



RBAC mit VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

This PDF was generated from <https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-105/concepts/rbac-vcenter-environment.html> on July 24, 2026. Always check docs.netapp.com for the latest.

Inhalt

- RBAC mit VMware vSphere 1
 - Wie vCenter Server-RBAC mit ONTAP tools funktioniert 1
 - Illustration einer vCenter Server-Berechtigung 1
 - Komponenten einer vCenter Server-Berechtigung 2
 - vCenter Server-RBAC-Überlegungen für ONTAP tools 2
 - vCenter Rollen und das Administratorkonto 2
 - vSphere Objekthierarchie 3
 - Mit ONTAP tools for VMware vSphere 10 enthaltene Rollen 3
 - vSphere-Objekte und ONTAP Storage Backends 6
 - Arbeiten mit vCenter Server-RBAC 6

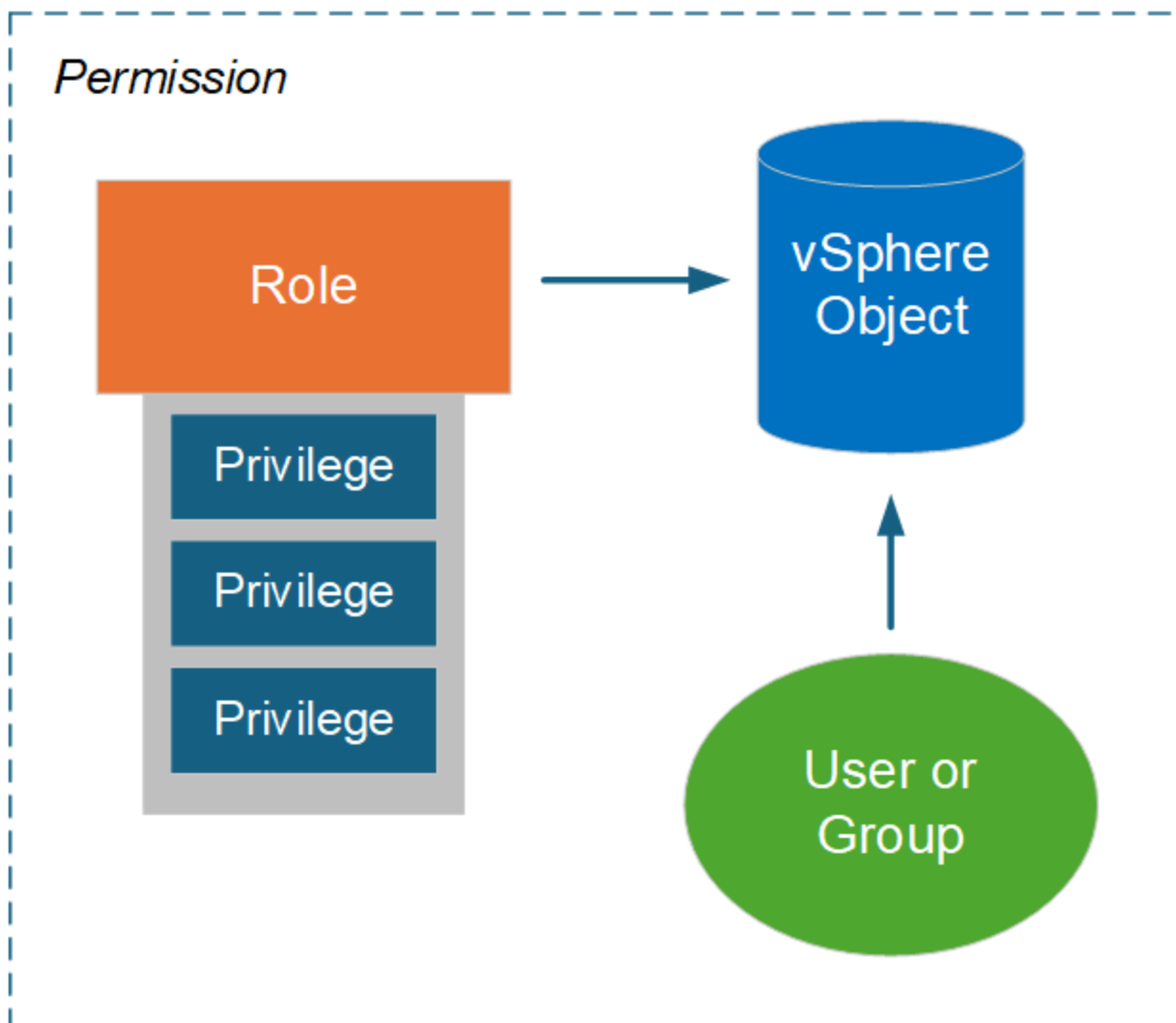
RBAC mit VMware vSphere

Wie vCenter Server-RBAC mit ONTAP tools funktioniert

VMware vCenter Server bietet eine RBAC-Funktion, die die Kontrolle des Zugriffs auf vSphere-Objekte ermöglicht. Dies ist ein wichtiger Bestandteil der zentralisierten Authentifizierungs- und Autorisierungsdienste von vCenter.

Illustration einer vCenter Server-Berechtigung

Eine Berechtigung bildet die Grundlage für die Durchsetzung der Zugriffskontrolle in der vCenter Server-Umgebung. Sie wird auf ein vSphere Objekt angewendet, wobei ein Benutzer oder eine Gruppe in der Berechtigungsdefinition enthalten ist. Eine schematische Darstellung einer vCenter Berechtigung ist in der folgenden Abbildung dargestellt.



Komponenten einer vCenter Server-Berechtigung

Eine vCenter Server-Berechtigung ist ein Paket aus mehreren Komponenten, die bei der Erstellung der Berechtigung miteinander verbunden werden.

vSphere Objekte

Berechtigungen werden vSphere-Objekten wie dem vCenter Server, ESXi Hosts, virtuellen Maschinen, Datenspeichern, Rechenzentren und Ordnern zugeordnet. Basierend auf den einem Objekt zugewiesenen Berechtigungen bestimmt der vCenter Server, welche Aktionen oder Aufgaben von den einzelnen Benutzern oder Gruppen an diesem Objekt durchgeführt werden können. Für die spezifischen Aufgaben der ONTAP tools for VMware vSphere werden alle Berechtigungen auf der Stamm- oder Stammordner-Ebene des vCenter Server zugewiesen und validiert. Weitere Informationen sind unter ["RBAC mit vCenter Server verwenden"](#) zu finden.

Privileges und Rollen

Es gibt zwei Arten von vSphere-Privileges, die mit ONTAP tools for VMware vSphere 10 verwendet werden. Zur Vereinfachung der Arbeit mit RBAC in dieser Umgebung stellen die ONTAP tools Rollen mit den erforderlichen nativen und benutzerdefinierten Privileges bereit. Zu den Privileges gehören:

- Native vCenter Server-Berechtigungen

Dies sind die von vCenter Server bereitgestellten Berechtigungen.

- ONTAP tools-spezifische Privileges

Dies sind benutzerdefinierte Privileges, die ausschließlich für ONTAP tools for VMware vSphere einzigartig sind.

Benutzer und Gruppen

Sie können Benutzer und Gruppen mithilfe von Active Directory oder der lokalen vCenter Server-Instanz definieren. In Kombination mit einer Rolle kann eine Berechtigung für ein Objekt in der vSphere Objekt-Hierarchie erstellt werden. Die Berechtigung gewährt Zugriff basierend auf den Privileges der zugehörigen Rolle. Zu beachten ist, dass Rollen nicht direkt isoliert Benutzern zugewiesen werden. Stattdessen erhalten Benutzer und Gruppen Zugriff auf ein Objekt durch Rollen-Privileges als Teil der umfassenderen vCenter Server-Berechtigung.

vCenter Server-RBAC-Überlegungen für ONTAP tools

Es gibt mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit vCenter Server, die vor der Verwendung in einer Produktionsumgebung berücksichtigt werden sollten.

vCenter Rollen und das Administratorkonto

Sie müssen benutzerdefinierte vCenter Serverrollen nur dann definieren und verwenden, wenn der Zugriff auf die vSphere Objekte und die zugehörigen administrativen Aufgaben eingeschränkt werden soll. Wenn eine Zugriffsbeschränkung nicht erforderlich ist, kann stattdessen ein Administratorkonto verwendet werden. Jedes Administratorkonto ist mit der Administratorrolle auf oberster Ebene der Objekthierarchie definiert. Dies ermöglicht den vollständigen Zugriff auf die vSphere Objekte, einschließlich der von ONTAP tools for VMware vSphere 10 hinzugefügten Objekte.

vSphere Objekthierarchie

Das vSphere-Objektinventar ist in einer Hierarchie organisiert. Beispielsweise kann in der Hierarchie wie folgt nach unten navigiert werden:

vCenter Server --> Datacenter --> Cluster --> ESXi host --> Virtual Machine

Alle Berechtigungen werden in der vSphere-Objekthierarchie validiert, mit Ausnahme der VAAI Plug-in-Operationen, die auf dem Ziel-ESXi-Host validiert werden.

Mit ONTAP tools for VMware vSphere 10 enthaltene Rollen

Um die Arbeit mit vCenter Server-RBAC zu vereinfachen, stellt ONTAP tools for VMware vSphere vordefinierte Rollen bereit, die auf verschiedene administrative Aufgaben zugeschnitten sind.



Sie können bei Bedarf neue benutzerdefinierte Rollen erstellen. Klonen Sie dazu eine der vorhandenen ONTAP tools-Rollen und bearbeiten Sie diese nach Bedarf. Nach den Konfigurationsänderungen müssen sich die betroffenen vSphere Client-Benutzer ausloggen und wieder anmelden, um die Änderungen zu aktivieren.

Um die ONTAP tools für VMware vSphere Rollen anzuzeigen, wählen Sie oben im vSphere Client **Menü** und klicken Sie links auf **Administration** und dann auf **Rollen**. Die folgenden Privileges müssen in der Rolle enthalten sein, die dem vCenter Benutzer zugewiesen ist, der für die Bereitstellung oder das Onboarding des vCenter Servers verantwortlich ist. Stellen Sie sicher, dass diese Privileges als Voraussetzung für den Bereitstellungs- oder Onboarding-Prozess konfiguriert sind.

- Alarme
 - Alarm bestätigen
- Inhaltsbibliothek
 - Bibliothekselement hinzufügen
 - Vorlage einchecken
 - Eine Vorlage kann angesehen werden
 - Dateien herunterladen
 - Storage importieren
 - Lesespeicher
 - Bibliothekselement synchronisieren
 - Synchronisierung der abonnierten Bibliothek
 - Konfigurationseinstellungen anzeigen
- Datenspeicher
 - Speicherplatz zuweisen
 - Datenspeicher durchsuchen
 - Dateioperationen auf niedriger Ebene
 - Datei entfernen
 - Aktualisieren Sie die Dateien der virtuellen Maschine
 - Metadaten der virtuellen Maschine aktualisieren

- ESX Agent Manager
 - Anzeigen
- Ordner
 - Ordner erstellen
- Host
 - Konfiguration
 - Erweiterte Einstellungen
 - Einstellungen ändern
 - Netzwerkkonfiguration
 - Systemressourcen
 - Konfiguration für den automatischen Start der virtuellen Maschine
 - Lokale Operationen
 - Virtuelle Maschine erstellen
 - Virtuelle Maschine löschen
 - Virtuelle Maschine neu konfigurieren
- Netzwerk
 - Netzwerk zuweisen
 - Konfigurieren
- OvfManager
 - OvfConsumer Zugang
- Hostprofil
 - Anzeigen
- Ressource
 - Virtuelle Maschine einem Ressourcenpool zuweisen
- Geplante Aufgabe
 - Aufgaben erstellen
 - Aufgabe ändern
 - Aufgabe ausführen
- Aufgaben
 - Aufgabe erstellen
 - Aufgabe aktualisieren
- vApp
 - Virtuelle Maschine hinzufügen
 - Ressourcenpool zuweisen
 - Weisen Sie vApp zu
 - Erstellen
 - Importieren

- Bewegen
- Ausschalten
- Einschalten
- Aus URL abrufen
- OVF-Umgebung anzeigen
- Virtuelle Maschine
 - Konfiguration ändern
 - Vorhandene Festplatte hinzufügen
 - Neue Festplatte hinzufügen
 - Gerät hinzufügen oder entfernen
 - Erweiterte Konfiguration
 - CPU-Anzahl ändern
 - Speicher ändern
 - Einstellungen ändern
 - Ressource ändern
 - Virtuelle Festplatte erweitern
 - Geräteeinstellungen ändern
 - Datenträger entfernen
 - Gastinformationen zurücksetzen
 - Kompatibilität der virtuellen Maschine aktualisieren
 - Inventar bearbeiten
 - Aus bestehendem erstellen
 - Neu erstellen
 - Bewegen
 - Anmeldung
 - Entfernen
 - Registrierung aufheben
 - Interaktion
 - Sicherungsvorgang auf virtueller Maschine
 - CD-Medien konfigurieren
 - Diskettenmedien konfigurieren
 - Geräte verbinden
 - Konsoleninteraktion
 - Systemmanagement des Gastbetriebssystems über die VIX API
 - Ausschalten
 - Einschalten
 - Zurücksetzen

- Aussetzen
- Bereitstellung
 - Festplattenzugriff zulassen
 - Klonvorlage
 - Gast anpassen
 - Bereitstellungsvorlage
 - Anpassungsspezifikation ändern
 - Anpassungsspezifikationen lesen
- Snapshot Verwaltung
 - Snapshot erstellen
 - Snapshot entfernen
 - Snapshot umbenennen
 - Auf Snapshot zurücksetzen

Es gibt drei vordefinierte Rollen, wie unten beschrieben.

NetApp ONTAP tools für VMware vSphere Administrator

Stellt alle nativen vCenter Server-Berechtigungen und ONTAP tools-spezifischen Berechtigungen bereit, die für die Ausführung der zentralen ONTAP tools für VMware vSphere Administratortasken erforderlich sind.

NetApp ONTAP tools for VMware vSphere Schreibgeschützt

Gewährt Lesezugriff auf ONTAP tools. Diese Benutzer können keine ONTAP tools for VMware vSphere zugriffsbeschränkten Aktionen durchführen.

NetApp ONTAP tools für VMware vSphere Provision

Stellt einige der nativen vCenter Server-Privileges und ONTAP tools-spezifischen Privileges bereit, die für die Bereitstellung von Storage erforderlich sind. Folgende Aufgaben sind möglich:

- Neue Datenspeicher erstellen
- Datenspeicher verwalten

vSphere-Objekte und ONTAP Storage Backends

Die beiden RBAC-Umgebungen arbeiten zusammen. Bei der Ausführung einer Aufgabe in der vSphere Client-Oberfläche werden zunächst die für den vCenter Server definierten ONTAP tools Rollen geprüft. Wenn die Operation von vSphere erlaubt ist, werden anschließend die Privileges der ONTAP Rolle geprüft. Dieser zweite Schritt erfolgt auf Grundlage der ONTAP Rolle, die dem Benutzer bei der Erstellung und Konfiguration des Storage-Backends zugewiesen wurde.

Arbeiten mit vCenter Server-RBAC

Es gibt einige Aspekte, die bei der Arbeit mit den vCenter Server-Berechtigungen und -Rechten zu berücksichtigen sind.

Erforderliche Berechtigungen

Für den Zugriff auf die Benutzeroberfläche von ONTAP tools for VMware vSphere 10 müssen Sie über die für

ONTAP tools spezifische Berechtigung „View“ verfügen. Wenn Sie sich ohne diese Berechtigung bei vSphere anmelden und auf das NetApp Symbol klicken, zeigt ONTAP tools for VMware vSphere eine Fehlermeldung an und verhindert, dass Sie auf die Benutzeroberfläche zugreifen können.

Die Zuweisungsebene in der vSphere-Objekthierarchie bestimmt, auf welche Teile der Benutzeroberfläche Sie zugreifen können. Durch die Zuweisung der Ansichtsberechtigung zum Stammobjekt kann auf ONTAP tools for VMware vSphere zugegriffen werden, indem auf das NetApp-Symbol geklickt wird.

Alternativ kann die Ansichtsberechtigung einer anderen, niedrigeren vSphere Objektebene zugewiesen werden. Dies beschränkt jedoch die ONTAP tools for VMware vSphere Menüs, auf die zugegriffen und die verwendet werden können.

Berechtigungen zuweisen

Sie müssen vCenter Server-Berechtigungen verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und Aufgaben einschränken möchten. Die Stelle, an der die Berechtigung in der vSphere-Objekthierarchie zugewiesen wird, bestimmt, welche Aufgaben mit den ONTAP tools for VMware vSphere 10 von Benutzern durchgeführt werden können.



Sofern Sie keine restriktiveren Zugriffsrechte definieren müssen, ist es im Allgemeinen eine gute Vorgehensweise, Berechtigungen auf der Ebene des Stammobjekts oder des Stammordners zuzuweisen.

Die mit ONTAP tools for VMware vSphere 10 verfügbaren Berechtigungen gelten für benutzerdefinierte Nicht-vSphere-Objekte, wie zum Beispiel Speichersysteme. Nach Möglichkeit sollten diese Berechtigungen dem ONTAP tools for VMware vSphere Stammobjekt zugewiesen werden, da es kein vSphere-Objekt gibt, dem sie zugewiesen werden könnten. Beispielsweise sollte jede Berechtigung, die das Privileg „Speichersysteme hinzufügen/ändern/entfernen“ für ONTAP tools for VMware vSphere beinhaltet, auf Ebene des Stammobjekts zugewiesen werden.

Wenn eine Berechtigung auf einer höheren Ebene der Objekthierarchie definiert wird, kann diese so konfiguriert werden, dass sie an die untergeordneten Objekte weitergegeben und von diesen geerbt wird. Falls erforderlich, können den untergeordneten Objekten zusätzliche Berechtigungen zugewiesen werden, die die vom übergeordneten Objekt geerbten Berechtigungen überschreiben.

Sie können eine Berechtigung jederzeit ändern. Wenn Sie eine der Berechtigungen innerhalb einer Berechtigung ändern, müssen sich die Benutzer, denen diese Berechtigung zugeordnet ist, aus vSphere ausloggen und wieder anmelden, damit die Änderung wirksam wird.

Copyright-Informationen

Copyright © 2026 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, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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