客户端授权
ONTAP 9

NetApp
January 17, 2025

目录

客户端授权

ONTAP客户端授权概述和选项

ONTAP OAuth2.0实施灵活可靠、可为您提供保护ONTAP环境所需的功能。有几个互斥配置选项可用。授权决策最终取决于OAuth2.0访问令牌中包含或派生的ONTAP REST角色。

您只能使用 "ONTAP REST角色" 为OAuth2.0配置授权时。不支持早期的ONTAP传统角色。

ONTAP会根据您的配置应用最合适的授权选项。有关ONTAP如何做出客户端访问决策的详细信息、请参见"ONTAP如何确定访问"。

OAuth2.0自包含范围

这些范围包含一个或多个自定义REST角色、每个角色封装在访问令牌的一个字符串中。它们与ONTAP角色定义无关。您需要在授权服务器上配置范围字符串。有关详细信息、请参见 "独立的OAuth2.0范围" 。

本地**ONTAP REST**角色

可以使用一个名为的REST角色、可以是内置角色、也可以是自定义角色。指定角色的作用域语法为*ONTAP角色<URL-encoded-ONTAP-role-name>。例如，如果ONTAP角色为范围字符串，则 `admin`为 `ontap-role-admin`。

用户

可以使用为访问应用程序"http"而定义的访问令牌中的用户名。系统将根据定义的身份验证方法按以下顺序对用户进行测试：密码、域(Active Directory)、nsswitch (LDAP)。

组

可以将授权服务器配置为使用ONTAP组进行授权。如果检查了本地ONTAP定义、但无法做出访问决定、则会使用Active Directory ("域")或LDAP ("nsswitch")组。可以通过以下两种方式之一指定组信息：

- OAuth2.0范围字符串

  支持使用客户端凭据流的机密应用程序、其中没有具有组成员资格的用户。此范围应命名为*ONTAP组-*ONTAP <URL-encoded-ONTAP-group-name>。例如、如果组为"developing"、则范围字符串将为"ONTAP组-developing"。

- 在"组"索赔中

  这适用于ADFS使用资源所有者(密码授予)流颁发的访问令牌。

有关详细信息、请参见 "使用组" 。

独立的OAuth2.0范围

自包含范围是指访问令牌中包含的字符串。每个角色都是一个完整的自定义角色定义、其中包括ONTAP做出访问决策所需的一切。此范围与ONTAP本身定义的任何REST角色是分开的、并与之不同。

范围字符串的格式

在基本级别、范围表示为连续字符串、由六个冒号分隔值组成。范围字符串中使用的参数如下所述。

ONTAP文字

范围必须以文字值开头 `ontap` 小写。此操作会将范围标识为特定于ONTAP的范围。

集群

此选项用于定义将哪个ONTAP集群范围设置为适用场景。这些值可以包括：

- 集群UUID

  标识单个集群。

- 星号(*)

  指示适用场景all集群的范围。

您可以使用ONTAP命令行界面命令 `cluster identity show` 以显示集群的UUID。如果未指定、则范围为适用场景all集群。

Role

自身作用域中包含的REST角色的名称。ONTAP不会检查此值、也不会将其与定义给ONTAP的任何现有REST角色匹配。此名称用于日志记录。

访问级别

此值指示在范围中使用API端点时应用于客户端应用程序的访问级别。下表介绍了六个可能的值。

访问级别	Description
无	拒绝对指定端点的所有访问。
-readonly	仅允许使用GET进行读取访问。
read_create	允许读取访问以及使用POST创建新资源实例。
read_modify	允许读取访问以及使用修补程序更新现有资源的功能。
read_create_modify	允许除删除以外的所有访问。允许的操作包括GET (读取)、POST (创建)和patch (更新)。
全部	允许完全访问。

SVM

集群中SVM的名称(范围为适用场景)。使用***值(星号)表示所有SVM。

ONTAP 9.14.1不完全支持此功能。您可以忽略SVM参数并使用星号作为占位符。查看 "《ONTAP 发行说明》" 以检查未来是否支持SVM。

REST API URI

指向一个资源或一组相关资源的完整或部分路径。字符串必须以开头 `/api`。如果未指定值、则会将范围限定为适用场景集群中的所有ONTAP端点。

范围示例

以下是一些独立范围的示例。

ONTAP：：joes-Role：read_cree_Modify：：/API/cluster
为分配了此角色的用户提供对的读取、创建和修改访问权限 `/cluster` 端点。

CLI管理工具

为了使独立范围的管理更轻松、更不容易出错、ONTAP提供了命令行界面命令 `security oauth2 scope` 根据输入参数生成范围字符串。

命令 `security oauth2 scope` 根据您的输入、有两个用例：

- CLI参数以限定字符串范围

  您可以使用此版本的命令根据输入参数生成范围字符串。

- 作用域字符串到CLI参数

  您可以使用此版本的命令根据输入范围字符串生成命令参数。

示例
以下示例将生成一个范围字符串、其输出包含在以下命令示例后面。定义适用场景all Clusters。

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

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

使用组

ONTAP提供了多个选项、用于根据授权服务器配置组。然后、可以将这些组映射到ONTAP用来确定访问权限的角色。

如何标识组

在授权服务器上配置组时、该组将使用名称或UUID在OAuth2.0访问令牌中进行标识和承载。在配置ONTAP之前、您需要了解授权服务器如何处理组。

如果一个访问令牌中包含多个组、则ONTAP将尝试使用每个组、直到找到匹配项为止。

组名称

许多授权服务器使用名称来标识和表示组。下面是由包含多个组的Active Directory联合身份验证服务(Active Directory Federation Service、ADFS)生成的JSON访问令牌的一个片段。有关详细信息、请参见 [管理具有名称的组] 。

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

组**UUID**

某些授权服务器使用UUID来标识和表示组。下面是由Microsoft Entra ID生成的JSON访问令牌的一个片段、其中包含多个组。有关详细信息、请参见 管理具有UID的组 。

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

管理具有名称的组

如果授权服务器使用名称来标识组、则需要确保将每个组定义为ONTAP。根据您的安全环境、您可能已经定义了组。

下面是一个命令行界面命令示例、用于将组定义为ONTAP。请注意、它使用的是样本访问令牌中的命名组。要发出此命令，您需要处于ONTAP *admin*权限级别。

示例

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

您也可以使用ONTAP REST API配置此功能。要了解更多信息，请访问 "ONTAP自动化文档"。

管理具有UID的组

如果授权服务器使用UUID值表示组、则在使用组之前、您需要执行两步配置。从Microsoft.161开始、提供了两个映射功能、并已通过ONTAP 9 ID测试。要发出命令行界面命令，您需要处于ONTAP *admin*权限级别。

您也可以使用ONTAP REST API配置这些功能。要了解更多信息，请访问 "ONTAP自动化文档"。

相关信息

- "ONTAP 命令行界面命令"

将组UUID映射到组名称

如果您使用的授权服务器使用UUID值表示组、则需要将组UUID映射到组名称。下面介绍了主要的ONTAP命令行界面操作。

创建

您可以使用命令定义新的组映射配置 `security login group create`。组UUID和名称应与授权服务器上的配置匹配。

Parameters

下面介绍了用于创建组映射的参数。

参数	Description
`vserver`	(可选)指定与组关联的SVM (SVM)的名称。如果省略此参数、则该组将与ONTAP集群关联。
`name`	ONTAP将使用的组的唯一名称。
`type`	此值表示组的来源标识提供程序。
`uuid`	指定授权服务器提供的组的通用唯一标识符。

下面是一个命令行界面命令示例、用于将组定义为ONTAP。请注意、它使用的是示例访问令牌中的UUID组。

示例

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

创建组后、将为该组生成唯一的只读整数标识符。

其他CLI操作

命令支持多项附加操作、包括：

- 显示
- 修改
- 删除

您可以使用 `show`选项检索为组生成的唯一组ID。有关详细信息、请参见ONTAP命令参考文档。

将组**UUID**映射到角色

如果您使用的授权服务器使用UUID值表示组、则可以将组映射到角色。下面介绍了主要的ONTAP命令行界面操作。此外，您需要处于ONTAP *admin*权限级别才能发出命令。

> 您需要首先将组UUID映射到组名称检索为组生成的唯一整数ID。您需要ID才能将组映射到角色。

创建

您可以使用命令定义新角色映射 `security login group role-mapping create`。

Parameters

下面介绍了用于将组映射到角色的参数。

参数	Description
`group-id`	使用命令指定为组生成的唯一ID `security login group create`。
`role`	组映射到的ONTAP角色的名称。

示例

```
security login group role-mapping create -group-id 1 -role admin
```

其他**CLI**操作

命令支持多项附加操作、包括：

- 显示
- 修改
- 删除

有关详细信息、请参见ONTAP命令参考文档。

外部角色映射

外部角色在配置为供ONTAP使用的标识提供程序中定义。您可以使用ONTAP命令行界面在这些外部角色与ONTAP角色之间创建和管理映射关系。

> 您还可以使用ONTAP REST API配置外部角色映射功能。要了解更多信息，请访问 "ONTAP自动化文档"。

相关信息

- "ONTAP 命令行界面命令"(英文)

访问令牌中的外部角色

下面是一个JSON访问令牌的片段、其中包含两个外部角色。

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

Configuration

您可以使用ONTAP命令行界面管理外部角色映射功能。

创建

您可以使用命令定义角色映射配置 `security login external-role-mapping create`。要发出此命令以及相关选项，您需要处于ONTAP *admin*权限级别。

Parameters

下面介绍了用于创建组映射的参数。

参数	Description
`external-role`	在外部身份提供程序中定义的角色的名称。
`provider`	身份提供程序的名称。这应该是系统的标识符。
`ontap-role`	指示外部角色映射到的现有ONTAP角色。

示例

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

其他CLI操作

命令支持多项附加操作、包括：

- 显示
- 修改

- 删除

有关详细信息、请参见ONTAP命令参考文档或ONTAP命令行界面手册页。

ONTAP如何确定客户端访问

要正确设计和实施OAuth2.0、您需要了解ONTAP如何使用您的授权配置来决定客户端的访问。下面根据ONTAP版本介绍了用于确定访问权限的主要步骤。

> 在ONTAP 9 15.1.中没有重要的OAuth2.0更新。如果您使用的是9.15.1版本、请参阅ONTAP 9 。14.1的说明。

相关信息

- "ONTAP中支持的OAuth2.0功能"

ONTAP 9.16.1.

OAuth.161扩展了标准ONTAP 9 2.0支持、包括本机Entra ID组的专用于Microsoft Entra ID的扩展以及外部角色映射。

确定**ONTAP 9**的客户端访问权限。**16.1.**

第**1**步：独立的范围

如果访问令牌包含任何自包含范围、则ONTAP会首先检查这些范围。如果没有独立范围、请转至步骤2。

如果存在一个或多个自包含范围，ONTAP将应用每个范围，直到可以明确地作出*ALLOW或*deny*决定为止。如果做出明确的决定、则处理将结束。

如果ONTAP无法做出明确的访问决定、请继续执行步骤2。

第**2**步：检查本地角色标志

ONTAP会检查布尔参数 `use-local-roles-if-present`。对于定义为ONTAP的每个授权服务器、此标志的值会单独设置。

- 如果值为 `true` 继续执行步骤3。
- 如果值为 `false` 处理结束、访问被拒绝。

第**3**步：命名**ONTAP REST**角色

如果访问令牌在或 `scp`字段中或作为声明包含一个命名的`REST`角色 `scope`、则ONTAP将使用该角色来做出访问决策。这始终会导致*ALLOW或*deny*决定和处理结束。

如果没有已命名的REST角色或未找到此角色、请继续执行步骤4。

第**4**步：用户

从访问令牌中提取用户名、并尝试将其与有权访问应用程序"http"的用户进行匹配。系统将根据身份验证方法按以下顺序检查用户：

- password
- 域(Active Directory)
- nsswitch (LDAP)

如果找到匹配的用户、ONTAP将使用为该用户定义的角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果用户不匹配或访问令牌中没有用户名、请继续执行步骤5。

第**5**步：组

如果包含一个或多个组、则会检查格式。如果这些组表示为UIDS、则会搜索内部组映射表。如果存在匹配的组和关联的角色、ONTAP将使用为该组定义的角色来做出访问决策。这始终会导致*ALLOW或*deny*决定和处理结束。有关详细信息，请参阅 "使用组"。

如果组表示为名称并配置了域或nsswitch授权、则ONTAP会尝试分别将其与Active Directory或LDAP组进行匹配。如果存在组匹配项、ONTAP将使用为组定义的角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果没有组匹配项或访问令牌中没有组、则会拒绝访问并结束处理。

ONTAP 9.14.1

支持的初始OAuth2.0是在ONTAP 9．14.1中基于标准OAuth2.0功能引入的。

确定**ONTAP 9**的客户端访问权限。**14.1**

第**1**步：独立的范围

如果访问令牌包含任何自包含范围、则ONTAP会首先检查这些范围。如果没有独立范围、请转至步骤2。

如果存在一个或多个自包含范围，ONTAP将应用每个范围，直到可以明确地作出*ALLOW或*deny*决定为止。如果做出明确的决定、则处理将结束。

如果ONTAP无法做出明确的访问决定、请继续执行步骤2。

第**2**步：检查本地角色标志

ONTAP会检查布尔参数 `use-local-roles-if-present`。对于定义为ONTAP的每个授权服务器、此标志的值会单独设置。

- 如果值为 `true` 继续执行步骤3。
- 如果值为 `false` 处理结束、访问被拒绝。

第**3**步：命名**ONTAP REST**角色

如果访问令牌在或 `scp`字段中包含一个命名的`REST`角色 `scope`、则ONTAP将使用该角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果没有已命名的REST角色或未找到此角色、请继续执行步骤4。

第**4**步：用户

从访问令牌中提取用户名、并尝试将其与有权访问应用程序"http"的用户进行匹配。系统将根据身份验证方法按以下顺序检查用户：

- password
- 域(Active Directory)
- nsswitch (LDAP)

如果找到匹配的用户、ONTAP将使用为该用户定义的角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果用户不匹配或访问令牌中没有用户名、请继续执行步骤5。

第**5**步：组

如果包含一个或多个组并为其配置了域或nsswitch授权、则ONTAP会尝试将其分别与Active Directory或LDAP组进行匹配。

如果存在组匹配项、ONTAP将使用为组定义的角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果没有组匹配项或访问令牌中没有组、则会拒绝访问并结束处理。