概念
ONTAP 9

NetApp
February 12, 2026

目錄

概念

ONTAP中的 OAuth 2.0 授權伺服器和存取令牌

授權伺服器會在 OAuth 2.0 授權架構中執行多項重要功能、做為中央元件。

OAuth 2.0 授權伺服器

授權伺服器主要負責建立和簽署存取權杖。這些權杖包含身分識別與授權資訊、可讓用戶端應用程式選擇性地存取受保護的資源。這些伺服器通常彼此隔離、可透過多種不同方式實作、包括獨立的專用伺服器、或是作為較大型的身分識別與存取管理產品的一部分。

授權伺服器有時會使用不同的術語、尤其是 OAuth 2.0 功能會封裝在較大的身分識別與存取管理產品或解決方案中。例如，術語 * 身分識別提供者（ IDP ） * 經常與 * 授權伺服器 * 互換使用。

系統管理

除了發行存取權杖之外、授權伺服器也會提供相關的管理服務、通常是透過 Web 使用者介面。例如、您可以定義和管理：

- 使用者和使用者驗證
- 範圍
- 透過租戶和領域進行管理隔離
- 原則強制執行
- 連線至各種外部服務
- 支援其他身分識別傳輸協定（例如 SAML ）

ONTAP 與符合 OAuth 2.0 標準的授權伺服器相容。

定義至 **ONTAP**

您需要定義一或多個 ONTAP 授權伺服器。ONTAP 會安全地與每部伺服器通訊、以驗證權杖、並執行其他相關工作來支援用戶端應用程式。

ONTAP 組態的主要層面如下所示。另請參閱 "OAuth 2.0 部署案例" 以取得更多資訊。

存取權杖的驗證方式與位置

驗證存取權杖有兩個選項。

- 本機驗證

  ONTAP 可以根據發行權杖的授權伺服器所提供的資訊、在本機驗證存取權杖。從授權伺服器擷取的資訊會由 ONTAP 快取、並定期重新整理。

- 遠端自我反思

  您也可以使用遠端自我反思來驗證授權伺服器上的權杖。introspection 是一種允許授權方查詢授權伺服器有

關存取權杖的通訊協定。它提供 ONTAP 從存取權杖擷取特定中繼資料並驗證權杖的方法。由於效能原因、ONTAP 會快取部分資料。

網路位置

ONTAP 可能位於防火牆後方。在這種情況下、您需要將 Proxy 識別為組態的一部分。

授權伺服器的定義方式

您可以使用任何管理介面（包括 CLI 、系統管理員或 REST API ）來定義 ONTAP 的授權伺服器。例如、您可以使用 CLI 使用命令 `security oauth2 client create`。

如"指令參考資料ONTAP"需詳細 `security oauth2 client create`資訊，請參閱。

授權伺服器數量

您最多可以定義八個授權伺服器到單一 ONTAP 叢集。只要發卡行或發卡行 / 受眾聲明是唯一的、同一授權伺服器就可以多次定義到同一個 ONTAP 叢集。例如、使用 Keycloak 時、使用不同領域時、這種情況永遠都會發生。

ONTAP 支援的 OAuth 2.0 功能

OAUTH 2.0 的支援最初隨 ONTAP 9 提供。 14.1 之後的版本將持續增強。ONTAP 支援的 OAuth 2.0 功能如下所述。

隨特定 ONTAP 版本推出的功能將會持續到未來的版本。

ONTAP 9.16.1.

ONTAP 9 。 16.1 擴充標準 OAuth 2.0 功能，以納入原生 Entra ID 群組的 Entra ID 專屬副檔名。這涉及在存取權杖中使用 GUID ，而非名稱。此外，此版本還新增外部角色對應支援，可利用存取權杖中的「角色」欄位，將原生身分識別提供者角色對應至 ONTAP 角色。

ONTAP 9.14.1.

從 ONTAP 9 。 14.1 開始，授權伺服器可透過下列標準 OAuth 2.0 功能來支援使用的應用程式：

- OAuth 2.0 標準欄位包括「 iss 」，「 aud 」和「 exp 」，如和 "RFC 7519 ： JSON Web Token （ JWT ）"中所述 "RFC6749 ： OAuth 2.0 授權架構"。這也支援透過存取權杖中的欄位來唯一識別使用者，例如「 UPN 」，「 AppID 」，「 Sub" ，「使用者名稱」或「 Preferred _UserName 」。
- 針對具有「群組」欄位的群組名稱，針對特定於供應商的 ADFS 副檔名。
- Azure 廠商專屬的群組 UUID 延伸功能，並具有「群組」欄位。
- 使用 OAuth 2.0 存取權杖範圍內的獨立角色和具名角色來提供授權支援的 ONTAP 延伸功能。其中包括「範圍」和「 scp 」欄位，以及範圍內的群組名稱。

使用 OAuth 2.0 存取權杖

由授權伺服器發出的 OAuth 2.0 存取權杖是由 ONTAP 驗證、用於為 REST API 用戶端要求做出角色型存取決策。

取得存取權杖

您需要從定義至 ONTAP 叢集的授權伺服器取得存取權杖、以便在其中使用 REST API 。若要取得權杖、您必須直接聯絡授權伺服器。

ONTAP 不會核發存取權杖、也不會將用戶端的要求重新導向至授權伺服器。

您要求權杖的方式取決於多項因素、包括：

- 授權伺服器及其組態選項
- OAuth 2.0 授與類型
- 用於發出要求的用戶端或軟體工具

授與類型

_Grant 是定義完善的程序、包括一組網路流量、用於要求及接收 OAuth 2.0 存取權杖。視用戶端、環境和安全性需求而定、可使用多種不同的授與類型。下表列出熱門的補助類型清單。

授與類型	說明
用戶端認證	一種僅使用認證（例如 ID 和共用密碼）的常用授與類型。假設用戶端與資源擁有者有密切的信任關係。
密碼	資源擁有者密碼認證授與類型可用於資源擁有者與用戶端建立信任關係的情況。將舊版 HTTP 用戶端移轉至 OAuth 2.0 時、這項功能也很實用。
授權代碼	這是機密用戶端的理想授與類型、是以重新導向為基礎的流程為基礎。它可用於取得存取權杖和重新整理權杖。

JWT 內容

OAuth 2.0 存取權杖格式化為 JWT 。內容是由授權伺服器根據您的組態建立。不過、這些 Token 對用戶端應用程式來說是不透明的。用戶端沒有理由檢查權杖或是知道其內容。

每個 JWT 存取權杖都包含一組宣告。聲明說明發卡行的特性、以及根據授權伺服器的管理定義進行的授權。下表說明部分已登錄於標準的索賠。所有字串都區分大小寫。

請款	關鍵字	說明
發卡行	ISS	識別發出權杖的主體。請款處理是針對特定應用程式。
主旨	子	權杖的主旨或使用者。名稱的範圍是全域或本機唯一的。
目標對象	AUD	權杖的目標收件者。以字串陣列形式實作。
過期	到期	權杖過期且必須拒絕的時間。

請參閱 "RFC 7519 ： JSON Web Token" 以取得更多資訊。

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
`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
```

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。

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。

使用ONTAP 的OAuth 2.0 部署場景

將授權伺服器定義為 ONTAP 時、有幾個組態選項可供使用。根據這些選項，您可以使用多種部署案例之一，定義適合您環境的授權伺服器。

組態參數摘要

將授權伺服器定義為 ONTAP 時、有幾個組態參數可供使用。這些參數通常在所有管理介面中都受到支援。

個別參數或欄位使用的名稱可能會因 ONTAP 管理介面而異。為了因應管理介面的差異，表格中的每個參數都會使用單一通用名稱。根據上下文，與特定介面搭配使用的確切名稱應該是顯而易見的。

參數	說明
名稱	ONTAP 已知的授權伺服器名稱。
應用程式	定義所適用的 ONTAP 內部應用程式。這必須是 * http * 。
發卡行 URI	具有路徑的 FQDN 、可識別發出權杖的站台或組織。
提供者 JWKS URI	ONTAP 取得用於驗證存取權杖之 JSON 網頁金鑰集的路徑和檔案名稱 FQDN 。
JWKS 重新整理時間間隔	決定 ONTAP 從提供者 JWKS URI 重新整理憑證資訊的頻率的時間間隔。此值以 ISO-8601 格式指定。
introspection 端點	ONTAP 透過自我介紹來執行遠端權杖驗證所使用的路徑 FQDN 。
用戶端ID	授權伺服器上定義的用戶端名稱。包含此值時、您也需要根據介面提供相關的用戶端機密。
傳出 Proxy	這是為了在 ONTAP 位於防火牆後方時提供對授權伺服器的存取。URI 必須為 cURL 格式。
如果存在、請使用本機角色	判斷是否使用本機 ONTAP 定義的布林旗標、包括具名 REST 角色和本機使用者。
遠端使用者請款	ONTAP 用來比對本機使用者的替代名稱。使用 `sub` 存取權杖中的欄位、以符合本機使用者名稱。
目標對象	此欄位定義可使用存取權杖的端點。

部署案例

以下提供幾種常見的部署案例。它們是根據權杖驗證是由 ONTAP 在本機執行、還是由授權伺服器遠端執行來組織。每個案例都包含所需組態選項的清單。請參閱 "在 ONTAP 中部署 OAuth 2.0" 以取得組態命令的範例。

定義授權伺服器之後、您可以透過 ONTAP 管理介面顯示其組態。例如、使用命令 `security oauth2 client show` 使用 ONTAP CLI 。

本機驗證

下列部署案例是以 ONTAP 在本機執行權杖驗證為基礎。

使用不含 **Proxy** 的自我控制範圍

這是僅使用 OAuth 2.0 獨立範圍的最簡單部署。不會使用任何本機 ONTAP 身分識別定義。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 發卡行 URI

您也需要在授權伺服器上新增範圍。

在 **Proxy** 中使用自我包含的範圍

此部署案例使用 OAuth 2.0 獨立範圍。不會使用任何本機 ONTAP 身分識別定義。但是授權伺服器位於防火牆後方、因此您需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 傳出 Proxy
- 發卡行 URI
- 目標對象

您也需要在授權伺服器上新增範圍。

使用本機使用者角色和預設使用者名稱對應搭配 **Proxy**

此部署案例使用具有預設名稱對應的本機使用者角色。遠端使用者宣告使用的預設值 `sub` 因此、存取權杖中的這個欄位是用來比對本機使用者名稱。使用者名稱必須少於 40 個字元。授權伺服器位於防火牆後方、因此您也需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 如果存在、請使用本機角色 (`true`)
- 傳出 Proxy
- 發卡行

您必須確定本機使用者已定義為 ONTAP 。

使用本機使用者角色和替代使用者名稱對應搭配 **Proxy**

此部署案例使用具有替代使用者名稱的本機使用者角色、用於與本機 ONTAP 使用者配對。授權伺服器位於防火牆後方、因此您需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI

- 如果存在、請使用本機角色 (`true`)
- 遠端使用者請款
- 傳出 Proxy
- 發卡行 URI
- 目標對象

您必須確定本機使用者已定義為 ONTAP 。

遠端自我反思

下列部署組態是以 ONTAP 透過自我反思遠端執行權杖驗證為基礎。

使用不含 **Proxy** 的自我控制範圍

這是以 OAuth 2.0 獨立範圍為基礎的簡單部署。不會使用任何 ONTAP 身分識別定義。您必須包含下列參數：

- 名稱
- 應用程式（ http ）
- introspection 端點
- 用戶端ID
- 發卡行 URI

您需要在授權伺服器上定義範圍以及用戶端和用戶端機密。

相關資訊

- "安全 oauth2 用戶端展示"

使用 OAuth 2.0 Mutual TLS 進行ONTAP客戶端身份驗證

視您的安全需求而定、您可以選擇性地設定相互 TLS （ MTLS ）來實作強式用戶端驗證。搭配 ONTAP 搭配 OAuth 2.0 部署使用時、 MTLS 保證存取權杖只能由最初核發的用戶端使用。

與 OAuth 2.0 共同使用 TLS

傳輸層安全性（ TLS ）用於在兩個應用程式（通常是用戶端瀏覽器和 Web 伺服器）之間建立安全的通訊通道。相互 TLS 可透過用戶端憑證提供用戶端的強大識別功能、藉此延伸此功能。在具有 OAuth 2.0 的 ONTAP 叢集中使用時、可透過建立和使用寄件者限制的存取權杖來擴充基礎 MTLS 功能。

傳送者限制的存取權杖只能由最初核發的用戶端使用。若要支援此功能、請提出新的確認聲明 (`cnf`）插入令牌中。欄位包含內容 `x5t#S256` 其中包含要求存取權杖時所使用的用戶端憑證摘要。此值由 ONTAP 驗證、作為驗證權杖的一部分。未受寄件者限制的授權伺服器所核發的存取權杖、不包含額外的確認宣告。

您需要將 ONTAP 設定為針對每個授權伺服器分別使用 MTLS 。例如、 CLI 命令 `security oauth2 client` 包含參數 `use-mutual-tls` 根據下表所示的三個值來控制 MTLS 處理。

在每個組態中、 ONTAP 所採取的結果和行動、都要視組態參數值、以及存取權杖和用戶端憑證的內容而定。表格中的參數是從最少組織到最嚴格的組織。

參數	說明
無	授權伺服器的 OAuth 2.0 相互 TLS 驗證已完全停用。ONTAP 不會執行 MTLS 用戶端憑證驗證、即使憑證中有確認宣告、或是用戶端憑證隨附 TLS 連線。
要求	如果用戶端提供寄件者限制的存取權杖、則會強制執行 OAuth 2.0 相互 TLS 驗證。也就是說、只有在確認宣告（含屬性）時、才會強制執行 MTLS `x5t#S256`）存在於存取權杖中。這是預設設定。
必要	對於由授權伺服器發出的所有存取權杖、都會強制執行 OAuth 2.0 相互 TLS 驗證。因此、所有存取權杖都必須受寄件者限制。如果存取權杖中沒有確認宣告、或是用戶端憑證無效、驗證和 REST API 要求就會失敗。

高階實作流程

在 ONTAP 環境中搭配 OAuth 2.0 使用 MTLS 時所涉及的一般步驟如下所示。請參閱 "RFC 8705 ： OAuth 2.0 雙向 TLS 用戶端驗證和憑證繫結存取權杖" 以取得更多詳細資料。

步驟 **1** ：建立及安裝用戶端憑證

建立用戶端身分識別的基礎、是證明客戶端私密金鑰的知識。對應的公開金鑰會放置在用戶端提供的簽署 X.509 憑證中。在較高層級、建立用戶端憑證所涉及的步驟包括：

1. 產生公開金鑰與私密金鑰配對
2. 建立憑證簽署要求
3. 將 CSR 檔案傳送至知名的 CA
4. CA 會驗證要求並核發簽署的憑證

您通常可以在本機作業系統中安裝用戶端憑證、或直接搭配一般公用程式（例如 Curl ）使用。

步驟 **2** ：將 **ONTAP** 設定為使用 **MTLS**

您需要設定 ONTAP 以使用 MTLS 。每個授權伺服器都會分別完成此組態設定。例如、使用 CLI 命令 `security oauth2 client` 與選用參數搭配使用 `use-mutual-tls`。請參閱 "在 ONTAP 中部署 OAuth 2.0" 以取得更多資訊。

步驟 **3** ：用戶端要求存取權杖

用戶端需要從設定為 ONTAP 的授權伺服器要求存取權杖。用戶端應用程式必須在步驟 1 中建立並安裝憑證時使用 MTLS 。

步驟 **4** ：授權伺服器會產生存取權杖

授權伺服器會驗證用戶端要求並產生存取權杖。在此過程中、它會建立用戶端憑證的訊息摘要、並將其作為確認宣告（欄位 `cnf`）。

步驟 **5** ：用戶端應用程式會將存取權杖呈現給 **ONTAP**

用戶端應用程式會對 ONTAP 叢集進行 REST API 呼叫、並在授權要求標頭中以 * 承載權杖 * 的形式包含存取權杖。用戶端必須使用 MTLS 搭配用於要求存取權杖的相同憑證。

步驟 **6** ： **ONTAP** 會驗證用戶端和權杖。

ONTAP 會在 HTTP 要求中接收存取權杖、以及作為 MTLS 處理一部分的用戶端憑證。ONTAP 會先驗證存取權杖中的簽章。根據組態、 ONTAP 會產生用戶端憑證的訊息摘要、並將其與權杖中的確認宣告 **cnf** 進行比較。如果這兩個值相符、 ONTAP 已確認發出 API 要求的用戶端與最初發出存取權杖的用戶端相同。

相關資訊

- "安全oauth2客戶端"