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

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

# Inhalt

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

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.

## Komponenten von vCenter Server-Berechtigungen

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

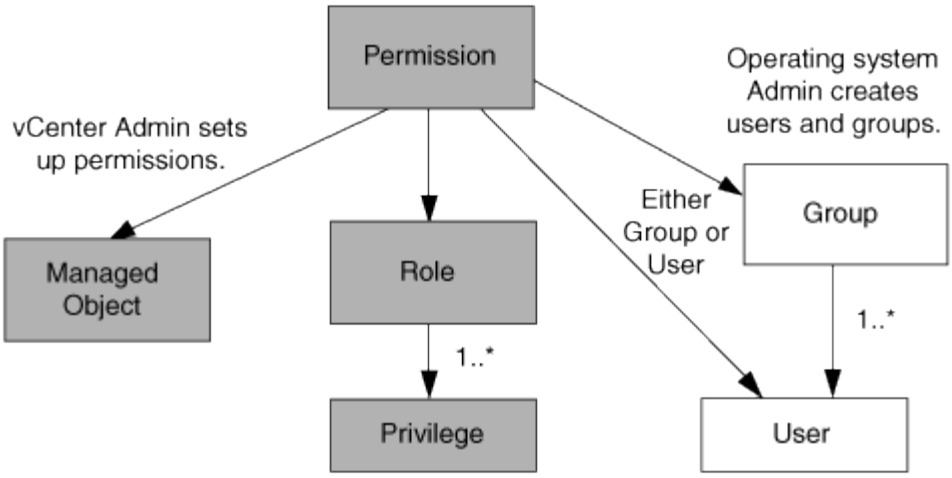
  Das Objekt ist das Ziel für die Aufgaben.

- 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.

> 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.




## 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.

> 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.

| Berechtigung | Rollen | Aufgaben |
|---|---|---|
| Menü:NetApp Virtual Storage Console[View] | • VSC Administrator<br>• VSC Provisionierung<br>• VSC schreibgeschützt | Für alle spezifischen Aufgaben von VSC und VASA Provider ist die View Berechtigung erforderlich. |

| Berechtigung | Rollen | Aufgaben |
|---|---|---|
| Menü:NetApp Virtual Storage Console[richtlinienbasiertes Management > Management] oder Menü:privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label[Management] | VSC Administrator | 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-Ordnerebene (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.

> 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.

## Kernpunkte zum Zuweisen und Ändern von Berechtigungen für vCenter Server

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.

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.

## Standardrollen in Verbindung mit der virtuellen Appliance für VSC, VASA Provider und SRA

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.

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:

| Rolle | Beschreibung |
|---|---|
| VSC Administrator | Bietet alle nativen vCenter Server-Berechtigungen und VSC-spezifische Berechtigungen, die zur Durchführung aller VSC-Aufgaben erforderlich sind. |
| VSC schreibgeschützt | Bietet schreibgeschützten Zugriff auf VSC<br><br>Diese Benutzer können keine VSC Aktionen ausführen, die durch den Zugriff gesteuert werden. |
| VSC Provisionierung | Bietet alle nativen vCenter Server-Berechtigungen und VSC-spezifische Berechtigungen, die für die Bereitstellung von Storage erforderlich sind.<br><br>Sie können die folgenden Aufgaben ausführen:<br><br>• Erstellen neuer Datenspeicher<br>• Datastores zerstören<br>• Zeigt Informationen zu Storage-Funktionsprofilen an |

## Richtlinien zur Verwendung von VSC Standardrollen

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.

# Für VSC Aufgaben erforderliche Berechtigungen

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.

"So konfigurieren Sie RBAC für die Virtual Storage Console"

## Berechtigung auf Produktebene erforderlich von VSC für VMware vSphere

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:

| Berechtigung | Beschreibung | Zuweisungsebene |
| --- | --- | --- |
| Anzeigen | 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. | Die Zuweisungsebene legt fest, welche Teile der Benutzeroberfläche angezeigt werden können.<br><br>Durch das Zuweisen der View-Berechtigung im Root-Objekt (Ordner) können Sie VSC durch Klicken auf das NetApp Symbol eingeben.<br><br>Sie können die View-Berechtigung einer anderen vSphere Objektebene zuweisen. Dabei ist jedoch die VSC-Menüs, die Sie anzeigen und verwenden können, beschränkt.<br><br>Das Root-Objekt ist der empfohlene Ort, um alle Berechtigungen zuzuweisen, die die View-Berechtigung enthalten. |

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

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.

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

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

  "Konfigurieren von Benutzerrollen und -Berechtigungen"

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

  "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.

1. Ermitteln

   Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.

2. Speicher Erstellen

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

3. 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.

4. 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.

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

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

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

  - ONTAP System Manager 9.7 oder höher

  "Konfigurieren von Benutzerrollen und -Berechtigungen"

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

  "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.

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

- "VSC, VASA und SRA 7.0 ONTAP RBAC-Konfiguration"
- "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.

## Konfigurieren von Benutzerrollen und -Berechtigungen

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

1. Entpacken Sie die heruntergeladene Datei `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` Datei:
2. Greifen Sie auf ONTAP System Manager zu.
3. Klicken Sie auf Menü:CLUSTER[Einstellungen > Benutzer und Rollen].
4. Klicken Sie Auf **Benutzer Hinzufügen**.
5. Wählen Sie im Dialogfeld * Benutzer hinzufügen* die Option **Virtualisierungsprodukte** aus.
6. Klicken Sie auf **Durchsuchen**, um die JSON-Datei der ONTAP-Berechtigungen auszuwählen und hochzuladen.

   DAS PRODUKTFELD wird automatisch ausgefüllt.

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

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

8. Geben Sie den erforderlichen Benutzernamen und das erforderliche Passwort ein.
9. 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.