Conceptos

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Conceptos

Servidores de autorización y tokens de acceso

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" si quiere 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`.

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.

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" si quiere más información.

Opciones para la autorización de cliente de ONTAP

Hay varias opciones disponibles para personalizar la autorización de cliente de ONTAP. Las decisiones de autorización se basan, en última instancia, en los roles REST DE ONTAP contenidos en o derivados de los tokens de acceso.

> Solo puede utilizar "Roles DE REST de ONTAP" Al configurar la autorización para OAuth 2,0. No se admiten los roles tradicionales de ONTAP anteriores.

Introducción

La implementación de OAuth 2,0 en ONTAP está diseñada para ser flexible y robusta, proporcionando las opciones que necesita para proteger el entorno ONTAP. En un nivel superior, hay tres categorías de

configuración principales para definir la autorización de cliente de ONTAP. Estas opciones de configuración son mutuamente excluyentes.

ONTAP aplica la opción más adecuada en función de su configuración. Consulte "Cómo ONTAP determina el acceso" Para obtener más información sobre cómo ONTAP procesa sus definiciones de configuración para tomar decisiones de acceso.

OAuth 2,0 ámbitos independientes

Estos ámbitos contienen uno o más roles REST personalizados, cada uno encapsulado en una sola cadena. Son independientes de las definiciones de roles de ONTAP. Debe definir estas cadenas de ámbito en el servidor de autorización.

Roles y usuarios de REST locales específicos de ONTAP

Según su configuración, las definiciones de identidad ONTAP locales se pueden utilizar para tomar decisiones de acceso. Las opciones incluyen:

- Rol REST con nombre único
- La coincidencia del nombre de usuario con un usuario de ONTAP local

La sintaxis del ámbito para un rol con nombre es **ontap-role-**<URL-encoded-ONTAP-role-name>. Por ejemplo, si el rol es «admin», la cadena de alcance será «ontap-role-admin».

Grupos de Active Directory o LDAP

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).

Alcances OAuth 2,0 autónomos

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 de clúster

  Identifica un único clúster.

- Asterisco (*)

  Indica que el ámbito se aplica a todos los clusters.

Puede usar el comando de la CLI de ONTAP `cluster identity show` Para mostrar el UUID del clúster. Si no se especifica, el ámbito se aplica a todos los clusters.

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 la "Notas de la versión de ONTAP" Para comprobar si hay compatibilidad futura con SVM.

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` extremo.

Herramienta administrativa de la CLI

Para que la administración de los ámbitos autónomos sea más sencilla y menos propensa a errores, ONTAP proporciona el comando de la 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 información:

- 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
```

Cómo ONTAP determina el acceso

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.

Paso 1: Ámbitos autónomos

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina esos 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 valor de la bandera `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 con el paso 3.
- Si el valor es `false` el procesamiento finaliza y se deniega el acceso.

Paso 3: Se denomina rol REST ONTAP

Si el token de acceso contiene un rol REST con nombre, 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 locales de ONTAP

Extraiga el nombre de usuario del token de acceso e intente relacionarlo con un usuario local de ONTAP.

Si un usuario local de ONTAP coincide, ONTAP utiliza el rol definido para que el usuario tome una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

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

Paso 5: Asignación de grupos a roles

Extraiga el grupo del token de acceso e intente relacionarlo con un grupo. Los grupos se definen mediante Active Directory o un servidor LDAP equivalente.

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 despliegue de OAuth 2,0

Hay varias opciones de configuración disponibles al definir un servidor de autorización en ONTAP. Basándose en estas opciones, puede crear un servidor de autorización adecuado para su entorno de despliegue.

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.

Los nombres de los parámetros pueden variar levemente dependiendo de la interfaz administrativa de ONTAP. Por ejemplo, al configurar la introspección remota, el punto final se identifica mediante el parámetro de comando CLI `-introspection-endpoint`. Pero con System Manager, el campo equivalente es *Authorization server token introspection URI*. Para acomodar todas las interfaces administrativas de ONTAP, se proporciona una descripción general de los parámetros. El parámetro o campo exacto debe ser obvio en función del 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.
Eliminar reclamación de usuario	Nombre alternativo que utiliza ONTAP para coincidir con los usuarios locales. Utilice la `sub` del token de acceso para que coincida con el nombre de usuario local.

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 ver 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 CLI 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 tanto, este campo en el 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
- Utilice 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
- Utilice 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.

Autenticación de clientes mediante TLS mutuo

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, una nueva reclamación de confirmación (`cnf`) se inserta en el token. El campo contiene propiedad `x5t#S256` 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 de la 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 solo 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 detalles.

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" si quiere 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.