RBAC mit VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Inhalt

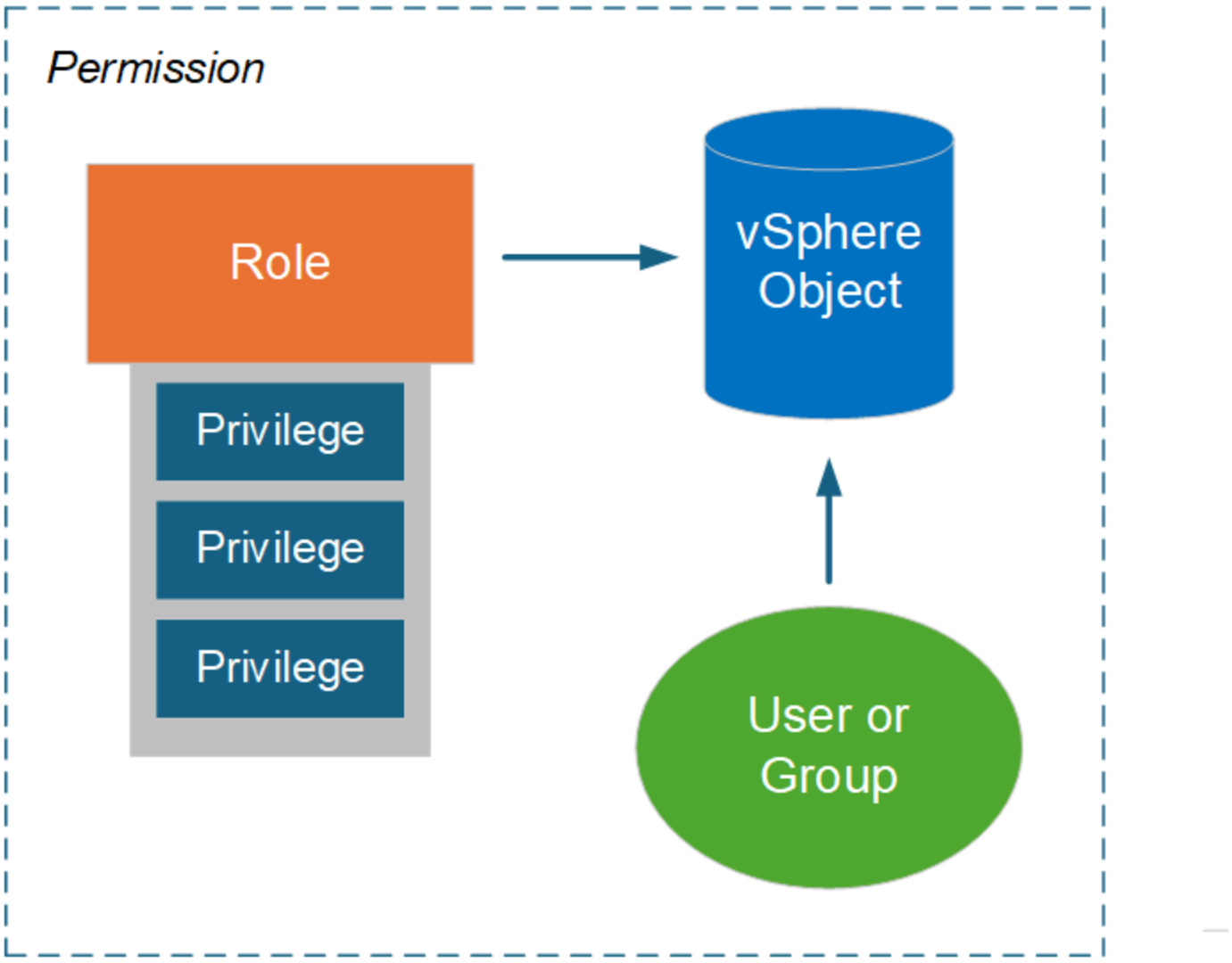
RBAC mit VMware vSphere

vCenter Server RBAC-Umgebung mit ONTAP tools for VMware vSphere 10

VMware vCenter Server bietet eine RBAC-Funktion, mit der Sie den Zugriff auf vSphere-Objekte steuern können. Es 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. Es wird auf ein vSphere-Objekt mit einem Benutzer oder einer Gruppe angewendet, der bzw. die in der Berechtigungsdefinition enthalten ist. Eine allgemeine Darstellung einer vCenter-Berechtigung finden Sie in der folgenden Abbildung.



Komponenten einer vCenter Server-Berechtigung

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

vSphere-Objekte

Berechtigungen sind mit vSphere-Objekten verknüpft, beispielsweise mit dem vCenter Server, ESXi-Hosts, virtuellen Maschinen, Datenspeichern, Rechenzentren und Ordnern. Basierend auf den dem Objekt zugewiesenen Berechtigungen bestimmt vCenter Server, welche Aktionen oder Aufgaben von jedem Benutzer oder jeder Gruppe am Objekt ausgeführt werden können. Für die für ONTAP tools for VMware vSphere spezifischen Aufgaben werden alle Berechtigungen auf der Stamm- oder Stammordnerebene von vCenter Server zugewiesen und validiert. Sehen "Verwenden von RBAC mit vCenter-Server" für weitere Informationen.

Privileges und Rollen

Es gibt zwei Arten von vSphere-Berechtigungen, die mit ONTAP tools for VMware vSphere 10 verwendet werden. Um die Arbeit mit RBAC in dieser Umgebung zu vereinfachen, stellen ONTAP Tools Rollen bereit, die die erforderlichen nativen und benutzerdefinierten Berechtigungen enthalten. Zu den Privilegien gehören:

- Native vCenter Server-Berechtigungen

  Dies sind die von vCenter Server bereitgestellten Berechtigungen.

- ONTAP -Tool-spezifische Berechtigungen

  Dies sind benutzerdefinierte Berechtigungen, die nur für ONTAP tools for VMware vSphere gelten.

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.

Verwenden Sie vCenter Server RBAC mit ONTAP tools for VMware vSphere 10

Es gibt mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit vCenter Server, die Sie berücksichtigen sollten, bevor Sie sie in einer Produktionsumgebung verwenden.

vCenter-Rollen und das Administratorkonto

Sie müssen die benutzerdefinierten vCenter Server-Rollen nur definieren und verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und die zugehörigen Verwaltungsaufgaben 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 vollständigen Zugriff auf die vSphere-Objekte, einschließlich derjenigen, die von ONTAP tools for VMware vSphere 10 hinzugefügt wurden.

vSphere-Objekthierarchie

Das vSphere-Objektinventar ist hierarchisch organisiert. Sie können sich beispielsweise wie folgt in der Hierarchie nach unten bewegen:

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

Alle Berechtigungen werden in der vSphere-Objekthierarchie validiert, mit Ausnahme der VAAI-Plug-In-Vorgänge, die anhand des ESXi-Zielhosts validiert werden.

In den ONTAP tools for VMware vSphere 10 enthaltene Rollen

Um die Arbeit mit vCenter Server RBAC zu vereinfachen, bieten ONTAP tools for VMware vSphere vordefinierte Rollen, die auf verschiedene Verwaltungsaufgaben zugeschnitten sind.

> Sie können bei Bedarf neue benutzerdefinierte Rollen erstellen. In diesem Fall sollten Sie eine der vorhandenen ONTAP -Tool-Rollen klonen und nach Bedarf bearbeiten. Nach dem Vornehmen der Konfigurationsänderungen müssen sich die betroffenen vSphere-Client-Benutzer abmelden und erneut 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 auf **Verwaltung** und dann links auf **Rollen**. Es gibt drei vordefinierte Rollen, die unten beschrieben werden.

NetApp ONTAP tools for VMware vSphere Administrator

Bietet alle nativen vCenter Server-Berechtigungen und ONTAP Tool-spezifischen Berechtigungen, die zum Ausführen zentraler ONTAP tools for VMware vSphere Administratoraufgaben erforderlich sind.

NetApp ONTAP tools for VMware vSphere Read Only

Bietet schreibgeschützten Zugriff auf ONTAP -Tools. Diese Benutzer können keine ONTAP tools for VMware vSphere Aktionen ausführen, für die der Zugriff kontrolliert wird.

NetApp ONTAP tools for VMware vSphere Provision

Bietet einige der nativen vCenter Server-Berechtigungen und ONTAP Tool-spezifischen Berechtigungen, die für die Speicherbereitstellung erforderlich sind. Sie können die folgenden Aufgaben ausführen:

- Erstellen neuer Datenspeicher
- Verwalten von Datenspeichern

vSphere-Objekte und ONTAP -Speicher-Backends

Die beiden RBAC-Umgebungen arbeiten zusammen. Beim Ausführen einer Aufgabe in der vSphere-Clientschnittstelle werden zuerst die für vCenter Server definierten ONTAP -Toolrollen überprüft. Wenn der Vorgang von vSphere zugelassen wird, werden die ONTAP Rollenberechtigungen geprüft. Dieser zweite Schritt wird basierend auf der ONTAP Rolle ausgeführt, die dem Benutzer beim Erstellen und Konfigurieren des Speicher-Backends zugewiesen wurde.

Arbeiten mit vCenter Server RBAC

Beim Arbeiten mit den Privilegien und Berechtigungen des vCenter Servers sind einige Dinge zu beachten.

Erforderliche Berechtigungen

Um auf die Benutzeroberfläche der ONTAP tools for VMware vSphere 10 zugreifen zu können, benötigen Sie das für ONTAP -Tools spezifische *Anzeige*-Privileg. 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. Wenn Sie dem Stammobjekt die Berechtigung „Anzeigen“ zuweisen, können Sie durch Klicken auf das NetApp -Symbol auf ONTAP tools for VMware vSphere zugreifen.

Sie können die Anzeigeberechtigung stattdessen einer anderen niedrigeren vSphere-Objektebene zuweisen. Dadurch werden jedoch die ONTAP tools for VMware vSphere -Menüs eingeschränkt, auf die Sie zugreifen und die Sie verwenden können.

Berechtigungen zuweisen

Sie müssen vCenter Server-Berechtigungen verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und -Aufgaben beschränken möchten. Wo Sie in der vSphere-Objekthierarchie Berechtigungen zuweisen, bestimmt, welche ONTAP tools for VMware vSphere 10-Aufgaben Benutzer ausführen können.

Sofern Sie keinen restriktiveren Zugriff definieren müssen, empfiehlt es sich im Allgemeinen, Berechtigungen auf der Ebene des Stammobjekts oder des Stammordners zuzuweisen.

Die mit den ONTAP tools for VMware vSphere 10 verfügbaren Berechtigungen gelten für benutzerdefinierte Nicht-vSphere-Objekte, beispielsweise Speichersysteme. Wenn möglich, sollten Sie diese Berechtigungen den ONTAP tools for VMware vSphere Stammobjekt zuweisen, da es kein vSphere-Objekt gibt, dem Sie sie zuweisen können. Beispielsweise sollte jede Berechtigung, die ein ONTAP tools for VMware vSphere Privileg zum „Hinzufügen/Ändern/Entfernen von Speichersystemen“ umfasst, auf der Stammobjektebene zugewiesen werden.

Wenn Sie eine Berechtigung auf einer höheren Ebene in der Objekthierarchie definieren, können Sie die Berechtigung so konfigurieren, dass sie weitergegeben und von den untergeordneten Objekten geerbt 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 Berechtigungen innerhalb einer Berechtigung ändern, müssen sich die mit der Berechtigung verknüpften Benutzer von vSphere abmelden und erneut anmelden, um die Änderung zu aktivieren.