RBAC

ONTAP automation

NetApp
January 18, 2026

Índice

RBAC . . . 1
- Prepare-se para usar o RBAC usando a API REST do ONTAP . . . 1
- Crie funções . . . 1
  - Limitar o acesso a operações de volume do SVM com a API REST do ONTAP . . . 1
  - Ative a administração da proteção de dados usando a API REST do ONTAP . . . 3
  - Permitir a geração de relatórios do ONTAP usando a API REST do ONTAP . . . 4
- Crie um usuário com uma função usando a API REST do ONTAP . . . 5
  - Etapa 1: Listar os SVMs de dados no cluster . . . 5
  - Etapa 2: Listar os usuários definidos para o SVM . . . 6
  - Etapa 3: Listar as funções REST definidas no SVM . . . 6
  - Passo 4: Crie uma FUNÇÃO REST personalizada . . . 7
  - Passo 5: Atualize a função adicionando mais Privileges . . . 8
  - Passo 6: Crie um usuário . . . 9

RBAC

Prepare-se para usar o RBAC usando a API REST do ONTAP

Você pode usar a funcionalidade RBAC do ONTAP de várias maneiras diferentes, dependendo do seu ambiente. Alguns cenários comuns são apresentados como fluxos de trabalho nesta seção. Em cada caso, o foco está em um objetivo específico de segurança e administração.

Antes de criar quaisquer funções e atribuir uma função a uma conta de usuário do ONTAP, você deve se preparar revisando os principais requisitos e opções de segurança apresentados abaixo. Certifique-se também de rever os conceitos gerais do fluxo de trabalho em "Prepare-se para usar os fluxos de trabalho".

Qual versão do ONTAP você está usando?

A versão do ONTAP determina quais endpoints REST e recursos RBAC estão disponíveis.

Identificar os recursos e o escopo protegidos

Você precisa identificar os recursos ou comandos a serem protegidos e o escopo (cluster ou SVM).

Que acesso o usuário deve ter?

Depois de identificar os recursos e o escopo, você precisa determinar o nível de acesso a ser concedido.

Como os usuários acessarão o ONTAP?

O usuário pode acessar o ONTAP por meio da API REST ou CLI ou ambos.

Uma das funções incorporadas é suficiente ou é necessária uma função personalizada?

É mais conveniente usar uma função integrada existente, mas você pode criar uma nova função personalizada, se necessário.

Que tipo de papel é necessário?

Com base nos requisitos de segurança e no acesso à ONTAP, você precisa escolher se deseja criar uma FUNÇÃO REST ou tradicional.

Crie funções

Limitar o acesso a operações de volume do SVM com a API REST do ONTAP

É possível definir uma função para restringir a administração de volumes de storage em uma SVM.

Sobre este fluxo de trabalho

Uma função tradicional é criada pela primeira vez para permitir o acesso a todas as principais funções de administração de volume, exceto a clonagem. A função é definida com as seguintes caraterísticas:

- Capaz de executar todas as operações de volume CRUD, incluindo obter, criar, modificar e excluir
- Não é possível criar um clone de volume

Você pode, então, opcionalmente, atualizar a função conforme necessário. Nesse fluxo de trabalho, a função é alterada na segunda etapa para permitir que o usuário crie um clone de volume.

Passo 1: Crie a função

Você pode emitir uma chamada de API para criar a função RBAC.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

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

Exemplo de entrada JSON

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

Passo 2: Atualize a função

Você pode emitir uma chamada de API para atualizar a função existente.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Parâmetros de entrada adicionais para exemplos curl

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados no exemplo curl nesta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
SVM_ID	Caminho	Sim	Este é o UUID do SVM que contém a definição de função.
NOME_FUNÇÃO	Caminho	Sim	Esse é o nome da função na SVM a ser atualizada.

Curl exemplo

```
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
```

Exemplo de entrada JSON

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

Ative a administração da proteção de dados usando a API REST do ONTAP

Você pode fornecer a um usuário recursos limitados de proteção de dados.

Sobre este fluxo de trabalho

O papel tradicional criado é definido com as seguintes caraterísticas:

- Capaz de criar e excluir snapshots, bem como atualizar relacionamentos do SnapMirror
- Não é possível criar ou modificar objetos de nível superior, como volumes ou SVMs

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

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

Exemplo de entrada 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"}
  ]
}
```

Permitir a geração de relatórios do ONTAP usando a API REST do ONTAP

Você pode criar uma FUNÇÃO REST para fornecer aos usuários a capacidade de gerar relatórios do ONTAP.

Sobre este fluxo de trabalho

A função criada é definida com as seguintes caraterísticas:

- Capaz de recuperar todas as informações de objetos de storage relacionadas à capacidade e performance (como volume, qtree, LUN, agregados, nó e relacionamentos SnapMirror)
- Não é possível criar ou modificar objetos de nível superior (como volumes ou SVMs)

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

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

Exemplo de entrada 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"}
  ]
}
```

Crie um usuário com uma função usando a API REST do ONTAP

Você pode usar esse fluxo de trabalho para criar um usuário com uma FUNÇÃO REST associada.

Sobre este fluxo de trabalho

Este fluxo de trabalho inclui as etapas típicas necessárias para criar uma FUNÇÃO REST personalizada e associá-la a uma nova conta de usuário. O usuário e a função têm um escopo do SVM e estão associados a um SVM de dados específico. Algumas das etapas podem ser opcionais ou precisam mudar dependendo do seu ambiente.

Etapa 1: Listar os SVMs de dados no cluster

Execute a seguinte chamada de API REST para listar os SVMs no cluster. O UUID e o nome de cada SVM são fornecidos na saída.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/svm/svms

Curl exemplo

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

Depois de terminar

Selecione o SVM desejado na lista onde você criará o novo usuário e a função.

Etapa 2: Listar os usuários definidos para o SVM

Execute a seguinte chamada à API REST para listar os usuários definidos no SVM selecionado. Você pode identificar o SVM por meio do parâmetro proprietário.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/security/accounts

Curl exemplo

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

Depois de terminar

Com base nos usuários já definidos no SVM, escolha um nome exclusivo para o novo usuário.

Etapa 3: Listar as funções REST definidas no SVM

Execute a seguinte chamada à API REST para listar as funções definidas no SVM selecionado. Você pode identificar o SVM por meio do parâmetro proprietário.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/security/roles

Curl exemplo

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

Depois de terminar

Com base nas funções já definidas no SVM, escolha um nome exclusivo para a nova função.

Passo 4: Crie uma FUNÇÃO REST personalizada

Execute a seguinte chamada de API REST para criar uma FUNÇÃO REST personalizada no SVM. A função inicialmente tem apenas um privilégio que estabelece um acesso padrão de **none** para que todo o acesso seja negado.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

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

Exemplo de entrada JSON

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

Depois de terminar

Opcionalmente, execute a etapa 3 novamente para exibir a nova função. Você também pode exibir as funções na CLI do ONTAP.

Passo 5: Atualize a função adicionando mais Privileges

Execute a seguinte chamada de API REST para modificar a função adicionando Privileges conforme necessário.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles/"owner.uuuid"//Privileges

Parâmetros de entrada adicionais para exemplos curl

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados no exemplo curl nesta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
SVM_ID	Caminho	Sim	UUID do SVM que contém a definição de função.
NOME_FUNÇÃO	Caminho	Sim	O nome da função no SVM a ser atualizado.

Curl exemplo

```
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
```

Exemplo de entrada JSON

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

Depois de terminar

Opcionalmente, execute a etapa 3 novamente para exibir a nova função. Você também pode exibir as funções na CLI do ONTAP.

Passo 6: Crie um usuário

Execute a seguinte chamada de API REST para criar uma conta de usuário. A função **dprole1** criada acima está associada ao novo usuário.

Você pode criar o usuário sem uma função. Nesse caso, é atribuída ao usuário uma função padrão (`admin`ou `vsadmin`), dependendo se o usuário está definido com escopo de cluster ou SVM. Você precisará modificar o usuário para atribuir uma função diferente.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/accounts

Curl exemplo

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

Exemplo de entrada JSON

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

Depois de terminar

Você pode fazer login na interface de gerenciamento do SVM usando as credenciais do novo usuário.

Informações sobre direitos autorais

Informações sobre marcas comerciais