多要素認証（MFA）

SnapCenter Software 6.0

NetApp
September 23, 2024

目次

多要素認証（MFA）

多要素認証（MFA）を管理します。

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

多要素認証（MFA）を有効にする

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

タスクの内容

- 同じAD FSで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。一部のAD FS構成では、AD FSセッションの持続性に応じて、セキュリティ上の理由から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は、を実行して確認できます `Get-Help command_name`。または、を参照することもできます "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、Cisco Duoなど、AD FSがサポートする多要素認証サービスが必要です。
- SnapCenterサーバと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サーバ用に許可された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-F5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ハイアベイラビリティ構成でのアップグレード、修復、またはディザスタリカバリ（DR）中に自己署名証明書が再作成されないようにすることで、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、を参照してください "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）ホストに接続します。
2. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。
3. ダウンロードしたファイルをSnapCenterサーバにコピーして、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サーバにログインします。
5. PowerShellセッションを使用して、_New-SmMultifactorAuthenticationMetadata-path_cmdlet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サーバホストにMFAメタデータファイルを保存するパスを指定します。

6. 生成されたファイルをAD FSホストにコピーして、SnapCenterをクライアントエンティティとして設定します。
7. コマンドレットを使用して、SnapCenterサーバのMFAを有効にします `Set-SmMultiFactorAuthentication` 。
8. （オプション）コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。
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、 [**Certificates**] を選択し、 [**Add**] をクリックします。
   c. [証明書] スナップインウィンドウで、 [**Computer account**] 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］の順にクリックします。
   e. SnapCenter にバインドされているCA証明書を右クリックし、すべてのタスク>*秘密鍵の管理*を選択します。
   f. Permissions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。

      チェックが正常に終了したら、* 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（Rel証明 書利用者信頼）]>[証明書利用者信頼の追加（Add Rel証明 書利用者信頼）]>[開始
    b. 2番目のオプションを選択してSnapCenter MFAメタデータファイルを参照し、*次へ*をクリックします。
    c. 表示名を指定し、*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、*[Next]*をクリックします。
    e. 次のタブでデフォルトに設定を選択します。
    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るようになりました。
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. クレームルール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、発信クレームタイプとして「 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. メタデータがインポートされたことを確認するには、次の手順を実行します。

a. 証明書利用者信頼を右クリックし、* Properties *を選択します。

b. [Endpoints]、[Identifiers]、および[Signature]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、を参照してください "複数のタブで同時にログインを試行すると、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サーバで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. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。"

2. ダウンロードしたファイルをSnapCenterサーバにコピーして、MFA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

ADFSサーバで修復、CA証明書の更新、DRなど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]をクリックします。
   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*をクリックします。

      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。

      を参照して "多要素認証を有効にします"

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**）を無効にする

手順

1. MFAを無効にし、コマンドレットを使用してMFAを有効にし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` 。
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を使用して多要素認証（MFA）を管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIからサポートされます。MFAは、AD FSアイデンティティマネージャを介し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をOAuth/OIDCとしてセットアップします

- Windows GUIウィザードを使用してAD FSを構成します*
  1. Server Manager Dashboard **>** Tools **>** ADFS Management *に移動します。
  2. **>**[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. を選択し、[アプリケーション名]*と入力します。
     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. コピー*クライアントID *。

     これはクライアントIDです。..リダイレクトURLにコールバックURL（SnapCenterサーバURL）を追加します。..「 * 次へ * 」をクリックします。

4. [Generate shared secret]*を選択します。

   シークレット値をコピーします。これはクライアントの秘密です。..「 * 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. 新しく追加した*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. [アプリケーションのプロパティ]から*[アプリケーションの追加]*を選択します。

8. [アプリケーションの追加]*をクリックします。

   [Web API]を選択し、*[Next]*をクリックします。

9. [Web APIの構成]ページで、前の手順で作成したSnapCenterサーバのURLとクライアント識別子を[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. [Choose Access Control Policy]ページで、要件に基づいて制御ポリシーを選択し（[Permit Everyone and Require MFA]など）、*[Next]*をクリックします。

11. [アプリケーション権限の設定]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おり、*[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. 承認サーバー(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」または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サーバ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。

    ユーザー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の右上にある* Tools メニューの下にある AD FS Management *ツールを開きます。

    a. 左側のサイドバーから* Application Groups *フォルダを選択します。

    b. Web APIを選択し、* edit *をクリックします。

    c. [発行トランスフォームルール]タブに移動します

17. [* ルールの追加 *] をクリックします。

    a. [Claim rule template]ドロップダウンで、*[Send LDAP Attributes as Claims]*を選択します。

    b. 「 * 次へ * 」をクリックします。

18. [Claim rule]*の名前を入力します。

a. [属性ストア]ドロップダウンで*[Active Directory]*を選択します。

b. [LDAP Attribute]ドロップダウンで*を選択し、**[O*utgoing Claim Type]***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コマンドを使用してアプリケーショングループを作成します

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、<link to KB article>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` 許可後のリダイレクションの有効な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. 変換ルール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トランスフォームルールを定義します。

```
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を更新します

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

- このタスクについて *
- アクセストークンは、ユーザー、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、有効期限が切れるまで有効です。
- デフォルトでは、アクセストークンの有効期限は60分です。この最小限の有効期限は十分であり、拡張されています。ビジネスクリティカルなジョブが継続的に発生しないように、十分な価値を提供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Bearerトークンを取得します

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、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、第2要素認証(あなたが持っているも

のとあなたがいるもの)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サーバから設定できます。デフォルトの有効期間は60分です。

フィールド	値
付与タイプ	承認コード
コールバック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。
認証URL	[ADFS-domain-name]/ADFS/OAuth2/authorize
アクセストークンURL	[ADFS-domain-name]/ADFS/OAuth2/token
クライアントID	AD FSクライアントIDを入力します
クライアントシークレット	AD FSクライアントシークレットを入力します
適用範囲	OpenID
クライアント認証	基本認証ヘッダーとして送信します
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トークンでは「AUD」値として表示されます。

PowerShell、SCCLI、REST APIを使用してSnapCenterサーバでMFAを設定します

SnapCenter Serverでは、PowerShell、SCCLI、およびREST APIを使用して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」というもう1つのフィールドで拡張し、ベアラー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 <access token>クライアント(Postmanやswaggerなど)でBearerトークンを_Authorization = Bearer _の形式で使用し、ヘッダーにユーザRoleNameを指定すると、SnapCenterからの応答が成功します。

MFA REST API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、あらゆる処理を実行します。
- 手順 *
- AD FS MFAを介して認証する場合*

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、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。

+ユーザ名は、user@domainまたはdomain\userの形式で指定する必要があります。

1. [パスワード]テキストボックスにパスワードを入力します。
2. *ログイン*をクリックします。
3. [サインインオプション]*セクションで、認証オプションを選択し、（設定に応じて）認証します。
   - プッシュ：電話機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認証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。
4. 認証が成功すると、Access、ID、およびRefresh Tokenを含むポップアップが開きます。

   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。

5. REST APIでは、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。
6. SnapCenterは、AD FSからこのアクセストークンを検証します。

   有効なトークンである場合、SnapCenterはそれをデコードし、ユーザー名を取得します。

7. SnapCenterは、ユーザ名とロール名を使用して、API実行のためにユーザを認証します。

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

REST API、CLI、GUIのSnapCenter MFA機能を有効または無効にします

- GUI *
- 手順 *
  1. SnapCenter管理者としてSnapCenterサーバにログインします。
  2. >[グローバル設定]>[MultiFactorAuthentication（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インターフェイス*
- 手順 *
  1. PowerShellまたはCLIコマンドを実行して、GUI、REST API、PowerShell、SCCLIのMFAを有効にします。

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

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

  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たSnapCenter GUI、REST API、PowerShell、およびSCCLIのMFAを有効にします。

  1. コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。
- SCCLIインターフェイス*
- 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でMFAを有効にするには、次のPOST APIを実行します。

パラメータ	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
リクエストボディ	{"IsGuiMFAEnabled"：false 、"IsRestApiMFAEnabled"：true 、"IsCliMFAEnabled"：false 、"ADFSConfigFilePath" ："C:\\ADFS_METADATA\\abc.xml"}

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

2. 以下のAPIを使用してMFA構成のステータスと設定を確認します。

パラメータ	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	取得
応答本文	{"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