Configurar e implementar

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Configurar e implementar

Prepárese para implementar OAuth 2,0 con ONTAP

Antes de configurar OAuth 2,0 en un entorno ONTAP, debe prepararse para el despliegue. A continuación se incluye un resumen de las principales tareas y decisiones. La disposición de las secciones generalmente está alineada con el orden que debe seguir. Sin embargo, si bien es aplicable a la mayoría de las implementaciones, debe adaptarlo a su entorno según sea necesario. También debe considerar la creación de un plan de despliegue formal.

> En función del entorno, puede seleccionar la configuración de los servidores de autorización definidos en ONTAP. Esto incluye los valores de parámetros que necesita especificar para cada tipo de despliegue. Consulte "Escenarios de despliegue de OAuth 2,0" si quiere más información.

Recursos protegidos y aplicaciones cliente

OAuth 2,0 es un marco de autorización para controlar el acceso a los recursos protegidos. Dado esto, un primer paso importante en cualquier implementación es determinar cuáles son los recursos disponibles y qué clientes necesitan acceder a ellos.

Identificar aplicaciones cliente

Debe decidir qué clientes utilizarán OAuth 2,0 al emitir llamadas a la API REST y a qué puntos finales API necesitan acceso.

Revisar los roles DE REST DE ONTAP y los usuarios locales existentes

Debe revisar las definiciones de identidad ONTAP existentes, incluidos los roles REST y los usuarios locales. Dependiendo de cómo configure OAuth 2,0, estas definiciones se pueden utilizar para tomar decisiones de acceso.

Transición global a OAuth 2,0

Aunque puede implementar la autorización OAuth 2,0 gradualmente, también puede mover todos los clientes de la API REST a OAuth 2,0 inmediatamente estableciendo un indicador global para cada servidor de autorización. Esto permite tomar decisiones de acceso según la configuración de ONTAP existente sin necesidad de crear ámbitos independientes.

Servidores de autorización

Los servidores de autorización desempeñan un papel importante en su implementación de OAuth 2,0 mediante la emisión de tokens de acceso y la aplicación de la política administrativa.

Seleccione e instale el servidor de autorización

Debe seleccionar e instalar uno o más servidores de autorización. Es importante familiarizarse con las opciones de configuración y los procedimientos de sus proveedores de identidad, incluido cómo definir ámbitos.

Determine si es necesario instalar el certificado de CA raíz de autorización

ONTAP utiliza el certificado del servidor de autorización para validar los tokens de acceso firmados presentados por los clientes. Para hacerlo, ONTAP necesita el certificado de CA raíz y todos los certificados

intermedios. Estos pueden preinstalarse con ONTAP. Si no es así, debe instalarlos.

Evalúe la ubicación y la configuración de la red

Si el servidor de autorización está detrás de un firewall, ONTAP debe configurarse para utilizar un servidor proxy.

Autenticación y autorización de clientes

Hay varios aspectos de la autenticación y autorización del cliente que debe considerar.

Ámbitos autónomos o definiciones de identidad locales de ONTAP

En un nivel superior, puede definir ámbitos independientes definidos en el servidor de autorización o basarse en las definiciones de identidad de ONTAP local existentes, incluidos los roles y los usuarios.

Opciones con procesamiento ONTAP local

Si utiliza las definiciones de identidad de ONTAP, debe decidir cuáles aplicar, entre ellas:

- Rol REST con nombre
- Coincide con los usuarios locales
- Grupos de Active Directory o LDAP

Validación local o introspección remota

Debe decidir si los tokens de acceso serán validados localmente por ONTAP o en el servidor de autorización mediante introspección. También hay varios valores relacionados que se deben tener en cuenta, como el intervalo de refrescamiento.

Tokens de acceso restringidos por el remitente

Para entornos que requieren un alto nivel de seguridad, puede utilizar tokens de acceso con restricciones de envío basados en MTLS. Esto requiere un certificado para cada cliente.

Interfaz administrativa

Puede realizar la administración de OAuth 2,0 a través de cualquiera de las interfaces ONTAP, incluyendo:

- Interfaz de línea de comandos
- System Manager
- API REST

Cómo solicitan los clientes tokens de acceso

Las aplicaciones cliente deben solicitar tokens de acceso directamente desde el servidor de autorización. Debe decidir cómo se hará esto, incluido el tipo de subvención.

Configure ONTAP

Debe realizar varias tareas de configuración de ONTAP.

Defina los roles REST y los usuarios locales

En función de la configuración de autorización, se puede utilizar el procesamiento de identificación de ONTAP local. En este caso, debe revisar y definir los roles REST y las definiciones de usuario.

Configuración central

Hay tres pasos principales necesarios para llevar a cabo la configuración principal de ONTAP, incluyendo los

siguientes:

- Opcionalmente, instale el certificado raíz (y cualquier certificado intermedio) para la CA que firmó el certificado del servidor de autorización.
- Defina el servidor de autorización.
- Habilite el procesamiento de OAuth 2,0 para el clúster.

Desplegar OAuth 2,0 en ONTAP

La implementación de la funcionalidad principal de OAuth 2,0 implica tres pasos principales.

Antes de empezar

Debe prepararse para el despliegue de OAuth 2,0 antes de configurar ONTAP. Por ejemplo, debe evaluar el servidor de autorización, incluido cómo se firmó su certificado y si está detrás de un firewall. Consulte "Prepárese para implementar OAuth 2,0 con ONTAP" si quiere más información.

Paso 1: Instale el certificado del servidor de autenticación

ONTAP incluye un gran número de certificados de CA raíz preinstalados. Por lo tanto, en muchos casos, el certificado para su servidor de autorización será reconocido inmediatamente por ONTAP sin configuración adicional. Pero dependiendo de cómo se haya firmado el certificado del servidor de autorización, es posible que necesite instalar un certificado de CA raíz y cualquier certificado intermedio.

Siga las instrucciones proporcionadas a continuación para instalar el certificado si es necesario. Debe instalar todos los certificados necesarios en el nivel de clúster.

Elija el procedimiento correcto en función de cómo acceda a ONTAP.

Ejemplo 1. Pasos

System Manager

1. En System Manager, selecciona **Clúster** > **Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en → junto a **Certificados**.
4. En la pestaña **Autoridades de certificación de confianza**, haga clic en **Agregar**.
5. Haga clic en **Importar** y seleccione el archivo de certificado.
6. Complete los parámetros de configuración del entorno.
7. Haga clic en **Agregar**.

CLI

1. Comience la instalación:

   ```
   security certificate install -type server-ca
   ```

2. Busque el siguiente mensaje de la consola:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Abra el archivo de certificado con un editor de texto.
4. Copie todo el certificado, incluidas las siguientes líneas:

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. Pegue el certificado en el terminal después del símbolo del sistema.
6. Presione **Enter** para completar la instalación.
7. Confirme la instalación del certificado mediante uno de los siguientes métodos:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Paso 2: Configure el servidor de autorización

Debe definir al menos un servidor de autorización para ONTAP. Debe elegir los valores de los parámetros en función de su plan de configuración e implementación. Revisar "Situaciones de puesta en marcha de OAuth2" para determinar los parámetros exactos necesarios para la configuración.

> Para modificar una definición de servidor de autorización, puede suprimir la definición existente y crear una nueva.

El ejemplo que se proporciona a continuación se basa en el primer escenario de implementación simple en "Validación local". Los ámbitos autónomos se utilizan sin un proxy.

Elija el procedimiento correcto en función de cómo acceda a ONTAP. El procedimiento de la CLI utiliza variables simbólicas que hay que reemplazar antes de emitir el comando.

Ejemplo 2. Pasos

System Manager

1. En System Manager, selecciona **Clúster** > **Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en **+** junto a **Autorización OAuth 2,0**.
4. Selecciona **Más opciones**.
5. Proporcione los valores necesarios para el despliegue, como:
   - Nombre
   - Aplicación (http)
   - URI de JWKS de Proveedor
   - URI del emisor
6. Haga clic en **Agregar**.

CLI

1. Vuelva a crear la definición:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   Por ejemplo:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

Paso 3: Habilite OAuth 2,0

El paso final es habilitar OAuth 2,0. Se trata de una configuración global para el clúster de ONTAP.

> No habilite el procesamiento de OAuth 2,0 hasta que confirme que ONTAP, los servidores de autorización y los servicios de soporte se han configurado correctamente.

Elija el procedimiento correcto en función de cómo acceda a ONTAP.

Ejemplo 3. Pasos

System Manager

1. En System Manager, selecciona **Clúster** > **Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en → junto a **OAuth 2,0 AUTORIZATION**.
4. Habilita **OAuth 2,0 autorización**.

CLI

1. Activar OAuth 2,0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirme que OAuth 2,0 está activado:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Emita una llamada a la API REST mediante OAuth 2,0

La implementación de OAuth 2,0 en ONTAP es compatible con las aplicaciones del cliente API de REST. Puede emitir una llamada a la API de REST simple usando cURL para comenzar a usar OAuth 2,0. El ejemplo que se presenta a continuación recupera la versión del cluster de ONTAP.

Antes de empezar

Tiene que configurar y habilitar la función OAuth 2,0 para el clúster de ONTAP. Esto incluye la definición de un servidor de autorización.

Paso 1: Adquiera un token de acceso

Debe adquirir un token de acceso para utilizarlo con la llamada de la API de REST. La solicitud de token se realiza fuera de ONTAP y el procedimiento exacto depende del servidor de autorización y de su configuración. Puede solicitar el token a través de un navegador web, con un comando curl o utilizando un lenguaje de programación.

Para fines ilustrativos, a continuación se presenta un ejemplo de cómo se puede solicitar un token de acceso desde Keycloak usando curl.

Ejemplo de Keycloak

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Debe copiar y guardar el token devuelto.

Paso 2: Emita la llamada a la API de REST

Una vez que tenga un token de acceso válido, puede usar un comando cURL con el token de acceso para emitir una llamada a la API de REST.

Parámetros y variables

Las dos variables del ejemplo de curl se describen en la tabla siguiente.

Variable	Descripción
$FQDN_IP	El nombre de dominio completo o la dirección IP de la LIF de gestión de ONTAP.
$ACCESS_TOKEN	El token de acceso OAuth 2,0 emitido por el servidor de autorización.

Primero debe definir estas variables en el entorno de shell de Bash antes de emitir el ejemplo de cURL. Por ejemplo, en la CLI de Linux escriba el siguiente comando para establecer y mostrar la variable FQDN:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Después de definir ambas variables en el shell Bash local, puede copiar el comando cURL y pegarlo en la CLI. Presione **Enter** para sustituir las variables y emitir el comando.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```