Préparez-vous à installer le plug-in SnapCenter pour Microsoft SQL Server

SnapCenter Software 5.0

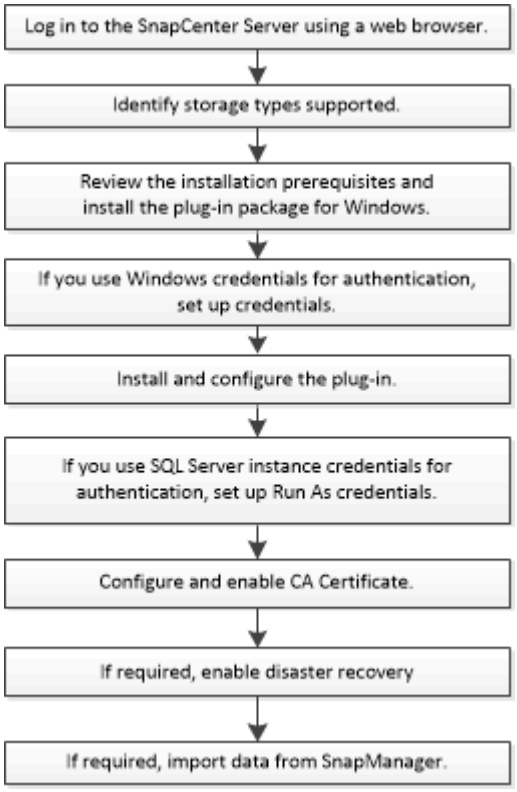
NetApp
July 18, 2024

Sommaire

Préparez-vous à installer le plug-in SnapCenter pour Microsoft SQL Server

Workflow d'installation pour le plug-in SnapCenter pour Microsoft SQL Server

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



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

Avant d'ajouter un hôte et d'installer les packages de plug-ins, vous devez respecter toutes les exigences.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous devez disposer d'un utilisateur disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- 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 sysadmin sur le serveur SQL.

  Le plug-in SnapCenter pour Microsoft SQL Server utilise l'infrastructure VDI Microsoft, qui requiert l'accès sysadmin.

"Article 2926557 du support Microsoft : les opérations de sauvegarde et de restauration VDI SQL Server nécessitent des privilèges sysadmin"

- 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 SnapManager pour Microsoft SQL Server est installé, vous devez avoir arrêté ou désactivé le service et les programmes.

  Si vous envisagez d'importer des tâches de sauvegarde ou de clonage dans SnapCenter, ne désinstallez pas SnapManager pour Microsoft SQL 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 court 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>

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, consultez le "Matrice d'interopérabilité NetApp".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
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.

Élément	De formation
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, consultez le "Matrice d'interopérabilité NetApp". Pour . Informations de dépannage spécifiques au RÉSEAU, voir "La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."

Configurer les informations d'identification pour le progiciel de plug-ins 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 des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

Avant de commencer

- Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.
- Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.
- Authentification SQL sur les hôtes Windows

  Vous devez configurer les informations d'identification SQL après l'installation des plug-ins.

  Si vous déployez le plug-in SnapCenter pour Microsoft SQL Server, vous devez configurer les informations d'identification SQL après l'installation des plug-ins. Configurez les informations d'identification d'un utilisateur avec les autorisations SQL Server sysadmin.

  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 ou la détection des ressources.

Étapes

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

3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ…	Procédez comme ça…
Nom d'identification	Entrez un nom pour l'identifiant.
Nom d'utilisateur/Mot de passe	Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification. • Administrateur de domaine Spécifiez l'administrateur de domaine 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 pour le champ Nom d'utilisateur est : `UserName` N'utilisez pas de guillemets (") ou de contre-coches (') dans les mots de passe. Vous ne devez pas utiliser moins de (<) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins<!10, moins dix<!, contre-recul 12.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser. Si vous sélectionnez le mode d'authentification SQL, vous devez également spécifier l'instance de serveur SQL et l'hôte où se trouve l'instance SQL.

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

Configurer les informations d'identification d'une ressource SQL Server individuelle

Vous pouvez configurer les informations d'identification pour exécuter des tâches de protection des données sur des ressources SQL Server individuelles pour chaque utilisateur. Bien que vous puissiez configurer les informations d'identification globalement, vous pouvez ne le faire que pour une ressource particulière.

Description de la tâche

- Si vous utilisez des informations d'identification Windows pour l'authentification, vous devez configurer vos informations d'identification avant d'installer les plug-ins.

  Toutefois, si vous utilisez une instance SQL Server pour l'authentification, vous devez ajouter les informations d'identification après l'installation des plug-ins.

- Si vous avez activé l'authentification SQL lors de la configuration des informations d'identification, l'instance découverte ou la base de données s'affiche avec une icône de cadenas rouge.

  Si l'icône de cadenas apparaît, vous devez spécifier les informations d'identification de l'instance ou de la base de données pour pouvoir ajouter l'instance ou la base de données à un groupe de ressources.

- Vous devez attribuer ces informations d'identification à un utilisateur de contrôle d'accès basé sur des rôles (RBAC) sans accès sysadmin dans les conditions suivantes :
  - Les informations d'identification sont affectées à une instance SQL.
  - L'instance ou l'hôte SQL est affecté à un utilisateur RBAC.

    L'utilisateur doit disposer à la fois des privilèges de groupe de ressources et de sauvegarde.

Étape 1 : ajout et configuration des informations d'identification

1. Dans le volet de navigation de gauche, sélectionnez **Paramètres**.
2. Dans la page Paramètres, sélectionnez **informations d'identification**.
   a. Pour ajouter une nouvelle information d'identification, sélectionnez **Nouveau**.
   b. Dans la page informations d'identification, configurez les informations d'identification :

Pour ce champ…	Procédez comme ça…
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ…	Procédez comme ça…
Nom d'utilisateur	Entrez le nom d'utilisateur utilisé pour l'authentification SQL Server. • 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 **Username** sont : ◦ *NetBIOS\username* ◦ *Domain FQDN\username* • Administrateur local (pour les 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 pour le champ **Nom d'utilisateur** est : *nom_utilisateur*
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification SQL Server. Vous pouvez également choisir l'authentification Windows si l'utilisateur Windows dispose de privilèges sysadmin sur le serveur SQL.
Hôte	Sélectionnez l'hôte.
Instance SQL Server	Sélectionnez l'instance SQL Server.

c. Sélectionnez **OK** pour ajouter les informations d'identification.

Étape 2 : configurer les instances

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**.
2. Dans la page Ressources, sélectionnez **instance** dans la liste **Affichage**.
   a. Sélectionnez [icône de filtre], puis sélectionnez le nom d'hôte pour filtrer les instances.
   b. Sélectionnez [icône de filtre] pour fermer le volet de filtre.
3. Dans la page protection d'instance, protégez l'instance et, si nécessaire, sélectionnez **configurer les informations d'identification**.

   Si l'utilisateur connecté au serveur SnapCenter n'a pas accès au plug-in SnapCenter pour Microsoft SQL Server, alors l'utilisateur doit configurer les informations d'identification.

   L'option d'informations d'identification ne s'applique pas aux bases de données et aux groupes de disponibilité.

4. Sélectionnez **Actualiser les ressources**.

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.

Avant de commencer

- 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,…>
.. Exécutez `Get-ADServiceAccount` la commande 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 le 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.

Installez le plug-in SnapCenter pour Microsoft SQL Server

Ajoutez des hôtes et installez le package de plug-ins SnapCenter pour Windows

Vous devez utiliser la page SnapCenter **Ajouter hôte** pour ajouter des hôtes et installer le module de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants.

Avant de commencer

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré, vous devez désactiver l'UAC sur l'hôte.
- Vous devez vous assurer que le service de mise en file d'attente des messages est en cours d'exécution.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

  "Configurez le compte de service géré par groupe sous Windows Server 2012 ou version ultérieure pour

SQL"

Description de la 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 les modules d'extension pour un hôte individuel ou pour un cluster. Si vous installez les plug-ins sur un cluster ou Windows Server Failover Clustering (WSFC), les plug-ins sont installés sur tous les nœuds du cluster.

Pour plus d'informations sur la gestion des hôtes, reportez-vous à la section "Gérer les hôtes".

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Sélectionnez **Ajouter**.
4. Dans la page hôtes, procédez comme suit :

Pour ce champ…	Procédez comme ça…
Type d'hôte	Sélectionnez Windows comme type d'hôte. Le serveur SnapCenter ajoute l'hôte, puis installe le plug-in pour Windows si le plug-in n'est pas déjà installé sur l'hôte. Si vous sélectionnez l'option Microsoft SQL Server sur la page Plug-ins, le serveur SnapCenter installe le plug-in pour SQL Server.
Nom d'hôte	Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. L'adresse IP n'est prise en charge pour les hôtes de domaine non approuvés que si elle résout le FQDN. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN. Vous pouvez entrer les adresses IP ou FQDN de l'un des éléments suivants : • Hôte autonome • WSFC si vous ajoutez un hôte à l'aide de SnapCenter et que l'hôte fait partie d'un sous-domaine, vous devez fournir le FQDN.

Pour ce champ…	Procédez comme ça…
Informations d'identification	Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des 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.

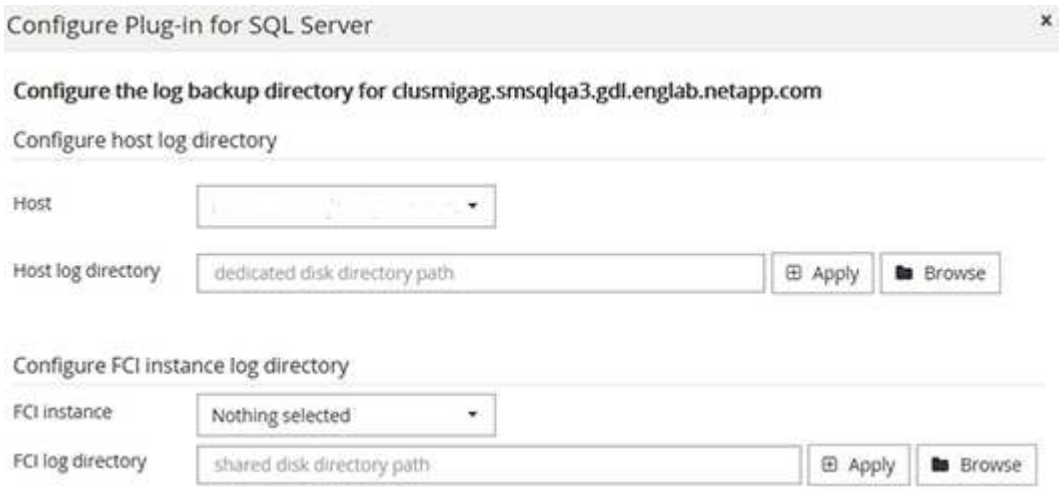
5. Dans la section **Select Plug-ins to Install**, sélectionnez les plug-ins à installer.
6. Sélectionnez **plus d'options**.

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.
Chemin d'installation	Le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez éventuellement personnaliser le chemin.
Ajoutez tous les hôtes du cluster	Cochez cette case pour ajouter tous les nœuds du cluster dans un WSFC ou un groupe de disponibilité SQL. Vous devez ajouter tous les nœuds du cluster en cochant la case de cluster appropriée dans l'interface graphique si vous souhaitez gérer et identifier plusieurs groupes de disponibilité SQL disponibles dans un cluster.

Pour ce champ…	Procédez comme ça…
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 au format suivant : domainname\accountName$. Si l'hôte est ajouté avec GMSA et si le GMSA dispose de privilèges d'ouverture de session et d'administrateur système, le GMSA sera utilisé pour se connecter à l'instance SQL.

7. Sélectionnez **soumettre**.
8. Pour le plug-in SQL, sélectionnez l'hôte pour configurer le répertoire du journal.
   a. Sélectionnez **Configure log Directory** et dans la page Configure host log Directory, sélectionnez **Browse** et procédez comme suit :

      Seules les LUN NetApp (disques) sont répertoriées pour être sélectionnées. SnapCenter sauvegarde et réplique le répertoire journal de l'hôte dans le cadre de l'opération de sauvegarde.



      i. Sélectionnez la lettre de lecteur ou le point de montage sur l'hôte sur lequel le journal hôte sera stocké.
      ii. Choisissez un sous-répertoire, le cas échéant.
      iii. Sélectionnez **Enregistrer**.
9. Sélectionnez **soumettre**.

Si vous n'avez pas coché la case **Ignorer les contrôles préalables**, l'hôte est validé pour vérifier qu'il répond aux exigences d'installation du plug-in. L'espace disque, RAM, version de PowerShell, . La version du RÉSEAU, l'emplacement (pour les plug-ins Windows) et la version de Java (pour les plug-ins Linux) sont validés en fonction de la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des 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 l'adresse 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.

10. Surveillez la progression de l'installation.

Installez le plug-in SnapCenter pour Microsoft SQL Server sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer le plug-in SnapCenter pour Microsoft SQL Server simultanément sur plusieurs hôtes à l'aide de l'applet de commande Install-SmHostPackage PowerShell.

Avant de commencer

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

Étapes

1. Lancer PowerShell.
2. 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.
3. Installez le plug-in SnapCenter pour Microsoft SQL Server sur plusieurs hôtes distants à l'aide de l'applet de commande Install-SmHostPackage et des 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 à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

   Vous pouvez utiliser l'option -skipprecheck lorsque 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.

4. Saisissez vos informations d'identification pour l'installation à distance.

Installez le plug-in SnapCenter pour Microsoft SQL Server silencieusement à partir de la ligne de commande

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

Avant de commencer

- 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 logiciel du plug-in pour SQL Server depuis 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. Installez le plug-in pour le logiciel SQL Server :

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

   Remplacez les valeurs de paramètre fictif par vos données

   - Debug_Log_Path est le nom et l'emplacement du fichier journal du programme d'installation de la suite.
   - Log_Path est l'emplacement des journaux d'installation des composants du plug-in (SCW, SCSQL et SMCore).
   - Num est le port sur lequel SnapCenter communique avec SMCore
   - Install_Directory_Path est le répertoire d'installation du module d'extension hôte.
   - Domaine\Administrator est le compte de service Web SnapCenter Plug-in pour Microsoft Windows.
   - Mot de passe est le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows.
     ```
     "snapcenter_windows_host_plugin.exe"/silent
     /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
     SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
     BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
     ISFeatureInstall=SCW,SCSQL
     ```

   Tous les paramètres transmis lors de l'installation de Plug-in pour SQL Server sont sensibles à la casse.

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 que les programmes d'installation msiexe.exe installent le logiciel sans erreur.

L'installation du plug-in pour SQL Server 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 de l'installation du plug-in pour SQL Server

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.

Description de la 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 n'a pas pu démarrer en raison d'avertissements
- En file d'

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins 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.

La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$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.

Avant de commencer

- 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 à la "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**.

Une fois que vous avez terminé

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 de l'autorité de certification n'est ni activé ni attribué à l'hôte du plug-in.
- * * Indique que le certificat de l'autorité de certification a été validé avec succès.
- * * Indique que le certificat de l'autorité de certification 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.

Configurer la reprise après incident

Reprise après incident du plug-in SnapCenter pour SQL Server

Lorsque le plug-in SnapCenter pour SQL Server est arrêté, procédez comme suit pour basculer vers un autre hôte SQL et restaurer les données.

Avant de commencer

- L'hôte secondaire doit avoir le même système d'exploitation, l'application et le même nom d'hôte que l'hôte principal.
- Placez le plug-in SnapCenter pour SQL Server sur un autre hôte à l'aide de la page **Ajouter hôte** ou **Modifier hôte**. Voir "Gérer les hôtes" pour plus d'informations.

Étapes

1. Sélectionnez l'hôte dans la page **hosts** pour modifier et installer le plug-in SnapCenter pour SQL Server.
2. (Facultatif) remplacez les fichiers de configuration du plug-in SnapCenter pour SQL Server de la sauvegarde de reprise après sinistre vers la nouvelle machine.
3. Importez les planifications Windows et SQL à partir du dossier du plug-in SnapCenter pour SQL Server à partir de la sauvegarde DR.

Informations associées

Voir la "API de reprise après incident" vidéo.

Stockage de reprise après incident pour le plug-in SnapCenter pour SQL Server

Vous pouvez restaurer le plug-in SnapCenter pour stockage SQL Server en activant le mode DR pour le stockage sur la page Paramètres globaux.

Avant de commencer

- Assurez-vous que les plug-ins sont en mode de maintenance.
- Interrompre la relation SnapMirror/SnapVault "Repousser les relations SnapMirror"
- Reliez le LUN du système secondaire à l'ordinateur hôte avec la même lettre de lecteur.
- Assurez-vous que tous les disques sont connectés à l'aide des mêmes lettres que celles utilisées avant le DR.
- Redémarrez le service serveur MSSQL.
- Assurez-vous que les ressources SQL sont de nouveau en ligne.

Description de la tâche

La reprise après incident n'est pas prise en charge sur les configurations VMDK et RDM.

Étapes

1. Dans la page Paramètres, accédez à **Paramètres** > **Paramètres globaux** > **reprise après sinistre**.
2. Sélectionnez **Activer la récupération après sinistre**.
3. Cliquez sur **appliquer**.
4. Vérifiez si le travail DR est activé ou non en cliquant sur **Monitor** > **Jobs**.

Une fois que vous avez terminé

- Si de nouvelles bases de données sont créées après le basculement, celles-ci seront en mode non-DR.

  Les nouvelles bases de données continueront à fonctionner comme elles l'ont fait avant le basculement.

- Les nouvelles sauvegardes créées en mode DR seront répertoriées sous SnapMirror ou SnapVault (secondaire) sur la page topologie.

  Une icône « i » s'affiche en regard des nouvelles sauvegardes pour indiquer que ces sauvegardes ont été créées en mode DR.

- Vous pouvez supprimer le plug-in SnapCenter pour les sauvegardes SQL Server qui ont été créées pendant le basculement à l'aide de l'interface utilisateur ou de l'applet de commande suivante : `Remove-SmBackup`
- Après le basculement, si vous souhaitez que certaines ressources soient en mode non-DR, utilisez l'applet de commande suivante : `Remove-SmResourceDRMode`

  Pour plus d'informations, reportez-vous au "Guide de référence de l'applet de commande du logiciel SnapCenter".

- Le serveur SnapCenter gère les ressources de stockage individuelles (bases de données SQL) en mode reprise après incident ou autre, mais pas le groupe de ressources avec les ressources de stockage en mode DR ou non.

Rétablissement du plug-in SnapCenter pour le stockage secondaire SQL Server vers le stockage primaire

Une fois le stockage primaire du plug-in SnapCenter pour SQL Server de nouveau en ligne, il est préférable de revenir au stockage primaire.

Avant de commencer

- Placez le plug-in SnapCenter pour SQL Server en mode **Maintenance** à partir de la page hôtes gérés.
- Déconnectez le stockage secondaire de l'hôte et connectez-le au stockage principal.
- Pour revenir au stockage primaire, assurez-vous que la direction de la relation reste identique avant le basculement en effectuant l'opération de resynchronisation inverse.

  Pour conserver les rôles de stockage primaire et secondaire après l'opération de resynchronisation inverse, effectuez à nouveau l'opération de resynchronisation inverse.

  Pour plus d'informations, voir "Resynchronisation inverse des relations du miroir"

- Redémarrez le service serveur MSSQL.
- Assurez-vous que les ressources SQL sont de nouveau en ligne.

> Lors du basculement ou de la restauration du plug-in, l'état global du plug-in n'est pas immédiatement actualisé. L'état global des hôtes et des plug-ins est mis à jour lors de l'opération de mise à jour suivante.

Étapes

1. Dans la page Paramètres, accédez à **Paramètres** > **Paramètres globaux** > **reprise après sinistre**.
2. Désélectionnez **Activer la reprise après sinistre**.
3. Cliquez sur **appliquer**.
4. Vérifiez si le travail DR est activé ou non en cliquant sur **Monitor** > **Jobs**.

Une fois que vous avez terminé

Vous pouvez supprimer le plug-in SnapCenter pour les sauvegardes SQL Server qui ont été créées pendant le basculement à l'aide de l'interface utilisateur ou de l'applet de commande suivante : `Remove-SmDRFailoverBackups`

Informations sur le copyright

Informations sur les marques commerciales