RBAC

ONTAP Automation

NetApp
July 11, 2024

Tabla de contenidos

RBAC

Prepárese para el uso de RBAC

Es posible usar la funcionalidad de control de acceso basado en roles de ONTAP de varias formas diferentes, según el entorno. En esta sección se presentan algunos escenarios comunes como flujos de trabajo. En cada caso, el enfoque se centra en un objetivo administrativo y de seguridad específico.

Antes de crear cualquier rol y asignar un rol a una cuenta de usuario de ONTAP, debe prepararse revisando los requisitos y opciones de seguridad principales que se presentan a continuación. También asegúrese de revisar los conceptos generales del flujo de trabajo en "Prepárese para usar los flujos de trabajo".

¿Qué versión de ONTAP utiliza?

La versión de ONTAP determina qué extremos DE REST y las funciones RBAC están disponibles.

Identificar los recursos y el alcance protegidos

Debe identificar los recursos o comandos que se van a proteger y el alcance (clúster o SVM).

¿Qué acceso debería tener el usuario?

Después de identificar los recursos y el ámbito, debe determinar el nivel de acceso que se concederá.

¿Cómo accederán los usuarios a ONTAP?

El usuario puede acceder a ONTAP a través de la API de REST o la interfaz de línea de comandos o ambos.

¿Es suficiente uno de los roles integrados o se necesita un rol personalizado?

Es más conveniente utilizar una función integrada existente, pero se puede crear una nueva función personalizada si es necesario.

¿Qué tipo de rol es necesario?

En función de los requisitos de seguridad y del acceso a ONTAP, debe elegir si desea crear UN rol tradicional o DE REST.

Crear roles

Limite el acceso a las operaciones de volumen de SVM

Puede definir un rol para restringir la administración de volúmenes de almacenamiento dentro de una SVM.

Acerca de este flujo de trabajo

Se crea en primer lugar un rol tradicional para permitir inicialmente el acceso a todas las funciones principales de administración de volúmenes, excepto la clonación. El rol se define con las siguientes características:

- Es capaz de realizar todas las operaciones de volumen CRUD, incluidos Get, CREATE, Modify y DELETE
- No se puede crear un clon de volumen

A continuación, puede actualizar opcionalmente el rol según sea necesario. En este flujo de trabajo, se cambia el rol en el segundo paso para que el usuario pueda crear un clon de volumen.

Paso 1: Crear el rol

Puede emitir una llamada API para crear el rol de RBAC.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

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

Ejemplo 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" }
    ]
}
```

Paso 2: Actualice el rol

Puede emitir una llamada API para actualizar el rol existente.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene la definición de rol.
$ROLE_NAME	Ruta	Sí	Es el nombre del rol dentro de la SVM que se va a actualizar.

Ejemplo de curl

```
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
```

Ejemplo de entrada JSON

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

Permita la administración de la protección de datos

Puede proporcionar a un usuario funcionalidades de protección de datos limitadas.

Acerca de este flujo de trabajo

El rol tradicional creado se define con las siguientes características:

- Es posible crear y eliminar copias Snapshot, así como actualizar las relaciones de SnapMirror
- No se pueden crear ni modificar objetos de nivel superior como volúmenes o SVM

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

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

Ejemplo 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 la generación de informes de ONTAP

Puede crear un rol DE REST para proporcionar a los usuarios la capacidad de generar informes de ONTAP.

Acerca de este flujo de trabajo

El rol creado se define con las siguientes características:

- Se puede recuperar toda la información sobre objetos de almacenamiento relacionada con la capacidad y el rendimiento (como volumen, qtree, LUN, agregados, nodo, Y las relaciones de SnapMirror)
- No se pueden crear ni modificar objetos de nivel superior (como volúmenes o SVM).

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

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

Ejemplo 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"}
  ]
}
```

Crear un usuario con un rol

Es posible utilizar este flujo de trabajo para crear un usuario con un rol DE REST asociado.

Acerca de este flujo de trabajo

Este flujo de trabajo incluye los pasos típicos necesarios para crear un rol REST personalizado y asociarlo con una nueva cuenta de usuario. Tanto el usuario como el rol tienen un ámbito de SVM y están asociados con una SVM de datos específica. Es posible que algunos de los pasos sean opcionales o que deban cambiar según tu entorno.

Paso 1: Enumere las SVM de datos en el clúster

Realice la siguiente llamada de API REST para enumerar las SVM en el clúster. El UUID y el nombre de cada SVM se proporcionan en la salida.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/svm/svm

Ejemplo de curl

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

Después de terminar

Seleccione la SVM deseada en la lista donde va a crear el usuario y el rol nuevos.

Paso 2: Enumere los usuarios definidos para la SVM

Realice la siguiente llamada de API de REST para enumerar los usuarios definidos en la SVM seleccionada. Se puede identificar la SVM mediante el parámetro owner.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/seguridad/cuentas

Ejemplo de curl

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

Después de terminar

Según los usuarios ya definidos en la SVM, elija un nombre único para el nuevo usuario.

Paso 3: Enumera los roles REST definidos para la SVM

Realice la siguiente llamada de API de REST para enumerar los roles definidos en la SVM seleccionada. Se puede identificar la SVM mediante el parámetro owner.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/seguridad/roles

Ejemplo de curl

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

Después de terminar

Según los roles ya definidos en la SVM, elija un nombre único para el nuevo rol.

Paso 4: Crear un rol REST personalizado

Realice la siguiente llamada de API DE REST para crear un rol de REST personalizado en la SVM. El rol tiene inicialmente sólo un privilegio que establece un acceso por defecto de **ninguno** para que se deniegue todo acceso.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

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

Ejemplo de entrada JSON

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

Después de terminar

De manera opcional, vuelva a ejecutar el paso 3 para mostrar el nuevo rol. También puede mostrar los roles en la interfaz de línea de comandos de ONTAP.

Paso 5: Actualice el rol agregando más privilegios

Realice la siguiente llamada a la API de REST para modificar el rol, añadiendo privilegios según sea necesario.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles/{owner.uuid}/{name}/privilegios

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	El UUID de la SVM que contiene la definición de rol.
$ROLE_NAME	Ruta	Sí	El nombre del rol dentro de la SVM que se va a actualizar.

Ejemplo de curl

```
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
```

Ejemplo de entrada JSON

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

Después de terminar

De manera opcional, vuelva a ejecutar el paso 3 para mostrar el nuevo rol. También puede mostrar los roles en la interfaz de línea de comandos de ONTAP.

Paso 6: Crear un usuario

Realice la siguiente llamada a la API DE REST para crear una cuenta de usuario. El rol **dprole1** creado arriba está asociado con el nuevo usuario.

Es posible crear el usuario sin un rol. En este caso, se asigna al usuario un rol predeterminado (ya sea `admin` o. `vsadmin`) En función de si el usuario está definido con el ámbito del clúster o de SVM. Tendrás que modificar el usuario para asignar un rol diferente.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/cuentas

Ejemplo de curl

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

Ejemplo 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":"netapp123"
}
```

Después de terminar

Puede iniciar sesión en la interfaz de gestión de SVM con las credenciales del nuevo usuario.

Información de copyright

Información de la marca comercial