Sécurité RBAC

ONTAP automation

NetApp
January 13, 2026

Sommaire

Sécurité RBAC

Présentation de la sécurité RBAC avec l'API REST ONTAP

ONTAP inclut des fonctionnalités robustes et évolutives de contrôle d'accès basé sur des rôles (RBAC). Vous pouvez attribuer chaque compte un rôle différent afin de contrôler l'accès de l'utilisateur aux ressources exposées via l'API REST et l'interface de ligne de commande. Les rôles définissent les différents niveaux d'accès administratif des différents utilisateurs ONTAP.

La fonction RBAC d'ONTAP s'est poursuivie et a été considérablement améliorée grâce à ONTAP 9.11.1 (et aux versions suivantes). Voir "Résumé de l'évolution du RBAC" et "Nouveautés de l'API REST ONTAP" pour plus d'informations.

Rôles ONTAP

Un rôle est un ensemble de privilèges qui définissent collectivement les actions que l'utilisateur peut effectuer. Chaque privilège identifie un chemin d'accès spécifique et le niveau d'accès associé. Les rôles sont attribués aux comptes utilisateur et appliqués par ONTAP lors de décisions de contrôle d'accès.

Types de rôles

Il existe deux types de rôles. Elles ont été introduites et adaptées à différents environnements, comme ONTAP a évolué.

Il y a des avantages et des inconvénients lors de l'utilisation de chaque type de rôle. Voir "Comparaison des types de rôle" pour en savoir plus.

Type	Description
REPOS	Les rôles REST ont été introduits avec ONTAP 9.6 et sont généralement appliqués aux utilisateurs qui accèdent à ONTAP via l'API REST. La création d'un rôle REST crée automatiquement un rôle *mapping* traditionnel.
Traditionnel	Il s'agit des rôles hérités inclus avant ONTAP 9.6. Elles ont été ajoutées à l'environnement CLI d'ONTAP et continuent d'être essentielles à la sécurité du RBAC.

Portée

Chaque rôle a une portée ou un contexte dans lequel il est défini et appliqué. Le périmètre détermine où et comment un rôle spécifique est utilisé.

Les comptes utilisateur ONTAP ont également un périmètre similaire qui détermine la façon dont un utilisateur est défini et utilisé.

Portée	Description
Cluster	Les rôles ayant une étendue du cluster sont définis au niveau du cluster ONTAP. Ils sont associés aux comptes utilisateur au niveau du cluster.

Portée	Description
SVM	Les rôles ayant une portée SVM sont définis pour une SVM de données spécifique. Ils sont affectés aux comptes utilisateurs dans la même SVM.

Source des définitions de rôle

Il existe deux façons de définir un rôle ONTAP.

Source du rôle	Description
Personnalisées	L'administrateur ONTAP peut créer des rôles personnalisés. Ces rôles peuvent être adaptés à un environnement spécifique et à des exigences de sécurité spécifiques.
Intégrée	Bien que les rôles personnalisés offrent davantage de flexibilité, il existe également un ensemble de rôles intégrés disponibles au niveau du cluster et des SVM. Ces rôles sont prédéfinis et peuvent être utilisés pour de nombreuses tâches administratives courantes.

Mapping de rôles et traitement ONTAP

Selon la version de ONTAP que vous utilisez, tous ou presque tous les appels de l'API REST sont redirigés vers une ou plusieurs commandes de l'interface de ligne de commande. Lorsque vous créez un rôle DE REPOS, un rôle traditionnel ou hérité est également créé. Ce rôle traditionnel **mappé** est basé sur les commandes CLI correspondantes et ne peut pas être manipulé ni modifié.

Le mappage de rôle inverse n'est pas pris en charge. C'est-à-dire que la création d'un rôle traditionnel ne crée pas de rôle DE REPOS correspondant.

Résumé de l'évolution du RBAC

Ces rôles sont inclus dans toutes les versions de ONTAP 9. Les rôles DE REPOS ont été introduits plus tard et ont évolué comme décrit ci-dessous.

ONTAP 9.6

L'API REST a été introduite avec ONTAP 9.6. Les rôles DE REPOS étaient également inclus dans cette version. De plus, lorsque vous créez un rôle DE REPOS, un rôle traditionnel correspondant est également créé.

ONTAP 9.7 à 9.10.1

Chaque version de ONTAP de 9.7 à 9.10.1 inclut des améliorations de l'API REST. Par exemple, des terminaux REST supplémentaires ont été ajoutés à chaque version. Toutefois, la création et la gestion des deux types de rôles sont demeurées distinctes. Par ailleurs, ONTAP 9.10.1 a ajouté LA prise en charge du RBAC REST pour le terminal REST de snapshots `/api/storage/volumes/{vol.uuid}/snapshots` qui est un noeud final qualifié de ressource.

ONTAP 9.11.1

La possibilité de configurer et de gérer les rôles classiques à l'aide de l'API REST a été ajoutée avec cette version. Des niveaux d'accès supplémentaires pour LES rôles REST ont également été ajoutés.

Utilisation des rôles et des utilisateurs dans l'API REST ONTAP

Une fois que vous avez compris les fonctionnalités RBAC de base, vous pouvez commencer à travailler avec les rôles et les utilisateurs ONTAP.

Voir "Workflows RBAC" Le fournit des exemples de création et d'utilisation de rôles avec l'API REST ONTAP.

Accès administratif

Vous pouvez créer et gérer des rôles ONTAP via l'API REST ou l'interface de ligne de commande. Les informations d'accès sont décrites ci-dessous.

API REST

Plusieurs terminaux peuvent être utilisés avec des rôles RBAC et des comptes utilisateur. Les quatre premiers du tableau sont utilisés pour créer et gérer les rôles. Les deux derniers sont utilisés pour créer et gérer des comptes utilisateur.

Vous pouvez accéder à la ONTAP en ligne "Référence API" Documentation pour plus d'informations, notamment des exemples d'utilisation de l'API.

Point final	Description
`/security/roles`	Ce noeud final vous permet de créer un nouveau rôle DE REPOS. Vous pouvez également définir un rôle traditionnel à partir de ONTAP 9.11.1. Dans ce cas, ONTAP détermine le type de rôle en fonction des paramètres d'entrée. Vous pouvez également récupérer une liste des rôles définis.
`/security/roles/{owner.UUID}/{name}`	Vous pouvez récupérer ou supprimer un cluster ou un rôle SVM défini. La valeur UUID identifie le SVM où le rôle est défini (cluster ou SVM des données). La valeur nom correspond au nom du rôle.
`/security/roles/{owner.UUID}/{name}/privileges`	Ce noeud final vous permet de configurer les privilèges pour un rôle spécifique. Les rôles intégrés peuvent être récupérés mais pas mis à jour. Pour plus d'informations, consultez la documentation de référence sur les API de votre version de ONTAP.
`/security/roles/{owner.UUID}/{name}/privileges/[path]`	Vous pouvez récupérer, modifier et supprimer le niveau d'accès et la valeur d'interrogation facultative d'un privilège spécifique. Pour plus d'informations, consultez la documentation de référence sur les API de votre version de ONTAP.
`/security/accounts`	Ce noeud final vous permet de créer un nouveau compte utilisateur défini au niveau du cluster ou du SVM. Plusieurs types d'informations doivent être inclus ou ajoutés par la suite avant que le compte ne soit opérationnel. Vous pouvez également récupérer une liste des comptes utilisateur définis.

Point final	Description
`/security/accounts/{owner.UUID}/{name}`	Vous pouvez récupérer, modifier et supprimer un cluster ou un compte utilisateur délimité par des SVM. La valeur UUID identifie le SVM où l'utilisateur est défini (cluster ou SVM de données). La valeur nom correspond au nom du compte.

Interface de ligne de commandes

Les commandes CLI ONTAP correspondantes sont décrites ci-dessous. Toutes les commandes sont accessibles au niveau du cluster par le biais d'un compte d'administrateur.

Commande	Description
`security login`	Il s'agit du répertoire contenant les commandes nécessaires à la création et à la gestion d'un login utilisateur.
`security login rest-role`	Il s'agit du répertoire contenant les commandes nécessaires à la création et à la gestion d'un rôle REST associé à une connexion utilisateur.
`security login role`	Il s'agit du répertoire contenant les commandes nécessaires à la création et à la gestion d'un rôle traditionnel associé à une connexion utilisateur.

Définitions de rôle

Les rôles REST et traditionnels sont définis via un ensemble d'attributs.

Propriétaire et portée

Un rôle peut être qui appartient au cluster ONTAP ou à un SVM de données spécifique au sein du cluster. Le propriétaire détermine aussi implicitement la portée du rôle.

Nom unique

Chaque rôle doit avoir un nom unique dans son périmètre. Le nom d'un rôle de cluster doit être unique au niveau du cluster ONTAP, tandis que les rôles de SVM doivent être uniques au sein de la SVM spécifique.

> Le nom d'un nouveau rôle DE REPOS doit être unique entre les rôles DE REPOS ainsi que les rôles traditionnels. En effet, la création d'un rôle REST entraîne également un nouveau rôle *mapping* traditionnel avec le même nom.

Ensemble de privilèges

Chaque rôle contient un ensemble d'un ou plusieurs privilèges. Chaque privilège identifie une ressource ou une commande spécifique et le niveau d'accès associé.

Privilèges

Un rôle peut contenir un ou plusieurs privilèges. Chaque définition de privilège est un tuple et établit le niveau d'accès à une ressource ou une opération spécifique.

Chemin de ressource

Le chemin de la ressource est identifié comme un point de terminaison REST ou comme chemin de répertoire commande/commande CLI.

Terminal REST

Un noeud final API a identifié la ressource cible pour un rôle REST.

Commande CLI

Une commande CLI identifie la cible d'un rôle traditionnel. Un répertoire de commandes peut également être spécifié, qui inclura ensuite toutes les commandes en aval dans la hiérarchie de l'interface de ligne de commande ONTAP.

Niveau d'accès

Le niveau d'accès définit le type d'accès dont dispose le rôle à la commande ou au chemin de ressources spécifique. Les niveaux d'accès sont identifiés par un ensemble de mots-clés prédéfinis. Trois niveaux d'accès ont été introduits avec ONTAP 9.6. Elles peuvent être utilisées pour les rôles traditionnels et LES rôles DE REPOS. En outre, trois nouveaux niveaux d'accès ont été ajoutés avec ONTAP 9.11.1. Ces nouveaux niveaux d'accès ne peuvent être utilisés qu'avec les rôles REST.

> Les niveaux d'accès suivent le modèle CRUD. Avec REST, ceci est basé sur les méthodes HTTP principales (POST, GET, PATCH, SUPPRESSION). Les opérations de l'interface de ligne de commande correspondantes sont généralement associées aux opérations REST (création, affichage, modification, suppression).

Niveau d'accès	Primitives REST	Ajouté	Rôle REST uniquement
Aucune	s/o	9.6	Non
lecture seule	OBTENEZ	9.6	Non
tous	OBTENIR, PUBLIER, CORRIGER, SUPPRIMER	9.6	Non
read_create	GET, POST	9.11.1	Oui.
lire_modifier	OBTENIR, CORRECTIF	9.11.1	Oui.
read_create_modify	OBTENIR, PUBLIER, CORRIGER	9.11.1	Oui.

Requête facultative

Lorsque vous créez un rôle traditionnel, vous pouvez éventuellement inclure une valeur **query** pour identifier le sous-ensemble d'objets applicables pour le répertoire de commande ou de commande.

Récapitulatif des rôles intégrés

Il existe plusieurs rôles prédéfinis inclus dans ONTAP que vous pouvez utiliser au niveau du cluster ou des SVM.

Rôles liés à la portée du cluster

Plusieurs rôles intégrés sont disponibles au niveau du cluster.

Voir "Rôles prédéfinis pour les administrateurs du cluster" pour en savoir plus.

Rôle	Description
admin	Les administrateurs ayant ce rôle possèdent des droits sans restriction et peuvent effectuer toutes les opérations nécessaires sur le système ONTAP. Ils peuvent configurer toutes les ressources au niveau du cluster et des SVM.
AutoSupport	Il s'agit d'un rôle spécial, spécialement conçu pour le compte AutoSupport.
sauvegarde	Ce rôle spécial pour les logiciels de sauvegarde qui doivent sauvegarder le système.
SnapLock	Il s'agit d'un rôle spécial, spécialement conçu pour le compte SnapLock.
lecture seule	Les administrateurs ayant ce rôle peuvent afficher tout au niveau du cluster, mais ne peuvent pas apporter de modifications.
Aucune	Aucune fonctionnalité d'administration n'est fournie.

Rôles évalués du SVM

Il existe plusieurs rôles intégrés disponibles dans le cadre du SVM. Le **vsadmin** donne accès aux fonctions les plus générales et les plus puissantes. Il existe plusieurs rôles supplémentaires adaptés à des tâches administratives spécifiques, notamment :

- volume vsadmin
- protocole vsadmin
- sauvegarde vsadmin
- vsadmin-snaplock
- vsadmin-readdisponible

Voir "Rôles prédéfinis pour les administrateurs des SVM" pour en savoir plus.

Comparaison des types de rôle

Avant de sélectionner un rôle **REST** ou **traditionnel**, vous devez être conscient des différences. Vous trouverez ci-dessous quelques méthodes de comparaison des deux types de rôle.

Pour les cas d'utilisation RBAC plus avancés ou plus complexes, vous devez généralement utiliser un rôle classique.

Comment l'utilisateur accède à ONTAP

Avant de créer un rôle, il est important de savoir comment l'utilisateur accède au système ONTAP. Un type de rôle peut être déterminé en fonction de ce type.

L'accès	Type suggéré
API REST uniquement	Le rôle REST est conçu pour être utilisé avec l'API REST.
API REST ET INTERFACE DE LIGNE DE COMMANDES	Vous pouvez définir un rôle REST qui crée également un rôle traditionnel correspondant.

L’accès	Type suggéré
Interface de ligne de commandes uniquement	Vous pouvez créer un rôle traditionnel.

Précision du chemin d’accès

Le chemin d’accès défini pour un rôle REST est basé sur un terminal REST. Le chemin d’accès d’un rôle traditionnel repose sur une commande ou un répertoire de commande CLI. En outre, vous pouvez inclure un paramètre de requête facultatif avec un rôle traditionnel afin de restreindre davantage l’accès en fonction des valeurs des paramètres de la commande.

Informations sur le copyright

Informations sur les marques commerciales