



# **Implementierung und Upgrade**

VSC, VASA Provider, and SRA 9.7

NetApp  
April 01, 2025

# Inhalt

Implementierung und Upgrade .....	1
Übersicht über die virtuelle Appliance für VSC, VASA Provider und SRA .....	1
Virtual Storage Console (VSC) .....	1
VASA Provider .....	2
Storage Replication Adapter (SRA) .....	2
Implementierungs-Workflow für neue Benutzer der virtuellen VSC, VASA Provider und SRA .....	2
Implementierungs-Workflow für bestehende Benutzer von VSC, VASA Provider und SRA .....	3
Anforderungen für die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA .....	4
Port-Anforderungen für VSC .....	4
Unterstützte Storage-Systeme, Lizenzen und Applikationen für die virtuelle Appliance für VSC, VASA Provider und SRA .....	5
Überlegungen und Anforderungen für die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA .....	6
Implementierung oder Upgrade von VSC, VASA Provider und SRA .....	9
So laden Sie die virtuelle Appliance für VSC, VASA Provider und SRA herunter .....	9
Implementieren Sie die virtuelle Appliance für VSC, VASA Provider und SRA .....	9

# Implementierung und Upgrade

## Übersicht über die virtuelle Appliance für VSC, VASA Provider und SRA

Die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) bietet lückenloses Lifecycle-Management für Virtual Machines in VMware Umgebungen, die NetApp Storage-Systeme verwenden. Es vereinfacht das Storage- und Datenmanagement für VMware Umgebungen, da Administratoren Storage direkt innerhalb des vCenter Server managen können.

Mit vSphere 6.5 hat VMware einen neuen HTML5-basierten Client namens vSphere Client eingeführt. Die Version 9.6 der virtuellen Appliance für VSC, VASA Provider und SRA unterstützt nur vSphere Client. Die virtuelle Appliance für VSC, VASA Provider und SRA lässt sich in vSphere Client integrieren, sodass Sie SSO-Services (Single Sign On) verwenden können. In einer Umgebung mit mehreren vCenter Serverinstanzen muss jede vCenter Server-Instanz, die Sie managen möchten, eine eigene, registrierte VSC-Instanz aufweisen.

Jede Komponente in der virtuellen Appliance für VSC, VASA Provider und SRA bietet Funktionen zum effizienteren Management des Storage.

### Virtual Storage Console (VSC)

Mit VSC führen Sie die folgenden Aufgaben aus:

- Fügen Sie Storage-Controller hinzu, weisen Sie Anmeldedaten zu, und richten Sie Berechtigungen für Storage-Controller an VSC ein, von der sowohl SRA als auch VASA Provider profitieren können
- Bereitstellung von Datenspeichern
- Überwachen Sie die Performance von Datastores und Virtual Machines in Ihrer vCenter Server Umgebung
- Steuern Sie den Administratorzugriff auf vCenter Server-Objekte, indem Sie die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) auf zwei Ebenen nutzen:
  - vSphere Objekte wie Virtual Machines und Datastores

Diese Objekte werden über die vCenter Server RBAC gemanagt.

- ONTAP Storage

Die Storage-Systeme werden über die rollenbasierte Zugriffssteuerung von ONTAP gemanagt.

- Die Hostereinstellungen der ESXi-Hosts anzeigen und aktualisieren, die mit dem Speicher verbunden sind

VSC Bereitstellungsvorgänge profitieren vom Einsatz des NFS-Plug-in für VMware vStorage APIs für Array Integration (VAAI). Das NFS-Plug-in für VAAI ist eine Softwarebibliothek, in der die VMware Virtual Disk Libraries integriert sind, die auf dem ESXi-Host installiert sind. Das Paket VMware VAAI ermöglicht die Auslagerung bestimmter Aufgaben von den physischen Hosts an das Storage Array. Aufgaben wie Thin Provisioning und Hardwarebeschleunigung können auf Array-Ebene ausgeführt werden, um die Workloads auf den ESXi Hosts zu verringern. Die Funktion zum Offload und zur Speicherplatzreservierung verbessern die Performance des VSC-Betriebs.

Das NetApp NFS Plug-in für VAAI wird nicht mit VSC ausgeliefert. Aber Sie können das Plug-in

Installationspaket herunterladen und die Anweisungen für die Installation des Plug-ins von der erhalten.

## VASA Provider

VASA Provider für ONTAP sendet Informationen über den von VMware vSphere APIs for Storage Awareness (VASA) verwendeten Storage an den vCenter Server. Die virtuelle Appliance für VSC, VASA Provider und SRA, VASA Provider ist in VSC integriert und VASA Provider ermöglicht Ihnen die Ausführung folgender Aufgaben:

- Bereitstellen von Datastores mit VMware Virtual Volumes (VVols)
- Erstellen und nutzen Sie Storage-Funktionsprofile, um unterschiedliche Storage Service Level Objectives (SLOs) für die Umgebung zu definieren
- Überprüfen Sie die Compliance zwischen den Datastores und den Storage-Funktionsprofilen
- Legen Sie Alarme fest, um zu warnen, wenn Volumes und Aggregate sich den Schwellenwerten nähern
- Überwachen Sie die Performance von Virtual Machine Disks (VMDKs) und den Virtual Machines, die auf VVols Datastores erstellt werden

Bei Verwendung von ONTAP 9.6 oder einer älteren Version kommuniziert VASA Provider über VASA APIs mit dem vCenter Server und kommuniziert über APIs, die zapis genannt werden, mit ONTAP. Um das vVol Dashboard für ONTAP 9.6 und früher anzuzeigen, müssen Sie mit Ihrem vCenter Server installiert und registriert haben. Wenn Sie ONTAP 9.7 verwenden, müssen Sie nicht bei VASA Provider registriert werden, um das vVol Dashboard anzuzeigen.



Für ONTAP 9.6 oder früher benötigt VASA Provider eine dedizierte Instanz von OnCommand API Services. Eine Instanz der OnCommand API Services kann nicht mit mehreren VASA-Provider-Instanzen gemeinsam genutzt werden.

## Storage Replication Adapter (SRA)

Wenn SRA aktiviert und in Verbindung mit VMware Site Recovery Manager (SRM) verwendet wird, können bei einem Ausfall die vCenter Server-Datenspeicher und die Virtual Machines wiederhergestellt werden. Mit SRA lassen sich geschützte Standorte und Recovery-Standorte in der Umgebung nach einem Ausfall für die Disaster Recovery konfigurieren.

### Verwandte Informationen

["NetApp Dokumentation: OnCommand API Services"](#)

["NetApp Dokumentation: NetApp NFS Plug-in für VMware VAAI"](#)

["NetApp Support"](#)

## Implementierungs-Workflow für neue Benutzer der virtuellen VSC, VASA Provider und SRA

Wenn Sie neu bei VMware sind und noch kein NetApp VSC Produkt verwendet haben, müssen Sie Ihren vCenter Server konfigurieren und einen ESXi Host einrichten, bevor Sie die virtuelle Appliance für VSC, VASA Provider und SRA implementieren und konfigurieren.

## Implementierungs-Workflow für bestehende Benutzer von VSC, VASA Provider und SRA

Die 9.7 Versionen der virtuellen Appliance für VSC, VASA Provider und SRA unterstützen ein direktes Upgrade auf die neueste Version.

In den früheren Versionen einzelner Applikationen wie VSC, VASA Provider und SRA wird ein anderer Upgrade-Prozess verwendet. Wenn VSC oder VASA Provider oder SRA in Ihrem Setup installiert sind, sollten Sie die folgenden Vorgänge durchführen:

1. Implementieren Sie die aktuelle Version der virtuellen Appliance für VSC, VASA Provider und SRA.
2. Migrieren Sie alle vorhandenen Konfigurationsdaten.

Die Konfigurationsdaten umfassen Anmeldeinformationen des Storage-Systems sowie die Einstellungen in `kaminoprefs.xml` Und `vscPreferences.xml` Dateien:

### "Konfigurieren Sie die VSC Preferences-Dateien"

In vielen Fällen sind Konfigurationsdaten möglicherweise nicht notwendig. Wenn Sie die Voreinstellungen jedoch bereits zuvor angepasst haben, sollten Sie sie überprüfen und ähnliche Änderungen an der neu implementierten virtuellen Appliance vornehmen. Sie können eine der folgenden Aktionen ausführen:

- Nutzung "[Import Utility für SnapCenter und Virtual Storage Console](#)" Migrieren der Anmeldeinformationen des Storage-Systems von VSC 6.X und SRA 4.X zur neuen Implementierung.
- Fügen Sie die Speichersysteme der neu implementierten virtuellen Appliance hinzu und geben Sie die Anmeldeinformationen beim Hinzufügen an.

Wenn Sie ein Upgrade von VASA Provider 6.X durchführen, sollten Sie vor dem Upgrade VASA Provider aus registrieren. Weitere Informationen finden Sie in der Dokumentation zu Ihrer aktuellen Version.

Wenn Sie auch ein Upgrade von SRA 4.0 oder früher durchführen:

- Wenn Sie SRA 4.0P1 verwenden, müssen Sie zuerst auf SRA 9.6 aktualisieren und erst dann können Sie ein Upgrade des SRA 9.6 auf die neueste Version durchführen.

### "Upgrade auf die virtuelle 9.7.1 Appliance für VSC, VASA Provider und SRA"

- Bei Verwendung von SRA 2.1 oder 3.0 sollten Sie zunächst die vorhandenen Standortkonfigurationsdetails beachten.

*Installations- und Setup-Leitfaden für Storage Replication Adapter 4.0 für ONTAP* enthält die detaillierten Anweisungen im Abschnitt „Upgrade-Übersicht“. Diese SRA Versionen nutzen auch den VASA Provider. Das Registrieren von VASA Provider muss also aufgehoben und anschließend die aktuelle Version der virtuellen Appliance für VSC, VASA Provider und SRA implementiert werden. Die vorherige Version des Servers (`.ova`) Kann entfernt werden, wenn die Aktualisierung abgeschlossen ist.

Bei jedem SRA-Upgrade die SRA-Software (der Adapter auf dem Site Recovery Manager-Server, installiert vom `.msi` Datei) sollte vom Site Recovery Manager-Server entfernt werden. Sie können die Windows-Systemsteuerung verwenden, um die Software zu deinstallieren und dann die neueste SRA-Software auf dem SRA-Server mithilfe der zu installieren `.msi` Datei:

Bei der Implementierung von VASA Provider müssen Sie nach dem Upgrade aus der bestehenden Einrichtung die Speichergröße für Ihre virtuelle Appliance mithilfe der 12 GB konfigurieren `Edit Settings` Option. Sie

müssen auch die virtuelle Speicherreservierung ändern. Die virtuelle Maschine muss ausgeschaltet sein, um die Speichergröße zu ändern.

Ein direktes Upgrade von einer Version vor 9.7 auf 9.7P2 oder höher wird von der virtuellen Appliance für VSC, VASA Provider und SRA nicht unterstützt. Sie sollten zunächst Ihre vorhandene Einrichtung auf Version 9.7 der virtuellen Appliance für VSC, VASA Provider und SRA aktualisieren, bevor Sie ein Upgrade auf eine spätere Version durchführen.

Wenn Sie die neueste Version der virtuellen Appliance implementieren möchten, müssen Sie das Thema „Anforderungen für die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA lesen.“ Das Thema „Upgrade auf Version 9.6 der virtuellen Appliance für VSC, VASA Provider und SRA“ enthält Informationen zur Durchführung eines vorhandenen Upgrades.

## **Verwandte Informationen**

["NetApp ToolChest: NetApp Import Utility für SnapCenter und Virtual Storage Console"](#)

["Anforderungen für die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA"](#)

["Upgrade auf die virtuelle 9.7.1 Appliance für VSC, VASA Provider und SRA"](#)

# **Anforderungen für die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA**

Sie sollten die Implementierungsanforderungen kennen, bevor Sie die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) implementieren. Außerdem sollten Sie die gewünschten Aufgaben festlegen. Sie können je nach Aufgabe das Implementierungsmodell zur Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA auswählen.

## **Port-Anforderungen für VSC**

Standardmäßig verwendet (VSC) bestimmte Ports, um die Kommunikation zwischen seinen Komponenten zu ermöglichen. Dazu gehören Storage-Systeme und VMware vCenter Server. Wenn Firewalls aktiviert sind, müssen Sie sicherstellen, dass die Firewalls so eingestellt sind, dass Ausnahmen zugelassen werden.

Bei Firewalls anderer als Windows sollten Sie manuell Zugriff auf bestimmte Ports gewähren, die von VSC verwendet werden. Wenn Sie diesen Ports keinen Zugriff gewähren, wird eine Fehlermeldung wie die folgende angezeigt.

*Kommunikation mit dem Server nicht möglich*

VSC verwendet die folgenden bidirektionalen TCP-Standardports:

Standard-Portnummer	Beschreibung
9083	Bei Aktivierung verwenden sowohl VASA Provider als auch Storage Replication Adapter (SRA) diesen Port zur Kommunikation mit dem vCenter Server. Dieser Port wird auch zum Abrufen der TCP/IP-Einstellungen benötigt.
443	Je nach Konfiguration Ihrer Anmeldedaten achten VMware vCenter Server und die Speichersysteme auf die sichere Kommunikation auf diesem Port.
8143	VSC wartet auf eine sichere Kommunikation von diesem Port.
7	VSC sendet eine Echo-Anfrage an ONTAP zur Überprüfung der Erreichbarkeit. Diese ist nur beim Hinzufügen eines Storage-Systems erforderlich und kann später deaktiviert werden.

Sie sollten das Internet Control Message Protocol (ICMP) aktivieren, bevor Sie die virtuelle Appliance für VSC, VASA Provider und SRA implementieren.



Wenn ICMP deaktiviert ist, schlägt die Erstkonfiguration der virtuellen Appliance für VSC, VASA Provider und SRA fehl und VSC kann die VSC- und VASA-Provider-Services nach der Implementierung nicht starten. Nach der Implementierung müssen Sie die VSC- und VASA-Provider-Services manuell aktivieren.

## Unterstützte Storage-Systeme, Lizenzen und Applikationen für die virtuelle Appliance für VSC, VASA Provider und SRA

Bevor Sie mit der Implementierung der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) beginnen, sollten Sie die grundlegenden Anforderungen des Storage-Systems, der Applikations- und Lizenzierungsanforderungen kennen.

Der (IMT) enthält aktuelle Informationen zu den unterstützten Versionen von ONTAP, vCenter Server, ESXi Hosts, Plug-in-Applikationen und Site Recovery Manager (SRM).

- ["Interoperabilitäts-Matrix-Tool VSC 9.7.1"](#)
- ["Interoperabilitäts-Matrix-Tool VASA Provider 9.7.1"](#)
- ["Interoperabilitäts-Matrix-Tool SRA 9.7.1"](#)

Sie müssen die FlexClone Lizenz aktivieren, um Snapshot-Vorgänge für Virtual Machines und Klonvorgänge für VMware Virtual Volumes (VVols) Datastores durchzuführen.

Storage Replication Adapter (SRA) erfordert die folgenden Lizenzen:

- SnapMirror Lizenz

Sie müssen die SnapMirror Lizenz aktivieren, um Failover-Vorgänge für SRA auszuführen.

- FlexClone Lizenz

Sie müssen die FlexClone Lizenz aktivieren, um Test-Failover-Vorgänge für SRA durchzuführen.

Um die IOPS für einen Datastore anzuzeigen, müssen Sie entweder die Storage-I/O-Steuerung aktivieren oder das Kontrollkästchen „Storage-I/O-Statistiksammlung deaktivieren“ in der Konfiguration des Storage-I/O-Steuersystems deaktivieren. Sie können die Storage-I/O-Steuerung nur aktivieren, wenn Sie über die Enterprise Plus-Lizenz von VMware verfügen.

- ["VMware KB Artikel 1022091: Fehlerbehebung bei Storage I/O Control"](#)
- ["Dokumentation der VMware vSphere Storage I/O Control Anforderungen"](#)

## Überlegungen und Anforderungen für die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA

Bevor Sie die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) implementieren, sollten Sie die Implementierung planen und entscheiden, wie VSC, VASA Provider und SRA in Ihrer Umgebung konfiguriert werden sollen.

In der folgenden Tabelle finden Sie eine Übersicht über die Überlegungen, die vor der Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA berücksichtigt werden sollten.

Überlegungen	Beschreibung
Erstmalige Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA	Wenn die virtuelle Appliance für VSC, VASA Provider und SRA implementiert wird, werden die VSC Funktionen automatisch installiert. <a href="#">"Implementierung oder Upgrade von VSC, VASA Provider und SRA"</a>  <a href="#">"Implementierungs-Workflow für neue Benutzer der virtuellen VSC, VASA Provider und SRA"</a>



Überlegungen	Beschreibung
Upgrade von einer bestehenden VSC Implementierung	<p>Das Upgrade-Verfahren von einer vorhandenen VSC Implementierung zur virtuellen Appliance für VSC, VASA Provider und SRA hängt von der Version von VSC ab und ob VSC, VASA Provider und SRA implementiert wurden. Der Abschnitt zu Bereitstellungs-Workflows und Upgrade enthält weitere Informationen. <a href="#">"Implementierungs-Workflow für bestehende Benutzer von VSC, VASA Provider und SRA"</a></p> <p>Best Practices vor einem Upgrade:</p> <ul style="list-style-type: none"> <li>• Sie sollten Informationen über die verwendeten Speichersysteme und deren Anmeldeinformationen erfassen.</li> </ul> <p>Nach dem Upgrade sollten Sie überprüfen, ob alle Speichersysteme automatisch erkannt wurden und die korrekten Anmeldedaten besitzen.</p> <ul style="list-style-type: none"> <li>• Wenn Sie eine der Standard-VSC Rollen geändert haben, sollten Sie diese Rollen kopieren, um Ihre Änderungen zu speichern.</li> </ul> <p>VSC überschreibt bei jedem Neustart des VSC Service die Standardrollen mit den aktuellen Standardeinstellungen.</p>
Erneutes Generieren eines SSL-Zertifikats für VSC	<p>Das SSL-Zertifikat wird automatisch generiert, wenn Sie die virtuelle Appliance für VSC, VASA Provider und SRA implementieren. Möglicherweise müssen Sie das SSL-Zertifikat erneut generieren, um ein standortspezifisches Zertifikat zu erstellen. <a href="#">"Erstellen Sie ein SSL-Zertifikat für neu"</a></p>
Festlegen der ESXi-Serverwerte	<p>Obwohl die meisten ESXi-Serverwerte standardmäßig festgelegt sind, empfiehlt es sich, die Werte zu überprüfen. Diese Werte basieren auf internen Tests. Je nach Umgebung müssen Sie möglicherweise einige der Werte ändern, um die Leistung zu verbessern.</p> <ul style="list-style-type: none"> <li>• <a href="#">"Konfigurieren Sie Multipathing- und Zeitüberschreitungseinstellungen für ESXi-Server"</a></li> <li>• <a href="#">"ESXi-Hostwerte werden mit Virtual Storage Console für VMware vSphere festgelegt"</a></li> </ul>

Überlegungen	Beschreibung
Werte für die Zeitüberschreitung des Gastbetriebssystems	Die Timeout-Skripte für Gastbetriebssysteme (Gast-OS) legen die SCSI I/O-Zeitüberschreitungswerte für die unterstützten Linux, Solaris und Windows Gastbetriebssysteme fest, um das richtige Failover-Verhalten sicherzustellen.

Die folgende Tabelle zeigt eine Übersicht über die erforderlichen Komponenten zur Konfiguration der virtuellen Appliance für VSC, VASA Provider und SRA.

Überlegungen	Beschreibung
Anforderungen der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)	<p>VSC unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC. Das Konto, über das VSC bei vCenter Server registriert wird (mit <code>https://&lt;appliance_ip&gt;:8143/Register.html</code>) Muss ein vCenter Server Administrator sein (dem vCenter Server Administrator oder der Administratorrolle zugewiesen). Wenn Sie planen, VSC als Administrator auszuführen, müssen Sie über alle erforderlichen Berechtigungen und Berechtigungen für alle Aufgaben verfügen.</p> <p>Wenn in Ihrem Unternehmen der Zugriff auf vSphere Objekte eingeschränkt werden muss, können Sie Benutzer Standard-VSC-Rollen erstellen und zuweisen, um die Anforderungen von vCenter Server zu erfüllen.</p> <p>Mithilfe von ONTAP System Manager können Sie die empfohlenen ONTAP-Rollen erstellen. Dabei wird die JSON-Datei verwendet, die in der virtuellen Appliance für VSC, VASA Provider und SRA enthalten ist.</p> <p>Wenn ein Benutzer versucht, eine Aufgabe ohne die entsprechenden Berechtigungen und Berechtigungen auszuführen, werden die Aufgabenoptionen ausgegraut.</p> <ul style="list-style-type: none"> <li>• <a href="#">"Standardrollen in Verbindung mit der virtuellen Appliance für VSC, VASA Provider und SRA"</a></li> <li>• <a href="#">"Empfohlene ONTAP Rollen bei der Verwendung von VSC für VMware vSphere"</a></li> </ul>
ONTAP-Version	Ihre Storage-Systeme müssen mit ONTAP 9.1, 9.3, 9.5, 9.6 oder 9.7 ausgeführt werden.

Überlegungen	Beschreibung
Storage-Funktionsprofile	<p>Um Storage-Funktionsprofile zu verwenden oder Alarme einzurichten, müssen Sie VASA Provider für ONTAP aktivieren. Nach der Aktivierung von VASA Provider können Sie VMware Virtual Volumes (VVols) Datastores konfigurieren und Storage-Funktionsprofile und Alarme erstellen und managen.</p> <p>Die Alarme warnen Sie, wenn ein Volume oder ein Aggregat fast voll ausgelastet ist oder wenn ein Datenspeicher nicht mehr dem zugehörigen Storage-Funktionsprofil entspricht.</p>

## Implementierung oder Upgrade von VSC, VASA Provider und SRA

Sie müssen die virtuelle Appliance für VSC, VASA Provider und SRA in Ihrer VMware vSphere Umgebung herunterladen und implementieren und dann die erforderlichen Applikationen auf Basis der Aufgaben konfigurieren, die Sie mit VSC, VASA Provider, SRAVSC, VASA Provider und SRA durchführen möchten.

### Verwandte Informationen

[Aktivieren Sie VASA Provider zur Konfiguration von virtuellen Datastores](#)

### So laden Sie die virtuelle Appliance für VSC, VASA Provider und SRA herunter

Sie können die heruntergeladene .ova Datei für die virtuelle Appliance für Virtual Storage Console, VASA Provider und Storage Replication Adapter von der .

Der .ova Dazu gehören VSC, VASA Provider und SRA. Nach Abschluss der Implementierung sind alle drei Produkte in Ihrer Umgebung installiert. Standardmäßig funktioniert VSC bereits, wenn Sie ein Folgemodell nutzen möchten und wählen, ob Sie VASA Provider und SRA basierend auf den Anforderungen aktivieren möchten.

Sie können die virtuelle Appliance für VSC, VASA Provider und SRA über heruntergeladenen ["NetApp Support Website"](#) Mit der Software Download-Seite.

Wenn Sie SRA bei der Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA aktivieren möchten, müssen Sie das SRA-Plug-in auf dem Site Recovery Manager (SRM) Server installiert haben. Sie können die Installationsdatei für das SRA-Plug-in im Menü **Storage Replication Adapter für ONTAP** im Abschnitt **Software-Downloads** herunterladen.

### Implementieren Sie die virtuelle Appliance für VSC, VASA Provider und SRA

Sie sollten die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) in Ihrer Umgebung implementieren und die erforderlichen Parameter angeben, um die Appliance verwenden zu können.

## Bevor Sie beginnen

- Sie müssen eine unterstützte Version von vCenter Server ausführen.



Die virtuelle Appliance für VSC, VASA Provider und SRA kann bei einer Windows Implementierung von vCenter Server oder einer Implementierung der VMware vCenter Server Virtual Appliance (vCSA) registriert werden.

### "Interoperabilitäts-Matrix-Tool VSC 9.7"

- Sie müssen Ihre vCenter Server-Umgebung konfiguriert und eingerichtet haben.
- Sie müssen einen ESXi-Host für Ihre virtuelle Maschine einrichten.
- Sie müssen das heruntergeladen haben .ova Datei:
- Sie müssen über die Anmeldedaten des Administrators für Ihre vCenter Server-Instanz verfügen.
- Sie müssen alle Browser-Sessions des vSphere Clients abgemeldet, geschlossen und den Browser-Cache gelöscht haben, um Probleme mit dem Browser-Cache während der Bereitstellung der virtuellen Appliance für VSC, VASA Provider und SRA zu vermeiden.

### Reinigen Sie die heruntergeladenen Plug-in-Pakete von vSphere im Cache

- Sie müssen das Internet Control Message Protocol (ICMP) aktiviert haben.

Wenn ICMP deaktiviert ist, schlägt die Erstkonfiguration der virtuellen Appliance für VSC, VASA Provider und SRA fehl und VSC kann die VSC- und VASA-Provider-Services nach der Implementierung nicht starten. Nach der Implementierung müssen Sie die VSC- und VASA-Provider-Services manuell aktivieren.

## Über diese Aufgabe

Wenn Sie eine neue Installation der virtuellen Appliance für VSC, VASA Provider und SRA implementieren, ist VASA Provider standardmäßig aktiviert. Bei einem Upgrade von einer früheren Version der virtuellen Appliance bleibt der Status von VASA Provider erhalten, und VASA Provider muss möglicherweise manuell aktiviert werden.

### "Aktivieren Sie VASA Provider zur Konfiguration von virtuellen Datastores"

## Schritte

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie Menü:Startseite[Host & Clusters].
3. Klicken Sie mit der rechten Maustaste auf das gewünschte Rechenzentrum und klicken Sie dann auf **OVA-Vorlage bereitstellen**.
4. Wählen Sie die anzuwendende Methode zur Bereitstellung der Bereitstellungsdatei für VSC, VASA Provider und SRA aus, und klicken Sie dann auf **Weiter**.

Standort	Aktion
URL	Geben Sie die URL für das an .ova Datei für die virtuelle Appliance für VSC, VASA Provider und SRA.

Standort	Aktion
Ordner	Wählen Sie die aus .ova Datei für die virtuelle Appliance für VSC, VASA Provider und SRA vom gespeicherten Speicherort aus

5. Geben Sie die Details ein, um den Bereitstellungsassistenten anzupassen.

Siehe "[Überlegungen zur Anpassung der Implementierung](#)" Vollständige Angaben.

6. Überprüfen Sie die Konfigurationsdaten, und klicken Sie dann auf **Weiter**, um die Bereitstellung abzuschließen.

Wenn Sie warten, bis die Bereitstellung abgeschlossen ist, können Sie den Fortschritt der Bereitstellung über die Registerkarte **Aufgaben** anzeigen.

7. Schalten Sie die virtuelle Appliance ein, und öffnen Sie dann eine Konsole der virtuellen Maschine, auf der die virtuelle Appliance ausgeführt wird.

8. Überprüfen Sie, ob VSC, VASA Provider und SRA-Services nach Abschluss der Implementierung ausgeführt werden.

9. Wenn die virtuelle Appliance für VSC, VASA Provider und SRA nicht mit einem vCenter Server registriert ist, nutzen Sie [https://appliance\\_ip:8143/Register.html](https://appliance_ip:8143/Register.html) Um die VSC Instanz zu registrieren.

10. Melden Sie sich ab- und erneut beim vSphere Client an, um die implementierte virtuelle Appliance für VSC, VASA Provider und SRA anzuzeigen.

Es kann ein paar Minuten dauern, bis das Plug-in im vSphere Client aktualisiert wird.



Wenn Sie das Plug-in nicht selbst nach der Anmeldung anzeigen können, müssen Sie den vSphere Client-Cache reinigen. [Reinigen Sie die heruntergeladenen Plug-in-Pakete von vSphere im Cache](#)

## Nachdem Sie fertig sind

[NOTE]

====

Wenn Sie ONTAP 9.6 oder früher verwenden, dann um das vVol Dashboard anzuzeigen, müssen Sie herunterladen und installieren . Für ONTAP 9.7 müssen Sie jedoch nicht beim VASA Provider registriert werden.

====

xref:{relative\_path}task-register-oncommand-api-services-with-the-virtual-appliance-for-vsc-vasa-provider-and-sra.adoc[Melden Sie sich mit der virtuellen Appliance für VSC, VASA Provider und SRA an]

:leveloffset: +1

```
[[ID7a837518afe88fe39b427edbaf111353]]
```

= Überlegungen zur Anpassung der Implementierung

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Bei der Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA müssen Sie einige Einschränkungen berücksichtigen.

== Benutzerpasswort für den Appliance-Administrator

Sie dürfen keine Leerzeichen im Administratorpasswort verwenden.

== Anmeldedaten für die Appliance-Wartungskonsole

Sie müssen über den Benutzernamen „`maint`“ auf die Wartungskonsole zugreifen. Sie können das Passwort für den Benutzer „`maint`“ während der Bereitstellung festlegen. Sie können das Passwort über das Menü \*Anwendungskonfiguration\* der Wartungskonsole Ihrer virtuellen Appliance für VSC, VASA Provider und SRA ändern.

== Anmeldedaten für vCenter Server-Administrator

Sie können die Administratoranmeldedaten für vCenter Server festlegen, während Sie die virtuelle Appliance für VSC, VASA Provider und SRA implementieren.

Wenn sich das Kennwort für den vCenter Server ändert, können Sie das Kennwort für den Administrator mithilfe der folgenden URL aktualisieren: `\_https\_://<IP>:8143/Register.html` Dabei handelt es sich die IP-Adresse der virtuellen Appliance für VSC, VASA Provider und SRA, die Sie während der Implementierung bereitstellen.

== IP-Adresse des vCenter Server

\* Sie sollten die IP-Adresse (IPv4 oder IPv6) der vCenter Server Instanz

angeben, in der die virtuelle Appliance für VSC, VASA Provider und SRA registriert werden soll.

+

Der generierte Typ von VSC- und VASA-Zertifikaten hängt von der IP-Adresse (IPv4 oder IPv6) ab, die Sie während der Bereitstellung bereitgestellt haben. Wenn Sie während der Bereitstellung der virtuellen Appliance für VSC, VASA Provider und SRA keine statischen IP-Details und kein DHCP eingegeben haben, bietet das Netzwerk sowohl IPv4- als auch IPv6-Adressen.

\* Die virtuelle Appliance für VSC, VASA Provider und SRA IP-Adresse, die zur Registrierung mit vCenter Server verwendet wird, hängt von der Art der vCenter Server IP-Adresse (IPv4 oder IPv6) ab, die im Implementierungsassistenten eingegeben wurde.

+

Sowohl VSC- als auch VASA-Zertifikate werden mit derselben IP-Adresse generiert, die bei der vCenter Server Registrierung verwendet wird.

[NOTE]

====

IPv6 wird nur ab vCenter Server 6.7 unterstützt.

====

== Netzwerkeigenschaften von Appliances

Wenn Sie DHCP nicht verwenden, geben Sie einen gültigen DNS-Hostnamen (nicht qualifiziert) sowie die statische IP-Adresse für die virtuelle Appliance für VSC, VASA Provider und SRA und die anderen Netzwerkparameter an. Alle diese Parameter sind für eine ordnungsgemäße Installation und Betrieb erforderlich.

:leveloffset: -1

[[IDf30e931667a33cfdaa99075002b0b3d9]]

= Aktivieren Sie VASA Provider zur Konfiguration von virtuellen Datastores

:allow-uri-read:

:experimental:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Bei der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und dem Storage Replication Adapter (SRA) sind die VASA Provider-Funktion standardmäßig aktiviert. Sie können Datastores von VMware Virtual Volumes (VVols) mit den erforderlichen Storage-Funktionsprofilen für jeden VVols Datastore konfigurieren.

.Bevor Sie beginnen

- \* Sie müssen Ihre vCenter Server-Instanz eingerichtet und ESXi konfiguriert haben.
- \* Sie müssen die virtuelle Appliance für VSC, VASA Provider und SRA implementiert haben.

.Über diese Aufgabe

Wenn die VASA Provider-Funktion deaktiviert wird, bevor ein Upgrade auf Version 9.7.1 der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) durchgeführt wird, bleibt die VASA Provider-Funktion nach dem Upgrade deaktiviert. In dieser Version können Sie die VVols Replizierungsfunktion für VVols Datastores aktivieren.

.Schritte

- . Melden Sie sich bei der Web-Benutzeroberfläche von VMware vSphere an.
- . Klicken Sie im vSphere Client auf MENU:Menü[Virtuelle Speicherkonsole].
- . Klicken Sie Auf \*Einstellungen\*.
- . Klicken Sie auf der Registerkarte \*Administrative Einstellungen\* auf \*Funktionen verwalten\*.
- . Wählen Sie im Dialogfeld \*Funktionen verwalten\* die zu Aktivieren anzuwählende VASA Provider-Erweiterung aus.
- . Wenn Sie die Replikationsfunktion für VVols-Datastores verwenden möchten, verwenden Sie die Schaltfläche \*VVols-Replizierung aktivieren\* umschalten.
- . Geben Sie die IP-Adresse der virtuellen Appliance für VSC, VASA Provider und SRA sowie das Administratorpasswort ein, und klicken Sie dann auf \*Anwenden\*.

.Nachdem Sie fertig sind

Bei Verwendung von ONTAP 9.6 oder älteren Clustern müssen Sie sich bei VASA Provider registrieren, um Details zu VVols Datastores und Virtual Machines zu erhalten, die in den Berichten über SAN VVols VM und SAN VVols Datastores verwendet werden. Aber wenn Sie ONTAP 9.7 oder höher verwenden, müssen Sie sich nicht bei VASA Provider registrieren.



:leveloffset: +1

[[ID59f119d98a517cd5b3c233729lead0d6]]

= Melden Sie sich mit der virtuellen Appliance für VSC, VASA Provider und SRA an

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Bei Verwendung von ONTAP 9.6 oder einer älteren Version können Sie über das vVol Dashboard nur Details zu VMware Virtual Volumes (VVols) Datastores und Virtual Machines anzeigen, wenn Sie sich für VASA Provider registriert haben, um Daten für die VVols-VM- und Datastore-Berichte abzurufen.

.Bevor Sie beginnen

Sie müssen 2.1 oder höher von heruntergeladen haben.

[NOTE]

====

Das vVol Dashboard zeigt Performance-Kennzahlen nur an, wenn SAN VVols Datastores und Virtual Machines mit ONTAP 9.3 oder höher konfiguriert werden.

====

.Schritte

. Klicken Sie auf der Virtual Storage Console (VSC) \*Startseite\*-Seite auf \*Einstellungen\*.

. Klicken Sie auf der Registerkarte \*Administrative Einstellungen\* auf \*Erweiterung verwalten\*.

. Verwenden Sie zum Aktivieren den Schieberegler \* OnCommand API Services\* registrieren.

. Geben Sie die IP-Adresse, den Service-Port und die Anmeldeinformationen für ein.

+

Sie können auch das Dialogfeld \*VASA Provider Extensions\* verwalten für die folgenden Änderungen verwenden:

+

\*\* So aktualisieren Sie die Registrierung, wenn Änderungen an den Anmeldedaten vorgenommen werden:

\*\* Um die Registrierung rückgängig zu machen, wenn Sie das vVol Dashboard nicht mehr benötigen.

+

Um die Registrierung für den VASA Provider zu entfernen, müssen Sie das Kontrollkästchen \* OnCommand API Services registrieren\* deaktivieren.

. Klicken Sie Auf \*Anwenden\*.

+

Das vVol Dashboard zeigt die Metriken für ONTAP 9.6 oder frühere SAN vVol Datastores nur an, nachdem die Registrierung abgeschlossen ist.

\*Verwandte Informationen\*

[https://mysupport.netapp.com/site/\["NetApp Support"^\]](https://mysupport.netapp.com/site/[)

:leveloffset: -1

[[ID053c993ec2fa48dd9f642f3b32b222f5]]

= Installieren Sie das NFS VAAI Plug-in

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Sie können das NFS-Plug-in für VMware vStorage APIs for Array Integration (VAAI) mithilfe der GUI der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) installieren.

.Bevor Sie beginnen

\* Sie müssen das Installationspaket für das NFS-Plug-in für VAAI heruntergeladen haben (`.vib`) Von .

+

[https://mysupport.netapp.com/site/\["NetApp Support"^\]](https://mysupport.netapp.com/site/[)

\* Sie müssen ESXi Host 6.5 oder höher und ONTAP 9.1 oder höher installiert haben.

\* Sie müssen den ESXi-Host eingeschaltet und einen NFS-Datastore gemountet

haben.

\* Sie müssen die Werte des festgelegt haben

`DataMover.HardwareAcceleratedMove`, `DataMover.HardwareAcceleratedInit`,  
und `VMFS3.HardwareAcceleratedLocking` Hosteinstellungen auf „1“.

+

Diese Werte werden automatisch auf dem ESXi-Host gesetzt, wenn das  
Dialogfeld *\*Empfohlene Einstellungen\** aktualisiert wird.

\* Sie müssen die vstorage-Option auf dem aktiviert haben, indem Sie die  
verwenden `vserver nfs modify -vserver vserver\_name -vstorage enabled`  
Befehl.

#### .Schritte

. Benennen Sie den um `.vib` Datei, die Sie von auf heruntergeladen haben  
`NetAppNasPlugin.vib` Um den von der VSC definierten Namen anzupassen.

. Klicken Sie auf der VSC Startseite auf *\*Einstellungen\**.

. Klicken Sie auf die Registerkarte *\*NFS VAAI Tools\**.

. Klicken Sie im Abschnitt *\*vorhandene Version\** auf *\*Ändern\**.

. Durchsuchen und wählen Sie den umbenannten aus `.vib` Datei, und klicken  
Sie dann auf *\*Upload\**, um die Datei auf das virtuelle Gerät hochzuladen.

. Wählen Sie im Abschnitt *\*auf ESXi Hosts installieren\** den ESXi Host aus,  
auf dem Sie das NFS VAAI Plug-in installieren möchten, und klicken Sie  
dann auf *\*Installieren\**.

+

Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation  
abzuschließen. Sie können den Installationsfortschritt im Abschnitt  
Aufgaben von vSphere Web Client überwachen.

. Starten Sie den ESXi-Host nach Abschluss der Installation neu.

+

Beim Neustart des ESXi Hosts erkennt VSC automatisch das NFS VAAI Plug-in.  
Sie müssen keine weiteren Schritte durchführen, um das Plug-in zu  
aktivieren.

[[ID499ee9caa704af4971d7a80f9040e5b7]]

= Aktivieren Sie Storage Replication Adapter

:allow-uri-read:

:experimental:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) bietet die Möglichkeit, die SRA Funktionen gemeinsam mit VSC zum Konfigurieren der Disaster Recovery zu nutzen.

.Bevor Sie beginnen

- \* Sie müssen Ihre vCenter Server-Instanz eingerichtet und ESXi konfiguriert haben.
- \* Sie müssen die virtuelle Appliance für VSC, VASA Provider und SRA implementiert haben.
- \* Sie müssen das heruntergeladen haben `.msi`` Datei für das SRA Plug-in oder das `.tar.gz`` Datei für die SRM-Appliance nur dann, wenn Sie die Disaster-Recovery-Lösung von Site Recovery Manager (SRM) konfigurieren möchten.

+

[https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install\\_config.doc/GUID-B3A49FFF-E3B9-45E3-AD35-093D896596A0.html](https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install_config.doc/GUID-B3A49FFF-E3B9-45E3-AD35-093D896596A0.html)["Site Recovery Manager Installation und Konfiguration Site Recovery Manager 8.2"^] Bietet weitere Informationen.

.Über diese Aufgabe

Dank der Flexibilität, VASA Provider und SRA Funktionen zu aktivieren, können Sie nur die Workflows ausführen, die Sie für Ihr Unternehmen benötigen.

.Schritte

- . Melden Sie sich bei der Web-Benutzeroberfläche von VMware vSphere an.
- . Klicken Sie im vSphere Client auf MENU:Menü[Virtuelle Speicherkonsole].
- . Klicken Sie Auf `*Einstellungen*`.
- . Klicken Sie auf der Registerkarte `*Administrative Einstellungen*` auf `*Funktionen verwalten*`.
- . Wählen Sie im Dialogfeld `*Funktionen verwalten*` die SRA-Erweiterung aus, die aktiviert werden soll.
- . Geben Sie die IP-Adresse der virtuellen Appliance für VSC, VASA Provider und SRA sowie das Administratorpasswort ein, und klicken Sie dann auf `*Anwenden*`.
- . Nutzen Sie für die Implementierung von SRA eine der folgenden Methoden:

+

[cols="1a,1a"]

|===

| Option | Beschreibung

a|  
Für Windows SRM  
a|  
.. Doppelklicken Sie auf das heruntergeladene `.msi` Installationsprogramm für das SRA-Plug-in.  
.. Befolgen Sie die Anweisungen auf dem Bildschirm.  
.. Geben Sie die IP-Adresse und das Kennwort Ihrer bereitgestellten virtuellen Appliance ein.

a|  
Für SRM Appliance  
a|  
.. Rufen Sie die SRM-Appliance-Seite auf und gehen Sie dann zur Seite \*Storage Replication Adapter\* der SRM-Appliance.  
.. Klicken Sie Auf \*Neuer Adapter\*.  
.. Laden Sie das Installationsprogramm für .tar.gz für das SRA-Plug-in auf SRM hoch.  
.. Überprüfen Sie die Adapter erneut, ob die Details auf der Seite SRM \*Storage Replication Adapter\* aktualisiert werden.

|===  
+  
Sie müssen sich vom vSphere Client abmelden und dann erneut anmelden, um zu überprüfen, ob die ausgewählte Erweiterung für die Konfiguration verfügbar ist.

\*Verwandte Informationen\*

xref:{relative\_path}concept-configure-storage-replication-adapter-for-disaster-recovery.adoc[Storage Replication Adapter für Disaster Recovery konfigurieren]

:leveloffset: +1

[[ID73c9251cb40b300e735623d38fd66ceb]]  
= Anmeldedaten für Storage Replication Adapter (SRA) aktualisieren  
:allow-uri-read:  
:icons: font

```
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Damit SRM mit SRA kommunizieren kann, sollten Sie die SRA-Anmeldedaten auf dem SRM-Server aktualisieren, wenn Sie die Anmeldedaten geändert haben.

.Bevor Sie beginnen

Sie sollten die im Thema „Configuring SRA on SRM Appliance“ genannten Schritte ausführen.

xref:{relative\_path}task-configure-sra-on-srm-appliance.adoc[Konfigurieren Sie SRA auf der SRM Appliance]

.Schritte

. Löschen Sie den Inhalt des ``/srm/sra/conf``Verzeichnis verwenden:

+

```
.. cd/srm/sra/conf
```

```
.. rm -rf *
```

. Führen Sie den Perl-Befehl aus, um SRA mit den neuen Zugangsdaten zu konfigurieren:

+

```
.. cd/srm/sra/
```

```
.. perl command.pl -i <va-IP> Administrator <va-password>
```

```
:leveloffset: -1
```

```
[[ID82810f44bb819731a05c4a0f630e04a3]]
```

= Migration von Windows SRM auf eine SRM Appliance

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Wenn Sie Windows-basierten Site Recovery Manager (SRM) für Disaster Recovery verwenden und die SRM-Appliance für dasselbe Setup verwenden

möchten, sollten Sie Ihr Windows Disaster Recovery-Setup auf die Appliance-basierte SRM migrieren.

Bei der Migration der Disaster Recovery sind folgende Schritte zu beachten:

- . Aktualisieren Sie Ihre vorhandene virtuelle Appliance für VSC, VASA Provider und SRA auf Version 9.7.1.

+

xref:{relative\_path}task-upgrade-to-the-9-7-1-virtual-appliance-for-vsc-vasa-provider-and-sra.html["Upgrade auf die virtuelle 9.7.1 Appliance für VSC, VASA Provider und SRA"^]

- . Migrieren von Windows-basiertem Storage Replication Adapter auf Appliance-basierte SRA

- . Migration von Windows SRM-Daten zu einer SRM-Appliance

[https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install\\_config.doc/GUID-F39A84D3-2E3D-4018-97DD-5D7F7E041B43.html](https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install_config.doc/GUID-F39A84D3-2E3D-4018-97DD-5D7F7E041B43.html)["Klicken Sie hier"^] Für detaillierte Schritte.

[[IDf98d8a7b6dd266b0ebc7820c3e52c137]]

= Upgrade auf die virtuelle 9.7.1 Appliance für VSC, VASA Provider und SRA

:allow-uri-read:

:experimental:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Anhand der hier angegebenen Anweisungen können Sie bei Ihrem vorhandenen Setup 9.7 ein direktes Upgrade auf die Version 9.7.1 der virtuellen Appliance für VSC, VASA Provider und SRA durchführen.

.Bevor Sie beginnen

- \* Sie müssen das heruntergeladen haben `.iso`` Datei zu Version 9.7.1 der virtuellen Appliance für VSC, VASA Provider und SRA.

- \* Sie müssen mindestens 12 GB RAM für die virtuelle Appliance reserviert haben, damit VSC, VASA Provider und SRA nach dem Upgrade optimal funktionieren können.

- \* Sie müssen den vSphere Client-Browser-Cache reinigen.

+

xref:{relative\_path}task-clean-the-vsphere-cached-downloaded-plugin-in-

packages.adoc[Reinigen Sie die heruntergeladenen Plug-in-Pakete von vSphere im Cache]

#### .Über diese Aufgabe

Nach dem Upgrade bleibt der Status von VASA Provider aus der vorhandenen Implementierung erhalten. Sie sollten VASA Provider anhand der Anforderungen nach dem Upgrade manuell aktivieren oder deaktivieren. VASA Provider sollte jedoch auch dann aktiviert werden, wenn nicht VMware Virtual Volumes (VVols) verwendet werden sollen, da damit Storage-Funktionsprofile für die herkömmliche Datastore-Bereitstellung und Storage-Alarme aktiviert werden können.

#### [NOTE]

====

Ein direktes Upgrade von einer Version vor 9.7 auf 9.7P2 oder höher wird von der virtuellen Appliance für VSC, VASA Provider und SRA nicht unterstützt. Sie sollten zunächst Ihre vorhandene Einrichtung auf Version 9.7 der virtuellen Appliance für VSC, VASA Provider und SRA aktualisieren, bevor Sie ein Upgrade auf eine spätere Version durchführen. Wenn Sie ein Upgrade auf Version 9.7.1 der virtuellen Appliance für VSC, VASA Provider und SRA durchführen und die VVols Replizierung nutzen möchten, müssen Sie noch einen vCenter Server mit installierter Virtual Appliance mit Site Recovery Manager (SRM) einrichten.

====

#### .Schritte

. Mounten Sie den heruntergeladenen ``.iso`` Datei zur virtuellen Appliance:  
+  
.. Klicken Sie auf Menü:Einstellungen bearbeiten[DVD/CD-ROM-Laufwerk].  
.. Wählen Sie in der Dropdown-Liste die Option `*Datastore ISO*`-Datei aus.  
.. Navigieren Sie zu dem heruntergeladenen Ordner, und wählen Sie es aus ``.iso`` Datei und dann das Kontrollkästchen `*beim Einschalten verbinden*` aktivieren.

. Öffnen Sie die Registerkarte `*Zusammenfassung*` Ihrer bereitgestellten virtuellen Appliance.

. Klicken Sie Auf `*image:../media/launch-maintenance-console.gif[""]*` Um die Wartungskonsole zu starten.

. Geben Sie an der Eingabeaufforderung „``Main Menu``“ die Option ein ``2``  
Geben Sie für `*Systemkonfiguration*` die Option ein ``8`` Für `*Upgrade*`.

+

Nach Abschluss des Upgrades wird die virtuelle Appliance neu gestartet. Die virtuelle Appliance für VSC, VASA Provider und SRA ist beim vCenter



Server mit derselben IP-Adresse wie vor dem Upgrade registriert.

. Wenn die virtuelle Appliance für VSC, VASA Provider und SRA beim vCenter Server mit der IPv6-Adresse registriert werden soll, müssen Sie Folgendes durchführen:

+

.. Lösen Sie die virtuelle Appliance für VSC, VASA Provider und SRA.  
.. Registrieren Sie die IPv6-Adresse der virtuellen Appliance für VSC, VASA Provider und SRA über die Seite \*Registrieren\* für vCenter Server.  
.. Erstellen Sie nach der Registrierung VSC- und VASA Provider-Zertifikate erneut.

+

[NOTE]

====

IPv6 wird nur ab vCenter Server 6.7 unterstützt.

====

. Melden Sie sich beim vSphere Client an und melden Sie sich erneut an, um die implementierte virtuelle Appliance für VSC, VASA Provider und SRA anzuzeigen.

+

.. Melden Sie sich von Ihrem vorhandenen vSphere Web Client oder vSphere Client ab, und schließen Sie das Fenster.  
.. Melden Sie sich beim vSphere Client an.

+

Es kann ein paar Minuten dauern, bis das Plug-in im vSphere Client aktualisiert wird.

\*Verwandte Informationen\*

xref:{relative\_path}task-enable-vasa-provider-for-configuring-virtual-datastores.adoc[Aktivieren Sie VASA Provider zur Konfiguration von virtuellen Datastores]

[[ID7509819e252510e7a1e424ed73615d49]]

= Aktualisieren Sie Den Storage Replication Adapter

:allow-uri-read:

:experimental:

:icons: font

```
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Nach einem Upgrade der virtuellen Appliance für VSC, VASA Provider und SRA oder der Implementierung der neuesten Version der virtuellen Appliance müssen Kunden ihr Storage Replication Adapter (SRA) aktualisieren.

```
.Schritte
```

. Sie müssen ein Upgrade auf den neuesten Adapter anhand einer der folgenden Verfahren durchführen, die auf Ihrem Adapter basieren:

```
+
```

```
[cols="1a,1a"]
```

```
|==
```

```
| * Für...* | Führen Sie folgende Schritte durch...
```

```
a|
```

```
*Windows*
```

```
a|
```

.. Melden Sie sich beim SRM Windows Server an.

.. Deinstallieren Sie das vorhandene SRA `_.msi_` -Installationsprogramm vom SRM-Server.

.. Ändern Sie den Systempfad in ``C:\Program Files\VMware\VMware vCenter Site Recovery Manager\external\perl\c\bin``

.. Doppelklicken Sie auf das Installationsprogramm für `_.msi_`, das Sie von der NetApp Support-Website heruntergeladen haben, und befolgen Sie die Anweisungen auf dem Bildschirm.

.. Geben Sie die IP-Adresse und das Passwort der implementierten virtuellen Appliance für VSC, VASA Provider und SRA ein.

```
a|
```

```
*Appliance-basierter Adapter*
```

```
a|
```

.. Melden Sie sich auf der SRM Appliance Management-Seite an.

.. Klicken Sie auf `*Storage Replication Adapter*` und klicken Sie auf `*Löschen*`, um die vorhandene SRA zu entfernen.

.. Klicken Sie auf Menü:Neuer Adapter[Durchsuchen].

.. Klicken Sie hier, um die aktuelle SRA Tarball-Datei auszuwählen, die Sie von der NetApp Support-Website heruntergeladen haben, und klicken Sie dann auf `*Installieren*`.

.. Konfigurieren Sie SRA auf der SRM Appliance.

```

+
xref:{relative_path}task-configure-sra-on-srm-appliance.adoc[Konfigurieren
Sie SRA auf der SRM Appliance]

|===

:leveloffset: -1

[[ID1aef5125dfdc489f25b77edacf853ee6]]
= Konfigurieren Sie Ihre Virtual Storage Console für VMware vSphere
Umgebung
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
(VSC) unterstützt zahlreiche Umgebungen. Einige Funktionen in diesen
Umgebungen erfordern möglicherweise zusätzliche Konfigurationen.

Möglicherweise müssen Sie einige der folgenden Aufgaben durchführen, um
Ihre ESXi Hosts, Gastbetriebssysteme und VSC zu konfigurieren:

* Überprüfen der ESXi-Hosteinstellungen, einschließlich der UNMAP-
Einstellungen
* Hinzufügen von Timeout-Werten für Gastbetriebssysteme
* Erneutes Generieren des VSC SSL-Zertifikats
* Erstellung von Storage-Funktionsprofilen und Schwellenwertwarnungen
* Ändern der Preferences-Datei, um das Mounten von Datastores über
verschiedene Subnetze zu ermöglichen

:leveloffset: +1

[[ID9bc9854778723513d3c6794784939c24]]
= Konfigurieren Sie Multipathing- und Zeitüberschreitungseinstellungen für

```

```
ESXi-Server
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Die Virtual Storage Console für VMware vSphere überprüft und legt die Einstellungen für Multipathing des ESXi Hosts und HBA-Zeitüberschreitungseinstellungen fest, die für Storage-Systeme am besten geeignet sind.

.Über diese Aufgabe

Dieser Prozess kann je nach Konfiguration und Systemlast sehr viel Zeit in Anspruch nehmen. Der Aufgabenfortschritt wird im Fenster \*Letzte Aufgaben\* angezeigt. Wenn die Aufgaben abgeschlossen sind, wird das Symbol für die Warnung des Host-Status durch das Symbol Normal oder das Symbol Ausstehender Neustart ersetzt.

.Schritte

. Klicken Sie auf der Seite VMware vSphere Web Client \*Home\* auf Menü:vCenter[Hosts].

. Klicken Sie mit der rechten Maustaste auf einen Host und wählen Sie dann Menü:Actions[NetApp VSC > Set Recommended Values] aus.

. Wählen Sie im Dialogfeld \*NetApp Recommended Settings\* die Werte aus, die für Ihr System am besten geeignet sind.

+

Standardmäßig werden die empfohlenen Standardwerte festgelegt.

+

image:.../media/vsc-recommended-hosts-settings.gif[die von vsc empfohlenen Hosteeinstellungen sind]

. Klicken Sie auf \*OK\*.

```
:leveloffset: +1
```

```
[[ID2ad215514ab5a6bf1f8f6443ab8f62d7]]
```

= ESXi-Hostwerte werden mit Virtual Storage Console für VMware vSphere festgelegt

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie können mithilfe der virtuellen Speicherkonsole für VMware vSphere Timeouts und andere Werte auf den ESXi-Hosts festlegen, um beste Leistung und erfolgreiches Failover zu gewährleisten. Die Werte, die Virtual Storage Console (VSC) setzt, basieren auf internen Tests.

Auf einem ESXi-Host können Sie die folgenden Werte festlegen:

== Erweiterte ESXi Konfiguration

\* \*VMFS3.HardwareAcceleratLocking\*

+

Sie sollten diesen Wert auf 1 setzen.

\* \*VMFS3.EnableBlockDelete\*

+

Sie sollten diesen Wert auf 0 setzen.

== NFS-Einstellungen

\* \*Net.TcpipHeapSize\*

+

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 32 setzen.

\* \*Net.TcpipHeapMax\*

+

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 1536 setzen.

\* \*NFS.MaxVolumes\*

+

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 256 setzen.

\* \*NFS41.MaxVolumes\*

+

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 256 setzen.

\* \*NFS.MaxQueueDepth\*

+

Wenn Sie vSphere 6.0 oder höhere ESXi Host-Version verwenden, sollten Sie diesen Wert auf 128 oder höher einstellen, um Engpässe zu vermeiden, in denen es zu Warteschlangen kommt.

+

Bei vSphere-Versionen vor 6.0 sollten Sie diesen Wert auf 64 einstellen.

\* \*NFS.HeartbeatMaxFailures\*

+

Sie sollten diesen Wert für alle NFS-Konfigurationen auf 10 setzen.

\* \*NFS.HeartbeatFrequency\*

+

Sie sollten diesen Wert für alle NFS-Konfigurationen auf 12 setzen.

\* \*NFS.HeartbeatTimeout\*

+

Sie sollten diesen Wert für alle NFS-Konfigurationen auf 5 setzen.

== FC-/FCoE-Einstellungen

\* \*Pfadauswahl-Richtlinie\*

+

Wenn FC-Pfade mit ALUA verwendet werden, sollten Sie diesen Wert auf „`RR`“ (Round Robin) setzen.

+

Sie sollten diesen Wert für alle anderen Konfigurationen auf „`FIXED`“ setzen.

+

Wenn Sie diesen Wert auf „`RR`“ setzen, ist für den Lastausgleich über alle aktiven/optimierten Pfade hinweg hilfreich. Der Wert „`FIXED`“ wird für ältere Konfigurationen ohne ALUA verwendet und verhindert Proxy-I/O

\* \*Disk.QFullSampleSize\*

+

Sie sollten diesen Wert für alle Konfigurationen auf 32 setzen. Durch die

Festlegung dieses Wertes werden I/O-Fehler verhindert.

\* \*Disk.QFullThreshold\*

+

Sie sollten diesen Wert für alle Konfigurationen auf 8 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

\* \* Emulex FC HBA-Timeouts\*

+

Standardwert verwenden.

\* \*QLogic FC HBA Timeouts\*

+

Standardwert verwenden.

== ISCSI-Einstellungen

\* \*Pfadauswahl-Richtlinie\*

+

Sie sollten diesen Wert für alle iSCSI-Pfade auf „`RR`“ setzen.

+

Wenn Sie diesen Wert auf „`RR`“ setzen, ist für den Lastausgleich über alle aktiven/optimierten Pfade hinweg hilfreich.

\* \*Disk.QFullSampleSize\*

+

Sie sollten diesen Wert für alle Konfigurationen auf 32 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

\* \*Disk.QFullThreshold\*

+

Sie sollten diesen Wert für alle Konfigurationen auf 8 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

[[IDc663fe27096bae5c3c9319939d758db9]]

= Konfigurieren von Gast-Betriebssystem-Skripten

:allow-uri-read:

```
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Die ISO-Images des Gastbetriebssystems (OS)-Skripte werden auf der Virtual Storage Console für VMware vSphere Server eingebunden. Damit Sie die Speicherzeituts für virtuelle Maschinen mithilfe der Gast-BS-Skripts festlegen können, müssen Sie die Skripte vom vSphere-Client mounten.

```
[cols="1a,1a,1a"]
```

```
|===
```

```
| Betriebssystemtyp | Einstellungen für das Zeitlimit von 60 Sekunden |
Einstellungen für das Zeitlimit von 190 Sekunden
```

```
a|
```

Linux

```
a|
```

```
`_https_://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-
install.iso`
```

```
a|
```

```
`_https_://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-
install.iso`
```

```
a|
```

Windows

```
a|
```

```
`_https_://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso
`
```

```
a|
```

```
`_https_://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190
.iso`
```

```
a|
```

Solaris

```
a|
```

```
`_https_://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-
install.iso`
```

```
a|
```

```
`_https_://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190
-install.iso`
```



|===

Sie sollten das Skript aus der Kopie der VSC-Instanz installieren, die beim vCenter Server registriert ist, der die Virtual Machine managt. Wenn in Ihrer Umgebung mehrere vCenter-Server enthalten sind, sollten Sie den Server auswählen, der die virtuelle Maschine enthält, für die Sie die Werte für das Speicherzeitlimit festlegen möchten.

Sie sollten sich bei der virtuellen Maschine anmelden und dann das Skript ausführen, um die Werte für die Speicherzeitüberschreitung festzulegen.

:leveloffset: +1

[[ID9361df91fc0a68fddd2091b5c335c152]]

= Legen Sie die Zeitüberschreitungswerte für Windows Gastbetriebssysteme fest

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Die Timeout-Skripte des Gastbetriebssystems (OS) legen die SCSI I/O Timeout-Einstellungen für Windows Gastbetriebssysteme fest. Sie können entweder eine Zeitüberschreitung von 60 Sekunden oder eine Zeitüberschreitung von 190 Sekunden angeben. Sie müssen das Windows Gast-Betriebssystem neu booten, damit die Einstellungen wirksam werden.

.Bevor Sie beginnen

Sie müssen das ISO-Image mit dem Windows-Skript angehängt haben.

.Schritte

. Greifen Sie auf die Konsole der virtuellen Windows-Maschine zu und melden Sie sich bei einem Konto mit Administratorrechten an.

. Wenn das Skript nicht automatisch startet, öffnen Sie das CD-Laufwerk, und führen Sie dann den aus `windows\_gos\_timeout.reg` Skript:

+

Das Dialogfeld Registry-Editor wird angezeigt.

. Klicken Sie auf \*Ja\*, um fortzufahren.

+

Die folgende Meldung wird angezeigt: `The keys and values contained in D:\windows\_gos\_timeout.reg have been successfully added to the registry.`

- . Starten Sie das Windows Gastbetriebssystem neu.
- . Heben Sie die Bereitstellung des ISO-Images auf.

```
[[IDc5b36d10d9e11622f452bdea4d966945]]
= Legen Sie Timeout-Werte für Solaris Gastbetriebssysteme fest
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]

Die Timeout-Skripte des Gastbetriebssystems (OS) legen die SCSI I/O Timeout-Einstellungen für Solaris 10 fest. Sie können entweder eine Zeitüberschreitung von 60 Sekunden oder eine Zeitüberschreitung von 190 Sekunden angeben.

.Bevor Sie beginnen

Sie müssen das ISO-Image mit dem Solaris-Skript angehängt haben.

.Schritte

. Greifen Sie auf die Konsole der virtuellen Solaris-Maschine zu und melden Sie sich bei einem Konto mit Root-Berechtigungen an.

. Führen Sie die aus `solaris\_gos\_timeout-install.sh` Skript:

+

Bei Solaris 10 wird eine Meldung wie die folgende angezeigt:

+

[listing]

----

Setting I/O Timeout for /dev/s-a - SUCCESS!

----

. Heben Sie die Bereitstellung des ISO-Images auf.

```
[[ID05304e330283bb44f310dfad45a1da73]]
= Legen Sie Timeout-Werte für Linux Gast-Betriebssysteme fest
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Die Timeout-Skripte des Gastbetriebssystems (OS) stellen die SCSI-I/O-Zeitüberschreitungseinstellungen für die Versionen 4, 5, 6 und 7 von Red hat Enterprise Linux sowie 9, 10 und 11 von SUSE Linux Enterprise Server ein. Sie können entweder eine Zeitüberschreitung von 60 Sekunden oder eine Zeitüberschreitung von 190 Sekunden angeben. Sie müssen das Skript jedes Mal ausführen, wenn Sie auf eine neue Linux-Version aktualisieren.

.Bevor Sie beginnen

Sie müssen das ISO-Image mit dem Linux-Skript angehängt haben.

.Schritte

. Greifen Sie auf die Konsole der virtuellen Linux-Maschine zu und melden Sie sich bei einem Konto mit Root-Berechtigungen an.

. Führen Sie die aus ``linux_gos_timeout-install.sh`` Skript:

+

Für Red hat Enterprise Linux 4 oder SUSE Linux Enterprise Server 9 wird eine Meldung wie die folgende angezeigt:

+

```
[listing]
```

```
----
```

```
Restarting udev... this may take a few seconds.
```

```
----
```

+

```
[listing]
```

```
----
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

```
----
```

+

Für Red hat Enterprise Linux 5, Red hat Enterprise Linux 6 und Red hat Enterprise Linux 7 wird eine Meldung wie die folgende angezeigt:

+

```
[listing]
```

```
----
```

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
----
```

+

```
[listing]
```

```
----
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
----
```

+

```
[listing]
```

```

-----
Restarting udev... this may take a few seconds.
-----
+
[listing]
-----
Starting udev: [ OK ]
-----
+
[listing]
-----
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
-----
+
Für SUSE Linux Enterprise Server 10 oder SUSE Linux Enterprise Server 11
wird eine Meldung wie die folgende angezeigt:

+
[listing]
-----
patching file /etc/udev/rules.d/50-udev-default.rules
-----
+
[listing]
-----
Hunk #1 succeeded at 114 (offset 1 line).
-----
+
[listing]
-----
Restarting udev ...this may take a few seconds.
-----
+
[listing]
-----
Updating all available device nodes in /dev:  done
-----
. Heben Sie die Bereitstellung des ISO-Images auf.

:leveloffset: -1

:leveloffset: -1

```

[[ID5981806882fa8d66dc22b362723be573]]

= Erstellen Sie ein SSL-Zertifikat für die virtuelle Speicherkonsole erneut

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Das SSL-Zertifikat wird bei der Installation (VSC) generiert. Der Distinguished Name (DN), der für das SSL-Zertifikat generiert wird, ist möglicherweise kein allgemeiner Name (CN), den die Clientcomputer erkennen. Durch Ändern der Passwörter für den Schlüsselspeicher und den privaten Schlüssel können Sie das Zertifikat erneut generieren und ein standortspezifisches Zertifikat erstellen.

.Über diese Aufgabe

Sie können die Remote-Diagnose mit der Wartungskonsole aktivieren und standortspezifisches Zertifikat generieren.

[https://kb.netapp.com/app/answers/answer\\_view/a\\_id/1075654](https://kb.netapp.com/app/answers/answer_view/a_id/1075654)["Antwort der NetApp Knowledgebase 1075654: Virtual Storage Console 7.x: Implementierung von CA-signierten Zertifikaten"^]

.Schritte

- . Melden Sie sich bei der Wartungskonsole an.
- . Eingabe `1` Für den Zugriff auf `Application Configuration` Menü.
- . Im `Application Configuration` Menü, ENTER `3` Um den VSC Service zu beenden.
- . Eingabe `7` Um das SSL-Zertifikat erneut zu generieren.

[[ID7000329000f5fbcee67e3d68760f7c43]]

= Voraussetzungen für die Registrierung von VSC in einer Umgebung mit mehreren vCenter Servern

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Wenn Sie Virtual Storage Console für VMware vSphere in einer Umgebung mit

einem einzelnen VMware vSphere HTML5-Client verwenden. Managt mehrere vCenter Server-Instanzen, müssen Sie eine Instanz von VSC bei jedem vCenter Server registrieren, sodass ein 1:1-Paarung zwischen der VSC und dem vCenter Server besteht. Auf diese Weise können Sie alle Server mit vCenter 6.0 oder höher sowohl im verknüpften Modus als auch im nicht verknüpften Modus von einem einzelnen vSphere HTML5 Client aus verwalten.

[NOTE]

====

Falls Sie VSC mit einem vCenter Server verwenden möchten, müssen Sie eine VSC-Instanz für jede zu verwaltende vCenter Server-Instanz eingerichtet oder registriert haben. Jede registrierte VSC Instanz muss von der gleichen Version sein.

====

Der verknüpfte Modus wird während der Bereitstellung von vCenter Server automatisch installiert. Der Linked-Modus verwendet den Microsoft Active Directory Application Mode (ADAM), um Daten über mehrere vCenter Server-Systeme hinweg zu speichern und zu synchronisieren.

Die Verwendung des vSphere HTML5 Client zur Durchführung von VSC Aufgaben über mehrere vCenter Server hinweg erfordert Folgendes:

- \* Für jeden vCenter Server im VMware Inventar, den Sie managen möchten, muss ein einzelner VSC Server mit einem eindeutigen 1:1-Paarungsvorgang registriert sein.

+

Zum Beispiel können Sie den VSC-Server A bei vCenter Server A registrieren, VSC-Server B bei vCenter Server B registriert sein, VSC-Server C bei vCenter Server C registriert sind usw.

+

Sie können \* nicht \* VSC Server Eine registriert haben, sowohl vCenter Server A und vCenter Server B.

+

Wenn ein VMware Inventar einen vCenter Server beinhaltet, für den kein VSC Server registriert ist, aber es gibt einen oder mehrere vCenter Server, die bei VSC registriert sind, Anschließend können Sie die Instanzen von VSC anzeigen und VSC Vorgänge für die vCenter Server ausführen, auf denen die VSC registriert ist.

- \* Sie müssen über die VSC-spezifische View-Berechtigung für jeden vCenter Server verfügen, der bei Single Sign-On (SSO) registriert ist.

+

Außerdem müssen Sie über die richtigen RBAC-Berechtigungen verfügen.

Wenn Sie eine Aufgabe ausführen, bei der Sie einen vCenter-Server angeben müssen, werden im Dropdown-Feld \*vCenter Server\* die verfügbaren vCenter-Server in alphanumerischer Reihenfolge angezeigt. Der standardmäßige vCenter Server ist immer der erste Server in der Dropdown-Liste.

Wenn der Speicherort des Speichers bekannt ist (z. B. wenn Sie den \*Provisioning\*-Assistenten verwenden und sich der Datastore auf einem Host befindet, der von einem bestimmten vCenter Server verwaltet wird), wird die vCenter Server-Liste als schreibgeschützte Option angezeigt. Dies geschieht nur, wenn Sie ein Element im vSphere Web Client mit der rechten Maustaste auswählen.

VSC warnt Sie, wenn Sie versuchen, ein Objekt auszuwählen, das nicht gemanagt wird.

Sie können Storage-Systeme auf der Grundlage eines bestimmten vCenter Servers von der VSC Übersichtsseite aus filtern. Für jede VSC Instanz, die mit einem vCenter Server registriert ist, wird eine Übersichtsseite angezeigt. Sie können die Storage-Systeme, die einer bestimmten VSC Instanz und vCenter Server zugeordnet sind, verwalten. Allerdings sollten Sie die Registrierungsinformationen für jedes Storage-System getrennt aufbewahren, wenn Sie mehrere Instanzen von VSC ausführen.

```
[[ID886136f0af90076c7dfe96ab018a4c18]]
= Konfigurieren Sie die VSC Preferences-Dateien
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Die Einstellungsdateien enthalten Einstellungen, die die Vorgänge Virtual Storage Console für VMware vSphere steuern. In den meisten Fällen müssen Sie die Einstellungen in diesen Dateien nicht ändern. Es ist hilfreich zu wissen, welche Vorzugsdateien (VSC) verwenden.

Die VSC enthält verschiedene Voreinstellungsdateien. Diese Dateien enthalten Eintragsschlüssel und Werte, die bestimmen, wie VSC verschiedene Vorgänge durchführt. Im Folgenden werden einige Präferenz-Dateien beschrieben, die VSC verwendet:

```
`/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml`
```

```
`/opt/netapp/vscserver/etc/vsc/vscPreferences.xml`
```

Möglicherweise müssen Sie die Voreinpräferenzen-Dateien in bestimmten Situationen ändern. Wenn Sie beispielsweise iSCSI oder NFS verwenden und das Subnetz zwischen Ihren ESXi Hosts und Ihrem Speichersystem unterschiedlich ist, müssen Sie die Voreinstellungen ändern. Falls Sie die Einstellungen in der Voreinstellungsdatei nicht ändern, schlägt die Datastore-Bereitstellung fehl, da VSC den Datastore nicht mounten kann.

```
:leveloffset: +1
```

```
[[ID4466744c1625a0646f7ccfee999c00e7]]
```

= Legen Sie IPv4 oder IPv6 fest

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Der Vorzugsdatei wurde eine neue Option hinzugefügt ``kaminoprefs.xml`` Die Sie einstellen können, dass IPv4 oder IPv6 für alle Storage-Systeme, die der VSC hinzugefügt werden, aktiviert werden.

\* Der `default.override.option.provision.mount.datastore.address.family` Der Parameter wurde dem hinzugefügt `kaminoprefs.xml` Bevorzugte Datei zur Festlegung eines bevorzugten LIF-Protokolls für die Bereitstellung von Datenspeichern.

+

Diese Präferenz gilt für alle neu zu VSC hinzugefügten Storage-Systeme.

\* Die Werte für die neue Option sind `IPv4`, `IPv6`, und `NONE`.

\* Der Wert ist standardmäßig auf festgelegt `NONE`.

```
[cols="1a,1a"]
```

```
|==
```

```
| Wert | Beschreibung
```

```
a|
```

KEINE

```
a|
```



- \* Bei der Bereitstellung wird derselbe IPv6- oder IPv4-Adresstyp von Daten-LIF wie der Typ des Clusters oder die Management-LIF verwendet, die zum Hinzufügen des Storage verwendet wird.
- \* Wenn der gleiche IPv6- oder IPv4-Adresstyp von Daten-LIF nicht in vorhanden ist, dann erfolgt die Bereitstellung über die andere Art von Daten-LIF, falls verfügbar.

```
a|
IPv4
```

```
a|
* Die Bereitstellung erfolgt über die IPv4 Daten-LIF in der ausgewählten .
* Wenn das keine IPv4-Daten-LIF hat, dann erfolgt die Bereitstellung über
die IPv6-Daten-LIF, wenn sie im verfügbar ist.
```

```
a|
IPv6
```

```
a|
* Die Bereitstellung erfolgt über die IPv6-Daten-LIF in der ausgewählten .
* Wenn das keine IPv6-Daten-LIF hat, dann erfolgt die Bereitstellung über
die IPv4-Daten-LIF, sofern sie im verfügbar ist.
```

```
|===
```

```
:leveloffset: -1
```

```
[[IDc762fb02193a6b279e35744c1221835f]]
= Aktivieren Sie das Mounten von Datenspeichern in unterschiedlichen
Subnetzen
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Wenn Sie iSCSI oder NFS verwenden und sich das Subnetz zwischen Ihren ESXi Hosts und Ihrem Speichersystem unterscheidet, müssen Sie die

Voreinstellungen für Virtual Storage Console für VMware vSphere ändern.  
Wenn Sie die Voreinferenzdatei nicht ändern, schlägt die Bereitstellung von Datastore fehl, da (VSC) den Datastore nicht mounten kann.

.Über diese Aufgabe

Wenn die Bereitstellung von Datenspeichern fehlschlägt, protokolliert VSC die folgenden Fehlermeldungen:

```
`Unable to continue. No ip addresses found when cross-referencing kernel  
ip addresses and addresses on the controller.`
```

```
`Unable to find a matching network to NFS mount volume to these hosts.` ``
```

.Schritte

. Melden Sie sich bei Ihrer vCenter Server-Instanz an.

. Starten Sie die Wartungskonsole mit der virtuellen Maschine Ihrer vereinheitlichten Appliance.

+

```
xref:{relative_path}task-access-virtual-appliance-maintenance-console-  
options.html["Greifen Sie auf die Optionen der Wartungskonsole der  
virtuellen Appliance für VSC, VASA Provider und SRA zu"]
```

. Eingabe `4` Um die Option \*Support und Diagnose\* zu öffnen.

. Eingabe `2` Um die Option \*Access Diagnostic Shell\* zu öffnen.

. Eingabe `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` Um die zu aktualisieren `kaminoprefs.xml` Datei:

. Aktualisieren Sie die `kaminoprefs.xml` Datei:

+

```
[cols="1a,1a"]
```

```
|===
```

```
| Verwenden Sie... | Tun Sie das...
```

```
a|
```

```
ISCSI
```

```
a|
```

Ändern Sie den Wert der Eintragstaste `default.allow.iscsi.mount.networks` Von ALLEN bis zum Wert Ihrer ESXi Hostnetzwerke.

```
a|
```

```
NFS
```

```
a|
```

Ändern Sie den Wert der Eintragstaste `default.allow.nfs.mount.networks` Von ALLEN bis zum Wert Ihrer ESXi Hostnetzwerke.

|===

+

Die Vorgabedatei enthält Beispielwerte für diese Eintragstasten.

+

[NOTE]

=====

Der Wert „`ALL`“ bedeutet nicht alle Netzwerke. „`ALL`“ ermöglicht die Verwendung aller übereinstimmenden Netzwerke zwischen dem Host und dem Speichersystem zur Mounten von Datastores. Wenn Sie Hostnetzwerke angeben, können Sie das Mounten nur über die angegebenen Subnetze aktivieren.

=====

. Speichern und schließen Sie das `kaminoprefs.xml` Datei:

```
[[ID5e07642b8ce193c8e201a5e9fcbce8fe]]
```

= Greifen Sie auf die Optionen der Wartungskonsole der virtuellen Appliance für VSC, VASA Provider und SRA zu

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Ihre Applikations-, System- und Netzwerkkonfigurationen können über die Wartungskonsole der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) gemanagt werden. Sie können Ihr Administratorkennwort und Ihr Wartungskennwort ändern. Außerdem können Sie Supportpakete generieren, verschiedene Protokollebenen festlegen, TLS-Konfigurationen anzeigen und verwalten und die Remote-Diagnose starten.

.Bevor Sie beginnen

Nach der Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA müssen die VMware Tools installiert sein.

.Über diese Aufgabe

- \* Sie müssen „`maint`“ als Benutzername und das bei der Implementierung konfigurierte Passwort verwenden, um sich bei der Wartungskonsole der virtuellen Appliance für VSC, VASA Provider und SRA anzumelden.

- \* Sie müssen ein Passwort für den Benutzer „`diag`“ festlegen, während Sie die Ferndiagnose aktivieren.

.Schritte

. Öffnen Sie die Registerkarte \*Zusammenfassung\* Ihrer bereitgestellten virtuellen Appliance.

. Klicken Sie Auf `image:../media/launch-maintenance-console.gif[""]` Um die Wartungskonsole zu starten.

+

Sie können auf die folgenden Optionen für die Wartungskonsole zugreifen:

+

\*\* \*Anwendungskonfiguration\*

+

Folgende Optionen stehen zur Verfügung:

+

\*\*\* Zeigt eine Zusammenfassung des Serverstatus an

\*\*\* Starten Sie den Virtual Storage Console Service

\*\*\* Beenden Sie den Virtual Storage Console Service

\*\*\* Starten Sie VASA Provider und SRA Service

\*\*\* Beenden Sie den VASA Provider und den SRA Service

\*\*\* Ändern Sie das Benutzerpasswort „Administrator“

\*\*\* Zertifikate erneut generieren

\*\*\* Hard Reset KeyStore und Zertifikate

\*\*\* Hard Reset-Datenbank

\*\*\* ÄNDERN SIE DAS PROTOKOLL-Level für den Virtual Storage Console-Service

\*\*\* Ändern Sie DIE PROTOKOLLEBENE für den VASA Provider und den SRA Service

\*\*\* Anzeigen der TLS-Konfiguration

\*\*\* Aktivieren des TLS-Protokolls

\*\*\* Deaktivieren des TLS-Protokolls

\*\* \*Systemkonfiguration\*

+

Folgende Optionen stehen zur Verfügung:

+

\*\*\* Starten Sie die virtuelle Maschine neu

\*\*\* Virtuelle Maschine herunterfahren

\*\*\* Ändern Sie das Benutzerpasswort „Wartung“

\*\*\* Zeitzone ändern

\*\*\* NTP-Server ändern

+

Sie können eine IPv6-Adresse für Ihren NTP-Server angeben.

\*\*\* SSH-Zugriff aktivieren/deaktivieren

\*\*\* Erhöhen der Größe der Jail-Festplatte (/jail)

\*\*\* Upgrade

\*\*\* Installation der VMware Tools

\*\* \*Netzwerkkonfiguration\*

+

Folgende Optionen stehen zur Verfügung:

+

\*\*\* Zeigt die Einstellungen für die IP-Adresse an

\*\*\* Ändern Sie die IP-Adresseinstellungen

+

Sie können diese Option verwenden, um die IP-Adresse nach der Implementierung in IPv6 zu ändern.

\*\*\* Zeigen Sie die Einstellungen für die Suche nach Domain-Namen an

\*\*\* Ändern Sie die Einstellungen für die DNS-Suche

\*\*\* Statische Routen anzeigen

\*\*\* Ändern Sie statische Routen

+

Sie können diese Option verwenden, um eine IPv6-Route hinzuzufügen.

\*\*\* Änderungen speichern

\*\*\* Ping an einen Host

+

Sie können diese Option verwenden, um einen Ping an einen IPv6-Host zu senden.

\*\*\* Standardeinstellungen wiederherstellen

\*\* \*Support und Diagnose\*

+

Folgende Optionen stehen zur Verfügung:

+

\*\*\* Erzeugen Sie das Support Bundle

\*\*\* Zugriff auf die Diagnoseschale

\*\*\* Remote-Diagnosezugriff aktivieren

\*Verwandte Informationen\*

xref:{relative\_path}concept-virtual-storage-console-and-vasa-provider-log-files.adoc[Protokolldateien von VSC und VASA Provider]

```
[[ID45e8deedb8cef78db8feca0b415d78cb]]
= Ändern Sie das Administratorpasswort
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]

Sie können das Administratorpasswort der virtuellen Appliance für VSC, VASA Provider und SRA nach der Implementierung über die Wartungskonsole ändern.

.Schritte

- . Öffnen Sie über den vCenter Server eine Konsole für die virtuelle Appliance für VSC, VASA Provider und SRA.
- . Melden Sie sich als Wartungbenutzer an.
- . Eingabe `1` Wählen Sie in der Wartungskonsole *\*Anwendungskonfiguration\** aus.
- . Eingabe `6` So wählen Sie *\*Administratorpasswort ändern\** aus.
- . Geben Sie ein Passwort mit mindestens acht Zeichen und maximal 63 Zeichen ein.
- . Eingabe `y` Im Bestätigungsdialogfeld.

```
[[ID1e54e67ce39a18df7bb69271bc3580f5]]
= Konfigurieren Sie Hochverfügbarkeit für die virtuelle Appliance für VSC,
VASA Provider und SRA
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]

Die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) unterstützt eine Konfiguration (HA), sodass während eines Ausfalls unterbrechungsfreie Funktionen von VSC, VASA

Provider und SRA verfügbar gemacht werden.

Die virtuelle Appliance für VSC, VASA Provider und SRA basiert auf der VMware vSphere (HA)-Funktion und der vSphere Fehlertoleranz (FT)-Funktion. (HA)-Lösung bietet eine schnelle Recovery nach Ausfällen. Die folgenden Ursachen sind:

- \* Host-Ausfall
- \* Netzwerkausfall
- \* Fehler bei Virtual Machine (Ausfall des Gastbetriebssystems)
- \* Absturz der Applikation (VSC, VASA Provider und SRA)

Auf der virtuellen Appliance ist keine zusätzliche Konfiguration erforderlich. Nur vCenter-Server und ESXi-Hosts müssen mit der VMware vSphere HA-Funktion oder der vSphere FT-Funktion basierend auf ihren Anforderungen konfiguriert werden. Sowohl HA als AUCH FT erfordern Cluster-Hosts zusammen mit Shared Storage. FT hat zusätzliche Anforderungen und Einschränkungen.

Neben der VMware vSphere HA Lösung und der vSphere FT Lösung unterstützt die virtuelle Appliance auch dabei, VSC, VASA Provider und SRA Services jederzeit verfügbar zu halten. Der Watchdog-Prozess der virtuellen Appliance überwacht regelmäßig alle drei Dienste und startet sie automatisch neu, wenn Fehler erkannt werden. So wird Applikationsausfälle verhindert.

[NOTE]

====

VCenter HA wird von der virtuellen Appliance für VSC, VASA Provider und SRA nicht unterstützt.

====

:leveloffset: +1

[[ID52b7d283061c9c7f739977c061b0d254]]

= VMware vSphere HA

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Sie können Ihre vSphere Umgebung dort konfigurieren, wo die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) für (HA) implementiert wird. Die VMware HA-Funktion bietet Failover-Schutz vor Hardware-Ausfällen und Ausfällen des Betriebssystems in virtuellen Umgebungen.

Die VMware HA Funktion überwacht Virtual Machines und erkennt so Betriebssystemausfälle und Hardwareausfälle. Wenn ein Fehler erkannt wird, startet die VMware HA-Funktion die virtuellen Maschinen auf den anderen physischen Servern im Ressourcenpool neu. Wenn ein Serverfehler erkannt wird, ist keine manuelle Intervention erforderlich.

Das Verfahren zur Konfiguration von VMware HA hängt von der Version des vCenter Servers ab. Sie können beispielsweise den folgenden Referenzlink verwenden und die erforderliche vCenter Server-Version auswählen, um die Schritte zum Konfigurieren von VMware HA anzuzeigen.

<https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html>["VMware vSphere Dokumentation: Erstellen und Verwenden von vSphere HA-Clustern"]

```
[[IDd852a657f4cd90c3212b5e493a3dd7bb]]
= Fehlertoleranz für VMware vSphere
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Die VMware vSphere Fault Tolerance (FT) Funktion bietet (HA) auf höherer Ebene und ermöglicht es Ihnen, Virtual Machines ohne Datenverlust oder Verbindungen zu schützen. Sie müssen vSphere FT für die virtuelle Appliance für VSC, VASA Provider und SRA über Ihren vCenter Server aktivieren oder deaktivieren.

Stellen Sie sicher, dass Ihre vSphere Lizenz FT mit der Anzahl der vCPUs unterstützt, die die virtuelle Appliance in Ihrer Umgebung benötigt (mindestens 2 vCPUs; 4 vCPUs für große Umgebungen).

VSphere FT ermöglicht den Betrieb von Virtual Machines selbst bei Serverausfällen. Wenn vSphere FT auf einer virtuellen Maschine aktiviert ist, wird automatisch eine Kopie der primären virtuellen Maschine auf einem anderen Host (der sekundären virtuellen Maschine) erstellt, der vom



Distributed Resource Scheduler (DRS) ausgewählt wird. Wenn DRS nicht aktiviert ist, wird der Zielhost von den verfügbaren Hosts ausgewählt. VSphere FT betreibt die primäre virtuelle Maschine und die sekundäre virtuelle Maschine im Sperrmodus, wobei jeder den Ausführungsstatus der primären Virtual Machine auf die sekundäre Virtual Machine spiegelt.

Wenn ein Hardwarefehler auftritt, der dazu führt, dass die primäre virtuelle Maschine ausfällt, nimmt die sekundäre virtuelle Maschine sofort dort auf, wo die primäre virtuelle Maschine angehalten wurde. Die sekundäre Virtual Machine wird weiterhin ohne Verlust von Netzwerkverbindungen, Transaktionen oder Daten ausgeführt.

Ihr System muss die CPU-Anforderungen, die Grenzwerte für virtuelle Maschinen sowie die Lizenzierungsanforderungen für die Konfiguration von vSphere FT für Ihre vCenter Server-Instanz erfüllen.

Das Verfahren zur HA-Konfiguration hängt von der Version des vCenter Servers ab. Sie können beispielsweise den folgenden Referenzlink verwenden und die erforderliche vCenter Server-Version auswählen, um die Schritte zum Konfigurieren von HA anzuzeigen.

<https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.avail.doc/GUID-57929CF0-DA9B-407A-BF2E-E7B72708D825.html>["VMware vSphere Dokumentation: Fehlertoleranz, Beschränkungen und Lizenzierung"]

:leveloffset: -1

[[ID5238d05a9bceaa164f3636f8d5b2c4ed]]

= Von der virtuellen Appliance unterstützte MetroCluster Konfigurationen für VSC, VASA Provider und SRA

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) unterstützt Umgebungen, die MetroCluster IP- und FC-Konfigurationen für ONTAP verwenden. Der Support erfolgt meistens automatisch. Unter Umständen können Sie bei Verwendung einer MetroCluster Umgebung mit VSC und VASA Provider jedoch einige Unterschiede feststellen.

## == MetroCluster Konfigurationen und VSC

Sie müssen sicherstellen, dass die VSC die Storage-System-Controller am primären und sekundären Standort erkennt. In der Regel erkennt VSC automatisch Storage Controller. Wenn Sie eine Cluster-Management-LIF verwenden, empfehlen wir, sicherzustellen, dass die VSC die Cluster an beiden Standorten erkannt hat. Andernfalls können Sie die Storage Controller manuell zur VSC hinzufügen. Sie können auch den Benutzernamen und die Passwörter, die VSC für die Verbindung zu den Storage Controllern verwendet, ändern.

Bei einem Switchover wird der am sekundären Standort übertragen. Diese haben das Suffix „`-mc`“ an ihre Namen angehängt. Falls während eines Umschaltvorgangs z. B. zur Bereitstellung eines Datastores ein Switchover stattfindet, wird der Name des Speicherorts geändert und schließt dann das „`-mc`“-Suffix ein. Dieses Suffix wird beim Zurückwechsel abgebrochen und das Suffix am primären Standort wird mit der Steuerung fortgesetzt.

[NOTE]

====

Wenn Sie direkt mit der MetroCluster Konfiguration zur VSC hinzugefügt haben, so wird nach der Umschaltung die Änderung des SVM-Namens (hinzugefügt durch das „`-mc`“ Suffix) nicht wiedergegeben. Alle anderen Switchover-Vorgänge werden weiterhin normal ausgeführt.

====

Wenn ein Switchover oder ein Switchover stattfindet, kann die VSC einige Minuten dauern, um die Cluster automatisch zu erkennen und zu erkennen. Wenn dies während der Durchführung einer VSC-Operation wie der Bereitstellung eines Datenspeichers geschieht, kann es zu Verzögerungen kommen.

## == MetroCluster Konfigurationen und VASA Provider

VASA-Provider unterstützt automatisch Umgebungen, die MetroCluster-Konfigurationen verwenden. Die Umschaltung ist in VASA Provider-Umgebungen transparent. Sie können kein direktes Add-to-VASA-Provider hinzufügen.

[NOTE]

====

VASA Provider fügt nach einer Umschaltung das Suffix „`-mc`“ nicht an die

Namen des am sekundären Standort an.

====

== MetroCluster Konfigurationen und SRA

SRA unterstützt keine MetroCluster-Konfigurationen.

:leveloffset: -1

[[ID899147af30bf2d9681d0a31835e140d9]]

= Konfigurieren Sie Ihre Virtual Storage Console für VMware vSphere  
Storage-System-Umgebung

:allow-uri-read:

:experimental:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Virtual Storage Console für VMware vSphere bietet einen einzigen Mechanismus, mit dem Storage-Systeme erfasst und die Storage-Zugangsdaten festgelegt werden können. Sie stellen die ONTAP-Berechtigungen bereit, die erforderlich sind, damit Benutzer von Virtual Storage Console (VSC) mithilfe der Storage-Systeme Aufgaben durchführen können.

Bevor VSC die Storage-Ressourcen anzeigen und managen kann, muss VSC die Storage-Systeme erkennen. Im Rahmen des Erkennungsvorgangs müssen Sie die ONTAP Zugangsdaten für Ihre Storage-Systeme angeben. Hierbei handelt es sich um die Berechtigungen (oder Rollen), die mit dem Benutzernamen und dem Kennwort-Paar verknüpft sind, das jedem Speichersystem zugewiesen ist. Diese Benutzername und Passwort-Paare verwenden die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) von ONTAP und müssen aus ONTAP heraus eingerichtet werden. Sie können diese Anmeldedaten nicht in VSC ändern. Sie können ONTAP RBAC-Rollen mit definieren.

[NOTE]

====

Wenn Sie sich als Administrator anmelden, verfügen Sie automatisch über alle Berechtigungen für dieses Speichersystem.

====

Wenn Sie der VSC ein Storage-System hinzufügen, müssen Sie eine IP-Adresse für das Storage-System und den mit dem System verknüpften Benutzernamen und das Passwort eingeben. Sie können Standardanmeldeinformationen einrichten, die VSC während der Erkennung des Storage-Systems verwendet, oder Sie können manuell die Anmeldedaten eingeben, wenn das Speichersystem erkannt wird. Die Details des Storage-Systems, das zur VSC hinzugefügt wird, werden automatisch an die Erweiterungen weitergeleitet, die Sie bei Ihrer Implementierung aktivieren. Sie müssen nicht manuell Storage zu VASA Provider und Storage Replication Adapter (SRA) hinzufügen. VSC und SRA unterstützen das Hinzufügen von Anmeldeinformationen auf Cluster-Ebene und -Ebene. VASA Provider unterstützt nur Cluster-Level-Anmeldeinformationen zum Hinzufügen von Storage-Systemen.

Wenn in Ihrer Umgebung mehrere vCenter Server-Instanzen enthalten sind, wird beim Hinzufügen eines Storage-Systems zur VSC von der Seite Storage Systems aus ein vCenter Server-Feld angezeigt, in dem Sie angeben können, welcher vCenter Server-Instanz das Speichersystem hinzugefügt werden soll. Wenn Sie ein Speichersystem hinzufügen, indem Sie mit der rechten Maustaste auf einen Rechenzentrumsnamen klicken, können Sie keine vCenter Server-Instanz angeben, da der Server bereits mit diesem Datacenter verknüpft ist.

Die Bestandsaufnahme erfolgt auf eine der folgenden Arten. In jedem Fall müssen Sie die Anmeldeinformationen für jedes neu entdeckte Speichersystem angeben.

- \* Sobald der VSC Service gestartet wird, beginnt die VSC den automatischen Prozess der Bestandsaufnahme.

- \* Sie können auf der Seite Storage Systems auf die Schaltfläche \*ALLE WIEDERENTDECKEN\* klicken oder auf einem Host oder einem Rechenzentrum klicken, um sie im Menü \*Aktionen\* auszuwählen (Menü:Aktionen[NetApp VSC > Host- und Speicherdaten aktualisieren]). Sie können auch auf der Registerkarte „erste Schritte“ im Abschnitt „Übersicht“ auf \*ENTDECKEN\* klicken.

Für alle VSC Funktionen sind spezielle Berechtigungen zum Durchführen von Aufgaben erforderlich. Sie können festlegen, was Benutzer basierend auf den mit der ONTAP-Rolle verknüpften Anmeldeinformationen tun können. Alle Benutzer mit demselben Benutzernamen und Kennwort-Paar des Speichersystems nutzen die gleichen Anmeldeinformationen für das Speichersystem und können dieselben Vorgänge ausführen.

:leveloffset: +1

```
[[ID4b8cda204e90f53a83bc6438d7d5578f]]
```

```
= Legen Sie die Standardanmeldeinformationen für Speichersysteme fest  
:allow-uri-read:  
:experimental:  
:icons: font  
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie können die virtuelle Speicherkonsole für VMware vSphere verwenden, um Standardanmeldeinformationen für ein Speichersystem in Ihrem vCenter Server festzulegen.

.Bevor Sie beginnen

Sie müssen den vCenter Server ausgewählt haben, den Sie zum Erstellen von Standardanmeldeinformationen verwenden möchten.

.Über diese Aufgabe

Wenn Sie Standardanmeldeinformationen für Storage-Systeme einrichten, verwendet (VSC) diese Zugangsdaten, um sich in einem Storage-System anzumelden, das die VSC gerade erkannt hat. Wenn die Standardanmeldeinformationen nicht funktionieren, müssen Sie sich manuell beim Speichersystem anmelden. VSC und SRA unterstützen das Hinzufügen von Anmeldeinformationen des Storage-Systems auf Cluster-Ebene oder -Ebene. Vasa Provider kann aber nur mit Anmeldedaten auf Cluster-Ebene arbeiten.

.Schritte

. Klicken Sie auf der VSC \*Home\* Seite auf Menü:Einstellungen[Administratoreinstellungen > Standardanmeldedaten für Storage-System konfigurieren].

. Geben Sie im Dialogfeld \*Speichersystemstandard-Anmeldeinformationen\* den Benutzernamen und das Kennwort für das Speichersystem ein.

+

Storage Controller-Anmeldedaten werden in ONTAP basierend auf dem Benutzernamen und dem Passwort-Paar zugewiesen. Die Zugangsdaten für den Storage Controller können entweder das Administratorkonto oder ein benutzerdefiniertes Konto, das die rollenbasierte Zugriffssteuerung verwendet.

+

Sie können die Rollen, die dem Benutzernamen und Passwort des Storage Controllers zugeordnet sind, nicht mit VSC ändern. Zum Ändern oder Erstellen einer neuen ONTAP Benutzerrolle zur Verwendung mit der virtuellen Appliance für VSC, VASA Provider und SRA können Sie System

Manager verwenden.

+

Weitere Informationen finden Sie im Abschnitt „`Konfigurieren von Benutzerrollen und -Berechtigungen`“ im Handbuch „\_Virtual Storage Console, VASA Provider und Storage Replication Adapter für VMware® vSphere Deployment and Setup Guide for 9.7 Release\_.

. Klicken Sie auf \*OK\*, um die Standardanmeldeinformationen zu speichern.

.Nachdem Sie fertig sind

Wenn Sie die Anmeldedaten des Speichersystems aktualisiert haben, weil ein Speichersystem den Status „`Authentifizierungsfehler`“ gemeldet hat, klicken Sie auf die Option \*ALLE WIEDERERKENNEN\*, die auf der Seite Speichersysteme verfügbar ist. Ist dies der Fall, versucht die VSC mithilfe der neuen Zugangsdaten, sich mit dem Storage-System zu verbinden.

```
[[ID561c7d6a3a697759131cfc445d856074]]
```

= Fügen Sie Storage-Systeme zur VSC hinzu

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie können Storage-System manuell zur Virtual Storage Console (VSC) hinzufügen.

.Über diese Aufgabe

Jedes Mal, wenn Sie starten (VSC) oder wählen Sie die Option \*ALLE\* WIEDERENTDECKEN, erkennt VSC automatisch die verfügbaren Speichersysteme.

.Schritte

. Fügen Sie zur VSC ein Storage-System über die VSC Startseite hinzu:

+

\*\* Klicken Sie auf Menü:Speichersysteme[Hinzufügen].

\*\* Klicken Sie auf Menü:Übersicht[erste Schritte] und dann auf die Schaltfläche \*HINZUFÜGEN\* unter \*Speichersystem hinzufügen\*.

. Geben Sie im Dialogfeld \*Storage-System hinzufügen\* die Management-IP-Adresse und die Anmeldeinformationen für dieses Speichersystem ein.

+

Sie können auch Speichersysteme hinzufügen, indem Sie die IPv6-Adresse des Clusters oder verwenden. In diesem Dialogfeld können Sie außerdem die Standardwerte für TLS und die Portnummer ändern.

+

Wenn Sie Speicher von der VSC *\*Storage System\** Seite hinzufügen, müssen Sie auch die vCenter Server Instanz angeben, wo sich der Speicher befindet. Das Dialogfeld *\*Storage-System hinzufügen\** enthält eine Dropdown-Liste der verfügbaren vCenter Server-Instanzen. Die VSC zeigt diese Option nicht an, wenn Sie einem Rechenzentrum Storage hinzufügen, das bereits einer vCenter Server-Instanz zugeordnet ist.

. Klicken Sie auf *\*OK\**, nachdem Sie alle erforderlichen Informationen hinzugefügt haben.

```
[[IDa18e06b2c58bbfaa2336aa9cb41bdb8c]]
```

= Erkennen von Storage-Systemen und Hosts

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Wenn Sie zum ersten Mal (VSC) in einem vSphere Client ausführen, erkennt VSC die ESXi Hosts, ihre LUNs und NFS Exporte und die NetApp Storage-Systeme, die im Besitz dieser LUNs und Exporte sind.

.Bevor Sie beginnen

- \* Alle ESXi-Hosts müssen eingeschaltet und verbunden sein.

- \* Alle zu erkannten Daten müssen ausgeführt werden, und jeder Cluster Node muss über mindestens eine Daten-LIF verfügen, die für das verwendete Storage-Protokoll (NFS, iSCSI oder FC) konfiguriert ist.

.Über diese Aufgabe

Sie können jederzeit neue Storage-Systeme ermitteln oder Informationen zu vorhandenen Storage-Systemen aktualisieren, um die aktuellsten Kapazitäts- und Konfigurationsinformationen zu erhalten. Sie können auch die Zugangsdaten, die VSC zur Anmeldung bei den Storage-Systemen verwendet, ändern.

Bei der Erkennung der Storage-Systeme erfasst VSC Informationen von den ESXi Hosts, die von der vCenter Server Instanz gemanagt werden.

#### .Schritte

- . Wählen Sie auf der Seite vSphere Client \*Home\* die Option \*Hosts und Cluster\* aus.

- . Klicken Sie mit der rechten Maustaste auf das gewünschte Datacenter und wählen Sie dann Menü:NetApp VSC[Update Host and Storage Data].

+

Die VSC zeigt ein Dialogfeld „Bestätigen“ an, in dem Sie darauf hingewiesen werden, dass dieser Vorgang viel Zeit in Anspruch nehmen kann.

- . Klicken Sie auf \*OK\*.

- . Wählen Sie die erkannten Speichercontroller mit dem Status „`Authentifizierungsfehler`“ aus, und klicken Sie dann auf Menü:AKTIONEN[Ändern].

- . Geben Sie die erforderlichen Informationen in das Dialogfeld \*Speichersystem ändern\* ein.

- . Wiederholen Sie die Schritte 4 und 5 für alle Speichercontroller mit dem Status „`Authentication Failure`“.

.Nachdem Sie fertig sind

Nach Abschluss des Erkennungsvorgangs führen Sie folgende Schritte aus:

- \* Verwenden Sie VSC, um ESXi Hosteinstellungen für Hosts zu konfigurieren, die das Warnsymbol in der Spalte \*Adaptoreinstellungen\*, der Spalte \*MPIO Settings\* oder der Spalte \*NFS Settings\* anzeigen.

- \* Geben Sie die Anmeldeinformationen des Speichersystems an.

```
[[ID865a7dad5c025baa25c79457eb023f7b]]
```

= Aktualisieren Sie die Anzeige des Speichersystems

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie können die von Virtual Storage Console für VMware vSphere bereitgestellte Aktualisierungsfunktion verwenden, um die Informationen zu Storage-Systemen zu aktualisieren und die Virtual Storage Console (VSC) zur Erkennung von Storage-Systemen zu erzwingen.



.Über diese Aufgabe

Die Option „`reFresh`“ ist nützlich, wenn Sie die Standardanmeldeinformationen für die Speichersysteme nach Erhalt eines Authentifizierungsfehlers geändert haben. Sie sollten immer einen Aktualisierungsvorgang durchführen, wenn Sie die Anmeldedaten des Speichersystems geändert haben, nachdem das Speichersystem „`Authentifizierungsfehler`“ gemeldet hat. Während des Updates versucht VSC, mithilfe der neuen Zugangsdaten eine Verbindung zum Storage-System herzustellen.

Je nach System-Setup kann dieser Vorgang viel Zeit in Anspruch nehmen.

.Schritte

. Klicken Sie auf der Seite VMware vSphere Client \*Home\* auf \*Storage Systems\*.

. Starten Sie das Update:

+

[cols="1a,1a"]

|===

| Wenn dieser Standort... | Klicken Sie Auf...

a|

Virtual Storage Console

a|

Das Symbol \* ALLE WIEDERENTDECKEN\*.

a|

Rechenzentrum

a|

Klicken Sie mit der rechten Maustaste auf das Datacenter und klicken Sie dann auf Menü:NetApp VSC[Update Host and Storage Data].

|===

. Klicken Sie im Dialogfeld \*Host- und Speicherdaten aktualisieren\* auf \*OK\*.

+

Je nach Anzahl der Hosts und Storage-Systeme in Ihrem Datacenter kann die Erkennung einige Minuten dauern. Dieser Erkennungsvorgang arbeitet im Hintergrund.

. Klicken Sie im Dialogfeld \*Erfolg\* auf \*OK\*.

```
:leveloffset: -1
```

```
[[ID21c6d040c377bcd729d084356f6154f]]
```

= Die rollenbasierte Zugriffssteuerung von vCenter Server in VSC für VMware vSphere

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

VCenter Server bietet rollenbasierte Zugriffssteuerung (RBAC), über die Sie den Zugriff auf vSphere Objekte kontrollieren können. In der Virtual Storage Console für VMware vSphere bestimmt die rollenbasierte Zugriffssteuerung von vCenter Server mit der ONTAP RBAC, welche VSC-Aufgaben ein bestimmter Benutzer auf Objekten auf einem bestimmten Storage-System ausführen kann.

Zum erfolgreichen Abschluss einer Aufgabe müssen Sie über die entsprechenden Berechtigungen für die rollenbasierte Zugriffssteuerung von vCenter Server verfügen. Während einer Aufgabe überprüft VSC die Berechtigungen eines Benutzers im vCenter Server, bevor sie die ONTAP-Berechtigungen des Benutzers überprüfen.

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

```
:leveloffset: +1
```

```
[[IDb2a1c1249f21b2d88389fe7d3541cd73]]
```

= Komponenten von vCenter Server-Berechtigungen

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]

Der vCenter Server erkennt Berechtigungen und keine Berechtigungen. Jede vCenter Server-Berechtigung besteht aus drei Komponenten.

Der vCenter Server verfügt über die folgenden Komponenten:

- \* Mindestens eine Berechtigung (die Rolle)

+

Die Berechtigungen definieren die Aufgaben, die ein Benutzer ausführen kann.

- \* VSphere Objekt

+

Das Objekt ist das Ziel für die Aufgaben.

- \* Ein Benutzer oder eine Gruppe

+

Der Benutzer oder die Gruppe definiert, wer die Aufgabe ausführen kann.

Wie das folgende Diagramm veranschaulicht, müssen Sie alle drei Elemente haben, um eine Berechtigung zu erhalten.

[NOTE]

====

In diesem Diagramm zeigen die grauen Felder Komponenten im vCenter Server an, und die weißen Felder geben die Komponenten an, die im Betriebssystem vorhanden sind, auf dem vCenter Server ausgeführt wird.

====

image:../media/permission-updated-graphic.png[Grafik mit Berechtigungen aktualisiert]

== Berechtigungen

Virtual Storage Console für VMware vSphere umfasst zwei Arten von Berechtigungen:

- \* Native vCenter Server-Berechtigungen

+

Diese Berechtigungen werden mit dem vCenter Server geliefert.

- \* VSC-spezifische Berechtigungen

+

Diese Berechtigungen werden für bestimmte VSC Aufgaben definiert. Sie sind nur bei VSC zu finden.

VSC-Aufgaben erfordern sowohl VSC-spezifische Berechtigungen als auch native vCenter Server-Berechtigungen. Diese Berechtigungen stellen die „Rolle“ für den Benutzer dar. Eine Berechtigung kann mehrere Berechtigungen haben. Diese Berechtigungen gelten für einen Benutzer, der beim vCenter Server angemeldet ist.

[NOTE]

====

Um die Arbeit mit der RBAC von vCenter Server zu vereinfachen, bietet VSC verschiedene Standardrollen mit allen VSC-spezifischen und nativen Berechtigungen, die zur Ausführung von VSC Aufgaben erforderlich sind.

====

Wenn Sie die Berechtigungen innerhalb einer Berechtigung ändern, sollte sich der Benutzer, der mit dieser Berechtigung verknüpft ist, ausloggen und sich dann anmelden, um die aktualisierte Berechtigung zu aktivieren.

[cols="1a,1a,1a"]

|===

| Berechtigung | Rollen | Aufgaben

a|

Menü:NetApp Virtual Storage Console[View]

a|

- \* VSC Administrator
- \* VSC Provisionierung
- \* VSC schreibgeschützt

a|

Für alle spezifischen Aufgaben von VSC und VASA Provider ist die View Berechtigung erforderlich.

a|

Menü:NetApp Virtual Storage Console[richtlinienbasiertes Management > Management] oder

Menü:privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label[Management]

a|

VSC Administrator

a|

VSC und VASA Provider Aufgaben bezüglich Storage-Funktionsprofilen und Schwellenwerteinstellungen.

|===

== VSphere Objekte

Berechtigungen werden mit vSphere Objekten verknüpft, z. B. vCenter Server, ESXi Hosts, Virtual Machines, Datastores, Datacenter, Und Ordner. Sie können jedem vSphere-Objekt Berechtigungen zuweisen. Auf Grundlage der Berechtigung, die einem vSphere-Objekt zugewiesen ist, bestimmt der vCenter Server, wer welche Aufgaben auf dem Objekt ausführen kann. Für VSC-spezifische Aufgaben werden Berechtigungen nur auf der Root-Ordnersebene (vCenter Server) und nicht auf einer anderen Einheit zugewiesen und validiert. Außer VAAI Plugin Betrieb, wo Berechtigungen gegen die betroffenen ESXi validiert werden.

== Benutzer und Gruppen

Sie können Active Directory (oder den lokalen vCenter Server-Rechner) verwenden, um Benutzer und Benutzergruppen einzurichten. Sie können dann mit vCenter Server-Berechtigungen den Zugriff auf diese Benutzer oder Gruppen gewähren, damit sie bestimmte VSC-Aufgaben durchführen können.

[NOTE]

====

Diese vCenter Server Berechtigungen gelten für Benutzer von VSC vCenter, nicht für VSC-Administratoren. Standardmäßig haben VSC-Administratoren vollständigen Zugriff auf das Produkt und benötigen keine ihnen zugewiesenen Berechtigungen.

====

Benutzern und Gruppen sind ihnen keine Rollen zugewiesen. Sie erhalten Zugriff auf eine Rolle, indem sie Teil einer vCenter Server-Berechtigung sind.

[[ID766ac9fed20120ab66da509b722c0820]]

= Kernpunkte zum Zuweisen und Ändern von Berechtigungen für vCenter Server  
:allow-uri-read:  
:icons: font  
:relative\_path: ./deploy/  
:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Bei der Arbeit mit vCenter Server-Berechtigungen gibt es einige wichtige Punkte, die Sie beachten sollten. Ob eine Aufgabe der virtuellen Speicherkonsole für VMware vSphere erfolgreich ist, hängt davon ab, wo Sie eine Berechtigung zugewiesen haben oder welche Aktionen ein Benutzer nach einer Änderung der Berechtigung ergriffen hat.

== Berechtigungen werden zugewiesen

Sie müssen nur vCenter Server-Berechtigungen einrichten, wenn Sie den Zugriff auf vSphere-Objekte und -Aufgaben einschränken möchten. Andernfalls können Sie sich als Administrator anmelden. Mit dieser Anmeldung können Sie automatisch auf alle vSphere Objekte zugreifen.

Wenn Sie eine Berechtigung zuweisen, legt die VSC Aufgaben fest, die ein Benutzer ausführen kann.

Um den Abschluss einer Aufgabe zu gewährleisten, müssen Sie die Berechtigung auf einer höheren Ebene zuweisen, z. B. dem Root-Objekt. Dies ist der Fall, wenn eine Aufgabe eine Berechtigung erfordert, die nicht auf ein bestimmtes vSphere-Objekt angewendet wird (z. B. Tracking the Task), oder wenn eine erforderliche Berechtigung auf ein nicht-vSphere-Objekt (z. B. ein Storage-System) angewendet wird.

In diesen Fällen können Sie eine Berechtigung so einrichten, dass sie von den untergeordneten Entitäten übernommen wird. Sie können den untergeordneten Entitäten auch andere Berechtigungen zuweisen. Die einer untergeordneten Entität zugewiesene Berechtigung überschreibt immer die Berechtigung, die von der übergeordneten Einheit übernommen wurde. Dies bedeutet, dass Sie Berechtigungen für eine untergeordnete Einheit als Möglichkeit zur Einschränkung des Geltungsbereichs einer Berechtigung, die einem Root-Objekt zugewiesen und von der untergeordneten Einheit vererbt wurde, haben können.

TIP: Sofern die Sicherheitsrichtlinien Ihres Unternehmens keine restriktiveren Berechtigungen erfordern, empfiehlt es sich, dem Root-Objekt (auch als Stammordner bezeichnet) Berechtigungen zuzuweisen.

== Berechtigungen und nicht vSphere Objekte

Die von Ihnen erstellte Berechtigung wird auf ein nicht-vSphere-Objekt angewendet. Beispielsweise ist ein Storage-System kein vSphere-Objekt. Wenn eine Berechtigung für ein Storage-System gilt, müssen Sie dem VSC-Root-Objekt die Berechtigung mit dieser Berechtigung zuweisen, da es kein vSphere Objekt gibt, dem Sie es zuweisen können.

Beispielsweise müssen alle Berechtigungen, die ein Privileg enthalten, z. B. die VSC-Berechtigung „Storage-Systeme hinzufügen/ändern/überspringen“, auf der Root-Objektebene zugewiesen werden.

## == Ändern von Berechtigungen

Sie können jederzeit eine Berechtigung ändern.

Wenn Sie die Berechtigungen innerhalb einer Berechtigung ändern, muss sich der mit dieser Berechtigung verknüpfte Benutzer abmelden und sich dann wieder anmelden, um die aktualisierte Berechtigung zu aktivieren.

```
[[ID36c66cf1a639297debfd231ffb40800a]]
= Standardrollen in Verbindung mit der virtuellen Appliance für VSC, VASA
Provider und SRA
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Zur Vereinfachung der Arbeit mit vCenter Server-Berechtigungen und rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) bietet (VSC) standardmäßige VSC-Rollen, mit denen Sie wichtige VSC-Aufgaben ausführen können. Es gibt auch eine schreibgeschützte Rolle, mit der Sie VSC Informationen anzeigen, aber keine Aufgaben ausführen können.

Die VSC Standardrollen verfügen sowohl über die erforderlichen VSC-spezifischen Berechtigungen als auch über die nativen vCenter Server-Berechtigungen, die für Benutzer zur Ausführung von VSC Aufgaben erforderlich sind. Darüber hinaus werden die Rollen so eingerichtet, dass sie über die erforderlichen Berechtigungen für alle unterstützten Versionen des vCenter Servers verfügen.

Als Administrator können Sie diese Rollen bei Bedarf Benutzern zuweisen.

[NOTE]

====

Wenn Sie die VSC auf die neueste Version aktualisieren, werden die Standardrollen automatisch aktualisiert, um sie mit der neuen Version von VSC zu verwenden.

====

Sie können sich die VSC Standardrollen anzeigen lassen, indem Sie auf der vSphere Client \*Home\* Seite auf \*Rollen\* klicken.

Die Rollen der VSC ermöglichen Ihnen, die folgenden Aufgaben auszuführen:

[cols="1a,1a"]

|==

| Rolle | Beschreibung

a|

VSC Administrator

a|

Bietet alle nativen vCenter Server-Berechtigungen und VSC-spezifische Berechtigungen, die zur Durchführung aller VSC-Aufgaben erforderlich sind.

a|

VSC schreibgeschützt

a|

Bietet schreibgeschützten Zugriff auf VSC

Diese Benutzer können keine VSC Aktionen ausführen, die durch den Zugriff gesteuert werden.

a|

VSC Provisionierung

a|

Bietet alle nativen vCenter Server-Berechtigungen und VSC-spezifische Berechtigungen, die für die Bereitstellung von Storage erforderlich sind.

Sie können die folgenden Aufgaben ausführen:

- \* Erstellen neuer Datenspeicher

- \* Datastores zerstören

- \* Zeigt Informationen zu Storage-Funktionsprofilen an



|===

:leveloffset: +1

[[IDdfd0aa3346a03f2dad6ee8e4cc971731]]

= Richtlinien zur Verwendung von VSC Standardrollen

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Wenn Sie mit standardmäßigen Virtual Storage Console für VMware vSphere Rollen arbeiten, gibt es bestimmte Richtlinien, die Sie befolgen sollten.

Sie sollten die Standardrollen nicht direkt ändern. Wenn Sie das tun, überschreiben die Änderungen bei jedem VSC-Upgrade die VSC. Das Installationsprogramm aktualisiert bei jedem VSC-Upgrade die Standardrollendefinitionen. So wird sichergestellt, dass die Rollen sowohl für Ihre VSC-Version als auch für alle unterstützten Versionen des vCenter Server aktuell sind.

Sie können jedoch die Standardrollen verwenden, um Rollen zu erstellen, die auf Ihre Umgebung zugeschnitten sind. Dazu sollten Sie die VSC Standardrolle kopieren und dann die kopierte Rolle bearbeiten. Durch das Erstellen einer neuen Rolle können Sie diese Rolle auch beibehalten, wenn Sie den VSC Windows Service neu starten oder aktualisieren.

Möglicherweise verwenden Sie die VSC Standardrollen wie folgt:

- \* Verwenden Sie die VSC Standardrollen für alle VSC Aufgaben.

+

In diesem Szenario bieten die Standardrollen alle Berechtigungen, die ein Benutzer zur Durchführung der VSC-Aufgaben benötigt.

- \* Kombinieren Sie Rollen, um die Aufgaben zu erweitern, die ein Benutzer ausführen kann.

+

Wenn die VSC Standardrollen zu viel Granularität für Ihre Umgebung bieten, können Sie ihre Rollen erweitern, indem Sie Gruppen auf höherer Ebene mit mehreren Rollen erstellen.

+

Wenn ein Benutzer andere Aufgaben ausführen muss, die keine VSC erfordern, die zusätzliche native Berechtigungen von vCenter Server erfordern, können Sie eine Rolle erstellen, die diese Berechtigungen bereitstellt und sie der Gruppe auch hinzufügen.

\* Erstellung feingranularer Rollen

+

Wenn in Ihrem Unternehmen bestimmte Rollen restriktiver implementiert werden müssen als die VSC Standardrollen, können Sie mit den VSC Rollen neue Rollen erstellen.

+

In diesem Fall würden Sie die nötigen VSC Rollen klonen und dann die geklonte Rolle bearbeiten, damit sie nur die Berechtigungen hat, die Ihr Benutzer benötigt.

:leveloffset: -1

[[IDf28f221c08cadcc87597f7c17c4187b2]]

= Für VSC Aufgaben erforderliche Berechtigungen

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Für verschiedene Aufgaben der Virtual Storage Console für VMware vSphere sind unterschiedliche Kombinationen von Berechtigungen erforderlich, die spezifisch für (VSC) und native vCenter Server-Berechtigungen gelten.

Informationen zu den für VSC Aufgaben erforderlichen Berechtigungen finden Sie im NetApp Knowledgebase Artikel 1032542.

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/How\\_to\\_configure\\_RBAC\\_for\\_Virtual\\_Storage\\_Console](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/How_to_configure_RBAC_for_Virtual_Storage_Console)["So konfigurieren Sie RBAC für die Virtual Storage Console"^]

```
:leveloffset: +1
```

```
[[ID1c55fa3ac80669ca3ba6084254371bb2]]
```

= Berechtigung auf Produktebene erforderlich von VSC für VMware vSphere

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Um auf die Virtual Storage Console für VMware vSphere GUI zuzugreifen, müssen Sie über die VSC-spezifische View Berechtigung auf Produktebene, die auf der richtigen vSphere Objektebene zugewiesen ist, verfügen. Wenn Sie sich ohne diese Berechtigung anmelden, zeigt die VSC eine Fehlermeldung an, wenn Sie auf das NetApp Symbol klicken und verhindert, dass Sie auf die VSC zugreifen.

In den folgenden Informationen wird die VSC Berechtigung auf Produktebene View beschrieben:

```
[cols="1a,1a,1a"]
```

```
|===
```

```
| Berechtigung | Beschreibung | Zuweisungsebene
```

```
a|
```

Anzeigen

```
a|
```

Sie können auf die VSC GUI zugreifen. Diese Berechtigung ermöglicht Ihnen nicht, Aufgaben in der VSC auszuführen. Zum Ausführen von VSC Aufgaben müssen Sie über die richtigen VSC-spezifischen und nativen vCenter Server-Berechtigungen für diese Aufgaben verfügen.

```
a|
```

Die Zuweisungsebene legt fest, welche Teile der Benutzeroberfläche angezeigt werden können.

Durch das Zuweisen der View-Berechtigung im Root-Objekt (Ordner) können Sie VSC durch Klicken auf das NetApp Symbol eingeben.

Sie können die View-Berechtigung einer anderen vSphere Objektebene zuweisen. Dabei ist jedoch die VSC-Menüs, die Sie anzeigen und verwenden können, beschränkt.

Das Root-Objekt ist der empfohlene Ort, um alle Berechtigungen zuzuweisen, die die View-Berechtigung enthalten.

|===

```
[[IDeda69cfc93583bc4be6bf7767de3a998]]
```

= Rollenbasierte Zugriffssteuerung von ONTAP für die virtuelle Appliance für VSC, VASA Provider und SRA

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von ONTAP können Sie den Zugriff auf bestimmte Storage-Systeme steuern und die Aktionen steuern, die ein Benutzer auf diesen Storage-Systemen durchführen kann. In der Virtual Storage Console für VMware vSphere arbeitet die ONTAP RBAC mit der rollenbasierten Zugriffssteuerung von vCenter Server zusammen, um festzulegen, welche Aufgaben der Virtual Storage Console (VSC) ein bestimmter Benutzer auf den Objekten auf einem bestimmten Storage-System ausführen kann.

VSC verwendet die in VSC festgelegten Anmeldedaten (Benutzername und Passwort) zur Authentifizierung jedes Storage-Systems und zur Bestimmung der Storage-Vorgänge auf diesem Storage-System. VSC verwendet einen Satz Credentials für jedes Storage-System. Mit diesen Anmeldedaten wird festgelegt, welche VSC Aufgaben auf dem Storage-System ausgeführt werden können. Das heißt, die Anmeldedaten gelten für die VSC, nicht für einen individuellen VSC Benutzer.

ONTAP RBAC gilt nur für den Zugriff auf Storage-Systeme und die Durchführung von VSC-Aufgaben, die mit dem Storage zusammenhängen, beispielsweise für die Bereitstellung von Virtual Machines. Wenn Sie nicht über die entsprechenden ONTAP RBAC-Berechtigungen für ein bestimmtes Storage-System verfügen, können Sie auf einem vSphere Objekt, das auf diesem Storage-System gehostet wird, keine Aufgaben ausführen. Sie können die ONTAP RBAC zusammen mit den VSC-spezifischen Berechtigungen verwenden, um zu steuern, welche VSC Aufgaben ein Benutzer ausführen kann:

- \* Überwachung und Konfiguration von Storage- oder vCenter Server-Objekten in einem Storage-System
- \* Bereitstellung von vSphere Objekten in einem Storage-System

Durch den Einsatz der ONTAP RBAC mit den VSC-spezifischen Berechtigungen

wird eine Storage-orientierte Sicherheitsebene bereitgestellt, die der Storage-Administrator managen kann. Somit verfügen Sie über eine feingranulare Zugriffssteuerung als nur die ONTAP RBAC oder die alleine vCenter Server RBAC unterstützt. Mit der RBAC für vCenter Server können Sie beispielsweise vCenterUserB die Bereitstellung eines Datenspeichers im Storage zulassen und gleichzeitig vCenterUserA daran hindern, Datenspeicher bereitzustellen. Wenn die Anmeldeinformationen des Speichersystems für ein bestimmtes Speichersystem die Erstellung von Speicher nicht unterstützen, können weder vCenterUserB noch vCenterUserA einen Datenspeicher auf diesem Speichersystem bereitstellen.

Beim Starten einer VSC Aufgabe überprüft die VSC zunächst, ob Sie über die richtige vCenter Server-Berechtigung für diese Aufgabe verfügen. Wenn die Berechtigung des vCenter Servers nicht ausreicht, um eine Aufgabe ausführen zu können, muss die VSC die ONTAP-Berechtigungen für dieses Speichersystem nicht überprüfen, da Sie die erste Sicherheitsüberprüfung des vCenter Servers nicht bestanden haben. So kann nicht auf das Storage-System zugegriffen werden.

Falls die Berechtigung zum vCenter Server ausreichend ist, prüft VSC die ONTAP RBAC-Berechtigungen (Ihre ONTAP Rolle), die mit den Anmeldedaten des Storage-Systems verknüpft sind (Benutzername und Passwort). Um zu ermitteln, ob Sie über ausreichende Berechtigungen zur Durchführung der Storage-Operationen verfügen, die von dieser VSC Aufgabe auf diesem Storage-System benötigt werden. Wenn Sie die richtigen ONTAP-Rechte haben, können Sie auf das Storage-System zugreifen und die VSC-Aufgabe ausführen. Die ONTAP-Rollen bestimmen die VSC-Aufgaben, die Sie auf dem Storage-System durchführen können.

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 welche Aufgaben auf feingranularen vCenter Server-Objektebene und auf Ebene des Storage-Systems ausführen können.

- \* Audit-Informationen

+

In vielen Fällen bietet VSC ein Audit-Trail im Storage-System, anhand dessen Sie Ereignisse zurück an den vCenter Server Benutzer verfolgen können, der die Storage-Änderungen durchgeführt hat.

\* Benutzerfreundlichkeit

+

Sie können alle Controller-Anmeldedaten an einer Stelle beibehalten.

```
[[ID962554b0f28a5cc424ca2da3f9546cd3]]
```

= Empfohlene ONTAP Rollen bei der Verwendung von VSC für VMware vSphere

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

```
[role="lead"]
```

Sie können mehrere empfohlene ONTAP-Rollen für die Arbeit mit der Virtual Storage Console für VMware vSphere und der rollenbasierten Zugriffssteuerung einrichten. Diese Rollen enthalten die ONTAP-Berechtigungen, die erforderlich sind, um die erforderlichen Storage-Vorgänge auszuführen, die von den VSC-Aufgaben ausgeführt werden.

Um neue Benutzerrollen zu erstellen, müssen Sie sich als Administrator auf Storage-Systemen, auf denen ONTAP ausgeführt wird, einloggen. Sie können ONTAP Rollen mit einer der folgenden Elemente erstellen:

\* 9.7 oder höher

+

xref:{relative\_path}task-configure-user-role-and-privileges.html["Konfigurieren von Benutzerrollen und -Berechtigungen"]

\* RBAC Benutzer Creator für ONTAP Tool (bei Verwendung von ONTAP 9.6 oder früher)

+

<https://community.netapp.com/t5/Virtualization-Articles-and-Resources/RBAC-User-Creator-tool-for-VSC-VASA-Provider-and-Storage-Replication-Adapter-7-0/ta-p/133203>["RBAC Benutzer Creator Tool für VSC, VASA Provider und Storage Replication Adapter 7.0 für VMware vSphere"]

Jeder ONTAP-Rolle ist ein zugehöriger Benutzername und ein Passwort zugeordnet, was die Anmeldeinformationen der Rolle darstellt. Wenn Sie sich nicht mit diesen Anmeldedaten anmelden, können Sie nicht auf die Speichervorgänge zugreifen, die der Rolle zugeordnet sind.

Die VSC-spezifischen ONTAP-Rollen werden in hierarchischen Anordnung angeordnet. Das bedeutet, dass die erste Rolle die restriktivsten Rollen ist und nur die Berechtigungen besitzt, die mit dem Basissatz von VSC-Storage-Vorgängen verknüpft sind. Die nächste Rolle umfasst sowohl eigene Berechtigungen als auch alle Berechtigungen, die mit der vorherigen Rolle verknüpft sind. Jede zusätzliche Rolle ist hinsichtlich des unterstützten Storage-Betriebs weniger restriktiv.

Nachstehend finden Sie einige der empfohlenen ONTAP RBAC-Rollen beim Einsatz von VSC. Nachdem Sie diese Rollen erstellt haben, können Sie sie Benutzern zuweisen, die Storage-Aufgaben ausführen müssen, z. B. Virtual Machines bereitstellen.

. Ermitteln

+

Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.

. Speicher Erstellen

+

Mit dieser Rolle können Sie Speicher erstellen. Diese Rolle umfasst außerdem alle Berechtigungen, die mit der Ermittlungsrolle verknüpft sind.

. Speicher Ändern

+

Mit dieser Rolle können Sie Speicher ändern. Diese Rolle umfasst außerdem alle Berechtigungen, die der Bestandsernahmerrolle und der Rolle „Speicher erstellen“ zugeordnet sind.

. Speicher Zerstören

+

Mit dieser Rolle können Sie Speicher zerstören. Diese Rolle umfasst außerdem alle Berechtigungen, die der Bestandsernahmerrolle, der Rolle „Speicher erstellen“ und der Rolle „Speicher ändern“ zugeordnet sind.

Wenn Sie VASA Provider für ONTAP nutzen, sollten Sie auch eine richtlinienbasierte Managementrolle (PBM, richtlinienbasiertes Management) einrichten. Diese Rolle ermöglicht Ihnen das Storage-Management mithilfe von Storage-Richtlinien. Diese Rolle erfordert, dass Sie auch die Rolle ``Diskovery`` einrichten.

[[ID39b9fb495cbc48452f2c0e8075e04f48]]

= So konfigurieren Sie die rollenbasierte Zugriffssteuerung für ONTAP für VMware vSphere

```
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie müssen die rollenbasierte Zugriffssteuerung (RBAC) der ONTAP auf dem Storage-System konfigurieren, wenn Sie die rollenbasierte Zugriffssteuerung über die Virtual Storage Console für VMware vSphere (VSC) nutzen möchten. Über die ONTAP Funktion zur rollenbasierten Zugriffssteuerung können Sie ein oder mehrere benutzerdefinierte Benutzerkonten mit begrenzten Zugriffsberechtigungen erstellen.

VSC und SRA können auf Storage-Systeme entweder auf Cluster-Ebene oder auf Cluster-Ebene zugreifen. Wenn Sie Storage-Systeme auf Cluster-Ebene hinzufügen, müssen Sie die Anmeldedaten des Admin-Benutzers angeben, um alle erforderlichen Funktionen bereitzustellen. Wenn Sie Storage-Systeme durch direkte Hinzufügung von Details hinzufügen, müssen Sie beachten, dass der Benutzer „`vsadmin`“ nicht über alle erforderlichen Rollen und Funktionen zum Ausführen bestimmter Aufgaben verfügt.

VASA Provider kann nur auf Cluster-Ebene auf Storage-Systeme zugreifen. Wenn VASA Provider für einen bestimmten Storage Controller benötigt wird, muss das Storage-System der VSC auf Cluster-Ebene hinzugefügt werden, selbst wenn Sie VSC oder SRA verwenden.

Um einen neuen Benutzer zu erstellen und ein Cluster oder eine Verbindung zu VSC, VASA Provider und SRA herzustellen, sollten Sie Folgendes durchführen:

\* Erstellen eines Cluster-Administrators oder einer Administratorrolle  
+

[NOTE]

====

Sie können eine der folgenden Funktionen verwenden, um diese Rollen zu erstellen:

\*\* ONTAP System Manager 9.7 oder höher

```
xref:{relative_path}task-configure-user-role-and-
privileges.html["Konfigurieren von Benutzerrollen und -Berechtigungen"]
```

\*\* RBAC Benutzer Creator für ONTAP Tool (bei Verwendung von ONTAP 9.6 oder früher)



link:<https://community.netapp.com/t5/Virtualization-Articles-and-Resources/RBAC-User-Creator-tool-for-VSC-VASA-Provider-and-Storage-Replication-Adapter-7-0/ta-p/133203/t5/Virtualization-Articles-and-Resources/How-to-use-the-RBAC-User-Creator-for-Data-ONTAP/ta-p/86601>["RBAC Benutzer Creator Tool für VSC, VASA Provider und Storage Replication Adapter 7.0 für VMware vSphere"^]

====

\* Erstellen Sie Benutzer mit der zugewiesenen Rolle und dem entsprechenden Anwendungssatz mithilfe von ONTAP

+

Sie benötigen diese Storage-System-Anmeldedaten, um die Storage-Systeme für VSC zu konfigurieren. Sie können Storage-Systeme für VSC konfigurieren, indem Sie die Anmeldedaten in der VSC eingeben. Jedes Mal, wenn Sie sich mit diesen Anmeldedaten in einem Storage-System anmelden, erhalten Sie Berechtigungen für die VSC Funktionen, die Sie bei der Erstellung der Anmeldedaten in ONTAP eingerichtet hatten.

\* Fügen Sie das Storage-System zur VSC hinzu und stellen Sie die Zugangsdaten des gerade erstellten Benutzers bereit

== VSC Rollen

Die VSC klassifiziert die ONTAP Berechtigungen in folgende VSC-Rollen:

\* Ermitteln

+

Ermöglicht die Erkennung aller verbundenen Storage Controller

\* Speicher Erstellen

+

Ermöglicht die Erstellung von Volumes und LUNs (Logical Unit Number)

\* Speicher Ändern

+

Ermöglicht die Anpassung und Deduplizierung von Storage-Systemen

\* Speicher Zerstören

+

Aktiviert die Zerstörung von Volumes und LUNs

## == VASA Provider-Rollen

Sie können nur richtlinienbasiertes Management auf Cluster-Ebene erstellen. Diese Rolle ermöglicht ein richtlinienbasiertes Storage Management mithilfe von Storage-funktionsprofilen.

## == SRA-Rollen

SRA klassifiziert die ONTAP-Berechtigungen als SAN- oder NAS-Rolle auf Cluster-Ebene oder auf der Ebene. So können Benutzer SRM-Vorgänge ausführen.

[NOTE]

====

Wenn Sie Rollen und Berechtigungen mithilfe von ONTAP-Befehlen manuell konfigurieren möchten, müssen Sie sich in den Knowledge Base-Artikeln informieren.

====

\*

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/VSC%2C\\_VASA%2C\\_and\\_SRA\\_7.0\\_ONTAP\\_RBAC\\_Configuration\\_Version\\_1](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/VSC%2C_VASA%2C_and_SRA_7.0_ONTAP_RBAC_Configuration_Version_1)["VSC, VASA und SRA 7.0 ONTAP RBAC-Konfiguration"^]

\*

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/Roll\\_up\\_of\\_all\\_commands\\_for\\_VSC\\_and\\_SRA\\_for\\_SVM\\_level](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/Roll_up_of_all_commands_for_VSC_and_SRA_for_SVM_level)["Führen Sie alle Befehle auf VSC- und SRA-Ebene auf SVM-Ebene durch"^]

VSC führt eine erste Berechtigungsvalidierung der ONTAP RBAC-Rollen durch, wenn Sie das Cluster der VSC hinzufügen. Wenn Sie eine direkte Storage-IP hinzugefügt haben, führt VSC die erste Validierung nicht durch. VSC überprüft und erzwingt die Berechtigungen später im Task-Workflow.

```
[[ID25d1d3a94a03e1a4f5d865af28cede2c]]
```

```
= Konfigurieren von Benutzerrollen und -Berechtigungen
```

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Neue Benutzerrollen zum Management von Storage-Systemen können mit der JSON-Datei konfiguriert werden, die mit der virtuellen Appliance für VSC, VASA Provider, SRA und ONTAP System Manager bereitgestellt wird.

.Bevor Sie beginnen

- \* Sie sollten die Datei ONTAP-Berechtigungen mithilfe von von von von der virtuellen Appliance für VSC, VASA Provider und SRA heruntergeladen haben  
`+https://{virtual\_appliance\_IP}:9083/vsc/config/VSC\_ONTAP\_User\_Privileges.zip+`.
- \* Sie sollten ONTAP 9.7 System Manager konfiguriert haben.
- \* Sie sollten sich mit Administratorrechten für das Speichersystem angemeldet haben.

.Schritte

- . Entpacken Sie die heruntergeladene Datei  
`+https://{virtual\_appliance\_IP}:9083/vsc/config/VSC\_ONTAP\_User\_Privileges.zip+` Datei:
- . Greifen Sie auf ONTAP System Manager zu.
- . Klicken Sie auf Menü:CLUSTER[Einstellungen > Benutzer und Rollen].
- . Klicken Sie Auf \*Benutzer Hinzufügen\*.
- . Wählen Sie im Dialogfeld \* Benutzer hinzufügen\* die Option \*Virtualisierungsprodukte\* aus.
- . Klicken Sie auf \*Durchsuchen\*, um die JSON-Datei der ONTAP-Berechtigungen auszuwählen und hochzuladen.
- +
- DAS PRODUKTFELD wird automatisch ausgefüllt.

- . Wählen Sie die gewünschte Funktion aus dem Dropdown-Menü \* PRODUCT CAPABILITY\* aus.

+

Das Feld \* ROLLE\* wird automatisch ausgefüllt, basierend auf der ausgewählten Produktfunktion.

- . Geben Sie den erforderlichen Benutzernamen und das erforderliche Passwort ein.
- . Wählen Sie die für den Benutzer erforderlichen Berechtigungen (Discovery, Create Storage, Modify Storage, Destroy Storage) aus, und klicken Sie dann auf \*Add\*.

## .Ergebnisse

Die neue Rolle und der neue Benutzer werden hinzugefügt, und Sie können die detaillierten Berechtigungen unter der von Ihnen konfigurierten Rolle sehen.

```
:leveloffset: -1
```

```
:leveloffset: -1
```

```
[[ID80cf33fc587b498b71e8b4ab4b0c1e53]]
= Storage Replication Adapter für Disaster Recovery konfigurieren
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Wenn Sie Ihren vCenter Server für die Disaster Recovery konfigurieren möchten, müssen Sie den Storage Replication Adapter (SRA) aktivieren, nachdem Sie die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) implementiert haben. Nach der Implementierung der virtuellen Appliance wird VSC standardmäßig installiert. Nach der Implementierung der virtuellen Appliance muss SRA für den vCenter Server aktiviert werden.

\*Verwandte Informationen\*

```
xref:{relative_path}task-enable-storage-replication-
adapter.adoc[Aktivieren Sie Storage Replication Adapter]
```

```
:leveloffset: +1
```

```
[[IDb529a7bdc19b2a0e6ee281c90afd5960]]
= Konfigurieren Sie Storage Replication Adapter für die SAN-Umgebung
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie müssen die Storage-Systeme einrichten, bevor Sie Storage Replication Adapter (SRA) für Site Recovery Manager (SRM) ausführen.

.Bevor Sie beginnen

Sie müssen die folgenden Programme auf dem geschützten Standort und dem Wiederherstellungsstandort installiert haben:

\* SRM

+

Dokumentation zur Installation von SRM befindet sich auf der VMware Site.

+

[https://www.vmware.com/support/pubs/srm\\_pubs.html](https://www.vmware.com/support/pubs/srm_pubs.html)["VMware Site Recovery Manager - Dokumentation"^]

\* SRA

+

Der Adapter wird entweder auf SRM installiert.

.Schritte

. Vergewissern Sie sich, dass die primären ESXi-Hosts mit den LUNs im primären Speichersystem am geschützten Standort verbunden sind.

. Vergewissern Sie sich, dass die LUNS in Initiatorgruppen vorhanden sind, die über die verfügen ``*ostype*`` Option auf dem primären Storage-System auf `_vmware_` eingestellt.

. Überprüfen Sie, ob die ESXi-Hosts am Recovery-Standort über eine entsprechende FC- oder iSCSI-Konnektivität zum verfügen.

+

Sie können dies entweder tun, indem Sie überprüfen, ob die ESXi Hosts über lokale LUNs auf dem verbunden sind, oder verwenden Sie die ``fc show initiators`` Befehl oder das ``iscsi show initiators`` Befehl auf dem .

```
[[ID1fc961a60dd564cdfaef6c0f36d2bb63]]
```

= Konfigurieren Sie Storage Replication Adapter für NAS-Umgebungen

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

```
[role="lead"]
```

Sie müssen die Storage-Systeme konfigurieren, bevor Sie Storage Replication Adapter (SRA) für VMware vCenter Site Recovery Manager (SRM) ausführen.

.Bevor Sie beginnen

Sie müssen die folgenden Programme auf dem geschützten Standort und dem Wiederherstellungsstandort installiert haben:

\* SRM

+

Dokumentation zur Installation von SRM finden Sie auf der VMware-Website.

+

[https://www.vmware.com/support/pubs/srm\\_pubs.html](https://www.vmware.com/support/pubs/srm_pubs.html)["VMware Site Recovery Manager - Dokumentation"^]

\* SRA

+

Der Adapter wird auf SRM und dem SRA Server installiert.

.Schritte

. Überprüfen Sie, ob die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die bei vCenter Server registriert sind.

. Überprüfen Sie, ob die ESXi-Hosts auf der geschützten Seite die NFS-Exporte-Volumes von der montiert haben.

. Überprüfen Sie, ob gültige Adressen wie die IP-Adresse, der Hostname oder der FQDN, auf denen die NFS-Exporte vorhanden sind, im Feld \*NFS-Adressen\* angegeben sind, wenn Sie den Assistenten \*Array Manager\* zum Hinzufügen von Arrays zu SRM verwenden.

. Verwenden Sie die `ping` Befehl auf jedem ESXi-Host am Recovery-Standort um zu überprüfen, ob der Host einen VMkernel-Port hat, der auf die IP-Adressen zugreifen kann, die für NFS-Exporte von verwendet werden.

<https://mysupport.netapp.com/site/>["NetApp Support"^]

```
[[ID553859aadd112fb7084a74c266e8d0f3]]
```

= Konfiguration des Storage Replication Adapter für Umgebungen mit hohem Skalierbarkeit

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Um in stark skalierten Umgebungen optimal arbeiten zu können, müssen Sie die Storage-Timeout-Intervalle gemäß den empfohlenen Einstellungen für Storage Replication Adapter (SRA) konfigurieren.

#### == Einstellungen für Speicheranbieter

- \* Sie müssen den Wert des erhöhen `StorageProvider.resignatureTimeout` Einstellung von 900 Sekunden auf 12000 Sekunden.
- \* Sie müssen die aktivieren `StorageProvider.autoResignatureMode` Option.

Weitere Informationen zum Ändern der Speicheranbieter-Einstellungen finden Sie in der VMware-Dokumentation.

<https://docs.vmware.com/en/Site-Recovery-Manager/6.5/com.vmware.srm.admin.doc/GUID-E4060824-E3C2-4869-BC39-76E88E2FF9A0.html>["Dokumentation zu VMware vSphere: Ändern der Storage Provider-Einstellungen"^]

#### == Speichereinstellungen

Sie müssen den Wert des festlegen `storage.commandTimeout` Timeout-Intervall für Umgebungen mit hoher Skalierbarkeit auf 12,000 Sekunden

[NOTE]

====

Das angegebene Zeitüberschreitungsintervall ist der Höchstwert. Sie müssen nicht warten, bis die maximale Zeitüberschreitung erreicht ist. Die meisten Befehle sind innerhalb des festgelegten maximalen Timeout-Intervalls abgeschlossen.

====

[https://kb.netapp.com/app/answers/answer\\_view/a\\_id/1001111](https://kb.netapp.com/app/answers/answer_view/a_id/1001111)["Antwort auf die NetApp Knowledgebase 1001111: NetApp Storage Replication Adapter 4.0/7.X für den ONTAP Sizing Guide"^]

Die VMware Dokumentation zum Ändern der SAN-Provider-Einstellungen enthält weitere Informationen.

<https://docs.vmware.com/en/Site-Recovery-Manager/6.5/com.vmware.srm.admin.doc/GUID-711FD223-50DB-414C-A2A7-3BEB8FAFDBD9.html>["Dokumentation Zum Vmware Site Recovery Manager: Storage-Einstellungen Ändern"^]

:leveloffset: -1

[[ID3783aae7e5e8a402ab5c314e26c24046]]

= Fehlerbehebung mit der virtuellen Appliance für VSC, VASA Provider und SRA

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Falls bei der Installation oder Konfiguration der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) unerwarteter Verhalten aufkommt, können Sie die Ursachen solcher Probleme anhand spezifischer Fehlerbehebungsmaßnahmen identifizieren und beheben.

:leveloffset: +1

[[ID6980b1cc22089459efe6d5d44a04f1bc]]

= Reinigen Sie die heruntergeladenen Plug-in-Pakete von vSphere im Cache

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Wenn Plug-ins nach der Bereitstellung oder dem Upgrade der virtuellen Appliance für VSC, VASA Provider und SRA nicht automatisch aktualisiert werden, sollten Sie die im Cache gespeicherten Download-Plug-in-Pakete im Browser und auf dem vCenter Server bereinigen, um Probleme mit dem vCenter Server Plug-in zu lösen.



```
.Schritte
. Abmelden von Ihrem vorhandenen vSphere-Webclient oder vSphere-Client.
. Entfernen Sie den Browser-Cache.
. Entfernen Sie die im Cache gespeicherten Plug-in-Pakete von vSphere
Client.
+
[cols="1a,1a"]
|===
| Sie verwenden... | Führen Sie folgende Schritte durch...

a|
Windows vCenter Server
a|
Entfernen Sie die folgenden Ordner com.netapp.vasa.vvol.webclient-
x.x.x.xxxx, com.netapp.nvpf.webclient-x.x.x.xxxx und com.netapp.vsch5-
x.x.x.xxxx unter:

** VSphere Web Client-Pfad:
C:\ProgramData\VMware\vCenterServer\cfg\vsphere-Client\vc-Pakete\vsphere-
Client-Serenity
** VSphere Client(HTML5)-Pfad:
C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-Pakete\vsphere-
Client-Serenity

a|
VCSA
a|
.. SSH in die VCSA Appliance einbinden.
.. Ändern Sie Verzeichnisse in das vCenter Web-Client-UI-Verzeichnis
Erweiterungen mit `cd /etc/vmware/vsphere-client/vc-packages/vsphere-
client-serenity`
.. Entfernen Sie die zwischengespeicherten Plugin-Pakete mithilfe der
folgenden Befehle:
+
*** `rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx`
*** `rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx`
*** `rm -rf com.netapp.vsch5-x.x.x.xxxx`

.. Ändern Sie Verzeichnisse in das vCenter-Client(HTML5)-UI-Extensions-
Verzeichnis mit `cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-
serenity`
```

.. Entfernen Sie die zwischengespeicherten Plugin-Pakete mithilfe der folgenden Befehle:

+

```
*** `rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx`  
*** `rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx`  
*** `rm -rf com.netapp.vsch5-x.x.x.xxxx`
```

|===

. Melden Sie sich bei vSphere an und starten Sie vSphere Web Client und vSphere Client Services mit den folgenden Befehlen neu:

+

```
** `service-control --stop vsphere-client vsphere-ui`  
** `service-control --start vsphere-client vsphere-ui`
```

```
[[IDdebadd0aae8cc5da94f769b8e02a6cf9]]
```

= Durch die Deinstallation werden keine Standard-VSC-Rollen entfernt

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

Bei der Deinstallation der Virtual Storage Console für VMware vSphere (VSC) bleiben die VSC Standardrollen erhalten. Das erwartete Verhalten und es wirkt sich nicht auf die Performance der VSC aus oder auf die Fähigkeit zum Upgrade auf eine neue Version von VSC. Sie können diese Rollen bei Bedarf manuell löschen.

Während durch die Deinstallation die VSC-Rollen nicht entfernt werden, werden bei der Deinstallation die lokalisierten Namen für die VSC-spezifischen Berechtigungen entfernt und ihr folgendes Präfix angehängt: „`XXX fehlende Berechtigung`“. Wenn Sie zum Beispiel das Dialogfeld vSphere \*Rolle bearbeiten\* nach der Installation von VSC öffnen, werden die VSC-spezifischen Berechtigungen als aufgeführt angezeigt.

Dieses Verhalten geschieht, weil vCenter Server keine Option zum Entfernen von Berechtigungen bietet.

Wenn Sie VSC neu installieren oder ein Upgrade auf eine neuere Version von VSC durchführen, werden alle standardmäßigen VSC-Rollen und VSC-spezifischen Berechtigungen wiederhergestellt.

```
[[IDfac8f5b324211359ffc73e2611061ade]]  
= Protokolldateien von Virtual Storage Console und VASA Provider  
:allow-uri-read:  
:icons: font  
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]  
Sie können die Protokolldateien im überprüfen `/opt/netapp/vscserver/log`` Verzeichnis und das `/opt/netapp/vpserver/log`` Verzeichnis, wenn Fehler auftreten.

Die folgenden drei Log-Dateien können bei der Identifizierung von Problemen hilfreich sein:

- \* ``cxf.log``, Mit Informationen über API-Verkehr in und aus VASA Provider
- \* ``kaminoPrefs.xml``, Mit Informationen über VSC-Einstellungen
- \* ``vvolvp.log``, Mit allen Protokollinformationen über VASA Provider

Im Wartungsmenü der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) können Sie verschiedene Protokollebenen Ihren Anforderungen anpassen. Folgende Protokollebenen sind verfügbar:

- \* Info
- \* Debuggen
- \* Fehler
- \* Verfolgen

Wenn Sie die Protokollebenen festlegen, werden die folgenden Dateien aktualisiert:

- \* VSC-Server: ``kamino.log`` Und ``vvolvp.log``
- \* VASA Provider-Server: ``vvolvp.log``, ``error.log``, und ``netapp.log``

Darüber hinaus enthält die Seite über die Webbefehlszeilenschnittstelle (CLI) von VASA Provider die vorgemachten API-Aufrufe, die zurückgegebenen

Fehler sowie mehrere Performance-bezogene Zähler. Die Web-CLI-Seite finden Sie unter `\_https\_://<IP\_address\_or\_hostname>:9083/stats`.

```
[[ID9862fc3cb24b1d8559bfff4eba7bbd6a5]]
```

= Die VSC- und VASA Provider-Services werden in hoch skalierten Umgebungen neu gestartet

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

== Problem

Die virtuelle Appliance für VSC, VASA Provider und SRA führt möglicherweise nicht optimal in einer hochgradig skalierten Umgebung aus und kann zu Problemen wie VSC und VASA Provider Services führen, die häufig neu gestartet werden.

== Korrekturmaßnahme

Ändern Sie die RAM- und Heap-Speicheranforderungen der virtuellen Appliance für VSC, VASA Provider und SRA.

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/tune\\_memory\\_settings\\_of\\_VM\\_VSC%2C\\_VASA\\_Provider%2C\\_and\\_SRA\\_for\\_scale\\_and\\_performance\[\]](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance[])

```
[[ID1a394ef7239b03645d9581ab82a0dcc8]]
```

= Konfigurieren Sie VASA Provider für die Nutzung mit SSH

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie können VASA Provider zur Verwendung von SSH für sicheren Zugriff einrichten, indem Sie die virtuelle Appliance für Virtual Storage Console

(VSC), VASA Provider und Storage Replication Adapter (SRA) konfigurieren.

.Über diese Aufgabe

Wenn Sie SSH konfigurieren, müssen Sie sich als Benutzer für die Wartung einloggen. Der Grund dafür ist, dass der Root-Zugriff auf VASA Provider deaktiviert wurde. Wenn Sie andere Anmeldedaten verwenden, können Sie SSH nicht für den Zugriff auf VASA Provider verwenden.

.Schritte

. Öffnen Sie über den vCenter Server eine Konsole für die virtuelle Appliance für VSC, VASA Provider und SRA.

. Melden Sie sich als Wartungbenutzer an.

. Eingabe `3` So wählen Sie \*Systemkonfiguration\* aus.

. Eingabe `6` Wählen Sie \*SSH-Zugriff aktivieren\* aus.

. Eingabe `y` Im Bestätigungsdialogfeld.

```
[[ID42d6d2f1951d4b7c7353dbd948509f15]]
```

= Konfigurieren Sie die virtuelle Appliance für VSC, VASA Provider und SRA für den Remote-Diagnoszugriff über SSH

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Sie können die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) konfigurieren, um den SSH-Zugriff für den Diagnose-Benutzer zu aktivieren.

.Bevor Sie beginnen

Die VASA Provider-Erweiterung muss für Ihre vCenter Server-Instanz aktiviert sein.

.Über diese Aufgabe

Die Verwendung von SSH für den Zugriff auf den Diagnosebenutzer weist folgende Einschränkungen auf:

- \* Sie sind nur eine Anmeldung pro Aktivierung von SSH erlaubt.

- \* SSH-Zugriff auf den Diagnose-Benutzer ist deaktiviert, wenn eine der folgenden Ereignisse eintritt:

- +

- \*\* Die Zeit läuft ab.

- +

Die Anmeldesitzung bleibt nur bis Mitternacht am nächsten Tag gültig.

\*\* Sie melden sich erneut als Diagnose-Benutzer mit SSH an.

#### .Schritte

- . Öffnen Sie über den vCenter Server eine Konsole für VASA Provider.
- . Melden Sie sich als maint-Benutzer an.
- . Eingabe `4` So wählen Sie \*Support und Diagnose\* aus.
- . Eingabe `3` So wählen Sie \*Remote-Diagnosezugriff aktivieren\* aus.
- . Eingabe `y` Im Dialogfeld \*Bestätigung\* können Sie den Remote-Diagnosezugriff aktivieren.
- . Geben Sie ein Kennwort für den Remote-Diagnosezugriff ein.

```
[[IDb57447f5d76a27282357b5d18e26c771]]
= Die SRA-Installation schlägt mit einem Skriptfehler fehl
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

#### == Problem

Die Installation von Storage Replication Adapter (SRA) unter Windows 2008 R2 schlägt mit einem ungültigen Anmeldefehler fehl.

#### == Ursache

Dieser Fehler kann auftreten, wenn verschiedene Versionen von Transport Layer Security (TLS) auf der virtuellen Appliance für VSC, VASA Provider, SRA und Windows 2008 R2 aktiviert werden.

#### == Korrekturmaßnahme

Wenn Sie versuchen, SRA auf Windows 2008 R2 zu installieren, müssen Sie

TLSv1.0 für die virtuelle Appliance für VSC, VASA Provider und SRA aktivieren. Dabei müssen Sie die folgenden Schritte in der Wartungskonsole verwenden:

- . Melden Sie sich mithilfe der Benutzeranmeldeinformationen von „`maint`“ an der Wartungskonsole an.
- . Wählen Sie im Hauptmenü \*1\* für das Menü \*Anwendungskonfiguration\*.
- . Geben Sie im Menü \* Anwendungskonfiguration\* \* \* \* \* 13\* ein, um im Menü \*Anwendungskonfiguration\* \*TLS-Protokoll aktivieren\* auszuwählen.
- . Wählen Sie in der TLS-Protokoll-Liste \*TLSv1\* aus.

+

Die VSC- und VASA Provider-Services werden neu gestartet und TLSv1.0 ist aktiviert.

Sie können auch TLSv1.2 unter Windows 2008 R2 aktivieren.

```
[[ID4004f5f1d32333cea0418905c13ebaca]]
= SRA scheitert in einer stark skalierten Umgebung an der optimalen
Performance
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

== Problem

SRA führt in einer stark skalierten Umgebung nicht optimal aus (wenn VMware Maximalwerte wie 250 PGS, 250 RPS, 5000 VMs ausgeführt hat) und kann zu Problemen wie Timeout-Fehlern oder ONTAP-Timeouts führen.

== Korrekturmaßnahme

Sie müssen die Timeout-Intervalle ändern.

```
xref:{relative_path}reference-configure-storage-replication-adapter-for-
highly-scaled-environment.html["Konfiguration des Storage Replication
Adapter für Umgebungen mit hohem Skalierbarkeit"]
```

[NOTE]

====

Auch die Speichereinstellungen für Skalierung und Performance Ihrer virtuellen Appliance für VSC, VASA Provider und SRA lassen sich in stark skalierten Setups ändern.

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/tune\\_memory\\_settings\\_of\\_VM\\_VSC%2C\\_VASA\\_Provider%2C\\_and\\_SRA\\_for\\_scale\\_and\\_performance\[\]](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance[])

====

[[ID4ee50a3a3d4c9e04b9360343c570802c]]

= Das SRA-Plug-in konnte nicht installiert werden

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

== Problem

Während der Installation des Storage Replication Adapter (SRA) Plug-ins stoppt das System an der Server-IP-Adresse und dem Passwort-Bildschirm mit der folgenden Fehlermeldung: "`die eingegebenen Anmeldeinformationen sind ungültig. Geben Sie einen gültigen Hostnamen und ein gültiges Kennwort ein.`"

== Ursache

Der Fehler kann aus einem der folgenden Gründe auftreten:

- \* Sie haben falsche Anmeldedaten für den Administrator eingegeben.
- \* Die WinHTTP-Proxy-Einstellungen sind falsch.

== Korrekturmaßnahme

- \* Überprüfen Sie Ihre Administratordaten.



\* Der Knowledgebase-Artikel enthält weitere Informationen zur Lösung von Problemen mit WinHTTP Proxy-Einstellungen.

+

[https://kb.netapp.com/app/answers/answer\\_view/a\\_id/1005074](https://kb.netapp.com/app/answers/answer_view/a_id/1005074)["Antwort der NetApp Knowledgebase 1005074: Installieren des SRA 4.0P1-Client-Plug-ins (netapp\_sra\_4.0P1\_ontap\_64bit.msi) hängt am Server-IP- und Passwort-Bildschirm"^]

```
[[ID6a9d784ede7226d13e3c4c16fe989bc8]]
= NetApp Storage Replication Adapter für ONTAP wird nicht auf der Site
Recovery Manager-Appliance angezeigt
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

== Problem

Storage Replication Adapter (SRA) wird nach dem Hochladen und Konfigurieren von SRA nicht auf der Appliance-Schnittstelle des Site Recovery Manager (SRM) angezeigt.

== Ursache

Es wird kein Fehler angezeigt, wenn falsche SRA-Anmeldedaten (Benutzername oder Passwort) verwendet werden, um SRA mithilfe des folgenden Befehls zu konfigurieren.

```
`perl command.pl -I <sra-server-ip> <vp_username> <vp_passwd>`
```

== Korrekturmaßnahme

Aktualisieren Sie die Konfigurationsdetails von SRA mithilfe des folgenden Befehls: ``perl command.pl -U <sra-server-ip> <vp_username> <vp_passwd>``

```
[[ID9d2659154715ffa92592fbb5c6032e9e]]
```

= Fehler bei neuer Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

== Problem

Fehlerprotokoll „`vmware Tools OVF vCenter-Konfiguration nicht gefunden`“ wird bei der Neuimplementierung der virtuellen Appliance für VSC, VASA Provider und SRA angezeigt, wenn ungültige vCenter ServerIPv4-Adresse verwendet wird.

== Ursache

Die virtuelle Appliance für VSC, VASA Provider und SRA unterstützt IPv4- und IPv6-Adressen. Wenn der Benutzer eine IPv4-Adresse für vCenter Server bereitstellt, die im Netzwerk nicht verfügbar ist und keine IPv6-Adresse angegeben ist, werden diese Loggermeldungen auf der Wartungskonsole angezeigt.

== Korrekturmaßnahme

Zum Entfernen des Fehlers sollten Sie folgende Schritte ausführen:

- . Melden Sie sich bei der Wartungskonsole an.
- . Zugriff auf die Diagnose-Shell.
- . Ändern Sie den Benutzer von „`diag`“ in „`root`“ mit ``sudo su`` Befehl.
- . Bearbeiten Sie die Schnittstellendatei mit dem vi-Editor `vi /etc/network/interface`.
- . Entfernen Sie den Eintrag für „`inet6`“.
- . Speichern Sie die Datei, und starten Sie die virtuelle Appliance für VSC, VASA Provider und SRA neu.

Nach dem Neustart der virtuellen Appliance werden keine Fehlermeldungen angezeigt.

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

<<<

\*Copyright-Informationen\*

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, 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 [link:http://www.netapp.com/TM](http://www.netapp.com/TM) [http://www.netapp.com/TM^] aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.