Installez le plug-in SnapCenter pour Microsoft Exchange Server

SnapCenter Software 4.7

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-47/protect-sce/concept_install_snapcenter_plug_in_for_microsoft_exchange_server.html on January 18, 2024.
Always check docs.netapp.com for the latest.

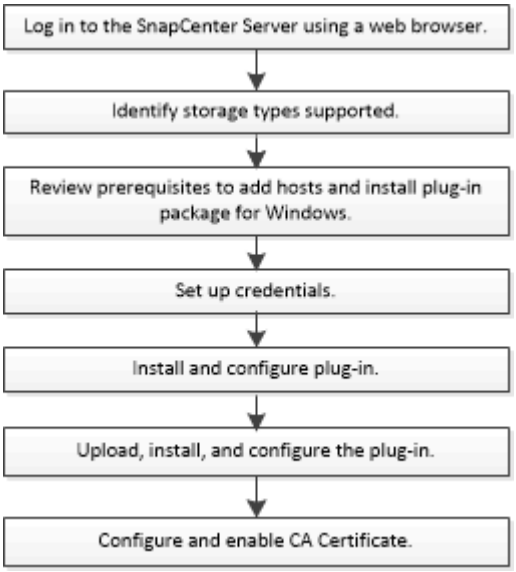
Sommaire

Installez le plug-in SnapCenter pour Microsoft Exchange Server . . . 1
Workflow d'installation du plug-in SnapCenter pour Microsoft Exchange Server . . . 1
Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour Microsoft Exchange Server . . . 1
Configuration des informations d'identification pour le plug-in SnapCenter pour Windows . . . 5
Configurez GMSA sur Windows Server 2012 ou version ultérieure . . . 7
Ajoutez des hôtes et installez le plug-in pour Exchange . . . 8
Installez le plug-in pour Exchange à partir de l'hôte SnapCenter Server à l'aide des applets de commande PowerShell . . . 13
Installez le plug-in SnapCenter pour l'échange silencieusement à partir de la ligne de commande . . . 14
Contrôler l'état d'installation du module d'extension SnapCenter . . . 16
Configurer le certificat CA . . . 17
Configurez SnapManager 7.x pour Exchange et SnapCenter afin qu'ils coexistent . . . 20

Installez le plug-in SnapCenter pour Microsoft Exchange Server

Workflow d'installation du plug-in SnapCenter pour Microsoft Exchange Server

Vous devez installer et configurer le plug-in SnapCenter pour Microsoft Exchange Server si vous souhaitez protéger les bases de données Exchange.



Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour Microsoft Exchange Server

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Vous devez utiliser Microsoft Exchange Server 2013, 2016 ou 2019 pour les configurations autonomes et de groupes de disponibilité de base de données.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Si vous gérez des nœuds de cluster dans SnapCenter, vous devez disposer d'un utilisateur disposant de privilèges d'administration sur tous les nœuds du cluster.
- Vous devez disposer d'un utilisateur avec des autorisations d'administration sur le serveur Exchange.
- Si SnapManager pour Microsoft Exchange Server et SnapDrive pour Windows sont déjà installés, vous devez annuler l'enregistrement du fournisseur de matériel VSS utilisé par SnapDrive pour Windows avant d'installer le plug-in pour Exchange sur le même serveur Exchange pour assurer la protection des données

à l'aide de SnapCenter.

- Si SnapManager pour Microsoft Exchange Server et le plug-in pour Exchange sont installés sur le même serveur, vous devez interrompre ou supprimer du planificateur Windows tous les planifications créés par SnapManager pour Microsoft Exchange Server.
- L'hôte doit être résolu au nom de domaine complet (FQDN) du serveur. Si le fichier hosts est modifié pour le rendre résolu et si le nom abrégé et le FQDN sont spécifiés dans le fichier hosts, créez une entrée dans le fichier hosts SnapCenter au format suivant : *<adresse_ip> <nom_hôte> <nom_hôte>*.
- Assurez-vous que les ports suivants ne sont pas bloqués dans le pare-feu, sinon l'opération d'ajout d'hôte échoue. Pour résoudre ce problème, vous devez configurer la plage de ports dynamiques. Pour plus d'informations, voir "Documentation Microsoft".
  - Plage de ports 50000 - 51000 pour Windows 2016 et Exchange 2016
  - Plage de ports 6000 - 6500 pour Windows 2012 R2 et Exchange 2013
  - Plage de ports 49152 - 65536 pour Windows 2019

> Pour identifier la plage de ports, exécutez les commandes suivantes :
>
> - netsh int ipv4 show dynamicport tcp
> - netsh int ipv4 show dynamicport udp
> - netsh int ipv6 show dynamicport tcp
> - netsh int ipv6 show dynamicport udp

Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO

Élément	De formation
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	5 GO Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.
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 les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp". Pour plus d'informations sur le dépannage de .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".

Privilèges Exchange Server requis

Pour permettre à SnapCenter d'ajouter un serveur Exchange ou un DAG et d'installer le plug-in SnapCenter pour Microsoft Exchange Server sur un hôte ou un DAG, vous devez configurer SnapCenter avec les informations d'identification d'un utilisateur disposant d'un ensemble minimal de privilèges et d'autorisations.

Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local et d'autorisations de connexion locales sur l'hôte Exchange distant, ainsi que de droits d'administration sur tous les nœuds du DAG. L'utilisateur du domaine requiert les autorisations minimales suivantes :

- Add-MailboxDatabaseCopy
- Démonter-base de données
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase

- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- GET-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:$true
- Montage de la base de données
- New-MailboxDatabase
- New-PublicFolderDatabase
- Supprimer-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Supprimer-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Définir-AdServerSettings
- Set-MailboxDatabase -allofilerestore:$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Configurez GMSA sur Windows Server 2012 ou version ultérieure

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO

Élément	De formation
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	5 GO Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.
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 les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp". Pour plus d'informations sur le dépannage de .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".

Configuration des informations d'identification pour le plug-in SnapCenter pour Windows

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation du module d'extension et des informations d'identification supplémentaires pour effectuer des opérations de protection des données sur les bases de données.

À propos de cette tâche

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Windows. Bien que vous puissiez créer des identifiants pour Windows après le déploiement d'hôtes et l'installation de plug-ins, il est conseillé de créer des identifiants après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

Configurez les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

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.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.

   La fenêtre Credential s'affiche.

4. Dans la page informations d'identification, procédez comme suit :

Pour ce champ…	**Procédez comme ça…**
Nom d'identification	Entrez un nom pour l'identifiant.
Nom d'utilisateur	Entrez le nom d'utilisateur utilisé pour l'authentification. • 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` • 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`
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Authentification	Sélectionnez Windows comme mode d'authentification.

5. Cliquez sur **OK**.

Configurez GMSA sur Windows Server 2012 ou version ultérieure

Windows Server 2012 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

Ce dont vous aurez besoin

- Vous devez disposer d'un contrôleur de domaine Windows Server 2012 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2012 ou version ultérieure, qui est membre du domaine.

Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediely
3. Créez et configurez votre GMSA :
   a. Créez un compte de groupe d'utilisateurs au format suivant :

   ```
    domainName\accountName$
   .. Ajouter des objets d'ordinateur au groupe.
   .. Utilisez le groupe d'utilisateurs que vous venez de créer pour
   créer le GMSA.
   ```

   Par exemple :

   ```
    New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
   -PrincipalsAllowedToRetrieveManagedPassword <group>
   -ServicePrincipalNames <SPN1,SPN2,…>
   .. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
   ```

4. Configurez le GMSA sur vos hôtes :
   a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

   Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Redémarrez votre hôte.

b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`

c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`

5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

   Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

Ajoutez des hôtes et installez le plug-in pour Exchange

Vous pouvez utiliser la page Ajouter un hôte SnapCenter pour ajouter des hôtes Windows. Le plug-in pour Exchange est automatiquement installé sur l'hôte spécifié. Il s'agit de la méthode recommandée pour installer les plug-ins. Vous pouvez ajouter un hôte et installer un plug-in pour un hôte individuel ou un cluster.

Ce dont vous aurez besoin

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, telles que SnapCenter Admin.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Le service de mise en file d'attente des messages doit être en cours d'exécution.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration. Pour plus d'informations, reportez-vous à la section"Configurez le compte de

service géré par groupe sous Windows Server 2012 ou version ultérieure pour Microsoft Exchange Server".

À propos de cette tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.
- Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte ou un cluster individuel.
- Si un nœud Exchange fait partie d'un DAG, vous ne pouvez pas ajouter qu'un seul noeud dans le serveur SnapCenter.
- Si vous installez des plug-ins sur un cluster (Exchange DAG), ils sont installés sur tous les nœuds du cluster, même si certains nœuds ne possèdent pas de bases de données sur des LUN NetApp.

Depuis SnapCenter 4.6, SCE prend en charge la colocation et vous pouvez ajouter un hôte en utilisant les méthodes suivantes :

Ajout d'une opération d'hôte	4.5 et versions antérieures	4.6 et versions ultérieures
Ajoutez un DAG sans IP dans un domaine transversal ou différent	Non pris en charge	Pris en charge
Ajoutez plusieurs groupes de travail IP avec des noms uniques, résidant dans le même domaine ou entre les domaines	Pris en charge	Pris en charge
Ajoutez plusieurs groupes DAG sans IP ou sans IP qui ont les mêmes noms d'hôte et/ou nom de base de données dans le domaine transversal	Non pris en charge	Pris en charge
Ajoutez plusieurs groupes DAG sans IP avec le même nom et le même domaine	Non pris en charge	Pris en charge
Ajoutez plusieurs hôtes autonomes avec le même nom et le même domaine	Non pris en charge	Pris en charge

Le plug-in pour Exchange dépend du package de plug-ins SnapCenter pour Windows et les versions doivent être identiques. Lors de l'installation du plug-in pour Exchange, le module SnapCenter Plug-ins Package pour Windows est sélectionné par défaut et est installé avec le fournisseur de matériel VSS.

Si SnapManager pour Microsoft Exchange Server et SnapDrive pour Windows sont déjà installés, Et que vous souhaitez installer le plug-in pour Exchange sur le même serveur Exchange, vous devez annuler l'enregistrement du fournisseur de matériel VSS utilisé par SnapDrive pour Windows car il est incompatible avec le fournisseur de matériel VSS installé avec le module Plug-in pour Exchange et le module de plug-ins SnapCenter pour Windows. Pour plus d'informations, voir "Comment enregistrer manuellement le fournisseur de matériel Data ONTAP VSS".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.

2. Vérifiez que **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, procédez comme suit :

Pour ce champ…	Procédez comme ça…
Type d'hôte	Sélectionnez **Windows** comme type d'hôte. SnapCenter Server ajoute l'hôte, puis installe le plug-in pour Windows sur l'hôte et le plug-in pour Exchange s'ils ne sont pas déjà installés. Le plug-in pour Windows et le plug-in pour Exchange doivent être de la même version. Si une version différente de Plug-in pour Windows était déjà installée, SnapCenter met à jour la version dans le cadre de l'installation.

Pour ce champ…	Procédez comme ça…
Nom d'hôte	Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le nom de domaine complet (FQDN). Une adresse IP n'est prise en charge pour les hôtes de domaine non approuvés que si elle résout le FQDN. Si vous ajoutez un hôte à l'aide de SnapCenter et qu'il fait partie d'un sous-domaine, vous devez fournir le FQDN. Vous pouvez saisir des adresses IP ou le FQDN de l'une des adresses suivantes : • Hôte autonome • DAG Exchange Pour un DAG Exchange, vous pouvez : ◦ Ajoutez un DAG en indiquant le nom du DAG, l'adresse IP du DAG, le nom du noeud ou l'adresse IP du noeud. ◦ Ajoutez le cluster DAG sans IP en fournissant l'adresse IP ou le FQDN de l'un des nœuds du cluster DAG. ◦ Ajoutez un DAG sans IP qui réside dans le même domaine ou dans un domaine différent. Vous pouvez également ajouter plusieurs groupes de travail IP/IP moins avec le même nom, mais des domaines différents. ⓘ Pour un hôte autonome ou un DAG Exchange (cross-domain ou même domaine), il est recommandé de fournir un FQDN ou l'adresse IP de l'hôte ou du DAG.

Pour ce champ…	Procédez comme ça…
Informations d'identification	Sélectionnez le nom d'identification que vous avez créé ou créez les nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus d'informations, reportez-vous à la section informations sur la création d'informations d'identification. Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom d'identification que vous avez spécifié. Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

   Lorsque vous sélectionnez Plug-in pour Exchange, le plug-in SnapCenter pour Microsoft SQL Server est automatiquement désélectionné. Microsoft recommande que SQL Server et Exchange Server ne soient pas installés sur le même système en raison de la quantité de mémoire utilisée et de toute autre utilisation des ressources requise par Exchange.

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ…	Procédez comme ça…
Port	Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut. Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.

Pour ce champ…	Procédez comme ça…
Chemin d'installation	Le chemin par défaut est `C:\Program Files\NetApp\SnapCenter`. Vous pouvez éventuellement personnaliser le chemin.
Ajoutez tous les hôtes dans le DAG	Cochez cette case lorsque vous ajoutez un DAG.
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	Cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in. Indiquez le nom GMSA dans le format suivant : *domainName\accountName$*. GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.

7. Cliquez sur **soumettre**.

   Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour déterminer s'il répond aux conditions requises pour installer le plug-in. Si la configuration minimale requise n'est pas respectée, les messages d'erreur ou d'avertissement appropriés s'affichent.

   Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à `C:\Program Files\NetApp\SnapCenter` WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.

   Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Surveillez la progression de l'installation.

Installez le plug-in pour Exchange à partir de l'hôte SnapCenter Server à l'aide des applets de commande PowerShell

Vous devez installer le plug-in pour Exchange à partir de l'interface utilisateur graphique de SnapCenter. Si vous ne souhaitez pas utiliser l'interface graphique, vous pouvez utiliser les applets de commande PowerShell sur l'hôte SnapCenter Server ou sur un

hôte distant.

Ce dont vous aurez besoin

- Le serveur SnapCenter doit avoir été installé et configuré.
- Vous devez être un administrateur local sur l'hôte ou un utilisateur disposant de privilèges d'administration.
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations de plug-in, d'installation et de désinstallation, telles que SnapCenter Admin.
- Vous devez avoir vérifié les conditions d'installation requises et les types de configurations prises en charge avant d'installer le plug-in pour Exchange.
- L'hôte sur lequel vous souhaitez installer le plug-in pour Exchange doit être un hôte Windows.

Étapes

1. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande *Open-SmConnection*, puis saisissez vos informations d'identification.
2. Ajoutez l'hôte sur lequel vous souhaitez installer le plug-in pour Exchange à l'aide de l'applet de commande *Add-SmHost* avec les paramètres requis.

   Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter au "Guide de référence de l'applet de commande du logiciel SnapCenter".

   L'hôte peut être un hôte autonome ou un DAG. Si vous spécifiez un DAG, le paramètre *-IsDAG* est requis.

3. Installez le plug-in pour Exchange à l'aide de l'applet de commande *Install-SmHostPackage* avec les paramètres requis.

   Cette commande installe le plug-in pour Exchange sur l'hôte spécifié, puis enregistre le plug-in avec SnapCenter.

Installez le plug-in SnapCenter pour l'échange silencieusement à partir de la ligne de commande

Vous devez installer le plug-in pour Exchange à partir de l'interface utilisateur SnapCenter. Cependant, si vous ne pouvez pas pour une raison quelconque, vous pouvez exécuter le programme d'installation de Plug-in pour Exchange sans surveillance en mode silencieux à partir de la ligne de commande Windows.

Ce dont vous aurez besoin

- Vous devez avoir sauvegardé vos ressources Microsoft Exchange Server.
- Vous devez avoir installé les modules du plug-in SnapCenter.
- Vous devez supprimer la version antérieure du plug-in SnapCenter pour Microsoft SQL Server avant de procéder à l'installation.

  Pour plus d'informations, voir "Comment installer un plug-in SnapCenter manuellement et directement à partir de l'hôte du plug-in".

Étapes

1. Vérifiez si le dossier *C:\temp* existe sur l'hôte du plug-in et que l'utilisateur connecté dispose d'un accès complet.
2. Téléchargez le plug-in SnapCenter pour Microsoft Windows depuis le site *C:\ProgramData\NetApp\SnapCenter\Package* Repository.

   Ce chemin est accessible à partir de l'hôte sur lequel le serveur SnapCenter est installé.

3. Copiez le fichier d'installation sur l'hôte sur lequel vous souhaitez installer le plug-in.
4. À partir d'une invite de commande Windows sur l'hôte local, accédez au répertoire dans lequel vous avez enregistré les fichiers d'installation du plug-in.
5. Entrez la commande suivante pour installer le remplacement des variables par vos données :

   _Snapcenter_Windows_host_plugin.exe"/muet /debuglog"<Debug_Log_Path>" /log"<Log_Path>« BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLSCE=« Install_Directory_Path> » EPBI_SEREACCOUNT=<SERVICONTAP__PRODUCT_install_SICMADE>

   Par exemple :

   _C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_Windows_host_plugin.exe »/Silent /debulog« C:\HPPSCSQL_Install.log » /log« C:\temp » BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR=« C:\Program Files\utilisateur_d'installation_de_HP_SICentrer=ISPs_SICentrer_SICentrer=s_SICentrer_SICentrer_SICentrer=s_SICentrer_SICentrer_SICentrer=s_SICentrer_SICentrer=s

   Tous les paramètres transmis lors de l'installation du plug-in pour Exchange sont sensibles à la casse.

   a. */muet /debuglog"C:\Installdebug.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Program Files" BI_SERVICEACCOUNT=DEMO\Administrator BI_SERVICEPWD=Netapp1! ISFeatureInstall=HPPW,SCW*

      Entrez les valeurs suivantes pour les variables :

Variable	Valeur
/debuglog »<Debug_Log_Path>	Spécifiez le nom et l'emplacement du fichier journal du programme d'installation de la suite, comme dans l'exemple suivant : *Setup.exe /debuglog"C:\PathToLog\setupexe.log*
BI_SNAPCENTER_PORT	Spécifiez le port sur lequel SnapCenter communique avec SMCore.
SUITE_INSTALLDIR	Spécifiez le répertoire d'installation du module de plug-in hôte.
BI_SERVICEACCOUNT	Spécifiez le compte de service Web SnapCenter Plug-in pour Microsoft Windows.

Variable	Valeur
BI_SERVICEPWD	Spécifiez le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows.
Installation de ISFeatureInstall	Spécifier la solution à déployer par SnapCenter sur un hôte distant

6. Surveillez le planificateur de tâches Windows, le fichier journal d'installation principal *C:\Installdebug.log* et les fichiers d'installation supplémentaires dans *C:\Temp*.
7. Surveillez le répertoire *%temp%* pour vérifier si les programmes d'installation *msiexe.exe* installent le logiciel sans erreur.

> L'installation du plug-in pour Exchange enregistre le plug-in sur l'hôte et non sur le serveur SnapCenter. Vous pouvez enregistrer le plug-in sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Une fois l'hôte ajouté, le plug-in est automatiquement découvert.

Contrôler l'état d'installation du module d'extension SnapCenter

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

- En cours
- Terminé avec succès
- Échec
- Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
- En file d'attente

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, pour filtrer la liste de manière à ce que seules les opérations d'installation du plug-in soient répertoriées, procédez comme suit :
   a. Cliquez sur **Filtrer**.
   b. Facultatif : spécifiez les dates de début et de fin.
   c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.

d. Dans le menu déroulant État, sélectionnez l'état de l'installation.

e. Cliquez sur **appliquer**.

4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Configurer le certificat CA

Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "Comment générer un fichier CSR de certificat CA".

> Si vous possédez le certificat de l'autorité de certification pour votre domaine (*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier** > **Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root** > **certificats – ordinateur local** > **autorités de certification racines de confiance** > **certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches** > **Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant…	Procédez comme suit…
Importer une clé privée	Sélectionnez l'option **Oui**, importez la clé privée, puis cliquez sur **Suivant**.
Importer le format de fichier	N'apportez aucune modification ; cliquez sur **Suivant**.
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur **Suivant**.
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur **Terminer** pour lancer l'importation.

Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : *.pfx, *.p12 et *.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
   a. Double-cliquez sur le certificat.
   b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
   c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
   d. Copiez les caractères hexadécimaux de la zone.
   e. Supprimez les espaces entre les nombres hexadécimaux.

      Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :
   a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

      Get-ChildItem -Path Cert:\Localmachine\My

   b. Copiez l'empreinte.

Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Par exemple :

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associez le certificat récemment installé aux services du plug-in hôte
   Windows, en exécutant les commandes suivantes :
   ```

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid"
   ```

   Par exemple :

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
   appid="$guid"
   ```

Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

Ce dont vous aurez besoin

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande run *set-SmCertificateSettings*.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de *get-SmCertificateSettings*.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter au "Guide de référence de l'applet de commande du logiciel SnapCenter".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.

2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

Après la fin

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

- Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
- Indique que le certificat CA a été validé avec succès.
- Indique que le certificat CA n'a pas pu être validé.
- indique que les informations de connexion n'ont pas pu être récupérées.

> Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

Configurez SnapManager 7.x pour Exchange et SnapCenter afin qu'ils coexistent

Pour permettre au plug-in SnapCenter pour Microsoft Exchange Server de coexister avec SnapManager pour Microsoft Exchange Server, vous devez installer le plug-in SnapCenter pour Microsoft Exchange Server sur le même serveur Exchange sur lequel SnapManager pour Microsoft Exchange Server est installé, désactiver les planifications SnapManager pour Exchange, Et configurer de nouveaux planifications et de nouvelles sauvegardes à l'aide du plug-in SnapCenter pour Microsoft Exchange Server.

Ce dont vous aurez besoin

- SnapManager pour Microsoft Exchange Server et SnapDrive pour Windows sont déjà installés. De plus, SnapManager pour les sauvegardes Microsoft Exchange Server est présent sur le système et dans le répertoire SnapInfo.
- Vous devez avoir supprimé ou récupéré les sauvegardes effectuées par SnapManager pour Microsoft Exchange Server dont vous n'avez plus besoin.
- Vous devez avoir suspendu ou supprimé tous les programmes créés par SnapManager pour Microsoft Exchange Server à partir du planificateur Windows.
- Le plug-in SnapCenter pour Microsoft Exchange Server et SnapManager pour Microsoft Exchange Server peuvent coexister sur le même serveur Exchange, mais vous ne pouvez pas mettre à niveau les installations SnapManager existantes pour Microsoft Exchange Server vers SnapCenter.

  SnapCenter ne propose pas d'option de mise à niveau.

- SnapCenter ne prend pas en charge la restauration des bases de données Exchange à partir de SnapManager pour sauvegarde Microsoft Exchange Server.

  Si vous ne désinstallez pas SnapManager pour Microsoft Exchange Server après l'installation du plug-in

SnapCenter pour Microsoft Exchange Server et que vous souhaitez restaurer une sauvegarde SnapManager pour Microsoft Exchange Server, vous devez effectuer des étapes supplémentaires.

Étapes

1. En utilisant PowerShell sur tous les nœuds DAG, déterminez si SnapDrive pour Windows VSS Hardware Provider est enregistré : *vssadmin list fournisseurs*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
   Version: 7. 1. 4. 6845
```

2. A partir du répertoire SnapDrive, désenregistrez le fournisseur de matériel VSS à partir de SnapDrive pour Windows : *navssprv.exe -r service –u*
3. Vérifiez que le fournisseur de matériel VSS a été supprimé : *vssadmin list fournisseurs*
4. Ajoutez l'hôte Exchange à SnapCenter, puis installez le plug-in SnapCenter pour Microsoft Windows et le plug-in SnapCenter pour Microsoft Exchange Server.
5. Dans le répertoire Plug-in SnapCenter pour Microsoft Windows de tous les nœuds DAG, vérifiez que le fournisseur de matériel VSS est enregistré : *vssadmin list fournisseurs*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. Arrêtez les planifications de sauvegarde SnapManager pour Microsoft Exchange Server.
7. À l'aide de l'interface graphique SnapCenter, créez des sauvegardes à la demande, configurez des sauvegardes planifiées et configurez les paramètres de conservation.
8. Désinstallez SnapManager pour Microsoft Exchange Server.

   Si vous ne désinstallez pas SnapManager pour Microsoft Exchange Server maintenant et ultérieurement souhaitez restaurer une sauvegarde SnapManager pour Microsoft Exchange Server :

   a. Annuler l'enregistrement du plug-in SnapCenter pour Microsoft Exchange Server à partir de tous les nœuds DAG : *navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

b. Dans le répertoire *C:\Program Files\NetApp\SnapDrive*, enregistrez SnapDrive pour Windows sur tous les nœuds du DAG : *navssprv.exe -r service -a hostname\\username -p password*

Informations sur le copyright

Copyright © 2024 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.