



設定與部署 ONTAP 9

NetApp
April 24, 2024

目錄

設定與部署	1
準備使用 ONTAP 部署 OAuth 2.0	1
在 ONTAP 中部署 OAuth 2.0	2
使用 OAuth 2.0 發出 REST API 呼叫	6

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=5iTUf9QLGxAoYaliR33v1D5A2xq09V7'
```

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"
```

版權資訊

Copyright © 2024 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。