RBAC mit ONTAP

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Inhalt

RBAC mit ONTAP

ONTAP RBAC-Umgebung mit ONTAP tools for VMware vSphere 10

ONTAP bietet eine robuste und erweiterbare RBAC-Umgebung. Sie können die RBAC-Funktion verwenden, um den Zugriff auf die Speicher- und Systemvorgänge zu steuern, die über die REST-API und CLI bereitgestellt werden. Es ist hilfreich, sich mit der Umgebung vertraut zu machen, bevor Sie sie mit einem ONTAP tools for VMware vSphere 10 verwenden.

Übersicht der administrativen Möglichkeiten

Bei der Verwendung von ONTAP RBAC stehen Ihnen je nach Umgebung und Zielen mehrere Optionen zur Verfügung. Nachfolgend finden Sie eine Übersicht über die wichtigsten Verwaltungsentscheidungen. Siehe auch "ONTAP -Automatisierung: Übersicht über die RBAC-Sicherheit" für weitere Informationen.

> ONTAP RBAC ist auf eine Speicherumgebung zugeschnitten und einfacher als die mit vCenter Server bereitgestellte RBAC-Implementierung. Mit ONTAP weisen Sie dem Benutzer direkt eine Rolle zu. Das Konfigurieren expliziter Berechtigungen, wie sie beispielsweise bei vCenter Server verwendet werden, ist bei ONTAP RBAC nicht erforderlich.

Arten von Rollen und Berechtigungen

Zum Definieren eines ONTAP Benutzers ist eine ONTAP -Rolle erforderlich. Es gibt zwei Arten von ONTAP -Rollen:

- AUSRUHEN

  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 Berechtigungen sind hinsichtlich des Zugriffs auf die ONTAP REST API-Endpunkte und die zugehörigen Aktionen definiert.

- Traditionell

  Dies sind die Legacy-Rollen, die vor ONTAP 9.6 enthalten waren. Sie sind weiterhin ein grundlegender Aspekt von RBAC. Die Berechtigungen werden in Bezug auf den Zugriff auf die ONTAP CLI-Befehle definiert.

Während die REST-Rollen erst vor kurzem eingeführt wurden, bieten die traditionellen Rollen einige Vorteile. Beispielsweise können optional zusätzliche Abfrageparameter eingefügt werden, sodass die Berechtigungen die Objekte, auf die sie angewendet werden, genauer definieren.

Umfang

ONTAP -Rollen können mit einem von zwei verschiedenen Bereichen 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. Sie können auch benutzerdefinierte Rollen definieren.

Arbeiten mit ONTAP REST-Rollen

Bei der Verwendung der in den ONTAP tools for VMware vSphere 10 enthaltenen ONTAP REST-Rollen sind mehrere Aspekte zu beachten.

Rollenzuordnung

Unabhängig davon, ob eine herkömmliche oder eine REST-Rolle verwendet wird, werden alle ONTAP Zugriffsentscheidungen auf Grundlage des zugrunde liegenden CLI-Befehls getroffen. Da die Berechtigungen in einer REST-Rolle jedoch in Bezug auf die REST-API-Endpunkte definiert sind, muss ONTAP für jede der REST-Rollen eine *zugeordnete* traditionelle Rolle erstellen. Daher wird jede REST-Rolle einer zugrunde liegenden traditionellen Rolle zugeordnet. Dadurch kann ONTAP unabhängig vom Rollentyp konsistente Entscheidungen zur Zugriffskontrolle treffen. Sie können die parallel zugeordneten Rollen nicht ändern.

Definieren einer REST-Rolle mit CLI-Berechtigungen

Da ONTAP immer die CLI-Befehle verwendet, um den Zugriff auf einer Basisebene zu bestimmen, ist es möglich, eine REST-Rolle mithilfe von CLI-Befehlsberechtigungen anstelle von REST-Endpunkten auszudrücken. Ein Vorteil dieses Ansatzes ist die zusätzliche Granularität, die mit den herkömmlichen Rollen verfügbar ist.

Verwaltungsschnittstelle beim Definieren von ONTAP Rollen

Sie können Benutzer und Rollen mit der ONTAP CLI und der REST API erstellen. Es ist jedoch bequemer, die System Manager-Schnittstelle zusammen mit der JSON-Datei zu verwenden, die über den ONTAP Tools Manager verfügbar ist. Sehen "Verwenden Sie ONTAP RBAC mit ONTAP tools for VMware vSphere 10" für weitere Informationen.

Verwenden Sie ONTAP RBAC mit ONTAP tools for VMware vSphere 10

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

Übersicht über den Konfigurationsprozess

ONTAP tools for VMware vSphere 10 unterstützen die Erstellung eines ONTAP Benutzers mit einer benutzerdefinierten Rolle. Die Definitionen sind in einer JSON-Datei verpackt, die Sie in den ONTAP Cluster hochladen können. Sie können den Benutzer erstellen und die Rolle an Ihre Umgebung und Sicherheitsanforderungen anpassen.

Die wichtigsten Konfigurationsschritte werden unten ausführlich beschrieben. Siehe"Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen" für weitere Details.

1. Vorbereiten

Sie benötigen Administratoranmeldeinformationen sowohl für den ONTAP Tools Manager als auch für den ONTAP Cluster.

2. Laden Sie die JSON-Definitionsdatei herunter

Nachdem Sie sich bei der Benutzeroberfläche des ONTAP Tools Manager angemeldet haben, können Sie die JSON-Datei mit den RBAC-Definitionen herunterladen.

3. Erstellen Sie einen ONTAP -Benutzer mit einer Rolle

Nachdem Sie sich beim System Manager angemeldet haben, können Sie den Benutzer und die Rolle erstellen:

1. Wählen Sie links **Cluster** und dann **Einstellungen**.
2. Scrollen Sie nach unten zu **Benutzer und Rollen** und klicken Sie auf −→ .
3. Wählen Sie unter **Benutzer Hinzufügen** und wählen Sie **Virtualisierungsprodukte**.
4. Wählen Sie die JSON-Datei auf Ihrer lokalen Workstation aus und laden Sie sie hoch.

4. Konfigurieren der Rolle

Im Rahmen der Rollendefinition müssen Sie mehrere administrative Entscheidungen treffen. SehenKonfigurieren der Rolle mit System Manager für weitere Details.

Konfigurieren der Rolle mit System Manager

Nachdem Sie mit dem Erstellen eines neuen Benutzers und einer neuen Rolle mit System Manager begonnen und die JSON-Datei hochgeladen haben, können Sie die Rolle basierend auf Ihrer Umgebung und Ihren Anforderungen anpassen.

Grundlegende Benutzer- und Rollenkonfiguration

Die RBAC-Definitionen sind als mehrere Produktfunktionen verpackt, darunter Kombinationen aus VSC, VASA Provider und SRA. Sie sollten die Umgebung(en) auswählen, in denen Sie RBAC-Unterstützung benötigen. Wenn Sie beispielsweise möchten, dass Rollen die Remote-Plug-In-Funktion unterstützen, wählen Sie VSC aus. Außerdem müssen Sie den Benutzernamen und das zugehörige Passwort wählen.

Privileges

Die Rollenberechtigungen sind in vier Gruppen unterteilt, basierend auf der erforderlichen Zugriffsebene auf den ONTAP Speicher. Zu den den Rollen zugrunde liegenden Berechtigungen gehören:

- Entdeckung

  Mit dieser Rolle können Sie Speichersysteme hinzufügen.

- Speicher erstellen

  Mit dieser Rolle können Sie Speicher erstellen. Es umfasst auch alle mit der Discovery-Rolle verbundenen Berechtigungen.

- Speicher ändern

  Mit dieser Rolle können Sie den Speicher ändern. Es umfasst auch alle Berechtigungen, die mit den Rollen „Erkennen“ und „Speicher erstellen“ verbunden sind.

- Speicher zerstören

  Mit dieser Rolle können Sie Speicher zerstören. Es umfasst außerdem alle Berechtigungen, die mit der Erkennung, Speichererstellung und Speicheränderungsrollen verbunden sind.

Generieren Sie den Benutzer mit einer Rolle

Nachdem Sie die Konfigurationsoptionen für Ihre Umgebung ausgewählt haben, klicken Sie auf **Hinzufügen** und ONTAP erstellt 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 (z. B. „OTV_10“)
- Die von Ihnen 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.