



多因素驗證 (MFA)

SnapCenter Software 5.0

NetApp
July 18, 2024

目錄

多因素驗證 (MFA)	1
管理多因素驗證 (MFA)	1
使用 REST API、PowerShell 和 sccli 來管理多因素驗證 (MFA)	4
使用 PowerShell、sccli 和 REST API 在 SnapCenter 伺服器中設定 MFA	8

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 and 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 FQDN>/Federation中繼 資料 /2007/06/Federation中繼 資料 .xml 下載 AD FS 同盟中繼資料檔案 "[https://<host](#)"。
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 Cmdlet 為 SnapCenter Server 啟用 MFA Set-SmMultiFactorAuthentication 。
8. (選用) 使用 Cmdlet 檢查 MFA 組態狀態和設定 Get-SmMultiFactorAuthentication 。
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 FQDN>/ 同盟中繼資料 /2007/06/Federation中繼 資料 .xml" 下載 AD FS 同盟中繼資料檔案 "<https://<host>>
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. 按一下*信賴廠商信任*。
 - b. 在建立SnapCenter 的依賴方信任上按一下滑鼠右鍵、然後按一下「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 並清除在使用 Cmdlet 啟用 MFA 時所建立的組態檔案 `Set-SmMultiFactorAuthentication`。
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 * 應用程式組 *，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 頁面中、於使用者名稱文字方塊中鍵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。

1. 在密碼文字方塊中、輸入您的密碼。
2. 按一下*登入*。

3. 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。
4. 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。
5. 在 REST API 中、您應該在標頭區段中傳遞存取權杖和角色名稱。
6. 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。
7. 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 Cmdlet 檢查 MFA 組態狀態和設定 `Get-SmMultiFactorAuthentication`。

*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" : false 、 "IsRestApiMFAEnabled" : true 、 "IsClimFAEnabled" : false 、 "FSConfigFilePath" : "C:\ADFS_中繼 資料 \abc.xml " }
回應本文	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false 、 "ADFSSConfigFilePath" : "C:\ADFS_中繼 資料 \abc.xml 、 "SCConfigFilePath" : null 、 "IsApRestiMFAEnabled" : true 、 "IsClimFAEnabled" : false 、 「 ADFSHostName 」 : 「 win-ads-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" : false 、 "ADFSSConfigFilePath" : "C:\ADFS_中繼 資料 \abc.xml 、 "SCConfigFilePath" : null 、 "IsApRestiMFAEnabled" : true 、 "IsClimFAEnabled" : false 、 「 ADFSHostName 」 : 「 win-ads-sc49.winscedom2.com 」 }

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 保留隨時變更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。