Authentification multifacteur (MFA)

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-49/install/enable_multifactor_authentication.html on September 26, 2025. Always check docs.netapp.com for the latest.

Sommaire

Authentification multifacteur (MFA) . . . 1
- Gestion de l'authentification multifacteur (MFA) . . . 1
  - Prise en charge de l'authentification multifacteur (MFA) . . . 1
  - Mettre à jour les métadonnées AD FS MFA . . . 3
  - Mettre à jour les métadonnées MFA de SnapCenter . . . 3
  - Désactivation de l'authentification multifacteur (MFA) . . . 4
- Gérez l'authentification multifacteur (MFA) avec l'API REST, PowerShell et SCCLI . . . 4
  - Configurer AD FS comme OAuth/OIDC . . . 4
  - Créez un groupe d'applications à l'aide des commandes PowerShell . . . 5
  - Mettre à jour l'heure d'expiration du jeton d'accès . . . 7
  - Obtenez le jeton porteur auprès d'AD FS . . . 7
- Configurez MFA dans SnapCenter Server à l'aide de PowerShell, SCCLI et de l'API REST . . . 8
  - Authentification SnapCenter MFA CLI . . . 8
  - Authentification SnapCenter MFA REST API . . . 8
  - Workflow de l'API REST MFA . . . 8
  - Activez ou désactivez la fonctionnalité SnapCenter MFA pour l'API REST, l'interface de ligne de commande et l'interface graphique . . . 9

Authentification multifacteur (MFA)

Gestion de l'authentification multifacteur (MFA)

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

Prise en charge de l'authentification multifacteur (MFA)

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

Description de la 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 exiger une authentification de l'utilisateur pour des raisons de sécurité, en fonction de la persistance de la session AD FS.
- Les informations concernant les paramètres qui peuvent être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également voir "Guide de référence de l'applet de commande du logiciel SnapCenter".

Avant de commencer

- Windows Active Directory Federation Service (AD FS) doit être opérationnel dans le domaine respectif.
- Vous devez disposer d'un service d'authentification multifacteur pris en charge par AD FS, tel que Azure MFA, Cisco Duo, etc.
- L'horodatage du serveur SnapCenter et AD FS doit être identique, quel que soit le fuseau horaire.
- Procurez-vous et configurez le certificat d'autorité de certification autorisé pour le serveur SnapCenter.

  Le certificat CA est obligatoire pour les raisons suivantes :

  - Garantit que les communications ADFS-F5 ne se rompez pas, 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 incident dans une configuration autonome ou haute disponibilité, le certificat autosigné ne sera pas recréé, ce qui évite la reconfiguration de l'authentification multifacteur.
  - Garantit les résolutions IP-FQDN.

    Pour plus d'informations sur le certificat CA, reportez-vous à la section "Générer le fichier CSR de 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 FQDN>/FederationMetadata/2007-06/FederationMetadata.xml ».
3. Copiez le fichier téléchargé sur le serveur SnapCenter pour activer la fonctionnalité MFA.
4. Connectez-vous au serveur SnapCenter en tant qu'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'enregistrement du fichier de métadonnées MFA sur l'hôte du serveur SnapCenter.

6. Copiez le fichier généré sur l'hôte AD FS pour configurer SnapCenter en tant qu'entité client.
7. Activez MFA pour SnapCenter Server à l'aide du `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 opérations suivantes :
   a. Cliquez sur **fichier** > **Ajouter/Supprimer Snapin**.
   b. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
   c. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
   d. Cliquez sur **Console Root** > **Certificates – local Computer** > **Personal** > **Certificates**.
   e. Cliquez avec le bouton droit de la souris sur le certificat d'autorité de certification lié à SnapCenter, puis sélectionnez **toutes les tâches** > **gérer les clés privées**.
   f. Sur l'assistant d'autorisations, effectuez les opérations suivantes :
      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 Nom d'objet, entrez 'IIS_IUSRS', puis cliquez sur **vérifier les noms** et cliquez sur **OK**.

      Si la vérification a réussi, cliquez sur **OK**.
10. Dans l'hôte AD FS, ouvrez l'assistant de gestion AD FS et effectuez les opérations suivantes :
    a. Cliquez avec le bouton droit de la souris sur **fiducies de partie de confiance** > **Ajouter confiance de partie de confiance** > **début**.
    b. Sélectionnez la deuxième option, parcourez le fichier de métadonnées MFA SnapCenter et cliquez sur **Suivant**.
    c. Spécifiez un nom d'affichage et cliquez sur **Suivant**.
    d. Choisissez une stratégie de contrôle d'accès, le cas échéant, et cliquez sur **Suivant**.
    e. Sélectionnez les paramètres par défaut dans l'onglet suivant.
    f. Cliquez sur **Terminer**.

    SnapCenter se reflète désormais comme une personne de confiance avec le nom d'affichage fourni.
11. Sélectionnez le nom et effectuez les opérations suivantes :
    a. Cliquez sur **Modifier la politique d'émission des demandes de remboursement**.
    b. Cliquez sur **Ajouter règle** et cliquez sur **Suivant**.
    c. Spécifiez un nom pour la règle de sinistre.
    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. Procédez comme suit pour confirmer que les métadonnées ont été importées avec succès.
    a. Cliquez avec le bouton droit de la souris sur la confiance de la partie de confiance et sélectionnez **Propriétés**.
    b. Assurez-vous que les champs points finaux, identificateurs 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 MFA de SnapCenter peut également être activée au moyen d'API REST.

Pour plus d'informations sur le dépannage, reportez-vous à la section "Les tentatives de connexion simultanées dans plusieurs onglets indiquent une erreur MFA".

Mettre à jour les métadonnées AD FS MFA

Vous devez mettre à jour les métadonnées AD FS MFA dans SnapCenter en cas de modification du serveur AD FS, telles que la mise à niveau, le renouvellement du certificat CA, la reprise sur incident, etc.

Étapes

1. Téléchargez le fichier de métadonnées de la fédération AD FS à partir de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml »
2. Copiez le fichier téléchargé sur le serveur SnapCenter 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 MFA de SnapCenter

Vous devez mettre à jour les métadonnées MFA SnapCenter dans AD FS en cas de modification du serveur ADFS, comme la réparation, le renouvellement du certificat CA, la reprise sur incident, etc.

Étapes

1. Dans l'hôte AD FS, ouvrez l'assistant de gestion AD FS et effectuez les opérations suivantes :
    a. Cliquez sur **confiance de la partie de confiance**.
    b. Cliquez avec le bouton droit de la souris sur la confiance de la partie de confiance créée pour SnapCenter et cliquez sur **Supprimer**.

       Le nom défini par l'utilisateur de la confiance de la partie utilisatrice s'affiche.

c. Activez 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.

Désactivation de l'authentification multifacteur (MFA)

Étapes

1. Désactivez MFA et nettoyez les fichiers de configuration créés lorsque MFA a été activé à l'aide du `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.

Gérez l'authentification multifacteur (MFA) avec l'API REST, PowerShell et SCCLI

La connexion MFA est prise en charge depuis le navigateur, l'API REST, PowerShell et SCCLI. L'authentification multifacteur est prise en charge par le biais d'un gestionnaire d'identité AD FS. Vous pouvez activer MFA, désactiver MFA et configurer MFA depuis l'interface graphique, l'API REST, PowerShell et SCCLI.

Configurer AD FS comme OAuth/OIDC

Configurer AD FS à l'aide de l'assistant GUI de Windows

1. Accédez à **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Accédez à **ADFS** > **groupes d'applications**.
   a. Cliquez avec le bouton droit de la souris sur **groupes d'applications**.
   b. Sélectionnez **Ajouter un groupe d'applications** et entrez **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 **complète**, cliquez sur **Fermer**.
6. Cliquez avec le bouton droit de la souris sur le **Groupe d'applications** nouvellement ajouté et sélectionnez **Propriétés**.
7. Sélectionnez **Ajouter une application** dans 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, entrez l'URL du serveur SnapCenter et l'identifiant client créés à l'étape précédente dans la section Identificateur.
   a. Cliquez sur **Ajouter**.
   b. Cliquez sur **Suivant**.
10. Sur la page **choisir la stratégie de contrôle d'accès**, sélectionnez la stratégie de contrôle en fonction de vos besoins (par exemple, Autoriser tout le monde et demander MFA) et cliquez sur **Suivant**.
11. Sur la page **configurer l'autorisation d'application**, openid est sélectionné par défaut comme portée, cliquez sur **Suivant**.
12. Sur la page **Résumé**, cliquez sur **Suivant**.

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

13. Sur la page **exemple de propriétés 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 déclaration « aud » ou 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 du client ont été correctement ajoutés.

    Configurez OpenID Connect pour fournir un nom d'utilisateur comme sinistres.

16. Ouvrez l'outil **AD FS Management** situé dans le menu **Tools** en haut à droite du Gestionnaire de serveur.
    a. Sélectionnez le dossier **application Groups** dans la barre latérale de gauche.
    b. Sélectionnez l'API Web et cliquez sur **EDIT**.
    c. Accédez à l'onglet règles de conversion d'émission
17. Cliquez sur **Ajouter règle**.
    a. Sélectionnez **Envoyer les attributs LDAP en tant que sinistres** dans la liste déroulante modèle de règle de sinistre.
    b. Cliquez sur **Suivant**.
18. Entrez le nom **Claim Rule**.
    a. Sélectionnez **Active Directory** dans la liste déroulante magasin d'attributs.
    b. Sélectionnez **User-principal-Name** dans la liste déroulante **LDAP Attribute** et **UPN** dans la liste déroulante O*utening Claim Type*.
    c. Cliquez sur **Terminer**.

Créez un groupe d'applications à l'aide des commandes PowerShell

Vous pouvez créer le groupe d'applications, l'API Web et ajouter la portée et les revendications à l'aide des commandes PowerShell. Ces commandes sont disponibles au format de script automatisé. Pour plus d'informations, voir <link to KB article>.

1. Créez le nouveau groupe d'applications dans AD FS en utilisant 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 ADFS Web API 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, il est affiché une seule fois.

   ```
   "client_id = $identifier"

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

5. Accordez à l'application AD FS les autorisations d'allatclaims et d'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. Notez 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 conversion 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 l'heure d'expiration du jeton d'accès

Vous pouvez mettre à jour l'heure 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 tokens d'accès ne peuvent pas être révoqués et sont valides 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 mis à l'échelle. Vous devez fournir une valeur suffisante pour éviter tout travail stratégique en cours.

Étape

Pour mettre à jour l'heure d'expiration du jeton d'accès pour un groupe d'applications WebAPI, utilisez la commande suivante dans le serveur AD FS.

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

Obtenez le jeton porteur auprès d'AD FS

Vous devez remplir les paramètres mentionnés ci-dessous dans n'importe quel client REST (tel que Postman) et vous invite à saisir les informations d'identification de l'utilisateur. En outre, vous devez entrer l'authentification second facteur (quelque chose que vous avez et quelque chose que vous êtes) pour obtenir le jeton porteur.

+ La validité du jeton porteur est configurable à partir du 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	Entrez l'URL de base de votre application si vous n'avez pas d'URL de rappel.

URL d'authentification	[adfs-domain-name]/adfs/oauth2/authorise
Accéder à l'URL du token	[adfs-domain-name]/adfs/oauth2/token
ID client	Entrez l'ID du client AD FS
Secret client	Entrez le secret du client AD FS
Portée	OpenID
Authentification du client	Envoyer en tant qu'en-tête AUTH de base
Ressource	Dans l'onglet **Options avancées**, ajoutez le champ ressource avec la même valeur que l'URL de rappel, qui se présente sous la forme d'une valeur "aud" dans le jeton JWT.

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

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

Authentification SnapCenter MFA CLI

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 exécute d'autres applets de commande SnapCenter.

Authentification SnapCenter MFA REST API

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

Workflow 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 suivantes (API REST SnapCenter) afin d'effectuer n'importe quelle opération.

Étapes

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 AD FS SSO où vous devez fournir vos informations d'identification AD et vous authentifier auprès de MFA. 1. Dans 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 en tant qu'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 d'ouverture de session**, sélectionnez une option d'authentification et authentifiez-vous (selon votre configuration).
   - Push : approuvez la notification Push envoyée à 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. Une fois l'authentification réussie, une fenêtre contextuelle contenant l'accès, l'ID et le jeton d'actualisation s'ouvre.

   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 de 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.

Activez ou désactivez la fonctionnalité SnapCenter MFA pour l'API REST, l'interface de ligne de commande et l'interface graphique

GUI

Étapes

1. Connectez-vous au serveur SnapCenter en tant qu'administrateur SnapCenter.
2. Cliquez sur **Paramètres** > **Paramètres globaux** > **Paramètres d'authentification multifacteur (MFA)**
3. Sélectionnez l'interface (GUI/RST API/CLI) pour activer ou désactiver la connexion MFA.

Interface PowerShell

Étapes

1. Exécutez les commandes PowerShell ou CLI pour activer MFA pour l'interface graphique, 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 l'authentification multifacteur pour l'interface graphique SnapCenter, l'API REST, PowerShell et SCCLI configurée avec un chemin de fichier de métadonnées AD FS spécifié.

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

Interface SCCLI

Étapes

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 post suivante pour activer MFA pour l'interface graphique, l'API REST, PowerShell et SCCLI.

Paramètre	Valeur
URL demandée	/api/4.9/settings/multifactorauthentication
Méthode HTTP	Post
Corps de la demande	{ "IsGuiMFAEnabled": FALSE, "IsRestApiMFAEnabled": Vrai, "IsCliMFAEnabled": FALSE, « ADFSConfigFilePath » : « C:\\ADFS_metadata\\abc.xml » }
Corps de réponse	{ « MFAConfiguration » : { "IsGuiMFAEnabled": FALSE, « ADFSConfigFilePath » : « C:\\ADFS_metadata\\abc.xml », « SCConfigFilePath » : nul, "IsRestApiMFAEnabled": Vrai, "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/multifactorauthentication
Méthode HTTP	Obtenez
Corps de réponse	{ « MFAConfiguration » : { "IsGuiMFAEnabled": FALSE, « ADFSConfigFilePath » : « C:\\ADFS_metadata\\abc.xml », « SCConfigFilePath » : nul, "IsRestApiMFAEnabled": Vrai, "IsCliMFAEnabled": FALSE, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.