用戶端授權
ONTAP 9

NetApp
January 17, 2025

目錄

用戶端授權 1
ONTAP 用戶端授權的總覽與選項 1
獨立 OAuth 2.0 範圍 1
與小組合作 3
外部角色對應 6
ONTAP 如何決定用戶端存取 8

用戶端授權

ONTAP 用戶端授權的總覽與選項

ONTAP OAUTH 2.0 實作的設計既靈活又穩健，提供您保護 ONTAP 環境所需的功能。有多種互斥的組態選項可供選擇。授權決策最終取決於 OAuth 2.0 存取權杖中包含或衍生的 ONTAP REST 角色。

您只能使用 "ONTAP REST 角色" 設定 OAuth 2.0 授權時。不支援舊版 ONTAP 傳統角色。

ONTAP 會根據您的組態，套用最適當的單一授權選項。如需 ONTAP 如何做出用戶端存取決策的詳細資訊，請參閱"ONTAP 如何決定存取"。

OAuth 2.0 獨立範圍

這些範圍包含一或多個自訂 REST 角色，每個角色都封裝在存取權杖中的單一字串內。它們不受 ONTAP 角色定義的影響。您需要在授權伺服器上設定範圍字串。如需詳細資訊、請參閱 "獨立 OAuth 2.0 範圍" 。

本機 **ONTAP REST** 角色

可以使用單一命名 REST 角色，無論是內建或自訂。命名角色的範圍語法是 *ONTAP 角色 <URL-encoded-ONTAP-role-name> 。例如，如果 ONTAP 角色是範圍字串，則 `admin`為 `ontap-role-admin`。

使用者

您可以使用存取權杖中定義的使用者名稱，以存取應用程式「 http 」。根據定義的驗證方法，以下列順序測試使用者：密碼，網域（ Active Directory ）， nsswitch （ LDAP ）。

群組

授權伺服器可設定為使用 ONTAP 群組進行授權。如果檢查本機 ONTAP 定義、但無法做出存取決定、則會使用 Active Directory （「網域」）或 LDAP （「 nsswitch 」）群組。群組資訊可透過下列兩種方式之一來指定：

- OAuth 2.0 範圍字串

  支援使用用戶端認證流程的機密應用程式、而該流程沒有使用者擁有群組成員資格。範圍應命名為 *ONTAP 群組 <URL-encoded-ONTAP-group-name> 。例如、如果群組為「開發」、範圍字串將為「 ontap 群組開發」。

- 在「群組」請款中

  這是針對使用資源擁有者（密碼授予）流程的 ADFS 所發行的存取權杖。

如需詳細資訊、請參閱 "與小組合作" 。

獨立 OAuth 2.0 範圍

自我包含的範圍是存取權杖中攜帶的字串。每個角色都是完整的自訂角色定義、包括 ONTAP 做出存取決策所需的一切。範圍與 ONTAP 本身定義的任何其他角色是分開的。

範圍字串的格式

在基礎層級、範圍會以連續字串表示、並由六個以冒號分隔的值組成。範圍字串中使用的參數如下所述。

ONTAP 文字

範圍必須以文字值開頭 `ontap` 以小寫形式顯示。這會將範圍識別為 ONTAP 特有的範圍。

叢集

這會定義範圍所適用的 ONTAP 叢集。這些值可以包括：

- 叢集 UUID

  識別單一叢集。

- 星號（ * ）

  表示範圍適用於所有叢集。

您可以使用 ONTAP CLI 命令 `cluster identity show` 顯示叢集的 UUID 。如果未指定、範圍會套用至所有叢集。

角色

包含在獨立範圍中的 REST 角色名稱。ONTAP 不會檢查此值、也不會與任何定義給 ONTAP 的現有 REST 角色相符。名稱用於記錄。

存取層級

此值表示在範圍內使用 API 端點時、套用至用戶端應用程式的存取層級。下表說明了六個可能的值。

存取層級	說明
無	拒絕對指定端點的所有存取。
唯讀	僅允許使用 GET 進行讀取存取。
read_create	允許讀取存取、以及使用 POST 建立新的資源執行個體。
Read_modify	允許讀取存取權、以及使用修補程式更新現有資源的能力。
read_create_modify	允許刪除以外的所有存取。允許的作業包括 GET （讀取）、 POST （建立）和修補程式（更新）。
全部	允許完整存取。

SVM

適用範圍之叢集內的 SVM 名稱。使用 * 值（星號）表示所有 SVM 。

ONTAP 9.14.1 不完全支援此功能。您可以忽略 SVM 參數、並使用星號做為預留位置。檢閱 "發行說明ONTAP" 檢查將來的 SVM 支援。

REST API URI

資源或一組相關資源的完整或部分路徑。字串必須以開頭 `/api`。如果您未指定值、範圍會套用至 ONTAP 叢集上的所有 API 端點。

範圍範例

以下是一些自我包含範圍的範例。

ONTAP ： * ： jjoes-role ： read_create_modify ： * ： /API/cluster
提供指派此角色的使用者讀取、建立及修改對的存取權 `/cluster` 端點：

CLI 管理工具

為了讓自我包含範圍的管理更容易且更容易出錯、 ONTAP 提供了 CLI 命令 `security oauth2 scope` 根據輸入參數產生範圍字串。

命令 `security oauth2 scope` 根據您的意見、有兩種使用案例：

- 範圍字串的 CLI 參數

  您可以使用此版本的命令來根據輸入參數產生範圍字串。

- 範圍字串至 CLI 參數

  您可以使用此版本的命令、根據輸入範圍字串產生命令參數。

範例
下列範例會產生範圍字串、並在下列命令範例之後包含輸出。此定義適用於所有叢集。

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

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

與小組合作

ONTAP 提供數個選項，可根據您的授權伺服器來設定群組。然後，這些群組便可對應至 ONTAP 用來判斷存取權限的角色。

如何識別群組

當您在授權伺服器上設定群組時，會使用名稱或 UUID 來識別並攜帶 OAuth 2.0 存取權杖。在設定 ONTAP 之前，您必須瞭解授權伺服器如何處理群組。

如果存取權杖中包含多個群組， ONTAP 會嘗試使用每個群組，直到有相符項目為止。

群組名稱

許多授權伺服器會使用名稱來識別和代表群組。以下是 Active Directory Federation Service （ADFS）所產生的 JSON 存取權杖片段，其中包含數個群組。如需詳細資訊、請參閱 [使用名稱管理群組] 。

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

群組 **UUID**

某些授權伺服器會使用 UUID 來識別和代表群組。以下是 Microsoft Entra ID 所產生的 JSON 存取權杖片段，其中包含數個群組。如需詳細資訊、請參閱 使用 UUID 管理群組 。

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

使用名稱管理群組

如果您的授權伺服器使用名稱來識別群組，則必須確定每個群組都已定義為 ONTAP 。視您的安全環境而定，您可能已經定義了群組。

以下是將群組定義為 ONTAP 的 CLI 命令範例。請注意，它使用範例存取權杖中的命名群組。您必須處於 ONTAP * 管理 * 權限層級，才能發出命令。

範例

```
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 來設定此功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

使用 UUID 管理群組

如果您的授權伺服器代表使用 UUID 值的群組，則需要先執行兩個步驟的組態，才能使用群組。從 ONTAP 9 。16.1 開始，我們提供兩項對應功能，並已使用 Microsoft Entra ID 進行測試。您必須處於 ONTAP * 管理 * 權限層級，才能發出 CLI 命令。

您也可以使用 ONTAP REST API 來設定這些功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

相關資訊

- "ONTAP CLI 命令"

將群組 UUID 對應至群組名稱

如果您使用的授權伺服器代表使用 UUID 值的群組，則需要將群組 UUID 對應至群組名稱。主要的 ONTAP CLI 作業如下所述。

建立

您可以使用命令來定義新的群組對應組態 `security login group create`。群組 UUID 和名稱應與授權伺服器上的組態相符。

參數

用於建立群組對應的參數如下所述。

參數	說明
`vserver`	選擇性地指定群組所關聯的 SVM （ Vserver ）名稱。如果省略，群組就會與 ONTAP 叢集相關聯。
`name`	ONTAP 將使用的群組唯一名稱。
`type`	此值表示群組來源的身分識別提供者。
`uuid`	指定授權伺服器所提供之群組的通用唯一識別碼。

以下是將群組定義為 ONTAP 的 CLI 命令範例。請注意，它使用範例存取權杖中的 UUID 群組。

範例

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

建立群組之後，會為群組產生唯一的唯讀整數識別碼。

其他 CLI 作業

此命令支援多項額外作業，包括：

- 顯示
- 修改

- 刪除

您可以使用 `show`選項來擷取為群組所產生的唯一群組 ID 。如需詳細資訊，請參閱 ONTAP 命令參考文件。

將群組 **UUID** 對應至角色

如果您使用的授權伺服器代表使用 UUID 值的群組，則可以將群組對應至角色。主要的 ONTAP CLI 作業如下所述。此外，您必須處於 ONTAP * 管理 * 權限層級，才能發出命令。

> 您需要先將群組 UUID 對應至群組名稱擷取為群組產生的唯一整數 ID 。您需要 ID 才能將群組對應至角色。

建立

您可以使用命令定義新的角色對應 `security login group role-mapping create`。

參數

用於將群組對應至角色的參數如下所述。

參數	說明
`group-id`	指定使用命令為群組產生的唯一 ID `security login group create` 。
`role`	群組對應的 ONTAP 角色名稱。

範例

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

其他 **CLI** 作業

此命令支援多項額外作業，包括：

- 顯示
- 修改
- 刪除

如需詳細資訊，請參閱 ONTAP 命令參考文件。

外部角色對應

外部角色是在設定供 ONTAP 使用的識別供應商處定義。您可以使用 ONTAP CLI 建立及管理這些外部角色與 ONTAP 角色之間的對應關係。

> 您也可以使用 ONTAP REST API 來設定外部角色對應功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

相關資訊

- "ONTAP CLI 命令"。

存取權杖中的外部角色

以下是包含兩個外部角色的 JSON 存取權杖片段。

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

組態

您可以使用 ONTAP 命令列介面來管理外部角色對應功能。

建立

您可以使用命令定義角色對應組態 `security login external-role-mapping create`。您必須處於 ONTAP * 管理 * 權限層級，才能發出此命令及相關選項。

參數

用於建立群組對應的參數如下所述。

參數	說明
`external-role`	在外部身分識別提供者定義的角色名稱。
`provider`	身分識別提供者的名稱。這應該是系統的識別碼。
`ontap-role`	表示外部角色對應的現有 ONTAP 角色。

範例

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

其他 CLI 作業

此命令支援多項額外作業，包括：

- 顯示

- 修改
- 刪除

如需詳細資訊，請參閱 ONTAP 命令參考文件或 ONTAP CLI 手冊頁。

ONTAP 如何決定用戶端存取

若要正確設計及實作 OAuth 2.0 、您必須瞭解 ONTAP 如何使用您的授權組態來為用戶端做出存取決策。根據 ONTAP 版本，決定存取權限的主要步驟如下所示。

ONTAP 9 · 15.1 沒有重大的 OAuth 2.0 更新。如果您使用的是 9.15.1 版，請參閱 ONTAP 9 。14.1 的說明。

相關資訊

- "ONTAP 支援的 OAuth 2.0 功能"

ONTAP 9.16.1.

ONTAP 9 。 16.1 擴充標準 OAuth 2.0 支援，以納入適用於原生 Entra ID 群組的 Microsoft Entra ID 特定副檔名，以及外部角色對應。

判斷 **ONTAP 9** 的用戶端存取權。 **16.1**

步驟 **1** ：自我包含的範圍

如果存取權杖包含任何獨立的範圍， ONTAP 會先檢查這些範圍。如果沒有獨立的範圍、請前往步驟 2 。

如果存在一個或多個獨立的範圍、 ONTAP 會套用每個範圍、直到可以做出明確的 * 允許 * 或 * 拒絕 * 決策為止。如果做出明確的決定、處理程序就會結束。

如果 ONTAP 無法做出明確的存取決策、請繼續執行步驟 2 。

步驟 **2** ：檢查本機角色旗標

ONTAP 檢查布爾參數 `use-local-roles-if-present`。此旗標的值會針對定義為 ONTAP 的每個授權伺服器分別設定。

- 如果值為 `true` 繼續進行步驟 3 。
- 如果值為 `false` 處理結束、存取遭拒。

步驟 **3** ：具名的 **ONTAP REST** 角色

如果存取權杖在 OR `scp` 欄位中包含具名的 REST 角色 `scope`，或是宣告， ONTAP 會使用該角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有指定的 REST 角色或找不到角色、請繼續執行步驟 4 。

步驟 **4** ：使用者

從存取權杖擷取使用者名稱，並嘗試將其與有權存取應用程式「 http 」的使用者配對。根據驗證方法，依下列順序檢查使用者：

- 密碼
- 網域（ Active Directory ）
- NSWITCH （ LDAP ）

如果找到相符的使用者， ONTAP 會使用為使用者定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果使用者不相符，或存取權杖中沒有使用者名稱，請繼續執行步驟 5 。

步驟 **5** ：群組

如果包含一個或多個群組，則會檢查格式。如果群組代表為 UUID ，則會搜尋內部群組對應表。如果有群組相符項目和相關角色， ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。如需更多資訊、請參閱 "與小組合作"。

如果群組是以名稱表示，並已設定網域或 nsswitch 授權，則 ONTAP 會分別嘗試將其與 Active Directory 或 LDAP 群組進行比對。如果有群組相符項目、 ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有符合的群組、或存取權杖中沒有群組、則會拒絕存取並結束處理。

ONTAP 9.14.1.

支援的初始 OAUTH 2.0 是根據標準 OAUTH 2.0 功能而在 ONTAP 9 中推出的。

決定 **ONTAP 9** 的用戶端存取權。 **14.1**

步驟 **1** ：自我包含的範圍

如果存取權杖包含任何獨立的範圍， ONTAP 會先檢查這些範圍。如果沒有獨立的範圍、請前往步驟 2 。

如果存在一個或多個獨立的範圍、 ONTAP 會套用每個範圍、直到可以做出明確的 * 允許 * 或 * 拒絕 * 決策為止。如果做出明確的決定、處理程序就會結束。

如果 ONTAP 無法做出明確的存取決策、請繼續執行步驟 2 。

步驟 **2** ：檢查本機角色旗標

ONTAP 檢查布爾參數 `use-local-roles-if-present`。此旗標的值會針對定義為 ONTAP 的每個授權伺服器分別設定。

- 如果值為 `true` 繼續進行步驟 3 。
- 如果值為 `false` 處理結束、存取遭拒。

步驟 **3** ：具名的 **ONTAP REST** 角色

如果存取權杖在 OR `scp` 欄位中包含具名的 REST 角色 `scope`， ONTAP 會使用該角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有指定的 REST 角色或找不到角色、請繼續執行步驟 4 。

步驟 **4** ：使用者

從存取權杖擷取使用者名稱，並嘗試將其與有權存取應用程式「 http 」的使用者配對。根據驗證方法，依下列順序檢查使用者：

- 密碼
- 網域（ Active Directory ）
- NSWITCH （ LDAP ）

如果找到相符的使用者， ONTAP 會使用為使用者定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果使用者不相符，或存取權杖中沒有使用者名稱，請繼續執行步驟 5 。

步驟 **5** ：群組

如果包含一個或多個群組，並設定了網域或 nsswitch 授權， ONTAP 會分別嘗試將它們與 Active Directory 或 LDAP 群組配對。

如果有群組相符項目、 ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有符合的群組、或存取權杖中沒有群組、則會拒絕存取並結束處理。

版權資訊

商標資訊