配置和部署
ONTAP 9

NetApp
April 24, 2024

目录

配置和部署

准备使用ONTAP部署OAuth2.0

在ONTAP环境中配置OAuth2.0之前、您应做好部署准备。主要任务和决定摘要如下。各部分的排列通常与您应遵循的顺序一致。但是、虽然它适用于大多数部署、但您应根据需要对其进行调整以适应您的环境。您还应考虑制定正式的部署计划。

> 您可以根据您的环境为定义给ONTAP的授权服务器选择配置。其中包括您需要为每种部署类型指定的参数值。请参见 "OAuth2.0部署方案" 有关详细信息 …

受保护的资源和客户端应用程序

OAuth2.0是一个授权框架、用于控制对受保护资源的访问。因此、任何部署的重要第一步都是确定可用资源是什么以及哪些客户端需要访问这些资源。

识别客户端应用程序

您需要确定哪些客户端在发出REST API调用时将使用OAuth2.0、以及它们需要访问哪些API端点。

查看现有**ONTAP REST**角色和本地用户

您应查看现有ONTAP标识定义、包括REST角色和本地用户。根据您配置OAuth2.0的方式、可以使用这些定义来决定访问。

全局过渡到**OAuth2.0**

虽然您可以逐步实施OAuth2.0授权、但也可以通过为每个授权服务器设置一个全局标志、将所有REST API客户端立即迁移到OAuth2.0。这样、无需创建独立的范围、即可根据现有ONTAP配置做出访问决策。

授权服务器

授权服务器通过颁发访问令牌并强制实施管理策略、在OAuth2.0部署中发挥着重要作用。

选择并安装授权服务器

您需要选择并安装一个或多个授权服务器。熟悉身份提供程序的配置选项和过程非常重要，包括如何定义范围。

确定是否需要安装授权根**CA**证书

ONTAP使用授权服务器的证书来验证客户端提供的签名访问令牌。为此、ONTAP需要根CA证书和任何中间证书。这些可能已随ONTAP预安装。如果不是、则需要安装它们。

评估网络位置和配置

如果授权服务器受防火墙保护、则需要将ONTAP配置为使用代理服务器。

客户端身份验证和授权

您需要考虑客户端身份验证和授权的几个方面。

自包含范围或本地**ONTAP**标识定义

概括地说、您可以定义在授权服务器上定义的自包含范围、也可以依赖现有的本地ONTAP身份定义(包括角色和用户)。

具有本地**ONTAP**处理的选项

如果您使用ONTAP标识定义、则必须确定要应用的定义、包括：

- 已命名REST角色
- 匹配本地用户
- Active Directory或LDAP组

本地验证或远程自省

您需要确定访问令牌是由ONTAP在本地验证、还是通过自省在授权服务器验证。此外、还需要考虑几个相关值、例如刷新间隔。

受发件人限制的访问令牌

对于需要高级别安全性的环境、您可以使用基于MTLS的发送受限访问令牌。这要求每个客户端都有一个证书。

管理界面

您可以通过任意ONTAP接口来管理OAuth2.0、其中包括：

- 命令行界面
- System Manager
- REST API

客户端如何请求访问令牌

客户端应用程序必须直接从授权服务器请求访问令牌。您需要决定如何执行此操作、包括授予类型。

配置 **ONTAP**

您需要执行多个ONTAP配置任务。

定义**REST**角色和本地用户

根据您的授权配置、可以使用本地ONTAP标识处理。在这种情况下、您需要查看并定义REST角色和用户定义。

核心配置

执行核心ONTAP配置需要三个主要步骤、其中包括：

- (可选)为签署授权服务器证书的CA安装根证书(以及任何中间证书)。
- 定义授权服务器。
- 为集群启用OAuth2.0处理。

在**ONTAP**中部署**OAuth2.0**

部署核心OAuth2.0功能主要包括三个步骤。

开始之前

在配置ONTAP之前、您必须为OAuth2.0部署做准备。例如、您需要评估授权服务器、包括其证书的签名方式以及是否位于防火墙之后。请参见 "准备使用ONTAP部署OAuth2.0" 有关详细信息 …

第1步：安装身份验证服务器证书

ONTAP包含大量预安装的根CA证书。因此、在许多情况下、ONTAP将立即识别授权服务器的证书、而无需进行额外配置。但是、根据授权服务器证书的签名方式、您可能需要安装根CA证书和任何中间证书。

如果需要、请按照下面提供的说明安装证书。您应在集群级别安装所有必需的证书。

根据您访问ONTAP的方式选择正确的操作步骤。

示例 **1.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*Security*部分。
3. 单击*Certificates*旁边的*→*。
4. 在“可信证书颁发机构”选项卡下，单击“添加”。
5. 单击*Import*并选择证书文件。
6. 完成环境的配置参数。
7. 单击 * 添加 * 。

命令行界面

1. 开始安装：

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

2. 查找以下控制台消息：

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

3. 使用文本编辑器打开证书文件。
4. 复制整个证书、包括以下行：

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

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

5. 在命令提示符后、将证书粘贴到终端中。
6. 按*Enter*键完成安装。
7. 使用以下方法之一确认已安装证书：

   ```
   security certificate show-user-installed

   security certificate show
   ```

第2步：配置授权服务器

您需要为ONTAP至少定义一个授权服务器。您应根据配置和部署计划选择参数值。请查看 "OAuth2部署方案" 以确定您的配置所需的确切参数。

> 要修改授权服务器定义，您可以删除现有定义并创建新定义。

下面提供的示例基于第一个简单部署方案、部署方案位于 "本地验证"。自包含范围不需要代理即可使用。

根据您访问ONTAP的方式选择正确的操作步骤。命令行界面操作步骤使用符号变量、您需要在发出命令之前替

换这些变量。

示例 **2.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*Security*部分。
3. 单击*OAuth2.0 authorizes*旁边的*+*。
4. 选择*更多选项*。
5. 为您的部署提供所需的值、例如：
   - Name
   - 应用程序(http)
   - 提供程序JWKS URI
   - 颁发者URI
6. 单击 * 添加 * 。

命令行界面

1. 重新创建定义：

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

   例如：

   ```
   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
   ```

第3步：启用OAuth2.0

最后一步是启用OAuth2.0。这是ONTAP集群的全局设置。

> 在确认ONTAP、授权服务器和任何支持服务均已正确配置之前、请勿启用OAuth2.0处理。

根据您访问ONTAP的方式选择正确的操作步骤。

示例 **3.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*安全性部分*。
3. 单击*OAuth2.0 authorizes*旁边的*→*。
4. 启用*OAuth2.0授权*。

命令行界面

1. 启用OAuth2.0：

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

2. 确认已启用OAuth2.0：

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

使用OAuth2.0对REST API调用执行问题描述

ONTAP中的OAuth2.0实施支持REST API客户端应用程序。您可以使用cURL对简单的REST API调用进行问题描述、以便开始使用OAuth2.0。以下示例将检索ONTAP集群版本。

开始之前

您必须为ONTAP集群配置并启用OAuth2.0功能。其中包括定义授权服务器。

第1步：获取访问令牌

您需要获取用于REST API调用的访问令牌。令牌请求在ONTAP之外执行、确切的操作步骤取决于授权服务器及其配置。您可以通过Web浏览器、使用CURL命令或使用编程语言来请求令牌。

为了便于说明、下面提供了一个示例、说明如何使用CURL从Key斗 篷请求访问令牌。

Keyloak示例

```
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'
```

您应复制并保存返回的令牌。

第2步：对REST API调用执行问题描述操作

获得有效的访问令牌后、您可以使用带有访问令牌的cURL命令对问题描述A REST API调用进行访问。

参数和变量

下表介绍了cURL示例中的两个变量。

变量	Description
$FQDN_IP	ONTAP管理LIF的完全限定域名或IP地址。
$access_令牌	授权服务器发出的OAuth2.0访问令牌。

您应先在Bash Shell环境中设置这些变量、然后再执行此CURL示例。例如、在Linux命令行界面中键入以下命令以设置和显示FQDN变量：

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

在本地bash shell中定义了这两个变量后、您可以复制此URL命令并将其粘贴到命令行界面中。按*Enter*键替换变量并问题描述命令。

curl 示例

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