Configuration du contrôle d'accès basé sur des rôles (RBAC)

SnapCenter Software 4.7

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-47/install/task_add_a_user_or_group_and_assign_role_and_assets.html on January 18, 2024. Always check docs.netapp.com for the latest.

Sommaire

Configuration du contrôle d’accès basé sur des rôles (RBAC) 1
Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources 1
Créer un rôle 4
Ajoutez un rôle RBAC ONTAP à l’aide des commandes de connexion de sécurité 5
Créez des rôles de SVM avec des privilèges minimaux 6
Créez des rôles de cluster ONTAP avec des privilèges minimaux 11
Configurez les pools d’applications IIS pour activer les autorisations de lecture d’Active Directory 17

Configuration du contrôle d’accès basé sur des rôles (RBAC)

Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources

Pour configurer le contrôle d’accès basé sur des rôles pour les utilisateurs SnapCenter, vous pouvez ajouter des utilisateurs ou des groupes et attribuer un rôle. Le rôle détermine les options auxquelles les utilisateurs de SnapCenter peuvent accéder.

Ce dont vous aurez besoin

- Vous devez avoir ouvert une session en tant que rôle « SnapCenterAdmin ».
- Vous devez avoir créé les comptes utilisateur ou groupe dans Active Directory dans le système d’exploitation ou la base de données. Vous ne pouvez pas utiliser SnapCenter pour créer ces comptes.

> À partir de SnapCenter 4.5, vous ne pouvez inclure que les caractères spéciaux suivants dans les noms d’utilisateur et de groupe : espace ( ), tiret (-), trait de soulignement (_) et deux-points (:). Si vous souhaitez utiliser un rôle que vous avez créé dans une version antérieure de SnapCenter avec ces caractères spéciaux, vous pouvez désactiver la validation du nom de rôle en changeant la valeur du paramètre 'disableSQLInjectionvalidation' à true dans le fichier web.config situé dans lequel se trouve la WebApp SnapCenter. Après avoir modifié la valeur, vous n’avez pas besoin de redémarrer le service.

- SnapCenter inclut plusieurs rôles prédéfinis.

  Vous pouvez soit attribuer ces rôles à l’utilisateur, soit créer de nouveaux rôles.

- Les utilisateurs AD et les groupes AD qui sont ajoutés au RBAC SnapCenter doivent disposer de l’autorisation DE LECTURE sur le conteneur d’utilisateurs et le conteneur d’ordinateurs dans Active Directory.
- Après avoir affecté un rôle à un utilisateur ou à un groupe qui contient les autorisations appropriées, vous devez attribuer l’accès de l’utilisateur aux ressources SnapCenter, telles que les hôtes et les connexions de stockage.

  Cela permet aux utilisateurs d’effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

- Vous devez à un moment ou à un autre attribuer un rôle à l’utilisateur ou au groupe afin de tirer profit des autorisations et des fonctionnalités d’efficacité RBAC.
- Vous pouvez affecter des ressources comme hôte, groupes de ressources, stratégie, connexion au stockage, plug-in, et les informations d’identification à l’utilisateur lors de la création de l’utilisateur ou du groupe.
- Les ressources minimales que vous devez affecter à un utilisateur pour effectuer certaines opérations sont les suivantes :

Fonctionnement	Affectation des ressources
Protéger les ressources	hôte, règle
Sauvegarde	hôte, groupe de ressources, stratégie
Restaurer	hôte, groupe de ressources
Clonage	hôte, groupe de ressources, stratégie
Cycle de vie des clones	hôte
Créer un groupe de ressources	hôte

- Lorsqu'un nouveau nœud est ajouté à un cluster Windows ou à un actif DAG (Groupe de disponibilité de la base de données Exchange Server) et si ce nouveau nœud est affecté à un utilisateur, vous devez réassigner le bien à l'utilisateur ou au groupe pour inclure le nouveau nœud à l'utilisateur ou au groupe.

  Vous devez réassigner l'utilisateur ou le groupe RBAC au cluster ou au DAG pour inclure le nouveau nœud à l'utilisateur ou au groupe RBAC. Par exemple, vous avez un cluster à deux nœuds et avez affecté un utilisateur ou un groupe RBAC au cluster. Lorsque vous ajoutez un autre nœud au cluster, vous devez réattribuer l'utilisateur ou le groupe RBAC au cluster afin d'inclure le nouveau nœud pour l'utilisateur ou le groupe RBAC.

- Si vous prévoyez de répliquer des copies Snapshot, vous devez attribuer la connexion de stockage aux volumes source et de destination à l'utilisateur effectuant l'opération.

  Vous devez ajouter des ressources avant d'attribuer l'accès aux utilisateurs.

> Si vous utilisez le plug-in SnapCenter pour les fonctions VMware vSphere pour protéger les machines virtuelles, les VMDK ou les datastores, vous devez utiliser l'interface graphique de VMware vSphere pour ajouter un utilisateur vCenter à un rôle de plug-in SnapCenter pour VMware vSphere. Pour plus d'informations sur les rôles VMware vSphere, reportez-vous à la section "Rôles prédéfinis avec le plug-in SnapCenter pour VMware vSphere".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **utilisateurs et accès** > +.
3. Dans la page Ajouter des utilisateurs/groupes à partir d'Active Directory ou Workgroup :

Pour ce champ…	Procédez comme ça…
Type d'accès	Sélectionnez domaine ou groupe de travail Pour le type d'authentification de domaine, vous devez spécifier le nom de domaine de l'utilisateur ou du groupe auquel vous souhaitez ajouter l'utilisateur à un rôle. Par défaut, il est pré-rempli avec le nom de domaine connecté. Vous devez enregistrer le domaine non approuvé dans la page **Paramètres** > **Paramètres globaux** > **Paramètres de domaine**.
Type	Sélectionnez utilisateur ou Groupe SnapCenter prend uniquement en charge le groupe de sécurité, et non le groupe de distribution.
Nom d'utilisateur	a. Saisissez le nom d'utilisateur partiel, puis cliquez sur **Ajouter**. Le nom d'utilisateur est sensible à la casse. b. Sélectionnez le nom d'utilisateur dans la liste de recherche. Lorsque vous ajoutez des utilisateurs d'un domaine différent ou d'un domaine non fiable, vous devez saisir le nom d'utilisateur entièrement car il n'existe aucune liste de recherche pour les utilisateurs d'un domaine à l'autre. Répétez cette étape pour ajouter d'autres utilisateurs ou groupes au rôle sélectionné.
Rôles	Sélectionnez le rôle auquel vous souhaitez ajouter l'utilisateur.

4. Cliquez sur **attribuer**, puis sur la page affecter des ressources :
   a. Sélectionnez le type de ressource dans la liste déroulante **Asset**.
   b. Dans le tableau actif, sélectionnez l'actif.

Les ressources sont répertoriées uniquement si l'utilisateur a ajouté les ressources à SnapCenter.

c. Répétez cette procédure pour tous les actifs requis.

d. Cliquez sur **Enregistrer**.

5. Cliquez sur **soumettre**.

Après avoir ajouté des utilisateurs ou des groupes et affecté des rôles, actualisez la liste des ressources.

Créer un rôle

En plus d'utiliser les rôles SnapCenter existants, vous pouvez créer vos propres rôles et personnaliser les autorisations.

Vous devriez avoir ouvert une session en tant que rôle « SnapCenterAdmin ».

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **rôles**.
3. Cliquez sur +.
4. Dans la page Ajouter un rôle, spécifiez un nom et une description pour le nouveau rôle.

> À partir de SnapCenter 4.5, vous ne pouvez inclure que les caractères spéciaux suivants dans les noms d'utilisateur et de groupe : espace ( ), tiret (-), trait de soulignement (_) et deux-points (:). Si vous souhaitez utiliser un rôle que vous avez créé dans une version antérieure de SnapCenter avec ces caractères spéciaux, vous pouvez désactiver la validation du nom de rôle en changeant la valeur du paramètre 'disableSQLInjectionvalidation' à true dans le fichier web.config situé dans lequel se trouve la WebApp SnapCenter. Après avoir modifié la valeur, vous n'avez pas besoin de redémarrer le service.

5. Select **tous les membres de ce rôle peuvent voir les objets d'autres membres** pour permettre aux autres membres du rôle d'afficher les ressources telles que les volumes et les hôtes après avoir actualisé la liste des ressources.

   Vous devez désélectionner cette option si vous ne souhaitez pas que les membres de ce rôle voient les objets auxquels les autres membres sont affectés.

> Lorsque cette option est activée, il n'est pas nécessaire d'attribuer aux utilisateurs un accès aux objets ou aux ressources si les utilisateurs appartiennent au même rôle que l'utilisateur qui a créé les objets ou les ressources.

6. Dans la page autorisations, sélectionnez les autorisations que vous souhaitez attribuer au rôle ou cliquez sur **Sélectionner tout** pour accorder toutes les autorisations au rôle.
7. Cliquez sur **soumettre**.

Ajoutez un rôle RBAC ONTAP à l'aide des commandes de connexion de sécurité

Vous pouvez utiliser les commandes de connexion de sécurité pour ajouter un rôle RBAC ONTAP lorsque vos systèmes de stockage exécutent clustered ONTAP.

Ce dont vous aurez besoin

- Avant de créer un rôle RBAC ONTAP pour les systèmes de stockage exécutant clustered ONTAP, vous devez identifier les éléments suivants :
  - La ou les tâches que vous souhaitez effectuer
  - Privilèges requis pour effectuer ces tâches
- Pour configurer un rôle RBAC, vous devez effectuer les actions suivantes :
  - Accorder des privilèges aux répertoires de commandes et/ou de commandes.

    Il existe deux niveaux d'accès pour chaque répertoire de commande/commande : All-Access et read-only.

  Vous devez toujours attribuer les privilèges All-Access en premier.

  - Attribuez des rôles aux utilisateurs.
  - Varier votre configuration selon que vos plug-ins SnapCenter sont connectés à l'IP d'administration du cluster pour tout le cluster ou directement connectés à un SVM au sein du cluster.

À propos de cette tâche

Pour simplifier la configuration de ces rôles sur les systèmes de stockage, vous pouvez utiliser l'outil RBAC utilisateur Creator pour Data ONTAP, disponible sur le forum des communautés NetApp.

Cet outil gère automatiquement la configuration correcte des privilèges ONTAP. Par exemple, l'outil Créateur d'utilisateurs RBAC pour Data ONTAP ajoute automatiquement les privilèges dans le bon ordre afin que les privilèges All-Access s'affichent en premier. Si vous ajoutez d'abord les privilèges en lecture seule, puis ajoutez les privilèges All-Access, ONTAP marque les privilèges All-Access en tant que doublons et les ignore.

> Si vous mettez à niveau SnapCenter ou ONTAP ultérieurement, vous devez exécuter à nouveau l'outil Créateur d'utilisateurs RBAC pour Data ONTAP afin de mettre à jour les rôles utilisateur que vous avez créés précédemment. Les rôles utilisateur créés pour une version antérieure de SnapCenter ou ONTAP ne fonctionnent pas correctement avec les versions mises à niveau. Lorsque vous exécutez de nouveau l'outil, il gère automatiquement la mise à niveau. Il n'est pas nécessaire de recréer les rôles.

Plus d'informations sur la configuration des rôles RBAC ONTAP, consultez le "Guide de l'authentification de l'administrateur ONTAP 9 et de l'alimentation RBAC".

> Dans un souci de cohérence, la documentation SnapCenter fait référence aux rôles en tant qu'utilisation des privilèges. L'interface graphique du Gestionnaire système OnCommand utilise le terme *attribute* au lieu de *Privilege*. Lors de la configuration de rôles RBAC ONTAP, ces deux termes désignent la même chose.

Étapes

1. Sur le système de stockage, créez un nouveau rôle en entrant la commande suivante :

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - svm_name est le nom du SVM. Si vous ne renseignez pas ce champ, l'administrateur de cluster est défini par défaut.
   - nom_rôle est le nom que vous spécifiez pour le rôle.
   - La commande correspond à la fonctionnalité ONTAP.

   > Vous devez répéter cette commande pour chaque autorisation. N'oubliez pas que les commandes All-Access doivent être répertoriées avant les commandes read-only.

   Pour plus d'informations sur la liste des autorisations, reportez-vous à la section "Commandes CLI ONTAP pour la création de rôles et l'attribution d'autorisations".

2. Créez un nom d'utilisateur en entrant la commande suivante :

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - nom_utilisateur est le nom de l'utilisateur que vous créez.
   - <password> est votre mot de passe. Si vous ne spécifiez pas de mot de passe, le système vous en demandera un.
   - svm_name est le nom du SVM.

3. Attribuez ce rôle à l'utilisateur en entrant la commande suivante :

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod <password\>
   ```

   - <nom_utilisateur> est le nom de l'utilisateur que vous avez créé à l'étape 2. Cette commande vous permet de modifier l'utilisateur pour l'associer au rôle.
   - <svm_name> est le nom du SVM.
   - <nom_rôle> est le nom du rôle que vous avez créé à l'étape 1.
   - <password> est votre mot de passe. Si vous ne spécifiez pas de mot de passe, le système vous en demandera un.

4. Vérifiez que l'utilisateur a été créé correctement en entrant la commande suivante :

   ```
   security login show -vserver <svm_name\> -user-or-group-name <user_name\>
   ```

   Nom_utilisateur est le nom de l'utilisateur que vous avez créé à l'étape 3.

Créez des rôles de SVM avec des privilèges minimaux

Il existe plusieurs commandes CLI ONTAP que vous devez exécuter lorsque vous créez un rôle pour un nouvel utilisateur SVM dans ONTAP. Ce rôle est requis si vous configurez des SVM dans ONTAP pour qu'ils soient utilisés avec SnapCenter et que vous ne

souhaitez pas utiliser le rôle vsadmin.

Étapes

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez-lui le rôle.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   ontapi -authmethod password -role <SVM_Role_Name\>
   ```

3. Déverrouiller l'utilisateur.

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

Commandes CLI ONTAP pour créer des rôles SVM et attribuer des autorisations

Vous devez exécuter plusieurs commandes ONTAP CLI pour créer des rôles SVM et attribuer des autorisations.

- `security login role create -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -vserver SVM_Name -access all`
- `security login role create -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -vserver SVM_Name -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun igroup rename" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname “volume managed-feature” -access all`

Créez des rôles de cluster ONTAP avec des privilèges minimaux

Vous devez créer un rôle de cluster ONTAP avec des privilèges minimaux afin de ne pas avoir à utiliser le rôle d’administrateur ONTAP pour effectuer des opérations dans SnapCenter. Vous pouvez exécuter plusieurs commandes de l’interface de ligne de commandes ONTAP pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

Étapes

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez-lui le rôle.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi -authmethod password -role <role_name\>
   ```

3. Déverrouiller l’utilisateur.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

Commandes CLI ONTAP permettant de créer des rôles de cluster et d’attribuer des autorisations

Vous devez exécuter plusieurs commandes CLI ONTAP pour créer des rôles de cluster et attribuer des autorisations.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"cluster modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"snapmirror policy show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"vserver" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

Configurez les pools d’applications IIS pour activer les autorisations de lecture d’Active Directory

Vous pouvez configurer IIS (Internet information Services) sur votre serveur Windows pour créer un compte de pool d’applications personnalisé lorsque vous devez activer les autorisations de lecture Active Directory pour SnapCenter.

Étapes

1. Ouvrez le Gestionnaire IIS sur le serveur Windows sur lequel SnapCenter est installé.
2. Dans le volet de navigation de gauche, cliquez sur **pools d’applications**.
3. Sélectionnez SnapCenter dans la liste pools d’applications, puis cliquez sur **Paramètres avancés** dans le volet actions.
4. Sélectionnez identité, puis cliquez sur **…** pour modifier l’identité du pool d’applications SnapCenter.
5. Dans le champ compte personnalisé, entrez un nom d’utilisateur de domaine ou de compte d’administrateur de domaine avec l’autorisation de lecture Active Directory.
6. Cliquez sur OK.

   Le compte personnalisé remplace le compte ApplicationPoolIdentity intégré pour le pool d’applications SnapCenter.

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.