準備安裝SnapCenter 完此伺服器

SnapCenter software

NetApp
February 20, 2026

目錄

準備安裝SnapCenter 完此伺服器

安裝 SnapCenter 伺服器的需求

在 Windows 或 Linux 主機上安裝 SnapCenter 伺服器之前，您應該先檢閱並確定符合您環境的所有需求。

Windows 主機的網域和工作群組需求

SnapCenter 伺服器可以安裝在網域或工作群組中的 Windows 主機上。

擁有管理 Privileges 的使用者可以安裝 SnapCenter 伺服器。

- Active Directory 網域：您必須使用具有本機系統管理員權限的網域使用者。網域使用者必須是Windows主機上本機系統管理員群組的成員。
- 工作群組：您必須使用具有本機系統管理員權限的本機帳戶。

雖然支援網域信任、多網域樹系和跨網域信任、但不支援跨樹系網域。Microsoft的Active Directory網域及信任相關文件包含更多資訊。

安裝SnapCenter 完支援服務器後、您不應變更SnapCenter 支援該主機的網域。如果您從SnapCenter 安裝了支援服務器的網域中移除此伺服器主機SnapCenter 、然後嘗試解除安裝SnapCenter 支援服務器、則解除安裝作業會失敗。

空間與規模需求

您應該熟悉空間和規模需求。

項目	Windows 主機需求	Linux 主機需求
作業系統	Microsoft Windows 僅支援英文、德文、日文及簡體中文版的作業系統。 有關受支援版本的最新信息，請參閱 "NetApp 互通性對照表工具"。	• Red Hat Enterprise Linux （ RHEL ） 8 和 9 • SUSE Linux Enterprise Server （ SLES ） 15. 有關受支援版本的最新信息，請參閱 "NetApp 互通性對照表工具"。
最小CPU數	4核心	4核心
最低RAM	8 GB MySQL伺服器緩衝資源池使用總RAM的20%。	8 GB

項目	Windows 主機需求	Linux 主機需求
不需佔用SnapCenter 太多硬碟空間、即可容納整個伺服器軟體和記錄	7 GB 如果SnapCenter 您在SnapCenter 安裝了S什麼 伺服器的同一個磁碟機上有這個版本的資訊庫、建議您使用15 GB的容量。	15 GB
不需SnapCenter 佔用太多硬碟空間	8 GB 附註：如果SnapCenter 您在SnapCenter 安裝了該系統資訊庫的同一個磁碟機中安裝了該伺服器、則建議您使用15 GB的容量。	不適用
必要的軟體套件	• ASP.NET Core Runtime 8.0.12 （以及所有後續 8.0.x 修補程式）代管產品組合 • PowerShell 7.4.2 或更新版本 如需 .NET 特定疑難排解資訊、請參閱 "對於沒有網際網路連線的舊版系統、 SnapCenter 升級或安裝失敗"。	• NET Framework 8.0.12 （以及所有後續的 8.0.x 修補程式） • PowerShell 7.4.2 或更新版本 • Nginx 是可做為反向 Proxy 的 Web 伺服器 • Pam-devel PAM （可插拔驗證模組）是一種系統安全工具、可讓系統管理員設定驗證原則、而無需重新編譯執行驗證的程式。

ASP.NET 核心需要 IIS_IUSRS 來存取 Windows 上 SnapCenter Server 中的暫存檔系統。

SAN主機需求

SnapCenter 不包含主機公用程式或 DSM 。如果 SnapCenter 主機是 SAN （ FC/iSCSI ）環境的一部分，您可能需要在 SnapCenter 伺服器主機上安裝及設定其他軟體。

- 主機公用程式：主機公用程式支援 FC 和 iSCSI ，可讓您在 Windows 伺服器上使用 MPIO 。 "深入瞭解"。
- Microsoft DSM for Windows MPIO ：此軟體可搭配 Windows MPIO 驅動程式使用，以管理 NetApp 和 Windows 主機電腦之間的多個路徑。高可用度組態需要DSM。

如果您使用ONTAP 的是功能不實的DSM、則應移轉至Microsoft DSM。如需詳細資訊、請參閱 "如何從ONTAP 功能需求DSM移轉至Microsoft DSM"。

瀏覽器需求

SnapCenter 軟體支援 Chrome 125 及更新版本，以及 Microsoft Edge 110.0.1587.17 及更新版本。

連接埠需求

SnapCenter 軟體需要不同的連接埠，才能在不同元件之間進行通訊。

- 應用程式無法共用連接埠。
- 對於可自訂的連接埠、如果您不想使用預設連接埠、可以在安裝期間選取自訂連接埠。
- 對於固定連接埠、您應該接受預設的連接埠號碼。
- 防火牆
  - 防火牆、Proxy或其他網路裝置不應干擾連線。
  - 如果您在安裝SnapCenter 時指定自訂連接埠、則應在外掛主機上新增防火牆規則、以供SnapCenter 該連接埠用於「支援程式載入器」。

下表列出不同的連接埠及其預設值。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
SnapCenter Web 連接埠	8146	HTTPS	雙向	此連接埠用於 SnapCenter 用戶端（ SnapCenter 使用者）與 SnapCenter 伺服器之間的通訊，也用於從外掛主機與 SnapCenter 伺服器之間的通訊。 您可以自訂連接埠號碼。
WSSMCore通訊連接埠SnapCenter	8145	HTTPS	雙向	此連接埠可用於SnapCenter 在Sfor the Sfor Server 和SnapCenter 安裝了該插件的主機之間進行通訊。 您可以自訂連接埠號碼。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
排程器服務連接埠	8154	HTTPS		此連接埠用於 SnapCenter 集中化伺服器主機內所有受管理外掛程式的 SnapCenter 排程器工作流程。 您可以自訂連接埠號碼。
RabbitMQ 連接埠	5672	TCP		這是 RabbitMQ 接聽的預設連接埠、用於排程器服務與 SnapCenter 之間的發行者訂購者模式通訊。
MySQL連接埠	3306	HTTPS		連接埠用於與 SnapCenter 儲存庫資料庫通訊。您可以建立從 SnapCenter 伺服器到 MySQL 伺服器的安全連線。"深入瞭解"
Windows外掛程式主機	135 、 445	TCP		此連接埠用於 SnapCenter 伺服器與正在安裝外掛程式的主機之間的通訊。Microsoft 指定的其他動態連接埠範圍也應該是開放的。
Linux或AIX外掛程式主機	22	SSH	單向	此連接埠用於 SnapCenter 伺服器與主機之間的通訊，從伺服器啟動至用戶端主機。
適用於 Windows ，Linux 或 AIX 的 SnapCenter 外掛程式套件	8145	HTTPS	雙向	此連接埠用於 SMCore 與安裝外掛程式套件的主機之間的通訊。可自訂。 您可以自訂連接埠號碼。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
Oracle資料庫的支援外掛程式SnapCenter	27216			Oracle的外掛程式會使用預設的JDBC連接埠來連線至Oracle資料庫。
SnapCenter Plug-in for Exchange 資料庫	909			預設的 NET 。 Windows 外掛程式使用 TCP 連接埠來連線至 Exchange VSS 回撥。
NetApp 支援的 SnapCenter 外掛程式	9090	HTTPS		這是僅在插件主機上使用的內部連接埠；不需要防火牆例外。 SnapCenter 伺服器和插件之間的通訊透過連接埠 8145 進行。
叢集或SVM通訊連接埠ONTAP	• 443（HTTPS） • 80（HTTP）	• HTTPS • HTTP	雙向	此連接埠由SAL（Storage Abstraction Layer、Storage Abstraction Layer）使用、用於執行SnapCenter 支援服務器和SVM的主機之間的通訊。此連接埠目前也用於SnapCenter Windows外掛程式主機上的SAL、用於SnapCenter 在支援該外掛程式的主機和SVM之間進行通訊。
SAP HANA資料庫適用的插件SnapCenter	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	雙向	對於多租戶資料庫容器（MDC）單一租戶、連接埠編號以13結尾；對於非MDC、連接埠編號以15結尾。 您可以自訂連接埠號碼。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
適用於 PostgreSQL 的 SnapCenter 外掛程式	5432			此連接埠是預設的 PostgreSQL 連接埠，可讓 PostgreSQL 外掛程式與 PostgreSQL 叢集進行通訊。 您可以自訂連接埠號碼。

註冊以存取 SnapCenter 軟體

如果您是 Amazon FSX for NetApp ONTAP 或 Azure NetApp Files 的新手，而且沒有現有的 NetApp 帳戶，則應註冊以存取 SnapCenter 軟體。

開始之前

- 您應該可以存取公司電子郵件 ID 。
- 如果您使用的是 Azure NetApp Files 、則應擁有 Azure 訂閱 ID 。
- 如果您使用的是 Amazon FSX for NetApp ONTAP 、則您應該擁有適用於 ONTAP 檔案系統的 FSX 檔案系統 ID 。

關於這項工作

您的註冊必須經過資訊驗證，並可能需要一天的時間，才能確認新的 NetApp 支援網站（ NSS ）帳戶，並將其升級為 * 來賓 * 存取權限的 * 完整 * 存取權限。

步驟

1. 按一下 https://mysupport.netapp.com/site/user/registration 以進行註冊。
2. 輸入您的公司電子郵件 ID ，完成 captcha ，接受 NetApp 的隱私權政策，然後按一下 * 提交 * 。
3. 輸入傳送至您電子郵件 ID 的 OTP 、以驗證登錄、然後按一下 * 繼續 * 。
4. 在登錄完成頁面上、輸入下列詳細資料以完成登錄。
   a. 選擇 * NetApp 客戶 / 終端使用者 * 。
   b. 在序號欄位中，如果您使用的是 Azure NetApp Files ，請輸入 Azure 訂閱 ID ；如果您使用的是 Amazon FSX for NetApp ONTAP ，請輸入檔案系統 ID 。

如果您在登錄期間遇到任何問題、或是為了瞭解狀態、您可以在提出問題單 https://mysupport.netapp.com/site/help 。

多因素驗證（MFA）

管理多因素驗證（ MFA ）

您可以在 Active Directory Federation Service （ AD FS ）伺服器和 SnapCenter 伺服器中

管理多因素驗證（ MFA ）功能。

啟用多因素驗證（ **MFA** ）

您可以使用 PowerShell 命令為 SnapCenter 伺服器啟用 MFA 功能。

關於這項工作

- 在相同的AD FS中設定其他應用程式時、支援SSO型登入。SnapCenter在某些AD FS組態中、SnapCenter由於安全原因、可能需要使用者驗證、視AD FS工作階段持續性而定。
- 有關可與 Cmdlet 搭配使用的參數及其描述的資訊，可透過執行取得 `Get-Help command_name`。或者、您也可以參閱 "《軟件指令程式參考指南》SnapCenter"。

開始之前

- Windows Active Directory Federation Service（AD FS）應在各自的網域中啟動並執行。
- 您應該擁有 AD FS 支援的多因素驗證服務、例如 Azure MFA 、 Cisco Duo 等。
- 無論時區為何、均應使用相同的資訊區和AD FS伺服器時間戳記。SnapCenter
- 取得SnapCenter 並設定驗證伺服器的授權CA憑證。

  CA憑證為必填、原因如下：

  - 確保 ADFS-F5 通訊不會中斷、因為自我簽署的憑證在節點層級是唯一的。
  - 確保在獨立式或高可用度組態的升級、修復或災難恢復（DR）期間、不會重新建立自我簽署的憑證、因此可避免重新設定MFA。
  - 確保IP FQDN解析度。

    如需CA憑證的相關資訊、請參閱 "產生CA認證CSR檔案"。

步驟

1. 連線至Active Directory Federation Services（AD FS）主機。
2. 從下載AD FS聯盟中繼資料檔案 "https://<host fqfq>/ 聯邦中繼資料 /2007/06/Federation中繼 資料 .xml" 。
3. 將下載的檔案複製到SnapCenter 支援MFA功能的伺服器。
4. 透過PowerShell以「管理員」使用者身分登入SnapCenter 到「伺服器」SnapCenter 。
5. 使用PowerShell工作階段SnapCenter 、使用_New-SmMultifactorAuthenticationMetadata -path_ Cmdlet來產生FismFA中繼資料檔案。

   path參數指定將MFA中繼資料檔案儲存到SnapCenter Sof the Server主機的路徑。
6. 將產生的檔案複製到AD FS主機、以設定SnapCenter 將SURE做為用戶端實體。
7. 使用為 SnapCenter 伺服器啟用 MFA `Set-SmMultiFactorAuthentication` Cmdlet。
8. （選用）使用檢查 MFA 組態狀態和設定 `Get-SmMultiFactorAuthentication` Cmdlet。
9. 前往Microsoft管理主控台（MMC）並執行下列步驟：
   a. 按一下*檔案*>*新增/移除Snapin *。
   b. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。

c. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。

d. 按一下*主控台根目錄*>*憑證–本機電腦*>*個人*>*憑證*。

e. 在繫結SnapCenter 至SUn供 參考的CA憑證上按一下滑鼠右鍵、然後選取*所有工作*>*管理私密金鑰*。

f. 在權限精靈上執行下列步驟：

i. 按一下「 * 新增 * 」。

ii. 按一下 * 位置 * 、然後選取相關主機（階層架構頂端）。

iii. 在*位置*快顯視窗中按一下*確定*。

iv. 在物件名稱欄位中、輸入「IIS_IUSRS」、然後按一下*檢查名稱*、再按一下*確定*。

如果檢查成功、請按一下「確定」。

10. 在AD FS主機中、開啟AD FS管理精靈、然後執行下列步驟：

a. 右鍵點選*信賴廠商信任*>*新增信賴廠商信任*>*開始*。

b. 選取第二個選項、然後瀏覽SnapCenter 「Some MFA中繼資料」檔案、然後按一下「* Next*（下一步）」。

c. 指定顯示名稱、然後按一下*「下一步*」。

d. 視需要選擇存取控制原則、然後按一下 * 下一步 * 。

e. 在下一個索引標籤中選取預設值。

f. 單擊*完成*。

目前以依賴方的形式呈現提供的顯示名稱。SnapCenter

11. 選取名稱並執行下列步驟：

a. 按一下*編輯請款發放政策*。

b. 單擊* Add Rule（添加規則），然後單擊 Next*（下一步*）。

c. 指定宣告規則的名稱。

d. 選擇* Active Directory *作為屬性儲存區。

e. 選取「使用者-主要名稱」屬性、並選取傳出的報銷類型為*名稱- ID*。

f. 單擊*完成*。

12. 在ADFS伺服器上執行下列PowerShell命令。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. 請執行下列步驟、確認中繼資料已成功匯入。

a. 在依賴方信任上按一下滑鼠右鍵、然後選取*內容*。

b. 確認已填入端點、識別項和簽名欄位。

14. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

也可使用REST API來啟用「支援MFA」功能。SnapCenter

如需疑難排解資訊，請參閱 "在多個索引標籤中同時嘗試登入會顯示 MFA 錯誤"。

更新**AD FS MFA**中繼資料

只要AD FS伺服器有任何修改、例如升級、CA憑證續約、DR等、您就應該更新SnapCenter 位於支援區的AD FS MFA中繼資料。

步驟

1. 從下載AD FS聯盟中繼資料檔案 "https://<host Fqd>>/資料中繼資料/2007/06/FedationMetadata。XML」
2. 將下載的檔案複製SnapCenter 到「伺服器」以更新MFA組態。
3. 執行下列Cmdlet來更新SnapCenter Sf1中的AD FS中繼資料：

   ```
   Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
   ```

4. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

更新**SnapCenter** 功能不支援**MFA**中繼資料

每當有任何修改ADFS伺服器（例如修復、CA憑證續約、DR等）時、您就應該更新SnapCenter AD FS中的功能完善的MFA中繼資料。

步驟

1. 在AD FS主機中、開啟AD FS管理精靈、然後執行下列步驟：
   a. 選擇 * 信賴方信任 * 。
   b. 在為 SnapCenter 建立的信賴方信任上按一下滑鼠右鍵，然後選取 * 刪除 * 。

      隨即顯示使用者定義的信賴關係人信任名稱。

   c. 啟用多因素驗證（MFA）。

      請參閱 "啟用多因素驗證"。
2. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

停用多因素驗證（**MFA**）

步驟

1. 停用 MFA 、並清除使用啟用 MFA 時所建立的組態檔案 `Set-SmMultiFactorAuthentication` Cmdlet。
2. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie 、然後再次登入。

使用 **REST API** 、 **PowerShell** 和 **sccli** 來管理多因素驗證（ **MFA** ）

瀏覽器、 REST API 、 PowerShell 和 sccli 支援 MFA 登入。MFA 可透過 AD FS 身分識別管理員提供支援。您可以從 GUI 、 REST API 、 PowerShell 和 sccli 啟用 MFA 、停用 MFA 、以及設定 MFA 。

將 **AD FS** 設定為 **OAUTH/OIDC**

- 使用 Windows GUI 精靈 * 設定 AD FS
  1. 瀏覽至 * 伺服器管理員儀表板 * > * 工具 * > * ADFS 管理 * 。
  2. 瀏覽至 **ADFS** > * 應用程式群組 * 。
     a. 在 * 應用程式群組 * 上按一下滑鼠右鍵。
     b. 選取 * 新增應用程式群組 * 、然後輸入 * 應用程式名稱 * 。
     c. 選取 * 伺服器應用程式 * 。
     d. 單擊 * 下一步 * 。
  3. 複本 * 用戶端識別碼 * 。

     這是用戶端 ID 。 …在重新導向 URL 中新增回撥 URL （ SnapCenter 伺服器 URL ）。 …單擊 * 下一步 * 。
  4. 選取 * 產生共用密碼 * 。

     複製機密值。這是用戶端的秘密。 …單擊 * 下一步 * 。
  5. 在 * 摘要 * 頁面上、按一下 * 下一步 * 。
     a. 在 * 完整 * 頁面上、按一下 * 關閉 * 。
  6. 右鍵單擊新添加的 * 應用程序組 * ，然後選擇 * 屬性 * 。
  7. 從應用程式內容中選取 * 新增應用程式 * 。
  8. 按一下 * 新增應用程式 * 。

     選取「網路 API 」、然後按一下「 * 下一步 * 」。
  9. 在「設定 Web API 」頁面上、在「識別碼」區段中、輸入上一步所建立的 SnapCenter 伺服器 URL 和用戶端識別碼。
     a. 按一下「 * 新增 * 」。
     b. 單擊 * 下一步 * 。
  10. 在 * 選擇存取控制原則 * 頁面上、根據您的需求選擇控制原則（例如、允許所有人並要求 MFA ）、然後按一下 * 下一步 * 。
  11. 在「 * 設定應用程式權限 * 」頁面上、依預設會選取 OpenID 作為範圍、按一下 * 下一步 * 。
  12. 在 * 摘要 * 頁面上、按一下 * 下一步 * 。

      在 * 完整 * 頁面上、按一下 * 關閉 * 。

13. 在 * 範例應用程式內容 * 頁面上、按一下 * 確定 * 。
14. 由授權伺服器（ AD FS ）發出的 JWT 權杖、並打算由資源使用。

    此權杖的「 aud 」或「 Audience 」宣告必須符合資源或 Web API 的識別碼。

15. 編輯選取的 WebAPI 、並檢查回撥 URL （ SnapCenter 伺服器 URL ）和用戶端識別碼是否正確新增。

    設定 OpenID Connect 以提供宣告的使用者名稱。

16. 開啟位於伺服器管理員右上角 * 工具 * 功能表下的 * AD FS 管理 * 工具。
    a. 從左側側欄中選擇 * 應用程式群組 * 資料夾。
    b. 選取 Web API 、然後按一下 * 編輯 * 。
    c. 前往「發行轉換規則」標籤
17. 按一下*新增規則*。
    a. 在請款規則範本下拉式清單中、選取 * 將 LDAP 屬性傳送為請款 * 。
    b. 單擊 * 下一步 * 。
18. 輸入 * 請款規則 * 名稱。
    a. 在屬性儲存區下拉式清單中選取 * Active Directory* 。
    b. 在 **LDAP Attribute** 下拉列表中選擇 **User-Princie-Name** ，在 o*utGo Claim Type* 下拉列表中選擇 **UPN** 。
    c. 單擊*完成*。

使用 **PowerShell** 命令建立應用程式群組

您可以使用 PowerShell 命令建立應用程式群組、 Web API 、並新增範圍和宣告。這些命令以自動指令碼格式提供。如需詳細資訊、請參閱 <link to KB article> 。

1. 使用下列組合在 AD FS 中建立新的應用程式群組。

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier` 應用程式群組的名稱

   `redirectURL` 授權後重新導向的有效 URL

2. 建立 AD FS 伺服器應用程式並產生用戶端機密。

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. 建立 ADFS Web API 應用程式、並設定其應使用的原則名稱。

   ```
   $identifier = (New-Guid).Guid
   ```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 從下列命令的輸出中取得用戶端 ID 和用戶端機密、因為只會顯示一次。

```
"client_id = $identifier"

"client_secret: "$($ADFSApp.ClientSecret)
```

5. 將 allats補助 和 OpenID 權限授予 AD FS 應用程式。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 寫出轉換規則檔案。

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 命名 Web API 應用程式、並使用外部檔案定義其「發行轉換規則」。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

更新存取權杖到期時間

您可以使用 PowerShell 命令更新存取權杖到期時間。

關於此工作

- 存取權杖只能用於使用者、用戶端和資源的特定組合。存取權杖無法撤銷、且在過期前有效。
- 依預設、存取權杖的到期時間為 60 分鐘。 這段最短的到期時間已足夠且已調整。您必須提供足夠的價值、以避免任何持續進行的業務關鍵工作。

步驟

若要更新應用程式群組 WebApi 的存取權杖到期時間、請在 AD FS 伺服器中使用下列命令。

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

從 **AD FS** 取得承載權杖

您應該在任何 REST 用戶端（例如 Postman ）中填入下列參數、並提示您填寫使用者認證。此外、您應該輸入第二因素驗證（您擁有的東西和您的東西）來取得承載權杖。

+ 承載權杖的有效性可從 AD FS 伺服器根據應用程式進行設定、預設的有效期為 60 分鐘。

欄位	價值
授與類型	授權代碼
回撥 URL	如果您沒有回撥 URL 、請輸入應用程式的基礎 URL 。
驗證 URL	[ADFS- 網域名稱]/ADFS/OAuth2/Authorize
存取權杖 URL	[ADFS- 網域名稱]/ADFS/OAuth2/token
用戶端ID	輸入 AD FS 用戶端 ID
用戶端機密	輸入 AD FS 用戶端機密
範圍	OpenID
用戶端驗證	以基本驗證標頭傳送
資源	在 **Advance Options** 標籤中、新增與 Callback URL 值相同的資源欄位、此值在 JWT Token 中會顯示為「 aud 」值。

使用 **PowerShell** 、 **sccli** 和 **REST API** 在 **SnapCenter** 伺服器中設定 **MFA**

您可以使用 PowerShell 、 sccli 和 REST API 在 SnapCenter 伺服器中設定 MFA 。

SnapCenter MFA CLI 驗證

在 PowerShell 和 sccli 中、現有的 Cmdlet （ Open-SmConnection ）會以另一個稱為「 AccessToken 」的欄位來延伸、以使用承載權杖來驗證使用者。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

執行上述 Cmdlet 之後，會建立工作階段，讓個別使用者進一步執行 SnapCenter Cmdlet 。

SnapCenter MFA REST API 驗證

在 REST API 用戶端（例如 Postman 或 swagger ）中使用 _Authorization=B承載 <access token> 格式的承載權杖、並在標頭中提及使用者 RoleName 、以取得 SnapCenter 的成功回應。

MFA REST API 工作流程

當 MFA 設定為 AD FS 時、您應該使用存取（承載）權杖進行驗證、以便透過任何 REST API 存取 SnapCenter 應用程式。

關於此工作

- 您可以使用任何 REST 用戶端、例如 Postman 、 Swagger UI 或 Fireplane 。
- 取得存取權杖、並使用它來驗證後續要求（ SnapCenter REST API ）以執行任何作業。

步驟

- 透過 AD FS MFA * 驗證
  1. 設定 REST 用戶端呼叫 AD FS 端點以取得存取權杖。

     當您按下按鈕以取得應用程式的存取權杖時、系統會將您重新導向至 AD FS SSO 頁面、您必須在其中提供 AD 認證並驗證 MFA 。 1. 在 AD FS SSO 頁面的「使用者名稱」文字方塊中、輸入您的使用者名稱或電子郵件。

     使用者名稱必須格式化為 user@domain 或 domain\user 。

  2. 在密碼文字方塊中、輸入您的密碼。
  3. 按一下*登入*。
  4. 在 * 登入選項 * 區段中、選取驗證選項並進行驗證（視您的組態而定）。
     - 推播：核准傳送至手機的推播通知。
     - QR 代碼：使用驗證點行動應用程式掃描 QR 代碼、然後輸入應用程式中顯示的驗證代碼
     - 一次性密碼：輸入 Token 的一次性密碼。
  5. 驗證成功後、會開啟一個快顯視窗、其中包含存取權、 ID 和重新整理 Token 。

     複製存取權杖、並在 SnapCenter REST API 中使用它來執行作業。

  6. 在 REST API 中、您應該在標頭區段中傳遞存取權杖和角色名稱。
  7. SnapCenter 會從 AD FS 驗證此存取權杖。

如果它是有效的權杖、 SnapCenter 會將其解碼、並取得使用者名稱。

8. SnapCenter 會使用使用者名稱和角色名稱來驗證使用者執行 API 。

   如果驗證成功、 SnapCenter 會傳回結果、否則會顯示錯誤訊息。

啟用或停用 **REST API** 、 **CLI** 和 **GUI** 的 **SnapCenter MFA** 功能

- 圖形使用者介面 *

步驟

1. 以 SnapCenter 管理員身分登入 SnapCenter Server 。
2. 按一下 * 設定 * > * 全域設定 * > * 多重資料驗證（ MFA ）設定 *
3. 選取介面（ GUI/RST API/CLI ）以啟用或停用 MFA 登入。
   - PowerShell 介面 *

步驟

1. 執行 PowerShell 或 CLI 命令、以啟用 MFA for GUI 、 REST API 、 PowerShell 和 sccli 。

   ```
   Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
   -IsCliMFAEnabled -Path
   ```

   path 參數會指定 AD FS MFA 中繼資料 XML 檔案的位置。

   啟用 MFA 以使用指定的 AD FS 中繼資料檔案路徑來設定 SnapCenter GUI 、 REST API 、 PowerShell 和 sccli 。

2. 使用檢查 MFA 組態狀態和設定 `Get-SmMultiFactorAuthentication` Cmdlet。

*sccli 介面 *

步驟

1. ```
   # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
   -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
   "C:\ADFS_metadata\abc.xml"
   ```
2. ```
   # sccli Get-SmMultiFactorAuthentication
   ```
   - REST API*
3. 執行下列 POST API 以啟用 MFA for GUI 、 REST API 、 PowerShell 和 sccli 。

參數	價值
要求的 URL	/API/4.9/settings/multitactorauthentication
HTTP方法	貼文

要求主體	｛ "IsGuiMFAEnabled" ：錯誤、 "IsRestApiMFAEnabled" ：對、 "IsClicMFAEnabled" ：錯、 "ADFSConfigFilePath" ： "C:\\ADFS_中繼 資料 \\abc.xml " }
回應本文	｛ "MFAConfiguration" ： { "IsGuiMFAEnabled" ： 錯誤、 "ADFSConfigFilePath" ： "C:\\ADFS_中繼 資料 \\abc.xml 、 "SCConfigFilePath" ： null 、 "IsRestApiMFAEnabled" ：對、 "IsClicMFAEnabled" ：錯、 "ADFSHostName" ： "win-adfs-sc49.winscedom2.com } }

4. 使用下列 API 檢查 MFA 組態狀態和設定。

參數	價值
要求的 URL	/API/4.9/settings/multitactorauthentication
HTTP方法	取得
回應本文	｛ "MFAConfiguration" ： { "IsGuiMFAEnabled" ： 錯誤、 "ADFSConfigFilePath" ： "C:\\ADFS_中繼 資料 \\abc.xml 、 "SCConfigFilePath" ： null 、 "IsRestApiMFAEnabled" ：對、 "IsClicMFAEnabled" ：錯、 "ADFSHostName" ： "win-adfs-sc49.winscedom2.com } }