多重身份驗證 (MFA)

SnapCenter software

NetApp
November 06, 2025

目錄

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 ，“ADFSConfigFilePath”：“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 ，“ADFSConfigFilePath”：“C：\\ADFS_metadata \\abc.xml”， 「SCConfigFilePath」：null ，「IsRestApiMFAEnabled」：true ，「IsCliMFAEnabled」：false ，「ADFSHostName」：「win-adfs-sc49.winscedom2.com」 } }

版權資訊

商標資訊