Authentification multifacteur (MFA)

SnapCenter software

NetApp
November 06, 2025

Sommaire

Authentification multifacteur (MFA)

Gérer l’authentification multifacteur (MFA)

Vous pouvez gérer la fonctionnalité d’authentification multifacteur (MFA) dans le serveur Active Directory Federation Service (AD FS) et le serveur SnapCenter .

Activer l’authentification multifacteur (MFA)

Vous pouvez activer la fonctionnalité MFA pour SnapCenter Server à l’aide des commandes PowerShell.

À propos de cette tâche

- SnapCenter prend en charge les connexions basées sur SSO lorsque d’autres applications sont configurées dans le même AD FS. Dans certaines configurations AD FS, SnapCenter peut nécessiter une authentification utilisateur pour des raisons de sécurité en fonction de la persistance de la session AD FS.
- Les informations concernant les paramètres pouvant être utilisés avec l’applet de commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name` . Alternativement, vous pouvez également voir "Guide de référence de l’applet de commande du logiciel SnapCenter" .

Avant de commencer

- Le service de fédération Windows Active Directory (AD FS) doit être opérationnel dans le domaine concerné.
- Vous devez disposer d’un service d’authentification multifacteur pris en charge par AD FS, tel qu’Azure MFA, Cisco Duo, etc.
- L’horodatage du serveur SnapCenter et AD FS doit être le même quel que soit le fuseau horaire.
- Procurez-vous et configurez le certificat CA autorisé pour SnapCenter Server.

  Le certificat CA est obligatoire pour les raisons suivantes :

  - Garantit que les communications ADFS-F5 ne sont pas interrompues car les certificats auto-signés sont uniques au niveau du nœud.
  - Garantit que lors de la mise à niveau, de la réparation ou de la reprise après sinistre (DR) dans une configuration autonome ou à haute disponibilité, le certificat auto-signé n’est pas recréé, évitant ainsi la reconfiguration MFA.
  - Assure les résolutions IP-FQDN.

    Pour plus d’informations sur le certificat CA, voir"Générer le fichier CSR du certificat CA" .

Étapes

1. Connectez-vous à l’hôte Active Directory Federation Services (AD FS).
2. Téléchargez le fichier de métadonnées de la fédération AD FS à partir de"https://<host Nom de domaine complet>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiez le fichier téléchargé sur SnapCenter Server pour activer la fonction MFA.
4. Connectez-vous à SnapCenter Server en tant qu’utilisateur administrateur SnapCenter via PowerShell.
5. À l’aide de la session PowerShell, générez le fichier de métadonnées SnapCenter MFA à l’aide de l’applet de commande *New-SmMultifactorAuthenticationMetadata -path*.

Le paramètre path spécifie le chemin d'accès pour enregistrer le fichier de métadonnées MFA dans l'hôte SnapCenter Server.

6. Copiez le fichier généré sur l'hôte AD FS pour configurer SnapCenter comme entité client.
7. Activer MFA pour SnapCenter Server à l'aide de l' `Set-SmMultiFactorAuthentication` applet de commande.
8. (Facultatif) Vérifiez l'état et les paramètres de configuration MFA à l'aide de `Get-SmMultiFactorAuthentication` applet de commande.
9. Accédez à la console de gestion Microsoft (MMC) et effectuez les étapes suivantes :
   a. Cliquez sur **Fichier** > **Ajouter/Supprimer un composant logiciel enfichable**.
   b. Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
   c. Dans la fenêtre du composant logiciel enfichable Certificats, sélectionnez l'option **Compte d'ordinateur**, puis cliquez sur **Terminer**.
   d. Cliquez sur **Racine de la console** > **Certificats – Ordinateur local** > **Personnel** > **Certificats**.
   e. Cliquez avec le bouton droit sur le certificat CA lié à SnapCenter , puis sélectionnez **Toutes les tâches** > **Gérer les clés privées**.
   f. Dans l'assistant d'autorisations, procédez comme suit :
      i. Cliquez sur **Ajouter**.
      ii. Cliquez sur **Emplacements** et sélectionnez l'hôte concerné (en haut de la hiérarchie).
      iii. Cliquez sur **OK** dans la fenêtre contextuelle **Emplacements**.
      iv. Dans le champ du nom de l'objet, saisissez « IIS_IUSRS » et cliquez sur **Vérifier les noms**, puis sur **OK**.

      Si la vérification est réussie, cliquez sur **OK**.
10. Dans l'hôte AD FS, ouvrez l'assistant de gestion AD FS et effectuez les étapes suivantes :
    a. Cliquez avec le bouton droit sur **Approbations de partie de confiance** > **Ajouter une approbation de partie de confiance** > **Démarrer**.
    b. Sélectionnez la deuxième option et parcourez le fichier de métadonnées SnapCenter MFA et cliquez sur **Suivant**.
    c. Spécifiez un nom d'affichage et cliquez sur **Suivant**.
    d. Choisissez une politique de contrôle d'accès selon vos besoins et cliquez sur **Suivant**.
    e. Sélectionnez les paramètres par défaut dans l'onglet suivant.
    f. Cliquez sur **Terminer**.

    SnapCenter est désormais reflété comme une partie de confiance avec le nom d'affichage fourni.
11. Sélectionnez le nom et effectuez les étapes suivantes :
    a. Cliquez sur **Modifier la politique d'émission de réclamation**.
    b. Cliquez sur **Ajouter une règle** et cliquez sur **Suivant**.
    c. Spécifiez un nom pour la règle de revendication.
    d. Sélectionnez **Active Directory** comme magasin d'attributs.

e. Sélectionnez l'attribut **User-Principal-Name** et le type de réclamation sortant comme **Name-ID**.

f. Cliquez sur **Terminer**.

12. Exécutez les commandes PowerShell suivantes sur le serveur ADFS.

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

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

13. Effectuez les étapes suivantes pour confirmer que les métadonnées ont été importées avec succès.

    a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance et sélectionnez **Propriétés**.

    b. Assurez-vous que les champs Points de terminaison, Identifiants et Signature sont renseignés.

14. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

La fonctionnalité SnapCenter MFA peut également être activée à l'aide des API REST.

Pour obtenir des informations de dépannage, consultez "Les tentatives de connexion simultanées dans plusieurs onglets affichent une erreur MFA" .

Mettre à jour les métadonnées AD FS MFA

Vous devez mettre à jour les métadonnées AD FS MFA dans SnapCenter chaque fois qu'une modification est apportée au serveur AD FS, comme une mise à niveau, un renouvellement de certificat d'autorité de certification, une reprise après sinistre, etc.

Étapes

1. Téléchargez le fichier de métadonnées de la fédération AD FS à partir de"https://<host Nom de domaine complet>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copiez le fichier téléchargé sur SnapCenter Server pour mettre à jour la configuration MFA.
3. Mettez à jour les métadonnées AD FS dans SnapCenter en exécutant l'applet de commande suivante :

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

4. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

Mettre à jour les métadonnées SnapCenter MFA

Vous devez mettre à jour les métadonnées SnapCenter MFA dans AD FS chaque fois qu'une modification est apportée au serveur ADFS, telle qu'une réparation, un renouvellement de certificat CA, une reprise après sinistre, etc.

Étapes

1. Dans l'hôte AD FS, ouvrez l'assistant de gestion AD FS et effectuez les étapes suivantes :

    a. Sélectionnez **Fiducies de partie de confiance**.

    b. Cliquez avec le bouton droit sur la partie de confiance qui a été créée pour SnapCenter et sélectionnez **Supprimer**.

Le nom défini par l'utilisateur de la partie de confiance sera affiché.

c. Activer l'authentification multifacteur (MFA).

Voir "Activer l'authentification multifacteur" .

2. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

Désactiver l'authentification multifacteur (MFA)

Étapes

1. Désactivez MFA et nettoyez les fichiers de configuration qui ont été créés lorsque MFA a été activé à l'aide de l' `Set-SmMultiFactorAuthentication` applet de commande.
2. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

Gérer l'authentification multifacteur (MFA) à l'aide de l'API Rest, de PowerShell et de SCCLI

La connexion MFA est prise en charge à partir du navigateur, de l'API REST, de PowerShell et de SCCLI. L'authentification multifacteur est prise en charge via un gestionnaire d'identité AD FS. Vous pouvez activer MFA, désactiver MFA et configurer MFA à partir de l'interface graphique, de l'API REST, de PowerShell et de SCCLI.

Configurer AD FS comme OAuth/OIDC

Configurer AD FS à l'aide de l'assistant d'interface graphique Windows

1. Accédez à **Tableau de bord du gestionnaire de serveur** > **Outils** > **Gestion ADFS**.
2. Accédez à **ADFS** > **Groupes d'applications**.
   a. Faites un clic droit sur **Groupes d'applications**.
   b. Sélectionnez **Ajouter un groupe d'applications** et saisissez **Nom de l'application**.
   c. Sélectionnez **Application serveur**.
   d. Cliquez sur **Suivant**.
3. Copier **Identifiant client**.

   Il s'agit de l'ID client. .. Ajoutez l'URL de rappel (URL du serveur SnapCenter) dans l'URL de redirection. .. Cliquez sur **Suivant**.

4. Sélectionnez **Générer un secret partagé**.

   Copiez la valeur secrète. C'est le secret du client. .. Cliquez sur **Suivant**.

5. Sur la page **Résumé**, cliquez sur **Suivant**.
   a. Sur la page **Terminé**, cliquez sur **Fermer**.
6. Cliquez avec le bouton droit sur le **Groupe d'applications** nouvellement ajouté et sélectionnez **Propriétés**.

7. Sélectionnez **Ajouter une application** dans les propriétés de l'application.
8. Cliquez sur **Ajouter une application**.

   Sélectionnez API Web et cliquez sur **Suivant**.

9. Sur la page Configurer l'API Web, saisissez l'URL du serveur SnapCenter et l'identifiant client créé à l'étape précédente dans la section Identificateur.
   a. Cliquez sur **Ajouter**.
   b. Cliquez sur **Suivant**.
10. Sur la page **Choisir la politique de contrôle d'accès**, sélectionnez la politique de contrôle en fonction de vos besoins (par exemple, Autoriser tout le monde et exiger l'authentification multifacteur) et cliquez sur **Suivant**.
11. Sur la page **Configurer l'autorisation d'application**, par défaut, openid est sélectionné comme étendue, cliquez sur **Suivant**.
12. Sur la page **Résumé**, cliquez sur **Suivant**.

    Sur la page **Terminé**, cliquez sur **Fermer**.

13. Sur la page **Propriétés de l'exemple d'application**, cliquez sur **OK**.
14. Jeton JWT émis par un serveur d'autorisation (AD FS) et destiné à être consommé par la ressource.

    La revendication « aud » ou d'audience de ce jeton doit correspondre à l'identifiant de la ressource ou de l'API Web.

15. Modifiez l'API Web sélectionnée et vérifiez que l'URL de rappel (URL du serveur SnapCenter) et l'identifiant client ont été ajoutés correctement.

    Configurez OpenID Connect pour fournir un nom d'utilisateur en tant que revendications.

16. Ouvrez l'outil **Gestion AD FS** situé sous le menu **Outils** en haut à droite du Gestionnaire de serveur.
    a. Sélectionnez le dossier **Groupes d'applications** dans la barre latérale gauche.
    b. Sélectionnez l'API Web et cliquez sur **MODIFIER**.
    c. Onglet Règles de transformation d'émission
17. Cliquez sur **Ajouter une règle**.
    a. Sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste déroulante Modèle de règle de revendication.
    b. Cliquez sur **Suivant**.
18. Saisissez le nom de la **règle de réclamation**.
    a. Sélectionnez **Active Directory** dans la liste déroulante Magasin d'attributs.
    b. Sélectionnez **Nom d'utilisateur principal** dans la liste déroulante **Attribut LDAP** et **UPN** dans la liste déroulante **Type de réclamation sortante**.
    c. Cliquez sur **Terminer**.

Créer un groupe d'applications à l'aide de commandes PowerShell

Vous pouvez créer le groupe d'applications, l'API Web et ajouter l'étendue et les revendications à l'aide des commandes PowerShell. Ces commandes sont disponibles au format de script automatisé. Pour plus

d'informations, voir <lien vers l'article de la base de connaissances>.

1. Créez le nouveau groupe d'applications dans AD FS à l'aide de la commande suivante.

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

   `ClientRoleIdentifier`nom de votre groupe d'applications

   `redirectURL`URL valide pour la redirection après autorisation

2. Créez l'application serveur AD FS et générez le secret client.

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

3. Créez l'application API Web ADFS et configurez le nom de la stratégie qu'elle doit utiliser.

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

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

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

4. Obtenez l'ID client et le secret client à partir de la sortie des commandes suivantes, car ils ne sont affichés qu'une seule fois.

   ```
   "client_id = $identifier"

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

5. Accordez à l'application AD FS les autorisations allatclaims et openid.

   ```
   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. Écrivez le fichier de règles de transformation.

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

7. Nommez l'application API Web et définissez ses règles de transformation d'émission à l'aide d'un fichier externe.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Mettre à jour le délai d'expiration du jeton d'accès

Vous pouvez mettre à jour le délai d'expiration du jeton d'accès à l'aide de la commande PowerShell.

À propos de cette tâche

- Un jeton d'accès ne peut être utilisé que pour une combinaison spécifique d'utilisateur, de client et de ressource. Les jetons d'accès ne peuvent pas être révoqués et sont valables jusqu'à leur expiration.
- Par défaut, le délai d'expiration d'un jeton d'accès est de 60 minutes. Ce délai d'expiration minimal est suffisant et évolutif. Vous devez fournir une valeur suffisante pour éviter toute tâche critique pour l'entreprise en cours.

Étape

Pour mettre à jour le délai d'expiration du jeton d'accès pour un groupe d'applications WebApi, utilisez la commande suivante sur le serveur AD FS.

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

Récupérez le jeton du porteur depuis AD FS

Vous devez remplir les paramètres mentionnés ci-dessous dans n'importe quel client REST (comme Postman) et il vous invite à remplir les informations d'identification de l'utilisateur. De plus, vous devez saisir l'authentification à deux facteurs (quelque chose que vous possédez et quelque chose que vous êtes) pour obtenir le jeton du porteur.

+ La validité du jeton porteur est configurable depuis le serveur AD FS par application et la période de validité par défaut est de 60 minutes.

Champ	Valeur
Type de subvention	Code d'autorisation

URL de rappel	Saisissez l'URL de base de votre application si vous n'avez pas d'URL de rappel.
URL d'authentification	[nom-de-domaine-adfs]/adfs/oauth2/authorize
URL du jeton d'accès	[nom-de-domaine-adfs]/adfs/oauth2/token
ID client	Saisissez l'ID client AD FS
Secret client	Entrez le secret du client AD FS
Portée	OpenID
Authentification du client	Envoyer comme en-tête d'authentification de base
Ressource	Dans l'onglet **Options avancées**, ajoutez le champ Ressource avec la même valeur que l'URL de rappel, qui est fournie sous la forme d'une valeur « aud » dans le jeton JWT.

Configurer MFA dans SnapCenter Server à l'aide de PowerShell, SCCLI et REST API

Vous pouvez configurer MFA dans SnapCenter Server à l'aide de PowerShell, SCCLI et REST API.

Authentification CLI SnapCenter MFA

Dans PowerShell et SCCLI, l'applet de commande existante (Open-SmConnection) est étendue avec un champ supplémentaire appelé « AccessToken » pour utiliser le jeton porteur pour authentifier l'utilisateur.

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

Une fois l'applet de commande ci-dessus exécutée, une session est créée pour que l'utilisateur concerné puisse exécuter d'autres applets de commande SnapCenter .

Authentification de l'API REST SnapCenter MFA

Utilisez le jeton porteur au format *Authorization=Bearer <jeton d'accès>* dans le client API REST (comme Postman ou Swagger) et mentionnez le RoleName de l'utilisateur dans l'en-tête pour obtenir une réponse réussie de SnapCenter.

Flux de travail de l'API REST MFA

Lorsque MFA est configuré avec AD FS, vous devez vous authentifier à l'aide d'un jeton d'accès (porteur) pour accéder à l'application SnapCenter par n'importe quelle API Rest.

À propos de cette tâche

- Vous pouvez utiliser n'importe quel client REST comme Postman, Swagger UI ou FireCamp.
- Obtenez un jeton d'accès et utilisez-le pour authentifier les demandes ultérieures (API SnapCenter Rest) afin d'effectuer n'importe quelle opération.

Mesures

Pour s'authentifier via AD FS MFA

1. Configurez le client REST pour appeler le point de terminaison AD FS afin d'obtenir le jeton d'accès.

   Lorsque vous appuyez sur le bouton pour obtenir un jeton d'accès pour une application, vous serez redirigé vers la page SSO AD FS où vous devrez fournir vos informations d'identification AD et vous authentifier avec MFA. 1. Sur la page AD FS SSO, saisissez votre nom d'utilisateur ou votre adresse e-mail dans la zone de texte Nom d'utilisateur.

   + Les noms d'utilisateur doivent être formatés comme utilisateur@domaine ou domaine\utilisateur.

2. Dans la zone de texte Mot de passe, saisissez votre mot de passe.
3. Cliquez sur **Connexion**.
4. Dans la section **Options de connexion**, sélectionnez une option d'authentification et authentifiez-vous (selon votre configuration).
   - Push : approuvez la notification push qui est envoyée sur votre téléphone.
   - Code QR : utilisez l'application mobile AUTH Point pour scanner le code QR, puis saisissez le code de vérification affiché dans l'application
   - Mot de passe à usage unique : saisissez le mot de passe à usage unique de votre jeton.
5. Après une authentification réussie, une fenêtre contextuelle s'ouvrira contenant l'accès, l'ID et le jeton d'actualisation.

   Copiez le jeton d'accès et utilisez-le dans l'API Rest SnapCenter pour effectuer l'opération.

6. Dans l'API Rest, vous devez transmettre le jeton d'accès et le nom du rôle dans la section d'en-tête.
7. SnapCenter valide ce jeton d'accès à partir d'AD FS.

   S'il s'agit d'un jeton valide, SnapCenter le décode et obtient le nom d'utilisateur.

8. À l'aide du nom d'utilisateur et du nom de rôle, SnapCenter authentifie l'utilisateur pour une exécution d'API.

   Si l'authentification réussit, SnapCenter renvoie le résultat, sinon un message d'erreur s'affiche.

Activer ou désactiver la fonctionnalité SnapCenter MFA pour l'API REST, la CLI et l'interface graphique

interface graphique

Mesures

1. Connectez-vous au serveur SnapCenter en tant qu'administrateur SnapCenter .

2. Cliquez sur **Paramètres** > **Paramètres globaux** > **Paramètres MultiFactorAuthentication (MFA)**
3. Sélectionnez l'interface (GUI/RST API/CLI) pour activer ou désactiver la connexion MFA.

Interface PowerShell

Mesures

1. Exécutez les commandes PowerShell ou CLI pour activer MFA pour l'interface graphique utilisateur, l'API REST, PowerShell et SCCLI.

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

   Le paramètre path spécifie l'emplacement du fichier XML de métadonnées AD FS MFA.

   Active MFA pour l'interface utilisateur graphique SnapCenter , l'API Rest, PowerShell et SCCLI configurés avec le chemin de fichier de métadonnées AD FS spécifié.

2. Vérifiez l'état et les paramètres de configuration MFA à l'aide de l' `Get-SmMultiFactorAuthentication` applet de commande.

Interface SCCLI

Mesures

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

API REST

1. Exécutez l'API de publication suivante pour activer MFA pour l'interface graphique utilisateur, l'API REST, PowerShell et SCCLI.

Paramètre	Valeur
URL demandée	/api/4.9/settings/authentification multifacteur
Méthode HTTP	Poste
Corps de la requête	{ "IsGuiMFAEnabled": faux, "IsRestApiMFAEnabled": vrai, "IsCliMFAEnabled": faux, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }

Corps de la réponse	{ "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. Vérifiez l'état et les paramètres de configuration MFA à l'aide de l'API suivante.

Paramètre	Valeur
URL demandée	/api/4.9/settings/authentification multifacteur
Méthode HTTP	Obtenir
Corps de la réponse	{ "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

Informations sur le copyright

Informations sur les marques commerciales