多要素認証（MFA）

SnapCenter software

NetApp
November 06, 2025

目次

多要素認証（MFA）

多要素認証（MFA）の管理

Active Directoryフェデレーション サービス（AD FS）サーバとSnapCenter Serverで多要素認証（MFA）機能を管理できます。

多要素認証（MFA）の有効化

SnapCenter ServerのMFA機能は、PowerShellコマンドを使用して有効にできます。

タスク概要

- 同じAD FSに他のアプリケーションが設定されている場合、SnapCenterはSSOベースのログインをサポートします。セキュリティ上の理由から、一部のAD FS構成では、AD FSセッションの永続化に応じて、SnapCenterでユーザ認証が必要になる場合があります。
- コマンドレットで使用できるパラメータとその説明に関する情報は、以下を実行することで取得できます。 `Get-Help command_name` 。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

開始する前に

- Windows Active Directoryフェデレーション サービス（AD FS）が、それぞれのドメインで稼働している必要があります。
- Azure MFAやCisco Duoなど、AD FSでサポートされている多要素認証サービスが必要です。
- SnapCenter ServerとAD FSサーバのタイムスタンプは、タイムゾーンに関係なく同じにする必要があります。
- SnapCenter Server用に、承認済みのCA証明書を取得して設定します。

  CA証明書は、次の理由で必須です。

  - 自己署名証明書はノード レベルで一意であるため、ADFSとF5間の通信が切断されないようにします。
  - スタンドアロン構成または高可用性構成でのアップグレード、修復、ディザスタ リカバリ（DR）の実行中に自己署名証明書が再作成されないようにして、MFAの再設定を回避します。
  - IP-FQDNの解決を保証します。

    CA証明書の詳細については、"CA証明書CSRファイルの生成" 。

手順

1. Active Directoryフェデレーション サービス（AD FS）のホストに接続します。
2. AD FSフェデレーションメタデータファイルを以下からダウンロードします。"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml" です。
3. ダウンロードしたファイルをSnapCenter Serverにコピーして、MFA機能を有効にします。
4. PowerShellを使用して、SnapCenter管理者ユーザとしてSnapCenter Serverにログインします。

5. PowerShell セッションで、*New-SmMultifactorAuthenticationMetadata -path* コマンドレットを使用してSnapCenter MFA メタデータ ファイルを生成します。

   pathパラメータには、SnapCenter ServerのホストにMFAメタデータ ファイルを保存するためのパスを指定します。

6. 生成されたファイルをAD FSのホストにコピーし、SnapCenterをクライアント エンティティとして設定します。
7. SnapCenter ServerのMFAを有効にするには、 `Set-SmMultiFactorAuthentication`コマンドレット。
8. （オプション）MFAの構成ステータスと設定を確認するには、 `Get-SmMultiFactorAuthentication`コマンドレット。
9. Microsoft管理コンソール（MMC）に移動し、次の手順を実行します。
   a. ファイル > *スナップインの追加と削除*をクリックします。
   b. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
   c. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
   d. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
   e. SnapCenterにバインドされた CA 証明書を右クリックし、[すべてのタスク] > [秘密キーの管理] を選択します。
   f. アクセス許可ウィザードで、次の手順を実行します。
      i. *[追加]*をクリックします。
      ii. *場所*をクリックし、該当するホスト（階層の最上位）を選択します。
      iii. *場所*ポップアップウィンドウで*OK*をクリックします。
      iv. オブジェクト名フィールドに「IIS_IUSRS」と入力し、[名前の確認] をクリックして、[OK] をクリックします。

          チェックが成功した場合は、[**OK**] をクリックします。

10. AD FSホストでAD FS管理ウィザードを開き、次の手順を実行します。
    a. 証明書利用者信頼 > 証明書利用者信頼の追加 > 開始 を右クリック。
    b. 2 番目のオプションを選択し、 SnapCenter MFA メタデータ ファイルを参照して、[次へ] をクリックします。
    c. 表示名を指定して、[次へ] をクリックします。
    d. 必要に応じてアクセス制御ポリシーを選択し、「次へ」をクリックします。
    e. 次のタブの設定をデフォルトに設定します。
    f. *[完了]*をクリックします。

       SnapCenterが、指定した表示名の証明書利用者として反映されます。

11. 名前を選択し、次の手順を実行します。
    a. *クレーム発行ポリシーの編集*をクリックします。

b. *ルールの追加*をクリックし、*次へ*をクリックします。

c. 要求規則の名前を指定します。

d. 属性ストアとして*Active Directory*を選択します。

e. 属性として*User-Principal-Name*を選択し、出力クレームの種類として*Name-ID*を選択します。

f. *[完了]*をクリックします。

12. ADFSサーバで、次のPowerShellコマンドを実行します。

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

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

13. 次の手順を実行して、メタデータがインポートされたことを確認します。

a. 証明書利用者信頼を右クリックし、[プロパティ] を選択します。

b. [エンドポイント]、[識別子]、[署名]フィールドに値が入力されていることを確認します。

14. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenterのMFA機能は、REST APIを使用して有効にすることもできます。

トラブルシューティング情報については、 "複数のタブで同時にログインしようとすると、MFAエラーが表示されます" 。

AD FS MFAメタデータの更新

アップグレード、CA証明書の更新、DRなど、AD FSサーバに何らかの変更があった場合は、SnapCenterでAD FS MFAメタデータを更新する必要があります。

手順

1. AD FSフェデレーションメタデータファイルを以下からダウンロードします。"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. ダウンロードしたファイルをSnapCenter Serverにコピーして、MFAの設定を更新します。
3. 次のコマンドレットを実行して、SnapCenterでAD FSメタデータを更新します。

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

4. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFAメタデータの更新

修復、CA証明書の更新、DRなど、ADFSサーバに何らかの変更があった場合は、AD FSでSnapCenter MFAメタデータを更新する必要があります。

手順

1. AD FSホストでAD FS管理ウィザードを開き、次の手順を実行します。
   a. *証明書利用者信頼*を選択します。
   b. SnapCenter用に作成された証明書利用者信頼を右クリックし、[削除] を選択します。

      証明書利用者信頼のユーザ定義名が表示されます。

   c. 多要素認証（MFA）を有効にします。

      見る"多要素認証を有効にする" 。
2. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

多要素認証（**MFA**）の無効化

手順

1. MFAを無効にし、MFAが有効になったときに作成された構成ファイルをクリーンアップします。 `Set-SmMultiFactorAuthentication`コマンドレット。
2. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

REST API、PowerShell、SCCLIを使用した多要素認証（MFA）の管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIでサポートされます。MFA は AD FS ID マネージャーを通じてサポートされます。GUI、REST API、PowerShell、SCCLIを使用して、MFAの有効化、MFAの無効化、およびMFAの設定を行うことができます。

AD FSのOAuth / OIDCとしてのセットアップ

Windows GUIウィザードを使用して**AD FS**を構成する

1. サーバー マネージャー ダッシュボード > ツール > **ADFS** 管理 に移動します。
2. **ADFS** > アプリケーション グループ に移動します。
   a. アプリケーション グループ を右クリックします。
   b. アプリケーション グループの追加 を選択し、アプリケーション名 を入力します。
   c. *サーバーアプリケーション*を選択します。
   d. *次へ*をクリックします。
3. *クライアント識別子*をコピーします。

   これがクライアントIDです。..[リダイレクトURI]にコールバックURL（SnapCenter ServerのURL）を追加します。..*次へ*をクリックします。

4. *共有シークレットの生成*を選択します。

シークレット値をコピーします。これがクライアントのシークレットです。..*次へ*をクリックします。

5. *概要*ページで*次へ*をクリックします。
   a. *完了*ページで*閉じる*をクリックします。
6. 新しく追加された*アプリケーション グループ*を右クリックし、*プロパティ*を選択します。
7. アプリのプロパティから*アプリケーションの追加*を選択します。
8. *アプリケーションを追加*をクリックします。

   Web APIを選択し、[次へ]をクリックします。

9. [Web APIの構成]ページで、SnapCenter ServerのURLと前の手順で作成したクライアントIDを[識別子]セクションに入力します。
   a. *[追加]*をクリックします。
   b. *次へ*をクリックします。
10. *アクセス制御ポリシーの選択*ページで、要件に基づいて制御ポリシーを選択し (たとえば、すべてのユーザーを許可し、MFA を要求する)、*次へ*をクリックします。
11. *アプリケーションの権限の構成*ページでは、デフォルトで openid がスコープとして選択されているので、*次へ*をクリックします。
12. *概要*ページで*次へ*をクリックします。

    *完了*ページで*閉じる*をクリックします。

13. サンプル アプリケーションのプロパティ ページで、**OK** をクリックします。
14. 承認サーバ（AD FS）によって発行され、リソースによって消費されることを意図したJWTトークン。

    このトークンの「aud」つまりオーディエンス要求は、リソースまたはWeb APIの識別子と一致している必要があります。

15. 選択したWebAPIを編集し、コールバックURL（SnapCenter ServerのURL）とクライアント識別子が正しく追加されていることを確認します。

    ユーザ名を要求として提供するようにOpenID Connectを設定します。

16. サーバー マネージャーの右上にある ツール メニューの下にある **AD FS** 管理 ツールを開きます。
    a. 左側のサイドバーから*アプリケーション グループ* フォルダを選択します。
    b. Web API を選択し、[編集] をクリックします。
    c. [発行変換規則]タブに移動します。
17. *ルールの追加*をクリックします。
    a. クレーム ルール テンプレートのドロップダウンで、**LDAP** 属性をクレームとして送信 を選択します。
    b. *次へ*をクリックします。
18. *クレームルール*の名前を入力します。
    a. 属性ストアのドロップダウンで*Active Directory*を選択します。

b. **LDAP** 属性 ドロップダウンで **User-Principal-Name** を選択し、送信クレーム タイプ ドロップダウンで **UPN** を選択します。

c. *[完了]*をクリックします。

PowerShellコマンドを使用したアプリケーション グループの作成

PowerShellコマンドを使用して、アプリケーション グループ、Web APIを作成し、スコープと要求を追加できます。これらのコマンドは、自動スクリプト形式で使用できます。詳細については、<KB 記事へのリンク>を参照してください。

1. 次のコマンドを使用して、AD FSに新しいアプリケーション グループを作成します。

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

`ClientRoleIdentifier`アプリケーショングループの名前

`redirectURL`承認後のリダイレクト用の有効なURL

2. AD FSサーバ アプリケーションを作成し、クライアント シークレットを生成します。

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

3. ADFS Web APIアプリケーションを作成し、使用するポリシー名を設定します。

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

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

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

4. クライアントIDとクライアント シークレットは1回しか表示されないため、次のコマンドの出力から取得します。

```
"client_id = $identifier"

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

5. AD FSアプリケーションにallatclaims権限とopenid権限を付与します。

```
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. 変換規則ファイルを書き出します。

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

7. Web APIアプリケーションに名前を付け、外部ファイルを使用してその発行変換規則を定義します。

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

アクセス トークンの有効期限の更新

PowerShellコマンドを使用して、アクセス トークンの有効期限を更新できます。

このタスクについて

- アクセス トークンは、ユーザ、クライアント、およびリソースの特定の組み合わせに対してのみ使用できます。アクセス トークンは無効にすることはできず、期限切れになるまで有効です。
- デフォルトでは、アクセス トークンの有効期間は60分です。最小値の有効期間でも十分な長さになるよう設定されています。現在進行中のビジネス クリティカルなジョブが妨げられないように、十分な値を指定する必要があります。

ステップ

アプリケーション グループWebAPIのアクセス トークンの有効期限を更新するには、AD FSサーバで次のコマンドを使用します。

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

AD FSからのBearerトークンの取得

RESTクライアント（Postmanなど）で以下のパラメータを入力する必要があります。RESTクライアントからユーザ クレデンシャルを入力するように求められます。さらに、ベアラー トークンを取得するには、2 要素認証 (ユーザーが所有している情報と、ユーザーが何者であるか) を入力する必要があります。

+ ベアラー トークンの有効期間はアプリケーションごとに AD FS サーバーから構成可能で、デフォルトの有効期間は 60 分です。

フィールド	Value
助成金の種類	Authorization Code
Callback URL	コールバックURLがない場合は、アプリケーションのベースURLを入力します。
Auth URL	[adfsドメイン名]/adfs/oauth2/authorize
Access token URL	[adfsドメイン名]/adfs/oauth2/トークン
クライアントID	AD FSクライアントIDを入力します。
Client secret	AD FSクライアント シークレットを入力します。
Scope	OpenID
クライアント認証	Send as Basic AUTH Header
リソース	詳細オプション タブで、コールバック URL と同じ値を持つリソース フィールドを追加します。この値は、JWT トークンの "aud" 値として提供されます。

PowerShell、SCCLI、REST APIを使用したSnapCenter ServerでのMFAの設定

PowerShell、SCCLI、およびREST APIを使用して、SnapCenter ServerでMFAを設定できます。

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレット（Open-SmConnection）を「AccessToken」という追加のフィールドで拡張し、Bearerトークンを使用してユーザを認証します。

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

上記のコマンドレットを実行すると、それぞれのユーザがSnapCenterコマンドレットを実行できるようにセッションが作成されます。

SnapCenter MFA REST API認証

REST API クライアント (Postman や swagger など) で *Authorization=Bearer <access token>* の形式のベアラ

ー トークンを使用し、ヘッダーにユーザーの RoleName を指定して、 SnapCenterから正常な応答を取得します。

MFA REST APIのワークフロー

MFAがAD FSで設定されている場合、REST APIを使用してSnapCenterアプリケーションにアクセスするには、アクセス（Bearer）トークンを使用して認証する必要があります。

このタスクについて

- Postman、Swagger UI、FireCampなど、任意のRESTクライアントを使用できます。
- アクセス トークンを取得し、それを使用して以降の要求（SnapCenter REST API）を認証し、任意の処理を実行します。

手順

AD FS MFA 経由で認証するには

1. AD FSエンドポイントを呼び出してアクセス トークンを取得するようにRESTクライアントを設定します。

   ボタンを押してアプリケーションのアクセス トークンを取得すると、AD FS SSOページにリダイレクトされます。そのページでADクレデンシャルを入力してMFAで認証する必要があります。1.AD FS SSOページで、[Username]テキスト ボックスにユーザ名または電子メールを入力します。

   + ユーザー名は、user@domain または domain\user の形式にする必要があります。

2. [Password]テキスト ボックスにパスワードを入力します。
3. *ログイン*をクリックします。
4. サインイン オプション セクションから認証オプションを選択し、認証します (構成によって異なります)。
   - プッシュ: 携帯電話に送信されるプッシュ通知を承認します。
   - QRコード: AUTH Pointモバイルアプリを使用してQRコードをスキャンし、アプリに表示される確認コードを入力します。
   - ワンタイム パスワード: トークンのワンタイム パスワードを入力します。
5. 認証が成功すると、アクセス、ID、およびリフレッシュ トークンを含むポップアップが表示されます。

   アクセス トークンをコピーし、SnapCenter REST APIで使用して操作を実行します。

6. REST APIのヘッダー セクションでアクセス トークンとロール名を渡す必要があります。
7. AD FSから取得したこのアクセス トークンをSnapCenterが検証します。

   有効なトークンである場合、SnapCenterはそのトークンをデコードし、ユーザ名を取得します。

8. SnapCenterがユーザ名とロール名を使用して、API実行のためにユーザ認証を行います。

   認証に成功した場合、SnapCenterは結果を返します。失敗した場合は、エラー メッセージが表示されます。

REST API、CLI、GUIのSnapCenter MFA機能の有効化または無効化

GUI

手順

1. SnapCenter管理者としてSnapCenter Serverにログインします。
2. 設定 > グローバル設定 > *多要素認証(MFA)設定*をクリックします
3. インターフェイス（GUI / RST API / CLI）を選択してMFAログインを有効または無効にします。

PowerShell インターフェース

手順

1. GUI、REST API、PowerShell、SCCLIのMFAを有効にするためのPowerShellコマンドまたはCLIコマンドを実行します。

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

   pathパラメータには、AD FS MFAメタデータxmlファイルの場所を指定します。

   SnapCenter GUI、REST API、PowerShell、およびSCCLIが、指定したAD FSメタデータ ファイル パスを使用して設定され、MFAが有効になります。

2. MFAの構成ステータスと設定を確認するには、 `Get-SmMultiFactorAuthentication`コマンドレット。

SCCLIインターフェース

手順

1. ```
   # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
   -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
   "C:\ADFS_metadata\abc.xml"
   ```
2. ```
   # sccli Get-SmMultiFactorAuthentication
   ```

REST API

1. GUI、REST API、PowerShell、SCCLIのMFAを有効にするには、次のPOST APIを実行します。

パラメータ	Value
要求のURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
要求の本文	{ "IsGuiMFAEnabled": false、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }

応答の本文	{ "MFAConfiguration": { "IsGuiMFAEnabled": false、 "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. 次のAPIを使用して、MFAのステータスと設定を確認します。

パラメータ	Value
要求のURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	Get
応答の本文	{ "MFAConfiguration": { "IsGuiMFAEnabled": false、 "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

著作権に関する情報

商標に関する情報