Préparez-vous à installer le serveur SnapCenter

SnapCenter software

NetApp
February 20, 2026

Sommaire

Préparez-vous à installer le serveur SnapCenter

Configuration requise pour installer le serveur SnapCenter

Avant d'installer SnapCenter Server sur un hôte Windows ou Linux, vous devez vérifier et vous assurer que toutes les conditions requises sont remplies pour votre environnement.

Configuration requise pour les domaines et les groupes de travail pour l'hôte Windows

Le serveur SnapCenter peut être installé sur un hôte Windows qui se trouve dans un domaine ou dans un groupe de travail.

L'utilisateur ayant admin Privileges est autorisé à installer le serveur SnapCenter.

- Domaine Active Directory : vous devez utiliser un utilisateur de domaine avec des droits d'administrateur local. L'utilisateur de domaine doit être membre du groupe administrateur local sur l'hôte Windows.
- Groupes de travail : vous devez utiliser un compte local disposant de droits d'administrateur local.

Bien que les approbations de domaine, les forêts multidomaines et les approbations interdomaines soient prises en charge, les domaines interforestiers ne sont pas pris en charge. La documentation Microsoft à propos des domaines et des fiducies Active Directory contient des informations supplémentaires.

> Après avoir installé le serveur SnapCenter, vous ne devez pas modifier le domaine dans lequel se trouve l'hôte SnapCenter. Si vous supprimez l'hôte SnapCenter Server du domaine dans lequel il se trouvait lors de l'installation du serveur SnapCenter, puis essayez de désinstaller le serveur SnapCenter, l'opération de désinstallation échoue.

Les besoins en termes d'espace et de dimensionnement

Vous devez connaître les exigences en matière d'espace et de dimensionnement.

Élément	Configuration requise pour les hôtes Windows	Configuration requise pour l'hôte Linux
Systèmes d'exploitation	Microsoft Windows Seules les versions anglaise, allemande, japonaise et chinoise simplifiée des systèmes d'exploitation sont prises en charge. Pour obtenir les informations les plus récentes sur les versions prises en charge, consultez "Matrice d'interopérabilité NetApp".	• Red Hat Enterprise Linux (RHEL) 8 et 9 • SUSE Linux Enterprise Server (SLES) 15 Pour obtenir les informations les plus récentes sur les versions prises en charge, consultez "Matrice d'interopérabilité NetApp".
Nombre minimal de processeurs	4 cœurs	4 cœurs

Élément	Configuration requise pour les hôtes Windows	Configuration requise pour l'hôte Linux
RAM minimale	8 Go Le pool de mémoire tampon du serveur MySQL utilise 20 % de la RAM totale.	8 Go
Espace minimal sur le disque dur pour le logiciel et les journaux du serveur SnapCenter	7 GO Si vous disposez du référentiel SnapCenter dans le lecteur où est installé le serveur SnapCenter, il est recommandé d'avoir 15 Go.	15 GO
Espace disque minimum pour le référentiel SnapCenter	8 Go REMARQUE : si le serveur SnapCenter se trouve dans le même lecteur que le référentiel SnapCenter, il est recommandé d'avoir 15 Go.	Sans objet
Packs logiciels requis	• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle • PowerShell 7.4.2 ou version ultérieure Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section "Échec de la mise à niveau ou de l'installation de SnapCenter pour les systèmes hérités qui ne disposent pas d'une connexion Internet".	• .NET Framework 8.0.12 (et tous les correctifs 8.0.x suivants) • PowerShell 7.4.2 ou version ultérieure • Ce serveur Web peut être utilisé comme proxy inverse • Devel-PAM PAM (Pluggable Authentication modules) est un outil de sécurité système qui permet aux administrateurs système de définir une stratégie d'authentification sans avoir à recompiler les programmes qui effectuent l'authentification.

Le noyau ASP.NET nécessite IIS_IUSRS pour accéder au système de fichiers temporaires dans le serveur SnapCenter sous Windows.

Exigences relatives à l'hôte SAN

SnapCenter n'inclut pas les utilitaires hôtes ou un DSM. Si l'hôte SnapCenter fait partie d'un environnement SAN (FC/iSCSI), vous devrez peut-être installer et configurer des logiciels supplémentaires sur l'hôte du serveur SnapCenter.

- Utilitaires hôtes : les utilitaires hôtes prennent en charge FC et iSCSI et vous permettent d'utiliser MPIO sur vos serveurs Windows. "En savoir plus".
- Microsoft DSM pour Windows MPIO : ce logiciel fonctionne avec les pilotes Windows MPIO pour gérer plusieurs chemins entre les ordinateurs hôtes NetApp et Windows. Un DSM est nécessaire pour les configurations haute disponibilité.

Si vous utilisiez ONTAP DSM, vous devez migrer vers Microsoft DSM. Pour plus d'informations, voir "Comment migrer de ONTAP DSM vers Microsoft DSM".

Navigateurs pris en charge

Le logiciel SnapCenter prend en charge Chrome 125 et versions ultérieures, ainsi que Microsoft Edge 110.0.1587.17 et versions ultérieures.

Configuration requise pour les ports

Le logiciel SnapCenter nécessite différents ports pour la communication entre les différents composants.

- Les applications ne peuvent pas partager de port.
- Pour les ports personnalisables, vous pouvez sélectionner un port personnalisé lors de l'installation si vous ne souhaitez pas utiliser le port par défaut.
- Pour les ports fixes, vous devez accepter le numéro de port par défaut.
- Pare-feu
  - Les pare-feu, proxys ou autres périphériques réseau ne doivent pas interférer avec les connexions.
  - Si vous spécifiez un port personnalisé lors de l'installation de SnapCenter, vous devez ajouter une règle de pare-feu sur l'hôte du plug-in pour ce port pour le chargeur Plug-in SnapCenter.

Le tableau ci-dessous répertorie les différents ports et leurs valeurs par défaut.

Nom du port	Numéros de port	Protocole	Direction	Description
Port Web SnapCenter	8146	HTTPS	Bidirectionnel	Ce port est utilisé pour la communication entre le client SnapCenter (l'utilisateur SnapCenter) et le serveur SnapCenter et est également utilisé pour la communication entre les hôtes de plug-in et le serveur SnapCenter. Vous pouvez personnaliser le numéro de port.
Port de communication SMCore de SnapCenter	8145	HTTPS	Bidirectionnel	Ce port est utilisé pour la communication entre le serveur SnapCenter et les hôtes sur lesquels les plug-ins SnapCenter sont installés. Vous pouvez personnaliser le numéro de port.
Port de service du planificateur	8154	HTTPS		Ce port permet d'orchestrer de manière centralisée les flux de travail du planificateur SnapCenter pour tous les plug-ins gérés au sein de l'hôte du serveur SnapCenter. Vous pouvez personnaliser le numéro de port.

Nom du port	Numéros de port	Protocole	Direction	Description
Port RabbitMQ	5672	TCP		Il s'agit du port par défaut sur lequel RabbitMQ écoute et il est utilisé pour la communication du modèle éditeur-abonné entre le service Planificateur et SnapCenter.
Port MySQL	3306	HTTPS		Le port est utilisé pour communiquer avec la base de données du référentiel SnapCenter. Vous pouvez créer des connexions sécurisées du serveur SnapCenter au serveur MySQL. "En savoir plus >>"
Hôtes du plug-in Windows	135, 445	TCP		Ce port est utilisé pour la communication entre le serveur SnapCenter et l'hôte sur lequel le plug-in est installé. La plage de ports dynamique supplémentaire spécifiée par Microsoft doit également être ouverte.
Hôtes du plug-in Linux ou AIX	22	SSH	Unidirectionnel	Ce port est utilisé pour la communication entre le serveur SnapCenter et l'hôte, lancé du serveur à l'hôte client.

Nom du port	Numéros de port	Protocole	Direction	Description
Module de plug-ins SnapCenter pour Windows, Linux ou AIX	8145	HTTPS	Bidirectionnel	Ce port est utilisé pour la communication entre SMCore et les hôtes sur lesquels le package de plug-ins est installé. Personnalisable. Vous pouvez personnaliser le numéro de port.
Plug-in SnapCenter pour bases de données Oracle	27216			Le port JDBC par défaut est utilisé par le plug-in pour Oracle pour se connecter à la base de données Oracle.
Plug-in SnapCenter pour base de données Exchange	909			Le NET par défaut. Le port TCP est utilisé par le plug-in pour Windows pour se connecter aux rappels Exchange VSS.
Plug-ins pris en charge par NetApp pour SnapCenter	9090	HTTPS		Il s'agit d'un port interne utilisé uniquement sur l'hôte du plug-in ; aucune exception de pare-feu n'est requise. La communication entre le serveur SnapCenter et les plug-ins est acheminée via le port 8145.

Nom du port	Numéros de port	Protocole	Direction	Description
Cluster ONTAP ou port de communication SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidirectionnel	Le port est utilisé par le SAL (Storage abstraction Layer) pour la communication entre l'hôte exécutant le serveur SnapCenter et le SVM. Le port est actuellement utilisé par le SAL sur SnapCenter pour les hôtes du plug-in Windows pour la communication entre l'hôte du plug-in SnapCenter et le SVM.
Plug-in SnapCenter pour base de données SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidirectionnel	Pour un seul tenant de conteneur de base de données multitenant (MDC), le numéro de port se termine par 13 ; pour non MDC, le numéro de port se termine par 15. Vous pouvez personnaliser le numéro de port.
Plug-in SnapCenter pour PostgreSQL	5432			Ce port est le port PostgreSQL par défaut utilisé pour la communication entre le plug-in pour PostgreSQL et le cluster PostgreSQL. Vous pouvez personnaliser le numéro de port.

Inscrivez-vous pour accéder au logiciel SnapCenter

Si vous découvrez Amazon FSX pour NetApp ONTAP ou Azure NetApp Files et ne possédez pas de compte SnapCenter, vous devez vous inscrire pour accéder au logiciel

NetApp.

Avant de commencer

- Vous devez avoir accès à l'ID de messagerie de l'entreprise.
- Si vous utilisez Azure NetApp Files, vous devez disposer de l'ID d'abonnement Azure.
- Si vous utilisez Amazon FSX pour NetApp ONTAP, vous devez disposer de l'ID du système de fichiers de votre système de fichiers FSX pour ONTAP.

Description de la tâche

Votre inscription est soumise à des validations d'informations et peut prendre jusqu'à une journée pour confirmer et mettre à niveau le nouveau compte du site de support NetApp (NSS) vers un accès **complet** à partir de l'accès **guest**.

Étapes

1. Cliquez sur https://mysupport.netapp.com/site/user/registration pour vous inscrire.
2. Entrez votre identifiant de courriel d'entreprise, remplissez le formulaire captcha, acceptez la politique de confidentialité de NetApp et cliquez sur **soumettre**.
3. Authentifiez l'enregistrement en saisissant le mot de passe à usage unique envoyé à votre ID de courriel et cliquez sur **Continuer**.
4. Sur la page de fin de l'inscription, entrez les informations suivantes pour terminer l'inscription.
   a. Sélectionnez **client NetApp / utilisateur final**.
   b. Dans le champ du NUMÉRO DE SÉRIE, entrez l'ID d'abonnement Azure si vous utilisez Azure NetApp Files ou l'ID du système de fichiers si vous utilisez Amazon FSX pour NetApp ONTAP.

Vous pouvez émettre un billet à https://mysupport.netapp.com/site/help si vous rencontrez un problème pendant l'enregistrement ou si vous connaissez le statut.

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 obtenir des informations de 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. Sélectionnez **fiducies de partie utilisatrice**.
   b. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrice qui a été créée pour SnapCenter et sélectionnez **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" } }