使用 OAuth 2.0 進行驗證與授權

ONTAP 9

NetApp
April 24, 2024

目錄

使用 OAuth 2.0 進行驗證與授權

ONTAP OAuth 2.0 實作總覽

從 ONTAP 9.14 開始、您可以選擇使用開放授權（ OAuth 2.0 ）架構來控制對 ONTAP 叢集的存取。您可以使用任何 ONTAP 管理介面（包括 ONTAP CLI 、系統管理員和 REST API ）來設定此功能。不過、 OAuth 2.0 授權和存取控制決策只能在用戶端使用 REST API 存取 ONTAP 時套用。

> OAuth 2.0 支援是 ONTAP 9.14.0 首次推出、因此可用度取決於您使用的 ONTAP 版本。請參閱 "發行說明ONTAP" 以取得更多資訊。

功能與優勢

以下說明搭配 ONTAP 使用 OAuth 2.0 的主要功能與優點。

支援 **OAuth 2.0** 標準

OAuth 2.0 是業界標準授權架構。它可用來限制及控制使用簽署存取權杖來存取受保護資源的權限。使用 OAuth 2.0 有幾個好處：

- 授權組態有許多選項
- 切勿洩漏用戶端認證、包括密碼
- 您可以根據組態將權杖設定為過期
- 非常適合與 REST API 搭配使用

使用數個熱門授權伺服器進行測試

ONTAP 實作的設計可與任何符合 OAuth 2.0 標準的授權伺服器相容。它已通過下列熱門伺服器或服務的測試、包括：

- 驗證0
- Active Directory Federation Service （ADFS）
- Keycloak

支援多個並行授權伺服器

您最多可以為單一 ONTAP 叢集定義八個授權伺服器。如此一來、您就能靈活地滿足各種安全環境的需求。

與 **REST** 角色整合

ONTAP 授權決策最終取決於指派給使用者或群組的其餘角色。這些角色可在存取權杖中作為獨立範圍、或是根據本機 ONTAP 定義以及 Active Directory 或 LDAP 群組來執行。

使用寄件者限制存取權杖的選項

您可以將 ONTAP 和授權伺服器設定為使用相互傳輸層安全性（ MTLS ）、以強化用戶端驗證。它保證 OAuth 2.0 存取權杖只能由最初核發的用戶端使用。此功能支援並符合數項常用的安全性建議、包括由 FAPI 和斜接建立的建議。

實作與組態

在較高層級、 OAuth 2.0 實作和組態有幾個層面、您應該在開始使用時考慮。

ONTAP 內的 OAuth 2.0 實體

OAuth 2.0 授權架構定義了數個實體、可對應至資料中心或網路中的實際或虛擬元素。下表列出 OAuth 2.0 實體及其對 ONTAP 的調適。

OAuth 2.0 實體	說明
資源	REST API 端點、可透過內部 ONTAP 命令存取 ONTAP 資源。
資源擁有者	建立受保護資源或依預設擁有資源的 ONTAP 叢集使用者。
資源伺服器	受保護資源的主機、即 ONTAP 叢集。
用戶端	代表或取得資源擁有者權限、要求存取 REST API 端點的應用程式。
授權伺服器	通常是負責發行存取權杖和強制執行管理原則的專用伺服器。

核心 ONTAP 組態

您需要設定 ONTAP 叢集以啟用和使用 OAuth 2.0 。這包括建立與授權伺服器的連線、以及定義所需的 ONTAP 授權組態。您可以使用任何管理介面來執行此組態、包括：

- 指令行介面ONTAP
- 系統管理員
- 靜態API ONTAP

環境與支援服務

除了 ONTAP 定義之外、您也需要設定授權伺服器。如果您使用群組對角色對應、也需要設定 Active Directory 群組或 LDAP 等量。

支援的 ONTAP 用戶端

從 ONTAP 9.14 開始、 REST API 用戶端可以使用 OAuth 2.0 存取 ONTAP 。在發出 REST API 呼叫之前、您需要從授權伺服器取得存取權杖。然後、用戶端使用 HTTP 授權要求標頭、將此權杖以 _bon承載 權杖的形式傳送至 ONTAP 叢集。視所需的安全性層級而定、您也可以在用戶端建立及安裝憑證、以使用以 MTLS 為基礎的寄件者限制權杖。

選定的術語

當您開始使用 ONTAP 探索 OAuth 2.0 部署時、熟悉其中一些詞彙是很有幫助的。請參閱 "其他資源" 取得有關 OAuth 2.0 的詳細資訊連結。

存取權杖

由授權伺服器發出的權杖、由 OAuth 2.0 用戶端應用程式用來發出存取受保護資源的要求。

JSON Web Token

用於格式化存取權杖的標準。JSON 用於以精簡格式呈現 OAuth 2.0 宣告、並將宣告分為三個主要區段。

寄件者限制的存取權杖

以相互傳輸層安全性（ MTLS ）傳輸協定為基礎的選用功能。藉由在權杖中使用額外的確認宣告、這可確保

存取權杖僅供最初核發的用戶端使用。

JSON Web 金鑰集

JWKS 是 ONTAP 用來驗證用戶端所呈現 JWT Token 的公開金鑰集合。金鑰集通常可透過專用 URI 在授權伺服器上使用。

範圍

範圍提供一種方法來限制或控制應用程式對受保護資源（例如 ONTAP REST API ）的存取。它們在存取權杖中以字串表示。

ONTAP REST 角色

REST 角色是 ONTAP 9.6 引進的、是 ONTAP RBAC 架構的核心部分。這些角色與 ONTAP 仍支援的舊版傳統角色不同。ONTAP 中的 OAuth 2.0 實作僅支援 REST 角色。

HTTP 授權標頭

HTTP 要求中包含的標頭、用於在進行 REST API 呼叫時識別用戶端及相關權限。視驗證和授權的執行方式而定、有多種類型或實作可供選擇。將 OAuth 2.0 存取權杖呈現給 ONTAP 時、該權杖會識別為 _stoning 權杖 _ 。

HTTP 基本驗證

ONTAP 仍支援早期的 HTTP 驗證技術。純文字認證（使用者名稱和密碼）會與冒號串連、並以 base64 編碼。字串會放在授權要求標頭中、並傳送至伺服器。

FAPI

OpenID Foundation 的工作群組、為金融產業提供通訊協定、資料架構及安全建議。API 原本稱為財務等級 API 。

斜接

一家私人非營利公司、為美國空軍和美國政府提供技術與安全指引。

其他資源

以下提供幾項額外資源。您應該檢閱這些網站、以取得有關 OAuth 2.0 及相關標準的更多資訊。

通訊協定與標準

- "RFC 6749 ： OAuth 2.0 授權架構"
- "RFC 7519 ： JSON Web Token （ JWT ）"
- "RFC 7523 ：適用於 OAuth 2.0 用戶端驗證和授權授與的 JSON Web Token （ JWT ）設定檔"
- "RFC 7662 ： OAUTH 2.0 Token 反思"
- "RFC 7800 ： JWTs 的持有證明金鑰"
- "RFC 8705 ： OAuth 2.0 雙向 TLS 用戶端驗證和憑證繫結存取權杖"

組織

- "OpenID Foundation"
- "FAPI 工作組"
- "斜接"

- "IANA - JWT"

產品與服務

- "驗證0"
- "ADFS 總覽"
- "Keycloak"

其他工具與公用程式

- "JWT by Auth0"
- "Openssl"

NetApp 文件與資源

- "ONTAP 自動化" 文件

概念

授權伺服器和存取權杖

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`。

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。

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。

ONTAP 用戶端授權選項

有幾個選項可供您自訂 ONTAP 用戶端授權。授權決策最終取決於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。

簡介

ONTAP 中的 OAuth 2.0 實作設計為靈活且穩健、提供您保護 ONTAP 環境所需的選項。在高層級、定義 ONTAP 用戶端授權的主要組態類別有三種。這些組態選項是互斥的。

ONTAP 會根據您的組態套用最適當的單一選項。請參閱 "ONTAP 如何決定存取" 深入瞭解 ONTAP 如何處理您的組態定義、以做出存取決策。

OAuth 2.0 獨立範圍

這些範圍包含一或多個自訂 REST 角色、每個角色都封裝在單一字串中。它們不受 ONTAP 角色定義的影響。您需要在授權伺服器上定義這些範圍字串。

本機 **ONTAP** 特有的 **REST** 角色和使用者

根據您的組態、本機 ONTAP 身分識別定義可用於做出存取決策。選項包括：

- 單一命名 REST 角色
- 將使用者名稱與本機 ONTAP 使用者配對

命名角色的範圍語法是 *ONTAP 角色 <URL-encoded-ONTAP-role-name> 。例如、如果角色為「 admin 」、範圍字串將為「 ontap 角色管理員」。

Active Directory 或 **LDAP** 群組

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。

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`

ONTAP 如何決定存取

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。

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 會檢查旗標的價值 `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

如果存取權杖包含具名的 REST 角色、 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** ：本機 **ONTAP** 使用者

從存取權杖擷取使用者名稱、並嘗試將其與本機 ONTAP 使用者配對。

如果符合本機 ONTAP 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。

如果本機 ONTAP 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** ：群組對角色對應

從存取權杖擷取群組、並嘗試將其與群組配對。這些群組是使用 Active Directory 或等效的 LDAP 伺服器來定義。

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。

OAuth 2.0 部署案例

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、您可以建立適合部署環境的授權伺服器。

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。

參數名稱可能會因 ONTAP 管理介面而稍有不同。例如、在設定遠端自我介紹時、會使用 CLI 命令參數來識別端點 `-introspection-endpoint`。但在 System Manager 中、對等欄位是 *Authorization server Token introspection URI* 。為了容納所有 ONTAP 管理介面、我們提供參數的一般說明。確切的參數或欄位應根據上下文而顯而易見。

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。
移除使用者請款	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。

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 。

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。

使用相互 **TLS** 的用戶端驗證

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。

設定與部署

準備使用 **ONTAP** 部署 **OAuth 2.0**

在 ONTAP 環境中設定 OAuth 2.0 之前、您應該先準備部署。主要任務和決定摘要如下。各節的排列方式通常與您應遵循的順序一致。不過、雖然它適用於大多數的部署、但您應該視需要調整以符合您的環境。您也應該考慮建立正式的部署計畫。

> 根據您的環境、您可以為定義為 ONTAP 的授權伺服器選取組態。這包括您需要針對每種部署類型指定的參數值。請參閱 "OAuth 2.0 部署案例" 以取得更多資訊。

受保護的資源和用戶端應用程式

OAuth 2.0 是一個授權架構、用於控制受保護資源的存取。有鑑於此、任何部署的重要第一步、就是判斷可用資源為何、以及哪些用戶端需要存取這些資源。

識別用戶端應用程式

您需要決定在發出 REST API 呼叫時、哪些用戶端會使用 OAuth 2.0 、以及哪些 API 端點需要存取。

檢閱現有的 **ONTAP REST** 角色和本機使用者

您應該檢閱現有的 ONTAP 身分識別定義、包括其餘角色和本機使用者。視您設定 OAuth 2.0 的方式而定、這些定義可用於做出存取決策。

全域移轉至 **OAuth 2.0**

雖然您可以逐步實作 OAuth 2.0 授權、但也可以為每個授權伺服器設定全域旗標、立即將所有其餘 API 用戶端移至 OAuth 2.0 。如此一來、就能根據現有的 ONTAP 組態來做出存取決策、而無需建立獨立的範圍。

授權伺服器

授權伺服器在 OAuth 2.0 部署中扮演重要角色、方法是核發存取權杖並強制執行管理原則。

選取並安裝授權伺服器

您需要選取並安裝一或多個授權伺服器。請務必熟悉身分識別供應商的組態選項和程序、包括如何定義範圍。

判斷是否需要安裝授權根 **CA** 憑證

ONTAP 使用授權伺服器的憑證來驗證用戶端所提供的已簽署存取權杖。為達此目的、 ONTAP 需要根 CA 憑證和任何中繼憑證。這些可能已預先安裝在 ONTAP 中。如果沒有、您需要安裝它們。

評估網路位置和組態

如果授權伺服器位於防火牆之後、則需要將 ONTAP 設定為使用 Proxy 伺服器。

用戶端驗證與授權

您需要考量用戶端驗證和授權的幾個層面。

獨立範圍或本機 **ONTAP** 身分識別定義

在高層級、您可以定義在授權伺服器上定義的自我包含範圍、或是仰賴現有的本機 ONTAP 身分識別定義、包括角色和使用者。

具有本機 **ONTAP** 處理功能的選項

如果您使用 ONTAP 身分識別定義、則必須決定要套用的項目、包括：

- 具名 REST 角色
- 符合本機使用者
- Active Directory 或 LDAP 群組

本機驗證或遠端自我反省

您需要決定存取權杖是由 ONTAP 在本機驗證、還是透過自我反省在授權伺服器驗證。也有幾個相關的值需要考量、例如重新整理時間間隔。

寄件者限制的存取權杖

對於需要高安全性的環境、您可以使用以 MTLS 為基礎的傳送限制存取權杖。這需要每個用戶端的憑證。

管理介面

您可以透過任何 ONTAP 介面執行 OAuth 2.0 管理、包括：

- 命令列介面
- 系統管理員
- REST API

用戶端如何要求存取權杖

用戶端應用程式必須直接從授權伺服器要求存取權杖。您需要決定如何執行、包括授與類型。

設定**ONTAP** 功能

您需要執行幾項 ONTAP 組態工作。

定義 **REST** 角色和本機使用者

根據您的授權組態、可使用本機 ONTAP 識別處理。在這種情況下、您需要檢閱並定義其餘角色和使用者定義。

核心組態

執行核心 ONTAP 組態需要三個主要步驟、包括：

- 您也可以為簽署授權伺服器憑證的 CA 安裝根憑證（及任何中繼憑證）。
- 定義授權伺服器。
- 啟用叢集的 OAuth 2.0 處理。

在 **ONTAP** 中部署 **OAuth 2.0**

部署核心 OAuth 2.0 功能需要三個主要步驟。

開始之前

您必須準備 OAuth 2.0 部署、才能設定 ONTAP 。例如、您需要評估授權伺服器、包括其憑證的簽署方式、以及它是否位於防火牆的後方。請參閱 "準備使用 ONTAP 部署 OAuth 2.0" 以取得更多資訊。

步驟 **1** ：安裝驗證伺服器憑證

ONTAP 包含大量預先安裝的根 CA 憑證。因此、在許多情況下、 ONTAP 會立即辨識您的授權伺服器憑證、而無需額外設定。但視授權伺服器憑證的簽署方式而定、您可能需要安裝根 CA 憑證和任何中繼憑證。

如有需要、請依照下列指示安裝憑證。您應該在叢集層級安裝所有必要的憑證。

根據您存取 ONTAP 的方式、選擇正確的程序。

範例 **1.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性 * 區段。
3. 單擊 * 證書 * 旁邊的 → 。
4. 在 * 信任的憑證授權單位 * 索引標籤下、按一下 * 新增 * 。
5. 按一下 * 匯入 * 並選取憑證檔案。
6. 完成環境的組態參數。
7. 按一下「 * 新增 * 」。

CLI

1. 開始安裝：

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

2. 查看下列主控台訊息：

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

3. 使用文字編輯器開啟憑證檔案。
4. 複製整個憑證、包括下列幾行：

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

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

5. 在命令提示字元之後、將憑證貼到終端機。
6. 按 **Enter** 鍵完成安裝。
7. 使用下列其中一項來確認已安裝憑證：

   ```
   security certificate show-user-installed

   security certificate show
   ```

步驟 **2** ：設定授權伺服器

您需要定義至少一個 ONTAP 授權伺服器。您應該根據組態和部署計畫來選擇參數值。檢閱 "OAuth2 部署案例" 以判斷您的組態所需的確切參數。

若要修改授權伺服器定義、您可以刪除現有定義並建立新定義。

以下提供的範例是根據第一個簡單部署案例、網址為： "本機驗證"。不使用 Proxy 就能使用獨立的範圍。

根據您存取 ONTAP 的方式、選擇正確的程序。CLI 程序會使用您在發出命令之前需要置換的符號變數。

範例 **2.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性 * 區段。
3. 按一下 * oAuth 2.0 授權 * 旁的 * + * 。
4. 選擇 * 更多選項 * 。
5. 提供部署所需的值、例如：
   - 名稱
   - 應用程式（ http ）
   - 提供者 JWKS URI
   - 發卡行 URI
6. 按一下「 * 新增 * 」。

CLI

1. 再次建立定義：

```
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
```

步驟 **3** ：啟用 **OAuth 2.0**

最後一步是啟用 OAuth 2.0 。這是 ONTAP 叢集的全域設定。

> 在您確認 ONTAP 、授權伺服器及任何支援服務均已正確設定之前、請勿啟用 OAuth 2.0 處理。

根據您存取 ONTAP 的方式、選擇正確的程序。

範例 **3.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性區段 * 。
3. 按一下 **OAuth 2.0** 授權 * 旁邊的 *→ 。
4. 啟用 * oAuth 2.0 授權 * 。

CLI

1. 啟用 OAuth 2.0 ：

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

2. 確認 OAuth 2.0 已啟用：

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

使用 **OAuth 2.0** 發出 **REST API** 呼叫

ONTAP 中的 OAuth 2.0 實作支援 REST API 用戶端應用程式。您可以使用 Curl 發出簡單的 REST API 呼叫、開始使用 OAuth 2.0 。以下範例擷取 ONTAP 叢集版本。

開始之前

您必須為 ONTAP 叢集設定並啟用 OAuth 2.0 功能。這包括定義授權伺服器。

步驟 **1** ：取得存取權杖

您必須取得存取權杖、才能與 REST API 呼叫搭配使用。權杖要求是在 ONTAP 之外執行、具體程序取決於授權伺服器及其組態。您可以透過網頁瀏覽器、使用 cURL 命令或使用程式設計語言來要求權杖。

以下是使用捲曲向 Keycloak 申請存取權杖的範例。

Keycloak 範例

```
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'
```

您應該複製並儲存傳回的權杖。

步驟 **2** ：發出 **REST API** 呼叫

擁有有效的存取權杖之後、您可以使用具有存取權杖的 cURL 命令來發出 REST API 呼叫。

參數與變數

下表說明了捲髮範例中的兩個變數。

變動	說明
$FQDN_IP	ONTAP 管理 LIF 的完整網域名稱或 IP 位址。
$access_token	由授權伺服器發出的 OAuth 2.0 存取權杖。

您應該先在 Bash Shell 環境中設定這些變數、然後再發佈 Curl 範例。例如、在 Linux CLI 中、輸入下列命令以設定及顯示 FQDN 變數：

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

在本機 Bash Shell 中定義兩個變數之後、您可以複製 curl 命令並將其貼到 CLI 中。按 **Enter** 以替換變數並發出命令。

Curl範例

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