Autorisation du client

ONTAP 9

NetApp
February 13, 2026

Sommaire

Autorisation du client

Présentation et options de l'autorisation client ONTAP

L'implémentation ONTAP OAuth 2.0 est conçue pour être flexible et robuste, et vous offre les fonctionnalités dont vous avez besoin pour sécuriser votre environnement ONTAP. Plusieurs options de configuration mutuellement exclusives sont disponibles. Les décisions d'autorisation sont finalement basées sur les rôles REST ONTAP contenus dans ou dérivés des jetons d'accès OAuth 2.0.

Vous pouvez uniquement utiliser "Rôles REST ONTAP" Lors de la configuration de l'autorisation pour OAuth 2.0. Les anciens rôles ONTAP traditionnels ne sont pas pris en charge.

ONTAP applique l'option d'autorisation la plus appropriée en fonction de votre configuration. Pour plus d'informations sur la manière dont ONTAP prend les décisions d'accès client, reportez-vous à la section"Comment ONTAP détermine l'accès".

Oscilloscopes autonomes OAuth 2.0

Ces étendues contiennent un ou plusieurs rôles REST personnalisés, chacun encapsulé dans une seule chaîne dans le jeton d'accès. Ils sont indépendants des définitions de rôles ONTAP. Vous devez configurer les chaînes de portée sur votre serveur d'autorisation. Voir "Oscilloscopes OAuth 2.0 autonomes" pour plus d'informations.

Rôles REST ONTAP locaux

Un seul rôle REST nommé, intégré ou personnalisé, peut être utilisé. La syntaxe de portée d'un rôle nommé est **ontap-role-**<URL-encoded-ONTAP-role-name>. Par exemple, si le rôle ONTAP est `admin` la chaîne de portée sera `ontap-role-admin`.

Utilisateurs

Le nom d'utilisateur dans le jeton d'accès défini avec l'accès à l'application « http » peut être utilisé. Un utilisateur est testé dans l'ordre suivant en fonction de la méthode d'authentification définie : mot de passe, domaine (Active Directory), nsswitch (LDAP).

Groupes

Les serveurs d'autorisation peuvent être configurés pour utiliser des groupes ONTAP pour l'autorisation. Si les définitions ONTAP locales sont examinées mais qu'aucune décision d'accès ne peut être prise, les groupes Active Directory (« domaine ») ou LDAP (« nsswitch ») sont utilisés. Les informations de groupe peuvent être spécifiées de deux manières :

- Chaîne de portée OAuth 2.0

  Prend en charge les applications confidentielles en utilisant le flux d'informations d'identification du client lorsqu'aucun utilisateur n'est membre d'un groupe. Le périmètre doit être nommé **ontap-group-**<URL-encoded-ONTAP-group-name>. Par exemple, si le groupe est « développement », la chaîne de portée sera « ontap-groupe-développement ».

- Dans la réclamation « Groupe »

  Ceci est destiné aux jetons d'accès émis par ADFS à l'aide du flux propriétaire de la ressource (mot de passe Grant).

Voir "Travailler avec des groupes IdP OAuth 2.0 ou SAML dans ONTAP" pour plus d'informations.

Portées OAuth 2.0 autonomes dans ONTAP

Les étendues autonomes sont des chaînes portées dans le jeton d'accès. Chacune d'entre elles constitue une définition de rôle personnalisée complète et comprend tout ce dont ONTAP a besoin pour prendre une décision d'accès. Le périmètre est distinct et celui de tous les rôles REST définis au sein de ONTAP lui-même.

Format de la chaîne de portée

Au niveau de la base, la portée est représentée sous la forme d'une chaîne contiguë et composée de six valeurs séparées par deux points. Les paramètres utilisés dans la chaîne de portée sont décrits ci-dessous.

Littéral ONTAP

La portée doit commencer par la valeur littérale `ontap` en minuscules. Cette opération identifie la portée en tant que spécifique à ONTAP.

Cluster

Il définit le cluster ONTAP auquel la portée s'applique. Les valeurs peuvent inclure :

- UUID de cluster

  Identifie un seul cluster.

- Astérisque (*)

  Indique que la portée s'applique à tous les clusters.

Vous pouvez utiliser la commande ONTAP CLI `cluster identity show` pour afficher l'UUID de votre cluster. Si elle n'est pas spécifiée, la portée s'applique à tous les clusters. Pour en savoir plus, `cluster identity show` consultez le "Référence de commande ONTAP".

Rôle

Nom du rôle REST contenu dans le périmètre autonome. Cette valeur n'est pas examinée par ONTAP ou associée à tout rôle REST existant défini sur ONTAP. Le nom est utilisé pour la journalisation.

Niveau d'accès

Cette valeur indique le niveau d'accès appliqué à l'application client lors de l'utilisation du noeud final de l'API dans le périmètre. Il existe six valeurs possibles, comme décrit dans le tableau ci-dessous.

Niveau d'accès	Description
Aucune	Refuse tout accès au noeud final spécifié.
lecture seule	Autorise uniquement l'accès en lecture à l'aide de GET.
read_create	Permet l'accès en lecture ainsi que la création de nouvelles instances de ressources à l'aide de POST.

Niveau d'accès	Description
lire_modifier	Permet l'accès en lecture ainsi que la mise à jour des ressources existantes à l'aide d'un CORRECTIF.
read_create_modify	Permet tous les accès sauf supprimer. Les opérations autorisées comprennent OBTENIR (lire), POST (créer) et PATCH (mettre à jour).
tous	Permet un accès complet.

SVM

Nom du SVM au sein du cluster auquel la portée s'applique. Utilisez la valeur * (astérisque) pour indiquer tous les SVM.

> Cette fonctionnalité n'est pas entièrement prise en charge par ONTAP 9.14.1. Vous pouvez ignorer le paramètre du SVM et utiliser un astérisque comme emplacement réservé. Vérifiez le "Notes de version de ONTAP" Pour vérifier la prise en charge future des SVM.

URI DE L'API REST

Chemin complet ou partiel d'une ressource ou d'un ensemble de ressources associées. La chaîne doit commencer par `/api`. Si vous ne spécifiez pas de valeur, la portée s'applique à tous les terminaux d'API du cluster ONTAP.

Exemples de portée

Quelques exemples de portées autonomes sont présentés ci-dessous.

ontap:*:joes-role:read_create_modify:*:/api/cluster

Permet à l'utilisateur affecté à ce rôle d'accéder en lecture, création et modification à `/cluster` point final.

Outil d'administration CLI

Pour faciliter l'administration des étendues autonomes et réduire le risque d'erreur, ONTAP fournit la commande CLI `security oauth2 scope` pour générer des chaînes de portée basées sur vos paramètres d'entrée.

La commande `security oauth2 scope` propose deux cas d'utilisation basés sur vos commentaires :

- Paramètres de l'interface de ligne de commande pour la chaîne de périmètre

  Vous pouvez utiliser cette version de la commande pour générer une chaîne de portée basée sur les paramètres d'entrée.

- Chaîne d'étendue aux paramètres CLI

  Vous pouvez utiliser cette version de la commande pour générer les paramètres de la commande en fonction de la chaîne de périmètre d'entrée.

Exemple

L'exemple suivant génère une chaîne de périmètre avec le résultat inclus après l'exemple de commande ci-dessous. La définition s'applique à tous les clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Pour en savoir plus, `security oauth2 scope` consultez le "Référence de commande ONTAP".

Mappage des rôles externes OAuth 2.0 dans ONTAP

Un rôle externe est défini dans un fournisseur d'identification configuré pour une utilisation par ONTAP. Vous pouvez créer et gérer des relations de mappage entre ces rôles externes et les rôles ONTAP à l'aide de l'interface de ligne de commandes ONTAP.

Vous pouvez également configurer la fonction de mappage de rôles externes à l'aide de l'API REST ONTAP. Pour en savoir plus, consultez le "Documentation sur l'automatisation ONTAP".

Rôles externes dans un jeton d'accès

Voici un fragment d'un jeton d'accès JSON contenant deux rôles externes.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuration

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour administrer la fonction de mappage de rôle externe.

Création

Vous pouvez définir une configuration de mappage de rôles à l'aide de la `security login external-role-mapping create` commande. Vous devez être au niveau de privilège ONTAP **admin** pour exécuter cette commande ainsi que les options associées.

Paramètres

Les paramètres utilisés pour créer un mappage de groupe sont décrits ci-dessous.

Paramètre	Description
`external-role`	Nom du rôle défini au niveau du fournisseur d'identité externe.
`provider`	Nom du fournisseur d'identité. Il doit s'agir de l'identifiant du système.
`ontap-role`	Indique le rôle ONTAP existant vers lequel le rôle externe est mappé.

Exemple

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Pour en savoir plus, `security login external-role-mapping create` consultez le "Référence de commande ONTAP".

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Informations associées

- "Référence de commande ONTAP"

Comment ONTAP détermine l'accès client

Pour bien concevoir et mettre en œuvre OAuth 2.0, vous devez comprendre comment ONTAP utilise votre configuration d'autorisation pour prendre des décisions d'accès pour les clients. Les principales étapes permettant de déterminer l'accès sont présentées ci-dessous en fonction de la version de ONTAP.

Il n'y a pas eu de mises à jour OAuth 2.0 significatives avec ONTAP 9.15.1. Si vous utilisez la version 9.15.1, reportez-vous à la description de ONTAP 9.14.1.

Informations associées

- "Fonctionnalités OAuth 2.0 prises en charge dans ONTAP"

ONTAP 9.16.1

ONTAP 9.16.1 étend la prise en charge standard d'OAuth 2.0 pour inclure des extensions spécifiques d'Entra ID Microsoft pour les groupes d'ID Entra natifs ainsi que le mappage de rôles externes.

Déterminez l'accès client pour ONTAP 9.16.1

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des étendues autonomes, ONTAP examine d'abord ces étendues. S'il n'y a pas de portées autonomes, passez à l'étape 2.

Avec une ou plusieurs portées autonomes présentes, ONTAP applique chaque portée jusqu'à ce qu'une décision explicite **ALLOW** ou **DENY** puisse être prise. Si une décision explicite est prise, le traitement prend fin.

Si ONTAP ne peut pas prendre de décision explicite en matière d'accès, passez à l'étape 2.

Étape 2 : vérifiez l'indicateur de rôles locaux

ONTAP examine le paramètre booléen `use-local-roles-if-present` . La valeur de cet indicateur est définie séparément pour chaque serveur d'autorisation défini sur ONTAP.

- Si la valeur est de `true` passez à l'étape 3.
- Si la valeur est de `false` le traitement se termine et l'accès est refusé.

Étape 3 : rôle REST ONTAP nommé

Si le jeton d'accès contient un rôle REST nommé dans le `scope` champ ou `scp`, ou en tant que sinistre, ONTAP utilise le rôle pour prendre la décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de rôle REST nommé ou si le rôle est introuvable, passez à l'étape 4.

Étape 4 : utilisateurs

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre aux utilisateurs ayant accès à l'application « http ». Les utilisateurs sont examinés en fonction de la méthode d'authentification dans l'ordre suivant :

- mot de passe
- Domaine (Active Directory)
- Nsswitch (LDAP)

Si un utilisateur correspondant est trouvé, ONTAP utilise le rôle défini pour l'utilisateur afin de prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ne correspond pas ou s'il n'y a pas de nom d'utilisateur dans le jeton d'accès, passez à l'étape 5.

Étape 5 : groupes

Si un ou plusieurs groupes sont inclus, le format est examiné. Si les groupes sont représentés par des UUID, une recherche est effectuée dans une table de mappage de groupes interne. En cas de correspondance entre un groupe et un rôle associé, ONTAP utilise le rôle défini pour le groupe afin de prendre une décision d'accès. Cela aboutit systématiquement à une décision d'autorisation (**ALLOW**) ou de refus (**DENY**), et le traitement est terminé. "Travailler avec des groupes IdP OAuth 2.0 ou SAML dans ONTAP" .

Si les groupes sont représentés par des noms et configurés avec l'autorisation domaine ou nsswitch, ONTAP tente de les faire correspondre à un groupe Active Directory ou LDAP, respectivement. S'il existe une correspondance de groupe, ONTAP utilise le rôle défini pour le groupe pour prendre une décision

d’accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S’il n’y a pas de correspondance de groupe ou s’il n’y a pas de groupe dans le jeton d’accès, l’accès est refusé et le traitement se termine.

ONTAP 9.14.1

La version initiale de OAuth 2.0 prise en charge est introduite avec ONTAP 9.14.1 en fonction des fonctionnalités standard de OAuth 2.0.

Déterminez l'accès client pour ONTAP 9.14.1

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des étendues autonomes, ONTAP examine d'abord ces étendues. S'il n'y a pas de portées autonomes, passez à l'étape 2.

Avec une ou plusieurs portées autonomes présentes, ONTAP applique chaque portée jusqu'à ce qu'une décision explicite **ALLOW** ou **DENY** puisse être prise. Si une décision explicite est prise, le traitement prend fin.

Si ONTAP ne peut pas prendre de décision explicite en matière d'accès, passez à l'étape 2.

Étape 2 : vérifiez l'indicateur de rôles locaux

ONTAP examine le paramètre booléen `use-local-roles-if-present` . La valeur de cet indicateur est définie séparément pour chaque serveur d'autorisation défini sur ONTAP.

- Si la valeur est de `true` passez à l'étape 3.
- Si la valeur est de `false` le traitement se termine et l'accès est refusé.

Étape 3 : rôle REST ONTAP nommé

Si le jeton d'accès contient un rôle REST nommé dans le `scope` champ ou `scp`, ONTAP utilise le rôle pour prendre la décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de rôle REST nommé ou si le rôle est introuvable, passez à l'étape 4.

Étape 4 : utilisateurs

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre aux utilisateurs ayant accès à l'application « http ». Les utilisateurs sont examinés en fonction de la méthode d'authentification dans l'ordre suivant :

- mot de passe
- Domaine (Active Directory)
- Nsswitch (LDAP)

Si un utilisateur correspondant est trouvé, ONTAP utilise le rôle défini pour l'utilisateur afin de prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ne correspond pas ou s'il n'y a pas de nom d'utilisateur dans le jeton d'accès, passez à l'étape 5.

Étape 5 : groupes

Si un ou plusieurs groupes sont inclus et configurés avec l'autorisation domain ou nsswitch, ONTAP tente de les associer à un groupe Active Directory ou LDAP, respectivement.

S'il existe une correspondance de groupe, ONTAP utilise le rôle défini pour le groupe pour prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de correspondance de groupe ou s'il n'y a pas de groupe dans le jeton d'accès, l'accès est refusé et le traitement se termine.