



RBAC mit VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

This PDF was generated from <https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-103/concepts/rbac-vcenter-environment.html> on November 17, 2025. Always check docs.netapp.com for the latest.

Inhalt

- RBAC mit VMware vSphere 1
 - RBAC-Umgebung für vCenter Server mit ONTAP Tools für VMware vSphere 10 1
 - Abbildung einer vCenter Server-Berechtigung 1
 - Komponenten einer vCenter Server-Berechtigung 2
 - Nutzen Sie die RBAC für vCenter Server mit ONTAP Tools für VMware vSphere 10 2
 - vCenter-Rollen und das Administratorkonto 2
 - VSphere Objekthierarchie 3
 - In ONTAP Tools für VMware vSphere 10 enthaltene Rollen 3
 - VSphere Objekte und ONTAP Storage Back-Ends 3
 - Arbeiten mit vCenter Server RBAC 3

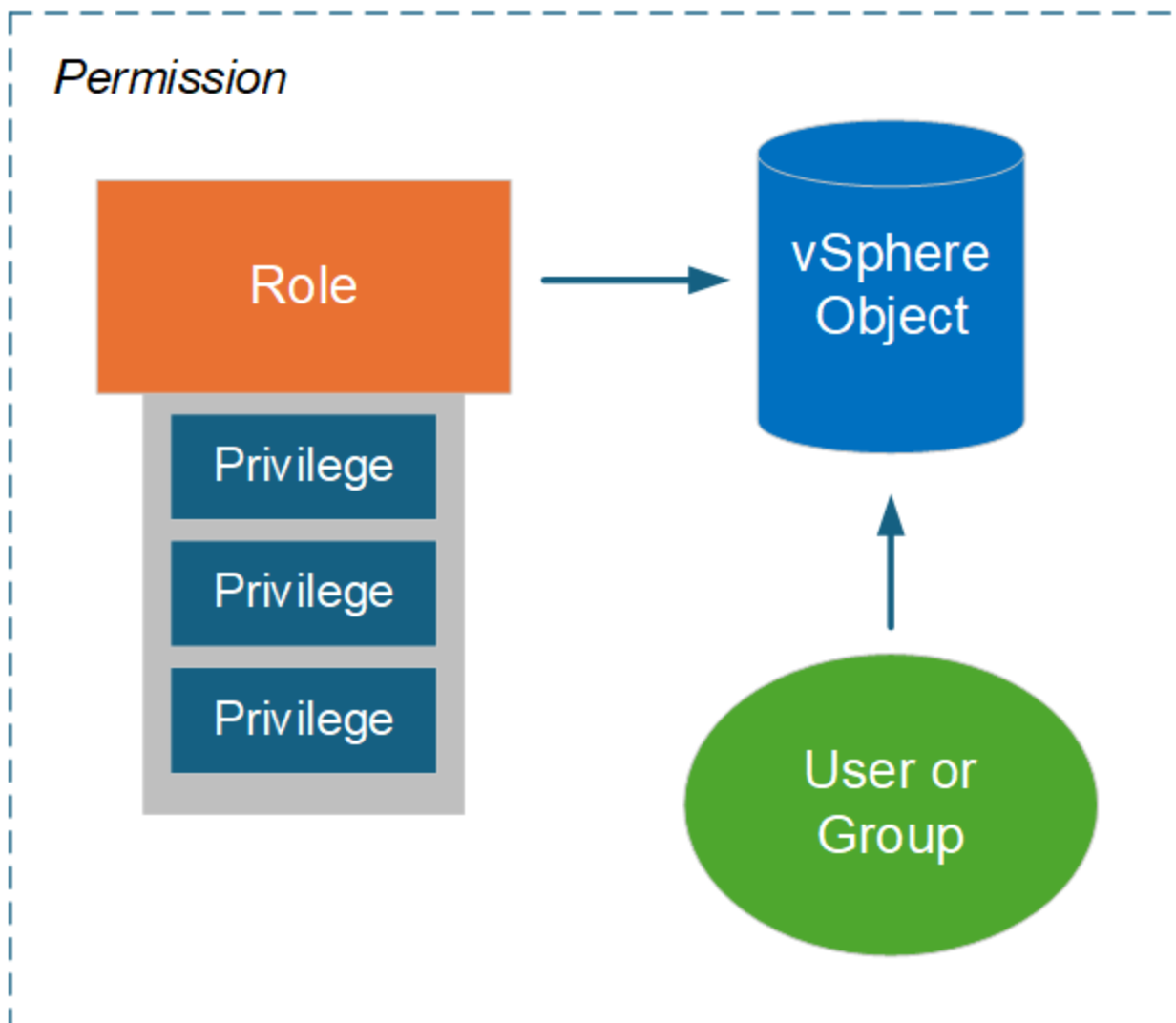
RBAC mit VMware vSphere

RBAC-Umgebung für vCenter Server mit ONTAP Tools für VMware vSphere 10

VMware vCenter Server bietet eine RBAC-Funktion, mit der Sie den Zugriff auf vSphere Objekte steuern können. Dies ist ein wichtiger Teil der zentralisierten Authentifizierungs- und Autorisierungssicherheitsdienste von vCenter.

Abbildung einer vCenter Server-Berechtigung

Eine Berechtigung ist die Grundlage für die Durchsetzung der Zugriffskontrolle in der vCenter Server-Umgebung. Sie wird auf ein vSphere-Objekt mit einem Benutzer oder einer Gruppe angewendet, der in der Berechtigungsdefinition enthalten ist. Die Abbildung unten zeigt eine allgemeine Darstellung einer vCenter-Berechtigung.



Komponenten einer vCenter Server-Berechtigung

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

VSphere Objekte

Berechtigungen sind vSphere-Objekten wie vCenter Server, ESXi-Hosts, virtuellen Maschinen, Datastores, Rechenzentren und Ordnern zugeordnet. Anhand der zugewiesenen Berechtigungen des Objekts bestimmt vCenter Server, welche Aktionen oder Aufgaben für das Objekt von jedem Benutzer oder jeder Gruppe ausgeführt werden können. Für die für ONTAP-Tools für VMware vSphere spezifischen Aufgaben werden alle Berechtigungen auf Root- oder Root-Ordnersebene von vCenter Server zugewiesen und validiert. Weitere Informationen finden Sie unter ["RBAC mit vCenter Server verwenden"](#).

Privileges und Rollen

Es gibt zwei Arten von vSphere Privileges, die mit ONTAP-Tools für VMware vSphere 10 verwendet werden. Um die Arbeit mit RBAC in dieser Umgebung zu vereinfachen, bietet ONTAP Tools Rollen, die die erforderlichen nativen und benutzerdefinierten Privileges enthalten. Die Privileges umfassen:

- Native vCenter Server-Berechtigungen

Dies sind die Privileges, die von vCenter Server bereitgestellt wird.

- Spezifische Berechtigungen für ONTAP-Tools

Hierbei handelt es sich um individuelle Privileges, die nur bei ONTAP Tools für VMware vSphere üblich 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 können Sie eine Berechtigung für ein Objekt in der vSphere-Objekthierarchie erstellen. Die Berechtigung gewährt Zugriff auf Basis der Privileges in der zugehörigen Rolle. Beachten Sie, dass Rollen nicht isoliert direkt Benutzern zugewiesen werden. Stattdessen erhalten Benutzer und Gruppen über die Rolle Privileges als Teil der größeren vCenter Server-Berechtigung Zugriff auf ein Objekt.

Nutzen Sie die RBAC für vCenter Server mit ONTAP Tools für VMware vSphere 10

Es gibt mehrere Aspekte der ONTAP Tools für die Implementierung von VMware vSphere 10 RBAC mit vCenter Server, die Sie vor Verwendung in einer Produktionsumgebung in Betracht ziehen sollten.

VCenter-Rollen und das Administratorkonto

Sie müssen nur die benutzerdefinierten vCenter Server-Rollen definieren und verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und die zugehörigen administrativen Aufgaben einschränken möchten. Wenn keine Zugriffsbeschränkung erforderlich ist, können Sie stattdessen ein Administratorkonto verwenden. Jedes Administratorkonto wird mit der Administratorrolle auf der obersten Ebene der Objekthierarchie definiert. Dies bietet vollen Zugriff auf die vSphere Objekte, einschließlich derer, die von ONTAP Tools für VMware vSphere

10 hinzugefügt wurden.

VSphere Objekthierarchie

Die vSphere-Objektinventar ist in einer Hierarchie organisiert. Sie können die Hierarchie beispielsweise wie folgt nach unten verschieben:

vCenter Server → Datacenter → Cluster → — Virtual Machine > ESXi host

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

In ONTAP Tools für VMware vSphere 10 enthaltene Rollen

Um die Arbeit mit RBAC für vCenter Server zu vereinfachen, bieten die ONTAP Tools für VMware vSphere vordefinierte Rollen, die auf verschiedene Administrationsaufgaben zugeschnitten sind.



Sie können bei Bedarf neue benutzerdefinierte Rollen erstellen. In diesem Fall sollten Sie eine der vorhandenen Rollen des ONTAP-Tools klonen und sie bei Bedarf bearbeiten. Nachdem Sie die Konfigurationsänderungen vorgenommen haben, müssen sich die betroffenen vSphere-Client-Benutzer ab- und wieder anmelden, um die Änderungen zu aktivieren.

Um die ONTAP-Tools für VMware vSphere-Rollen anzuzeigen, wählen Sie oben im vSphere-Client **Menü** aus und klicken Sie auf **Administration** und dann auf **Rollen** auf der linken Seite. Es gibt drei vordefinierte Rollen, wie unten beschrieben.

NetApp ONTAP-Tools für VMware vSphere Administrator

Bietet alle nativen vCenter Server Privileges- und ONTAP-Tools-spezifischen Privileges, die für das Ausführen zentraler ONTAP Tools für VMware vSphere Administrationsaufgaben erforderlich sind.

NetApp ONTAP-Tools für VMware vSphere schreibgeschützt

Bietet schreibgeschützten Zugriff auf ONTAP Tools. Diese Benutzer können keine ONTAP Tools für VMware vSphere Aktionen ausführen, die zugriffsgesteuert sind.

NetApp ONTAP Tools für VMware vSphere Bereitstellung

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:

- Erstellen neuer Datenspeicher
- Managen von Datastores

VSphere Objekte und ONTAP Storage Back-Ends

Die beiden RBAC-Umgebungen arbeiten zusammen. Bei der Ausführung einer Aufgabe in der vSphere-Client-Schnittstelle werden zunächst die für vCenter Server definierten ONTAP-Tools-Rollen aktiviert. Wenn der Vorgang von vSphere zugelassen ist, werden die ONTAP-Rollen-Privileges untersucht. Dieser zweite Schritt basiert auf der ONTAP-Rolle, die dem Benutzer beim Erstellen und Konfigurieren des Storage-Backends zugewiesen wurde.

Arbeiten mit vCenter Server RBAC

Beim Arbeiten mit vCenter Server Privileges und Berechtigungen sind einige Punkte zu beachten.

Erforderliche Berechtigungen

Um auf die Benutzeroberfläche von ONTAP Tools für VMware vSphere 10 zuzugreifen, müssen Sie über die spezifische Berechtigung „Ansicht“ für die ONTAP Tools verfügen. Wenn Sie sich ohne diese Berechtigung bei vSphere anmelden und auf das Symbol NetApp klicken, zeigt ONTAP Tools für 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. Wenn Sie dem Stammobjekt die Berechtigung Ansicht zuweisen, können Sie auf ONTAP-Tools für VMware vSphere zugreifen, indem Sie auf das Symbol NetApp klicken.

Sie können stattdessen die Berechtigung View einer anderen niedrigeren vSphere Objektebene zuweisen. Dies beschränkt jedoch die ONTAP Tools für VMware vSphere Menüs, auf die Sie zugreifen können und die Sie verwenden können.

Berechtigungen werden zugewiesen

Sie müssen vCenter Server-Berechtigungen verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und -Aufgaben einschränken möchten. Wenn Sie Berechtigungen in der vSphere-Objekthierarchie zuweisen, bestimmt dies die ONTAP-Tools für VMware vSphere 10-Aufgaben, die Benutzer ausführen können.



Sofern Sie keinen restriktiveren Zugriff definieren müssen, empfiehlt es sich in der Regel, Berechtigungen auf Root-Objekt- oder Root-Ordnersebene zuzuweisen.

Die mit den ONTAP-Tools für VMware vSphere 10 verfügbaren Berechtigungen gelten für benutzerdefinierte nicht-vSphere-Objekte, wie z. B. Speichersysteme. Wenn möglich, sollten Sie diese Berechtigungen ONTAP-Tools für VMware vSphere-Stammobjekt zuweisen, da es kein vSphere-Objekt gibt, dem Sie es zuweisen können. Beispielsweise sollten alle Berechtigungen, die eine Berechtigung zum Hinzufügen/Ändern/Entfernen von Speichersystemen von ONTAP-Tools für VMware vSphere enthalten, auf der Root-Objektebene zugewiesen werden.

Wenn Sie eine Berechtigung auf einer höheren Ebene in der Objekthierarchie definieren, können Sie die Berechtigung so konfigurieren, dass sie von den untergeordneten Objekten weitergegeben und vererbt wird. Bei Bedarf können Sie den untergeordneten Objekten zusätzliche Berechtigungen zuweisen, die die vom übergeordneten Objekt geerbten Berechtigungen überschreiben.

Sie können eine Berechtigung jederzeit ändern. Wenn Sie eine der Privileges innerhalb einer Berechtigung ändern, müssen sich Benutzer, die mit der Berechtigung verknüpft sind, bei vSphere abmelden und sich erneut anmelden, um die Änderung zu aktivieren.

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, 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.