



Los geht's

SnapCenter Plug-in for VMware vSphere 6.2

NetApp

December 09, 2025

Inhalt

| | |
|--|----|
| Los geht's | 1 |
| Implementierungsübersicht | 1 |
| Implementierungs-Workflow für vorhandene Benutzer | 1 |
| Anforderungen für die Bereitstellung von SCV | 2 |
| Implementierungsplanung und -Anforderungen | 2 |
| ONTAP-Berechtigungen erforderlich | 8 |
| Minimale vCenter-Berechtigungen erforderlich | 10 |
| Open Virtual Appliance (OVA) herunterladen | 10 |
| Implementieren Sie das SnapCenter Plug-in für VMware vSphere | 11 |
| Nach der Implementierung erforderliche Betriebsabläufe und Probleme | 15 |
| Erforderliche Vorgänge nach der Implementierung | 15 |
| Möglicherweise treten Bereitstellungsprobleme auf | 15 |
| Management von Authentifizierungsfehlern | 15 |
| Registrieren Sie das SnapCenter Plug-in für VMware vSphere mit SnapCenter Server | 16 |
| Melden Sie sich beim SnapCenter VMware vSphere-Client an | 17 |

Los geht's

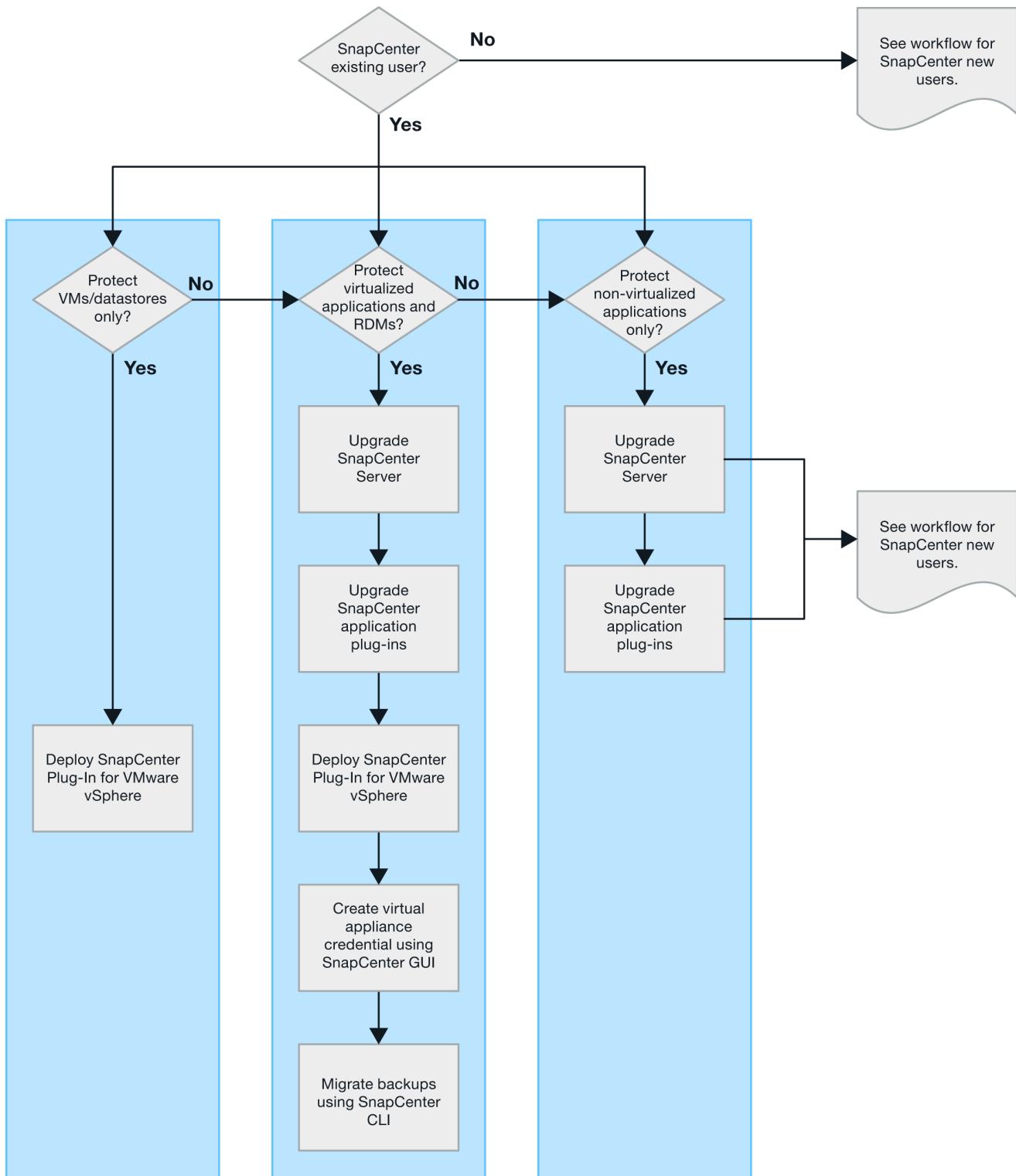
Implementierungsübersicht

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

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

Implementierungs-Workflow für vorhandene Benutzer

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



Anforderungen für die Bereitstellung von SCV

Implementierungsplanung und -Anforderungen

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

Host-Anforderungen erfüllt

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

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

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

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

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

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

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

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

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

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

- Was unterstützt wird:

- Erstellen von Ressourcengruppen

- Erstellen von Backups ohne konsistente VMs

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

Anschließen und Trennen von VMDKs

Montage und EntMounten von Datenspeichern

Wiederherstellung von Gastdateien

- Was nicht unterstützt wird:

Erstellen von Backups mit der Konsistenz von VMs

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

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

Lizenzanforderungen

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

Softwaresupport

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

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

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

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

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

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

Platz-, Dimensionierungs- und Skalierungsanforderungen

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

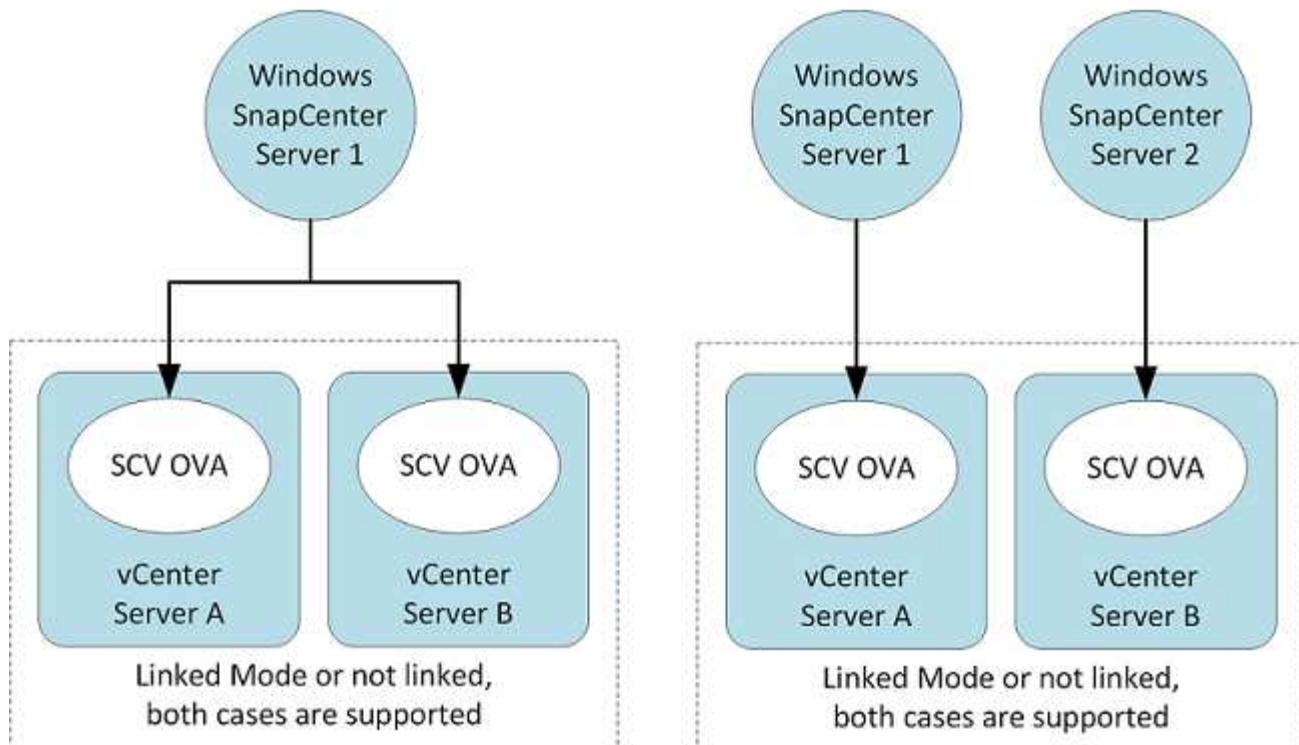
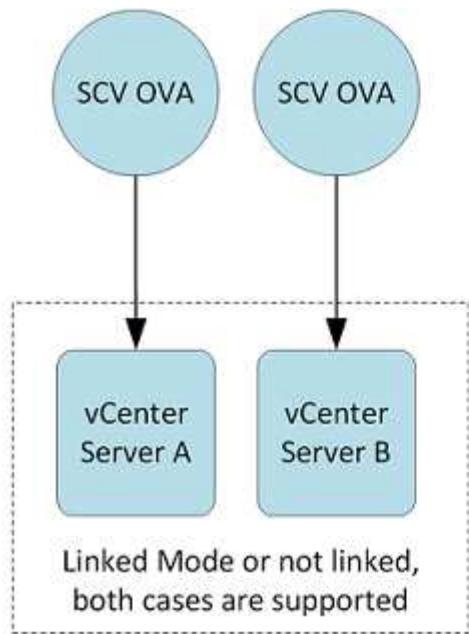
Verbindungs- und Portanforderungen

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

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

Unterstützte Konfigurationen

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



RBAC-Berechtigungen erforderlich

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

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

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

AutoSupport

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

ONTAP-Berechtigungen erforderlich

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



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

Mindestberechtigungen für ONTAP erforderlich

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

| |
|--|
| Alle Befehle: Minimale ONTAP Privileges. |
| Event Generate-AutoSupport-log |
| Job-Verlauf wird angezeigt Jobanzeigen Job beenden |
| lun lun create lun delete lun igrup hinzufügen lun igrup erstellen lun igrup löschen lun igrup umbenennen lun igrup 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 teilen starten Volume-Klon-Split-Status Volume-Clone-Split-Volume stoppen Volume erstellen Volume löschen Volume löschen Datei-Klon erstellen Volume-Datei zeigen-Disk-Nutzung Volume offline Volume online Volume-Volume verwalten Volume-Volume ändern Volume-qtree Volume erstellen qtree Volume löschen Volume-Volume ändern Volume-Snapshot Volume erstellen Volume löschen Snapshot Volume ändern Volume-SnapLock-Ablauf-Zeit Volume-Snapshot umbenennen Volume-Snapshot wiederherstellen-Datei-Volume-Snapshot wiederherstellen-Laufwerk zeigen Delta zeigen

vserver cifs vServer cifs Freigabe vserver erstellen cifs Freigabe vserver löschen vserver cifs shadowcopy vServer zeigen cifs share vserver zeigen vserver Export-Policy vServer Export-Policy vServer Export-Policy erstellen vServer Export-Policy löschen vServer NVMe-Subsystem vserver NVMe-Subsystem wserver vserver nvme-Subsystem abbilden vserver Export-Policy-Regel zeigen vserver Export-Policy zeigen vserver zeigen vserver iscsi vserver iscsi-Verbindung zeigen vserver zeigen vserver

Schreibgeschützte Befehle: Minimale ONTAP Privileges

Cluster Identity show Network Interface show vserver vserver Peer vserver show

Alle Befehle: Minimale ONTAP Privileges

Zeigt die Storage-Einheit der Konsistenzgruppe an

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



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

Weitere ONTAP-Informationen

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



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

Minimale vCenter-Berechtigungen erforderlich

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

Erforderliche Berechtigungen für vCenter Admin-Rolle

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

Erforderliche Berechtigungen für SnapCenter Plug-in für VMware vCenter

| Privilegien | Etikett |
|--|---|
| NetappSCV.Guest.RestoreDatei | Wiederherstellung Von Gastdateien |
| NetappSCV.Recovery.MountUnmount | Montieren/Entfernen |
| NetappSCV.Backup.DeleteBackupJob | Ressourcengruppe/Sicherung Löschen |
| NetappSCV.Configure.ConfigureStorageSystems.Delete | Storage-Systeme Entfernen |
| NetappSCV.View | Anzeigen |
| NetappSCV.Recovery.RecoverVM | Wiederherstellung von VM |
| NetappSCV.Configure.ConfigureStorageSystems.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 Vertrauenzertifikat unterzeichnet wurde, nicht mehr vertrauenswürdig. Zur Behebung des Problems müssen Sie das folgende Verfahren durchführen.

Schritte

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

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

- Wählen Sie aus der Liste der Produkte **SnapCenter Plug-in für VMware vSphere** aus und klicken Sie dann auf die Schaltfläche **Neueste Version** herunterladen.
 - Laden Sie das SnapCenter Plug-in für VMware vSphere herunter .tar Datei an jedem Speicherort.
2. Extrahieren Sie den Inhalt der tar-Datei. Die tar-Datei enthält den Ordner OVA und certs. Der Ordner „Zertifikaten“ enthält die Zertifikate „Stammanvertrauen“ und „Intermediate“.
3. Melden Sie sich mit dem vSphere Client am vCenter Server an.
4. Navigieren Sie zu **Administration > Zertifikate > Zertifikatverwaltung**.
5. Wählen Sie neben **Trusted Root Certificates Add**
- Wechseln Sie zum Ordner certs.
 - Wählen Sie Root- und Intermediate-Zertifikate anvertrauen aus.
 - Installieren Sie jedes Zertifikat einzeln.
6. Die Zertifikate werden zu einem Panel unter **Trusted Root Certificates** hinzugefügt. Sobald die Zertifikate installiert sind, kann OVA überprüft und bereitgestellt werden.



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

Implementieren Sie das SnapCenter Plug-in für VMware vSphere

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

Bevor Sie beginnen

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



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

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

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

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

Schritte

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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



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

- a. Wählen Sie unter **Setup Datum und Uhrzeit** die Zeitzone aus, in der sich das vCenter befindet.
14. Überprüfen Sie die Seite auf der Seite **Ready to Complete**, und wählen Sie **Finish**.

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

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

Wenn das SnapCenter-Plug-in für VMware vSphere erfolgreich bereitgestellt wurde, wird es als Linux-VM bereitgestellt, bei vCenter registriert und ein VMware vSphere-Client installiert.
15. Navigieren Sie zu der VM, auf der das SnapCenter-Plug-in für VMware vSphere bereitgestellt wurde, wählen Sie dann die Registerkarte **Zusammenfassung** aus, und wählen Sie dann das Feld **Einschalten** aus, um die virtuelle Appliance zu starten.
16. Während das SnapCenter-Plug-in für VMware vSphere eingeschaltet ist, klicken Sie mit der rechten Maustaste auf das bereitgestellte SnapCenter-Plug-in für VMware vSphere, wählen Sie **Gastbetriebssystem** aus und wählen Sie dann **VMware-Tools installieren** aus.

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

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

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

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

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

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

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

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

Nachdem Sie fertig sind

Sie müssen die erforderlichen Daten ausfüllen ["Vorgänge nach der Implementierung"](#).

Nach der Implementierung erforderliche Betriebsabläufe und Probleme

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

Erforderliche Vorgänge nach der Implementierung

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

Möglicherweise treten Bereitstellungsprobleme auf

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

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

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

Management von Authentifizierungsfehlern

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

Schritte

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

5. Wählen Sie **Senden**.

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

6. Wählen Sie im linken Navigationsbereich **Einstellungen**, dann die Registerkarte **Credential** und wählen Sie dann **Add**, um Anmeldeinformationen für die virtuelle Appliance hinzuzufügen.

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



Sie müssen Linux für das Feld Authentifizierung auswählen.

Nachdem Sie fertig sind

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

Melden Sie sich beim SnapCenter VMware vSphere-Client an

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

Bevor Sie beginnen

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

Schritte

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



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

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

Copyright-Informationen

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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