Rollenbasierte Zugriffssteuerung (RBAC)

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

Rollenbasierte Zugriffssteuerung (RBAC)

Erfahren Sie mehr über ONTAP tools RBAC

Die rollenbasierte Zugriffskontrolle (RBAC) ist ein Sicherheitsframework zur Steuerung des Zugriffs auf Ressourcen innerhalb einer Organisation. RBAC vereinfacht die Administration, indem Rollen mit spezifischen Berechtigungsstufen zur Ausführung von Aktionen definiert werden, anstatt einzelnen Benutzern Berechtigungen zuzuweisen. Die definierten Rollen werden Benutzern zugewiesen, was das Fehlerrisiko verringert und die Verwaltung der Zugriffskontrolle in der gesamten Organisation vereinfacht.

Das RBAC-Standardmodell besteht aus mehreren Implementierungstechnologien oder Phasen mit zunehmender Komplexität. Das Ergebnis ist, dass sich die tatsächlichen RBAC-Implementierungen, abhängig von den Anforderungen der Softwareanbieter und ihrer Kunden, unterscheiden und von relativ einfach bis sehr komplex reichen können.

RBAC-Komponenten

Grundsätzlich gibt es mehrere Komponenten, die in jeder RBAC-Implementierung enthalten sind. Diese Komponenten sind im Rahmen der Definition der Autorisierungsprozesse auf unterschiedliche Weise miteinander verbunden.

Privileges

Ein Privileg ist eine Aktion oder Fähigkeit, die erlaubt oder verweigert werden kann. Es kann sich um etwas Einfaches handeln, wie die Fähigkeit, eine Datei zu lesen, oder um eine abstraktere Operation, die spezifisch für ein bestimmtes Softwaresystem ist. Privileges können auch definiert werden, um den Zugriff auf REST API-Endpunkte und CLI-Befehle einzuschränken. Jede RBAC-Implementierung enthält vordefinierte Privilegien und kann Administratoren auch erlauben, benutzerdefinierte Privilegien zu erstellen.

Rollen

Eine Rolle ist ein Container, der ein oder mehrere Privileges umfasst. Rollen werden in der Regel anhand bestimmter Aufgaben oder Funktionen definiert. Wird einem Benutzer eine Rolle zugewiesen, erhält der Benutzer alle in der Rolle enthaltenen Privileges. Wie bei Privileges bieten Implementierungen vordefinierte Rollen und ermöglichen in der Regel auch die Erstellung benutzerdefinierter Rollen.

Objekte

Ein Objekt repräsentiert eine reale oder abstrakte Ressource innerhalb der RBAC-Umgebung. Die über die Privileges definierten Aktionen werden an oder mit den zugehörigen Objekten ausgeführt. Je nach Implementierung können Privileges einem Objekttyp oder einer bestimmten Objektinstanz gewährt werden.

Benutzer und Gruppen

Benutzern wird nach der Authentifizierung eine Rolle zugewiesen oder sie werden mit einer Rolle verknüpft. Einige RBAC-Implementierungen erlauben nur eine Rolle pro Benutzer, während andere mehrere Rollen pro Benutzer zulassen, wobei möglicherweise jeweils nur eine Rolle aktiv ist. Die Zuweisung von Rollen zu *Gruppen* kann die Sicherheitsverwaltung zusätzlich vereinfachen.

Berechtigungen

Eine Berechtigung ist eine Definition, die einen Benutzer oder eine Gruppe zusammen mit einer Rolle an ein Objekt bindet. Berechtigungen können in einem hierarchischen Objektmodell nützlich sein, da sie optional von den untergeordneten Elementen in der Hierarchie übernommen werden können.

Zwei RBAC Umgebungen

Bei der Arbeit mit ONTAP tools for VMware vSphere 10 sind zwei unterschiedliche RBAC-Umgebungen zu berücksichtigen. ONTAP tools for VMware vSphere 10 erfordert spezifische Privileges sowohl in vCenter als auch in ONTAP, um die jeweiligen Vorgänge auszuführen. Während ONTAP tools Speicherverwaltungsaufgaben automatisiert, werden keine Benutzerkonten in vCenter oder ONTAP erstellt. Dienstkonten müssen bei Bedarf von einem vSphere-Administrator erstellt werden. Diese Dokumentation enthält Hinweise für Administratoren zur Zuweisung der erforderlichen Rollen und Berechtigungen für eine effektive Verwaltung von ONTAP tools.

VMware vCenter Server

Die RBAC-Implementierung in VMware vCenter Server wird verwendet, um den Zugriff auf Objekte einzuschränken, die über die vSphere Client-Benutzeroberfläche bereitgestellt werden. Im Rahmen der Installation von ONTAP tools for VMware vSphere 10 wird die RBAC-Umgebung um zusätzliche Objekte erweitert, die die Fähigkeiten der ONTAP tools repräsentieren. Der Zugriff auf diese Objekte erfolgt über das Remote-Plug-in. Weitere Informationen sind unter "vCenter Server-RBAC-Umgebung" verfügbar.

ONTAP Cluster

ONTAP tools for VMware vSphere 10 stellt über die ONTAP REST API eine Verbindung zu einem ONTAP Cluster her, um speicherbezogene Vorgänge auszuführen. Der Zugriff auf die Speicherressourcen wird durch eine ONTAP Rolle gesteuert, die dem ONTAP Benutzer zugeordnet ist, der während der Authentifizierung angegeben wurde. Siehe "ONTAP RBAC Umgebung" für weitere Informationen.

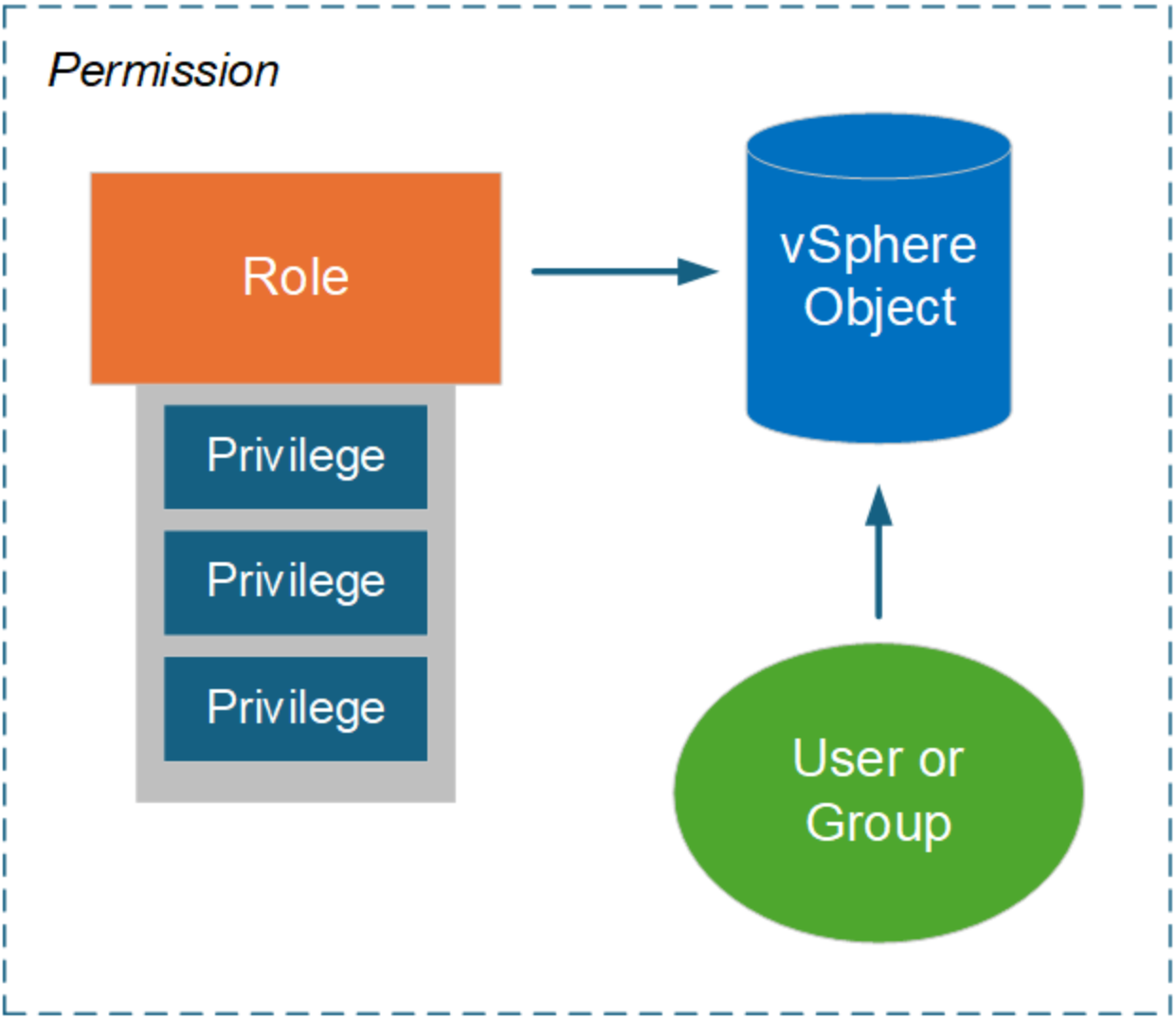
RBAC mit VMware vSphere

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 Administratoraufgaben 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.

RBAC mit ONTAP

Wie ONTAP RBAC mit ONTAP tools funktioniert

ONTAP bietet eine robuste und erweiterbare RBAC Umgebung. Die RBAC-Funktionalität ermöglicht die Steuerung des Zugriffs auf Speicher und Systemvorgänge, wie sie über die REST API und CLI bereitgestellt werden. Es ist hilfreich, mit der Umgebung vertraut zu sein, bevor sie mit einer ONTAP tools for VMware vSphere 10 Bereitstellung verwendet wird.

Überblick über die administrativen Optionen

Bei der Verwendung von ONTAP RBAC stehen je nach Ihrer Umgebung und Ihren Zielen verschiedene Optionen zur Verfügung. Nachfolgend ist ein Überblick über die wichtigsten administrativen Entscheidungen dargestellt. Siehe auch "ONTAP Automatisierung: Überblick über die RBAC-Sicherheit" für weitere Informationen.

ONTAP RBAC ist speziell für Speicherumgebungen entwickelt und einfacher als die mit dem vCenter Server bereitgestellte RBAC-Implementierung. Mit ONTAP wird die Rolle direkt dem Benutzer zugewiesen. Die Konfiguration expliziter Berechtigungen, wie sie mit dem vCenter Server verwendet werden, ist mit ONTAP RBAC nicht erforderlich.

Arten von Rollen und Privileges

Für die Definition eines ONTAP Benutzers ist eine ONTAP Rolle erforderlich. Es gibt zwei Arten von ONTAP Rollen:

- REST

Die REST-Rollen wurden mit ONTAP 9.6 eingeführt und werden im Allgemeinen auf Benutzer angewendet, die über die REST-API auf ONTAP zugreifen. Die in diesen Rollen enthaltenen Privileges sind im Hinblick auf den Zugriff auf die ONTAP REST API-Endpunkte und die zugehörigen Aktionen definiert.

- Traditionell

  Dies sind die Legacy-Rollen, die vor ONTAP 9.6 existierten. Sie sind weiterhin ein grundlegender Bestandteil von RBAC. Die Privileges werden anhand des Zugriffs auf die ONTAP CLI-Befehle definiert.

Obwohl die REST-Rollen erst vor Kurzem eingeführt wurden, bieten die traditionellen Rollen einige Vorteile. Beispielsweise können zusätzliche Abfrageparameter hinzugefügt werden, damit Privileges die Objekte, auf die sie angewendet werden, genauer definieren können.

Umfang

ONTAP Rollen können mit einem von zwei verschiedenen Gültigkeitsbereichen definiert werden. Sie können auf eine bestimmte Daten SVM (SVM-Ebene) oder auf den gesamten ONTAP Cluster (Cluster-Ebene) angewendet werden.

Rollendefinitionen

ONTAP bietet eine Reihe vordefinierter Rollen sowohl auf Cluster- als auch auf SVM-Ebene. Es besteht außerdem die Möglichkeit, benutzerdefinierte Rollen zu definieren.

Arbeiten mit ONTAP REST Rollen

Bei der Verwendung der mit ONTAP tools for VMware vSphere 10 enthaltenen ONTAP REST-Rollen sind mehrere Aspekte zu berücksichtigen.

Rollenzuordnung

Unabhängig davon, ob eine traditionelle Rolle oder eine REST-Rolle verwendet wird, werden alle ONTAP-Zugriffsentscheidungen auf Grundlage des zugrunde liegenden CLI-Befehls getroffen. Da die Privileges in einer REST-Rolle jedoch anhand der REST-API-Endpunkte definiert sind, muss ONTAP für jede REST-Rolle eine *zugeordnete* traditionelle Rolle erstellen. Daher ist jede REST-Rolle einer zugrunde liegenden traditionellen Rolle zugeordnet. Dies ermöglicht ONTAP, Zugriffskontrollentscheidungen unabhängig vom Rollentyp konsistent zu treffen. Die parallel zugeordneten Rollen können nicht geändert werden.

Definieren einer REST-Rolle mithilfe von CLI-Privileges

Da ONTAP die Zugriffsrechte grundsätzlich über CLI-Befehle festlegt, lässt sich eine REST-Rolle mithilfe von CLI-Befehlsberechtigungen anstelle von REST-Endpunkten definieren. Ein Vorteil dieses Ansatzes ist die zusätzliche Granularität der traditionellen Rollen.

Administrative Schnittstelle bei der Definition von ONTAP Rollen

Benutzer und Rollen können mit der ONTAP CLI und der REST API erstellt werden. Bequemer ist die Nutzung der System Manager Oberfläche zusammen mit der über den ONTAP tools Manager verfügbaren JSON-Datei. Siehe "ONTAP RBAC mit ONTAP tools für VMware vSphere 10 verwenden" für weitere Informationen.

ONTAP RBAC-Überlegungen für ONTAP tools

Es sind mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit ONTAP zu berücksichtigen, bevor diese in einer Produktionsumgebung verwendet werden.

Überblick über den Konfigurationsprozess

ONTAP tools for VMware vSphere umfasst Unterstützung für die Erstellung eines ONTAP Benutzers mit einer benutzerdefinierten Rolle. Die Definitionen sind in einer JSON-Datei zusammengefasst, die in den ONTAP Cluster hochgeladen werden kann. Der Benutzer und die Rolle können entsprechend der jeweiligen Umgebung und Sicherheitsanforderungen erstellt und angepasst werden.

Die wichtigsten Konfigurationsschritte werden im Folgenden grob beschrieben. Weitere Details sind unter "ONTAP Benutzerrollen und Privileges konfigurieren" zu finden.

1. Vorbereiten

Sie benötigen Administratorrechte sowohl für den ONTAP tools Manager als auch für den ONTAP Cluster.

2. Die JSON-Definitionsdatei herunterladen

Nach der Anmeldung an der ONTAP tools Manager Benutzeroberfläche kann die JSON-Datei mit den RBAC-Definitionen heruntergeladen werden.

3. Einen ONTAP Benutzer mit einer Rolle erstellen

Nach der Anmeldung im System Manager können der Benutzer und die Rolle erstellt werden:

1. Links **Cluster** und dann **Einstellungen** auswählen.
2. Scrollen Sie nach unten zu **Benutzer und Rollen** und klicken Sie auf −→.
3. Unter **Benutzer Hinzufügen** auswählen und dann **Virtualisierungsprodukte** auswählen.
4. Wählen Sie die JSON-Datei auf Ihrem lokalen Rechner aus und laden Sie sie hoch.

4. Die Rolle konfigurieren

Im Rahmen der Rollendefinition sind mehrere administrative Entscheidungen erforderlich. Siehe Die Rolle wird mithilfe von System Manager konfiguriert. für weitere Details.

Die Rolle wird mithilfe von System Manager konfiguriert.

Nachdem Sie mit System Manager einen neuen Benutzer und eine neue Rolle erstellt und die JSON-Datei hochgeladen haben, kann die Rolle an Ihre Umgebung und Bedürfnisse angepasst werden.

Kernbenutzer und Rollenkonfiguration

Die RBAC-Definitionen sind in verschiedenen Produktfunktionen zusammengefasst, darunter Kombinationen aus VSC, VASA Provider und SRA. Die Umgebung oder Umgebungen, in denen RBAC-Unterstützung benötigt wird, sollten ausgewählt werden. Wenn beispielsweise Rollen die Remote Plug-in-Funktion unterstützen sollen, ist VSC auszuwählen. Auch der Benutzername und das zugehörige Passwort müssen ausgewählt werden.

Privileges

Die Rollenberechtigungen sind in vier Gruppen unterteilt, basierend auf dem für ONTAP Storage benötigten Zugriffsniveau. Die den Rollen zugrunde liegenden Privileges umfassen:

- Entdeckung

  Diese Rolle ermöglicht es Ihnen, Speichersysteme hinzuzufügen.

- Speicher erstellen

  Diese Rolle ermöglicht Ihnen das Erstellen von Storage. Sie umfasst außerdem alle Privileges, die mit der

Discovery-Rolle verbunden sind.

- Speicher ändern

  Diese Rolle ermöglicht Ihnen, Speicher zu ändern. Sie umfasst außerdem alle Privileges, die mit den Rollen „Speicher ermitteln“ und „Speicher erstellen“ verbunden sind.

- Speicher zerstören

  Diese Rolle ermöglicht Ihnen, Speicher zu zerstören. Sie umfasst außerdem alle Privileges, die mit den Rollen „Speicher ermitteln“, „Speicher erstellen“ und „Speicher ändern“ verbunden sind.

Den Benutzer mit einer Rolle generieren

Nachdem Sie die Konfigurationsoptionen für Ihre Umgebung ausgewählt haben, auf **Hinzufügen** klicken, erstellt ONTAP den Benutzer und die Rolle. Der Name der generierten Rolle ist eine Verkettung der folgenden Werte:

- Konstanter Präfixwert, der in der JSON-Datei definiert ist (zum Beispiel "OTV_10")
- Die ausgewählte Produktfunktion
- Liste der Berechtigungssätze.

Beispiel

```
OTV_10_VSC_Discovery_Create
```

Der neue Benutzer wird der Liste auf der Seite „Benutzer und Rollen“ hinzugefügt. Beachten Sie, dass sowohl HTTP- als auch ONTAPI-Benutzeranmeldemethoden unterstützt werden.