Concepts

ONTAP 9

NetApp
April 24, 2024

Sommaire

Concepts

Serveurs d’autorisation et jetons d’accès

Les serveurs d’autorisation effectuent plusieurs fonctions importantes en tant que composant central dans le cadre d’autorisation OAuth 2.0.

Serveurs d’autorisation OAuth 2.0

Les serveurs d’autorisation sont principalement responsables de la création et de la signature des jetons d’accès. Ces tokens contiennent des informations d’identité et d’autorisation permettant à une application client d’accéder de manière sélective aux ressources protégées. Les serveurs sont généralement isolés les uns des autres et peuvent être mis en œuvre de différentes manières, notamment en tant que serveur dédié autonome ou dans le cadre d’un produit de gestion des identités et des accès plus large.

> Une terminologie différente peut parfois être utilisée pour un serveur d’autorisation, en particulier lorsque la fonctionnalité OAuth 2.0 est intégrée dans un produit ou une solution de gestion des identités et des accès plus large. Par exemple, le terme **Identity Provider (IDP)** est fréquemment utilisé de manière interchangeable avec **Authorization Server**.

L’administration

Outre l’émission de jetons d’accès, les serveurs d’autorisation fournissent également des services administratifs connexes, généralement via une interface utilisateur Web. Par exemple, vous pouvez définir et administrer :

- Authentification des utilisateurs et des utilisateurs
- Étendues
- Ségrégation administrative par les locataires et les royaumes
- Application des règles
- Connexion à divers services externes
- Prise en charge d’autres protocoles d’identité (tels que SAML)

ONTAP est compatible avec les serveurs d’autorisation conformes à la norme OAuth 2.0.

Définition de ONTAP

Vous devez définir un ou plusieurs serveurs d’autorisation sur ONTAP. ONTAP communique en toute sécurité avec chaque serveur pour vérifier les tokens et effectuer d’autres tâches connexes pour la prise en charge des applications client.

Les principaux aspects de la configuration ONTAP sont présentés ci-dessous. Voir aussi "Scénarios de déploiement OAuth 2.0" pour en savoir plus.

Comment et où les jetons d’accès sont validés

Il existe deux options pour valider les jetons d’accès.

- Validation locale

ONTAP peut valider les jetons d'accès localement en fonction des informations fournies par le serveur d'autorisation qui a émis le token. Les informations extraites du serveur d'autorisation sont mises en cache par ONTAP et actualisées à intervalles réguliers.

- Introspection à distance

  Vous pouvez également utiliser l'introspection à distance pour valider les tokens sur le serveur d'autorisation. L'introspection est un protocole permettant aux parties autorisées d'interroger un serveur d'autorisation sur un jeton d'accès. Il permet à ONTAP d'extraire certaines métadonnées d'un jeton d'accès et de valider le jeton. ONTAP met en cache une partie des données pour des raisons de performances.

Emplacement réseau

ONTAP peut se trouver derrière un pare-feu. Dans ce cas, vous devez identifier un proxy comme faisant partie de la configuration.

Définition des serveurs d'autorisation

Vous pouvez définir un serveur d'autorisation pour ONTAP à l'aide de n'importe quelle interface d'administration, notamment l'interface de ligne de commandes, System Manager ou l'API REST. Par exemple, avec l'interface de ligne de commandes, vous utilisez la commande `security oauth2 client create`.

Nombre de serveurs d'autorisation

Vous pouvez définir jusqu'à huit serveurs d'autorisation sur un seul cluster ONTAP. Le même serveur d'autorisation peut être défini plusieurs fois sur le même cluster ONTAP tant que les demandes d'émetteur ou d'émetteur/d'audience sont uniques. Par exemple, avec Keycloak, ce sera toujours le cas lorsque vous utilisez des domaines différents.

Utilisation des jetons d'accès OAuth 2.0

Les jetons d'accès OAuth 2.0 émis par les serveurs d'autorisation sont vérifiés par ONTAP et utilisés pour prendre des décisions d'accès basées sur les rôles pour les requêtes client de l'API REST.

Acquisition d'un jeton d'accès

Vous devez acquérir un jeton d'accès à partir d'un serveur d'autorisation défini sur le cluster ONTAP où vous utilisez l'API REST. Pour acquérir un jeton, vous devez contacter directement le serveur d'autorisation.

> ONTAP n'émet pas de tokens d'accès ni ne redirige pas les requêtes des clients vers les serveurs d'autorisation.

La façon dont vous demandez un jeton dépend de plusieurs facteurs, notamment :

- Serveur d'autorisation et ses options de configuration
- Type de subvention OAuth 2.0
- Client ou outil logiciel utilisé pour émettre la demande

Types de subventions

Un *Grant* est un processus bien défini, comprenant un ensemble de flux réseau, utilisé pour demander et recevoir un jeton d'accès OAuth 2.0. Plusieurs types d'octroi différents peuvent être utilisés en fonction du client, de l'environnement et des exigences de sécurité. Une liste des types de subventions les plus populaires est présentée dans le tableau ci-dessous.

Type de subvention	Description
Informations d'identification du client	Type de subvention populaire basé sur l'utilisation de références uniquement (par exemple, un ID et un secret partagé). Le client est supposé avoir une relation de confiance étroite avec le propriétaire de la ressource.
Mot de passe	Le type d'octroi d'autorisations de mot de passe du propriétaire de ressource peut être utilisé lorsque le propriétaire de la ressource a une relation de confiance établie avec le client. Elle peut également être utile lors de la migration de clients HTTP hérités vers OAuth 2.0.
Code d'autorisation	Il s'agit d'un type d'octroi idéal pour les clients confidentiels et basé sur un flux basé sur la redirection. Il peut être utilisé pour obtenir à la fois un jeton d'accès et un jeton d'actualisation.

Contenu JWT

Un jeton d'accès OAuth 2.0 est formaté en JWT. Le contenu est créé par le serveur d'autorisation en fonction de votre configuration. Cependant, les tokens sont opaques pour les applications client. Un client n'a aucune raison d'inspecter un jeton ou d'être au courant du contenu.

Chaque jeton d'accès JWT contient un ensemble de réclamations. Les réclamations décrivent les caractéristiques de l'émetteur et l'autorisation en fonction des définitions administratives du serveur d'autorisation. Certaines des réclamations enregistrées avec la norme sont décrites dans le tableau ci-dessous. Toutes les chaînes sont sensibles à la casse.

Réclamation	Mot-clé	Description
Émetteur	iss	Identifie le principal qui a émis le token. Le traitement de la demande est spécifique à l'application.
Objet	sous	L'objet ou l'utilisateur du jeton. Le nom est défini comme unique au niveau global ou local.
Public	aud	Destinataires pour lequel le token est destiné. Implémenté en tant que tableau de chaînes.
Expiration	date	Heure après laquelle le jeton expire et doit être rejeté.

Voir "RFC 7519 : tokens Web JSON" pour en savoir plus.

Options pour l'autorisation client ONTAP

Plusieurs options sont disponibles pour personnaliser votre autorisation client ONTAP. Les décisions d'autorisation sont finalement basées sur les rôles REST ONTAP contenus dans ou dérivés des jetons d'accès.

> 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.

Introduction

La mise en œuvre OAuth 2.0 au sein de ONTAP est conçue pour être flexible et robuste, offrant les options dont vous avez besoin pour sécuriser l'environnement ONTAP. À un niveau élevé, il existe trois principales

catégories de configuration permettant de définir l'autorisation du client ONTAP. Ces options de configuration s'excluent mutuellement.

ONTAP applique l'option la plus appropriée en fonction de votre configuration. Voir "Comment ONTAP détermine l'accès" Pour en savoir plus sur la façon dont ONTAP traite vos définitions de configuration pour prendre des décisions d'accès.

Oscilloscopes autonomes OAuth 2.0

Ces étendues contiennent un ou plusieurs rôles REST personnalisés, chacun encapsulé dans une seule chaîne. Ils sont indépendants des définitions de rôles ONTAP. Vous devez définir ces chaînes de portée sur votre serveur d'autorisation.

Utilisateurs et rôles REST spécifiques à ONTAP en local

En fonction de votre configuration, les définitions d'identité ONTAP locales peuvent être utilisées pour prendre des décisions d'accès. Les options sont les suivantes :

- Rôle REST nommé unique
- Correspondance du nom d'utilisateur avec un utilisateur ONTAP local

La syntaxe de portée d'un rôle nommé est **ontap-role-**<URL-encoded-ONTAP-role-name>. Par exemple, si le rôle est « admin », la chaîne de portée sera « ontap-role-admin ».

Groupes Active Directory ou LDAP

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).

Oscilloscopes OAuth 2.0 autonomes

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 CLI de ONTAP `cluster identity show` Pour afficher l'UUID de votre cluster. Si elle n'est pas spécifiée, la portée s'applique à tous les clusters.

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.
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
```

Comment ONTAP détermine l'accès

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.

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des périmètres autonomes, ONTAP examine d'abord ces périmètres. 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 la valeur de l'indicateur `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, ONTAP utilise ce 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 ONTAP locaux

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre à un utilisateur ONTAP local.

Si un utilisateur ONTAP local est associé, ONTAP utilise le rôle défini pour que l'utilisateur puisse prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ONTAP local 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 : mappage groupe-rôle

Extrayez le groupe du jeton d'accès et essayez de le faire correspondre à un groupe. Les groupes sont définis à l'aide d'Active Directory ou d'un serveur LDAP équivalent.

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.

Scénarios de déploiement OAuth 2.0

Plusieurs options de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. En fonction de ces options, vous pouvez créer un serveur d'autorisation adapté à votre environnement de déploiement.

Résumé des paramètres de configuration

Plusieurs paramètres de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. Ces paramètres sont généralement pris en charge dans toutes les interfaces administratives.

Les noms des paramètres peuvent varier légèrement en fonction de l'interface d'administration de ONTAP. Par exemple, lors de la configuration de l'introspection à distance, le noeud final est identifié à l'aide du paramètre de commande CLI `-introspection-endpoint`. Mais avec System Manager, le champ équivalent est *URI* d'introspection de jeton de serveur d'autorisation. Pour prendre en charge toutes les interfaces administratives ONTAP, une description générale des paramètres est fournie. Le paramètre ou le champ exact doit être évident en fonction du contexte.

Paramètre	Description
Nom	Nom du serveur d'autorisation tel qu'il est connu de ONTAP.
Client supplémentaire	Application interne ONTAP à laquelle s'applique la définition. Ce doit être **http**.
URI de l'émetteur	Nom de domaine complet avec chemin identifiant le site ou l'organisation qui émet les jetons.
URI du fournisseur JWKS	Nom de domaine complet avec chemin et nom de fichier où ONTAP obtient les jeux de clés Web JSON utilisés pour valider les jetons d'accès.
Intervalle de rafraîchissement JWKS	Intervalle de temps déterminant la fréquence à laquelle ONTAP actualise les informations de certificat à partir de l'URI JWKS du fournisseur. La valeur est spécifiée au format ISO-8601.
Point d'extrémité d'introspection	Nom de domaine complet avec chemin utilisé par ONTAP pour effectuer la validation de jeton à distance via l'introspection.
ID client	Nom du client tel que défini sur le serveur d'autorisation. Lorsque cette valeur est incluse, vous devez également fournir le secret client associé en fonction de l'interface.
Proxy sortant	Cela permet d'accéder au serveur d'autorisation lorsque ONTAP se trouve derrière un pare-feu. L'URI doit être au format curl.
Utilisez des rôles locaux, le cas échéant	Indicateur booléen déterminant si les définitions ONTAP locales sont utilisées, y compris un rôle REST nommé et des utilisateurs locaux.
Supprimer la réclamation utilisateur	Autre nom utilisé par ONTAP pour correspondre aux utilisateurs locaux. Utilisez le `sub` champ du jeton d'accès correspondant au nom d'utilisateur local.

Scénarios de déploiement

Vous trouverez ci-dessous plusieurs scénarios de déploiement courants. Ils sont organisés selon que la validation des tokens est effectuée localement par ONTAP ou à distance par le serveur d'autorisation. Chaque scénario inclut une liste des options de configuration requises. Voir "Déployer OAuth 2.0 dans ONTAP" pour des exemples de commandes de configuration.

> Après avoir défini un serveur d'autorisation, vous pouvez afficher sa configuration via l'interface d'administration ONTAP. Par exemple, utilisez la commande `security oauth2 client show` Via l'interface de ligne de commandes ONTAP.

Validation locale

Les scénarios de déploiement suivants sont basés sur l'exécution locale de la validation des jetons par ONTAP.

Utilisez des oscilloscopes autonomes sans proxy

Il s'agit du déploiement le plus simple utilisant uniquement des oscilloscopes autonomes OAuth 2.0. Aucune définition d'identité ONTAP locale n'est utilisée. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS

- URI de l'émetteur

Vous devez également ajouter les étendues au niveau du serveur d'autorisation.

Utiliser des portées autonomes avec un proxy

Ce scénario de déploiement utilise les étendues autonomes OAuth 2.0. Aucune définition d'identité ONTAP locale n'est utilisée. Mais le serveur d'autorisation est derrière un pare-feu et vous devez donc configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Proxy sortant
- URI de l'émetteur
- Public

Vous devez également ajouter les étendues au niveau du serveur d'autorisation.

Utilisez les rôles d'utilisateur local et le mappage de nom d'utilisateur par défaut avec un proxy

Ce scénario de déploiement utilise des rôles d'utilisateur local avec un mappage de noms par défaut. Le sinistre utilisateur distant utilise la valeur par défaut de `sub` ce champ du jeton d'accès est donc utilisé pour correspondre au nom d'utilisateur local. Le nom d'utilisateur doit comporter au maximum 40 caractères. Le serveur d'autorisation se trouve derrière un pare-feu, vous devez donc également configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Utilisez des rôles locaux, le cas échéant (`true`)
- Proxy sortant
- Émetteur

Vous devez vous assurer que l'utilisateur local est défini sur ONTAP.

Utilisez des rôles d'utilisateur locaux et un mappage de nom d'utilisateur alternatif avec un proxy

Ce scénario de déploiement utilise des rôles d'utilisateur local avec un autre nom d'utilisateur qui est utilisé pour correspondre à un utilisateur ONTAP local. Le serveur d'autorisation est derrière un pare-feu, vous devez donc configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Utilisez des rôles locaux, le cas échéant (`true`)
- Demande d'utilisateur à distance
- Proxy sortant
- URI de l'émetteur

- Public

Vous devez vous assurer que l'utilisateur local est défini sur ONTAP.

Introspection à distance

Les configurations de déploiement suivantes sont basées sur ONTAP qui effectue la validation des jetons à distance via l'introspection.

Utilisez des oscilloscopes autonomes sans proxy

Il s'agit d'un déploiement simple basé sur l'utilisation des oscilloscopes autonomes OAuth 2.0. Aucune définition d'identité ONTAP n'est utilisée. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- Point d'extrémité d'introspection
- ID client
- URI de l'émetteur

Vous devez définir les étendues ainsi que le secret client et client sur le serveur d'autorisation.

Authentification du client à l'aide d'un protocole TLS mutuel

Selon vos besoins en matière de sécurité, vous pouvez éventuellement configurer le protocole MTLS (Mutual TLS) pour mettre en œuvre une authentification client forte. Lorsqu'il est utilisé avec ONTAP dans le cadre d'un déploiement OAuth 2.0, MTLS garantit que les jetons d'accès ne sont utilisés que par les clients auxquels ils ont été initialement émis.

Protocole commun avec OAuth 2.0

TLS (transport Layer Security) est utilisé pour établir un canal de communication sécurisé entre deux applications, généralement un navigateur client et un serveur Web. Le protocole mutuel TLS étend cette fonction en fournissant une identification forte du client par le biais d'un certificat client. Lorsqu'elle est utilisée dans un cluster ONTAP avec OAuth 2.0, la fonctionnalité MTLS de base est étendue en créant et en utilisant des jetons d'accès limités par l'expéditeur.

Un jeton d'accès limité par l'expéditeur ne peut être utilisé que par le client auquel il a été émis à l'origine. Pour prendre en charge cette fonction, une nouvelle demande de confirmation (`cnf`) est inséré dans le jeton. Le champ contient la propriété `x5t#S256` qui contient un résumé du certificat client utilisé lors de la demande du jeton d'accès. Cette valeur est vérifiée par ONTAP dans le cadre de la validation du jeton. Les jetons d'accès émis par les serveurs d'autorisation qui ne sont pas soumis à des contraintes d'expéditeur n'incluent pas la demande de confirmation supplémentaire.

Vous devez configurer ONTAP pour qu'il utilise MTLS séparément pour chaque serveur d'autorisation. Par exemple, la commande CLI `security oauth2 client` inclut le paramètre `use-mutual-tls` Contrôler le traitement MTLS en fonction de trois valeurs, comme indiqué dans le tableau ci-dessous.

Dans chaque configuration, le résultat et l'action de ONTAP dépendent de la valeur du paramètre de configuration, ainsi que du contenu du jeton d'accès et du certificat client. Les paramètres du tableau sont organisés du moins au plus restrictif.

Paramètre	Description
Aucune	L'authentification mutuelle TLS OAuth 2.0 est complètement désactivée pour le serveur d'autorisation. ONTAP n'effectuera pas l'authentification du certificat du client MTLS même si la demande de confirmation est présente dans le jeton ou si un certificat client est fourni avec la connexion TLS.
demande	L'authentification mutuelle TLS OAuth 2.0 est appliquée si un jeton d'accès limité par l'expéditeur est présenté par le client. C'est-à-dire que MTLS est appliqué uniquement si la demande de confirmation (avec la propriété `x5t#S256`) est présent dans le jeton d'accès. Il s'agit du paramètre par défaut.
obligatoire	L'authentification mutuelle TLS OAuth 2.0 est appliquée pour tous les jetons d'accès émis par le serveur d'autorisation. Par conséquent, tous les tokens d'accès doivent être soumis à des contraintes d'expéditeur. L'authentification et la demande de l'API REST échouent si la demande de confirmation n'est pas présente dans le jeton d'accès ou si un certificat client n'est pas valide.

Flux de mise en œuvre de haut niveau

Les étapes typiques de l'utilisation de MTLS avec OAuth 2.0 dans un environnement ONTAP sont présentées ci-dessous. Voir "RFC 8705 : authentification du client mutuelle OAuth 2.0 et jetons d'accès liés au certificat" pour en savoir plus.

Étape 1 : création et installation d'un certificat client

L'établissement de l'identité du client repose sur la preuve de la connaissance d'une clé privée du client. La clé publique correspondante est placée dans un certificat X.509 signé présenté par le client. À un niveau élevé, les étapes impliquées dans la création du certificat client comprennent :

1. Générez une paire de clés publique et privée
2. Créez une demande de signature de certificat
3. Envoyez le fichier CSR à une autorité de certification connue
4. CA vérifie la demande et émet le certificat signé

Vous pouvez normalement installer le certificat client dans votre système d'exploitation local ou l'utiliser directement avec un utilitaire commun tel que curl.

Étape 2 : configurer ONTAP pour utiliser MTLS

Vous devez configurer ONTAP pour utiliser MTLS. Cette configuration est effectuée séparément pour chaque serveur d'autorisation. Par exemple, avec l'interface de ligne de commandes, la commande `security oauth2 client` est utilisé avec le paramètre facultatif `use-mutual-tls`. Voir "Déployer OAuth 2.0 dans ONTAP" pour en savoir plus.

Étape 3 : le client demande un jeton d'accès

Le client doit demander un jeton d'accès au serveur d'autorisation configuré sur ONTAP. L'application client doit utiliser MTLS avec le certificat créé et installé à l'étape 1.

Étape 4 : le serveur d'autorisation génère le jeton d'accès

Le serveur d'autorisation vérifie la demande du client et génère un jeton d'accès. Dans ce cadre, il crée un résumé de message du certificat client qui est inclus dans le jeton en tant que demande de confirmation (champ `cnf`).

Étape 5 : l'application client présente le jeton d'accès à ONTAP

L'application client effectue un appel d'API REST vers le cluster ONTAP et inclut le jeton d'accès dans l'en-tête de la demande d'autorisation en tant que **jeton porteur**. Le client doit utiliser MTLS avec le même certificat que celui utilisé pour demander le jeton d'accès.

Étape 6 : ONTAP vérifie le client et le jeton.

ONTAP reçoit le jeton d'accès dans une requête HTTP ainsi que le certificat client utilisé dans le cadre du traitement MTLS. ONTAP valide d'abord la signature dans le jeton d'accès. En fonction de la configuration, ONTAP génère un résumé de message du certificat client et le compare à la demande de confirmation **cnf** du jeton. Si les deux valeurs correspondent, ONTAP a confirmé que le client faisant la demande d'API est le même client auquel le jeton d'accès a été émis à l'origine.