RBAC

ONTAP Automation

NetApp
July 19, 2024

Sommario

RBAC

Preparati all'utilizzo del RBAC

Puoi utilizzare la funzionalità RBAC di ONTAP in diversi modi a seconda dell'ambiente. In questa sezione vengono presentati alcuni scenari comuni come flussi di lavoro. In ogni caso, l'attenzione è rivolta a uno specifico obiettivo amministrativo e di protezione.

Prima di creare ruoli e assegnare un ruolo a un account utente ONTAP, è necessario prepararsi esaminando i principali requisiti e le opzioni di protezione presentati di seguito. Inoltre, verificare i concetti generali del flusso di lavoro all'indirizzo "Preparati a utilizzare i flussi di lavoro".

Quale versione di ONTAP stai utilizzando?

La release ONTAP determina quali endpoint REST e le funzionalità RBAC sono disponibili.

Identificare le risorse protette e l'ambito

È necessario identificare le risorse o i comandi da proteggere e l'ambito (cluster o SVM).

Quale accesso deve avere l'utente?

Dopo aver identificato le risorse e l'ambito, è necessario determinare il livello di accesso da concedere.

In che modo gli utenti accedono a ONTAP?

L'utente può accedere a ONTAP tramite l'API REST o CLI o entrambi.

Uno dei ruoli integrati è sufficiente o è necessario un ruolo personalizzato?

È più conveniente utilizzare un ruolo integrato esistente, ma è possibile creare un nuovo ruolo personalizzato, se necessario.

Che tipo di ruolo è necessario?

In base ai requisiti di sicurezza e all'accesso a ONTAP, è necessario scegliere se creare un ruolo REST o tradizionale.

Creare ruoli

Limitare l'accesso alle operazioni dei volumi SVM

Puoi definire un ruolo per limitare l'amministrazione del volume storage all'interno di una SVM.

Questo flusso di lavoro

Viene dapprima creato un ruolo tradizionale per consentire inizialmente l'accesso a tutte le principali funzioni di amministrazione dei volumi, ad eccezione del cloning. Il ruolo viene definito con le seguenti caratteristiche:

- È in grado di eseguire tutte le operazioni dei volumi CRUD, tra cui Get, create, Modify ed Delete
- Impossibile creare un clone del volume

È quindi possibile aggiornare il ruolo in base alle esigenze. In questo flusso di lavoro, il ruolo viene modificato nel secondo passaggio per consentire all'utente di creare un clone del volume.

Fase 1: Creare il ruolo

Puoi emettere una chiamata API per creare il ruolo RBAC.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

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

Passaggio 2: Aggiornare il ruolo

È possibile eseguire una chiamata API per aggiornare il ruolo esistente.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUID della SVM che contiene la definizione del ruolo.
$NOME_RUOLO	Percorso	Sì	Nome del ruolo all'interno della SVM da aggiornare.

Esempio di arricciamento

```
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
```

Esempio di input JSON

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

Attivare l'amministrazione della protezione dei dati

Puoi fornire a un utente funzionalità di protezione dei dati limitate.

Questo flusso di lavoro

Il ruolo tradizionale creato viene definito con le seguenti caratteristiche:

- Possibilità di creare ed eliminare snapshot e aggiornare le relazioni di SnapMirror
- Impossibile creare o modificare oggetti di livello superiore come volumi o SVM

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

```
{
  "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"}
  ]
}
```

Consente la generazione di rapporti ONTAP

È possibile creare un ruolo REST per fornire agli utenti la possibilità di generare report ONTAP.

Questo flusso di lavoro

Il ruolo creato viene definito con le seguenti caratteristiche:

- In grado di recuperare tutte le informazioni relative a capacità e performance (ad esempio volume, qtree, LUN, aggregati, nodo, E relazioni SnapMirror)
- Impossibile creare o modificare oggetti di livello superiore (ad esempio volumi o SVM)

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

```
{
  "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"}
  ]
}
```

Creare un utente con un ruolo

È possibile utilizzare questo flusso di lavoro per creare un utente con un ruolo REST associato.

Questo flusso di lavoro

Questo flusso di lavoro include i passaggi tipici necessari per creare un ruolo REST personalizzato e associarlo a un nuovo account utente. Sia l'utente che il ruolo hanno un ambito SVM e sono associati a un SVM di dati specifico. Alcuni passaggi possono essere opzionali o devono essere modificati a seconda dell'ambiente.

Fase 1: Elenco delle SVM di dati nel cluster

Eseguire la seguente chiamata API REST per elencare le SVM nel cluster. L'UUID e il nome di ciascuna SVM sono forniti nell'output.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/svm/svm

Esempio di arricciamento

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

Al termine

Selezionare la SVM desiderata dall'elenco in cui creare il nuovo utente e il nuovo ruolo.

Fase 2: Elencare gli utenti definiti nella SVM

Eseguire la seguente chiamata API REST per elencare gli utenti definiti nella SVM selezionata. È possibile identificare la SVM attraverso il parametro owner.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/accounts

Esempio di arricciamento

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

Al termine

In base agli utenti già definiti nella SVM, scegliere un nome univoco per il nuovo utente.

Fase 3: Elencare i ruoli REST definiti per la SVM

Eseguire la seguente chiamata API REST per elencare i ruoli definiti nella SVM selezionata. È possibile identificare la SVM attraverso il parametro owner.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/ruoli

Esempio di arricciamento

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

Al termine

In base ai ruoli già definiti nella SVM, scegliere un nome univoco per il nuovo ruolo.

Passaggio 4: Creare un ruolo REST personalizzato

Eseguire la seguente chiamata API REST per creare un ruolo REST personalizzato nella SVM. Il ruolo inizialmente dispone di un solo privilegio che stabilisce un accesso predefinito di **nessuno** in modo che tutti gli accessi siano negati.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

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

Al termine

Eseguire di nuovo il passaggio 3 per visualizzare il nuovo ruolo. È inoltre possibile visualizzare i ruoli nella CLI di ONTAP.

Passaggio 5: Aggiornare il ruolo aggiungendo ulteriori privilegi

Eseguire la seguente chiamata API REST per modificare il ruolo aggiungendo i privilegi necessari.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/roles/{owner.uuid}/{name}/privileges

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	L'UUID della SVM che contiene la definizione del ruolo.
$NOME_RUOLO	Percorso	Sì	Nome del ruolo all'interno della SVM da aggiornare.

Esempio di arricciamento

```
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
```

Esempio di input JSON

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

Al termine

Eseguire di nuovo il passaggio 3 per visualizzare il nuovo ruolo. È inoltre possibile visualizzare i ruoli nella CLI di ONTAP.

Passaggio 6: Creare un utente

Eseguire la seguente chiamata API REST per creare un account utente. Il ruolo **dprole1** creato in precedenza è associato al nuovo utente.

È possibile creare l'utente senza un ruolo. In questo caso, all'utente viene assegnato un ruolo predefinito (uno dei due `admin` oppure `vsadmin`) A seconda che l'utente sia definito con cluster o ambito SVM. Sarà necessario modificare l'utente per assegnare un ruolo diverso.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/accounts

Esempio di arricciamento

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

Esempio di input JSON

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

Al termine

È possibile accedere all'interfaccia di gestione SVM utilizzando le credenziali del nuovo utente.

Informazioni sul copyright

Informazioni sul marchio commerciale