



用戶端授權 ONTAP 9

NetApp
February 12, 2026

目錄

用戶端授權	1
ONTAP 用戶端授權的總覽與選項	1
ONTAP中的獨立 OAuth 2.0 範圍	1
範圍字串的格式	2
範圍範例	3
CLI 管理工具	3
ONTAP中的 OAuth 2.0 外部角色映射	3
存取權杖中的外部角色	4
組態	4
ONTAP 如何決定用戶端存取	5
ONTAP 9.16.1.....	5
ONTAP 9.14.1.....	7

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。

看["在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組"](#)了解更多。

ONTAP中的獨立 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` 來顯示叢集的 UUID。如果未指定、範圍會套用至所有叢集。如["指令參考資料ONTAP"](#)需詳細 `cluster identity show` 資訊，請參閱。

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
```

如"[指令參考資料ONTAP](#)"需詳細 `security oauth2 scope` 資訊，請參閱。

ONTAP中的 OAuth 2.0 外部角色映射

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](#)"。

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
<code>external-role</code>	在外部身分識別提供者定義的角色名稱。
<code>provider</code>	身分識別提供者的名稱。這應該是系統的識別碼。
<code>ontap-role</code>	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
```

如["指令參考資料ONTAP"](#)需詳細 `security login external-role-mapping create` 資訊，請參閱。

其他 CLI 作業

此命令支援多項額外作業，包括：

- 顯示

- 修改
- 刪除

相關資訊

- ["指令參考資料ONTAP"](#)

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。

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，則檢查其格式。如果群組以 UUID 表示，則搜尋內部群組對應表。如果存在符合的群組和關聯的角色，ONTAP 將使用為該群組定義的角色做出存取決策。這始終會導致“允許”或“拒絕”決策，處理結束。有關更多信息，請參閱[在 ONTAP 中使用 OAuth 2.0 或 SAML IdP 群組](#)。

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

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。