



準備安裝**SnapCenter**伺服器

SnapCenter software

NetApp
November 06, 2025

目錄

準備安裝SnapCenter伺服器	1
安裝SnapCenter伺服器的要求	1
Windows 主機的網域和工作群組需求	1
空間和尺寸要求	1
SAN 主機需求	2
瀏覽器要求	3
端口要求	3
註冊以存取SnapCenter software	6
多重身份驗證 (MFA)	6
管理多重身分驗證 (MFA)	6
使用 Rest API、PowerShell 和 SCCLI 管理多重驗證 (MFA)	9
使用 PowerShell、SCCLI 和 REST API 在SnapCenter Server 中設定 MFA	13

準備安裝SnapCenter伺服器

安裝SnapCenter伺服器的要求

在 Windows 或 Linux 主機上安裝SnapCenter Server 之前，您應該檢查並確保滿足您的環境的所有要求。

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。

具有管理員權限的使用者可以安裝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 主機上本機管理員群組的成員。
- 工作群組：您必須使用具有本機管理員權限的本機帳戶。

雖然支援域信任、多域林和跨域信任，但不支援跨林域。有關 Active Directory 網域和信任的 Microsoft 文件包
含更多資訊。



安裝SnapCenter伺服器後，您不應變更SnapCenter主機所在的網域。如果從安裝SnapCenter Server 時所在的網域中移除SnapCenter Server 主機，然後嘗試解除安裝SnapCenter Server，則解除安裝作業將會失敗。

空間和尺寸要求

您應該熟悉空間和尺寸要求。

物品	Windows 主機需求	Linux 主機需求
作業系統	微軟 Windows 僅支援英文、德文、日文和簡體中文版本的作業系統。 有關受支援版本的最新信息，請參閱 https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT[\"NetApp 互通性表工具\"] 。	• Red Hat Enterprise Linux (RHEL) 8 與 9 • SUSE Linux 企業伺服器 (SLES) 15 有關受支援版本的最新信息，請參閱 https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT[\"NetApp 互通性表工具\"] 。
最小 CPU 數量	4 核	4 核

物品	Windows 主機需求	Linux 主機需求
最低記憶體	8GB  MySQL 伺服器緩衝池使用了總 RAM 的 20%。	8GB
SnapCenter 伺服器軟體和日誌的最小硬碟空間	7GB  如果 SnapCenter 儲存庫與安裝 SnapCenter Server 的磁碟機位於相同磁碟機中，則建議使用 15 GB。	15GB
SnapCenter 儲存庫的最小硬碟空間	8GB  注意：如果 SnapCenter 伺服器與安裝 SnapCenter 儲存庫的磁碟機相同，建議使用 15 GB。	不適用
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 7.4.2 或更高版本 有關 .NET 特定的故障排除信息，請參閱 "對於沒有 Internet 連線的傳統系統，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 或更高版本 • Nginx 是一個可以用作反向代理的 Web 伺服器 • Pam-devel PAM（可插入式身份驗證模組）是一種系統安全工具，它允許系統管理員設定身份驗證策略，而無需重新編譯執行身份驗證的程式。



ASP.NET 核心需要 IIS_IUSRS 才能存取 Windows 上 SnapCenter Server 中的暫存檔案系統。

SAN 主機需求

SnapCenter 不包括主機實用程式或 DSM。如果 SnapCenter 主機是 SAN（FC/iSCSI）環境的一部分，則可能需要在 SnapCenter Server 主機上安裝和設定其他軟體。

- 主機實用程式：主機實用程式支援 FC 和 iSCSI，它使您能夠在 Windows 伺服器上使用 MPIO。 ["了解更多"](#)

。

- Microsoft DSM for Windows MPIO：軟體與 Windows MPIO 驅動程式搭配使用，以管理NetApp和 Windows 主機之間的多條路徑。高可用性配置需要 DSM。



如果您使用的是ONTAP DSM，則應該遷移到 Microsoft DSM。有關更多信息，請參閱 ["如何從ONTAP DSM 遷移到 Microsoft DSM"](#)。

瀏覽器要求

SnapCenter software支援 Chrome 125 及更高版本以及 Microsoft Edge 110.0.1587.17 及更高版本。

端口要求

SnapCenter software需要不同的連接埠來實現不同元件之間的通訊。

- 應用程式不能共享連接埠。
- 對於可自訂的端口，如果您不想使用預設端口，您可以在安裝期間選擇自訂端口。
- 對於固定端口，您應該接受預設端口號。
- 防火牆
 - 防火牆、代理或其他網路設備不應干擾連線。
 - 如果在安裝SnapCenter時指定自訂端口，則應在插件主機上為SnapCenter插件Loader的該連接埠新增防火牆規則。

下表列出了不同的連接埠及其預設值。

連接埠名稱	連接埠號	協定	方向	描述
SnapCenter Web 連接埠	8146	HTTPS	雙向	此連接埠用於SnapCenter用戶端（SnapCenter用戶）與SnapCenter伺服器之間的通信，也用於從插件主機到SnapCenter伺服器的通訊。 您可以自訂連接埠號。
SnapCenter SMCORE 通訊端口	8145	HTTPS	雙向	此連接埠用於SnapCenter伺服器與安裝了SnapCenter插件的主機之間的通訊。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
調度程序服務端口	8154	HTTPS		此連接埠用於以集中方式協調SnapCenter伺服器主機內所有託管插件的SnapCenter調度程序工作流程。 您可以自訂連接埠號。
RabbitMQ 端口	5672	TCP		這是 RabbitMQ 監聽的預設端口，用於 Scheduler 服務和SnapCenter之間的發布者-訂閱者模型通訊。
MySQL 連接埠	3306	HTTPS		此連接埠用於與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。"了解更多"
Windows 插件主機	135 , 445	TCP		此連接埠用於SnapCenter伺服器與安裝插件的主機之間的通訊。 Microsoft 指定的其他動態連接埠範圍也應開放。
Linux 或 AIX 插件主機	22	SSH	單向	此連接埠用於SnapCenter伺服器和主機之間的通信，從伺服器發起到客戶端主機。
適用於 Windows、Linux 或 AIX 的SnapCenter插件包	8145	HTTPS	雙向	此連接埠用於SMCore與安裝插件包的主機進行通訊。可客製化。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
適用於 Oracle 資料庫的SnapCenter插件	27216			Oracle 插件使用預設 JDBC 連接埠來連接 Oracle 資料庫。
適用於 Exchange 資料庫的SnapCenter插件	909			Windows 插件使用預設的 NET.TCP 連接埠來連接 Exchange VSS 回呼。
NetApp支援的SnapCenter插件	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 and 插件之間的通訊透過連接埠 8145 進行。
ONTAP叢集或 SVM 通訊埠	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	雙向	此連接埠由 SAL（儲存抽象層）用於執行SnapCenter Server 的主機和 SVM 之間的通訊。SnapCenter for Windows 插件主機上的 SAL 目前也使用該連接埠來實作SnapCenter插件主機和 SVM 之間的通訊。
適用於 SAP HANA 資料庫的SnapCenter插件	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	雙向	對於多租戶資料庫容器（MDC）單一租戶，連接埠號碼以13結尾；對於非MDC，連接埠號碼以15結尾。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
適用於 PostgreSQL 的 SnapCenter 插件	5432			此連接埠是 PostgreSQL 外掛程式與 PostgreSQL 叢集通訊所使用的預設 PostgreSQL 連接埠。 您可以自訂連接埠號。

註冊以存取 SnapCenter software

如果您是 Amazon FSx for NetApp ONTAP 或 Azure NetApp Files 的新使用者且沒有現有的 NetApp 帳戶，則應該註冊以存取 SnapCenter software。

開始之前

- 您應該可以存取公司電子郵件 ID。
- 如果您使用 Azure NetApp Files，則應該擁有 Azure 訂閱 ID。
- 如果您使用的是 Amazon FSx for NetApp ONTAP，則應該擁有 FSx for ONTAP 檔案系統的檔案系統 ID。

關於此任務

您的註冊需要經過資訊驗證，可能需要一天時間才能確認並將新的 NetApp 支援網站 (NSS) 帳戶從 訪客 存取權限升級為 完全 存取權限。

步驟

1. 點選 <https://mysupport.netapp.com/site/user/registration> 進行註冊。
2. 輸入您的公司電子郵件 ID，完成驗證碼，接受 NetApp 的隱私權政策，然後按一下「提交」。
3. 透過輸入發送到您的電子郵件 ID 的 OTP 來驗證註冊，然後按一下「繼續」*。
4. 在註冊完成頁面，輸入以下詳細資訊以完成註冊。
 - a. 選擇* NetApp 客戶/最終使用者*。
 - 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。



您可以提交以下票證：<https://mysupport.netapp.com/site/help> 如果您在註冊過程中遇到任何問題或想了解狀態。

多重身份驗證 (MFA)

管理多重身分驗證 (MFA)

您可以管理 Active Directory 聯合驗證服務 (AD FS) 伺服器和 SnapCenter 伺服器中的多重驗證 (MFA) 功能。

啟用多重身份驗證 (MFA)

您可以使用 PowerShell 指令為 SnapCenter Server 啟用 MFA 功能。

關於此任務

- 當在相同 AD FS 中設定其他應用程式時，SnapCenter 支援基於 SSO 的登入。在某些 AD FS 配置中，SnapCenter 可能會出於安全性原因要求使用者進行身份驗證，具體取決於 AD FS 會話持久性。
- 可以透過執行以下命令來取得有關可與 cmdlet 一起使用的參數及其描述的信息 `Get-Help command_name`。或者，您也可以查看 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

開始之前

- Windows Active Directory 聯合驗證服務 (AD FS) 應該會在對應的網域中啟動並執行。
- 您應該擁有 AD FS 支援的多重驗證服務，例如 Azure MFA、Cisco Duo 等。
- 無論時區為何，SnapCenter 和 AD FS 伺服器時間戳記都應該相同。
- 為 SnapCenter Server 採購並配置授權 CA 憑證。

由於以下原因，CA 證書是強制性的：

- 確保 ADFS-F5 通訊不會中斷，因為自簽名憑證在節點層級是唯一的。
- 確保在獨立或高可用性配置中的升級、修復或災難復原 (DR) 期間，不會重新建立自簽名證書，從而避免重新配置 MFA。
- 確保 IP-FQDN 解析。

有關 CA 憑證的信息，請參閱 ["產生 CA 憑證 CSR 文件"](#)。

步驟

1. 連線至 Active Directory 聯合驗證服務 (AD FS) 主機。
2. 從下列位置下載 AD FS 聯合元資料文件 <https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml>。
3. 將下載的檔案複製到 SnapCenter Server 以啟用 MFA 功能。
4. 透過 PowerShell 以 SnapCenter 管理員使用者身分登入 SnapCenter 伺服器。
5. 使用 PowerShell 會話，使用 `New-SmMultifactorAuthenticationMetadata -path` cmdlet 產生 SnapCenter MFA 元資料檔。

`path` 參數指定在 SnapCenter Server 主機中儲存 MFA 元資料檔案的路徑。

6. 將產生的檔案複製到 AD FS 主機以將 SnapCenter 配置為客戶端實體。
7. SnapCenter `'Set-SmMultiFactorAuthentication'` 命令。
8. (可選) 使用以下方式檢查 MFA 配置狀態和設置 `'Get-SmMultiFactorAuthentication'` 命令。
9. 前往 Microsoft 管理控制台 (MMC) 並執行下列步驟：
 - a. 按一下“檔案”>“新增/刪除管理單元”。
 - b. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
 - c. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。

- d. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
- e. 右鍵點選綁定到SnapCenter 的CA 證書，然後選擇 所有任務 > 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. 點擊*位置*並選擇相關主機（層次結構的頂部）。
 - iii. 在「位置」彈出視窗中按一下「確定」。
 - iv. 在物件名稱欄位中，輸入“IIS_IUSRS”，然後按一下“檢查名稱”，然後按一下“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 管理精靈並執行下列步驟：
 - a. 右鍵點選*依賴方信任*>*新增依賴方信任*>*開始*。
 - b. 選擇第二個選項並瀏覽SnapCenter MFA 元資料文件，然後按一下「下一步」。
 - c. 指定顯示名稱並按一下“下一步”。
 - d. 根據需要選擇存取控制策略，然後按一下「下一步」。
 - e. 在下一個選項卡中選擇預設設定。
 - f. 按一下“完成”。

SnapCenter現在反映為具有所提供顯示名稱的依賴方。

11. 選擇名稱並執行以下步驟：
 - a. 按一下「編輯索賠簽發政策」。
 - b. 按一下“新增規則”，然後按一下“下一步”。
 - c. 指定聲明規則的名稱。
 - d. 選擇*Active Directory*作為屬性儲存。
 - e. 選擇屬性為 **User-Principal-Name**，傳出宣告類型為 **Name-ID**。
 - f. 按一下“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. 執行下列步驟以確認元資料已成功匯入。
 - a. 右鍵點選信賴方信任並選擇“屬性”。
 - b. 確保端點、標識符和簽名欄位已填入。
14. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

SnapCenter MFA 功能也可以使用 REST API 啟用。

有關故障排除信息，請參閱 ["在多個選項卡中同時嘗試登入時顯示 MFA 錯誤"](#)。

更新 AD FS MFA 元數據

每當 AD FS 伺服器發生任何修改（例如昇級、CA 憑證續約、DR 等）時，您都應該更新 SnapCenter 中的 AD FS MFA 元資料。

步驟

1. 從下列位置下載 AD FS 聯合元資料文件"<https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. 將下載的檔案複製到 SnapCenter Server 以更新 MFA 設定。
3. 透過執行以下 cmdlet 更新 SnapCenter 中的 AD FS 元資料：

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

4. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

更新 SnapCenter MFA 元數據

每當 ADFS 伺服器發生任何修改（例如修復、CA 憑證續約、DR 等）時，您都應該更新 AD FS 中的 SnapCenter MFA 元資料。

步驟

1. 在 AD FS 主機中，開啟 AD FS 管理精靈並執行下列步驟：
 - a. 選擇*依賴方信任*。
 - b. 右鍵點選為 SnapCenter 建立的信賴方信任並選擇「刪除」。

將顯示依賴方信任的使用者定義名稱。

- c. 啟用多重身份驗證 (MFA)。

看["啟用多重身份驗證"](#)。

2. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

停用多重身份驗證 (MFA)

步驟

1. 停用 MFA 並清理啟用 MFA 時建立的設定文件，方法是使用 `Set-SmMultiFactorAuthentication` 命令。
2. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

使用 Rest API、PowerShell 和 SCCLI 管理多重驗證 (MFA)

支援透過瀏覽器、REST API、PowerShell 和 SCCLI 進行 MFA 登入。MFA 透過 AD FS 身份管理器支援。您可以從 GUI、REST API、PowerShell 和 SCCLI 啟用 MFA、停用 MFA 和設定 MFA。

將 AD FS 設定為 OAuth/OIDC

使用 Windows GUI 精靈設定 AD FS

1. 導覽至 伺服器管理員儀表板 > 工具 > **ADFS 管理**。
2. 導覽至 **ADFS** > 應用程式群組。
 - a. 右鍵點選“應用程式群組”。
 - b. 選擇*新增應用程式群組*並輸入*應用程式名稱*。
 - c. 選擇*伺服器應用程式*。
 - d. 按一下“下一步”。
3. 複製*客戶端識別碼*。

這是客戶端 ID。..在重新導向 URL 中新增回呼 URL（SnapCenter伺服器 URL）。..按一下“下一步”。

4. 選擇*產生共享金鑰*。

複製秘密值。這是客戶的秘密。..按一下“下一步”。

5. 在「摘要」頁面上，按一下「下一步」。
 - a. 在*完成*頁面上，按一下*關閉*。
6. 右鍵點選新新增的*應用程式群組*並選擇*屬性*。
7. 從應用程式屬性中選擇*新增應用程式*。
8. 點擊“新增應用程式”。

選擇 Web API 並按一下「下一步」。

9. 在設定 Web API 頁面上，將上一個步驟建立的SnapCenter伺服器 URL 和用戶端識別碼輸入到識別碼部分。
 - a. 按一下“新增”。
 - b. 按一下“下一步”。
10. 在*選擇存取控制策略*頁面上，根據您的要求選擇控制策略（例如，允許所有人並要求 MFA），然後按一下*下一步*。
11. 在*配置應用程式權限*頁面，預設選擇openid作為範圍，點擊*下一步*。
12. 在「摘要」頁面上，按一下「下一步」。

在*完成*頁面上，按一下*關閉*。

13. 在「範例應用程式屬性」頁面上，按一下「確定」。
14. JWT 令牌由授權伺服器（AD FS）頒發，供資源使用。

此令牌的「aud」或受眾聲明必須與資源或 Web API 的識別碼相符。

15. 編輯選定的 WebAPI 並檢查回呼 URL（SnapCenter伺服器 URL）和用戶端識別碼是否正確新增。

配置 OpenID Connect 以提供使用者名稱作為聲明。

16. 開啟位於伺服器管理員右上角*工具*選單下的*AD FS 管理*工具。
 - a. 從左側邊欄中選擇“應用程式群組”資料夾。
 - b. 選擇 Web API 並點選 **EDIT**。
 - c. 前往發行轉換規則標籤
17. 按一下“新增規則”。
 - a. 在聲明規則範本下拉選單中選擇*將 LDAP 屬性作為聲明傳送*。
 - b. 按一下“下一步”。
18. 輸入*聲明規則*名稱。
 - a. 在屬性儲存下拉選單中選擇*Active Directory*。
 - b. 在 **LDAP Attribute** 下拉選單中選擇 **User-Principal-Name**，在 **O*utgoing Claim Type*** 下拉選單中選擇 **UPN**。
 - c. 按一下“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 並新增範圍和聲明。這些命令以自動腳本格式提供。欲了解更多信息，請參閱[連結至知識庫文章](#)。

1. 使用以下命令在 AD FS 中建立新的應用程式組。

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

`ClientRoleIdentifier` 您的應用程式群組的名稱

`redirectURL` 授權後重定向的有效 URL

2. 建立 AD FS 伺服器應用程式並產生客戶端機密。

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

3. 建立 ADFS Web API 應用程式並配置其應使用的策略名稱。

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

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

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

4. 從以下命令的輸出中取得客戶端 ID 和客戶端金鑰，因為它只顯示一次。

```
"client_id = $identifier"
```

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

5. 授予 AD FS 應用程式 allatclaims 和 openid 權限。

```
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。

```
$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文件定義其頒發轉換規則。

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

更新訪問令牌到期時間

您可以使用 PowerShell 指令更新存取權杖的到期時間。

關於此任務

- 存取令牌只能用於使用者、用戶端和資源的特定組合。存取令牌不能被撤銷，並且在到期前有效。
- 預設情況下，存取令牌的有效期為 60 分鐘。此最短到期時間足夠且可擴充。您必須提供足夠的價值以避免任何正在進行的關鍵業務工作。

步

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 取得持有者令牌

您應該在任何 REST 用戶端（如 Postman）中填寫下面提到的參數，它會提示您填寫使用者憑證。此外，您應該輸入第二因素身份驗證（您擁有的東西和您是誰的東西）來獲取承載令牌。

+ 持有者令牌的有效性可根據應用程式從 AD FS 伺服器進行配置，預設有效期為 60 分鐘。

場地	價值
資助類型	授權碼
回調URL	如果您沒有回調 URL，請輸入應用程式的基本 URL。
授權網址	[adfs 網域]/adfs/oauth2/授權
訪問令牌 URL	[adfs 網域]/adfs/oauth2/token
客戶端 ID	輸入 AD FS 用戶端 ID
客戶端機密	輸入 AD FS 用戶端機密
範圍	OpenID
客戶端身份驗證	作為基本 AUTH 標頭發送
資源	在「進階選項」標籤中，新增與回呼 URL 具有相同值的資源字段，該字段會作為 JWT 令牌中的「aud」值出現。

使用 PowerShell、SCCLI 和 REST API 在 SnapCenter Server 中設定 MFA

您可以使用 PowerShell、SCCLI 和 REST API 在 SnapCenter Server 中設定 MFA。

SnapCenter MFA CLI 身份驗證

在 PowerShell 和 SCCLI 中，現有的 cmdlet（Open-SmConnection）擴展了一個名為「AccessToken」的字段，以使用承載令牌對使用者進行身份驗證。

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

執行上述 cmdlet 後，將為對應使用者建立一個會話以執行進一步的 SnapCenter cmdlet。

SnapCenter MFA Rest API 驗證

在 REST API 用戶端（如 Postman 或 swagger）中使用格式為 *Authorization=Bearer <access token>* 的承載令牌，並在標頭中提及使用者 RoleName 以從 SnapCenter 獲得成功回應。

MFA Rest API 工作流程

當使用 AD FS 設定 MFA 時，您應該使用存取（承載）令牌進行身份驗證，以透過任何 Rest API 存取 SnapCenter 應用程式。

關於此任務

- 您可以使用任何 REST 用戶端，例如 Postman、Swagger UI 或 FireCamp。
- 取得存取權杖並使用它來驗證後續請求（SnapCenter Rest API）以執行任何操作。

步驟

透過 AD FS MFA 進行身份驗證

1. 配置 REST 用戶端以呼叫 AD FS 端點來取得存取權杖。

當您點擊按鈕以取得應用程式的存取權杖時，您將被重新導向至 AD FS SSO 頁面，您必須在該頁面提供您的 AD 憑證並使用 MFA 進行驗證。1. 在 AD FS SSO 頁面中，在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. 點選“登入”。
4. 從*登入選項*部分，選擇一個身份驗證選項並進行身份驗證（取決於您的配置）。
 - 推播：批准發送到您手機的推播通知。
 - 二維碼：使用 AUTH Point 手機應用程式掃描二維碼，然後輸入應用程式中顯示的驗證碼
 - 一次性密碼：輸入您的令牌的一次性密碼。
5. 身份驗證成功後，將開啟一個彈出窗口，其中包含存取、ID 和刷新令牌。

複製存取權杖並在 SnapCenter Rest API 中使用它來執行操作。

6. 在 Rest API 中，您應該在標題部分傳遞存取權杖和角色名稱。
7. SnapCenter 從 AD FS 驗證此存取權杖。

如果它是有效令牌，SnapCenter 會對其進行解碼並取得使用者名稱。

8. SnapCenter 使用使用者名稱和角色名稱對使用者進行身份驗證以執行 API。

如果驗證成功，SnapCenter 將傳回結果，否則將顯示錯誤訊息。

為 **Rest API**、**CLI** 和 **GUI** 啟用或停用**SnapCenter MFA** 功能

圖形使用者介面

步驟

- 1. 以SnapCenter管理員身分登入SnapCenter伺服器。
- 2. 點擊“設定”>“全域設定”>“多重身份驗證 (MFA) 設定”
- 3. 選擇介面（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 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

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

路徑參數指定 AD FS MFA 元資料 xml 檔案的位置。

使用指定的 AD FS 元資料檔案路徑配置的SnapCenter GUI、Rest API、PowerShell 和 SCCLI 啟用 MFA。

- 2. 使用 `Get-SmMultiFactorAuthentication` 命令。

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

- 1. 執行以下文章 API 以啟用 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

範圍	價值
請求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	郵政
請求正文	{ "IsGuiMFAEnabled" : false ， 「IsRestApiMFAEnabled」 : true ， 「IsCliMFAEnabled」 : false ， 「ADFSConfigFilePath」 : 「C:\ADFS_metadata\abc.xml」 }

回應主體	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false ， "ADFSSConfigFilePath" : "C : \\ADFS_metadata \\abc.xml" ， 「SCConfigFilePath」 : null ， 「IsRestApiMFAEnabled」 : true ， 「IsCliMFAEnabled」 : false ， 「ADFSHostName」 : 「win-adfs- sc49.winscedom2.com」 } }
------	--

2. 使用以下 API 檢查 MFA 配置狀態和設定。

範圍	價值
請求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	得到
回應主體	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false ， "ADFSSConfigFilePath" : "C : \\ADFS_metadata \\abc.xml" ， 「SCConfigFilePath」 : null ， 「IsRestApiMFAEnabled」 : true ， 「IsCliMFAEnabled」 : false ， 「ADFSHostName」 : 「win-adfs- sc49.winscedom2.com」 } }

版權資訊

Copyright © 2025 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。