Contrôle d'accès basé sur des rôles (RBAC) SnapCenter

SnapCenter Software 4.8

NetApp
January 18, 2024

Sommaire

Contrôle d’accès basé sur des rôles (RBAC) SnapCenter

Types de RBAC

Le contrôle d’accès basé sur des rôles (RBAC) SnapCenter et les autorisations ONTAP permettent aux administrateurs SnapCenter de déléguer le contrôle des ressources SnapCenter à différents utilisateurs ou groupes d’utilisateurs. Cet accès géré de manière centralisée permet aux administrateurs d’applications de travailler en toute sécurité dans les environnements délégués.

Vous pouvez créer et modifier des rôles, ajouter un accès aux ressources aux utilisateurs à tout moment, mais lorsque vous configurez SnapCenter pour la première fois, vous devez ajouter au moins des utilisateurs ou des groupes Active Directory aux rôles, puis ajouter un accès aux ressources à ces utilisateurs ou groupes.

> Vous ne pouvez pas utiliser SnapCenter pour créer des comptes d’utilisateur ou de groupe. Vous devez créer des comptes d’utilisateur ou de groupe dans Active Directory du système d’exploitation ou de la base de données.

SnapCenter utilise les types suivants de contrôle d’accès basé sur les rôles :

- RBAC SnapCenter
- Plug-in RBAC SnapCenter (pour certains plug-ins)
- RBAC au niveau des applications
- Autorisations ONTAP

RBAC SnapCenter

Rôles et autorisations

SnapCenter propose des rôles prédéfinis avec des autorisations déjà attribuées. Vous pouvez affecter des utilisateurs ou des groupes d’utilisateurs à ces rôles. Vous pouvez également créer de nouveaux rôles et gérer les autorisations et les utilisateurs.

Affectation d’autorisations aux utilisateurs ou aux groupes

Vous pouvez attribuer des autorisations aux utilisateurs ou aux groupes pour accéder aux objets SnapCenter tels que les hôtes, les connexions de stockage et les groupes de ressources. Vous ne pouvez pas modifier les autorisations du rôle SnapCenterAdmin.

Vous pouvez attribuer des autorisations RBAC aux utilisateurs et groupes au sein de la même forêt et aux utilisateurs appartenant à différentes forêts. Vous ne pouvez pas attribuer d’autorisations RBAC aux utilisateurs appartenant à des groupes imbriqués dans les forêts.

> Si vous créez un rôle personnalisé, il doit contenir toutes les autorisations du rôle d’administrateur SnapCenter. Si vous copiez uniquement certaines autorisations, par exemple, l’ajout ou le retrait d’hôte, vous ne pouvez pas effectuer ces opérations.

Authentification

Les utilisateurs doivent fournir une authentification lors de la connexion, via l'interface utilisateur graphique ou via les applets de commande PowerShell. Si les utilisateurs sont membres de plusieurs rôles, après avoir saisi des informations d'identification, ils sont invités à spécifier le rôle qu'ils souhaitent utiliser. Les utilisateurs doivent également fournir une authentification pour l'exécution des API.

RBAC au niveau des applications

SnapCenter utilise les identifiants pour vérifier que les utilisateurs SnapCenter autorisés disposent également des autorisations au niveau de l'application.

Par exemple, si vous souhaitez effectuer des opérations de copie Snapshot et de protection des données dans un environnement SQL Server, vous devez définir des identifiants avec les identifiants Windows ou SQL appropriés. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une ou l'autre méthode. Pour effectuer des opérations de copie Snapshot et de protection des données dans un environnement de système de fichiers Windows sur un système de stockage ONTAP, le rôle d'administrateur SnapCenter doit disposer de privilèges d'administration sur l'hôte Windows.

De même, si vous souhaitez effectuer des opérations de protection des données sur une base de données Oracle et si l'authentification du système d'exploitation est désactivée dans l'hôte de la base de données, vous devez définir les informations d'identification avec la base de données Oracle ou les informations d'identification Oracle ASM. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une de ces méthodes, en fonction de l'opération.

Plug-in SnapCenter pour VMware vSphere RBAC

Si vous utilisez le plug-in SnapCenter pour la protection de données cohérente avec les machines virtuelles, vCenter Server offre un niveau supplémentaire de contrôle d'accès basé sur des rôles (RBAC). Le plug-in SnapCenter prend en charge le RBAC de vCenter Server et le RBAC d'Data ONTAP.

Pour plus d'informations, reportez-vous à la section "Plug-in SnapCenter pour VMware vSphere RBAC"

Autorisations ONTAP

Vous devez créer un compte vsadmin avec les autorisations requises pour accéder au système de stockage

Pour plus d'informations sur la création du compte et l'attribution des autorisations, reportez-vous à la section "Créez un rôle de cluster ONTAP avec des privilèges minimaux"

Autorisations et rôles RBAC

Le contrôle d'accès basé sur des rôles (RBAC) SnapCenter vous permet de créer des rôles et d'attribuer des autorisations à ces rôles, puis d'attribuer des utilisateurs ou des groupes d'utilisateurs aux rôles. Les administrateurs SnapCenter peuvent ainsi créer un environnement géré de manière centralisée, tandis que les administrateurs d'applications peuvent gérer les tâches de protection des données. SnapCenter propose des rôles et des autorisations prédéfinis.

Rôles SnapCenter

SnapCenter propose les rôles prédéfinis suivants. Vous pouvez attribuer des utilisateurs et des groupes à ces rôles ou créer de nouveaux rôles.

Lorsque vous attribuez un rôle à un utilisateur, seuls les travaux pertinents à cet utilisateur sont visibles dans la page travaux, à moins que vous n'ayez affecté le rôle d'administrateur SnapCenter.

- Admin sauvegarde et clonage d'applications
- Sauvegardez et clonez Viewer
- Administrateur de l'infrastructure
- SnapCenter

Le plug-in SnapCenter pour les rôles VMware vSphere

Pour gérer la protection des données cohérente avec les machines virtuelles des machines virtuelles, des VMDK et des datastores, les rôles suivants sont créés dans vCenter par le plug-in SnapCenter pour VMware vSphere :

- Administrateur de distributeurs sélectifs
- Vue du distributeur auxiliaire
- Secours du distributeur auxiliaire
- Restauration du distributeur auxiliaire
- Restauration du fichier invité du distributeur auxiliaire

Pour plus d'informations, voir "Types de RBAC pour le plug-in SnapCenter pour les utilisateurs VMware vSphere"

Meilleure pratique : NetApp vous recommande de créer un rôle ONTAP pour les opérations du plug-in SnapCenter pour VMware vSphere et de lui attribuer tous les privilèges requis.

Autorisations SnapCenter

SnapCenter offre les autorisations suivantes :

- Groupe de ressources
- Politique
- Sauvegarde
- Hôte
- Connexion de stockage
- Clonage
- Provisionnement (uniquement pour la base de données Microsoft SQL)
- Tableau de bord
- Rapports
- Restaurer
    - Restauration du volume complet (uniquement pour les plug-ins personnalisés)

- Ressource

  Les privilèges de plug-in sont requis de la part de l'administrateur pour que les non-administrateurs puissent effectuer une opération de découverte des ressources.

- Installation ou désinstallation du plug-in

  Lorsque vous activez les autorisations d'installation du plug-in, vous devez également modifier l'autorisation Host pour activer les lectures et les mises à jour.

- Migration
- Montage (uniquement pour la base de données Oracle)
- Démonter (uniquement pour la base de données Oracle)
- Moniteur de tâche

  L'autorisation moniteur de tâches permet aux membres de différents rôles de voir les opérations sur tous les objets auxquels ils sont affectés.

Rôles et autorisations SnapCenter prédéfinis

SnapCenter propose des rôles prédéfinis, chacun avec un ensemble d'autorisations déjà activé. Lors de la configuration et de l'administration du contrôle d'accès basé sur des rôles (RBAC), vous pouvez utiliser ces rôles prédéfinis ou en créer de nouveaux.

SnapCenter inclut les rôles prédéfinis suivants :

- Rôle d'administrateur SnapCenter
- Rôle d'administrateur de clones et de sauvegarde des applications
- Rôle Backup and Clone Viewer
- Rôle d'administrateur de l'infrastructure

Lorsque vous ajoutez un utilisateur à un rôle, vous devez attribuer l'autorisation StorageConnection pour activer la communication SVM (Storage Virtual machine) ou affecter un SVM à l'utilisateur pour permettre l'utilisation de la SVM. L'autorisation Storage Connection permet aux utilisateurs de créer des connexions SVM.

Par exemple, un utilisateur avec le rôle administrateur SnapCenter peut créer des connexions SVM et les affecter à un utilisateur avec le rôle Administrateur App Backup and Clone, qui par défaut n'a pas la permission de créer ou de modifier des connexions SVM. Sans connexion SVM, les utilisateurs ne peuvent pas mener à bien les opérations de sauvegarde, de clonage ou de restauration.

Rôle d'administrateur SnapCenter

Toutes les autorisations sont activées pour le rôle d'administrateur SnapCenter. Vous ne pouvez pas modifier les autorisations pour ce rôle. Vous pouvez ajouter des utilisateurs et des groupes au rôle ou les supprimer.

Rôle d'administrateur de clones et de sauvegarde des applications

Le rôle d'administrateur d'applications et de clones dispose des autorisations nécessaires pour effectuer des

actions administratives pour les sauvegardes d'applications et les tâches liées au clonage. Ce rôle ne dispose pas des autorisations nécessaires pour la gestion des hôtes, le provisionnement, la gestion des connexions de stockage ou l'installation à distance.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Oui.	Oui.	Oui.	Oui.
Politique	Sans objet	Oui.	Oui.	Oui.	Oui.
Sauvegarde	Sans objet	Oui.	Oui.	Oui.	Oui.
Hôte	Sans objet	Oui.	Oui.	Oui.	Oui.
Connexion de stockage	Sans objet	Non	Oui.	Non	Non
Clonage	Sans objet	Oui.	Oui.	Oui.	Oui.
Provisionnement	Sans objet	Non	Oui.	Non	Non
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Installation/désinstallation du plug-in	Non	Sans objet		Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Oui.	Oui.	Sans objet	Sans objet	Sans objet
Démonter	Oui.	Oui.	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Non	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Rôle Backup and Clone Viewer

Le rôle de la visionneuse de sauvegarde et de clonage dispose d'une vue en lecture seule de toutes les autorisations. Ce rôle est également doté d'autorisations pour la découverte, le reporting et l'accès au Tableau de bord.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Non	Oui.	Non	Non
Politique	Sans objet	Non	Oui.	Non	Non
Sauvegarde	Sans objet	Non	Oui.	Non	Non
Hôte	Sans objet	Non	Oui.	Non	Non
Connexion de stockage	Sans objet	Non	Oui.	Non	Non
Clonage	Sans objet	Non	Oui.	Non	Non
Provisionnement	Sans objet	Non	Oui.	Non	Non
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Non	Non	Sans objet	Sans objet	Sans objet
Ressource	Non	Non	Oui.	Oui.	Non
Installation/désinstallation du plug-in	Non	Sans objet	Sans objet	Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Démonter	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Sans objet	Sans objet	Sans objet	Sans objet

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Rôle d’administrateur de l’infrastructure

Le rôle d’administrateur de l’infrastructure possède des autorisations pour la gestion des hôtes, la gestion du stockage, le provisionnement, les groupes de ressources, les rapports d’installation à distance, Et l’accès au Tableau de bord.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Oui.	Oui.	Oui.	Oui.
Politique	Sans objet	Non	Oui.	Oui.	Oui.
Sauvegarde	Sans objet	Oui.	Oui.	Oui.	Oui.
Hôte	Sans objet	Oui.	Oui.	Oui.	Oui.
Connexion de stockage	Sans objet	Oui.	Oui.	Oui.	Oui.
Clonage	Sans objet	Non	Oui.	Non	Non
Provisionnement	Sans objet	Oui.	Oui.	Oui.	Oui.
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Installation/désinstallation du plug-in	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Non	Sans objet	Sans objet	Sans objet	Sans objet
Démonter	Non	Sans objet	Sans objet	Sans objet	Sans objet

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Restauration complète du volume	Non	Non	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet