RBAC mit ONTAP

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Inhalt

RBAC mit ONTAP

ONTAP RBAC-Umgebung mit ONTAP Tools für VMware vSphere 10

ONTAP bietet eine robuste und erweiterbare RBAC-Umgebung. Über die RBAC-Funktion kann der Zugriff auf Storage- und Systemvorgänge gesteuert werden, da diese über die REST-API und CLI offengelegt werden. Es ist besonders hilfreich, mit der Umgebung vertraut zu sein, bevor sie mit ONTAP Tools für die Implementierung von VMware vSphere 10 verwendet wird.

Überblick über die administrativen Optionen

Bei der Nutzung von ONTAP RBAC stehen Ihnen je nach Umgebung und Zielen verschiedene Optionen zur Verfügung. Im Folgenden wird ein Überblick über die wichtigsten Verwaltungsentscheidungen gegeben. Weitere Informationen finden Sie unter "ONTAP Automatisierung: Überblick über die RBAC-Sicherheit".

> RBAC von ONTAP ist auf eine Storage-Umgebung zugeschnitten und ist einfacher als die RBAC-Implementierung, die über vCenter Server zur Verfügung steht. Mit ONTAP weisen Sie dem Benutzer direkt eine Rolle zu. Die Konfiguration expliziter Berechtigungen, wie sie beispielsweise mit vCenter Server verwendet werden, ist für die ONTAP RBAC nicht erforderlich.

Rollen- und Privileges-Typen

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

- RUHE

  DIE REST-Funktionen wurden mit ONTAP 9.6 eingeführt und werden in der Regel für Benutzer angewendet, die über DIE REST-API auf ONTAP zugreifen. Die in diesen Rollen enthaltenen Privileges werden als Zugriff auf die ONTAP REST-API-Endpunkte und die zugehörigen Aktionen definiert.

- Traditionell

  Hierbei handelt es sich um die älteren Rollen, die vor ONTAP 9.6 enthalten sind. Sie sind weiterhin ein grundlegender Aspekt der RBAC. Die Privileges sind für den Zugriff auf die ONTAP-CLI-Befehle definiert.

Während die ÜBRIGEN Rollen in jüngster Zeit eingeführt wurden, haben die traditionellen Rollen einige Vorteile. So können optional zusätzliche Abfrageparameter einbezogen werden, damit die Privileges die Objekte genauer definieren, auf die sie angewendet werden.

Umfang

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

Rollendefinitionen

ONTAP bietet vordefinierte Rollen auf Cluster- und SVM-Ebene. Sie können auch benutzerdefinierte Rollen definieren.

Arbeiten mit ONTAP-REST-Rollen

Bei der Verwendung der in ONTAP Tools für VMware vSphere 10 enthaltenen ONTAP REST-Rollen müssen verschiedene Aspekte berücksichtigt werden.

Rollenzuordnung

Alle Entscheidungen für den ONTAP-Zugriff basierend auf dem zugrunde liegenden CLI-Befehl werden unabhängig davon getroffen, ob sie eine klassische Rolle oder eine REST-Rolle verwenden. Da die Privileges in einer REST-Rolle jedoch in Bezug auf die REST-API-Endpunkte definiert sind, muss ONTAP für jede der REST-Rollen eine traditionelle *Mapping* Rolle erstellen. Daher wird jede REST-Rolle einer zugrunde liegenden herkömmlichen Rolle zugeordnet. Dadurch kann ONTAP unabhängig vom Rollentyp Entscheidungen zur Zugriffssteuerung konsistent treffen. Sie können die parallel zugeordneten Rollen nicht ändern.

Definieren einer REST-Rolle mithilfe von CLI-Privileges

Da ONTAP immer die CLI-Befehle verwendet, um den Zugriff auf Basisebene zu bestimmen, kann eine REST-Rolle über den CLI-Befehl Privileges anstelle von REST-Endpunkten ausgedrückt werden. Ein Vorteil dieses Ansatzes ist die zusätzliche Granularität, die mit den herkömmlichen Rollen verfügbar ist.

Administratorschnittstelle beim Definieren von ONTAP-Rollen

Sie können Benutzer und Rollen mit der ONTAP-CLI und REST-API erstellen. Es empfiehlt sich jedoch, die Benutzeroberfläche von System Manager zusammen mit der JSON-Datei zu verwenden, die über den ONTAP Tools Manager verfügbar ist. Weitere Informationen finden Sie unter "Nutzen Sie die rollenbasierte Zugriffssteuerung von ONTAP mit ONTAP-Tools für VMware vSphere 10" .

Nutzen Sie die rollenbasierte Zugriffssteuerung von ONTAP mit ONTAP-Tools für VMware vSphere 10

Es gibt verschiedene Aspekte der ONTAP Tools für die Implementierung der rollenbasierten Zugriffssteuerung von VMware vSphere 10 mit ONTAP, die Sie vor dem Einsatz in einer Produktionsumgebung in Betracht ziehen sollten.

Überblick über den Konfigurationsprozess

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

Die wichtigsten Konfigurationsschritte werden auf einer der folgenden Ebenen beschrieben. "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen"Weitere Informationen finden Sie unter.

1. Vorbereiten

Sie müssen über Administratoranmeldeinformationen sowohl für den ONTAP Tools Manager als auch für den ONTAP Cluster verfügen.

2. Laden Sie die JSON-Definitionsdatei herunter

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

3. Erstellen Sie einen ONTAP-Benutzer mit einer Rolle

Nach der Anmeldung bei System Manager können Sie den Benutzer und die Rolle erstellen:

1. Wählen Sie **Cluster** auf der linken Seite und dann **Einstellungen**.
2. Scrollen Sie nach unten zu **Benutzer und Rollen** und klicken Sie auf −→.
3. Wählen Sie **Add** unter **Users** und wählen Sie **Virtualization products** aus.
4. Wählen Sie die JSON-Datei auf Ihrer lokalen Workstation aus, und laden Sie sie hoch.

4. Konfigurieren Sie die Rolle

Im Rahmen der Definition der Rolle müssen Sie mehrere administrative Entscheidungen treffen. Weitere Informationen finden Sie unterKonfigurieren Sie die Rolle mit System Manager.

Konfigurieren Sie die 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 auf Ihre Umgebung und Ihre Anforderungen abstimmen.

Konfiguration von Kernbenutzern und -Rollen

Die RBAC-Definitionen sind in Form von verschiedenen Produktfunktionen gebündelt, darunter Kombinationen von VSC, VASA Provider und SRA. Wählen Sie die Umgebung oder die Umgebungen aus, in denen die RBAC-Unterstützung benötigt wird. Wenn Rollen beispielsweise die Remote Plug-in-Funktion unterstützen sollen, wählen Sie VSC aus. Außerdem müssen Sie den Benutzernamen und das zugehörige Kennwort auswählen.

Berechtigungen

Die Rolle Privileges sind in vier Sets basierend auf der Zugriffsebene angeordnet, die für den ONTAP Storage erforderlich ist. Zu den Privileges, auf denen die Rollen basieren, gehören:

- Ermitteln

  Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.

- Storage erstellen

  Mit dieser Rolle können Sie Speicher erstellen. Er umfasst außerdem alle Privileges, die der Erkennungsrolle zugeordnet sind.

- Speicher ändern

  Mit dieser Rolle können Sie Speicher ändern. Er umfasst auch alle Privileges, die der Ermittlung zugeordnet sind und Storage-Rollen erstellen.

- Zerstören Sie den Speicher

  Mit dieser Rolle können Sie Speicher zerstören. Sie umfasst auch alle Privileges, die der Ermittlung zugeordnet sind, Speicher erstellen und Speicherrollen ändern.

Benutzer mit einer Rolle generieren

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:

- In der JSON-Datei definierter konstanter Präfixwert (z.B. „OTV_10“)
- 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.