Créer des rôles

ONTAP automation

NetApp
January 18, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-automation/workflows/wf_rbac_role_limit_svm.html on January 18, 2026. Always check docs.netapp.com for the latest.

Sommaire

Créer des rôles . . . 1
Limitez l'accès aux opérations du volume du SVM à l'aide de l'API REST ONTAP . . . 1
Étape 1 : créer le rôle . . . 1
Étape 2 : mettez à jour le rôle . . . 2
Activez l'administration de la protection des données à l'aide de l'API REST ONTAP . . . 3
Autoriser la génération de rapports ONTAP à l'aide de l'API REST ONTAP . . . 4

Créer des rôles

Limitez l’accès aux opérations du volume du SVM à l’aide de l’API REST ONTAP

Vous pouvez définir un rôle de restriction de l’administration des volumes de stockage au sein d’une SVM.

A propos de ce flux de travail

Un rôle traditionnel est d’abord créé pour autoriser initialement l’accès à toutes les principales fonctions d’administration des volumes, à l’exception du clonage. Le rôle est défini avec les caractéristiques suivantes :

- Possibilité d’effectuer toutes les opérations de volume CRUD, y compris obtenir, créer, modifier et supprimer
- Impossible de créer un clone de volume

Vous pouvez ensuite, si nécessaire, mettre à jour le rôle. Dans ce workflow, le rôle est modifié dans la deuxième étape pour permettre à l’utilisateur de créer un clone de volume.

Étape 1 : créer le rôle

Vous pouvez émettre un appel d’API pour créer le rôle RBAC.

Méthode HTTP et noeud final

Cet appel d’API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/sécurité/rôles

Exemple de boucle

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

Exemple d'entrée JSON

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

Étape 2 : mettez à jour le rôle

Vous pouvez émettre un appel API pour mettre à jour le rôle existant.

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/sécurité/rôles

Paramètres d'entrée supplémentaires pour les exemples de boucles

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans l'exemple curl de cette étape.

Paramètre	Type	Obligatoire	Description
$SVM_ID	Chemin	Oui.	Il s'agit de l'UUID du SVM qui contient la définition du rôle.
$NOM_RÔLE	Chemin	Oui.	Voici le nom du rôle au sein de la SVM à mettre à jour.

Exemple de boucle

```
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
```

Exemple d'entrée JSON

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

Activez l'administration de la protection des données à l'aide de l'API REST ONTAP

Vous pouvez offrir à un utilisateur des fonctionnalités de protection des données limitées.

A propos de ce flux de travail

Le rôle traditionnel créé est défini avec les caractéristiques suivantes :

- Création et suppression de snapshots et mise à jour des relations SnapMirror
- Ne peut créer ou modifier des objets de niveau supérieur tels que des volumes ou des SVM

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/sécurité/rôles

Exemple de boucle

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

Exemple d'entrée 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"}
  ]
}
```

Autoriser la génération de rapports ONTAP à l'aide de l'API REST ONTAP

Vous pouvez créer un rôle REST pour permettre aux utilisateurs de générer des rapports ONTAP.

A propos de ce flux de travail

Le rôle créé est défini avec les caractéristiques suivantes :

- Possibilité de récupérer toutes les informations relatives à la capacité et aux performances de l'objet de stockage (par exemple, volume, qtree, LUN, agrégats, nœud, Et relations SnapMirror)
- Ne peut créer ni modifier des objets de niveau supérieur (tels que des volumes ou des SVM)

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/sécurité/rôles

Exemple de boucle

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

Exemple d'entrée 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"}
  ]
}
```

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.