RBAC mit VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Inhalt

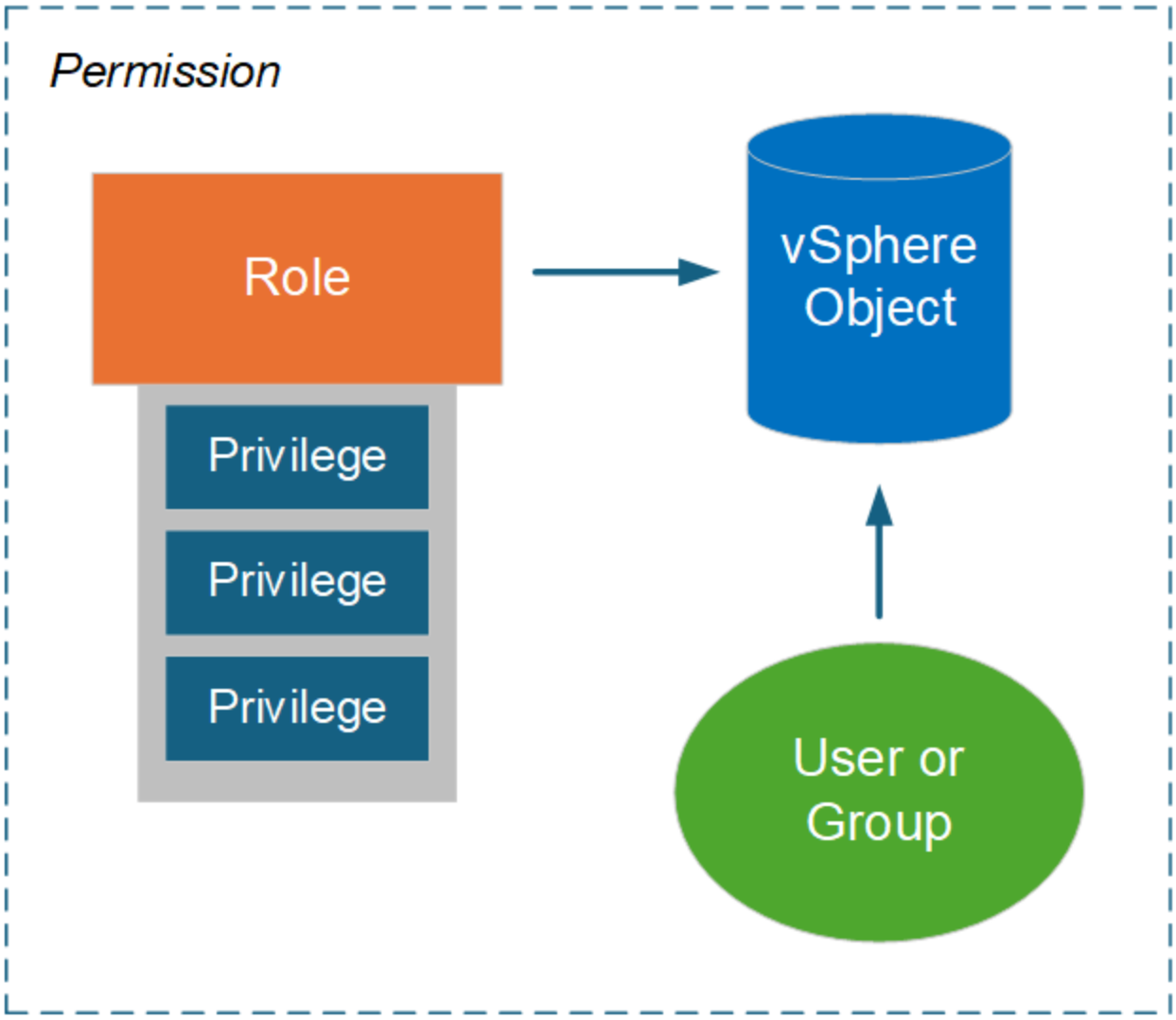
RBAC mit VMware vSphere

Wie vCenter Server-RBAC mit ONTAP tools funktioniert

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-Ordnerebene 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 über Active Directory oder die lokale 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 basierend auf den Berechtigungen der zugehörigen Rolle. Beachten Sie, dass Rollen nicht isoliert Benutzern direkt zugewiesen werden. Stattdessen erhalten Benutzer und Gruppen Zugriff auf ein Objekt über Rollenberechtigungen als Teil der umfassenderen vCenter Server-Berechtigung.

vCenter Server-RBAC-Überlegungen für ONTAP tools

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

- Alarm
  - Alarm bestätigen
- Inhaltsbibliothek
  - Bibliothekselement hinzufügen
  - Vorlage einchecken
  - Schau dir eine Vorlage an
  - Dateien herunterladen
  - Importspeicher
  - Lesespeicher
  - Bibliothekselement synchronisieren
  - Synchronisierung der abonnierten Bibliothek
  - Konfigurationseinstellungen anzeigen
- Datenspeicher
  - Speicherplatz zuweisen
  - Datenspeicher durchsuchen
  - Dateivorgänge auf niedriger Ebene
  - Datei entfernen
  - Aktualisieren der Dateien der virtuellen Maschine
  - Aktualisieren der Metadaten virtueller Maschinen

- ESX Agent Manager
  - Anzeigen
- Ordner
  - Ordner erstellen
- Gastgeber
  - Konfiguration
    - Erweiterte Einstellungen
    - Einstellungen ändern
    - Netzwerkkonfiguration
    - Systemressourcen
    - Konfiguration für den automatischen Start der virtuellen Maschine
  - Lokale Operationen
    - Erstellen einer virtuellen Maschine
    - Virtuelle Maschine löschen
    - Virtuelle Maschine neu konfigurieren
- Netzwerk
  - Netzwerk zuweisen
  - Konfigurieren
- OvfManager
  - Ovf-Verbraucherzugang
- Hostprofil
  - Anzeigen
- Ressource
  - Weisen Sie die virtuelle Maschine dem Ressourcenpool zu.
- Geplante Aufgabe
  - Aufgaben erstellen
  - Aufgabe ändern
  - Aufgabe ausführen
- Aufgaben
  - Aufgabe erstellen
  - Aufgabe aktualisieren
- vApp
  - Virtuelle Maschine hinzufügen
  - Ressourcenpool zuweisen
  - vApp zuweisen
  - Erstellen
  - Import

    - Bewegen
    - Strom aus
    - Strom einschalten
    - Aus URL abrufen
    - OVF-Umgebung anzeigen
- Virtual Machine
    - 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 mit virtuellen Maschinen verbessern
    - Inventar bearbeiten
        - Aus bestehenden erstellen
        - Neu erstellen
        - Bewegen
        - Anmeldung
        - Entfernen
        - Abmelden
    - Interaktion
        - Sicherungsvorgang auf virtueller Maschine
        - CD-Medien konfigurieren
        - Diskettenmedien konfigurieren
        - Geräte verbinden
        - Konsoleninteraktion
        - Gastbetriebssystemverwaltung über die VIX-API
        - Strom aus
        - Strom einschalten
        - Zurücksetzen

        - Aussetzen
    - Bereitstellung
        - Festplattenzugriff zulassen
        - Klonvorlage
        - Gäste anpassen
        - Bereitstellungsvorlage
        - Anpassungsspezifikation ändern
        - Lesen Sie die Anpassungsspezifikationen.
    - Snapshot-Verwaltung
        - Snapshot erstellen
        - Snapshot entfernen
        - Snapshot umbenennen
        - Auf Snapshot zurücksetzen

Es gibt drei vordefinierte Rollen, die unten beschrieben werden.

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 Administratoraufgaben 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-Ordnerebene 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.