Préparez-vous à installer le serveur SnapCenter

SnapCenter Software 4.8

NetApp
January 18, 2024

Sommaire

Préparez-vous à installer le serveur SnapCenter

Exigences relatives au domaine et au groupe de travail

Le serveur SnapCenter peut être installé sur des systèmes qui se trouvent dans un domaine ou dans un groupe de travail. L'utilisateur utilisé pour l'installation doit disposer de privilèges d'administrateur sur la machine en cas de groupe de travail et de domaine.

Pour installer les plug-ins SnapCenter Server et SnapCenter sur les hôtes Windows, utilisez l'une des méthodes suivantes :

- **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 des 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

Avant d'installer le serveur SnapCenter, vous devez connaître les exigences en matière d'espace et de dimensionnement. Vous devez également appliquer les mises à jour système et de sécurité disponibles.

Élément	De formation
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 dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".
Nombre minimal de processeurs	4 cœurs

Élément	De formation
RAM minimale	8 Go Le pool de mémoire tampon du serveur MySQL utilise 20 % de la RAM totale.
Espace minimal sur le disque dur pour le logiciel et les journaux du serveur SnapCenter	4 GO Si le référentiel SnapCenter se trouve sur le même lecteur sur lequel SnapCenter Server est installé, il est recommandé d'avoir 10 Go.
Espace disque minimum pour le référentiel SnapCenter	6 GO REMARQUE : si le serveur SnapCenter se trouve sur le même lecteur où le référentiel SnapCenter est installé, il est recommandé d'avoir 10 Go.
Packs logiciels requis	• Microsoft .NET Framework 4.7.2 ou version ultérieure • Windows Management Framework (WMF) 4.0 ou version ultérieure • PowerShell 4.0 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". Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".

Exigences relatives à l'hôte SAN

Si votre hôte SnapCenter fait partie d'un environnement FC/iSCSI, vous devrez peut-être installer des logiciels supplémentaires sur le système pour autoriser l'accès au stockage ONTAP.

SnapCenter n'inclut pas les utilitaires hôtes ou un DSM. Si votre hôte SnapCenter fait partie d'un environnement SAN, vous devrez peut-être installer et configurer les logiciels suivants :

- Utilitaires hôtes

Les utilitaires hôtes prennent en charge les protocoles FC et iSCSI, et il vous permet d'utiliser MPIO sur vos serveurs Windows. Pour plus d'informations, reportez-vous à la section "Documentation Host Utilities".

- Microsoft DSM pour Windows MPIO

  Ce logiciel fonctionne avec des pilotes Windows MPIO pour gérer plusieurs chemins d'accès 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".

Systèmes et applications de stockage pris en charge

Vous devez connaître le système de stockage, les applications et les bases de données pris en charge.

- SnapCenter prend en charge ONTAP 8.3.0 et versions ultérieures pour protéger vos données.
- SnapCenter prend en charge Amazon FSX pour NetApp ONTAP afin de protéger vos données contre la version 4.5 des correctifs P1 du logiciel SnapCenter.

  Si vous utilisez Amazon FSX pour NetApp ONTAP, assurez-vous que les plug-ins hôtes du serveur SnapCenter sont mis à niveau vers 4.5 P1 ou une version ultérieure pour réaliser les opérations de protection des données.

  Pour plus d'informations sur Amazon FSX pour NetApp ONTAP, consultez "Documentation Amazon FSX pour NetApp ONTAP".

- SnapCenter prend en charge la protection de différentes applications et bases de données.

  Pour plus d'informations sur les applications et bases de données prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".

Navigateurs pris en charge

Le logiciel SnapCenter peut être utilisé sur plusieurs navigateurs.

- Chrome

  Si vous utilisez v66, il se peut que vous n'ayez pas pu lancer l'interface utilisateur SnapCenter.

- Internet Explorer

  L'interface utilisateur SnapCenter ne se charge pas correctement si vous utilisez IE 10 ou des versions antérieures. Vous devez effectuer la mise à niveau vers IE 11.

  - Seule la sécurité au niveau par défaut est prise en charge.

    Les modifications apportées aux paramètres de sécurité d'Internet Explorer entraînent d'importants problèmes d'affichage du navigateur.

    - L'affichage de compatibilité d'Internet Explorer doit être désactivé.
- Microsoft Edge

Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".

Connexion et port requis

Assurez-vous que les connexions et les ports requis sont satisfaits avant d'installer le serveur SnapCenter et les plug-ins d'application ou de base de données.

- Les applications ne peuvent pas partager de port.

  Chaque port doit être dédié à l'application appropriée.

- Pour les ports personnalisables, vous pouvez sélectionner un port personnalisé lors de l'installation si vous ne souhaitez pas utiliser le port par défaut.

  Vous pouvez modifier un port de plug-in après l'installation à l'aide de l'assistant Modifier l'hôte.

- 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.

Type de port	Port par défaut
Port SnapCenter	8146 (HTTPS), bidirectionnel, personnalisable, comme dans l'URL *https://server:8146* Utilisé pour la communication entre le client SnapCenter (utilisateur SnapCenter) et le serveur SnapCenter. Utilisé également pour la communication entre les hôtes du plug-in et le serveur SnapCenter. Pour personnaliser le port, voir "Installez le serveur SnapCenter à l'aide de l'assistant d'installation."
Port de communication SMCore de SnapCenter	8145 (HTTPS), bidirectionnel, personnalisable Le port est utilisé pour la communication entre le serveur SnapCenter et les hôtes sur lesquels les plug-ins SnapCenter sont installés. Pour personnaliser le port, voir "Installez le serveur SnapCenter à l'aide de l'assistant d'installation."

Type de port	Port par défaut
Port MySQL	3306 (HTTPS), bidirectionnel Le port est utilisé pour la communication entre SnapCenter et la base de données de référentiel MySQL. Vous pouvez créer des connexions sécurisées entre le serveur SnapCenter et le serveur MySQL. "En savoir plus >>"
Hôtes du plug-in Windows	135, 445 (TCP) En plus des ports 135 et 445, la plage de ports dynamiques spécifiée par Microsoft doit également être ouverte. Les opérations d'installation à distance utilisent le service Windows Management Instrumentation (WMI), qui recherche dynamiquement cette plage de ports. Pour plus d'informations sur la plage de ports dynamiques prise en charge, reportez-vous à la section "Présentation du service et configuration requise du port réseau pour Windows" Les ports sont utilisés pour la communication entre le serveur SnapCenter et l'hôte sur lequel le plug-in est installé. Pour envoyer les binaires de modules enfichables aux hôtes du plug-in Windows, les ports doivent être ouverts uniquement sur l'hôte du plug-in et ils peuvent être fermés après l'installation.
Hôtes du plug-in Linux ou AIX	22 (SSH) Les ports sont utilisés pour la communication entre le serveur SnapCenter et l'hôte sur lequel le plug-in est installé. Les ports sont utilisés par SnapCenter pour copier les binaires de package plug-in vers les hôtes du plug-in Linux ou AIX et doivent être ouverts ou exclus du pare-feu ou des tables iptables.

Type de port	Port par défaut
Package de plug-ins SnapCenter pour Windows, offre de plug-ins SnapCenter pour Linux ou offre de plug-ins SnapCenter pour AIX	8145 (HTTPS), bidirectionnel, personnalisable Le port est utilisé pour la communication entre SMCore et les hôtes sur lesquels le package plug-ins est installé. Le chemin de communication doit également être ouvert entre la LIF de management du SVM et le serveur SnapCenter. Pour personnaliser le port, voir "Ajoutez des hôtes et installez le plug-in SnapCenter pour Microsoft Windows" ou "Ajoutez des hôtes et installez le module de plug-ins SnapCenter pour Linux ou AIX."
Plug-in SnapCenter pour bases de données Oracle	27216, personnalisable Le port JDBC par défaut est utilisé par le plug-in pour Oracle pour se connecter à la base de données Oracle. Pour personnaliser le port, voir "Ajoutez des hôtes et installez le module de plug-ins SnapCenter pour Linux ou AIX."
Plug-ins personnalisés pour SnapCenter	9090 (HTTPS), fixe Il s'agit d'un port interne utilisé uniquement sur l'hôte personnalisé du plug-in ; aucune exception de pare-feu n'est requise. La communication entre le serveur SnapCenter et les plug-ins personnalisés est routée via le port 8145.
Cluster ONTAP ou port de communication SVM	443 (HTTPS), bidirectional80 (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.

Type de port	Port par défaut
Plug-in SnapCenter pour base de données SAP HANA vCode Spell Checkerports	3instance_number13 ou 3instance_number15, HTTP ou HTTPS, bidirectionnel et personnalisable 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. Par exemple, 32013 est le numéro de port pour l'instance 20 et 31015 est le numéro de port pour l'instance 10. Pour personnaliser le port, voir "Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants."
Port de communication du contrôleur de domaine	Reportez-vous à la documentation Microsoft pour identifier les ports devant être ouverts dans le pare-feu sur un contrôleur de domaine afin que l'authentification fonctionne correctement. Il est nécessaire d'ouvrir les ports Microsoft requis sur le contrôleur de domaine pour que le serveur SnapCenter, les hôtes Plug-in ou tout autre client Windows puisse authentifier les utilisateurs.

Pour modifier les détails du port, voir "Modifier les hôtes du plug-in".

Licences SnapCenter

SnapCenter nécessite plusieurs licences pour permettre la protection des données des applications, des bases de données, des systèmes de fichiers et des machines virtuelles. Le type de licence SnapCenter que vous installez dépend de votre environnement de stockage et des fonctionnalités que vous souhaitez utiliser.

Licence	Si nécessaire
Contrôleur SnapCenter standard	Requis pour FAS et AFF La licence SnapCenter Standard est basée sur le contrôleur et incluse dans le bundle Premium. Si vous disposez de la licence SnapManager Suite, vous bénéficiez également des droits de licence SnapCenter Standard. Si vous souhaitez installer SnapCenter sous forme d'essai avec les systèmes de stockage FAS ou AFF, vous pouvez obtenir une licence d'évaluation Premium Bundle en contactant l'ingénieur commercial. SnapCenter fait également partie du pack de protection des données. Si vous avez acheté A400 ou une version ultérieure, vous devez acheter le pack de protection des données.
SnapCenter Standard basé sur la capacité	Requis avec ONTAP Select et Cloud Volumes ONTAP Si vous êtes un client Cloud Volumes ONTAP ou ONTAP Select, vous devez obtenir une licence basée sur la capacité par To en fonction des données gérées par SnapCenter. Par défaut, SnapCenter propose une licence d'évaluation standard basée sur la capacité SnapCenter 90 jours intégrée, avec une capacité de 100 To. Pour plus d'informations, contactez l'ingénieur commercial.
SnapMirror ou SnapVault	ONTAP Une licence SnapMirror ou SnapVault est requise si la réplication est activée dans SnapCenter.
SnapRestore	Indispensable pour restaurer et vérifier les sauvegardes. Sur les systèmes de stockage primaires • Indispensable sur les systèmes de destination SnapVault pour effectuer une vérification à distance et une restauration à partir d'une sauvegarde. • Nécessaire sur les systèmes de destination SnapMirror pour effectuer une vérification à distance.

Licence	Si nécessaire
FlexClone	Requises pour cloner les bases de données et les opérations de vérification. Sur les systèmes de stockage primaires et secondaires • Requis sur les systèmes de destination SnapVault pour créer des clones à partir d'une sauvegarde secondaire à distance. • Requis sur les systèmes de destination SnapMirror pour créer des clones à partir d'une sauvegarde SnapMirror secondaire
Protocoles	• Licence iSCSI ou FC pour LUN • Licence CIFS pour les partages SMB • Licence NFS pour VMDK de type NFS • Licence iSCSI ou FC pour les VMDK de type VMFS Indispensable sur les systèmes de destination SnapMirror pour transmettre les données en cas d'indisponibilité d'un volume source.
Licences SnapCenter Standard (en option)	Destinations secondaires Il est recommandé, mais pas obligatoire, d'ajouter des licences SnapCenter Standard aux destinations secondaires. Si les licences SnapCenter Standard ne sont pas activées sur les destinations secondaires, vous ne pouvez pas utiliser SnapCenter pour sauvegarder les ressources sur la destination secondaire après avoir effectué une opération de basculement. Une licence FlexClone est toutefois requise sur les destinations secondaires pour effectuer les opérations de clonage et de vérification.

Les licences SnapCenter Advanced et SnapCenter NAS File Services sont obsolètes et ne sont plus disponibles.

Vous devez installer une ou plusieurs licences SnapCenter. Pour plus d'informations sur l'ajout de licences, reportez-vous à la section "Ajout de licences SnapCenter standard basées sur le contrôleur" ou "Ajoutez des licences SnapCenter standard basées sur la capacité".

Licences Single Mailbox Recovery (SMBR)

Si vous utilisez le plug-in SnapCenter pour Exchange pour gérer les bases de données Microsoft Exchange Server et SMBR (Single Mailbox Recovery), vous devez disposer d'une licence supplémentaire pour SMBR qui doit être achetée séparément selon la boîte aux lettres des utilisateurs.

NetApp® Single Mailbox Recovery a pris fin le 12 mai 2023. Pour plus d'informations, reportez-vous à la section "CPC-00507". NetApp continuera d'assurer le support des clients ayant acheté une capacité de boîte aux lettres, des services de maintenance et un support via des références marketing introduites le 24 juin 2020, pendant la durée du support souscrit.

NetApp Single Mailbox Recovery est un produit partenaire fourni par Ontrack. OnTrack PowerControls offre des fonctionnalités similaires à celles de NetApp Single Mailbox Recovery. Les clients peuvent se procurer de nouvelles licences logicielles Ontrack PowerControls et des renouvellements de maintenance et de support Ontrack PowerControls auprès d'Ontrack (jusqu'à licensingteam@ontrack.com) pour une récupération granulaire des boîtes aux lettres après la date de fin de disponibilité du 12 mai 2023.

Méthodes d'authentification pour vos informations d'identification

Les informations d'identification utilisent différentes méthodes d'authentification en fonction de l'application ou de l'environnement. Les informations d'identification authentifient les utilisateurs pour qu'ils puissent exécuter des opérations SnapCenter. Vous devez créer un ensemble d'informations d'identification pour l'installation de plug-ins et un autre ensemble pour les opérations de protection des données.

Authentification Windows

La méthode d'authentification Windows s'authentifie auprès d'Active Directory. Pour l'authentification Windows, Active Directory est configuré en dehors de SnapCenter. L'authentification SnapCenter s'effectue sans configuration supplémentaire. Vous avez besoin d'une information d'identification Windows pour effectuer des tâches telles que l'ajout d'hôtes, l'installation de modules enfichables et les tâches de planification.

Authentification de domaine non fiable

SnapCenter permet la création d'informations d'identification Windows à l'aide d'utilisateurs et de groupes appartenant aux domaines non fiables. Pour que l'authentification réussisse, vous devez enregistrer les domaines non approuvés avec SnapCenter.

Authentification locale du groupe de travail

SnapCenter permet la création d'informations d'identification Windows avec des groupes et des utilisateurs de groupes de travail locaux. L'authentification Windows pour les utilisateurs et les groupes de travail locaux n'a pas lieu au moment de la création des informations d'identification Windows, mais est différée jusqu'à ce que l'enregistrement de l'hôte et d'autres opérations de l'hôte soient effectués.

Authentification SQL Server

La méthode d'authentification SQL s'authentifie par rapport à une instance SQL Server. Cela signifie qu'une instance SQL Server doit être découverte dans SnapCenter. Par conséquent, avant d'ajouter un identifiant SQL, vous devez ajouter un hôte, installer des modules de plug-in et actualiser les ressources. Vous avez

besoin de l'authentification SQL Server pour effectuer des opérations telles que la planification sur SQL Server ou la détection des ressources.

Authentification Linux

La méthode d'authentification Linux s'authentifie par rapport à un hôte Linux. Vous avez besoin d'une authentification Linux au cours de la première étape de l'ajout de l'hôte Linux et de l'installation du module SnapCenter Plug-ins Package pour Linux à distance à partir de l'interface graphique SnapCenter.

Authentification AIX

La méthode d'authentification AIX s'authentifie auprès d'un hôte AIX. L'authentification AIX doit être effectuée lors de l'étape initiale de l'ajout de l'hôte AIX et de l'installation du module plug-ins SnapCenter pour AIX à distance à partir de l'interface utilisateur graphique SnapCenter.

Authentification de la base de données Oracle

La méthode d'authentification de la base de données Oracle s'authentifie par rapport à une base de données Oracle. Une authentification de base de données Oracle est nécessaire pour effectuer des opérations sur la base de données Oracle si l'authentification du système d'exploitation est désactivée sur l'hôte de la base de données. Par conséquent, avant d'ajouter des informations d'identification de base de données Oracle, vous devez créer un utilisateur Oracle dans la base de données Oracle avec des privilèges sysdba.

Authentification Oracle ASM

La méthode d'authentification Oracle ASM s'authentifie par rapport à une instance Oracle Automatic Storage Management (ASM). Si vous devez accéder à l'instance Oracle ASM et si l'authentification du système d'exploitation est désactivée sur l'hôte de la base de données, vous devez disposer d'une authentification Oracle ASM. Par conséquent, avant d'ajouter une information d'identification Oracle ASM, vous devez créer un utilisateur Oracle avec des privilèges sysasm dans l'instance ASM.

Authentification du catalogue RMAN

La méthode d'authentification du catalogue RMAN s'authentifie par rapport à la base de données du catalogue Oracle Recovery Manager (RMAN). Si vous avez configuré un mécanisme de catalogue externe et enregistré votre base de données dans la base de données de catalogue, vous devez ajouter l'authentification de catalogue RMAN.

Connexions de stockage et identifiants

Avant d'effectuer les opérations de protection des données, configurez les connexions de stockage et ajoutez les identifiants que le serveur SnapCenter et les plug-ins SnapCenter utiliseront.

- * Connexions de stockage*

  Les connexions de stockage permettent au serveur SnapCenter et aux plug-ins SnapCenter d'accéder au système de stockage ONTAP. La configuration de ces connexions implique également la configuration des fonctions AutoSupport et EMS.

- **Informations d'identification**

- Administrateur de domaine ou tout membre du groupe d'administrateurs

  Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :

  - *NetBIOS\username*
  - *Domain FQDN\username*
  - *Username@upn*
- Administrateur local (groupes de travail uniquement)

  Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte.

Le format valide du champ Nom d'utilisateur est : *username*

- Informations d'identification pour des groupes de ressources individuels

  Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

Gestion de l'authentification multifacteur (MFA)

Cette rubrique décrit comment 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)

Cette rubrique décrit comment activer la fonctionnalité MFA dans le serveur AD FS (Active Directory Federation Service) et le serveur SnapCenter.

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".

Ce dont vous avez besoin

- 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 -Enable -Path` applet de commande.

   Le paramètre PATH spécifie l'emplacement du fichier xml de métadonnées MFA AD FS, qui a été copié sur le serveur SnapCenter à l'étape 3.
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 -Disable` 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.

Informations sur le copyright

Informations sur les marques commerciales