RBAC

ONTAP Automation

NetApp
July 19, 2024

Inhalt

RBAC

Bereiten Sie die Verwendung von RBAC vor

Je nach Umgebung können Sie die RBAC-Funktion von ONTAP auf unterschiedliche Weise nutzen. In diesem Abschnitt werden einige gängige Szenarien als Workflows dargestellt. In jedem Fall liegt der Fokus auf einem spezifischen Sicherheits- und Verwaltungsziel.

Bevor Sie Rollen erstellen und einem ONTAP-Benutzerkonto eine Rolle zuweisen, sollten Sie die folgenden wichtigen Sicherheitsanforderungen und Optionen prüfen. Überprüfen Sie auch die allgemeinen Workflow-Konzepte unter "Die Nutzung der Workflows wird vorbereitet".

Welche ONTAP Version verwenden Sie?

Die ONTAP Version legt fest, welche REST-Endpunkte und RBAC-Funktionen verfügbar sind.

Ermittlung der geschützten Ressourcen und des Umfangs

Sie müssen die zu sichernden Ressourcen oder Befehle und den Umfang (Cluster oder SVM) festlegen.

Welchen Zugriff sollte der Benutzer haben?

Nachdem Sie die Ressourcen und den Umfang ermittelt haben, müssen Sie die zuzugeteilte Zugriffsebene festlegen.

Wie greifen die Benutzer auf ONTAP zu?

Der Benutzer kann über die REST-API oder über die CLI oder beide auf ONTAP zugreifen.

Ist eine der integrierten Rollen ausreichend oder wird eine benutzerdefinierte Rolle benötigt?

Es ist bequemer, eine vorhandene integrierte Rolle zu verwenden, aber Sie können bei Bedarf eine neue benutzerdefinierte Rolle erstellen.

Welche Art von Rolle ist erforderlich?

Basierend auf den Sicherheitsanforderungen und dem ONTAP-Zugriff müssen Sie entscheiden, ob eine REST- oder eine herkömmliche Rolle erstellt werden soll.

Erstellen Sie Rollen

Beschränkung des Zugriffs auf SVM-Volume-Vorgänge

Sie können eine Rolle definieren, um die Storage-Volume-Administration innerhalb einer SVM zu beschränken.

Informationen zu diesem Workflow

Eine herkömmliche Rolle wird zuerst erstellt, um zunächst den Zugriff auf alle wichtigen Volume-Administrationsfunktionen außer dem Klonen zu ermöglichen. Die Rolle wird mit folgenden Merkmalen definiert:

- Alle CRUD Volume-Vorgänge einschließlich get, create, modify und delete
- Volume-Klon kann nicht erstellt werden

Sie können dann optional die Rolle nach Bedarf aktualisieren. In diesem Workflow wird die Rolle im zweiten Schritt geändert, damit der Benutzer einen Volume-Klon erstellen kann.

Schritt 1: Erstellen Sie die Rolle

Sie können einen API-Aufruf ausgeben, um die RBAC-Rolle zu erstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      { "path": "volume create", "access": "all" },
      { "path": "volume delete", "access": "all" }
    ]
}
```

Schritt 2: Aktualisieren Sie die Rolle

Sie können einen API-Aufruf ausgeben, um die vorhandene Rolle zu aktualisieren.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Rollendefinition enthält.
„ROLE_NAME“ IN US-DOLLAR	Pfad	Ja.	Dies ist der Name der Rolle innerhalb der zu aktualisierenden SVM.

Beispiel für die Wellung

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "path": "volume clone",
  "access": "all"
}
```

Administration der Datensicherung

Sie können einem Benutzer begrenzte Datensicherungsfunktionen zur Verfügung stellen.

Informationen zu diesem Workflow

Die traditionelle erstellte Rolle wird mit den folgenden Merkmalen definiert:

- Es sind möglich, Snapshots zu erstellen und zu löschen und auch SnapMirror Beziehungen zu aktualisieren
- Objekte höherer Ebene wie Volumes oder SVMs können nicht erstellt oder geändert werden

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "volume snapshot create", "access": "all"},
      {"path": "volume snapshot delete", "access": "all"},
      {"path": "volume show", "access": "readonly"},
      {"path": "vserver show", "access": "readonly"},
      {"path": "snapmirror show", "access": "readonly"},
      {"path": "snapmirror update", "access": "all"}
  ]
}
```

Erstellung von ONTAP-Berichten zulassen

Sie können EINE REST-Rolle erstellen, um Benutzern die Möglichkeit zu geben, ONTAP-Berichte zu generieren.

Informationen zu diesem Workflow

Die erstellte Rolle wird mit folgenden Merkmalen definiert:

- Abrufen aller Kapazitäts- und Performance-Objektinformationen (u. a. Volume, qtree, LUN, Aggregate, Node, Und SnapMirror Beziehungen)
- Objekte höherer Ebene (wie Volumes oder SVMs) können nicht erstellt oder geändert werden.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api/storage/volumes", "access": "readonly"},
      {"path": "/api/storage/qtrees", "access": "readonly"},
      {"path": "/api/storage/luns", "access": "readonly"},
      {"path": "/api/storage/aggregates", "access": "readonly"},
      {"path": "/api/cluster/nodes", "access": "readonly"},
      {"path": "/api/snapmirror/relationships", "access": "readonly"},
      {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

Erstellen Sie einen Benutzer mit einer Rolle

Sie können diesen Workflow verwenden, um einen Benutzer mit einer zugeordneten REST-Rolle zu erstellen.

Informationen zu diesem Workflow

Dieser Workflow enthält die typischen Schritte, die zum Erstellen einer benutzerdefinierten REST-Rolle und ihrer Zuordnung zu einem neuen Benutzerkonto erforderlich sind. Sowohl der Benutzer als auch die Rolle haben einen Umfang der SVM und sind einer spezifischen Daten-SVM zugeordnet. Einige der Schritte können optional sein oder müssen je nach Umgebung geändert werden.

Schritt: Listen Sie die Daten-SVMs im Cluster auf

Führen Sie den folgenden REST-API-Aufruf durch, um die SVMs im Cluster aufzulisten. Die UUID und der Name jeder SVM werden in der Ausgabe angegeben.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/svm/svms

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Nachdem Sie fertig sind

Wählen Sie die gewünschte SVM aus der Liste aus, in der Sie den neuen Benutzer und die neue Rolle erstellen möchten.

Schritt 2: Auflisten der Benutzer, die für die SVM definiert wurden

Führen Sie den folgenden REST-API-Aufruf durch, um die in der ausgewählten SVM definierten Benutzer aufzulisten. Sie können die SVM über den Eigner-Parameter angeben.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Sicherheit/Konten

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Nachdem Sie fertig sind

Wählen Sie basierend auf den bereits in der SVM definierten Benutzern einen eindeutigen Namen für den neuen Benutzer aus.

Schritt 3: Listen Sie die REST-Rollen auf, die für die SVM definiert sind

Führen Sie den folgenden REST-API-Aufruf durch, um die in der ausgewählten SVM definierten Rollen aufzulisten. Sie können die SVM über den Eigner-Parameter angeben.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Nachdem Sie fertig sind

Wählen Sie basierend auf den in der SVM bereits definierten Rollen einen eindeutigen Namen für die neue Rolle aus.

Schritt 4: Erstellen Sie eine benutzerdefinierte REST-Rolle

Führen Sie den folgenden REST-API-Aufruf zur Erstellung einer benutzerdefinierten REST-Rolle in der SVM aus. Die Rolle hat zunächst nur eine Berechtigung, die einen Standardzugriff von **none** schafft, so dass der Zugriff verweigert wird.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api", "access": "none"},
  ]
}
```

Nachdem Sie fertig sind

Führen Sie optional Schritt 3 erneut aus, um die neue Rolle anzuzeigen. Sie können die Rollen auch in der ONTAP-CLI anzeigen.

Schritt 5: Aktualisieren Sie die Rolle, indem Sie weitere Berechtigungen hinzufügen

Führen Sie den folgenden REST-API-Aufruf durch, um die Rolle zu ändern, indem Sie nach Bedarf Berechtigungen hinzufügen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Rollen/{owner.UUID}/{Name}/Privileges

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Die UUID der SVM, die die Rollendefinition enthält.
„ROLE_NAME“ IN US-DOLLAR	Pfad	Ja.	Der Name der Rolle in der zu aktualisierenden SVM

Beispiel für die Wellung

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

Nachdem Sie fertig sind

Führen Sie optional Schritt 3 erneut aus, um die neue Rolle anzuzeigen. Sie können die Rollen auch in der ONTAP-CLI anzeigen.

Schritt 6: Erstellen Sie einen Benutzer

Führen Sie den folgenden REST-API-Aufruf zu einem Benutzerkonto erstellen aus. Die oben erstellte Rolle **dprole1** ist mit dem neuen Benutzer verknüpft.

Sie können den Benutzer ohne Rolle erstellen. In diesem Fall wird dem Benutzer eine Standardrolle zugewiesen (entweder `admin` Oder `vsadmin`) Je nachdem, ob der Benutzer mit Cluster oder SVM-Umfang definiert ist. Sie müssen den Benutzer ändern, um eine andere Rolle zuzuweisen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Konten

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "owner": {"uuid":"daf84055-248f-11ed-a23d-005056ac4fe6"},
  "name": "david",
  "applications": [
      {"application":"ssh",
       "authentication_methods":["password"],
       "second_authentication_method":"none"}
  ],
  "role":"dprole1",
  "password":"netapp123"
}
```

Nachdem Sie fertig sind

Sie können sich mit den Anmeldedaten für den neuen Benutzer bei der SVM-Managementoberfläche anmelden.