# Gestion des rôles de contrôle d'accès

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/authentication/manage-access-control-roles-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

# Sommaire

# Gestion des rôles de contrôle d'accès

## Gérer la présentation des rôles de contrôle d'accès

Le rôle attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

## Modifiez le rôle attribué à un administrateur

Vous pouvez utiliser le `security login modify` Commande pour modifier le rôle d'un compte d'administrateur de cluster ou de SVM. Vous pouvez affecter un rôle prédéfini ou personnalisé.

**Avant de commencer**

Vous devez être un administrateur de cluster pour effectuer cette tâche.

**Étape**

1. Modifier le rôle d'un administrateur de cluster ou de SVM :

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   "Création ou modification de comptes de connexion"

   La commande suivante permet de changer le rôle du compte d'administrateur du cluster AD `DOMAIN1\guest1` au prédéfini `readonly` rôle.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   La commande suivante permet de changer le rôle des comptes administrateur du SVM dans le compte AD group `DOMAIN1\adgroup` au personnalisé `vol_role` rôle.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

## Définissez des rôles personnalisés

Vous pouvez utiliser le `security login role create` commande pour définir un rôle personnalisé. Vous pouvez exécuter la commande autant de fois que nécessaire pour

obtenir la combinaison exacte de fonctions que vous souhaitez associer au rôle.

**Description de la tâche**

- Un rôle, qu'il soit prédéfini ou personnalisé, accorde ou refuse l'accès aux commandes ou aux répertoires de commandes ONTAP.

  Un répertoire de commande (`volume`, par exemple) est un groupe de commandes et de sous-répertoires de commandes associés. Sauf comme décrit dans cette procédure, l'octroi ou le refus de l'accès à un répertoire de commandes accorde ou refuse l'accès à chaque commande du répertoire et de ses sous-répertoires.

- L'accès aux commandes ou aux sous-répertoires spécifiques remplace l'accès au répertoire parent.

  Si un rôle est défini à l'aide d'un répertoire de commandes, puis qu'il est défini à nouveau avec un niveau d'accès différent pour une commande spécifique ou pour un sous-répertoire du répertoire parent, le niveau d'accès spécifié pour la commande ou le sous-répertoire remplace celui du parent.

> Vous ne pouvez pas attribuer un administrateur SVM un rôle qui donne accès à une commande ou au répertoire de commande disponible uniquement pour le `admin` administrateur du cluster --par exemple, le `security` répertoire de commande.

**Avant de commencer**

Vous devez être un administrateur de cluster pour effectuer cette tâche.

**Étape**

1. Définissez un rôle personnalisé :

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   Les commandes suivantes permettent d'accorder le `vol_role` rôle accès complet aux commandes dans `volume` le répertoire de commande et l'accès en lecture seule aux commandes de l' `volume snapshot` sous-répertoire.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   Les commandes suivantes permettent d'accorder le `SVM_storage` accès en lecture seule du rôle aux commandes dans `storage` répertoire de commandes, pas d'accès aux commandes dans le `storage encryption` sous-répertoire et accès complet au `storage aggregate plex offline` commande non intrinsèque.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

## Rôles prédéfinis pour les administrateurs du cluster

Les rôles prédéfinis des administrateurs du cluster doivent répondre à la plupart des besoins. Vous pouvez créer des rôles personnalisés selon vos besoins. Par défaut un administrateur de cluster se voit attribuer le paramétrage prédéfini `admin` rôle.

Le tableau suivant répertorie les rôles prédéfinis pour les administrateurs du cluster :

| Ce rôle… | Dispose de ce niveau d'accès… | Aux commandes ou répertoires de commandes suivants |
|---|---|---|
| admin | tous | Tous les répertoires de commandes (`DEFAULT`) |
| admin-no-fsa (disponible à partir de ONTAP 9.12.1) | Lecture/écriture | • Tous les répertoires de commandes (`DEFAULT`)<br>• `security login rest-role`<br>• `security login role` |

| | | |
|---|---|---|
| Lecture seule | • security login rest-role create<br>• security login rest-role delete<br>• security login rest-role modify<br>• security login rest-role show<br>• security login role create<br>• security login role create<br>• security login role delete<br>• security login role modify<br>• security login role show<br>• volume activity-tracking<br>• volume analytics | Aucune |
| volume file show-disk-usage | AutoSupport | tous |
| • set<br>• system node autosupport | Aucune | Tous les autres répertoires de commandes (DEFAULT) |
| sauvegarde | tous | vserver services ndmp |
| lecture seule | volume | Aucune |
| Tous les autres répertoires de commandes (DEFAULT) | lecture seule | tous |
| • security login password<br>Pour la gestion du mot de passe local et des informations clés du compte utilisateur<br>• set | Aucune | security |

| | | |
|---|---|---|
| lecture seule | Tous les autres répertoires de commandes (`DEFAULT`) | Aucune |

> Le `autosupport` le rôle est affecté au prédéfini `autosupport` Compte, utilisé par AutoSupport OnDemand. ONTAP vous empêche de modifier ou de supprimer le `autosupport` compte. ONTAP vous empêche également d'attribuer le `autosupport` rôle vers d'autres comptes utilisateur.

# Rôles prédéfinis pour les administrateurs des SVM

Les rôles prédéfinis des administrateurs des SVM devraient répondre à la plupart des besoins. Vous pouvez créer des rôles personnalisés selon vos besoins. Par défault un administrateur SVM est affecté au prédéfini `vsadmin` rôle.

Le tableau suivant répertorie les rôles prédéfinis pour les administrateurs du SVM :

| Nom du rôle | Capacités |
|---|---|
| vsadmin | • Gestion du mot de passe local et des informations clés du compte utilisateur<br>• Gestion des volumes, à l'exception des déplacements de volumes<br>• Gestion des quotas, des qtrees, des copies Snapshot et des fichiers<br>• Gestion des LUN<br>• Exécution d'opérations SnapLock, sauf suppression privilégiée<br>• Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP<br>• Configuration des services : DNS, LDAP et NIS<br>• Surveillance des tâches<br>• Surveillance des connexions réseau et de l'interface réseau<br>• Contrôle de l'état de santé de la SVM |

| | |
|---|---|
| volume vsadmin | • Gestion du mot de passe local et des informations clés du compte utilisateur<br>• Gestion des volumes, y compris les déplacements de volumes<br>• Gestion des quotas, des qtrees, des copies Snapshot et des fichiers<br>• Gestion des LUN<br>• Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP<br>• Configuration des services : DNS, LDAP et NIS<br>• Surveillance de l'interface réseau<br>• Contrôle de l'état de santé de la SVM |
| protocole vsadmin | • Gestion du mot de passe local et des informations clés du compte utilisateur<br>• Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP<br>• Configuration des services : DNS, LDAP et NIS<br>• Gestion des LUN<br>• Surveillance de l'interface réseau<br>• Contrôle de l'état de santé de la SVM |
| sauvegarde vsadmin | • Gestion du mot de passe local et des informations clés du compte utilisateur<br>• Gestion des opérations NDMP<br>• Opérations de lecture/écriture d'un volume restauré<br>• Gestion des relations SnapMirror et des copies Snapshot<br>• Affichage des volumes et des informations réseau |

| | |
|---|---|
| vsadmin-snaplock | • Gestion du mot de passe local et des informations clés du compte utilisateur<br>• Gestion des volumes, à l'exception des déplacements de volumes<br>• Gestion des quotas, des qtrees, des copies Snapshot et des fichiers<br>• Exécution d'opérations SnapLock, y compris la suppression privilégiée<br>• Configuration des protocoles : NFS et SMB<br>• Configuration des services : DNS, LDAP et NIS<br>• Surveillance des tâches<br>• Surveillance des connexions réseau et de l'interface réseau |
| vsadmin-readdisponible | • Gestion du mot de passe local et des informations clés du compte utilisateur<br>• Contrôle de l'état de santé de la SVM<br>• Surveillance de l'interface réseau<br>• Affichage des volumes et des LUN<br>• Affichage des services et protocoles |

# Contrôlez l'accès administrateur

Le rôle attribué à un administrateur détermine les fonctions que l'administrateur peut exécuter avec System Manager. Les rôles prédéfinis pour les administrateurs du cluster et des VM de stockage sont fournis par System Manager. Vous attribuez le rôle lorsque vous créez le compte de l'administrateur ou vous pouvez lui attribuer un autre rôle ultérieurement.

En fonction de la manière dont vous avez activé l'accès au compte, vous devrez peut-être effectuer l'une des opérations suivantes :

- Associer une clé publique à un compte local.
- Installez un certificat numérique de serveur signé par une autorité de certification.
- Configuration de l'accès AD, LDAP ou NIS.

Vous pouvez effectuer ces tâches avant ou après l'activation de l'accès au compte.

## Attribution d'un rôle à un administrateur

Attribuez un rôle à un administrateur, comme suit :

**Étapes**

1. Sélectionnez **Cluster > Paramètres**.

2. Sélectionnez → À côté de **utilisateurs et rôles**.
3. Sélectionnez + Add Sous **utilisateurs**.
4. Spécifiez un nom d'utilisateur et sélectionnez un rôle dans le menu déroulant pour **role**.
5. Spécifiez une méthode de connexion et un mot de passe pour l'utilisateur.

## Modification du rôle d'un administrateur

Modifiez le rôle d'un administrateur comme suit :

### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Sélectionnez le nom de l'utilisateur dont vous souhaitez modifier le rôle, puis cliquez sur le bouton ⋮ s'affiche en regard du nom d'utilisateur.
3. Cliquez sur **Modifier**.
4. Sélectionnez un rôle dans le menu déroulant pour **role**.

**Informations sur le copyright**

Copyright © 2024 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.