Conceptos

ONTAP 9

NetApp
January 08, 2026

Tabla de contenidos

Conceptos . . . 1
- Servidores de autorización OAuth 2.0 y tokens de acceso en ONTAP . . . 1
  - Servidores de autorización OAuth 2,0 . . . 1
  - Funciones de OAuth 2,0 admitidas en ONTAP . . . 2
  - Uso de tokens de acceso OAuth 2,0 . . . 3
- Autorización de cliente . . . 4
  - Descripción general y opciones para la autorización del cliente de ONTAP . . . 4
  - Ámbitos OAuth 2.0 autónomos en ONTAP . . . 5
  - Mapeo de roles externos de OAuth 2.0 en ONTAP . . . 7
  - Cómo determina ONTAP el acceso del cliente . . . 9
- Escenarios de implementación de OAuth 2.0 con ONTAP . . . 13
  - Resumen de los parámetros de configuración . . . 13
  - Escenarios de puesta en marcha . . . 13
- Autenticación de cliente ONTAP mediante OAuth 2.0 Mutual TLS . . . 15
  - TLS Mutuo con OAuth 2,0 . . . 16
  - Flujo de implantación de alto nivel . . . 16

Conceptos

Servidores de autorización OAuth 2.0 y tokens de acceso en ONTAP

Los servidores de autorización realizan varias funciones importantes como componente central dentro del marco de autorización de OAuth 2,0.

Servidores de autorización OAuth 2,0

Los servidores de autorización son los principales responsables de crear y firmar tokens de acceso. Estos tokens contienen información de identidad y autorización que permite a una aplicación cliente acceder selectivamente a los recursos protegidos. Los servidores generalmente están aislados entre sí y se pueden implementar de varias maneras diferentes, incluyendo como un servidor dedicado independiente o como parte de un producto de gestión de identidad y acceso más grande.

> En ocasiones, se puede utilizar una terminología diferente para un servidor de autorización, especialmente cuando la funcionalidad OAuth 2,0 está empaquetada dentro de un producto o solución de gestión de acceso e identidad más grande. Por ejemplo, el término **proveedor de identidad (IDP)** se utiliza con frecuencia indistintamente con **servidor de autorización**.

Administración

Además de emitir tokens de acceso, los servidores de autorización también proporcionan servicios administrativos relacionados, normalmente a través de una interfaz de usuario web. Por ejemplo, puede definir y administrar:

- Autenticación de usuarios y usuarios
- Ámbitos
- Segregación administrativa a través de inquilinos y dominios
- Aplicación de políticas
- Conexión a varios servicios externos
- Compatibilidad con otros protocolos de identidad (como SAML)

ONTAP es compatible con los servidores de autorización que cumplen con el estándar OAuth 2,0.

Definición a ONTAP

Debe definir uno o varios servidores de autorización para ONTAP. ONTAP se comunica de forma segura con cada servidor para verificar tokens y realizar otras tareas relacionadas en soporte de las aplicaciones cliente.

A continuación se presentan los principales aspectos de la configuración de ONTAP. Consulte también "Escenarios de despliegue de OAuth 2,0"para obtener más información.

Cómo y dónde se validan los tokens de acceso

Hay dos opciones para validar tokens de acceso.

- Validación local

ONTAP puede validar los tokens de acceso localmente en función de la información proporcionada por el servidor de autorización que emitió el token. ONTAP almacena en caché la información recuperada del servidor de autorización y se actualiza periódicamente.

- Introspección remota

  También puede utilizar la introspección remota para validar tokens en el servidor de autorización. La introspección es un protocolo que permite a las partes autorizadas consultar un servidor de autorización sobre un token de acceso. Proporciona a ONTAP una forma de extraer ciertos metadatos de un token de acceso y validar el token. ONTAP almacena en la caché algunos datos por razones de rendimiento.

Ubicación de red

ONTAP puede estar detrás de un firewall. En este caso, debe identificar un proxy como parte de la configuración.

Cómo se definen los servidores de autorización

Puede definir un servidor de autorización para ONTAP mediante cualquiera de las interfaces de administración, incluida la CLI, System Manager o la API DE REST. Por ejemplo, con la CLI utiliza el comando `security oauth2 client create`.

Obtenga más información sobre `security oauth2 client create` en el "Referencia de comandos del ONTAP".

Número de servidores de autorización

Puede definir hasta ocho servidores de autorización en un solo clúster de ONTAP. El mismo servidor de autorización se puede definir más de una vez en el mismo clúster de ONTAP, siempre y cuando las reclamaciones del emisor o del emisor/público sean únicas. Por ejemplo, con Keycloak esto siempre será el caso cuando se utilizan diferentes dominios.

Funciones de OAuth 2,0 admitidas en ONTAP

La compatibilidad con OAuth 2,0 estaba disponible inicialmente con ONTAP 9.14,1 y continúa mejorándose con las versiones posteriores. A continuación se describen las funciones de OAuth 2,0 compatibles con ONTAP.

Las funciones introducidas con una versión específica de ONTAP se transfieren a futuras versiones.

ONTAP 9.16.1

ONTAP 9.16,1 amplía las características estándar de OAuth 2,0 para incluir extensiones específicas de Entra ID para grupos nativos de Entra ID. Esto implica el uso de GUID en el token de acceso en lugar de nombres. Además, la versión agrega compatibilidad con la asignación de roles externos para asignar los roles de proveedor de identidad nativos a los roles de ONTAP mediante el campo “roles” en el token de acceso.

ONTAP 9.14.1

A partir de ONTAP 9.14,1, los servidores de autorización son compatibles con las siguientes funciones estándar de OAuth 2,0 para aplicaciones que utilizan:

- OAuth 2,0 con los campos estándar incluyendo “iss”, “aud” y “exp” como se describe en "RFC6749: El Marco de Autorización OAuth 2,0" y "RFC 7519: Token web JSON (JWT)". Esto también incluye soporte para la identificación única de usuarios a través de campos en el token de acceso como “upn”, “appid”,

“sub”, “username” o “preferred_username”.

- Extensiones específicas del proveedor de ADFS para nombres de grupo con el campo de grupo.
- Extensiones específicas del proveedor de Azure para UUID de grupo con el campo de grupo.
- Extensiones ONTAP para soporte de autorización mediante roles independientes y con nombre dentro del alcance del token de acceso OAuth 2,0. Esto incluye los campos “Alcance” y “scp”, así como los nombres de grupo dentro del alcance.

Uso de tokens de acceso OAuth 2,0

Los tokens de acceso OAuth 2,0 emitidos por los servidores de autorización son verificados por ONTAP y utilizados para tomar decisiones de acceso basadas en roles para las solicitudes del cliente API REST.

Adquiriendo un token de acceso

Es necesario adquirir un token de acceso de un servidor de autorización definido en el clúster de ONTAP donde se utiliza la API DE REST. Para adquirir un token, debe ponerse en contacto directamente con el servidor de autorización.

ONTAP no emite tokens de acceso ni redirige las solicitudes de los clientes a los servidores de autorización.

La forma en que se solicita un token depende de varios factores, entre ellos:

- Servidor de autorización y sus opciones de configuración
- Tipo de concesión OAuth 2,0
- Cliente o herramienta de software utilizada para emitir la solicitud

Tipos de concesión

Un *grant* es un proceso bien definido, que incluye un conjunto de flujos de red, utilizado para solicitar y recibir un token de acceso OAuth 2,0. Se pueden utilizar varios tipos de concesión diferentes en función del cliente, el entorno y los requisitos de seguridad. En la tabla siguiente se presenta una lista de los tipos de subvención más populares.

Tipo de concesión	Descripción
Credenciales de cliente	Tipo de concesión popular basado en el uso de solo credenciales (como un ID y un secreto compartido). Se supone que el cliente tiene una relación de confianza cercana con el propietario del recurso.
Contraseña	El tipo de concesión de credenciales de contraseña de propietario del recurso se puede utilizar en los casos en que el propietario del recurso tenga una relación de confianza establecida con el cliente. También puede ser útil al migrar clientes HTTP heredados a OAuth 2,0.
Código de autorización	Este es un tipo de concesión ideal para clientes confidenciales y se basa en un flujo basado en redirección. Se puede utilizar para obtener un token de acceso y un token de refrescamiento.

Contenido de JWT

Un token de acceso OAuth 2,0 se formatea como JWT. El contenido es creado por el servidor de autorización

en función de su configuración. Sin embargo, los tokens son opacos para las aplicaciones cliente. Un cliente no tiene ninguna razón para inspeccionar un token o para ser consciente de su contenido.

Cada token de acceso JWT contiene un juego de reclamaciones. Las reclamaciones describen las características del emisor y la autorización en función de las definiciones administrativas del servidor de autorización. Algunas de las reclamaciones registradas con el estándar se describen en la siguiente tabla. Todas las cadenas distinguen mayúsculas de minúsculas.

Reclamación	Palabra clave	Descripción
Emisor	iss	Identifica el principal que emitió el token. El procesamiento de la reclamación es específico de la aplicación.
Asunto	secundario	Asunto o usuario del token. El ámbito del nombre es global o localmente único.
Destinatarios	aud	Destinatarios para los que está destinado el token. Implementado como una matriz de cadenas.
Caducidad	esp	Hora después de la cual el token caduca y debe rechazarse.

Consulte "RFC 7519: Tokens web JSON" para obtener más información.

Autorización de cliente

Descripción general y opciones para la autorización del cliente de ONTAP

La implementación de ONTAP OAuth 2,0 está diseñada para ser flexible y robusta, proporcionando las características que necesita para proteger su entorno ONTAP. Hay varias opciones de configuración mutuamente excluyentes disponibles. Las decisiones de autorización se basan en última instancia en los roles REST DE ONTAP contenidos en o derivados de los tokens de acceso OAuth 2,0.

Sólo puede utilizarse "Roles DE REST de ONTAP" al configurar la autorización para OAuth 2,0. No se admiten los roles tradicionales de ONTAP anteriores.

ONTAP aplica la opción de autorización más adecuada en función de su configuración. Consulte "Cómo ONTAP determina el acceso" para obtener más información acerca de cómo ONTAP toma decisiones sobre el acceso de los clientes.

OAuth 2,0 ámbitos independientes

Estos ámbitos contienen uno o más roles REST personalizados, cada uno encapsulado dentro de una única cadena en el token de acceso. Son independientes de las definiciones de roles de ONTAP. Debe configurar las cadenas de ámbito en el servidor de autorización. Consulte "Alcances OAuth 2,0 autónomos" para obtener más información.

Roles DE REST DE ONTAP local

Se puede utilizar un único rol REST con nombre, ya sea Builtin o Custom. La sintaxis del ámbito para un rol con nombre es **ontap-role-**<URL-encoded-ONTAP-role-name>. Por ejemplo, si el rol ONTAP es `admin` la cadena de ámbito será `ontap-role-admin`.

Usuarios

Se puede utilizar el nombre de usuario en el token de acceso definido con acceso a la aplicación http. Un usuario se prueba en el siguiente orden según el método de autenticación definido: Contraseña, dominio (Active Directory), nsswitch (LDAP).

Grupos

Los servidores de autorización se pueden configurar para utilizar grupos ONTAP para su autorización. Si se examinan las definiciones de ONTAP locales pero no se puede tomar ninguna decisión de acceso, se utilizan los grupos de Active Directory («dominio») o LDAP («nsswitch»). La información del grupo se puede especificar de dos formas:

- Cadena de ámbito de OAuth 2,0

  Admite aplicaciones confidenciales mediante el flujo de credenciales de cliente donde no hay ningún usuario con una pertenencia a grupo. El ámbito debe denominarse **ontap-group-**<URL-encoded-ONTAP-group-name>. Por ejemplo, si el grupo está en «desarrollo», la cadena de alcance será «ontap-group-development».

- En el reclamo de “grupo”

  Esto está destinado a los tokens de acceso emitidos por ADFS mediante el flujo de propietario de recursos (concesión de contraseña).

Ver "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" Para más información.

Ámbitos OAuth 2.0 autónomos en ONTAP

Los ámbitos autónomos son cadenas que se llevan en el token de acceso. Cada una de ellas es una definición de función personalizada completa e incluye todo lo que ONTAP necesita para tomar una decisión de acceso. El ámbito está separado y distinto de cualquiera de los roles de REST definidos en el propio ONTAP.

Formato de la cadena de ámbito

En un nivel base, el ámbito se representa como una cadena contigua y se compone de seis valores separados por dos puntos. Los parámetros utilizados en la cadena de ámbito se describen a continuación.

ONTAP literal

El ámbito debe comenzar con el valor literal `ontap` en minúscula. Identifica el ámbito como específico de ONTAP.

Clúster

Esto define al cluster de ONTAP al que se aplica el ámbito. Los valores pueden incluir:

- UUID del clúster

  Identifica un único clúster.

- Asterisco (*)

  Indica que el ámbito se aplica a todos los clusters.

Puede utilizar el comando de la CLI de ONTAP `cluster identity show` para mostrar el UUID de su clúster. Si no se especifica, el ámbito se aplica a todos los clusters. Obtenga más información sobre `cluster identity show` en el "Referencia de comandos del ONTAP".

Función

Nombre del rol REST contenido en el ámbito autónomo. ONTAP no examina este valor ni se relaciona con ningún rol de REST existente definido con ONTAP. El nombre se utiliza para el registro.

Nivel de acceso

Este valor indica el nivel de acceso aplicado a la aplicación cliente cuando se utiliza el punto final de API en el ámbito. Hay seis valores posibles, como se describe en la tabla siguiente.

Nivel de acceso	Descripción
ninguno	Deniega todo el acceso al punto final especificado.
sólo lectura	Permite solo el acceso de lectura mediante GET.
read_create	Permite el acceso de lectura, así como la creación de nuevas instancias de recursos mediante POST.
read_modify	Permite el acceso de lectura, así como la capacidad de actualizar los recursos existentes MEDIANTE PARCHE.
read_create_modify	Permite todos los accesos excepto eliminar. Las operaciones permitidas incluyen GET (READ), POST (CREATE) y PARCHE (UPDATE).
todo	Permite un acceso completo.

SVM

El nombre de la SVM dentro del clúster al que se aplica el ámbito. Utilice el valor * (asterisco) para indicar todas las SVM.

> Esta función no es totalmente compatible con ONTAP 9.14.1. Puede ignorar el parámetro SVM y usar un asterisco como marcador de posición. Revise el "Notas de la versión de ONTAP" para comprobar si hay compatibilidad con SVM en el futuro.

URI DE LA API DE REST

Ruta de acceso completa o parcial a un recurso o juego de recursos relacionados. La cadena debe comenzar por `/api`. Si no especifica un valor, el alcance se aplica a todos los extremos de API en el clúster de ONTAP.

Ejemplos de ámbito

A continuación se presentan algunos ejemplos de ámbitos autónomos.

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

Proporciona al usuario asignado a este rol acceso de lectura, creación y modificación al `/cluster` punto final.

Herramienta administrativa de la CLI

Para que la administración de los ámbitos autónomos sea más fácil y menos propensa a errores, ONTAP proporciona el comando CLI `security oauth2 scope` para generar cadenas de alcance basadas en los parámetros de entrada.

El comando `security oauth2 scope` tiene dos casos de uso basados en su entrada:

- Parámetros de CLI para la cadena de ámbito

  Puede utilizar esta versión del comando para generar una cadena de ámbito basada en los parámetros de entrada.

- Cadena de ámbito para parámetros de CLI

  Puede utilizar esta versión del comando para generar los parámetros del comando basados en la cadena de ámbito de entrada.

Ejemplo

El siguiente ejemplo genera una cadena de ámbito con la salida incluida después del siguiente ejemplo de comando. La definición se aplica a todos los clusters.

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

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

Obtenga más información sobre `security oauth2 scope` en el "Referencia de comandos del ONTAP".

Mapeo de roles externos de OAuth 2.0 en ONTAP

Un rol externo se define en un proveedor de identificación configurado para su uso por ONTAP. Es posible crear y administrar relaciones de asignación entre estos roles externos y los roles de ONTAP mediante la CLI de ONTAP.

> También es posible configurar la función de asignación de roles externos mediante la API DE REST DE ONTAP. Obtenga más información en el "Documentación de automatización de ONTAP".

Roles externos en un token de acceso

Aquí hay un fragmento de un token de acceso JSON que contiene dos roles externos.

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

Configuración

Puede utilizar la interfaz de línea de comandos de ONTAP para administrar la función de asignación de roles externos.

Crear

Puede definir una configuración de asignación de roles con `security login external-role-mapping create` el comando. Debe estar en el nivel de privilegio **admin** de ONTAP para emitir este comando, así como las opciones relacionadas.

Parámetros

A continuación se describen los parámetros utilizados para crear una asignación de grupo.

Parámetro	Descripción
`external-role`	Nombre del rol definido en el proveedor de identidad externo.
`provider`	Nombre del proveedor de identidad. Este debe ser el identificador del sistema.
`ontap-role`	Indica el rol de ONTAP existente al que está asignado el rol externo.

Ejemplo

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

Obtenga más información sobre `security login external-role-mapping create` en el "Referencia de comandos del ONTAP".

Operaciones de CLI adicionales

El comando admite varias operaciones adicionales, entre las que se incluyen:

- Mostrar
- Modificar

- Eliminar

Información relacionada

- "Referencia de comandos del ONTAP"

Cómo determina ONTAP el acceso del cliente

Para diseñar e implementar correctamente OAuth 2,0, es necesario comprender cómo ONTAP utiliza su configuración de autorización para tomar decisiones de acceso para los clientes. Los pasos principales utilizados para determinar el acceso se presentan a continuación en función de la versión de ONTAP.

No hubo actualizaciones significativas de OAuth 2,0 con ONTAP 9.15,1. Si utiliza la versión 9.15.1, consulte la descripción de ONTAP 9.14,1.

Información relacionada

- "Funciones de OAuth 2,0 admitidas en ONTAP"

ONTAP 9.16.1

ONTAP 9.16,1 amplía la compatibilidad estándar con OAuth 2,0 para incluir extensiones específicas de Microsoft Entra ID para grupos nativos de Entra ID, así como la asignación de roles externos.

Determine el acceso de clientes para ONTAP 9.16,1

Paso 1: Ámbitos autónomos

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina estos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

Paso 2: Compruebe el indicador de roles locales

ONTAP examina el parámetro booleano `use-local-roles-if-present` . El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true`, continúe en el paso 3.
- Si el valor `false` finaliza el procesamiento y se deniega el acceso.

Paso 3: Se denomina rol REST ONTAP

Si el token de acceso contiene un rol REST con nombre en el `scope` campo o `scp`, o como una reclamación, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

Paso 4: Usuarios

Extraiga el nombre de usuario del token de acceso e intente hacer coincidir el nombre con los usuarios que tienen acceso a la aplicación «http». Los usuarios se examinan según el método de autenticación en el siguiente orden:

- contraseña
- Dominio (Active Directory)
- Conmutador ns(LDAP)

Si se encuentra un usuario coincidente, ONTAP utiliza el rol definido para el usuario para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario no coincide o no hay nombre de usuario en el token de acceso, continúe con el paso 5.

Paso 5: Grupos

Si se incluyen uno o más grupos, se examina el formato. Si los grupos se representan como UUID, se busca en una tabla interna de mapeo de grupos. Si hay una coincidencia de grupo y un rol asociado, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento finaliza. Para más información, consulte "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" .

Si los grupos se representan como nombres y se configuran con autorización de dominio o nsswitch, ONTAP intenta relacionarlos con un grupo de Active Directory o LDAP, respectivamente. Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.

ONTAP 9.14.1

OAuth 2,0 inicial admitido se introduce con ONTAP 9.14,1 basado en las características estándar de OAuth 2,0.

Determine el acceso de clientes para ONTAP 9.14,1

Paso 1: Ámbitos autónomos

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina estos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

Paso 2: Compruebe el indicador de roles locales

ONTAP examina el parámetro booleano `use-local-roles-if-present` . El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true`, continúe en el paso 3.
- Si el valor `false` finaliza el procesamiento y se deniega el acceso.

Paso 3: Se denomina rol REST ONTAP

Si el token de acceso contiene un rol REST con nombre en el `scope` campo OR `scp`, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

Paso 4: Usuarios

Extraiga el nombre de usuario del token de acceso e intente hacer coincidir el nombre con los usuarios que tienen acceso a la aplicación «http». Los usuarios se examinan según el método de autenticación en el siguiente orden:

- contraseña
- Dominio (Active Directory)
- Conmutador ns(LDAP)

Si se encuentra un usuario coincidente, ONTAP utiliza el rol definido para el usuario para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario no coincide o no hay nombre de usuario en el token de acceso, continúe con el paso 5.

Paso 5: Grupos

Si se incluyen uno o más grupos y se configuran con autorización de dominio o nsswitch, ONTAP intenta relacionarlos con un grupo LDAP o Active Directory, respectivamente.

Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.

Escenarios de implementación de OAuth 2.0 con ONTAP

Hay varias opciones de configuración disponibles al definir un servidor de autorización en ONTAP. En función de estas opciones, puede definir un servidor de autorización adecuado para su entorno mediante uno de los varios escenarios de implementación.

Resumen de los parámetros de configuración

Hay varios parámetros de configuración disponibles al definir un servidor de autorización en ONTAP. Estos parámetros se admiten generalmente en todas las interfaces administrativas.

> El nombre utilizado para un parámetro o campo individual puede variar en función de la interfaz administrativa de ONTAP. Para acomodar las diferencias en las interfaces administrativas, se utiliza un único nombre genérico para cada parámetro de la tabla. El nombre exacto utilizado con una interfaz específica debe ser obvio basado en el contexto.

Parámetro	Descripción
Nombre	Nombre del servidor de autorización tal y como lo conoce ONTAP.
Cliente más	Aplicación interna de ONTAP a la que se aplica la definición. Debe ser **http**.
URI del emisor	El FQDN con ruta que identifica el sitio u organización que emite los tokens.
URI de JWKS de Proveedor	El FQDN con ruta y nombre de archivo donde ONTAP obtiene los conjuntos de claves web JSON utilizados para validar los tokens de acceso.
Intervalo de refrescamiento de JWKS	Intervalo de tiempo que determina la frecuencia con la que ONTAP refresca la información de certificado del URI JWKS del proveedor. El valor se especifica en formato ISO-8601.
Punto final de introspección	El FQDN con ruta que ONTAP utiliza para realizar la validación remota de tokens mediante introspección.
ID del cliente	El nombre del cliente tal y como se define en el servidor de autorización. Cuando se incluye este valor, también debe proporcionar el secreto de cliente asociado basado en la interfaz.
Proxy saliente	Esto es para proporcionar acceso al servidor de autorización cuando ONTAP está detrás de un firewall. El URI debe tener el formato cURL.
Utilice roles locales si están presentes	Un indicador booleano que determina si se usan las definiciones de ONTAP locales, incluido un rol REST con nombre y los usuarios locales.
Reclamación de usuario remoto	Nombre alternativo que utiliza ONTAP para coincidir con los usuarios locales. Utilice `sub` el campo del token de acceso para que coincida con el nombre de usuario local.
Destinatarios	Este campo define los puntos finales en los que se puede utilizar el token de acceso.

Escenarios de puesta en marcha

A continuación se presentan varios escenarios de implementación comunes. Se organizan en función de si ONTAP realiza la validación de tokens de forma local o remota mediante el servidor de autorización. Cada escenario incluye una lista de las opciones de configuración necesarias. Consulte "Desplegar OAuth 2,0 en

ONTAP" para obtener ejemplos de los comandos de configuración.

Después de definir un servidor de autorización, puede mostrar su configuración a través de la interfaz administrativa de ONTAP. Por ejemplo, utilice el comando `security oauth2 client show` con la interfaz de línea de comandos de ONTAP.

Validación local

Los siguientes escenarios de implementación se basan en que ONTAP realiza la validación de tokens localmente.

Utilice ámbitos autónomos sin proxy

Esta es la implementación más sencilla utilizando solo los ámbitos autónomos de OAuth 2,0. No se utiliza ninguna definición de identidad ONTAP local. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- URI del emisor

También debe añadir los ámbitos en el servidor de autorización.

Utilice ámbitos autónomos con un proxy

Este escenario de despliegue utiliza los ámbitos autónomos de OAuth 2,0. No se utiliza ninguna definición de identidad ONTAP local. Pero el servidor de autorización está detrás de un firewall y, por lo tanto, debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Proxy saliente
- URI del emisor
- Destinatarios

También debe añadir los ámbitos en el servidor de autorización.

Use los roles de usuario local y la asignación predeterminada del nombre de usuario con un proxy

Este escenario de despliegue utiliza roles de usuario local con asignación de nombres por defecto. La reclamación de usuario remoto utiliza el valor predeterminado de `sub`, por lo que este campo del token de acceso se utiliza para coincidir con el nombre de usuario local. El nombre de usuario debe tener 40 caracteres o menos. El servidor de autorización está detrás de un firewall, por lo que también debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Usar roles locales si están presentes (`true`)
- Proxy saliente

- Emisor

Debe asegurarse de que el usuario local esté definido en ONTAP.

Use roles de usuario local y una asignación de nombre de usuario alternativa con un proxy

Este escenario de despliegue utiliza roles de usuario local con un nombre de usuario alternativo que se utiliza para que coincida con un usuario local de ONTAP. El servidor de autorización está detrás de un firewall, por lo que debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Usar roles locales si están presentes (`true`)
- Reclamación de usuario remoto
- Proxy saliente
- URI del emisor
- Destinatarios

Debe asegurarse de que el usuario local esté definido en ONTAP.

Introspección remota

Las siguientes configuraciones de implementación se basan en que ONTAP realiza la validación de tokens de forma remota a través de introspección.

Utilice ámbitos autónomos sin proxy

Esta es una implementación sencilla basada en el uso de los ámbitos autónomos OAuth 2,0. No se utiliza ninguna definición de identidad de ONTAP. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- Punto final de introspección
- ID del cliente
- URI del emisor

Debe definir los ámbitos, así como el secreto de cliente y cliente en el servidor de autorización.

Información relacionada

- "Mostrar cliente de seguridad OAuth2"

Autenticación de cliente ONTAP mediante OAuth 2.0 Mutual TLS

Dependiendo de sus necesidades de seguridad, puede configurar opcionalmente TLS mutuo (MTLS) para implementar una autenticación de cliente fuerte. Cuando se utiliza con ONTAP como parte de una implementación de OAuth 2,0, MTLS garantiza que los tokens de acceso solo son utilizados por los clientes a los que se emitieron

originalmente.

TLS Mutuo con OAuth 2,0

La seguridad de la capa de transporte (TLS) se utiliza para establecer un canal de comunicación seguro entre dos aplicaciones, normalmente un explorador de cliente y un servidor web. El TLS Mutuo amplía esto proporcionando una identificación sólida del cliente a través de un certificado de cliente. Cuando se utiliza en un clúster de ONTAP con OAuth 2,0, la funcionalidad MTLS base se amplía mediante la creación y el uso de tokens de acceso restringidos por el remitente.

Un token de acceso restringido por remitente solo puede ser utilizado por el cliente para el que se emitió originalmente. Para admitir esta función, (`cnf`se inserta una nueva reclamación de confirmación) en el token. El campo contiene la propiedad `x5t#S256` que contiene un resumen del certificado de cliente utilizado al solicitar el token de acceso. ONTAP verifica este valor como parte de la validación del token. Los tokens de acceso emitidos por los servidores de autorización que no están restringidos por el remitente no incluyen la reclamación de confirmación adicional.

Debe configurar ONTAP para que utilice MTLS por separado para cada servidor de autorización. Por ejemplo, el comando CLI `security oauth2 client` incluye el parámetro `use-mutual-tls` para controlar el procesamiento MTLS basado en tres valores como se muestra en la tabla siguiente.

> En cada configuración, el resultado y la acción de ONTAP dependen del valor del parámetro de configuración, así como del contenido del token de acceso y del certificado del cliente. Los parámetros de la tabla se organizan desde el más mínimo hasta el más restrictivo.

Parámetro	Descripción
ninguno	La autenticación TLS mutua OAuth 2,0 está completamente desactivada para el servidor de autorización. ONTAP no realizará la autenticación del certificado de cliente MTLS incluso si la reclamación de confirmación está presente en el token o si se proporciona un certificado de cliente con la conexión TLS.
petición	OAuth 2,0 La autenticación TLS mutua se aplica si el cliente presenta un token de acceso restringido por el remitente. Es decir, MTLS se aplica sólo si la reclamación de confirmación (con propiedad `x5t#S256`) está presente en el token de acceso. Esta es la configuración predeterminada.
obligatorio	La autenticación TLS mutua OAuth 2,0 se aplica a todos los tokens de acceso emitidos por el servidor de autorización. Por lo tanto, todos los tokens de acceso deben estar restringidos por el remitente. Se producen errores en la autenticación y la solicitud de API de REST si la reclamación de confirmación no está presente en el token de acceso o si existe un certificado de cliente no válido.

Flujo de implantación de alto nivel

A continuación se presentan los pasos típicos que implica el uso de MTLS con OAuth 2,0 en un entorno ONTAP. Consulte "RFC 8705: Autenticación de cliente Mutual-TLS de OAuth 2,0 y tokens de acceso vinculados a certificados" para obtener más información.

Paso 1: Crear e instalar un certificado de cliente

El establecimiento de la identidad del cliente se basa en demostrar el conocimiento de una clave privada del cliente. La clave pública correspondiente se coloca en un certificado X,509 firmado presentado por el cliente. En un nivel alto, los pasos involucrados en la creación del certificado de cliente incluyen:

1. Generar un par de claves públicas y privadas
2. Cree una solicitud de firma de certificación
3. Envíe el archivo CSR a una CA conocida
4. CA verifica la solicitud y emite el certificado firmado

Normalmente, puede instalar el certificado de cliente en su sistema operativo local o usarlo directamente con una utilidad común, como cURL.

Paso 2: Configure ONTAP para usar MTLS

Debe configurar ONTAP para que utilice MTLS. Esta configuración se realiza por separado para cada servidor de autorización. Por ejemplo, con la CLI el comando `security oauth2 client` se utiliza con el parámetro opcional `use-mutual-tls` . Consulte "Desplegar OAuth 2,0 en ONTAP" para obtener más información.

Paso 3: El cliente solicita un token de acceso

El cliente necesita solicitar un token de acceso desde el servidor de autorización configurado en ONTAP. La aplicación cliente debe utilizar MTLS con el certificado creado e instalado en el paso 1.

Paso 4: El servidor de autorización genera el token de acceso

El servidor de autorización verifica la solicitud del cliente y genera un token de acceso. Como parte de esto, crea un resumen de mensaje del certificado de cliente que se incluye en el token como una reclamación de confirmación (campo `cnf`).

Paso 5: La aplicación cliente presenta el token de acceso a ONTAP

La aplicación cliente realiza una llamada a la API REST al clúster de ONTAP e incluye el token de acceso en el encabezado de solicitud de autorización como un token **portador**. El cliente debe utilizar MTLS con el mismo certificado utilizado para solicitar el token de acceso.

Paso 6: ONTAP verifica el cliente y el token.

ONTAP recibe el token de acceso en una solicitud HTTP, así como el certificado de cliente utilizado como parte del procesamiento MTLS. ONTAP valida primero la firma en el token de acceso. En función de la configuración, ONTAP genera un resumen de mensaje del certificado de cliente y lo compara con la reclamación de confirmación **cnf** en el token. Si los dos valores coinciden, ONTAP ha confirmado que el cliente que hace la solicitud API es el mismo cliente al que se emitió originalmente el token de acceso.

Información relacionada

- "cliente de seguridad oauth2"