



# **Rollenbasierte Zugriffssteuerung**

## ONTAP tools for VMware vSphere 10

NetApp  
September 30, 2025

This PDF was generated from [https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-100/concepts/concept\\_vcenter\\_server\\_role\\_based\\_access\\_control\\_features\\_in\\_vsc\\_for\\_vmware\\_vsphere.html](https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-100/concepts/concept_vcenter_server_role_based_access_control_features_in_vsc_for_vmware_vsphere.html) on September 30, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

Rollenbasierte Zugriffssteuerung . . . . .	1
Übersicht über die rollenbasierte Zugriffssteuerung in den ONTAP Tools . . . . .	1
Wichtige Punkte zum Zuweisen und Ändern von Rollen für vCenter Server. . . . .	2
Standardrollen in Paket mit ONTAP Tools . . . . .	2
Berechtigungen für ONTAP Storage Back-Ends und vSphere Objekte. . . . .	3
Empfohlene ONTAP-Rollen bei der Verwendung von ONTAP Tools für VMware vSphere . . . . .	3

# Rollenbasierte Zugriffssteuerung

## Übersicht über die rollenbasierte Zugriffssteuerung in den ONTAP Tools

VCenter Server bietet rollenbasierte Zugriffssteuerung (RBAC), über die Sie den Zugriff auf vSphere Objekte kontrollieren können. VCenter Server bietet zentralisierte Authentifizierungs- und Autorisierungsservices auf vielen verschiedenen Ebenen innerhalb des Bestands unter Verwendung von Benutzer- und Gruppenrechten mit Rollen und Berechtigungen. VCenter Server umfasst fünf Hauptkomponenten für das Management von RBAC:

Komponenten	Beschreibung
Berechtigungen	Eine Berechtigung aktiviert oder verweigert den Zugriff auf Aktionen in vSphere.
Rollen	Eine Rolle enthält mindestens eine Systemberechtigung, bei der jede Berechtigung ein Administratorrecht für ein bestimmtes Objekt oder einen Objekttyp im System definiert. Wenn Sie einem Benutzer eine Rolle zuweisen, erbt der Benutzer die Fähigkeiten der in dieser Rolle definierten Berechtigungen.
Benutzer und Gruppen	Benutzer und Gruppen werden in Berechtigungen verwendet, um Rollen aus Active Directory (AD) oder potenziell lokalen Windows-Benutzern/Gruppen zuzuweisen (nicht empfohlen)
Berechtigungen	Mit Berechtigungen können Sie Benutzern oder Gruppen Berechtigungen zuweisen, um bestimmte Aktionen durchzuführen und Änderungen an Objekten in vCenter Server vorzunehmen. VCenter Server-Berechtigungen betreffen nur die Benutzer, die sich bei vCenter Server anmelden, und nicht die Benutzer, die sich direkt bei einem ESXi-Host anmelden.
Objekt	Eine Einheit, auf der Aktionen ausgeführt werden. VMware vCenter Objekte sind Datacenter, Ordner, Ressourcen-Pools, Cluster, Hosts, und VMs

Um eine Aufgabe erfolgreich abzuschließen, müssen Sie über die entsprechenden RBAC-Rollen für vCenter Server verfügen. Während einer Aufgabe prüft ONTAP Tools die vCenter Server-Rollen eines Benutzers, bevor die ONTAP-Berechtigungen des Benutzers überprüft werden.



Die vCenter Server-Rollen gelten für ONTAP Tools vCenter-Benutzer und nicht für Administratoren. Standardmäßig haben Administratoren vollen Zugriff auf das Produkt und benötigen keine Rollen, die ihnen zugewiesen sind.

Die Benutzer und Gruppen erhalten Zugriff auf eine Rolle, indem sie Teil einer vCenter Server-Rolle sind.

## Wichtige Punkte zum Zuweisen und Ändern von Rollen für vCenter Server

Sie müssen nur vCenter Server-Rollen 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 Rolle zuweisen, werden die Aufgaben der ONTAP-Tools festgelegt, die ein Benutzer ausführen kann. Sie können eine Rolle jederzeit ändern. Wenn Sie die Berechtigungen innerhalb einer Rolle ändern, muss sich der Benutzer, der dieser Rolle zugeordnet ist, abmelden und sich dann wieder anmelden, um die aktualisierte Rolle zu aktivieren.

### Standardrollen in Paket mit ONTAP Tools

Um die Arbeit mit vCenter Server-Berechtigungen und RBAC zu vereinfachen, bieten die ONTAP Tools standardmäßige ONTAP Tools, mit denen Sie wichtige Aufgaben im ONTAP Tool ausführen können. Es gibt auch eine schreibgeschützte Rolle, mit der Sie die Informationen anzeigen, aber keine Aufgaben ausführen können.

Sie können die Standardrollen der ONTAP-Tools anzeigen, indem Sie auf der vSphere Client-Startseite auf **Rollen** klicken. Mit den Rollen, die ONTAP-Tools zur Verfügung stellen, können Sie die folgenden Aufgaben ausführen:

* Rolle*	Beschreibung
NetApp ONTAP Tools Administrator	Bietet alle nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Ausführung einiger ONTAP-Tools-Aufgaben erforderlich sind.
NetApp ONTAP-Tools schreibgeschützt	Bietet schreibgeschützten Zugriff auf ONTAP Tools. Diese Benutzer können keine ONTAP-Tools-Aktionen ausführen, die über Zugriffskontrollmöglichkeiten verfügen.
Bereitstellung mit NetApp ONTAP Tools	Bietet einige der nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Bereitstellung von Speicher erforderlich sind. Sie können die folgenden Aufgaben ausführen: <ul style="list-style-type: none"><li>• Erstellen neuer Datenspeicher</li><li>• Managen von Datastores</li></ul>

Die Administratorrolle für die Manager-Benutzeroberfläche ist nicht bei vCenter registriert. Diese Rolle ist spezifisch für die Manager-Benutzeroberfläche.

Wenn in Ihrem Unternehmen Rollen implementiert werden müssen, die restriktiver sind als die Standardrollen für ONTAP-Tools, können Sie mithilfe der Rollen im Bereich ONTAP-Tools neue Rollen erstellen.

In diesem Fall klonen Sie die erforderlichen Rollen der ONTAP-Tools und bearbeiten dann die geklonte Rolle, sodass nur die Berechtigungen zum Benutzer gehören.

## Berechtigungen für ONTAP Storage Back-Ends und vSphere Objekte

Wenn die Berechtigungen für vCenter Server ausreichen, prüfen ONTAP Tools anschließend die RBAC-Berechtigungen von ONTAP (Ihre ONTAP Rolle), die mit den Anmelddaten für Storage-Back-Ends (Benutzername und Passwort) verknüpft sind, um zu ermitteln, ob Sie über ausreichende Berechtigungen verfügen, um die Speichervorgänge auszuführen, die für diese ONTAP-Tools-Aufgabe auf diesem Speicher-Back-End erforderlich sind. Wenn Sie über die richtigen ONTAP-Berechtigungen verfügen, können Sie auf das zugreifen Storage Back-Ends einsetzen und ONTAP Tools durchführen. Die ONTAP-Rollen legen die Aufgaben der ONTAP-Tools fest, die Sie auf dem Storage-Back-End durchführen können.

## Empfohlene ONTAP-Rollen bei der Verwendung von ONTAP Tools für VMware vSphere

Sie können mehrere empfohlene ONTAP-Rollen für die Arbeit mit ONTAP Tools für VMware vSphere und rollenbasierte Zugriffssteuerung einrichten. Diese Rollen verfügen über die ONTAP-Berechtigungen, die zur Durchführung der erforderlichen Storage-Vorgänge erforderlich sind, die von den ONTAP-Tools-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 ONTAP System Manager 9.8P1 oder höher erstellen. Siehe "[Liste der Mindestberechtigungen, die für einen nicht-Administrator-Cluster mit globalem Umfang erforderlich sind](#)" Finden Sie weitere Informationen.

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

Als Sicherheitsmaßnahme werden die ONTAP-Tools-spezifischen ONTAP-Rollen hierarchisch geordnet. Dies bedeutet, dass die erste Rolle die restriktivste Rolle ist und nur über die Berechtigungen verfügt, die mit dem grundlegendsten Satz von ONTAP-Tools-Speichervorgängen 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.

Im Folgenden finden Sie einige der empfohlenen ONTAP RBAC-Rollen bei der Verwendung von ONTAP Tools. 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 Bestandsernahmerolle 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 Bestandsernahmerolle, der Rolle „Speicher erstellen“ und der Rolle „Speicher ändern“ zugeordnet sind.

Wenn Sie VASA Provider für ONTAP nutzen, sollten Sie auch einerichtlinienbasierte Managementrolle (PBM,richtlinienbasiertes Management) einrichten. Diese Rolle ermöglicht Ihnen das Storage-Management mithilfe von Storage-Richtlinien. Diese Rolle erfordert, dass Sie auch die Rolle “Diskcovery” einrichten.

## Copyright-Informationen

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

## Markeninformationen

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