RBAC-Sicherheit

ONTAP Automation

NetApp
July 19, 2024

Inhalt

RBAC-Sicherheit

Überblick über die RBAC-Sicherheit

ONTAP verfügt über eine robuste und erweiterbare Funktion zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC). Sie können jedem Konto eine eigene Rolle zuweisen, um den Zugriff des Benutzers auf die Ressourcen zu kontrollieren, die über DIE REST-API und die Rest-CLI offengelegt werden. Die Rollen definieren für verschiedene ONTAP Benutzer verschiedene Zugriffsebenen.

Die RBAC-Funktion von ONTAP wurde kontinuierlich erweitert und in ONTAP 9.11.1 (und nachfolgenden Versionen) deutlich verbessert. Weitere Informationen finden Sie unter "Zusammenfassung der Entwicklung der RBAC" und "Neuerungen bei der ONTAP REST-API" .

ONTAP Rollen

Eine Rolle ist eine Reihe von Berechtigungen, die kollektiv definieren, welche Aktionen der Benutzer ergreifen kann. Jede Berechtigung identifiziert einen bestimmten Zugriffspfad und die zugehörige Zugriffsebene. Rollen werden Benutzerkonten zugewiesen und von ONTAP bei Zugriffskontrollentscheidungen angewendet.

Rollentypen

Es gibt zwei Arten von Rollen. Sie wurden mit der Weiterentwicklung von ONTAP auf verschiedene Umgebungen eingeführt und angepasst.

Bei der Verwendung jeder Rollenart gibt es vor- und Nachteile. Siehe "Vergleichen der Rollentypen" Finden Sie weitere Informationen.

Typ	Beschreibung
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. Durch das Erstellen einer RUHEROLLE wird automatisch eine traditionelle *Mapping*-Rolle erzeugt.
Traditionell	Hierbei handelt es sich um die älteren Rollen, die vor ONTAP 9.6 enthalten sind. Sie wurden für die ONTAP CLI Umgebung eingeführt und sind weiterhin von grundlegender Bedeutung für die RBAC-Sicherheit.

Umfang

Jede Rolle hat einen Umfang oder Kontext, in dem sie definiert und angewendet wird. Der Umfang legt fest, wo und wie eine bestimmte Rolle verwendet wird.

ONTAP-Benutzerkonten haben einen ähnlichen Umfang und bestimmen, wie ein Benutzer definiert und verwendet wird.

Umfang	Beschreibung
Cluster	Rollen mit Clusterumfang werden auf ONTAP Cluster-Ebene definiert. Sie sind mit Benutzerkonten auf Cluster-Ebene verbunden.

Umfang	Beschreibung
SVM	Rollen mit SVM-Umfang werden für eine bestimmte Daten-SVM definiert. Sie sind Benutzerkonten in derselben SVM zugewiesen.

Quelle der Rollendefinitionen

Es gibt zwei Möglichkeiten, wie eine ONTAP-Rolle definiert werden kann.

Rollenquelle	Beschreibung
Individuell	Der ONTAP-Administrator kann benutzerdefinierte Rollen erstellen. Diese Rollen können an eine spezifische Umgebung und Sicherheitsanforderungen angepasst werden.
Integriert	Während individuelle Rollen für mehr Flexibilität sorgen, gibt es auch eine Reihe integrierter Rollen, die sowohl auf Cluster- als auch auf SVM-Ebene verfügbar sind. Diese Rollen sind vordefiniert und können für viele allgemeine administrative Aufgaben verwendet werden.

Rollenzuordnung und ONTAP-Verarbeitung

Abhängig von der verwendeten ONTAP Version werden alle oder fast alle REST-API-Aufrufe einem oder mehreren CLI-Befehlen zugeordnet. Wenn Sie eine RUDERROLLE erstellen, wird auch eine traditionelle oder ältere Rolle erstellt. Diese traditionelle **Mapping** Rolle basiert auf den entsprechenden CLI Befehlen und kann nicht manipuliert oder verändert werden.

Reverse Role Mapping wird nicht unterstützt. Das heißt, die Schaffung einer traditionellen Rolle schafft keine entsprechende RUHEROLLE.

Zusammenfassung der Entwicklung der RBAC

Die herkömmlichen Rollen sind bei allen Versionen von ONTAP 9 enthalten. DIE RESTLICHEN Rollen wurden später eingeführt und haben sich wie unten beschrieben weiterentwickelt.

ONTAP 9.6

DIE REST API wurde mit ONTAP 9.6 eingeführt. IN dieser Version wurden auch die REST-Rollen enthalten. Wenn Sie eine RUSTROLLE anlegen, wird auch eine entsprechende traditionelle Rolle erzeugt.

ONTAP 9.7 bis 9.10.1

Jede ONTAP Version von 9.7 bis 9.10.1 enthält Verbesserungen an DER REST API. So wurden beispielsweise jeder Version weitere REST-Endpunkte hinzugefügt. Die Erstellung und Verwaltung der beiden Rollentypen blieb jedoch getrennt. Zudem wurde in ONTAP 9.10.1 DIE REST-RBAC-Unterstützung für den Rest-Endpunkt von Snapshots hinzugefügt `/api/storage/volumes/{vol.uuid}/snapshots` Bei diesem Punkt handelt es sich um einen ressourcenqualifizierten Endpunkt.

ONTAP 9.11.1

Mit diesem Release wurde die Möglichkeit hinzugefügt, herkömmliche Rollen mit DER REST API zu konfigurieren und zu managen. Weitere Zugriffsebenen für DIE REST-Rollen wurden hinzugefügt.

Arbeiten Sie mit Rollen und Benutzern

Nachdem Sie die grundlegenden RBAC-Funktionen kennen, können Sie sofort mit den ONTAP Rollen und Benutzern arbeiten.

Siehe "RBAC-Workflows" Beispiele für das Erstellen und Verwenden von Rollen mit der ONTAP-REST-API

Administrativen Zugriff

Sie können die ONTAP Rollen über DIE REST-API oder die Befehlszeilenschnittstelle erstellen und managen. Die Zugriffsdetails sind unten beschrieben.

REST API

Es gibt verschiedene Endpunkte, die bei der Arbeit mit RBAC-Rollen und Benutzerkonten verwendet werden können. Die ersten vier in der Tabelle werden zum Erstellen und Verwalten der Rollen verwendet. Die letzten beiden werden zum Erstellen und Verwalten von Benutzerkonten verwendet.

Sie können online auf das ONTAP zugreifen "API-Referenz" Dokumentation Weitere Informationen einschließlich Beispiele für die Verwendung der API.

Endpunkt	Beschreibung
`/security/roles`	Mit diesem Endpunkt können Sie eine neue REST-Rolle erstellen. Ab ONTAP 9.11.1 können Sie auch eine traditionelle Rolle spielen. In diesem Fall bestimmt ONTAP den Rollentyp basierend auf den Eingabeparametern. Sie können auch eine Liste der definierten Rollen abrufen.
`/security/roles/{owner.UUID}/{name}`	Sie können eine bestimmte Cluster- oder SVM-Scoped-Rolle abrufen oder löschen. Der UUID-Wert gibt die SVM an, in der die Rolle definiert ist (Cluster oder Daten-SVM). Der Name ist der Name der Rolle.
`/security/roles/{owner.UUID}/{name}/privileges`	Mit diesem Endpunkt können Sie die Berechtigungen für eine bestimmte Rolle konfigurieren. Die eingebauten Rollen können abgerufen, aber nicht aktualisiert werden. Weitere Informationen finden Sie in der API-Referenzdokumentation für Ihre ONTAP Version.
`/security/roles/{owner.UUID}/{name}/privileges/[path]`	Sie können die Zugriffsebene und den optionalen Abfragewert für eine bestimmte Berechtigung abrufen, ändern und löschen. Weitere Informationen finden Sie in der API-Referenzdokumentation für Ihre ONTAP Version.
`/security/accounts`	Mit diesem Endpunkt können Sie ein neues Benutzerkonto im Umfang des Clusters oder der SVM erstellen. Es müssen mehrere Arten von Informationen enthalten oder anschließend hinzugefügt werden, bevor das Konto betriebsbereit ist. Sie können auch eine Liste der definierten Benutzerkonten abrufen.
`/security/accounts/{owner.UUID}/{name}`	Sie können ein bestimmtes Benutzerkonto mit Cluster oder SVM-Umfang abrufen, ändern und löschen. Der UUID-Wert gibt die SVM an, in der der Benutzer definiert ist (Cluster oder Daten-SVM). Der Name ist der Name des Kontos.

Befehlszeilenschnittstelle

Die entsprechenden ONTAP CLI Befehle werden im Folgenden beschrieben. Auf alle Befehle wird auf der Cluster-Ebene über ein Administratorkonto zugegriffen.

Befehl	Beschreibung
`security login`	Dies ist das Verzeichnis mit den Befehlen, die zum Erstellen und Verwalten einer Benutzeranmeldung benötigt werden.
`security login rest-role`	Dies ist das Verzeichnis mit den Befehlen, die zum Erstellen und Verwalten einer REST-Rolle benötigt werden, die einer Benutzeranmeldung zugeordnet ist.
`security login role`	Dies ist das Verzeichnis mit den Befehlen, die zum Erstellen und Managen einer traditionellen Rolle benötigt werden, die einer Benutzeranmeldung zugeordnet ist.

Rollendefinitionen

DIE REST- und traditionellen Rollen werden durch eine Reihe von Attributen definiert.

Eigentümer und Umfang

Eine Rolle kann im Besitz des ONTAP Clusters oder einer spezifischen Daten-SVM innerhalb des Clusters sein. Der Eigentümer bestimmt auch implizit den Umfang der Rolle.

Eindeutiger Name

Jede Rolle muss einen eindeutigen Namen in ihrem Geltungsbereich haben. Der Name einer Cluster-Rolle muss auf ONTAP Cluster-Ebene eindeutig sein, während die SVM-Rollen innerhalb der spezifischen SVM eindeutig sein müssen.

> Der Name einer neuen REST-Rolle muss sowohl unter DEN REST-Rollen als auch den traditionellen Rollen eindeutig sein. Das liegt daran, dass die Schaffung einer RUHEROLLE auch zu einer neuen traditionellen *Mapping* Rolle mit dem gleichen Namen führt.

Satz von Berechtigungen

Jede Rolle enthält einen Satz von mindestens einer Berechtigung. Jede Berechtigung identifiziert eine bestimmte Ressource oder einen bestimmten Befehl und die zugehörige Zugriffsebene.

Berechtigungen

Eine Rolle kann eine oder mehrere Berechtigungen enthalten. Jede Berechtigungsdefinition ist ein Tupel und legt die Zugriffsebene für eine bestimmte Ressource oder Operation fest.

Ressourcenpfad

Der Ressourcenpfad wird entweder als REST-Endpunkt oder als CLI-Befehl-/Befehlsverzeichnispfad identifiziert.

REST-Endpunkt

Ein API-Endpunkt hat die Zielressource für eine REST-Rolle identifiziert.

CLI-Befehl

Ein CLI-Befehl gibt das Ziel für eine herkömmliche Rolle an. Es kann auch ein Befehlsverzeichnis angegeben werden, das dann alle nachgelagerten Befehle in die ONTAP-CLI-Hierarchie enthält.

Zugangsstufe

Die Zugriffsebene definiert den Zugriffstyp, den die Rolle zum spezifischen Ressourcenpfad oder Befehl hat. Die Zugriffsebenen werden durch eine Reihe vordefinierter Schlüsselwörter identifiziert. Mit ONTAP 9.6 wurden drei Zugriffsebenen eingeführt. Sie können sowohl für traditionelle als auch FÜR REST-Rollen verwendet werden. Darüber hinaus haben ONTAP 9.11.1 drei neue Zugriffsebenen hinzugefügt. Diese neuen Zugriffsebenen können nur mit REST-Rollen verwendet werden.

Die Zugriffsebenen folgen dem CRUD-Modell. Bei REST basiert dies auf den primären HTTP-Methoden (POST, GET, PATCH, DELETE). Die entsprechenden CLI-Vorgänge werden im Allgemeinen den REST-Vorgängen zugeordnet (Erstellen, Anzeigen, Ändern, Löschen).

Zugangsstufe	RUHT primitives	Hinzugefügt	Nur RUSTFUNKTION
Keine	k. A.	9.6	Nein
readonly	GET	9.6	Nein
Alle	ABRUFEN, POSTEN, PATCHEN, LÖSCHEN	9.6	Nein
Read_create	GET, POST	9.11.1	Ja.
Lesen_ändern	GET, PATCH	9.11.1	Ja.
Lesen_create_modify	ABRUFEN, POST, PATCH	9.11.1	Ja.

Optionale Abfrage

Beim Erstellen einer traditionellen Rolle können Sie optional einen **query**-Wert angeben, um die Teilmenge der für das Befehlsverzeichnis oder das Befehlsverzeichnis relevanten Objekte zu identifizieren.

Zusammenfassung der integrierten Rollen

ONTAP enthält verschiedene vordefinierte Rollen, die Sie auf Cluster- oder SVM-Ebene verwenden können.

Cluster-Scoped-Rollen

Im Umfang des Clusters sind verschiedene integrierte Rollen verfügbar.

Siehe "Vordefinierte Rollen für Cluster-Administratoren" Finden Sie weitere Informationen.

Rolle	Beschreibung
Admin	Administratoren mit dieser Rolle haben uneingeschränkte Rechte und können alles im ONTAP-System tun. Sie können alle Ressourcen auf Cluster-Ebene und SVM-Ebene konfigurieren.
AutoSupport	Dies ist eine spezielle Rolle, die speziell auf das AutoSupport-Konto zugeschnitten ist.
Backup	Diese besondere Rolle für Backup-Software, die das System sichern muss.
SnapLock	Dies ist eine spezielle Rolle, die speziell auf das SnapLock-Konto zugeschnitten ist.

Rolle	Beschreibung
readonly	Administratoren mit dieser Rolle können sämtliche Daten auf Cluster-Ebene anzeigen, jedoch keine Änderungen vornehmen.
Keine	Es werden keine Administrationsfunktionen bereitgestellt.

SVM-Scoped-Rollen

Im Umfang der SVM sind verschiedene integrierte Rollen verfügbar. Der **vsadmin** bietet Zugriff auf die allgemeinsten und leistungsfähigsten Funktionen. Es gibt verschiedene zusätzliche Rollen, die auf bestimmte administrative Aufgaben zugeschnitten sind. Dazu zählen:

- Vsadmin-Volume
- Vsadmin-Protokoll
- Vsadmin-Backup
- Vsadmin-snaplock
- Vsadmin-Readonly

Siehe "Vordefinierte Rollen für SVM-Administratoren" Finden Sie weitere Informationen.

Vergleichen der Rollentypen

Bevor Sie eine **REST**-Rolle oder **traditionelle**-Rolle auswählen, sollten Sie sich der Unterschiede bewusst sein. Im Folgenden werden einige Möglichkeiten beschrieben, wie die beiden Rollentypen verglichen werden können.

Für erweiterte oder komplexere RBAC-Anwendungsfälle sollten Sie normalerweise eine herkömmliche Rolle verwenden.

Wie der Benutzer auf ONTAP zugreift

Vor dem Erstellen einer Rolle ist es wichtig zu wissen, wie der Benutzer auf das ONTAP-System zugreifen kann. Auf dieser Grundlage kann ein Rollentyp ermittelt werden.

Datenzugriff	Vorgeschlagener Typ
Nur REST API	DIE REST-Rolle wurde für die Verwendung mit DER REST-API konzipiert.
REST API UND CLI	Sie können eine RUHEROLLE definieren, die auch eine entsprechende traditionelle Rolle erzeugt.
Nur CLI	Sie können eine traditionelle Rolle erstellen.

Präzision des Zugriffspfads

Der für eine REST-Rolle definierte Zugriffspfad basiert auf einem REST-Endpunkt. Der Zugriffspfad für eine herkömmliche Rolle basiert auf einem CLI-Befehl oder einem Befehlsverzeichnis. Darüber hinaus können Sie einen optionalen Abfrageparameter mit einer traditionellen Rolle hinzufügen, um den Zugriff anhand der Befehlsparameter-Werte weiter zu beschränken.