiguration an</a>".</li> <li>• Interne Zähler werden nach jedem primären oder sekundären Backup aktualisiert. Die Dashboard-Kachel wird alle sechs Stunden aktualisiert. Die Aktualisierungszeit kann nicht geändert werden. Hinweis: Wenn Sie eine Mirror-Vault-Schutzrichtlinie verwenden, werden die Zähler für die Sicherungszusammenfassung im SnapVault-Übersichtsdiagramm und nicht im SnapMirror Diagramm angezeigt.</li> </ul>
Konfiguration	Gesamtzahl der jeden Objekttyp, die vom SnapCenter Plug-in für VMware vSphere gemanagt wird

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

## Überwachen von Jobs

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

### Schritte

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

Wenn das Dashboard keine Jobinformationen anzeigt, lesen Sie die ["KB-Artikel: SnapCenter vSphere-Client-Dashboard zeigt keine Jobs an"](#).

## Job-Protokolle herunterladen

Sie können die Jobprotokolle von der Registerkarte Job Monitor auf dem Dashboard des SnapCenter VMware vSphere Clients herunterladen.

Wenn bei der Verwendung des VMware vSphere-Clients ein unerwartetes Verhalten auftritt, können Sie

mithilfe der Protokolldateien die Ursache identifizieren und das Problem lösen.



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

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**, wählen Sie einen vCenter-Server aus und klicken Sie dann im Dashboard-Bereich auf die Registerkarte **Job Monitor**.
2. Wählen Sie in der Titelleiste des Job Monitors das Download-Symbol aus.

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

Sie können auch auf einen Job doppelklicken, um auf das Fenster Job Details zuzugreifen und dann auf **Job Logs herunterladen** klicken.

### Ergebnis

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

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

## Aufrufen von Berichten

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

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

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**, wählen Sie einen vCenter-Server aus und klicken Sie dann auf die Registerkarte **Berichte**.
2. Für Backup-Berichte können Sie Folgendes tun:

- a. Ändern Sie den Bericht

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

- b. Erstellen eines detaillierten Berichts

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

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

Sie können auch auf das Download-Symbol klicken, um Plug-in-Protokolle herunterzuladen.

## Berichtstypen vom VMware vSphere Client

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



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

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

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

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

## Generieren Sie ein Support Bundle aus dem SnapCenter Plug-in für VMware vSphere

### Bevor Sie beginnen

Um sich beim SnapCenter Plug-in für die Management-GUI von VMware vSphere anzumelden, müssen Sie die IP-Adresse und die Anmeldedaten kennen. Sie müssen



auch das MFA-Token notieren, das von der Wartungskonsole generiert wurde.

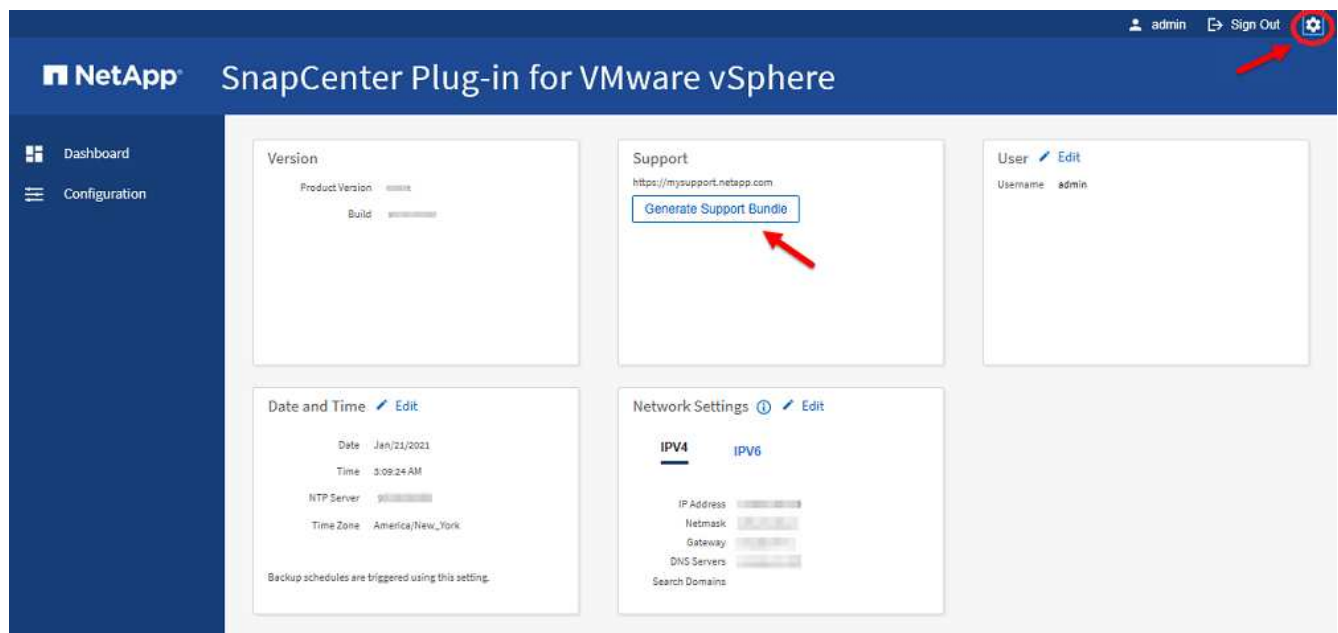
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-VMware-Plug-ins angezeigt.
- Verwenden Sie die Login-Anmeldedaten, die bei der Bereitstellung des SnapCenter VMware Plug-ins oder einer späteren Änderung zur Verfügung gestellt werden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

### Schritte

1. Melden Sie sich im SnapCenter Plug-in für VMware vSphere an.

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

2. Klicken Sie in der oberen Symbolleiste auf das Symbol Einstellungen.



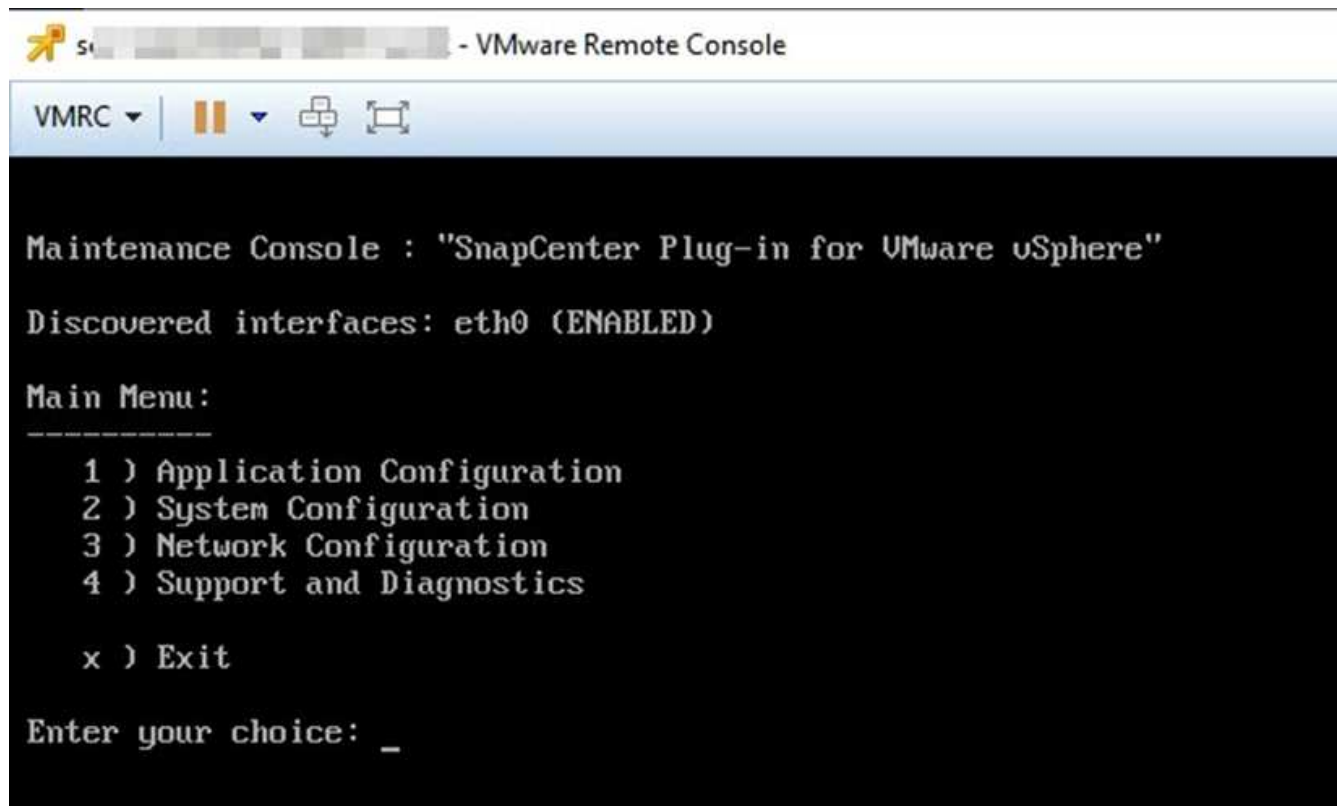
3. Klicken Sie auf der Seite **Einstellungen** im Abschnitt **Support** auf **Support** Paket generieren.
4. Nachdem das Support Bundle generiert wurde, klicken Sie auf den Link, der zur Verfügung steht, um das Bundle auf NetApp herunterzuladen.

## Generieren Sie ein Support-Bundle über die Wartungskonsole

### Schritte

1. Wählen Sie auf dem VMware vSphere-Client die VM aus, auf der sich das SnapCenter VMware Plug-in befindet.
2. Klicken Sie mit der rechten Maustaste auf die VM und anschließend auf der Registerkarte **Zusammenfassung** der virtuellen Appliance auf **Remote-Konsole starten** oder **Webkonsole starten**, um ein Fenster der Wartungskonsole zu öffnen und sich dann anzumelden.

Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter "[Öffnen Sie die Wartungskonsole](#)".



```
VMware Remote Console
VMRC | [Pause] [Fullscreen]
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
Main Menu:
-----
 1 ) Application Configuration
 2 ) System Configuration
 3 ) Network Configuration
 4 ) Support and Diagnostics

 x ) Exit

Enter your choice: _
```

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

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

## Prüfprotokolle

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

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

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

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

Die Standardkonfigurationen der Audit-Dateien sind:

- Die verwendete Audit-Log-Datei kann auf maximal 10 MB anwachsen

- Es werden maximal 10 Audit-Log-Dateien aufbewahrt

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

Status	Beschreibung
MANIPULIERT	Der Inhalt der Audit-Log-Datei wird geändert
NORMAL	Audit-Log-Datei wurde nicht geändert
ROLLOVER LÖSCHEN	- Audit-Log-Datei wird auf der Grundlage der Aufbewahrung gelöscht - standardmäßig werden nur 10 Dateien beibehalten
UNERWARTETES LÖSCHEN	Audit-Log-Datei wird gelöscht
AKTIV	- Audit-Log-Datei wird verwendet - gilt nur für audit.log

Die Ereignisse lassen sich in drei Hauptkategorien einteilen:

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

## Ereignisse Auf Der Datensicherung

Die Ressourcen in SCV sind:

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

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

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

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

## Ereignisse Der Wartungskonsole

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

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

## Ereignisse Der Admin-Konsole

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

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

## Konfigurieren Sie Syslog-Server

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

### Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

### Über diese Aufgabe

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

### Schritte

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

## Ändern Sie die Einstellungen des Überwachungsprotokolls

Sie können die Standardkonfigurationen der Protokolleinstellungen ändern.

### Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

### Über diese Aufgabe

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

### Schritte

1. Melden Sie sich beim SnapCenter-Plug-in für VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen > Audit-Protokolle > Einstellungen**.
3. Geben Sie im Bereich **Audit Log Settings** die maximale Anzahl an Audit Log Files und die maximale Größe der Audit Log Files ein.

# Storage-Management

## Erweitern Sie Ihren Storage

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

- Welche GUI verwendet werden soll

Verwenden Sie den VMware vSphere Client, um Storage hinzuzufügen.

- Große LUNs

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

- VMware Virtual Volumes (VVols)

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

Weitere Informationen finden Sie unter ["ONTAP Tools für VMware vSphere"](#)

### Bevor Sie beginnen

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

### Über diese Aufgabe

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



Wenn Sie das SnapCenter VMware Plug-in zur Unterstützung applikationsbasierter Backups auf VMDKs verwenden, müssen Sie über die Benutzeroberfläche von SnapCenter die Details zur Storage-Authentifizierung eingeben und die Speichersysteme registrieren.

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

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

Wenn Sie eine Storage-VM mit einem Namen hinzufügen, der nicht zur Management-LIF auflöst, schlagen geplante Backup-Jobs fehl, da das Plug-in keine Datenspeicher oder Volumes auf dieser Storage-VM finden kann. Falls dies der Fall ist, fügen Sie entweder die Storage VM zur SnapCenter hinzu und geben Sie die Management-LIF an, oder fügen Sie einen Cluster hinzu, der die Storage-VM enthält, und geben Sie die Cluster-Management-LIF an.

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

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Storage Systems**.
2. Wählen Sie auf der Seite Speichersysteme die Option **Hinzufügen** aus.
3. Geben Sie im Assistenten \* Storage System\* die grundlegenden Speicher-VM oder Cluster-Informationen ein, wie in der folgenden Tabelle aufgeführt:

Für dieses Feld...	Do this...
Storage-System	Geben Sie die IP-Adresse eines Storage-Clusters oder einer Storage-VM des FQDN oder Management LIF ein. Das SnapCenter VMware Plug-in unterstützt nicht mehrere Storage-VMs mit demselben Namen in verschiedenen Clustern.
Authentifizierungsmethode	Wählen Sie entweder Anmeldeinformationen oder Zertifikat aus. Es werden zwei Arten von Zertifikaten unterstützt: "KANN signiertes Zertifikat" - - "Selbstsigniertes Zertifikat"
Benutzername	Dieses Feld wird angezeigt, wenn Sie Anmeldeinformationen als Authentifizierungsmethode auswählen. Geben Sie den ONTAP-Benutzernamen ein, mit dem Sie sich bei der Storage-VM oder beim Cluster anmelden.
Passwort	Dieses Feld wird angezeigt, wenn Sie Anmeldeinformationen als Authentifizierungsmethode auswählen. Geben Sie das Passwort für die Storage-VM oder das Cluster-Login ein.
Zertifikat	Dieses Feld wird angezeigt, wenn Sie Zertifikat als Authentifizierungsmethode auswählen. Wählen Sie die Zertifikatdatei aus.
Privater Schlüssel	Dieses Feld wird angezeigt, wenn Sie Zertifikat als Authentifizierungsmethode auswählen. Wählen Sie die Datei mit dem privaten Schlüssel aus.
Protokoll	Wählen Sie das Storage-Protokoll aus.
Port	Port, den das Speichersystem akzeptiert. - 443 für HTTPS-Verbindung - 80 für HTTP-Verbindung
Zeitüberschreitung	Geben Sie die Anzahl der Sekunden ein, die das SnapCenter-VMware-Plug-in warten soll, bevor Sie den Vorgang absetzen. Die Standardeinstellung ist 60 Sekunden.

Für dieses Feld...	Do this...
Bevorzugte IP	Wenn die Storage VM über mehrere Management-IP-Adressen verfügt, aktivieren Sie dieses Kontrollkästchen und geben Sie die IP-Adresse ein, die das SnapCenter-VMware-Plug-in verwenden soll. <b>Hinweis:</b> Verwenden Sie keine eckigen Klammern ([ ]), wenn Sie die IP-Adresse eingeben.
Einstellungen für Ereignismanagement-System (EMS) und AutoSupport	Wenn Sie EMS-Meldungen an das Syslog-Speichersystem senden möchten oder wenn Sie AutoSupport-Meldungen für den angewendeten Schutz, abgeschlossene Wiederherstellungsvorgänge oder fehlgeschlagene Vorgänge an das Speichersystem senden möchten, aktivieren Sie das entsprechende Kontrollkästchen. Aktivieren Sie das Kontrollkästchen <b>AutoSupport-Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden</b> und das Kontrollkästchen * SnapCenter-Serverereignisse in syslog*, um AutoSupport-Benachrichtigungen zu aktivieren.
Protokollieren von SnapCenter-Serverereignissen im Syslog	Aktivieren Sie das Kontrollkästchen, um Ereignisse für das SnapCenter VMware Plug-in zu protokollieren.
AutoSupport-Benachrichtigung für fehlgeschlagenen Vorgang an das Speichersystem senden	Aktivieren Sie das Kontrollkästchen, wenn AutoSupport-Benachrichtigungen für fehlgeschlagene Datensicherungsaufträge angezeigt werden sollen. Sie müssen auch AutoSupport auf der Storage VM aktivieren und die AutoSupport E-Mail-Einstellungen konfigurieren.

#### 4. Klicken Sie Auf **Hinzufügen**.

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

## Management von Storage-Systemen

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

### Ändern Sie Storage-VMs

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

Wenn Sie eine Storage-VM ändern, die automatisch als Teil eines Clusters hinzugefügt wurde (manchmal auch als implizite Storage-VM bezeichnet), dann ändert sich diese Storage-VM in eine explizite Storage-VM und



kann separat gelöscht werden, ohne die restlichen Storage-VMs in diesem Cluster zu ändern. Auf der Seite Storage Systems wird der Benutzername als N/A angezeigt, wenn die Authentifizierungsmethode über das Zertifikat erfolgt. Benutzernamen werden nur für explizite Speicher-VMs in der Cluster-Liste angezeigt und lassen das ExplicitSVM-Flag auf true gesetzt. Alle Storage-VMs werden immer unter dem zugehörigen Cluster aufgeführt.



Wenn Sie Storage-VMs für applikationsbasierte Datensicherungsvorgänge über die SnapCenter GUI hinzugefügt haben, müssen Sie diese Storage-VMs über dieselbe GUI ändern.

### Schritte

1. Klicken Sie im linken Navigator-Fenster des SCV-Plug-ins auf **Speichersysteme**.
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 klicken Sie dann auf **Aktualisieren**, um die Änderungen anzuwenden.

## Edit Storage System ✕

Storage System

Platform

Authentication Method  Credentials  Certificate

Username

Password

Protocol

Port

Timeout  Seconds

Preferred IP

Event Management System(EMS) & AutoSupport Setting

Log Snapcenter server events to syslog

Send AutoSupport Notification for failed operation to storage system

## Storage-VMs entfernen

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



Wenn Sie Storage-VMs für applikationsbasierte Datensicherungsvorgänge über die SnapCenter GUI hinzugefügt haben, müssen Sie diese Storage-VMs über dieselbe GUI ändern.

### Bevor Sie beginnen

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

### Über diese Aufgabe

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

### Schritte

1. Klicken Sie im linken Navigator-Fenster des SCV-Plug-ins auf **Speichersysteme**.
2. Wählen Sie auf der Seite **Storage Systems** die zu entfernenden Speicher-VM aus und klicken Sie dann auf **Löschen**.
3. Aktivieren Sie im Bestätigungsfeld **Speichersystem entfernen** das Kontrollkästchen für **Speichersysteme löschen** und klicken Sie dann zur Bestätigung auf **Ja**. **Hinweis:** nur ESXi 7.0U1 und neuere Versionen werden unterstützt.

["Starten Sie den VMware vSphere-Client-Service neu"](#).

## Ändern Sie die konfigurierte Storage-Zeitüberschreitung

Auch wenn Backups in der Vergangenheit erfolgreich ausgeführt wurden, werden sie möglicherweise fehlschlagen, wenn das SnapCenter Plug-in für VMware vSphere auf das Storage-System warten muss, über dem konfigurierten Zeitraum der Zeitüberschreitung. Wenn diese Bedingung eintritt, können Sie die konfigurierte Zeitüberschreitung erhöhen.

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

### Schritte

1. Klicken Sie im VMware vSphere-Client auf **Storage-Systeme**.
2. Wählen Sie auf der Seite Speichersysteme das zu bearbeitendes Speichersystem aus und klicken Sie auf **Bearbeiten**.
3. Erhöhen Sie im Feld Timeout die Anzahl der Sekunden.



Für große Umgebungen wird 180 Sekunden empfohlen.

# Sichern von Daten

## Datensicherungs-Workflow

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

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

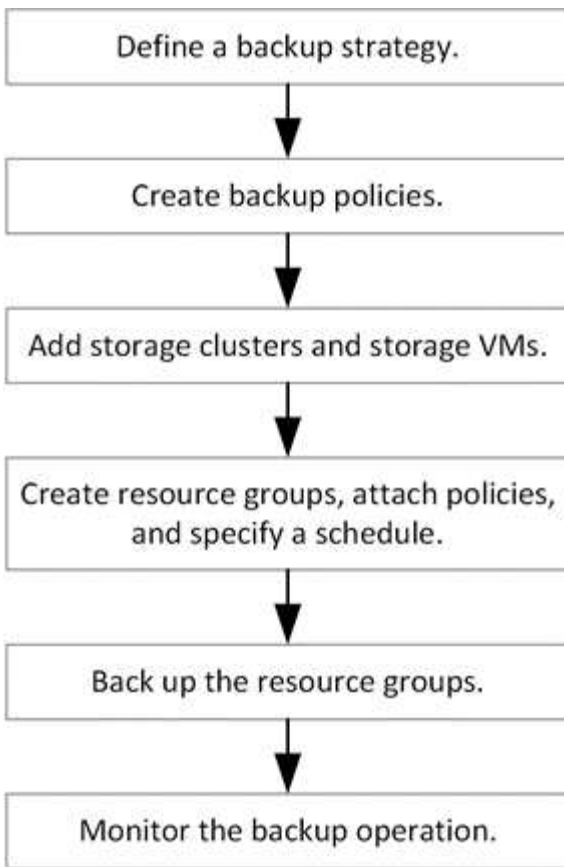
Backup- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressourcengruppe durchgeführt werden.

Überprüfen Sie die Informationen zum Funktionen des SnapCenter VMware Plug-ins und dessen Unterstützung. ["Implementierungsplanung und -Anforderungen"](#)

In MetroCluster Konfigurationen:

- Das SnapCenter VMware Plug-in kann nach einem Failover möglicherweise keine Sicherheitsbeziehung erkennen. Siehe ["KB-Artikel: Kann die SnapMirror oder SnapVault-Beziehung nach dem MetroCluster Failover nicht erkennen"](#).
- Wenn Backups nach Umschaltung/Wechsel zurück mit dem Fehler für NFS- und VMFS-VMs fehlschlagen `Unable to discover resources on SCV: <xxx>...`, starten Sie die SnapCenter-Services von der Wartungskonsole aus neu.

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



## Zeigen Sie VM- und Datastore-Backups an

Wenn Sie das Backup oder die Wiederherstellung einer VM oder eines Datenspeichers vorbereiten, sollten Sie eventuell alle Backups sehen, die für die Ressource verfügbar sind, und die Details zu diesen Backups anzeigen.

### Über diese Aufgabe

Das Durchsuchen von großen Dateordnern, z. B. 10k-Dateordnern, kann beim ersten Mal ein oder mehrere Minuten dauern. Nachfolgende Browsersitzungen nehmen weniger Zeit in Anspruch.

### Schritte

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

Name	Status	Locations	Snapshot Lock Expiration	Created Time	Mounted	Policy	VMware Snapshot
TPS_vol_10-05-2023_140...	Completed	Primary & Secondary	10/6/2023 11:33:57 PM	10/5/2023 11:33:58 PM	No	TPS_vol1	No
withoutexpiry_10-05-2023_...	Completed	Primary & Secondary	-	10/5/2023 11:27:44 PM	No	ondemandvaut	No
withoutexpiry_10-05-2023_...	Completed	Primary & Secondary	-	10/5/2023 11:25:18 PM	No	ondemandvaut	No
TPS_vol_10-05-2023_131...	Completed	Primary & Secondary	10/6/2023 11:09:26 PM	10/5/2023 11:09:28 PM	No	TPS_vol1	No
TPS_vol_10-05-2023_131...	Completed	Primary	10/6/2023 10:40:25 PM	10/5/2023 10:40:26 PM	No	TPS_vol1	No
withoutexpiry_10-04-2023_12...	Completed	Primary	10/6/2023 10:19:48 PM	10/4/2023 10:19:50 PM	No	TPS_vol1	No
withoutexpiry_10-03-2023_12...	Completed	Primary	10/4/2023 10:09:05 PM	10/3/2023 10:09:07 PM	No	TPS_vol1	No
withoutexpiry_09-28-2023_...	Completed	Primary	-	9/27/2023 6:17:15 AM	No	ondemandvaut	No
withoutexpiry_09-25-2023_...	Completed	Primary	-	9/25/2023 10:39:54 PM	No	ondemandvaut	No

2. Klicken Sie auf das Backup, das Sie anzeigen möchten.

# Erstellen von Backup-Richtlinien für VMs und Datastores

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

## Bevor Sie beginnen

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

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

Informationen darüber, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie unter ["SnapCenter-Informationen zur Nutzung der rollenbasierten Zugriffssteuerung"](#).

- Wenn Sie VM-konsistente Backups wünschen, müssen VMware Tools installiert und ausgeführt werden. Um VMs stillzulegen, sind VMware Tools erforderlich. VM-konsistente Backups werden für vVol VMs nicht unterstützt.
- SnapMirror Business Continuity (SM-BC) sorgt dafür, dass die Business Services auch bei einem vollständigen Standortausfall weiterlaufen und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen.



SM-BC wird nur für VMFS Datastores unterstützt.

Zum Schutz eines VMFS-Datenspeichers in einer SM-BC-Bereitstellung müssen Sie als SnapCenter-Administrator Folgendes tun:

- Konfigurieren Sie Cluster und Mediator wie im technischen Bericht beschrieben: ["TR-4878: SnapMirror Business Continuity"](#).
- Fügen Sie das dem VMFS-Datastore zugeordnete Volume zur Konsistenzgruppe hinzu und erstellen Sie mithilfe der *AutomatedFailOver* -Schutzrichtlinie zwischen zwei ONTAP-Storage-Systemen eine Datensicherungsbeziehung.

## Über diese Aufgabe

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

## Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Richtlinien**.
2. Wählen Sie auf der Seite **Policies Create** aus, um den Assistenten zu starten.
3. Wählen Sie auf der Seite **New Backup Policy** den vCenter Server aus, der die Richtlinie verwendet, und geben Sie dann den Namen der Richtlinie und eine Beschreibung ein.

- Verknüpfter Modus

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

- Nicht unterstützte Zeichen

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

Ein Unterstrich ( \_ ) ist zulässig.

4. Geben Sie die Frequenzeinstellungen an.

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

5. Aktivieren Sie das Kontrollkästchen **Sperrzeitraum**, um die Snapshot-Sperrung zu aktivieren. Sie können die Sperrfrist für Snapshots als Tage/Monate/Jahre auswählen.
6. Legen Sie die Aufbewahrungseinstellungen fest.








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





Der maximale Aufbewahrungswert sind 1018 Backups für Ressourcen auf ONTAP 9.4 oder höher und 254 Backups für Ressourcen auf ONTAP 9.3 oder früher. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Das gilt auch für das Spanning von Datenspeichern. Wenn ein Spanning Datastore Ressourcen sowohl auf ONTAP 9.3 als auch früher sowie auf ONTAP 9.4 und höher enthält, müssen Sie den Aufbewahrungswert unter 254 festlegen.


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

Für dieses Feld...	Do this...
Aktualisierung von SnapMirror nach dem Backup	<p>Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen, das über eine SnapMirror Beziehung zum primären Backup Volume verfügt. Wenn ein Volume mit einer Mirror-Vault-Beziehung konfiguriert ist, müssen Sie nur die Option <b>Update SnapVault after Backup</b> auswählen, wenn Sie Backups auf die Mirror-Vault Ziele kopieren möchten.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Diese Option wird für Datastores in FlexGroup Volumes im SnapCenter Plug-in für VMware vSphere 4.5 und höher unterstützt.</p> <p> Zum Schutz des VMFS-Datstore auf der SM-BC-Bereitstellung müssen Sie die im Abschnitt <i>before you begin</i> genannten Voraussetzungen erfüllen und <b>Update SnapMirror after Backup</b> aktivieren.</p> </div>
SnapVault nach Backup aktualisieren	<p>Wählen Sie diese Option aus, um Disk-to-Disk Backup-Replikation auf einem anderen Volume mit einer SnapVault-Beziehung zum primären Backup Volume durchzuführen.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Wenn ein Volume mit einer Mirror-Vault-Beziehung konfiguriert ist, müssen Sie nur diese Option auswählen, wenn Sie Backups auf die Mirror-Vault Ziele kopieren möchten.</p> <p> Diese Option wird für Datastores in FlexGroup Volumes im SnapCenter Plug-in für VMware vSphere 4.5 und höher unterstützt.</p> </div>
Snapshot-Etikett	<p>Geben Sie eine optionale, benutzerdefinierte Beschriftung ein, die zu den mit dieser Richtlinie erstellten SnapVault und SnapMirror Snapshots hinzugefügt werden soll. Das Snapshot-Label hilft, mit dieser Richtlinie erstellte Snapshots von anderen Snapshots auf dem sekundären Storage-System zu unterscheiden.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Für Snapshot-Etiketten sind maximal 31 Zeichen zulässig.</p> </div>

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

Für dieses Feld...	Do this...
VM-Konsistenz	<p>Aktivieren Sie dieses Kontrollkästchen, um die VMs stillzulegen und jedes Mal, wenn der Backup-Job ausgeführt wird, einen VMware-Snapshot zu erstellen.</p> <p>Diese Option wird für VVols nicht unterstützt. Bei vVol VMs werden nur absturzkonsistente Backups durchgeführt.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Sie müssen VMware Tools auf der VM ausführen, um VM-konsistente Backups durchzuführen. Wenn VMware Tools nicht ausgeführt wird, wird stattdessen ein absturzkonsistentes Backup durchgeführt.</p> <p> Wenn Sie das Kontrollkästchen für die Konsistenz der VM aktivieren, können Backup-Vorgänge länger dauern und mehr Speicherplatz benötigen. In diesem Szenario werden die VMs zuerst stillgelegt, dann führt VMware einen VM-konsistenten Snapshot durch, dann führt SnapCenter seinen Backup-Vorgang durch und anschließend werden die VM-Vorgänge wieder aufgenommen. Der VM-Gast Speicher ist nicht in den Konsistenz-Snapshots der VMs enthalten.</p> </div>
Einbeziehen von Datastores mit unabhängigen Festplatten	<p>Aktivieren Sie dieses Kontrollkästchen, um alle Datenspeicher mit unabhängigen Festplatten, die temporäre Daten enthalten, in das Backup einzubeziehen.</p>



Für dieses Feld...	Do this...
Skripte	<p>Geben Sie den vollständig qualifizierten Pfad des Prescript oder Postscript ein, das das SnapCenter VMware Plug-in vor oder nach dem Backup ausführen soll. Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren und Protokolle zu senden. Der Skriptpfad wird zum Zeitpunkt der Ausführung des Skripts validiert.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Prescripts und Postscripts müssen auf der VM der virtuellen Appliance liegen. Um mehrere Skripte einzugeben, drücken Sie nach jedem Skriptpfad <b>Enter</b>, um jedes Skript in einer eigenen Zeile aufzulisten. Das Zeichen „;“ ist nicht zulässig.</p> </div>

### 9. Klicken Sie Auf **Hinzufügen**.

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

## Erstellen von Ressourcengruppen

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

Eine Ressourcengruppe kann Folgendes enthalten:

- Herkömmliche VMs und Datenspeicher

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

- FlexGroup Datenspeicher

Einem einzelnen FlexGroup Datastore. Spanning FlexGroup Datastores werden nicht unterstützt. Ein FlexGroup Datastore kann nicht mit herkömmlichen VMs oder Datastores kombiniert werden.

- FlexVol Datenspeicher

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

- VVol VMs

Eine oder mehrere vVol VMs. VVol VMs können nicht mit herkömmlichen VMs oder Datastores kombiniert werden.

- vSphere-Tag

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

- VVol VMs in einem Ordner

Alle VVols in einem einzelnen, angegebenen vVol Ordner. Wenn der Ordner eine Kombination aus vVol VMs und herkömmlichen VMs enthält, sichert das SnapCenter Plug-in für VMware vSphere die vVol VMs und überspringt die herkömmlichen VMs.

Für alle Ressourcengruppen:



Wenn Sie VMware vSphere Cluster Service (VCLS) verwenden, schließen Sie keine VMs ein, die von VCLS in SnapCenter VMware Plug-in-Ressourcengruppen verwaltet werden.



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



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

### Bevor Sie beginnen

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

Weitere Informationen finden Sie unter ["ONTAP Tools für VMware vSphere"](#).

### Über diese Aufgabe

Sie können jederzeit Ressourcen einer Ressourcengruppe hinzufügen oder aus dieser entfernen.

- Sicherung einer einzelnen Ressource

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

- Sicherung 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 ausführen, müssen Sie nach einem Switchover oder einem Switchover den SnapCenter VMware Plug-in-Service neu starten und die SnapMirror Beziehungen neu synchronisieren, bevor Sie Ressourcen in MetroCluster Umgebungen sichern.

In ONTAP 9.8 hängen die Backups nach dem Wechsel zurück. Dieses Problem wurde in ONTAP 9.9 behoben.

- Optimieren Von Snapshots

Um Snapshots zu optimieren, sollten Sie VMs und Datenspeicher, die mit demselben Volume verbunden

sind, in einer Ressourcengruppe gruppieren.

- Backup-Richtlinien

Sie können zwar eine Ressourcengruppe ohne Sicherungsrichtlinie erstellen, aber Datensicherheitsvorgänge sind nur möglich, wenn mindestens eine Richtlinie an die Ressourcengruppe angehängt ist. Sie haben die Möglichkeit, eine vorhandene Richtlinie zu verwenden oder während des Erstellungsprozesses einer Ressourcengruppe eine neue zu erstellen.



Wenn Sie eine Backup-Richtlinie mit Sperrfrist für Snapshots auswählen, müssen Sie die Version von ONTAP 9.12.1 oder höher auswählen.

- Kompatibilitätsprüfungen

Beim Erstellen einer Ressourcengruppe führt SnapCenter Kompatibilitätsprüfungen durch.

[Managen Sie Fehler bei der Kompatibilitätsprüfung](#)

### Schritte


1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Ressourcengruppen** und wählen Sie dann **Erstellen**, um den Assistenten zu starten.

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

- Um eine Ressourcengruppe für eine VM zu erstellen, klicken Sie auf **Menü > Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf eine VM, wählen Sie NetApp SnapCenter und wählen Sie dann **Ressourcengruppe erstellen** aus.
- Um eine Ressourcengruppe für einen Datastore zu erstellen, klicken Sie auf **Menü > Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf einen Datastore, wählen Sie dann **NetApp SnapCenter** und wählen Sie dann **Ressourcengruppe erstellen** aus.

- a. Gehen Sie auf der Seite **Allgemeine Informationen & Benachrichtigungen** im Assistenten wie folgt vor:

Für dieses Feld...	Do this...
VCenter Server	Wählen Sie einen vCenter-Server aus.
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Verwenden Sie die folgenden Sonderzeichen nicht in VM-, Datastore-, Richtlinien-, Backup- oder Ressourcengruppenamen: % & * € # @ ! \ / : * ? " < > - [vertikaler Balken] ; ' , . Ein Unterstrich ( _ ) ist zulässig. VM- oder Datastore-Namen mit Sonderzeichen werden abgeschnitten, was die Suche nach einem bestimmten Backup erschwert. Im Linked Modus verfügt jedes vCenter über ein separates VMware Plug-in-Repository von SnapCenter. Daher können Sie doppelte Namen in allen vCenters verwenden.

Für dieses Feld...	Do this...
Beschreibung	Geben Sie eine Beschreibung der Ressourcengruppe ein.
Benachrichtigung	Wählen Sie aus, wann Sie Benachrichtigungen über Vorgänge dieser Ressourcengruppe erhalten möchten: Fehler oder Warnungen: Nur Fehler und Warnungen senden: Nur Benachrichtigungen für Fehler senden immer nur senden: Benachrichtigung für alle Nachrichtentypen senden nie: Keine Benachrichtigung senden
E-Mail senden von	Geben Sie die E-Mail-Adresse ein, von der die Benachrichtigung gesendet werden soll.
E-Mail senden an	Geben Sie die E-Mail-Adresse der Person ein, die Sie erhalten möchten. Verwenden Sie für mehrere Empfänger ein Komma, um die E-Mail-Adressen zu trennen.
E-Mail-Betreff	Geben Sie den gewünschten Betreff für die Benachrichtigungs-E-Mails ein.
Der Name des Snapshot	<p>Wenn das Suffix „_recent“ zum letzten Snapshot hinzugefügt werden soll, aktivieren Sie dieses Kontrollkästchen. Das Suffix „_recent“ ersetzt Datum und Zeitstempel.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Für jede Richtlinie, die einer Ressourcengruppe zugeordnet ist, wird ein <code>_recent</code> Backup erstellt. Daher werden für eine Ressourcengruppe mit mehreren Richtlinien mehrere Backups erstellt <code>_recent</code> . Benennen Sie Backups nicht manuell um <code>_recent</code> .</p> </div>

Für dieses Feld...	Do this...
Benutzerdefiniertes Snapshot-Format	<p>Wenn Sie ein benutzerdefiniertes Format für die Snapshot-Namen verwenden möchten, aktivieren Sie dieses Kontrollkästchen, und geben Sie das Namensformat ein.</p> <ul style="list-style-type: none"> <li>• Diese Funktion ist standardmäßig deaktiviert.</li> <li>• Die standardmäßigen Snapshot-Namen verwenden das Format <code>&lt;ResourceGroup&gt;_&lt;Date-TimeStamp&gt;</code>. Sie können jedoch ein benutzerdefiniertes Format angeben, indem Sie die Variablen Ressourcengruppe, Richtlinie für US-Dollar, Hostname für US-Dollar, Planungstyp für US-Dollar und CustomText für US-Dollar verwenden. Verwenden Sie die Dropdown-Liste im benutzerdefinierten Namensfeld, um auszuwählen, welche Variablen Sie verwenden möchten, und in welcher Reihenfolge sie verwendet werden. Wenn Sie CustomText in US-Dollar auswählen, lautet das Namensformat <code>&lt;CustomName&gt;_&lt;Date-TimeStamp&gt;</code>. Geben Sie den benutzerdefinierten Text in das zusätzliche Feld ein, das bereitgestellt wird. [HINWEIS]: Wenn Sie auch das Suffix „_recent“ auswählen, müssen Sie sicherstellen, dass die benutzerdefinierten Snapshot-Namen im Datastore eindeutig sind. Daher sollten Sie dem Namen die Variablen „Ressourcengruppe USD“ und „Richtlinie USD“ hinzufügen.</li> <li>• Sonderzeichen für Sonderzeichen in Namen, befolgen Sie die gleichen Richtlinien für das Namensfeld.</li> </ul>

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

Für dieses Feld...	Do this...
Umfang	Wählen Sie den Ressourcentyp aus, den Sie sichern möchten: * Datastores (alle herkömmlichen VMs in einem oder mehreren angegebenen Datastores). Sie können keinen vVol Datastore auswählen. * Virtual Machines (einzelne traditionelle oder vVol VMs; im Feld müssen Sie zu dem Datenspeicher navigieren, der die VMs oder vVol VMs enthält). Sie können keine einzelnen VMs in einem FlexGroup Datastore auswählen. * Tags Tag-basierter Datastore-Schutz wird nur für NFS- und VMFS-Datastores sowie für virtuelle Maschinen und virtuelle vVol-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 oder Datastores oder Ordnern, die Sie hinzufügen möchten. Namen von VMs und Datenspeichern in einer Ressourcengruppe müssen eindeutig sein.
Verfügbare Einheiten	Wählen Sie die Ressourcen aus, die Sie schützen möchten, und klicken Sie dann auf >, um Ihre Auswahl in die Liste der ausgewählten Einheiten zu verschieben.

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

Wenn die Meldung `Selected <resource-name> is not SnapCenter compatible` angezeigt wird, ist eine ausgewählte Ressource nicht mit SnapCenter kompatibel. Weitere Informationen finden Sie unter [Managen Sie Fehler bei der Kompatibilitätsprüfung](#).

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

c. Wählen Sie auf der Seite **Spanning Disks** eine Option für VMs mit mehreren VMDKs über mehrere Datastores aus:

- Schließen Sie immer alle Spanning Datastores aus (dies ist der Standard für Datastores.)
- Berücksichtigen Sie immer alle spannenden Datenspeicher (dies ist der Standard für VMs).
- Wählen Sie manuell die Spanning-Datenspeicher aus, die einbezogen werden sollen

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

d. Wählen oder erstellen Sie auf der Seite **Richtlinien** eine oder mehrere Backup-Richtlinien, wie in der folgenden Tabelle dargestellt:

Um... zu verwenden	Do this...
Eine vorhandene Richtlinie	Wählen Sie eine oder mehrere Richtlinien aus der Liste aus.
Eine neue Richtlinie	<ul style="list-style-type: none"> <li>i. Wählen Sie <b>Erstellen</b>.</li> <li>ii. Schließen Sie den Assistenten für neue Backup-Richtlinien ab, um zum Assistenten „Ressourcengruppe erstellen“ zurückzukehren.</li> </ul>

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

- e. Konfigurieren Sie auf der Seite **Schedules** den Backup-Zeitplan für jede ausgewählte Richtlinie.

### Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules
- ✓ 6. Summary

mv\_policy ▼

Type Hourly

Every 1 hour ▼

Starting 08/07/2020 📅

At 08 04 AM

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

Wenn Sie im Feld \* each\* eine Anzahl von Tagen auswählen, werden die Backups an Tag 1 des Monats und danach in jedem angegebenen Intervall durchgeführt. Wenn Sie zum Beispiel die Option **alle 2 Tage** wählen, dann werden Backups am Tag 1, 3, 5, 7 usw. im Laufe des Monats durchgeführt, unabhängig davon, ob das Startdatum gerade oder ungerade ist.

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

["Ändern der Zeitzonen für Backups"](#).

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

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

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



Wenn der Quiesce-Vorgang für eine der VMs im Backup fehlschlägt, dann ist der Backup als nicht VM-konsistent gekennzeichnet, auch wenn die ausgewählte Richtlinie die VM-Konsistenz ausgewählt hat. In diesem Fall ist es möglich, dass einige der VMs erfolgreich stillgelegt wurden.

## Managen Sie Fehler bei der Kompatibilitätsprüfung

Beim Erstellen einer Ressourcengruppe führt SnapCenter Kompatibilitätsprüfungen durch.

Gründe für eine Inkompatibilität können sein:

- VMDKs sind auf nicht unterstütztem Storage; z. B. auf einem ONTAP System mit 7-Mode oder auf einem Gerät ohne ONTAP.
- Ein Datastore befindet sich auf NetApp Storage mit Clustered Data ONTAP 8.2.1 oder einer älteren Version.

SnapCenter Version 4.x unterstützt ONTAP 8.3.1 und höher.

Das SnapCenter Plug-in für VMware vSphere führt keine Kompatibilitätsprüfungen für alle ONTAP Versionen durch – nur für ONTAP Versionen 8.2.1 und frühere Versionen. Daher finden Sie immer die neuesten Informationen zum SnapCenter-Support im ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#) .

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

Gehen Sie wie folgt vor, um einen Kompatibilitätsfehler zu beheben:

1. Stellen Sie sicher, dass die Storage-VM ausgeführt wird.
2. Stellen Sie sicher, dass das Storage-System, auf dem sich die VMs befinden, zum SnapCenter Plug-in für den VMware vSphere Inventory hinzugefügt wurde.
3. Stellen Sie sicher, dass die Storage-VM zu SnapCenter hinzugefügt wird. Verwenden Sie die Option Add Storage System in der VMware vSphere Client GUI.
4. Wenn VMs über VMDKs sowohl auf NetApp als auch auf Datastores anderer Anbieter verfügen, verschieben Sie die VMDKs zu NetApp Datastores.

## Vorschriften und Postskripte

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



## Unterstützte Skripttypen

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

## Speicherort des Skriptpfads

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

Beispiel: \* Ein PERL-Skriptpfad könnte `/support/support/script.pl` \* Ein Shell-Skriptpfad sein `/support/support/script.sh`

Der Skriptpfad wird zum Zeitpunkt der Ausführung des Skripts validiert.

## Angeben von Skripten

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

Um mehrere Skripte festzulegen, drücken Sie nach jedem Skriptpfad **Enter**, um jedes Skript in einer eigenen Zeile aufzulisten. Semikolons (;) sind nicht zulässig. Sie können mehrere Vorschriften und mehrere Postskripte angeben. Ein einziges Skript kann sowohl als Vorskript als auch als Postscript codiert werden und kann andere Skripte aufrufen.

## Wenn Skripte ausgeführt werden

Skripte werden gemäß dem für `BACKUP_PHASE` eingestellten Wert ausgeführt.

- `BACKUP_PHASE=PRE_BACKUP`

In DER PHASE `PRE_BACKUP` des Vorgangs werden Prescripts ausgeführt.



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

- `BACKUP_PHASE=POST_BACKUP` ODER `BACKUP_PHASE=FAILED_BACKUP`

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



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

Überprüfen Sie Folgendes, um sicherzustellen, dass die Skriptwerte ausgefüllt sind: \* Für PERL-Skripte: `/support/support/log_env.log` Für Shell-Skripte: `/support/support/log_file.log`

## Umgebungsvariablen an Skripte übergeben

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

Umgebungsvariable	Beschreibung
BACKUP_NAME	Name des Backups. Variable nur in Postskripten übergeben.
BACKUP_DATE	Datum der Sicherung, in der Formatvariable, <code>yyyymmdd</code> die nur in Postscripts übergeben wird.
BACKUP_TIME	Zeitpunkt der Sicherung, in der Formatvariable, <code>hhmmss</code> die nur in Postscripts übergeben wird.
BACKUP_PHASE	Die Phase des Backups, in der das Skript ausgeführt werden soll. Gültige Werte sind: <code>PRE_BACKUP</code> , <code>POST_BACKUP</code> , and <code>FAILED_BACKUP</code> . Variable in Vorschriften und Postskripten übergeben.
STORAGE_SNAPSHOTS	Die Anzahl der Speicher-Snapshots im Backup. Variable nur in Postskripten übergeben.
STORAGE_SNAPSHOT.#	Einer der definierten Speicher-Snapshots, im folgenden Format: <code>&lt;filer&gt;:/vol/&lt;volume&gt;:&lt;ONTAP-snapshot-name&gt;</code> Variable wird nur in Postscripts übergeben.
VIRTUAL_MACHINES	Die Anzahl der VMs im Backup. Variable in Vorschriften und Postskripten übergeben.
VIRTUAL_MACHINE.#	Eine der definierten virtuellen Maschinen, im folgenden Format: <code>&lt;VM name&gt;[vertical bar]&lt;VM UUID&gt;[vertical bar]&lt;power-state&gt;[vertical bar]&lt;VM snapshot&gt;[vertical bar]&lt;ip-addresses&gt;</code> <code>&lt;power-state&gt;</code> has the values <code>POWERED_ON</code> , <code>POWERED_OFF</code> , or <code>SUSPENDED</code> <code>&lt;VM snapshot&gt;</code> Hat die Werte <code>true</code> oder <code>false</code> Variablen in Verordnungen und Postscripts übergeben.

## Skript-Timeouts

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

## Beispiel PERL-Skript #1

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

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

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

## Beispiel PERL-Skript #2

Im folgenden Beispiel werden Informationen zum Backup gedruckt.

```
#!/usr/bin/perl  
use warnings;  
use strict;  
  
my $argnum;  
my $logfile = '/support/support/log_env.log';  
open (FH, '>>', $logfile) or die $!;  
  
print FH "BACKUP_PHASE is $ENV{'BACKUP_PHASE'}\n";  
print FH "Backup name $ENV{'BACKUP_NAME'}\n";  
print FH "Virtual Machine $ENV{'VIRTUAL_MACHINES'}\n";  
print FH "VIRTUAL_MACHINE # is $ENV{'VIRTUAL_MACHINE.1'}\n";  
print FH "BACKUP_DATE is $ENV{'BACKUP_DATE'}\n";  
print FH "BACKUP_TIME is $ENV{'BACKUP_TIME'}\n";  
print FH "STORAGE_SNAPSHOTS is $ENV{'STORAGE_SNAPSHOTS'}\n";  
print FH "STORAGE_SNAPSHOT # is $ENV{'STORAGE_SNAPSHOT.1'}\n";  
  
print FH "PWD is $ENV{'PWD'}\n";  
print FH "INVOCATION_ID is $ENV{'INVOCATION_ID'}\n";  
  
print FH "=====\n";  
close (FH);
```

## Beispiel für Shell-Skript

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

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

Jede vorhandene Ressourcengruppe, die durch das SnapCenter Plug-in für VMware vSphere gemanagt wird, kann rasch eine einzelne VM oder einen Datenspeicher hinzugefügt werden.

### Über diese Aufgabe

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

### Schritte

1. Klicken Sie in der VMware vSphere-Client-GUI in der Symbolleiste auf **Menü** und navigieren Sie zu der VM oder dem Datastore, die Sie hinzufügen möchten.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf die VM oder den Datenspeicher, wählen Sie in der Dropdown-Liste **NetApp SnapCenter** aus und wählen Sie dann in der sekundären Dropdown-Liste **zur Ressourcengruppe hinzufügen** aus.

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

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

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

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

## Fügen Sie mehrere VMs und Datenspeicher einer Ressourcengruppe hinzu

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


Eine Ressourcengruppe kann eine der folgenden Elemente enthalten:

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



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

### Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und klicken Sie dann auf  **Ressourcengruppe bearbeiten**, um den Assistenten zu starten.
2. Gehen Sie auf der Seite **Ressource** wie folgt vor:

- a. Navigieren Sie im Feld Datastores zu den VMs oder Datastores, die Sie hinzufügen möchten.
- b. Wählen Sie in der Liste Verfügbare Einheiten eine oder mehrere VMs oder Datastores aus, die der Ressourcengruppe hinzugefügt werden sollen. Klicken Sie dann auf >, um Ihre Auswahl in die Liste der ausgewählten Einheiten zu verschieben. Klicken Sie auf >>, um alle verfügbaren Entitäten zu verschieben.

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

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

3. Wiederholen Sie Schritt 2 für jede VM oder jeden Datenspeicher, den Sie hinzufügen möchten.
4. Klicken Sie auf **Weiter**, bis Sie die Seite **Zusammenfassung** öffnen und dann die Zusammenfassung prüfen und auf **Fertig stellen** klicken.

## Backup des umbenannten Speichers wiederherstellen

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

### Schritte

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

Verwenden Sie die folgende API, um den Speicher umzubenennen:

PATCH /4.1/Storage-System

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

Antwort:

```
{ „StatusMessage“: „OK“, „StatusCode“: 200, „ResponseMessage“: [ „Storage System wurde erfolgreich umbenannt.“ ] }
```

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

## Bei Bedarf das Sichern von Ressourcengruppen sichern

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

### Bevor Sie beginnen

Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.




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

### Über diese Aufgabe

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

### Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und wählen Sie dann  **Jetzt ausführen**, um die Sicherung zu starten.
2. Wenn die Ressourcengruppe mehrere Richtlinien konfiguriert hat, wählen Sie im Dialogfeld **Jetzt sichern** die Richtlinie aus, die Sie für diesen Sicherungsvorgang verwenden möchten.
3. Klicken Sie auf **OK**, um die Sicherung zu starten.
4. Optional: Überwachen Sie den Betriebsfortschritt, indem Sie unten im Fenster auf **Letzte Aufgaben** oder auf dem Dashboard **Job Monitor** klicken, um weitere Informationen zu erhalten. .Result

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

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

Das SnapCenter VMware Plug-in 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 zudem ein Backup des Repositories vor Migrationen oder Upgrades durchführen.

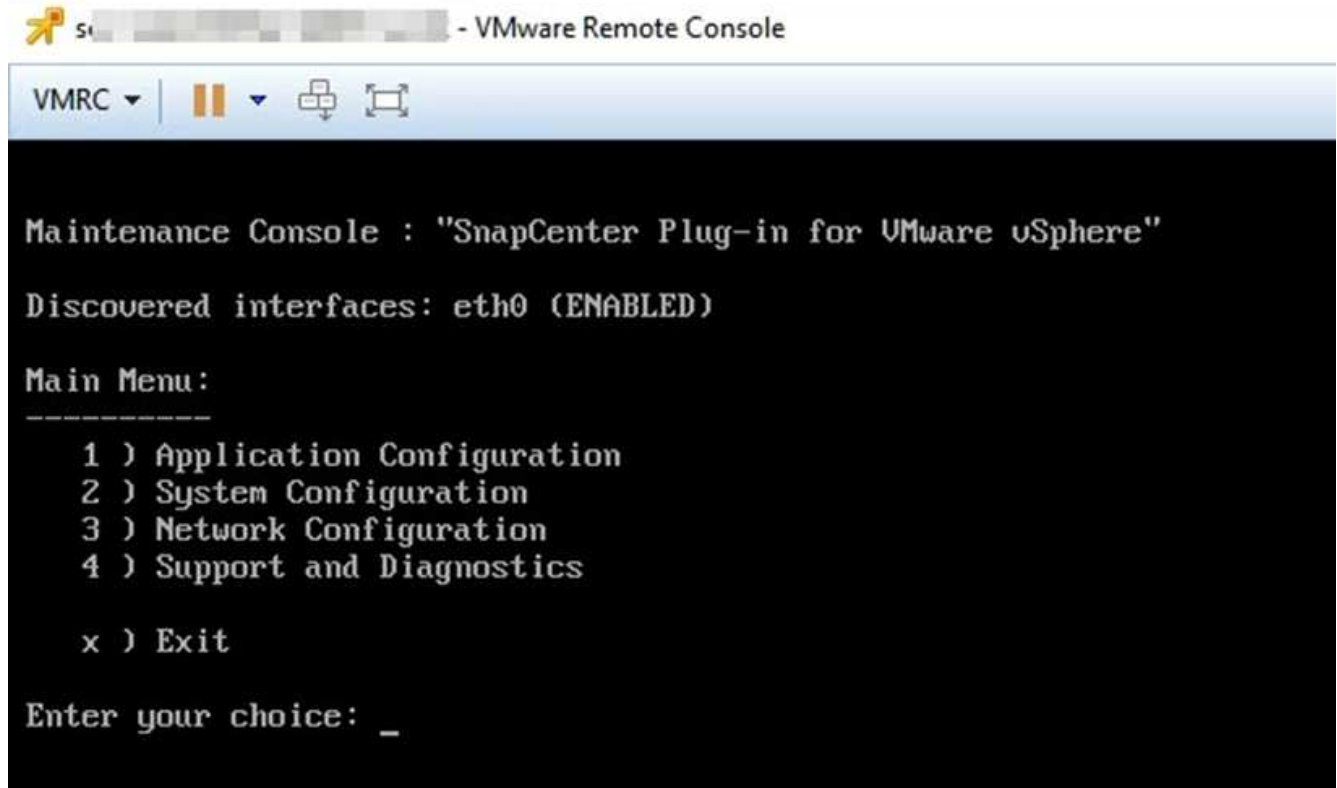
### Bevor Sie beginnen

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

wird.

### Schritte

1. Wählen Sie auf dem VMware vSphere-Client die VM aus, auf der sich das SnapCenter VMware Plug-in befindet.
2. Klicken Sie mit der rechten Maustaste auf die VM und dann auf der Registerkarte **Zusammenfassung** der virtuellen Appliance auf **Remote-Konsole starten** oder **Webkonsole starten**, um ein Fenster der Wartungskonsole zu öffnen.



```
st - VMware Remote Console
VMRC | || |
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
Main Menu:
-----
1 ) Application Configuration
2 ) System Configuration
3 ) Network Configuration
4 ) Support and Diagnostics
x ) Exit
Enter your choice: _
```

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

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



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

## Verwalten von Ressourcengruppen

Sie können Backup-Ressourcengruppen erstellen, ändern und löschen und Backup-

Vorgänge für Ressourcengruppen durchführen.



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

## Unterbrechen und Fortsetzen des Betriebs von Ressourcengruppen

Sie können geplante Vorgänge vorübergehend vom Starten einer Ressourcengruppe deaktivieren. Später können Sie diese Vorgänge aktivieren.

### Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Resource Groups**, klicken Sie mit der rechten Maustaste auf eine Ressourcengruppe und klicken Sie auf **Suspend** (oder klicken Sie auf **Resume**).
2. Klicken Sie im Bestätigungsfeld zur Bestätigung auf **OK**.

### Nachdem Sie fertig sind

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

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

## Ressourcengruppen ändern

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

### Über diese Aufgabe

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

% & \* # @ ! \ / : \* ? " < > - ; ' , .

Ein Unterstrich (`_`) ist zulässig.

### Schritte

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

Sie können Änderungen in mehreren Kategorien vornehmen.

3. Klicken Sie auf **Weiter**, bis die Übersichtsseite angezeigt wird, und klicken Sie dann auf **Fertig stellen**.

## Löschen von Ressourcengruppen

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 für VMware vSphere aus vCenter entfernen.

### Über diese Aufgabe



Alle Löschvorgänge der Ressourcengruppe werden als erzwang Löschvorgänge ausgeführt. Der Löschvorgang trennt alle Richtlinien aus der vCenter-Ressourcengruppe, entfernt die Ressourcengruppe aus dem SnapCenter-Plug-in für VMware vSphere und löscht alle Backups 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 OnCommand System Manager oder die ONTAP CLI verwenden, um die SnapVault-Beziehung zu entfernen. Anschließend müssen Sie den letzten Snapshot löschen.

### Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Ressourcengruppen**, wählen Sie dann eine Ressourcengruppe aus und klicken Sie auf **Löschen**.
2. Klicken Sie im Bestätigungsfeld **Ressourcengruppe löschen** auf **OK**, um zu bestätigen.

## Management von Richtlinien

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

### Richtlinien trennen

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

### Über diese Aufgabe

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

### Schritte

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

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

3. Nehmen Sie zusätzliche Änderungen an der Ressourcengruppe im Rest des Assistenten vor, und klicken Sie dann auf **Fertig stellen**.

### Richtlinien ändern

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

## Über diese Aufgabe

Das Ändern der Backup-Richtlinien für das SnapCenter VMware Plug-in unterscheidet sich von der Änderung der Backup-Richtlinien für applikationsbasierte SnapCenter Plug-ins. Wenn Sie die Plug-in-Richtlinien ändern, müssen Sie keine Richtlinien von Ressourcengruppen trennen.

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

- Erhöhen der Replizierungs- oder Aufbewahrungseinstellungen

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

- Verringerung der Replizierungs- oder Aufbewahrungseinstellungen

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



Zum Ändern eines Zeitplans für eine SnapCenter VMware Plug-in-Richtlinie müssen Sie den Zeitplan in der Plug-in-Ressourcengruppe ändern.

## Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Richtlinien**, wählen Sie dann eine Richtlinie aus und klicken Sie auf **Bearbeiten**.
2. Ändern Sie die Richtlinienfelder.
3. Wenn Sie fertig sind, klicken Sie auf **Aktualisieren**.

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

## Richtlinien löschen

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

### Bevor Sie beginnen

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

## Schritte

1. Klicken Sie im linken Navigator-Bereich des SCV-Plug-ins auf **Richtlinien**, wählen Sie dann eine Richtlinie aus und klicken Sie auf **Entfernen**.
2. Klicken Sie im Bestätigungsdiaologfeld auf **OK**.

# Backup-Management

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

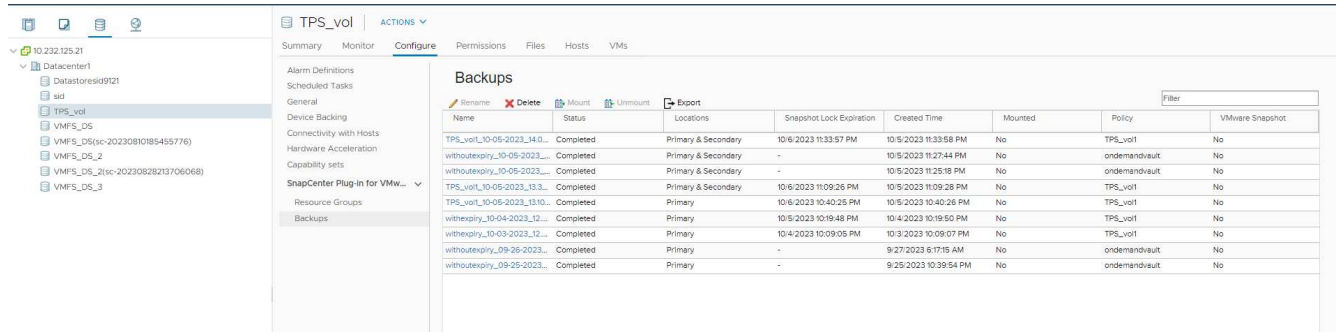
## Backups umbenennen

Sie können das SnapCenter Plug-in für VMware vSphere Backups umbenennen, wenn Sie einen besseren

Namen geben möchten, um die Suchbarkeit zu verbessern.

## Schritte

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



Name	Status	Locations	Snapshot Lock Expiration	Created Time	Mounted	Policy	VMware Snapshot
TPS_vol_10-05-2023_140...	Completed	Primary & Secondary	10/6/2023 11:33:57 PM	10/5/2023 11:33:58 PM	No	TPS_vol1	No
withoutexpiry_10-05-2023_...	Completed	Primary & Secondary	-	10/5/2023 11:27:44 PM	No	ondemand/vault	No
withoutexpiry_10-05-2023_...	Completed	Primary & Secondary	-	10/5/2023 11:25:18 PM	No	ondemand/vault	No
TPS_vol_10-05-2023_133...	Completed	Primary & Secondary	10/6/2023 11:09:26 PM	10/5/2023 11:09:28 PM	No	TPS_vol1	No
TPS_vol_10-05-2023_1310...	Completed	Primary	10/6/2023 10:40:25 PM	10/5/2023 10:40:26 PM	No	TPS_vol1	No
withoutexpiry_10-04-2023_12...	Completed	Primary	10/5/2023 10:19:48 PM	10/4/2023 10:19:50 PM	No	TPS_vol1	No
withoutexpiry_10-03-2023_12...	Completed	Primary	10/4/2023 10:09:05 PM	10/3/2023 10:09:07 PM	No	TPS_vol1	No
withoutexpiry_09-26-2023_...	Completed	Primary	-	9/27/2023 6:17:15 AM	No	ondemand/vault	No
withoutexpiry_09-25-2023_...	Completed	Primary	-	9/25/2023 10:38:54 PM	No	ondemand/vault	No

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

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

## Backups löschen

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

### Bevor Sie beginnen

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

### Über diese Aufgabe

Snapshots auf dem Sekundärspeicher werden über Ihre ONTAP Aufbewahrungseinstellungen gemanagt, nicht über das SnapCenter VMware Plug-in. Wenn Sie das SnapCenter-VMware-Plug-in zum Löschen eines Backups verwenden, werden Snapshots auf dem primären Speicher gelöscht, Snapshots auf dem sekundären Speicher jedoch nicht gelöscht. Wenn ein Snapshot noch auf dem sekundären Storage vorhanden ist, behält das SnapCenter VMware Plug-in die mit dem Backup verbundenen Metadaten bei, um Wiederherstellungsanforderungen zu unterstützen. Wenn der sekundäre Snapshot durch den ONTAP Aufbewahrungsvorgang gelöscht wird, löscht das SnapCenter VMware Plug-in die Metadaten mithilfe eines Löschjobs, der in regelmäßigen Abständen ausgeführt wird.

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

The screenshot shows the vSphere Backup console for the storage object 'TPS\_vol'. The left sidebar contains a navigation tree with 'TPS\_vol' selected. The main area displays the 'Backups' section with a table of backup records. The table has columns for Name, Status, Locations, Snapshot Lock Expiration, Created Time, Mounted, Policy, and VMware Snapshot. There are 11 backup entries listed, all with a status of 'Completed'.

Name	Status	Locations	Snapshot Lock Expiration	Created Time	Mounted	Policy	VMware Snapshot
TPS_vol_10-05-2023_14.0...	Completed	Primary & Secondary	10/6/2023 11:33:57 PM	10/5/2023 11:33:58 PM	No	TPS_vol1	No
withoutexpiry_10-05-2023...	Completed	Primary & Secondary	-	10/5/2023 11:27:44 PM	No	ondemandvault	No
withoutexpiry_10-05-2023...	Completed	Primary & Secondary	-	10/5/2023 11:25:18 PM	No	ondemandvault	No
TPS_vol_10-05-2023_13.3...	Completed	Primary & Secondary	10/6/2023 11:09:26 PM	10/5/2023 11:09:28 PM	No	TPS_vol1	No
TPS_vol_10-05-2023_13.10...	Completed	Primary	10/6/2023 10:40:25 PM	10/5/2023 10:40:26 PM	No	TPS_vol1	No
withexpiry_10-04-2023_12...	Completed	Primary	10/5/2023 10:19:48 PM	10/4/2023 10:19:50 PM	No	TPS_vol1	No
withexpiry_10-03-2023_12...	Completed	Primary	10/4/2023 10:09:05 PM	10/3/2023 10:09:07 PM	No	TPS_vol1	No
withoutexpiry_09-26-2023...	Completed	Primary	-	9/27/2023 6:17:15 AM	No	ondemandvault	No
withoutexpiry_09-25-2023...	Completed	Primary	-	9/25/2023 10:38:54 PM	No	ondemandvault	No

2. Wählen Sie eine oder mehrere Backups aus und klicken Sie auf **Löschen**.

Sie können maximal 40 Backups zum Löschen auswählen.

3. Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

4. Aktualisieren Sie die Backup-Liste, indem Sie auf das Aktualisierungssymbol in der linken Menüleiste von vSphere klicken.

# Mounten und Unmounten von Datastores

## Mounten Sie ein Backup

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

Sie können einen vVol Datastore nicht mounten.

### Bevor Sie beginnen

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

Wenn Sie an einem alternativen ESXi Host mounten möchten, müssen Sie sicherstellen, dass der alternative ESXi Host eine Verbindung zum Speicher herstellen kann und Folgendes hat: **Gleiche UID und GID wie beim ursprünglichen Host** gleiche virtuelle Appliance für SnapCenter-Plug-in für VMware vSphere-Version wie beim ursprünglichen Host

- Zuordnen von Storage-Initiatoren zu ESXi

Stellen Sie sicher, dass die Initiatoren für das Speichersystem dem ESXi zugeordnet sind.

- Bereinigen Sie veraltete LUNs

Da ESXi nur eine eindeutige LUN pro Datenspeicher feststellen kann, schlägt der Vorgang fehl, wenn mehr als eine LUN gefunden wird. Dies kann auftreten, wenn Sie einen Mount-Vorgang vor Abschluss eines vorherigen Mount-Vorgangs starten oder wenn Sie LUNs manuell klonen oder wenn Klone während eines Abmounten nicht aus dem Speicher gelöscht werden. Um das Auffinden von mehreren Klonen zu vermeiden, sollten Sie alle veralteten LUNs auf dem Storage aufräumen.

### Über diese Aufgabe

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

### Schritte

1. Klicken Sie im VMware vSphere-Client in der Symbolleiste auf **Menü** und wählen Sie dann in der Dropdown-Liste **Storage** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Datenspeicher und wählen Sie in der Dropdown-Liste **NetApp SnapCenter** aus, und wählen Sie dann in der sekundären Dropdown-Liste **Sicherung** aus.
3. Wählen Sie auf der Seite \* Mount Datastore\* ein Backup und einen Backup-Speicherort (primär oder sekundär) aus, und klicken Sie dann auf **Finish**.
4. Optional: Gehen Sie wie folgt vor, um zu überprüfen, ob der Datenspeicher angehängt ist:
  - a. Klicken Sie in der Symbolleiste auf **Menü** und wählen Sie dann in der Dropdown-Liste **Storage** aus.
  - b. Im linken Navigator-Fenster wird der Datenspeicher angezeigt, der Sie oben in der Liste montiert haben.

Wenn Sie einen Attach- oder Mount-Vorgang auf einem SnapVault-Ziel-Volumen durchführen, das durch SnapVault-Zeitpläne geschützt ist und ONTAP 8.3 ausführt, wird möglicherweise ein zusätzlicher Snapshot im Dialogfeld „Anhängen“ oder „Bereitstellen“ aufgeführt. Das liegt daran, dass durch den Attach- oder Mount-Vorgang das SnapVault Ziel-Volumen kloniert und ONTAP das Volumen durch Erstellung eines neuen Snapshots aktualisiert.

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

## Heben Sie die Bereitstellung eines Backups auf

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

Wenn ein Backup in der VMware vSphere-Client-GUI als gemountet aufgeführt ist, es aber nicht im Bildschirm Unmount Backup aufgeführt ist, müssen Sie die REST-API verwenden `/backup/{backup-Id}/cleanup`, um die nicht gebundenen Datastores zu bereinigen, und versuchen Sie dann erneut, das Unmount-Verfahren zu wiederholen.

Wenn Sie versuchen, eine Backup-Kopie eines NFS-Datenspeichers auf einer Storage-VM (SVM) mit dem Root-Volumen in einer Load-Sharing-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.` auf, um dieses Problem zu verhindern, ändern Sie die Einstellung für maximale Volumens, indem Sie zu **ESX > Verwalten > Einstellungen > Erweiterte Systemeinstellungen** navigieren und das NFS ändern. Wert für MaxVolumes. Der maximale Wert ist 256.

### Schritte

1. Klicken Sie im VMware vSphere-Client in der Symbolleiste auf **Menü** und wählen Sie dann in der Dropdown-Liste **Storage** aus.
2. Klicken Sie im linken Navigator-Fenster mit der rechten Maustaste auf einen Datenspeicher, wählen Sie dann in der Dropdown-Liste **NetApp SnapCenter** aus und wählen Sie dann in der sekundären Dropdown-Liste **Unmount** aus.



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

3. Wählen Sie im Dialogfeld **geklonter Datastore** einen Datastore aus, aktivieren Sie das Kontrollkästchen **Unmount the geklonten Datastore** und klicken Sie dann auf **Unmount**.

# Restore aus Backups

## Restore-Übersicht

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

- VM-Wiederherstellungsziele

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

Sie können vVol VMs zum ursprünglichen Host wiederherstellen.

- VMDK-Wiederherstellungsziele

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

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

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

Sie können Folgendes nicht wiederherstellen:

- Datenspeicher

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

- Backups entfernter VMs

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

## Durchführen von Restore-Vorgängen

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

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



Restore-Vorgänge	Von	Durchgeführt mit
FlexGroup-VMs	Sekundäre Backups	<p>NFS-Umgebungen:</p> <ul style="list-style-type: none"> <li>• ONTAP SnapMirror Wiederherstellen, wenn Sie ONTAP Version 9.10.1 und höher verwenden</li> <li>• Klonen und Mounten mit Storage VMotion für ONTAP vorherige Versionen</li> </ul> <p>VMFS-Umgebungen: Nicht unterstützt für FlexGroups</p>



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

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



Während eines Wiederherstellungsvorgangs kann der Fehler auftreten, oder dieser tritt auf `Host unresolved volumes is null Exception while calling pre-restore on SCV...Error mounting cloned LUN as datastore...`, wenn das SnapCenter VMware-Plug-in versucht, den Klon neu zu signieren. Aufgrund der Beschränkungen von VMware kann das SnapCenter VMware Plug-in den automatischen Neusignatur-Wert in erweiterten ESXi-Konfigurationen nicht steuern.

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

## Suche nach Backups

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

### Schritte

1. Klicken Sie in der VMware vSphere-Client-GUI in der Symbolleiste auf **Menü** und führen Sie dann einen der folgenden Schritte aus:

So zeigen Sie Backups für... an	Gehen Sie wie folgt vor...
VMs	Klicken Sie auf die Menüoption <b>Hosts und Cluster</b> , wählen Sie dann eine VM aus, klicken Sie dann auf die Registerkarte <b>Configure</b> und klicken Sie dann im Abschnitt <b>SnapCenter Plug-in für VMware vSphere</b> auf <b>Backups</b> .

So zeigen Sie Backups für... an	Gehen Sie wie folgt vor...
Datenspeicher	Klicken Sie auf die Menüoption <b>Speicherung</b> , wählen Sie dann einen Datenspeicher aus, klicken Sie dann auf die Registerkarte <b>Konfigurieren</b> und klicken Sie dann im Abschnitt <b>SnapCenter Plug-in für VMware vSphere</b> auf <b>Backups</b> .

2. Erweitern Sie im linken Navigator-Fensterbereich das Rechenzentrum, das die VM oder den Datastore enthält.
3. Optional: Klicken Sie mit der rechten Maustaste auf eine VM oder einen Datenspeicher, wählen Sie dann in der Dropdown-Liste **NetApp SnapCenter** aus und wählen Sie dann in der sekundären Dropdown-Liste **Wiederherstellen** aus.
4. Geben Sie im Assistenten \* Wiederherstellen\* einen Suchnamen ein und klicken Sie auf **Suchen**.

Sie können die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie dann aus, ob Backups mit VMware-Snapshots erstellt werden sollen, ob Backups gemountet werden sollen und ob der Speicherort vorhanden ist. Klicken Sie auf **OK**.

## Wiederherstellung von VMs aus Backups

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

Sie können VMs an folgenden Orten wiederherstellen:

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



Sie können vVol VMs nicht auf einem alternativen Host wiederherstellen.



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



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

## Bevor Sie beginnen

- Ein Backup muss vorhanden sein.

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



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

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

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

- FEHLER bei DER HA-Konfiguration

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

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

## Über diese Aufgabe

- VM ist nicht registriert und erneut registriert

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

- Wiederherstellen von Datenspeichern

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

- Wiederherstellung von vVol VMs

- vVol Datastores, die über VMs verfügen, werden nicht unterstützt. Da angeschlossene VMDKs in einem VM-Spanning-vVol Datastore nicht gesichert werden, enthalten die wiederhergestellten VMs nur teilweise VMDKs.
- Sie können ein vVol nicht auf einem alternativen Host wiederherstellen.

- Der automatische Lastausgleich von vVol wird nicht unterstützt.
- VMware Konsistenz Snapshot-Fehler bei einer VM

Auch wenn ein VMware Konsistenz-Snapshot für eine VM ausfällt, wird die VM trotzdem gesichert. Sie können die Einheiten, die in der Backup-Kopie im Wiederherstellungsassistenten enthalten sind, anzeigen und für Wiederherstellungsvorgänge verwenden.

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

## Schritte

1. Klicken Sie in der VMware vSphere-Client-GUI in der Symbolleiste auf **Menü** und wählen Sie dann in der Dropdown-Liste **VMs und Vorlagen** aus.



Wenn Sie eine gelöschte VM wiederherstellen, müssen die Anmeldeinformationen für die Speicher-VM, die zum SnapCenter-VMware-Plug-in hinzugefügt wurden, ein Benutzerkonto oder sein `vsadmin`, das über alle gleichen Berechtigungen verfügt wie `vsadmin`. Der Host muss sich auf einem Storage-System mit ONTAP 8.2.2 oder höher befinden.

2. Klicken Sie im linken Navigator mit der rechten Maustaste auf eine VM, wählen Sie dann in der Dropdown-Liste **NetApp SnapCenter** aus und wählen Sie dann in der sekundären Dropdown-Liste **Wiederherstellen** aus, um den Assistenten zu starten.
3. Wählen Sie im **Restore**-Assistenten auf der Seite **Backup auswählen** den Backup-Snapshot aus, den Sie wiederherstellen möchten.

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

4. Wählen Sie auf der Seite **Bereich auswählen** im Feld **Umfang wiederherstellen gesamte virtuelle Maschine** aus, wählen Sie dann den Speicherort für die Wiederherstellung aus, und geben Sie dann die Zielinformationen ein, auf denen das Backup gemountet werden soll.

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

Bei der Wiederherstellung von Teilersicherungen wird die Seite **Bereich auswählen** mit dem Wiederherstellungsvorgang übersprungen.

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

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

6. Überprüfen Sie die Übersichtsseite und klicken Sie dann auf **Fertig stellen**.
7. Optional: Überwachen Sie den Arbeitsfortschritt, indem Sie unten auf dem Bildschirm auf **Letzte Aufgaben** klicken.

Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

## Nachdem Sie fertig sind

- IP-Adresse ändern

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

- Fügen Sie wiederhergestellte VMs zu Ressourcengruppen hinzu

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

## Gelöschte VMs aus Backups wiederherstellen

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

Sie können VMs an folgenden Orten wiederherstellen:

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



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



Sie können vVol VMs nicht an einem anderen Speicherort wiederherstellen.



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

### Bevor Sie beginnen

- Das Benutzerkonto für das Speichersystem muss auf der Seite Storage Systems im VMware vSphere Client über die verfügen "[Mindestberechtigungen für ONTAP für ONTAP erforderlich](#)".
- Das Benutzerkonto in vCenter muss über die verfügen "[Minimale vCenter-Berechtigungen, die für das SnapCenter Plug-in für VMware vSphere erforderlich sind](#)".
- Ein Backup muss vorhanden sein.

Bevor Sie die VMDKs auf dieser VM wiederherstellen können, müssen Sie ein Backup der VM mit dem

SnapCenter Plug-in für VMware vSphere erstellt haben.



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

### Über diese Aufgabe

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

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

### Schritte

1. Klicken Sie auf **Menü** und wählen Sie die Menüoption **Speicherung**, wählen Sie dann einen Datenspeicher aus, wählen Sie dann die Registerkarte **Konfigurieren** aus und klicken Sie dann im Abschnitt **SnapCenter Plug-in für VMware vSphere** auf **Backups**.
2. Durch Doppelklicken auf ein Backup wird eine Liste aller VMs angezeigt, die im Backup enthalten sind.
3. Wählen Sie die gelöschte VM aus der Sicherungsliste aus und klicken Sie auf **Wiederherstellen**.
4. Wählen Sie im Assistenten \* Wiederherstellen\* auf der Seite **Sicherung auswählen** die Sicherungskopie aus, die Sie wiederherstellen möchten.

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

5. Wählen Sie auf der Seite **Bereich auswählen** im Feld **Umfang wiederherstellen gesamte virtuelle Maschine** aus, wählen Sie dann den Speicherort für die Wiederherstellung aus, und geben Sie dann die ESXi-Zielinformationen ein, auf denen das Backup gemountet werden soll.

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

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

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

## Wiederherstellung von VMDKs aus Backups

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

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



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

### Bevor Sie beginnen

- Ein Backup muss vorhanden sein.

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

- Die VM darf nicht während der Übertragung sein.

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

### Über diese Aufgabe

- Wenn die VMDK gelöscht oder von der VM getrennt wird, wird die VMDK durch den Wiederherstellungsvorgang an die VM angeschlossen.
- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn der Storage Tier der FabricPool, auf dem sich die VM befindet, nicht verfügbar ist.
- Verbinden Sie VMDKs über den Standard-SCSI-Controller und stellen Sie Wiederherstellungsvorgänge her. VMDKs, die mit einem NVME-Controller an eine VM angeschlossen sind, werden gesichert, doch für Anschluss- und Restore-Vorgänge werden sie über einen SCSI-Controller zurückverbunden.

### Schritte

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

Sie können nach einem bestimmten Backup-Namen oder einem partiellen Backup-Namen suchen, oder Sie können die Backup-Liste filtern, indem Sie auf das Filtersymbol klicken und einen Datums- und Zeitbereich auswählen. Wählen Sie aus, ob Sie Backups mit VMware-Snapshots erstellen möchten, ob Sie gemountete Backups möchten. Und primären oder sekundären Standort. Klicken Sie auf **OK**, um zum Assistenten zurückzukehren.

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

Wiederherstellen auf...	Geben Sie das Wiederherstellungsziel... an
Den ursprünglichen Datenspeicher verwendet	Wählen Sie in der Dropdown-Liste * bestimmtes Laufwerk* aus und klicken Sie dann auf <b>Weiter</b> . In der Tabelle Datastore Selection können Sie beliebige VMDKs auswählen oder deren Auswahl aufheben.
Einen alternativen Datenspeicher an einem alternativen Speicherort	Klicken Sie auf den Ziel-Datastore und wählen Sie einen anderen Datastore aus der Liste aus.

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

## Stellen Sie das neueste Backup der MySQL-Datenbank wieder her

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

### Schritte

1. Öffnen Sie ein Fenster der Wartungskonsole.

["Öffnen Sie die Wartungskonsole"](#).

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

Die MySQL Backup Datenbank wird an ihren ursprünglichen Speicherort wiederhergestellt.

## Stellen Sie ein bestimmtes Backup der MySQL-Datenbank wieder her

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

### Schritte

1. Öffnen Sie ein Fenster der Wartungskonsole.

["Öffnen Sie die Wartungskonsole"](#).

2. Geben Sie im Hauptmenü die Option **1) Anwendungskonfiguration** ein.
3. Geben Sie im Menü Anwendungskonfiguration die Option **6) MySQL-Sicherung und -Wiederherstellung** ein.
4. Geben Sie im Menü MySQL Backup and Restore Configuration die Option **2) MySQL-Backups** ein und notieren Sie sich dann das Backup, das Sie wiederherstellen möchten.



5. Geben Sie im Menü MySQL Backup and Restore Configuration die Option **4) Restore MySQL Backup** ein.
6. Geben Sie an der Eingabeaufforderung „Wiederherstellen mit dem neuesten Backup“ **n** ein.
7. Geben Sie an der Eingabeaufforderung „Backup to restore from“ den Sicherungsnamen ein, und drücken Sie dann **Enter**.

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

# Anschließen und Trennen von VMDKs

## Weisen Sie VMDKs an eine VM oder vVol VM zu

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

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

### Über diese Aufgabe

Sie haben die folgenden Zusatzoptionen:

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

Die folgenden Einschränkungen gelten für das Anbinden virtueller Laufwerke:

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

Fügen Sie in diesem Fall die SCSI-Controller manuell hinzu, und versuchen Sie es erneut.

- Sie können keine virtuelle Festplatte manuell anschließen, die als Teil eines Wiederherstellungsvorgangs für die Gastdatei angehängt oder angehängt wurde.
- Verbinden Sie VMDKs über den Standard-SCSI-Controller und stellen Sie Wiederherstellungsvorgänge her. VMDKs, die mit einem NVME-Controller an eine VM angeschlossen sind, werden gesichert, doch für Anschluss- und Restore-Vorgänge werden sie über einen SCSI-Controller zurückverbunden.

### Schritte

1. Klicken Sie in der VMware vSphere-Client-GUI in der Symbolleiste auf **Menü** und wählen Sie dann in der Dropdown-Liste **Hosts und Cluster** aus.
2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf eine VM, wählen Sie dann in der Dropdown-Liste **NetApp SnapCenter** aus und wählen Sie dann in der sekundären Dropdown-Liste **virtuelles Laufwerk anhängen** aus.
3. Wählen Sie im Fenster **Virtuelles Laufwerk anhängen** im Abschnitt **Sicherung** ein Backup aus.

Sie können die Sicherungsliste filtern, indem Sie das Filtersymbol auswählen und einen Datums- und Zeitbereich auswählen. Wählen Sie aus, ob Sie Backups mit VMware-Snapshots erstellen möchten, ob Sie Backups mounten möchten, und wählen Sie den Speicherort aus. Klicken Sie auf **OK**.

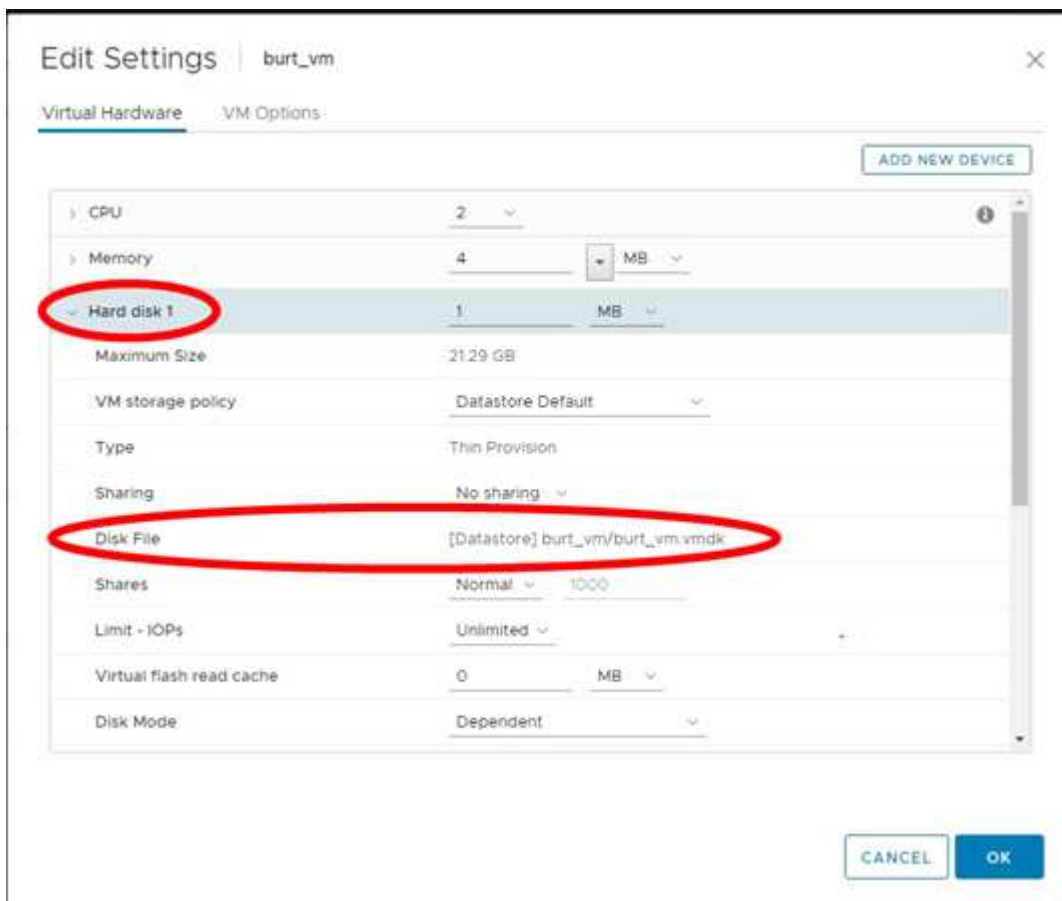
4. Wählen Sie im Abschnitt **Select Disks** ein oder mehrere Festplatten aus, die Sie verbinden möchten, und den Speicherort, an den Sie anschließen möchten (primäre oder sekundäre).

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

- Standardmäßig sind die ausgewählten virtuellen Laufwerke an die übergeordnete VM angeschlossen. Klicken Sie hier, um die ausgewählten virtuellen Laufwerke an eine alternative VM im selben ESXi-Host anzuhängen und geben Sie die alternative VM an.
- Klicken Sie Auf **Anhängen**.
- Optional: Überwachen Sie den Arbeitsfortschritt im Abschnitt \* Letzte Aufgaben\*.

Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

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



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

## Ergebnis

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

# Trennen Sie eine virtuelle Festplatte

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

## Schritte

1. Klicken Sie in der VMware vSphere-Client-GUI in der Symbolleiste auf **Menü** und wählen Sie dann in der Dropdown-Liste **VMs und Vorlagen** aus.
2. Wählen Sie im linken Navigator eine VM aus.
3. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf die VM, wählen Sie dann in der Dropdown-Liste **NetApp SnapCenter** aus und wählen Sie dann in der sekundären Dropdown-Liste **Virtual Disk trennen** aus.
4. Wählen Sie auf dem Bildschirm **Virtuelles Laufwerk trennen** eine oder mehrere Festplatten aus, die Sie entfernen möchten, und aktivieren Sie dann das Kontrollkästchen **Ausgewählte Datenträger trennen** und klicken Sie auf **ENTFERNEN**.



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

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

Aktualisieren Sie den Bildschirm, um aktualisierte Informationen anzuzeigen.

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

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

# Wiederherstellung von Gastdateien und Ordern

## Workflow, Voraussetzungen und Einschränkungen

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

### Workflow zur Wiederherstellung von Gastspielen

Zur Wiederherstellung von Gastbetriebssystemen gehören die folgenden Schritte:

#### 1. Anhängen

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

#### 2. Warten

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

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

Gesendet.

#### 3. Wählen Sie Dateien oder Ordner aus

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

#### 4. Wiederherstellen

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

### Voraussetzungen für die Wiederherstellung von Gastdateien und -Ordern

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

- VMware-Tools müssen installiert und ausgeführt werden.

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

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

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#).

- Anmeldedaten für die Ziel-VM müssen das integrierte Domain-Administratorkonto oder das integrierte lokale Administratorkonto angeben. Der Benutzername muss „Administrator“ sein. Vor dem Start des Wiederherstellungsvorgangs müssen die Anmeldeinformationen für die VM konfiguriert werden, an die Sie

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



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

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

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

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

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

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

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

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

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

- Die Wiederherstellung von einem Linux-Gastbetriebssystem wird nicht unterstützt

Sie können keine Dateien und Ordner von einer VM wiederherstellen, auf der das Linux Gastbetriebssystem ausgeführt wird. Sie können jedoch eine VMDK anhängen und dann die Dateien und Ordner manuell wiederherstellen. Aktuelle Informationen zu unterstützten Gast-OS finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#).

## Einschränkungen bei der Wiederherstellung von Gastdateien

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

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

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

Ordner manuell wiederherstellen. Aktuelle Informationen zu unterstützten Gast-OS finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#).

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

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

- Sie können Gastdateien nicht aus einer geklonten VMDK oder einer nicht initialisierten VMDK wiederherstellen.
- Sie können keine sekundären Backups wiederherstellen, wenn das Backup auf einem System mit ONTAP 9.2 oder neuer ausgeführt wurde und die Option VMware Consistency aktiviert war.
- Sie können die Verzeichnisstruktur für eine Datei nicht wiederherstellen.

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

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

## Wiederherstellung von Gastdateien und Ordnern über VMDKs

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

### Über diese Aufgabe

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

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





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



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

## Schritte

1. Klicken Sie auf **Menü** und wählen Sie die Menüoption **Hosts und Cluster** aus, wählen Sie dann eine VM aus, wählen Sie dann **NetApp SnapCenter** aus und klicken Sie dann auf **Wiederherstellung der Gastdatei**.
2. Klicken Sie im VMware vSphere-Client in der sekundären Dropdown-Liste auf **Guest File Restore**, um den Assistenten zu starten.
3. Geben Sie auf der Seite **Wiederherstellungsumfang** das Backup an, das das virtuelle Laufwerk enthält, das Sie anhängen möchten, indem Sie wie folgt vorgehen:
  - a. Wählen Sie in der Tabelle **Backup Name** das Backup aus, das das virtuelle Laufwerk enthält, das Sie anhängen möchten.
  - b. Wählen Sie in der Tabelle **VMDK** das virtuelle Laufwerk aus, das die Dateien oder Ordner enthält, die Sie wiederherstellen möchten.
  - c. Wählen Sie in der Tabelle **Locations** den primären oder sekundären Speicherort des virtuellen Laufwerks aus, das Sie verbinden möchten.
4. Gehen Sie auf der Seite **Gästedetails** wie folgt vor:
  - a. Wählen Sie, wo das virtuelle Laufwerk angeschlossen werden soll:

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

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

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



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



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

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

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

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

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

- Um die Dateien zu finden, die Sie von der angeschlossenen virtuellen Festplatte wiederherstellen möchten, klicken Sie auf **Menü > SnapCenter-Plug-in für VMware vSphere**, dann im linken Navigator-Bereich klicken Sie **Gastdateiwiederherstellung** und wählen Sie die Registerkarte **Gastkonfiguration**.

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

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

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

- Klicken Sie auf das Symbol **Dateien durchsuchen**, um eine Liste von Dateien und Ordnern auf dem virtuellen Laufwerk anzuzeigen.

Wenn Sie zum Durchsuchen und Auswählen einzelner Dateien auf einen Ordner doppelklicken, kann es zu einer bestimmten Zeit kommen, während die Liste der Dateien abgerufen wird, da der Abrufvorgang zur Laufzeit durchgeführt wird.

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

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


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

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

10. Wählen Sie eine oder mehrere Dateien oder Ordner aus, die wiederhergestellt werden sollen, und klicken Sie dann auf **Speicherort wiederherstellen**.

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

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

Option	Beschreibung
Wiederherstellen des Pfads	Geben Sie den UNC-Freigabepfad zum Gast ein, auf dem die ausgewählten Dateien wiederhergestellt werden. IPv4-Beispiel: \\10.60.136.65\c\$ IPv6-Beispiel: \\fd20-8b1e-b255-832e-61.ipv6-literal.net\C\restore
Wenn Originaldatei(en) vorhanden ist	Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die wiederherzustellende Datei oder der wiederherzustellende Ordner bereits auf dem Wiederherstellungsziel vorhanden ist: Immer überschreiben oder immer überspringen.  <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  Wenn der Ordner bereits vorhanden ist, wird der Inhalt des Ordners mit dem vorhandenen Ordner zusammengeführt. </div>
Trennen Sie die Gastsitzung nach erfolgreicher Wiederherstellung	Wählen Sie diese Option aus, wenn die Wiederherstellungssitzung der Gastdatei gelöscht werden soll, wenn der Wiederherstellungsvorgang abgeschlossen ist.

12. Klicken Sie Auf **Wiederherstellen**.

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

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

# Einrichten von Proxy-VMs für Wiederherstellungsvorgänge

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

## Schritte

1. Klicken Sie im VMware vSphere-Client auf **Wiederherstellung der Gastdatei**.
2. Führen Sie im Abschnitt \* Ausführen als Anmeldeinformationen\* einen der folgenden Schritte aus:

Um dies zu tun...	Do this...
Verwenden Sie vorhandene Anmeldedaten	Wählen Sie eine der konfigurierten Anmeldeinformationen aus.
Neue Anmeldedaten hinzufügen	<ol style="list-style-type: none"><li>a. Wählen Sie <b>Hinzufügen</b>.</li><li>b. Geben Sie im Dialogfeld <b>Ausführen als Anmeldeinformationen</b> die Anmeldeinformationen ein.</li><li>c. Klicken Sie auf <b>Select VM</b> und wählen Sie dann im Dialogfeld <b>Proxy VM</b> eine VM aus. Klicken Sie auf <b>Speichern</b>, um zum Dialogfeld <b>Ausführen als Anmeldeinformationen</b> zurückzukehren.</li><li>d. Geben Sie die Anmeldeinformationen ein. Für den Benutzernamen müssen Sie „Administrator“ eingeben.</li></ol>

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

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

3. Klicken Sie im Abschnitt **Proxy Credentials** auf **Add**, um eine VM hinzuzufügen, die als Proxy verwendet werden soll.
4. Füllen Sie im Dialogfeld **Proxy VM** die Informationen aus und klicken Sie dann auf **Speichern**.



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

## Konfigurieren Sie die Anmeldedaten für die Wiederherstellung von VM-Gastdateien

Wenn Sie ein virtuelles Laufwerk zur Wiederherstellung von Gastdateien oder Ordnern

anschließen, muss die Ziel-VM für die Anbindung die Anmeldeinformationen konfiguriert haben, bevor Sie die Wiederherstellung durchführen.

### Über diese Aufgabe

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

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

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

### Schritte

1. Klicken Sie im VMware vSphere-Client auf **Wiederherstellung der Gastdatei**.
2. Führen Sie im Abschnitt \* Ausführen als Anmeldeinformationen\* einen der folgenden Schritte aus:

<b>Um dies zu tun...</b>	<b>Do this...</b>
Verwenden Sie vorhandene Anmeldedaten	Wählen Sie eine der konfigurierten Anmeldeinformationen aus.

Um dies zu tun...	Do this...
Neue Anmeldedaten hinzufügen	<ol style="list-style-type: none"> <li>Wählen Sie <b>Hinzufügen</b>.</li> <li>Geben Sie im Dialogfeld <b>Ausführen als Anmeldeinformationen</b> die Anmeldeinformationen ein. Für den Benutzernamen müssen Sie „Administrator“ eingeben.</li> <li>Klicken Sie auf <b>Select VM</b> und wählen Sie dann im Dialogfeld <b>Proxy VM</b> eine VM aus. Klicken Sie auf <b>Speichern</b>, um zum Dialogfeld <b>Ausführen als Anmeldeinformationen</b> zurückzukehren. Wählen Sie die VM aus, die zur Authentifizierung der Anmeldedaten verwendet werden soll.</li> </ol>

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

- Klicken Sie Auf **Speichern**.

## Verlängern Sie die Zeit für die Wiederherstellung von Gastdateien

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

### Über diese Aufgabe

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

### Schritte

- Klicken Sie im VMware vSphere-Client auf **Wiederherstellung der Gastdatei**.
- Wählen Sie eine Gastdatei-Wiederherstellungssitzung aus, und klicken Sie in der Titelleiste des Gastsession-Monitors auf das Symbol Ausgewählte Gastsitzung erweitern.

Die Sitzung wird um weitere 24 Stunden verlängert.

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

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

## Die Sitzung zur Wiederherstellung der Gastdatei ist leer

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

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

## Der Vorgang zum Wiederherstellen der Gastdatei schlägt fehl

Dieses Problem tritt auf, wenn Sie eine Wiederherstellung einer Gastdatei starten, aber der Vorgang der angebotenen Festplatte schlägt fehl, obwohl VMware-Tools ausgeführt werden und die Anmeldedaten 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 Windows-Dienst für VMware-Tools auf dem Gastbetriebssystem neu, und wiederholen Sie dann den Wiederherstellungsvorgang für die Gastdatei.

## Gast-E-Mail-Shows ??????? Für den Dateinamen

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

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

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

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

# Managen Sie das SnapCenter Plug-in für VMware vSphere Appliance

## Starten Sie den VMware vSphere-Client-Service neu

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

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

### Bevor Sie beginnen

Sie müssen vCenter 7.0U1 oder höher ausführen.

### Schritte

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

```
shell
```

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

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

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

```
etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/  
  
rm -rf com.netapp.scv.client-<version_number>
```



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

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

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

## Öffnen Sie die Wartungskonsole

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

### Bevor Sie beginnen

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

## Über diese Aufgabe

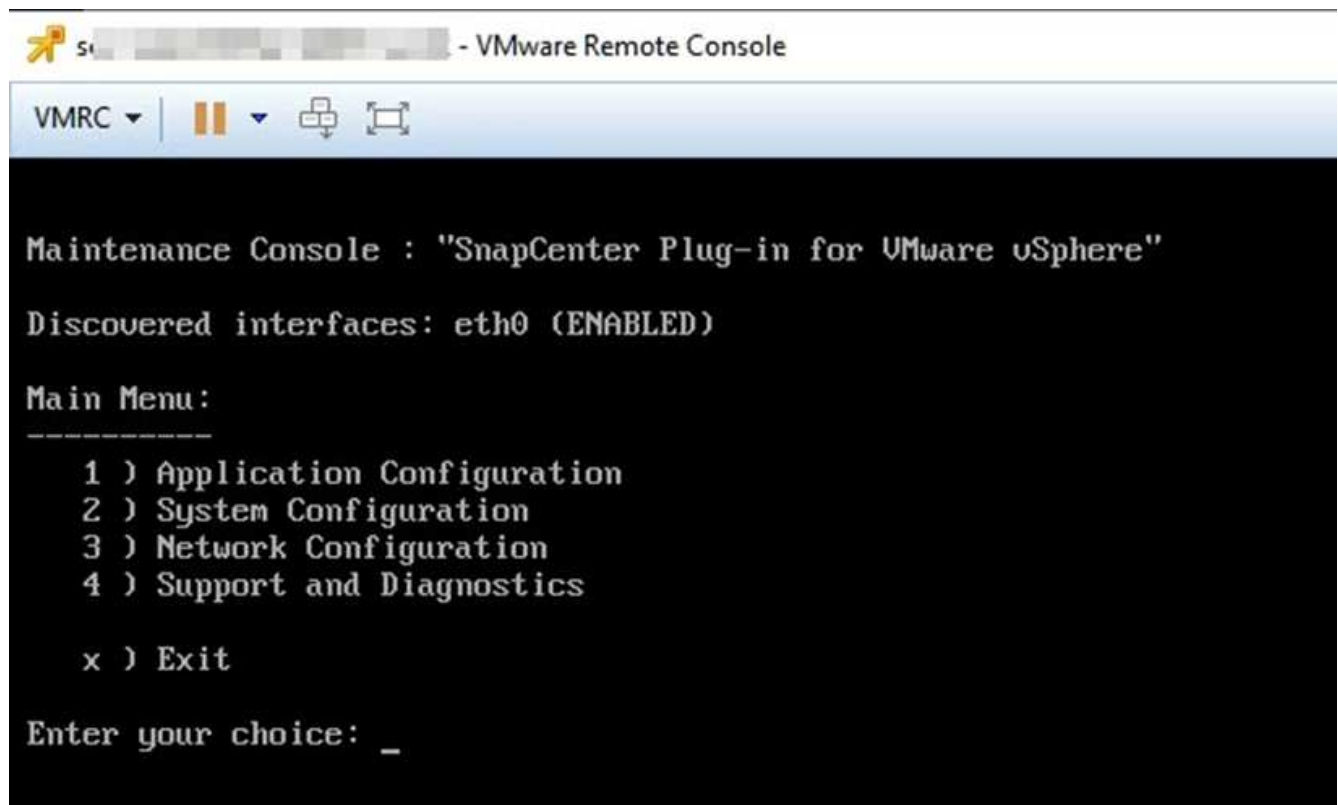
- Im SnapCenter-Plug-in für VMware vSphere 4.6P1 müssen Sie beim ersten Installieren des SnapCenter-Plug-ins für VMware vSphere ein Passwort angeben. Wenn Sie von Version 4.6 oder früher auf Version 4.6P1 oder höher aktualisieren, wird das frühere Standardpasswort akzeptiert.
- Sie müssen ein Passwort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

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

## Schritte

1. Wählen Sie auf dem VMware vSphere-Client die VM aus, auf der sich das SnapCenter VMware Plug-in befindet.
2. Klicken Sie mit der rechten Maustaste auf die VM und dann auf der Registerkarte **Zusammenfassung** der virtuellen Appliance auf **Remote-Konsole starten**, um ein Fenster der Wartungskonsole zu öffnen.

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



```
si-... - VMware Remote Console
VMRC | || |
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
Main Menu:
-----
1 ) Application Configuration
2 ) System Configuration
3 ) Network Configuration
4 ) Support and Diagnostics
x ) Exit
Enter your choice: _
```

3. Sie können folgende Vorgänge durchführen:

- Option 1: Anwendungskonfiguration

Anzeigen einer Zusammenfassung des SnapCenter VMware Plug-ins Starten oder beenden des SnapCenter VMware Plug-in-Dienstes Ändern Sie den Benutzernamen oder das Passwort für das SnapCenter VMware Plug-in Ändern Sie das MySQL-Passwort Sichern und Wiederherstellen MySQL, konfigurieren und auflisten Sie MySQL-Backups

- Option 2: Systemkonfiguration



Virtuelle Maschine neu starten virtuelle Maschine herunterfahren Benutzerpasswort ändern Zeitzone ändern NTP-Server aktivieren SSH-Zugriff aktivieren Jail-Festplattengröße erhöhen (/Jail) Upgrade VMware Tools MFA-Token generieren installieren



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 Änderungen bestätigen Ping an einen Host

+ \* Option 4: Support und Diagnose

+ Generate Support Bundle Access Diagnostic Shell enable Remote Diagnostic Access Generate Core Dump Bundle

## Ändern Sie das Passwort für das SnapCenter VMware Plug-in von der Wartungskonsole aus

Wenn Sie das Admin-Passwort für das SnapCenter-Plug-in für die Management-GUI von VMware vSphere nicht kennen, können Sie über die Wartungskonsole ein neues Passwort festlegen.

### Bevor Sie beginnen

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

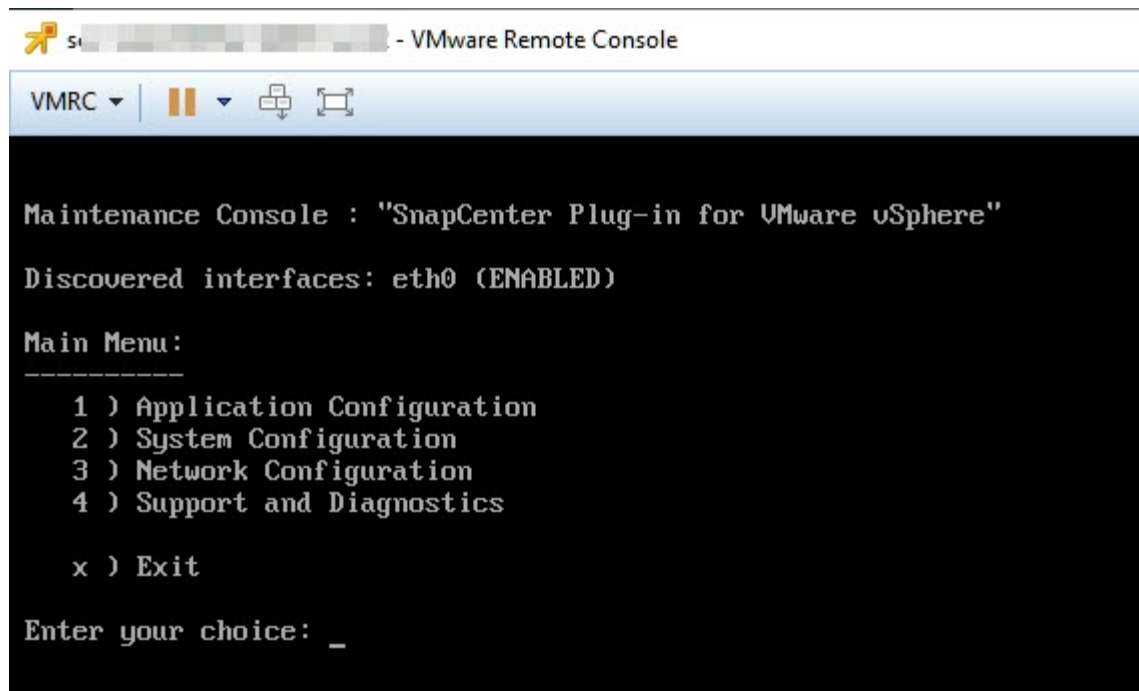
### Über diese Aufgabe

Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter ["Öffnen Sie die Wartungskonsole"](#).

### Schritte

1. Wählen Sie auf dem VMware vSphere-Client die VM aus, auf der sich das SnapCenter VMware Plug-in befindet.
2. Klicken Sie mit der rechten Maustaste auf die VM und dann auf der Registerkarte **Zusammenfassung** der virtuellen Appliance auf **Remote-Konsole starten**, um ein Fenster der Wartungskonsole zu öffnen und sich dann anzumelden.

Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter ["Öffnen Sie die Wartungskonsole"](#).



```
VMware Remote Console
VMRC | || |
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
Main Menu:
-----
1 ) Application Configuration
2 ) System Configuration
3 ) Network Configuration
4 ) Support and Diagnostics
x ) Exit
Enter your choice: _
```

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

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

## Erstellen und Importieren von Zertifikaten

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

Siehe "[KB-Artikel: Erstellen und/oder importieren Sie ein SSL-Zertifikat in SnapCenter Plug-in für VMware vSphere](#)".

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

Wenn Sie den SnapCenter VMware Plug-in-Service in einem vCenter beenden, das sich im verknüpften Modus befindet, sind Ressourcengruppen in allen verknüpften vCenters nicht verfügbar, selbst wenn der SnapCenter VMware Plug-in-Service in den anderen verknüpften vCenters ausgeführt wird.

Sie müssen die SnapCenter-VMware-Plug-in-Erweiterungen manuell aufheben.

### Schritte

1. Navigieren Sie im verknüpften vCenter mit dem SnapCenter-VMware-Plug-in-Service angehalten 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** aus, um eine Liste der registrierten Erweiterungen anzuzeigen.
3. Heben Sie die Registrierung der Erweiterungen `com.netapp.scv.client` und ``com.netapp.aegis`` auf.

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

Wenn Sie die SnapCenter Datensicherungsfunktionen nicht mehr benötigen, müssen Sie die Konfiguration des SnapCenter VMware Plug-ins 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.

### Über diese Aufgabe

Wenn Sie das SnapCenter VMware Plug-in deaktivieren, werden alle Ressourcengruppen ausgesetzt und das Plug-in wird als Erweiterung in vCenter nicht registriert.

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

["Sichern Sie das SnapCenter Plug-in für VMware vSphere MySQL Datenbank"](#).

2. Melden Sie sich in der SnapCenter VMware Plug-in Management GUI über das Format ``https://<OVA-IP-address>:8080`` an. Melden Sie sich bei der Implementierung mit dem Admin-Benutzernamen und -Passwort an, und verwenden Sie das MFA-Token, das über die Wartungskonsole generiert wurde.

Die IP des SnapCenter-VMware-Plug-ins wird bei der Bereitstellung des Plug-ins angezeigt.

3. Klicken Sie im linken Navigationsbereich auf **Konfiguration** und dann im Abschnitt **Plug-in-Details** auf die Option Service, um das Plug-in zu deaktivieren.

4. Bestätigen Sie Ihre Auswahl.

- Wenn Sie das SnapCenter VMware Plug-in nur zur Durchführung VM-konsistenter Backups verwendet haben

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

- Wenn Sie mithilfe des SnapCenter VMware Plug-ins applikationskonsistente Backups durchführen

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

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

## Entfernen Sie das SnapCenter Plug-in für VMware vSphere

Wenn Sie die Datensicherungsfunktionen von SnapCenter nicht mehr verwenden müssen, müssen Sie das SnapCenter VMware Plug-in deaktivieren, um es von vCenter aus wiederzuregistrieren, dann das SnapCenter VMware Plug-in aus vCenter zu entfernen und übrig gebliebene Dateien manuell zu löschen.

### Bevor Sie beginnen

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

### Schritte

1. Melden Sie sich in der SnapCenter VMware Plug-in Management GUI über das Format ``https://<OVA-IP-address>:8080`` an.

Die IP des SnapCenter-VMware-Plug-ins wird bei der Bereitstellung des Plug-ins angezeigt.

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

### Nachdem Sie fertig sind

Die virtuelle Appliance wird weiterhin bereitgestellt, das SnapCenter VMware Plug-in wird jedoch entfernt.

Nach dem Entfernen der Host-VM für das SnapCenter-VMware-Plug-in bleibt das Plug-in möglicherweise bis zur Aktualisierung des lokalen vCenter Caches im vCenter verfügbar. Da das Plug-in entfernt wurde, können auf diesem Host jedoch keine SnapCenter VMware vSphere Vorgänge durchgeführt werden. Wenn Sie den lokalen vCenter-Cache aktualisieren möchten, stellen Sie zunächst sicher, dass sich die Appliance auf der Konfigurationsseite des SnapCenter VMware Plug-ins in einem deaktivierten Zustand befindet, und starten Sie dann den vCenter Web-Client-Service neu.

# Managen Sie Ihre Konfiguration

## Ändern der Zeitzonen für Backups

### Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldedaten für das SnapCenter Plug-in für die Management-GUI von VMware vSphere kennen. Sie müssen auch das MFA-Token notieren, das von der Wartungskonsole generiert wurde.

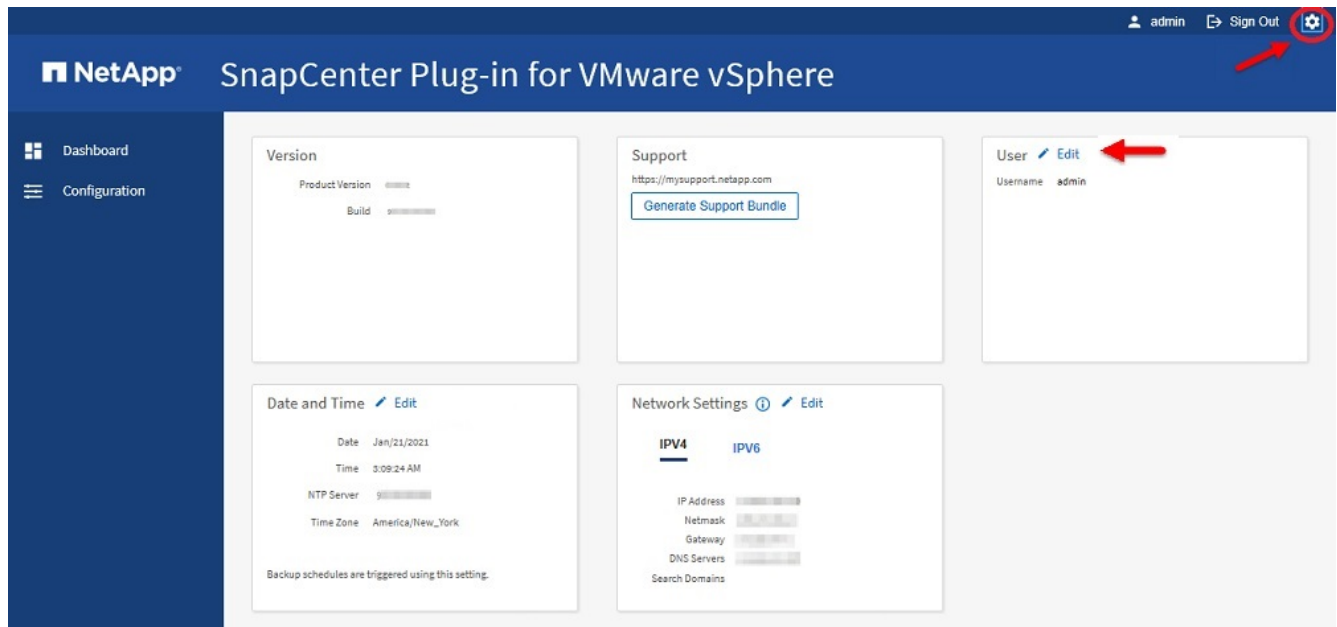
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-VMware-Plug-ins angezeigt.
- Verwenden Sie die Login-Anmeldedaten, die bei der Bereitstellung des SnapCenter VMware Plug-ins oder einer späteren Änderung zur Verfügung gestellt werden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

### Schritte

1. Melden Sie sich bei der Management-GUI von SnapCenter VMware Plug-in an.

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

2. Klicken Sie in der oberen Symbolleiste auf das Symbol Einstellungen.



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

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

## Ändern der Anmeldeinformationen

Die Anmeldeinformationen für das SnapCenter-Plug-in für die Management-GUI von

VMware vSphere können geändert werden.

### Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldedaten für das SnapCenter Plug-in für die Management-GUI von VMware vSphere kennen. Sie müssen auch das MFA-Token notieren, das von der Wartungskonsole generiert wurde.

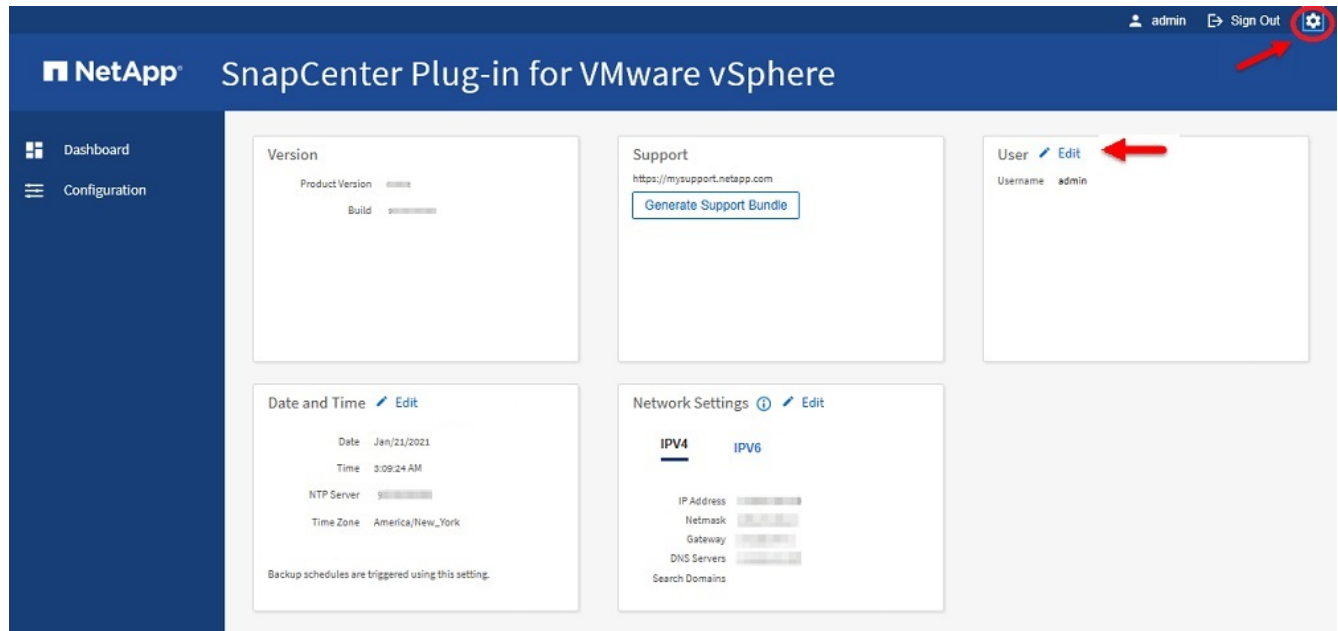
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-VMware-Plug-ins angezeigt.
- Verwenden Sie die Login-Anmeldedaten, die bei der Bereitstellung des SnapCenter VMware Plug-ins oder einer späteren Änderung zur Verfügung gestellt werden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

### Schritte

1. Melden Sie sich bei der Management-GUI von SnapCenter VMware Plug-in an.

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

2. Klicken Sie in der oberen Symbolleiste auf das Symbol Einstellungen.



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

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

## Ändern Sie die Anmeldedaten für vCenter-Anmeldung

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

## Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldedaten für das SnapCenter Plug-in für die Management-GUI von VMware vSphere kennen. Sie müssen auch das MFA-Token notieren, das von der Wartungskonsole generiert wurde.

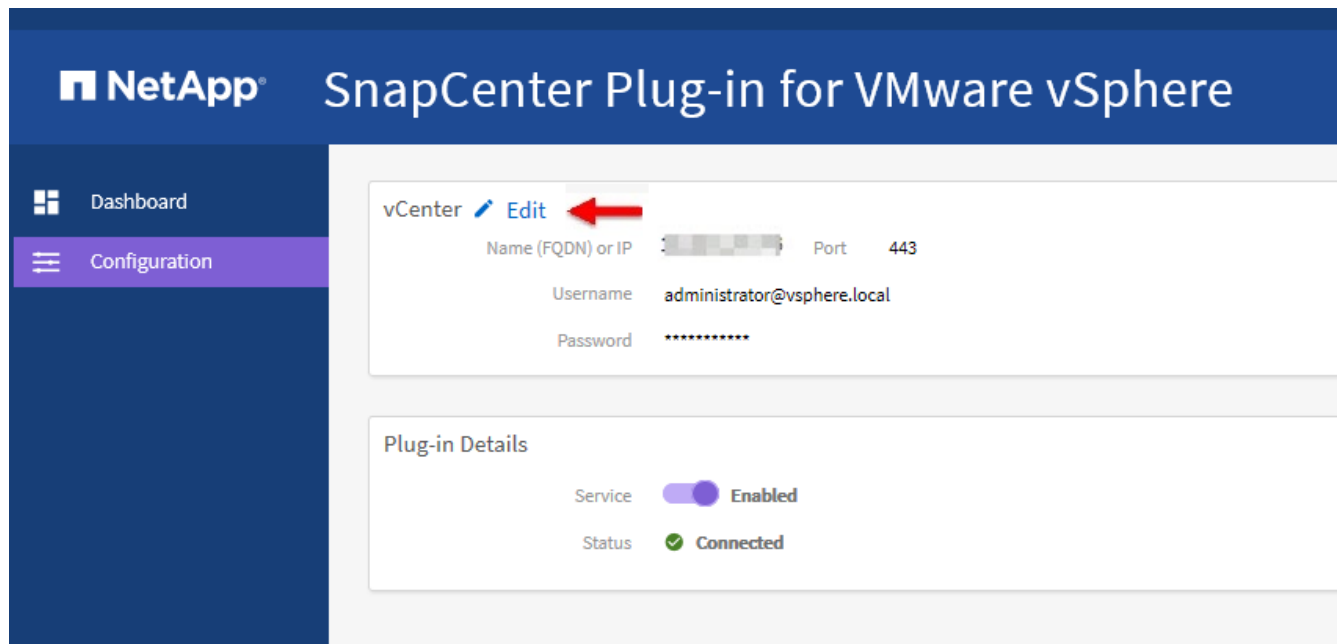
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-VMware-Plug-ins angezeigt.
- Verwenden Sie die Login-Anmeldedaten, die bei der Bereitstellung des SnapCenter VMware Plug-ins oder einer späteren Änderung zur Verfügung gestellt werden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

## Schritte

1. Melden Sie sich bei der Management-GUI von SnapCenter VMware Plug-in an.

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

2. Klicken Sie im linken Navigationsbereich auf **Konfiguration**.



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

Ändern Sie die Portnummer nicht.

## Ändern Sie die Netzwerkeinstellungen

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

## Bevor Sie beginnen

Sie müssen die IP-Adresse und die Anmeldedaten für das SnapCenter Plug-in für die Management-GUI von VMware vSphere kennen. Sie müssen auch das MFA-Token notieren, das von der Wartungskonsole generiert

wurde.

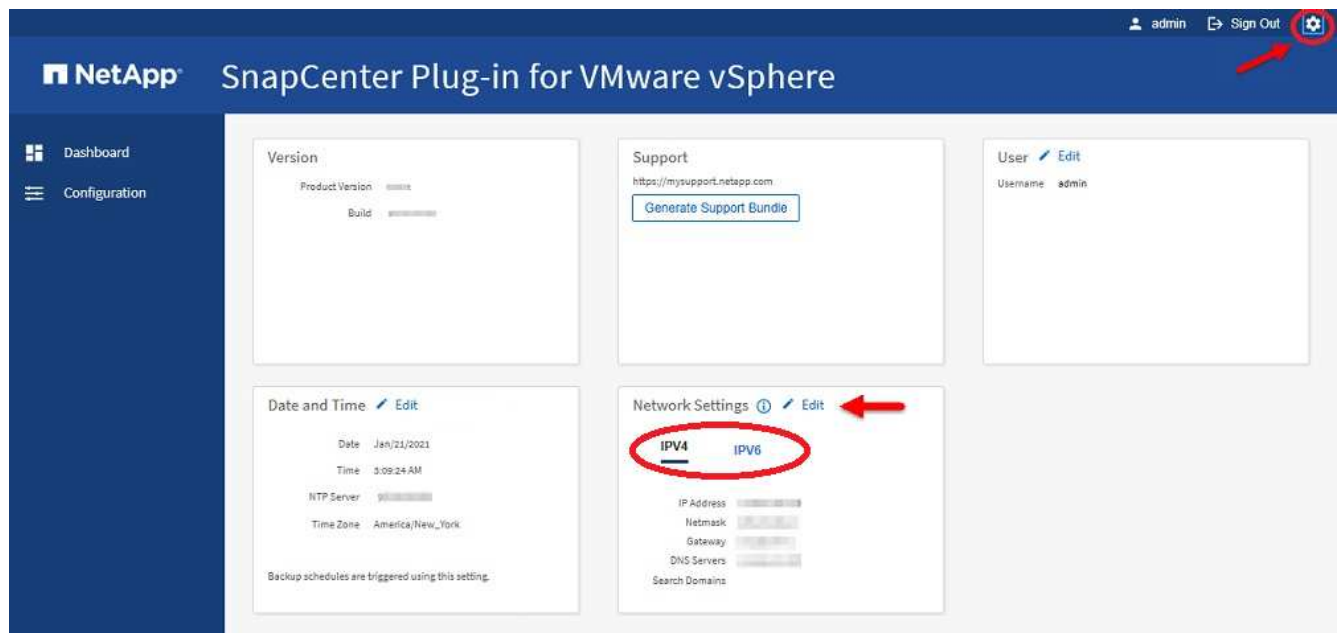
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-VMware-Plug-ins angezeigt.
- Verwenden Sie die Login-Anmeldedaten, die bei der Bereitstellung des SnapCenter VMware Plug-ins oder einer späteren Änderung zur Verfügung gestellt werden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

## Schritte

1. Melden Sie sich bei der Management-GUI von SnapCenter VMware Plug-in an.

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

2. Klicken Sie in der oberen Symbolleiste auf das Symbol Einstellungen.



3. Klicken Sie auf der Seite **Einstellungen** im Abschnitt **Netzwerkeinstellungen** auf **IPv4** oder **IPv6** und dann auf **Bearbeiten**.

Geben Sie die neuen Informationen ein und klicken Sie auf **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 klicken Sie dann auf **Speichern**.
- IPv6: Geben Sie im Feld **IP-Adresse** ein `:::0` und klicken Sie dann auf **Speichern**.



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

## Ändern Sie die Standardwerte der Konfiguration

Um die betriebliche Effizienz zu verbessern, können Sie die `scbr.override` Konfigurationsdatei so ändern, dass die Standardwerte geändert werden. Diese Werte steuern Einstellungen wie die Anzahl der während eines Backups erstellten oder



gelöschten VMware Snapshots oder die Zeit, bis ein Backup-Skript nicht mehr ausgeführt wird.

Die `scbr.override` Konfigurationsdatei wird vom SnapCenter Plug-in für VMware vSphere in Umgebungen verwendet, die applikationsbasierte SnapCenter Datensicherungsvorgänge unterstützen. Wenn diese Datei nicht vorhanden ist, müssen Sie sie aus der Vorlagendatei erstellen.

## Erstellen Sie die Konfigurationsdatei `scbr.override`

Die `scbr.override` Konfigurationsdatei wird vom SnapCenter Plug-in für VMware vSphere in Umgebungen verwendet, die applikationsbasierte SnapCenter Datensicherungsvorgänge unterstützen.

1. Gehen Sie zu `/opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.override-template`.
2. Kopieren Sie die `scbr.override-template` Datei in eine neue Datei, die im Verzeichnis aufgerufen `scbr.override` `\opt\netapp\scvservice\standalone_aegis\etc\scbr` wird.

## Eigenschaften, die Sie überschreiben können

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

- Standardmäßig verwendet die Vorlage Hash-Symbol, um die Konfigurationseigenschaften zu kommentieren. Um einen Konfigurationswert mit einer Eigenschaft zu ändern, müssen Sie die Zeichen entfernen `#`.
- Sie müssen den Service auf dem SnapCenter Plug-in für VMware vSphere Host neu starten, damit die Änderungen wirksam werden.

Sie können die folgenden Eigenschaften verwenden, die in der Konfigurationsdatei aufgeführt sind `scbr.override`, um die 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“.

- **`Deaktivier.schwächCiphers=true`**

Deaktiviert die folgenden Schwächungskipher für den Kommunikationskanal zwischen SnapCenter Plug-in für VMware vSphere und SnapCenter sowie alle zusätzlichen Schwächungskipher, die in aufgeführt sind

`include.weakCiphers: TLS_128_RSA_WITH_128_AES_256_128`

`128_CBC_SHA256_SHA256_TLS_DHE_RSA_256`

`256_SHA256_SHA256_SHA256_AES_SHA256_SHA256_SHA256_SHA256_SHA256_TLS_SHA256_SH`

`A256_SHA24_SHA24_SHA24_SHA24_SHA24_SHAEB6_SHA24_SHA24_SHAEB6_SHA24_SHA24_SH`

`A24_SHA24_SHAEBS256`

- **`Global.ds.exclusion.pattern`**

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

Beispiel 1: Der Ausdruck `global.ds.exclusion.pattern=.*21` schließt Datastores aus, die ein allgemeines Muster haben, z. B. `datastore21` und `dstest21` würden ausgeschlossen werden.

Beispiel 2: Der Ausdruck `global.ds.exclusion.pattern=ds-.*|^vol123` schließt alle Datastores aus, die (zum Beispiel) enthalten `ds-scvs-test`` oder mit `beginnen `vol123`.

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

Gibt das Zeitintervall in Sekunden an, das SnapCenter Plug-in für VMware vSphere zum Abschluss von Gastoperationen auf dem Gastsystem überwacht (Online-Festplatte und Restore-Dateien). Die gesamte Wartezeit wird von und festgelegt `guestFileRestore.online.disk.timeout`  
`guestFileRestore.restore.files.timeout`.

Der Standardwert ist „5“.

- **GuestFileRestore.MonitorIntervall=30**

Gibt das Zeitintervall in Minuten an, das das SnapCenter VMware Plug-in für die Wiederherstellung von Gastdateien mit abgelaufen ist. Jede Sitzung, die über die konfigurierte Sitzungszeit hinaus ausgeführt wird, wird getrennt.

Der Standardwert ist „30“.

- **GuestFileRestore.online.Disk.Timeout=100**

Gibt in Sekunden an, zu welcher Zeit das VMware Plug-in von SnapCenter auf die Fertigstellung eines Online-Festplattenvorgangs auf einer Gast-VM wartet. Beachten Sie, dass es eine weitere 30-Sekunden-Wartezeit gibt, bevor das Plug-in abfragt, um den Online-Festplattenvorgang abgeschlossen zu haben.

Der Standardwert ist „100“.

- **GuestFileRestore.restore.files.Timeout=3600**

Gibt die Zeit in Sekunden an, zu der das VMware Plug-in von SnapCenter auf die Fertigstellung eines Dateivorgangs auf einer Gast-VM wartet. Wenn die Zeit überschritten wird, wird der Prozess beendet und der Job als fehlgeschlagen markiert.

Der Standardwert ist "3600" (1 Stunde).

- **GuestFileRestore.robotcopy.Directory.Flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP**

Gibt die zusätzlichen robocopy-Flags an, die beim Kopieren von Verzeichnissen während der Wiederherstellung von Gastdateien verwendet werden sollen.

Entfernen oder hinzufügen Sie nicht `/NJH /NJS`, da dadurch die Analyse der Wiederherstellungsausgabe unterbrochen wird.

Erlauben Sie keine unbegrenzten Wiederholungen (durch Entfernen des `/R` Flags), da dies zu endlosen Wiederholungen für fehlgeschlagene Kopien führen kann.

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

- **GuestFileRestore.robotcopy.file.Flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP**

Gibt die zusätzlichen robocopy-Flags an, die beim Kopieren einzelner Dateien während der Wiederherstellung von Gastdateien verwendet werden sollen.

Entfernen oder hinzufügen Sie nicht `/NJH /NJS`, da dadurch die Analyse der Wiederherstellungsausgabe unterbrochen wird.

Erlauben Sie keine unbegrenzten Wiederholungen (durch Entfernen des `/R` Flags), da dies zu endlosen Wiederholungen für fehlgeschlagene Kopien führen kann.

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

- **guestFileRestore.sessionTime=1440**

Gibt die Zeit in Minuten an, zu der das SnapCenter Plug-in für VMware vSphere eine Wiederherstellungssitzung für Gastdateien aktiv hält.

Der Standardwert ist "1440" (24 Stunden).

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

Gibt an, ob beim Erstellen von Sitzungen zur Wiederherstellung von Gastdateien ein benutzerdefiniertes Skript zum Einlegen von Datenträgern und Abrufen von Laufwerksbuchstaben verwendet werden soll. Das Skript muss sich unter befinden `[Install Path] \etc\guestFileRestore_onlineDisk.ps1`. Bei der Installation wird ein Standardskript bereitgestellt. Die Werte `[Disk_Serial_Number]`, `[Online_Disk_Output]` und `[Drive_Output]` werden während des Anhängenvorgangs im Skript ersetzt.

Der Standardwert ist „false“.

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

Gibt an, dass das SnapCenter VMware Plug-in iSCSI- und FCP-Initiator-IDs von allen ESXi Hosts im Cluster in der Applikation über VMDK-Workflows umfassen sollte.

Der Standardwert ist „false“.

- **Include.schwächCiphers**

Wenn `disable.weakCiphers` auf `true` festgelegt ist, gibt die schwachen Chiffren an, die deaktiviert werden sollen, zusätzlich zu den schwachen Chiffren, die standardmäßig deaktiviert werden `disable.weakCiphers`.

- **Max.Concurrent.ds.Storage.query.count=15**

Gibt die maximale Anzahl gleichzeitiger Anrufe an, die das SnapCenter VMware Plug-in zum SnapCenter Server führen kann, um den Storage-Platzbedarf für die Datenspeicher zu ermitteln. Das Plug-in ruft diese Anrufe ab, wenn Sie den Linux-Dienst auf dem SnapCenter-VMware-Plug-in-VM-Host neu starten.

- **nfs.Datastore.Mount.retry.count=3**

Gibt die maximale Anzahl der Male an, die das SnapCenter VMware Plug-in versucht, ein Volume als NFS-

Datenspeicher in vCenter zu mounten.

Der Standardwert ist „3“.

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

Gibt die Zeit in Millisekunden an, die das SnapCenter VMware Plug-in zwischen den Versuchen wartet, ein Volume als NFS-Datenspeicher in vCenter zu mounten,

Der Standardwert ist „60000“ (60 Sekunden).

- **script.virtual.machine.count.variable.name= VIRTUELLE\_MASCHINEN**

Gibt den Namen der Umgebungsvariable an, der die Anzahl der virtuellen Maschinen enthält. Sie müssen die Variable definieren, bevor Sie während eines Backup-Jobs benutzerdefinierte Skripte ausführen.

BEISPIELSWEISE bedeutet VIRTUAL\_MACHINES=2, dass zwei virtuelle Maschinen gesichert werden.

- **script.virtual.machine.info.variable.name=VIRTUAL\_MACHINE.%s**

Gibt den Namen der Umgebungsvariable an, die Informationen über die n. Virtuelle Maschine im Backup enthält. Sie müssen diese Variable festlegen, bevor Sie während einer Sicherung benutzerdefinierte Skripts ausführen.

Beispielsweise liefert die Umgebungsvariable VIRTUAL\_MACHINE.2 Informationen über die zweite virtuelle Maschine im Backup.

- \* **script.virtual.machine.info.format= %s \***

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

Im Folgenden finden Sie ein Beispiel für die Informationen, die Sie bereitstellen können:

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

- **Storage.connection.Timeout=600000**

Gibt den Zeitraum in Millisekunden an, den der SnapCenter-Server auf eine Antwort des Storage-Systems wartet.

Der Standardwert ist "600000" (10 Minuten).

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

Es gibt keinen Standardwert. Sie verwenden diesen Wert, um die ESXi IP-Adresse der VMkernel IP-Adresse zuzuordnen. Das SnapCenter VMware Plug-in verwendet standardmäßig die Management-VMkernel-Adapter-IP-Adresse des ESXi Hosts. Wenn das SnapCenter VMware Plug-in eine andere IP-Adresse für den VMkernel-Adapter verwenden soll, müssen Sie einen Überschreibwert angeben.

Im folgenden Beispiel ist die IP-Adresse des Management-VMkernel-Adapters 10.225.10.56; das SnapCenter VMware Plug-in verwendet jedoch die angegebene Adresse von 10.225.11.57 und 10.225.11.58. Und wenn die Management-VMkernel-Adapter-IP-Adresse 10.225.10.60 ist, verwendet das Plug-in die Adresse 10.225.11.61.

```
vmware.esx.ip.kernel.ip.map=10.225.10.56:10.225.11.57,10.225.11.58;  
10.225.10.60:10.225.11.61
```

- **vmware.max.Concurrent.Snapshots=30**

Gibt die maximale Anzahl gleichzeitiger VMware Snapshots an, die das SnapCenter VMware Plug-in auf dem Server durchführt.

Diese Zahl wird pro Datenspeicher geprüft und nur dann aktiviert, wenn für die Richtlinie „VM-konsistent“ ausgewählt ist. Wenn Sie absturzkonsistente Backups durchführen, gilt diese Einstellung nicht.

Der Standardwert ist „30“.

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

Gibt die maximale Anzahl von gleichzeitigen Löschvorgängen von VMware Snapshots pro Datenspeicher an, die das SnapCenter VMware Plug-in auf dem Server durchführt.

Diese Nummer wird pro Datenspeicher geprüft.

Der Standardwert ist „30“.

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

Gibt die maximale Anzahl an Meiten an, die das SnapCenter VMware Plug-in erneut versucht, eine Anfrage über nicht behobene Volumes zu senden, da das „...Zeitlimit beim Abhalten von I/O...“-Fehlern liegt.

Der Standardwert ist „10“.

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

Gibt die maximale Anzahl von Male an, die das SnapCenter VMware Plug-in erneut versucht, eine Abfrage über VMware-Snapshots zu senden, weil die „...Zeitgrenze zum Abhalten von I/O...“-Fehlern während eines Backups beträgt.

Der Standardwert ist „0“.

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

Gibt den Zeitraum an, in Sekunden, den das SnapCenter VMware Plug-in zwischen dem Senden der Abfragen zum VMware-Snapshot „...Time Limit for Hold off I/O...“-Fehler während eines Backups wartet.

Der Standardwert ist „5“.

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

Gibt den Zeitraum in Millisekunden an, den das SnapCenter VMware Plug-in zwischen dem Senden von Anfragen zu nicht behobenen Volumes wartet, da es „...Zeitlimit für das Warten auf I/O...“-Fehler gibt. Dieser Fehler tritt auf, wenn ein VMFS-Datastore geklont wird.

Der Standardwert ist „60000“ (60 Sekunden).

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

Gibt die maximale Anzahl der Male an, die das SnapCenter VMware Plug-in erneut versucht, eine Anfrage

über die Neukonfiguration einer VM zu senden, da das „...Zeitlimit zum Abhalten von I/O...“-Fehlern beträgt.

Der Standardwert ist „10“.

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

Gibt die maximale Zeit in Millisekunden an, die das SnapCenter VMware Plug-in zwischen dem Senden von Abfragen bezüglich der Neukonfiguration einer VM wartet, weil die „...Zeitgrenze zum Abhalten von I/O...“-Fehlern beträgt.

Der Standardwert ist „30000“ (30 Sekunden).

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

Gibt an, wie lange das SnapCenter VMware Plug-in in Millisekunden zwischen dem Senden der Abfragen zum erneuten Scannen des Host-Bus-Adapters wartet, da es „...Zeitlimit für das Abhalten von I/O...“-Fehlern gibt.

Der Standardwert ist „3“.

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

Gibt die maximale Anzahl an Male an, die das SnapCenter VMware Plug-in Anfragen wiederholt, um den Host Bus Adapter erneut zu scannen.

Der Standardwert ist „30000“.

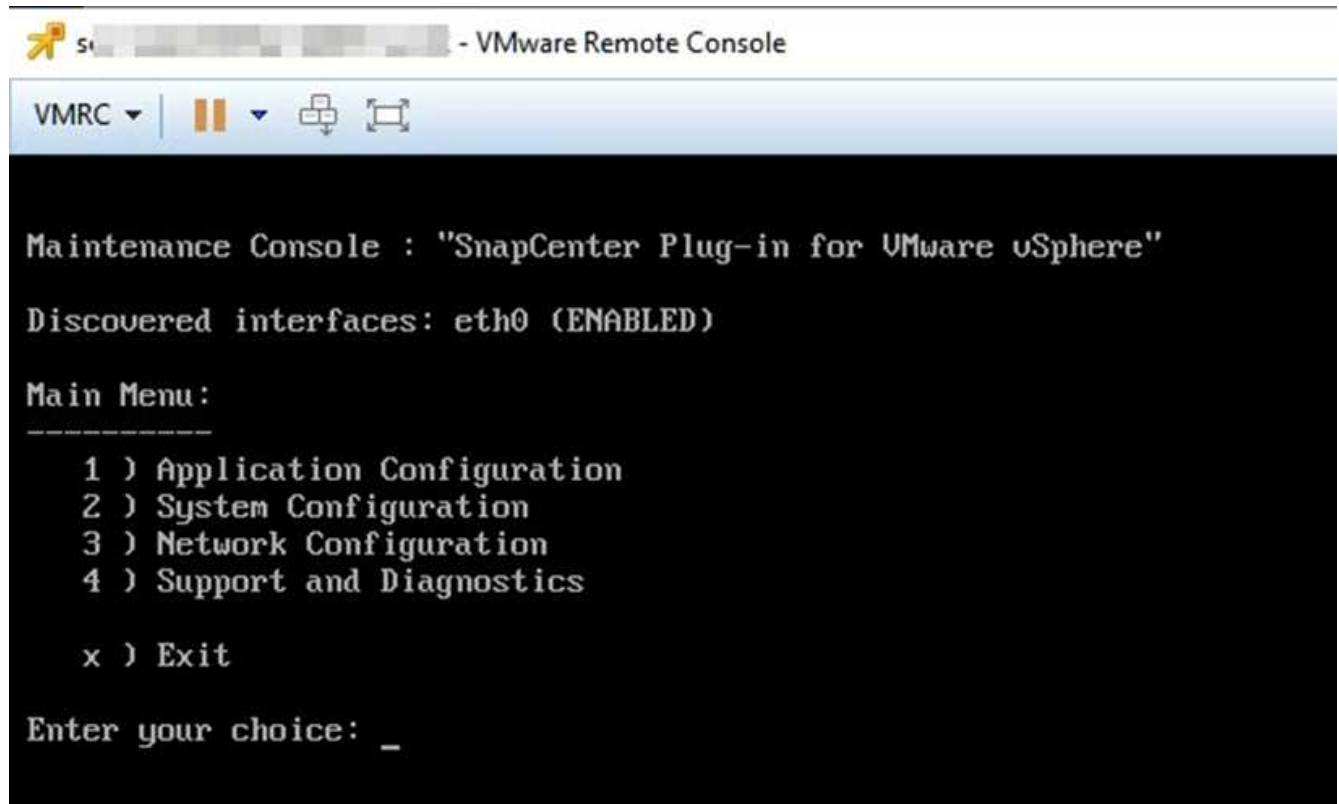
## Aktivieren Sie das SSH for SnapCenter Plug-in für VMware vSphere

Bei der Implementierung des SnapCenter VMware Plug-ins ist SSH standardmäßig deaktiviert.

### Schritte

1. Wählen Sie auf dem VMware vSphere-Client die VM aus, auf der sich das SnapCenter VMware Plug-in befindet.
2. Klicken Sie mit der rechten Maustaste auf die VM und dann auf der Registerkarte **Zusammenfassung** der virtuellen Appliance auf **Remote-Konsole starten**, um ein Fenster der Wartungskonsole zu öffnen und sich dann anzumelden.

Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter ["Öffnen Sie die Wartungskonsole"](#).



The screenshot shows a VMware Remote Console window titled "VMware Remote Console". The interface includes a toolbar with "VMRC", a pause button, a refresh button, and a full-screen button. The main display area shows the following text:

```
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)

Main Menu:
-----
 1 ) Application Configuration
 2 ) System Configuration
 3 ) Network Configuration
 4 ) Support and Diagnostics

 x ) Exit

Enter your choice: _
```

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

# Rest-APIs

## Überblick

Sie können das SnapCenter Plug-in für VMware vSphere REST-APIs verwenden, um allgemeine Datensicherungsvorgänge auszuführen. Das Plug-in hat verschiedene Swagger-Webseiten von den Windows SnapCenter-Swagger-Webseiten.

- REST-API-Workflows werden für folgende Operationen auf VMs und Datastores dokumentiert. Dazu verwendet die REST-APIs für VMware vSphere:
  - Fügen Sie Storage-VMs und -Cluster hinzu, ändern oder löschen Sie sie
  - Ressourcengruppen erstellen, ändern und löschen
  - Backup von geplanten und On-Demand-VMs
  - Wiederherstellung vorhandener VMs und gelöschter VMs
  - Wiederherstellung von VMDKs
  - Anschließen und Trennen von VMDKs
  - Mounten und Unmounten von Datastores
  - Laden Sie Jobs herunter und erstellen Sie Berichte
  - Integrierte Zeitpläne ändern
- Operationen, die von DEN REST-APIs für VMware vSphere nicht unterstützt werden
  - Wiederherstellung von Gastdateien
  - Installation und Konfiguration des SnapCenter VMware Plug-ins
  - Weisen Sie Benutzern RBAC-Rollen oder -Zugriff zu
- `uri` Parameter

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

- Zeitüberschreitung bei der Anmeldung

Die standardmäßige Zeitüberschreitung beträgt 120 Minuten (2 Stunden). In den vCenter-Einstellungen können Sie einen anderen Timeout-Wert konfigurieren.

- Token-Management

REST-APIs verwenden aus Sicherheitsgründen ein obligatorisches Token, das mit jeder Anforderung übergeben wird und in allen API-Aufrufen zur Client-Validierung verwendet wird. DIE REST-APIs für VMware vSphere erhalten das Token mithilfe der VMware-Authentifizierungs-API. VMware stellt das Token-Management bereit.

Verwenden Sie zum Abrufen des Tokens `/4.1/auth/login` REST API und geben Sie die vCenter-Anmeldedaten ein.

- API-Versionsbezeichnungen

Jeder REST-API-Name enthält die SnapCenter-Versionsnummer, in der die REST-API zum ersten Mal freigegeben wurde. Beispielsweise wurde die REST-API `/4.1/datastores/{moref}/backups` zum



ersten Mal im SnapCenter 4.1 veröffentlicht.

REST-APIs in zukünftigen Versionen werden in der Regel abwärtskompatibel sein und je nach Bedarf an neuen Funktionen angepasst werden.

## Greifen Sie über die Swagger API-Webseite auf REST-APIs zu

REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um entweder den SnapCenter-Server oder das SnapCenter-Plug-in für VMware vSphere REST-APIs anzuzeigen und einen API-Aufruf manuell auszuführen. Verwenden Sie das SnapCenter Plug-in für VMware vSphere REST-APIs zur Durchführung von Vorgängen bei VMs und Datastores.

Das Plug-in hat verschiedene Swagger-Webseiten von den SnapCenter-Serverdolch-Webseiten.

### Bevor Sie beginnen

Beim SnapCenter Plug-in für VMware vSphere REST-APIs müssen Sie entweder die IP-Adresse oder den Host-Namen des SnapCenter VMware Plug-ins kennen.



Das Plug-in unterstützt nur REST APIs zur Integration mit Applikationen anderer Anbieter. PowerShell Commandlets oder CLI werden nicht unterstützt.

### Schritte

1. Geben Sie in einem Browser die URL ein, um auf die Plug-in Swagger Webseite zuzugreifen:

```
https://<SCV_IP>:8144/api/swagger-ui/index.html
```



Verwenden Sie nicht die folgenden Zeichen in DER REST-API-URL: +, ., % Und &.

### Beispiel

Zugriff auf die SnapCenter VMware Plug-in REST-APIs:

```
https://<SCV_IP>:8144/api/swagger-ui/index.html  
https://OVAhost:8144/api/swagger-ui/index.html
```

Melden Sie sich mit dem vCenter-Authentifizierungsmechanismus an, um das Token zu generieren.

2. Klicken Sie auf einen API-Ressourcentyp, um die APIs in diesem Ressourcentyp anzuzeigen.

## REST-API-Workflows zum Hinzufügen und Ändern von Storage-VMs

Zum Hinzufügen und Ändern von Storage-VM-Vorgängen mit dem SnapCenter Plug-in für VMware vSphere REST-APIs müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>` , um

einen vollständigen Endpunkt zu bilden.

So fügen Sie Storage-VM-Vorgänge hinzu:

Schritt	REST API	Kommentare
1	/4.1/storage-system	Add Storage System Fügt die angegebene Storage-VM zum SnapCenter-Plug-in für VMware vSphere hinzu.

Führen Sie den folgenden Workflow aus, um Vorgänge für Storage-VMs zu ändern:

Schritt	REST API	Kommentare
1	/4.1/storage-system	getSvmAll Ruft die Liste aller verfügbaren Storage VMs ab. Beachten Sie den <b>Namen</b> der Speicher-VM, die Sie ändern möchten.
2	/4.1/storage-system	Modify Storage System Ändert die angegebene Storage-VM. Übergeben Sie den <b>Name</b> aus Schritt 1 zusätzlich zu allen anderen erforderlichen Attributen.

## REST-API-Workflows zum Erstellen und Ändern von Ressourcengruppen

Zum Erstellen und Ändern von Gruppenoperationen über das SnapCenter Plug-in für VMware vSphere REST-APIs müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

Gehen Sie zum Erstellen von Ressourcengruppen wie folgt vor:

Schritt	REST API	Kommentare
1	/4.1/policies	Get Policies Ruft die Liste der VMware vSphere Client-Richtlinien ab. Beachten Sie die <b>Richtliniend</b> , die Sie beim Erstellen der Ressourcengruppe und der Richtlinie <b>Frequency</b> verwenden möchten. Wenn keine Richtlinien aufgeführt sind, erstellen Sie mit der Create Policy REST API eine neue Richtlinie.

Schritt	REST API	Kommentare
2	/4.1/resource-groups	Create a Resource Group Erstellt eine Ressourcengruppe mit der angegebenen Richtlinie. Geben Sie die <b>RichtlinieID</b> aus Schritt 1 ein und geben Sie zusätzlich zu allen anderen erforderlichen Attributen die Richtlinie <b>Frequenz</b> -Details ein.

Gehen Sie wie folgt vor, um Ressourcengruppen zu ändern:

Schritt	REST API	Kommentare
1	/4.1/resource-groups	Get List of Resource Groups Ruft die Liste der VMware vSphere Client-Ressourcengruppen ab. Beachten Sie die <b>resourceGroupID</b> , die Sie ändern möchten.
2	/4.1/policies	Wenn Sie die zugewiesenen Richtlinien ändern möchten, Get Policies ruft die Liste der VMware vSphere-Client-Richtlinien ab. Beachten Sie die <b>Policy ID</b> , die Sie beim Ändern der Ressourcengruppe und der Richtlinie <b>Frequency</b> verwenden möchten.
3	/4.1/resource-groups/{resourceGroupId}	Update a Resource Group Ändert die angegebene Ressourcengruppe. Übergeben Sie die <b>resourceGroupID</b> von Schritt 1. Übergeben Sie optional die <b>policyID</b> aus Schritt 2 und geben Sie zusätzlich zu allen anderen erforderlichen Attributen die <b>Frequency</b> -Details ein.

## REST-API-Workflow für Backup nach Bedarf

Um Backup-Vorgänge On-Demand mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, 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. Beachten Sie die <b>resourceGroupID</b> und die <b>Policy ID</b> für die Ressourcengruppe, die Sie sichern möchten.
2	/4.1/resource-groups/backupnow	Run a backup on a Resource Group Sichert die Ressourcengruppe nach Bedarf. Übergeben Sie die <b>resourceGroupID</b> und die <b>policyId</b> aus Schritt 1.

## REST-API-Workflow zur Wiederherstellung von VMs

Um die Restore-Vorgänge für VM-Backups mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

Schritt	REST API	Kommentare
1	Gehen Sie zu <code>http://&lt;vCenter-IP&gt;/mob</code>	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den <b>moref</b> für die VM, die Sie wiederherstellen möchten.
2	/4.1/vm/{moref}/backups	Get VM Backups Ruft eine Liste der Backups für die angegebene VM ab. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>Backupid</b> des Backups, das Sie wiederherstellen möchten.
3	/4.1/vm/backups/{backupId} / snapshotlocations	Get snapshot locations Ruft den Speicherort des Snapshots für das angegebene Backup ab. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Beachten Sie die <b>snapshotStandorteList</b> Informationen.

Schritt	REST API	Kommentare
4	/4.1/vm/{moref}/backups/availableesxhosts	Get available ESX Hosts Ruft die Informationen für den Host ab, auf dem das Backup gespeichert ist. Beachten Sie die <b>verfügbarEsxHostsList</b> Informationen.
5	/4.1/vm/{moref}/backups/{backupId}/restore	Restore a VM from a backup Stellt das angegebene Backup wieder her. Geben Sie die Informationen aus den Schritten 3 und 4 im Attribut <b>restoreLocations</b> weiter.  <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">  Wenn es sich bei der VM-Sicherung um ein partielles Backup handelt, setzen Sie den <code>restartVM</code> Parameter auf „false“. </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">  Sie können keine VM wiederherstellen, die eine Vorlage ist. </div>

## REST-API-Workflow zur Wiederherstellung gelöschter VMs

Um die Restore-Vorgänge für VM-Backups mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

Schritt	REST API	Kommentare
1	Gehen Sie zu <code>http://&lt;vCenter-IP&gt;/mob</code>	Suchen Sie die VM-UUID aus der URL der von VMware gemanagten Objekte. Beachten Sie die <b>UUID</b> für die VM, die Sie wiederherstellen möchten.

Schritt	REST API	Kommentare
2	/4.1/vm/{uuid}/backups	Get VM Backups Ruft eine Liste der Backups für die angegebene VM ab. Geben Sie die <b>UUID</b> von Schritt 1. Beachten Sie die <b>Backupid</b> des Backups, das Sie wiederherstellen möchten.
3	/4.1/vm/backups/{backupId}/ /snapshotlocations	Get snapshot locations Ruft den Speicherort des Snapshots für das angegebene Backup ab. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Beachten Sie die <b>snapshotStandorteList</b> Informationen.
4	/4.1/vm/{moref}/backups/ availableesxhosts	Get available ESX Hosts Ruft die Informationen für den Host ab, auf dem das Backup gespeichert ist. Beachten Sie die <b>verfügbarEsxHostsList</b> Informationen.
5	/4.1/vm/{uuid}/backups/ {backupId}/restore	Restore VM from a backup using uuid or restore a deleted VM Stellt das angegebene Backup wieder her. Geben Sie die <b>UUID</b> von Schritt 1. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Geben Sie die Informationen aus den Schritten 3 und 4 im Attribut <b>restoreLocations</b> weiter. Wenn es sich bei der VM-Sicherung um ein partielles Backup handelt, setzen Sie den <b>restartVM</b> Parameter auf „false“. <b>Hinweis:</b> eine VM, die eine Vorlage ist, kann nicht wiederhergestellt werden.

## REST-API-Workflow zur Wiederherstellung von VMDKs

Um Restore-Vorgänge für VMDKs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

Schritt	REST API	Kommentare
1	Gehen Sie zu <code>http://&lt;vCenter-IP&gt;/mob</code>	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den <b>moref</b> für die VM, in der sich die VMDK befindet.
2	<code>/4.1/vm/{moref}/backups</code>	Get VM Backups Ruft eine Liste der Backups für die angegebene VM ab. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>Backupid</b> des Backups, das Sie wiederherstellen möchten.
3	<code>/4.1/vm/backups/{backupId}/ snapshotlocations</code>	Get snapshot locations Ruft den Speicherort des Snapshots für das angegebene Backup ab. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Beachten Sie die <b>snapshotStandorteList</b> Informationen.
4	<code>/4.1/vm/{moref}/backups/ vmdklocations</code>	Get Vmdk Locations Ruft eine Liste der VMDKs für die angegebene VM ab. Beachten Sie die <b>vmdk-StandorteList</b> -Informationen.
5	<code>/4.1/vm/{ moref}/backups/ {backupId}/ availabledatastores</code>	Get Available Datastores Ruft eine Liste der Datastores ab, die für den Wiederherstellungsvorgang verfügbar sind. Übergeben Sie den <b>moref</b> von Schritt 1. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Beachten Sie die <b>DatastoreNameList</b> -Informationen.
6	<code>/4.1/vm/{moref}/backups/ availableesxhosts</code>	Get available ESX Hosts Ruft die Informationen für den Host ab, auf dem das Backup gespeichert ist. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>verfügbarEsxHostsList</b> Informationen.

Schritt	REST API	Kommentare
7	/4.1/vm/{moref}/backups/{backupId}/restorevmdks	<p>Restore a VMDK from a backup Stellt die angegebene VMDK aus dem angegebenen Backup wieder her. Geben Sie im Attribut <b>esxHost</b> die Informationen aus <b>availEsxHostsList</b> in Schritt 6 weiter. Geben Sie die Informationen von den Schritten 3 bis 5 an das Attribut <b>VMDKsRestoreLocations</b> weiter:</p> <ul style="list-style-type: none"> <li>• Geben Sie im Attribut <b>RestoresFromLocation</b> die Informationen aus <b>snapshotStandorteList</b> in Schritt 3 weiter.</li> <li>• Geben Sie im Attribut <b>VMDKsToRestore</b> die Informationen aus <b>VMDKs-StandorteList</b> in Schritt 4 weiter.</li> <li>• Geben Sie im Attribut <b>restoreToDatastore</b> die Informationen aus <b>DatastoreNameList</b> in Schritt 5 weiter.</li> </ul>

## REST-API-Workflows zum Verbinden und Trennen von VMDKs


Um mithilfe des SnapCenter Plug-ins für VMware vSphere REST-APIs Verbindungen zu und Abtrennen von VMDKs durchzuführen, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

### Gehen Sie wie folgt vor, um VMDKs anzuhängen:

Schritt	REST API	Kommentare
1	Gehen Sie zu <code>http://&lt;vCenter-IP&gt;/mob</code>	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den <b>moref</b> für die VM, an die Sie eine VMDK anhängen möchten.



Schritt	REST API	Kommentare
2	/4.1/vm/{moref}/backups	Get VM Backups Ruft eine Liste der Backups für die angegebene VM ab. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>Backupid</b> des Backups, das Sie wiederherstellen möchten.
3	/4.1/vm/{moref}/backups/{backupId}/vmdklocations	Get VMDK Locations Ruft eine Liste der VMDKs für die angegebene VM ab. Bestehen Sie die <b>Backupid</b> aus Schritt 2 und den <b>moref</b> aus Schritt 1. Beachten Sie die <b>vmdk-StandorteList</b> -Informationen.
4	/4.1/vm/{moref}/attachvmdks	<p>Attach VMDKs Bindet die angegebene VMDK an die ursprüngliche VM an. Bestehen Sie die <b>Backupid</b> aus Schritt 2 und den <b>moref</b> aus Schritt 1. Geben Sie die <b>VMDKs StandorteListe</b> von Schritt 3 bis zum Attribut <b>VMDKs Locations</b> weiter.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Um eine VMDK an eine andere VM anzuhängen, übergeben Sie den <b>moref</b> der Ziel-VM im <b>altersVmMoref</b> Attribut.</p> </div>

### Gehen Sie zum Trennen von VMDKs wie folgt vor:

Schritt	REST API	Kommentare
1	Gehen Sie zu <code>http://&lt;vCenter-IP&gt;/mob</code>	Suchen Sie den VM-moref aus der URL der von VMware gemanagten Objekte. Beachten Sie den <b>moref</b> für die VM, auf der Sie eine VMDK abtrennen möchten.
2	/4.1/vm/{moref}/backups	Get VM Backups Ruft eine Liste der Backups für die angegebene VM ab. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>Backupid</b> des Backups, das Sie wiederherstellen möchten.

Schritt	REST API	Kommentare
3	/4.1/vm/{moref}/backups/{backupId}/vmdklocations	Get VMDK Locations Ruft eine Liste der VMDKs für die angegebene VM ab. Bestehen Sie die <b>Backupid</b> aus Schritt 2 und den <b>moref</b> aus Schritt 1. Beachten Sie die <b>vmdk-StandorteList</b> -Informationen.
4	/4.1/vm/{moref}/detachvmdks	Detach VMDKs Trennt die angegebene VMDK. Übergeben Sie den <b>moref</b> von Schritt 1. Geben Sie die VMDK <b>vmdk-StandorteListe</b> Details von Schritt 3 bis zum <b>VMDKs ToDetach</b> -Attribut.

## REST-API-Workflows zum Mounten und Unmounten von Datastores

Um Mount- und Unmount-Vorgänge für Datastore-Backups mit dem SnapCenter Plug-in für VMware vSphere REST-APIs durchzuführen, müssen Sie die vorgegebene Sequenz von REST-API-Aufrufen befolgen.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

### Folgen Sie zum Mounten von Datastores diesem Workflow:

Schritt	REST API	Kommentare
1	Gehen Sie zu <code>http://&lt;vCenter-IP&gt;/mob</code>	Suchen Sie den Datastore-moref aus der URL von VMware Managed Objects. Beachten Sie den <b>moref</b> für den Datastore, den Sie mounten möchten.
2	/4.1/datastores/{moref}/backups	Get the list of backups for a datastore Ruft eine Liste der Backups für den angegebenen Datastore ab. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>Backupid</b> , die Sie montieren möchten.

Schritt	REST API	Kommentare
3	/4.1/datastores/backups/{backupId}/snapshotlocations	Get the list of Snapshot Locations Ruft Details zum Speicherort des angegebenen Backups ab. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Beachten Sie den <b>Datastore</b> und den Standort aus der Liste <b>snapshotStandorteList</b> .
4	/4.1/datastores/{moref}/availableEsxHosts	Get the list of Available Esxi Hosts Ruft die Liste der ESXi-Hosts ab, die für Mount-Vorgänge verfügbar sind. Übergeben Sie den <b>moref</b> von Schritt 1. Beachten Sie die <b>verfügbarEsxHostsList</b> Informationen.
5	/4.1/datastores/backups/{backupId}/mount	Mount datastores for a backup Mountet das angegebene Datastore-Backup. Übergeben Sie die <b>Backupid</b> aus Schritt 2. Geben Sie in den Attributen <b>Datastore</b> und <b>Location</b> die Informationen aus Schritt 3 weiter snapshotLocationsList . Geben Sie im Attribut <b>esxHostName</b> die Informationen aus <b>availEsxHostsList</b> in Schritt 4 weiter.

### Folgen Sie zum Unmounten von Datastores diesem Workflow:

Schritt	REST API	Kommentare
1	/4.1/datastores/backups/{backupId}/mounted	Get the list of mounted datastores. Beachten Sie den Datenspeicher <b>moref(s)</b> , den Sie unmounten möchten.
2	/4.1/datastores/unmount	UnMount datastores for a backup Hängt das angegebene Datastore-Backup ab. Übergeben Sie den Datenspeicher <b>moref(s)</b> aus Schritt 1.

## REST-APIs zum Herunterladen von Jobs und zum Generieren von Berichten

Zum Generieren von Berichten und Herunterladen von Protokollen für VMware vSphere Client-Jobs mithilfe des SnapCenter Plug-ins für VMware vSphere REST-APIs müssen

SIE DIE REST-API-Aufrufe für VMware vSphere verwenden.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um einen vollständigen Endpunkt zu bilden.

**Verwenden Sie die folgenden REST-APIs im Abschnitt Jobs, um detaillierte Informationen über Jobs zu erhalten:**

REST API	Kommentare
<code>/4.1/jobs</code>	Get all jobs Ruft die Jobdetails für mehrere Jobs ab. Sie können den Umfang der Anforderung einschränken, indem Sie einen Jobtyp angeben, z. B. <code>backup</code> , <code>mountBackup</code> oder <code>restore</code> .
<code>/4.1/jobs/{id}</code>	Get job details Ruft detaillierte Informationen für den angegebenen Job ab.

**Verwenden Sie die folgende REST-API im Abschnitt Jobs zum Herunterladen von Jobprotokollen:**

REST API	Kommentare
<code>/4.1/jobs/{id}/logs</code>	<code>getJobLogsById</code> lädt die Protokolle für den angegebenen Job herunter.

**Verwenden Sie die folgenden REST-APIs im Abschnitt Berichte zum Generieren von Berichten:**

REST API	Kommentare
<code>4.1/reports/protectedVM</code>	Get Protected VM List Ruft eine Liste der geschützten VMs der letzten sieben Tage ab.
<code>/4.1/reports/unProtectedVM</code>	Get Unprotected VM List Ruft eine Liste der ungeschützten VMs der letzten sieben Tage ab.

## REST-API-Workflow zum Ändern integrierter Zeitpläne

Um integrierte Zeitpläne für VMware vSphere Client-Jobs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs zu ändern, müssen Sie die vorgeschriebene Sequenz von REST-API-Aufrufen befolgen.

Integrierte Zeitpläne sind die Zeitpläne, die als Teil des Produkts bereitgestellt werden, z. B. der Zeitplan für den MySQL-Datenbank-Dump. Sie können die folgenden Zeitpläne ändern:

Schedule-DatabaseDump  
Schedule-PurgeBackups  
Schedule-AsupDataCollection  
Schedule-ComputeStorageSaving  
Schedule-PurgeJobs

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>`, um

einen vollständigen Endpunkt zu bilden.

Schritt	REST API	Kommentare
1	/4.1/schedules	Get all built-in Zeitpläne ruft eine Liste der Jobpläne ab, die ursprünglich im Produkt bereitgestellt wurden. Notieren Sie sich den Planungsnamen, den Sie ändern möchten, und den zugeordneten cron-Ausdruck.
2	/4.1/schedules	Modify any built-in schedule Ändert den angegebenen Zeitplan. Übergeben Sie den Planungsnamen aus Schritt 1 und erstellen Sie einen neuen cron-Ausdruck für den Zeitplan.

## REST-API zum Markieren von eingeklemmten Jobs als fehlgeschlagen

Um Job-IDs für VMware vSphere-Client-Jobs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs zu finden, müssen DIE REST-API-Aufrufe für VMware vSphere verwendet werden. Diese REST-APIs wurden im SnapCenter Plug-in für VMware vSphere 4.4 hinzugefügt.

Fügen Sie für jede REST-API `https://<server>:<port>` an der Vorderseite der REST-API hinzu, um einen vollständigen Endpunkt zu bilden.

Verwenden Sie die folgende REST-API im Abschnitt Jobs, um Jobs zu ändern, die sich in einem laufenden Zustand befinden, in einen fehlgeschlagenen Status:

REST API	Kommentare
/4.1/jobs/{id}/failJobs	Wenn Sie die IDs von Jobs übergeben, die in einem laufenden Status stecken, <code>failJobs</code> markiert diese Jobs als fehlgeschlagen. Um Jobs zu identifizieren, die sich in einem laufenden Zustand befinden, können Sie über die Job-Monitor-GUI den Status jedes Jobs und die Job-ID anzeigen.

## REST-APIs zur Erstellung von Prüfprotokollen

Sie können die Audit-Log-Details von Swagger Rest APIs sowie die SCV Plugin-Benutzeroberfläche sammeln.

Unten sind die Swagger Rest APIs angegeben:

1. ERHALTEN Sie 4.1/Audit/Logs: Erhalten Sie Audit-Daten für alle Protokolle
2. GET 4.1/Audit/logs/{filename}: Get Audit-Daten für eine bestimmte Protokolldatei

3. NACH 4.1/Audit/Verify: Prüfung des Prüfprotokolls auslösen
4. GET 4.1/Audit/config: Get the Audit and syslog Server config
5. PUT 4.1/Audit/config: Aktualisieren Sie die Audit- und syslog-Server-Konfiguration

Um Prüfprotokolle für VMware vSphere Client-Jobs mit dem SnapCenter Plug-in für VMware vSphere REST-APIs zu generieren, müssen REST-API-Aufrufe für VMware vSphere verwendet werden.

Fügen Sie für jede REST-API an der Vorderseite der REST-API hinzu `https://<server>:<port>/api`, um einen vollständigen Endpunkt zu bilden.

Verwenden Sie die folgenden REST-APIs im Abschnitt Jobs, um detaillierte Informationen über Jobs zu erhalten:

REST API	Kommentare
4.1/audit/logs	Gibt Audit-Log-Dateien mit Integritätsdaten zurück
4.1/audit/logs/{filename}	Erhalten Sie eine spezifische Audit-Log-Datei mit Integritätsdaten
4.1/audit/verify	Löst die Überprüfung des Audits aus
4.1/audit/syslogcert	Aktualisiert das Syslog-Serverzertifikat

# Upgrade

## Upgrade von einer früheren Version des SnapCenter Plug-ins für VMware vSphere



Das Upgrade auf SCV 5.0 wird nur auf VMware vCenter Server 7 Update 1 und höheren Versionen unterstützt. Für VMware vCenter Server vor Version 7 Update 1 sollten Sie weiterhin SCV 4.7 verwenden. Bei nicht unterstützten Versionen des VMware vCenter Servers wird das Upgrade nicht beeinträchtigt.

Wenn Sie das SnapCenter Plug-in für virtuelle VMware vSphere Appliance verwenden, können Sie ein Upgrade auf eine neuere Version durchführen. Beim Upgrade-Prozess wird das bestehende Plug-in wieder registriert und ein Plug-in wird implementiert, das nur mit vSphere 7.0U1 und höheren Versionen kompatibel ist.

### Upgrade-Pfade

Wenn Sie SnapCenter Plugin für VMware vSphere (SCV) Version sind...	Sie können direkt ein Upgrade des SnapCenter Plugin für VMware vSphere durchführen auf...
SCV 4,9	Upgrade auf SCV 5.0
SCV 4,8	Upgrade auf SCV 4.9 und SCV 5.0
SCV 4,7	Upgrade auf SCV 4.8 und SCV 4.9
SCV 4,6	Upgrade auf SCV 4.7 und SCV 4.8



Sichern Sie das SnapCenter Plug-in für VMware vSphere OVA, bevor Sie ein Upgrade starten.

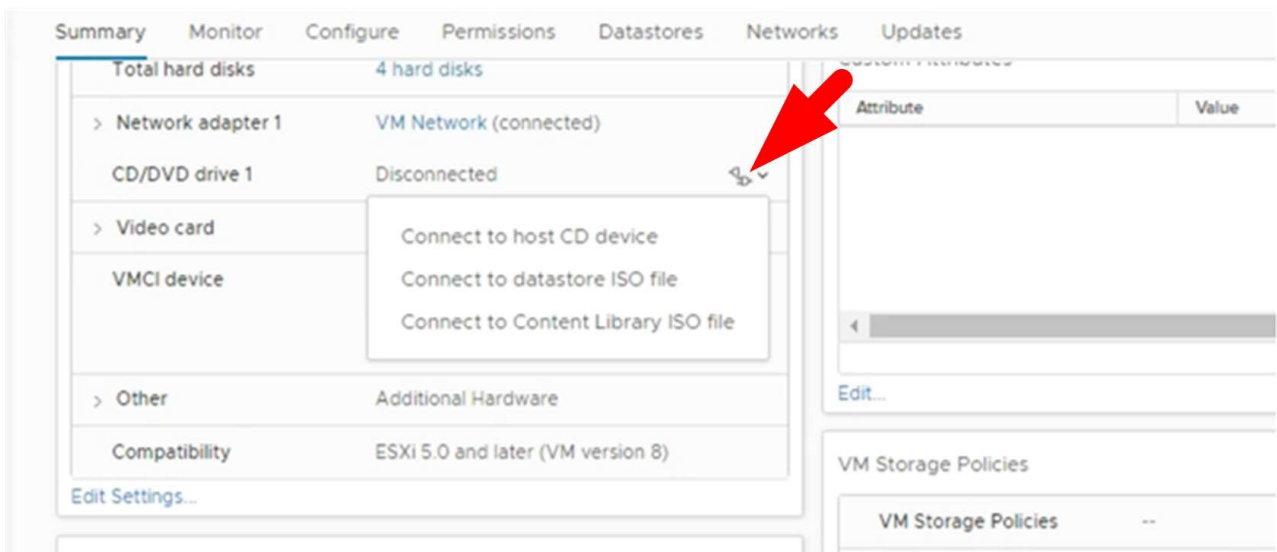


Das Umschalten der Netzwerkkonfiguration von statisch auf DHCP wird nicht unterstützt.

### Schritte

1. Bereiten Sie sich auf das Upgrade vor, indem Sie das SnapCenter Plug-in für VMware vSphere deaktivieren.
  - a. Melden Sie sich im SnapCenter Plug-in für die Management-GUI von VMware vSphere an. Die IP wird angezeigt, wenn Sie das SnapCenter VMware Plug-in bereitstellen.
  - b. Klicken Sie im linken Navigationsbereich auf **Konfiguration** und dann im Abschnitt Plug-in-Details auf die Option **Service**, um das Plug-in zu deaktivieren.
2. Laden Sie die Aktualisierungsdatei herunter `.iso`.
  - a. Melden Sie sich auf der NetApp Support-Website an (<https://mysupport.netapp.com/products/index.html>).
  - b. Wählen Sie aus der Liste der Produkte **SnapCenter Plug-in für VMware vSphere** und klicken Sie dann auf die Schaltfläche **NEUESTE VERSION HERUNTERLADEN**.
  - c. Laden Sie die Upgrade-Datei für das SnapCenter Plug-in für VMware vSphere an einen beliebigen Speicherort herunter `.iso`.
3. Installieren Sie das Upgrade.

- a. Navigieren Sie im Browser zu VMware vSphere vCenter.
- b. Klicken Sie auf der vCenter GUI auf **vSphere Client (HTML)**.
- c. Melden Sie sich auf der Seite **VMware vCenter Single Sign-On** an.
- d. Klicken Sie im Navigator-Fenster auf die VM, die Sie aktualisieren möchten, und klicken Sie dann auf die Registerkarte **Zusammenfassung**.
- e. Klicken Sie im Fensterbereich **Related Objects** auf einen beliebigen Datenspeicher in der Liste und dann auf die Registerkarte **Summary**.
- f. Klicken Sie auf der Registerkarte **Dateien** für den ausgewählten Datenspeicher auf einen beliebigen Ordner in der Liste und dann auf **Dateien hochladen**.
- g. Navigieren Sie im Popup-Fenster „Hochladen“ zu dem Speicherort, an dem Sie die Datei heruntergeladen `.iso` haben, klicken Sie dann auf das `.iso` Dateibild und klicken Sie dann auf **Öffnen**. Die Datei wird in den Datastore hochgeladen.
- h. Navigieren Sie zurück zu VM, die Sie aktualisieren möchten, und klicken Sie auf die Registerkarte **Zusammenfassung**. Im Fenster **VM Hardware** im Feld CD/DVD sollte der Wert „getrennt“ sein.
- i. Klicken Sie auf das Verbindungssymbol im Feld CD/DVD und wählen Sie **mit CD/DVD-Image verbinden auf einem Datastore** aus.



- j. Gehen Sie im Assistenten wie folgt vor:
  - i. Wählen Sie in der Spalte Datastores den Datastore aus, in den Sie die Datei hochgeladen `.iso` haben.
  - ii. Navigieren Sie in der Spalte Inhalt zu der `.iso` hochgeladenen Datei, stellen Sie sicher, dass im Feld Dateityp „ISO-Image“ ausgewählt ist, und klicken Sie dann auf **OK**. Warten Sie, bis der Status „verbunden“ angezeigt wird.
- k. Melden Sie sich an der Wartungskonsole an, indem Sie auf die Registerkarte **Zusammenfassung** des virtuellen Geräts zugreifen und dann auf den grünen Laufpfeil klicken, um die Wartungskonsole zu starten.
  - l. Geben Sie **2** für die Systemkonfiguration ein, und geben Sie dann **8** für die Aktualisierung ein.
- m. Geben Sie **y** ein, um mit dem Upgrade fortzufahren und zu starten.



# Upgraden Sie auf einen neuen Patch derselben Version des SnapCenter Plug-ins für VMware vSphere

Wenn Sie ein Upgrade auf einen neuen Patch derselben Version durchführen, müssen Sie das SnapCenter Plug-in für VMware vSphere Cache auf dem vCenter Webserver löschen und den Server vor dem Upgrade oder der Registrierung neu starten.

Wenn der Plug-in-Cache nicht gelöscht wird, werden die letzten Jobs in den folgenden Szenarien nicht im Dashboard und auf der Jobüberwachung angezeigt:

- Das SnapCenter Plug-in für VMware vSphere wurde mithilfe von vCenter bereitgestellt und später auf ein Patch in derselben Version aktualisiert.
- Die virtuelle SnapCenter VMware Appliance wurde in vCenter 1 implementiert. Später wurde dieses SnapCenter VMware Plug-in bei einem neuen vCenter2 registriert. Eine neue Instanz des SnapCenter VMware Plug-ins wird mit einem Patch erstellt und bei vCenter1 registriert. Da vCenter1 jedoch immer noch das gecachte Plug-in aus dem ersten SnapCenter VMware Plug-in ohne Patch besitzt, muss der Cache gelöscht werden.

## Schritte zum Löschen des Caches

1. Suchen Sie den `vsphere-client-serenity` Ordner, suchen Sie ihn, `com.netapp.scv.client-<release-number>` und löschen Sie ihn.

Der Ordnername ändert sich für jedes Release.

Informationen zum Speicherort des Ordners für Ihr Betriebssystem finden Sie in der VMware-Dokumentation `vsphere-client-serenity`.

2. Starten Sie vCenter Server neu.

Anschließend können Sie ein Upgrade des SnapCenter VMware Plug-ins durchführen.

## Informationen, die nach dem Upgrade auf einen neuen Patch derselben Version nicht angezeigt werden

Nach dem Upgrade des SnapCenter Plug-ins für VMware vSphere auf einen neuen Patch derselben Version werden aktuelle Jobs oder andere Informationen möglicherweise nicht im Dashboard und auf der Jobüberwachung angezeigt.

Wenn Sie ein Upgrade auf einen neuen Patch derselben Version durchführen, müssen Sie das SnapCenter Plug-in für VMware vSphere Cache auf dem vCenter Webserver löschen und den Server vor dem Upgrade oder der Registrierung neu starten.

Wenn der Plug-in-Cache nicht gelöscht wird, werden die letzten Jobs in den folgenden Szenarien nicht im Dashboard und auf der Jobüberwachung angezeigt:

- Das SnapCenter Plug-in für VMware vSphere wurde mithilfe von vCenter bereitgestellt und später auf ein Patch in derselben Version aktualisiert.
- Die virtuelle SnapCenter VMware Appliance wurde in vCenter 1 implementiert. Später wurde dieses SnapCenter VMware Plug-in bei einem neuen vCenter2 registriert. Eine neue Instanz des SnapCenter

VMware Plug-ins wird mit einem Patch erstellt und bei vCenter1 registriert. Da vCenter1 jedoch immer noch das gecachte Plug-in aus dem ersten SnapCenter VMware Plug-in ohne Patch besitzt, muss der Cache gelöscht werden.

Der Cache befindet sich an den folgenden Orten, abhängig vom Typ des Serverbetriebssystems:

- VCenter Server Linux Appliance

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

- Windows-OS

```
%PROGRAMFILES%/VMware/vSphere client/vc-packages/vsphere-client-serenity/
```

## Problemumgehung, wenn Sie bereits vor dem Löschen des Caches aktualisiert haben

1. Melden Sie sich bei der Management-GUI von SnapCenter VMware Plug-in an.

Die IP wird angezeigt, wenn Sie das SnapCenter VMware Plug-in bereitstellen.

2. Klicken Sie im linken Navigationsbereich auf **Konfiguration** und dann im Abschnitt **Plug-in Details** auf die Option Service, um das Plug-in zu deaktivieren.

Der SnapCenter VMware Plug-in-Service ist deaktiviert, und die Erweiterung ist in vCenter nicht registriert.

3. Suchen Sie den `vsphere-client-serenity` Ordner, suchen Sie ihn, `com.netapp.scv.client-<release-number>` und löschen Sie ihn.

Der Ordnername ändert sich für jedes Release.

4. Starten Sie vCenter Server neu.

5. Melden Sie sich beim VMware vSphere-Client an.

6. Klicken Sie im linken Navigationsbereich auf **Konfiguration** und dann im Abschnitt **Plug-in-Details** auf die Option Service, um das Plug-in zu aktivieren.

Der SnapCenter VMware Plug-in Service ist aktiviert und die Erweiterung ist in vCenter registriert.

# Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

## Urheberrecht

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

["Hinweis zum SnapCenter Plug-in für VMware vSphere 5.0"](#)

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

## Markeninformationen

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