RBAC mit ONTAP

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

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.