Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA

SnapCenter Software 4.7

NetApp
January 18, 2024

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

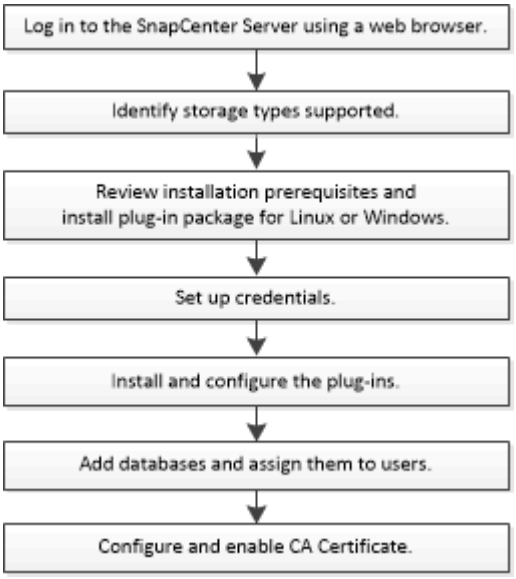
Sommaire

Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA 1
Workflow d'installation du plug-in SnapCenter pour la base de données SAP HANA 1
Conditions préalables pour l'ajout d'hôtes et l'installation du plug-in SnapCenter pour la base de données SAP HANA 1
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows 2
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux 3
Configurer les identifiants du plug-in SnapCenter pour la base de données SAP HANA 4
Configurez GMSA sur Windows Server 2012 ou version ultérieure 7
Installez le plug-in SnapCenter pour les bases de données SAP HANA 8
Configurer le certificat CA 14

Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA

Workflow d'installation du plug-in SnapCenter pour la base de données SAP HANA

Vous devez installer et configurer le plug-in SnapCenter pour base de données SAP HANA si vous souhaitez protéger vos bases de données SAP HANA.



Conditions préalables pour l'ajout d'hôtes et l'installation du plug-in SnapCenter pour la base de données SAP HANA

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour base de données SAP HANA est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 1.8 64 bits sur votre hôte.

  IBM Java n'est pas pris en charge.

- Vous devez avoir installé le terminal interactif de la base de données SAP HANA (client HDBSQL) sur l'hôte.
- Pour Windows, Plug-in Creator Service doit être en cours d'exécution à l'aide de l'utilisateur Windows « LocalSystem », ce qui est le comportement par défaut lorsque Plug-in pour SAP HANA Database est installé en tant qu'administrateur de domaine.
- Pour Windows, les clés de la boutique utilisateur doivent être créées en tant qu'utilisateur SYSTÈME.
- 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 plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in SAP HANA sur les hôtes Windows.

- Pour l'hôte Linux, les clés HDB Secure User Store sont accessibles en tant qu'utilisateur HDBSQL OS.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte de base de données SAP HANA.

Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour base de données SAP HANA sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 1.8 64 bits sur votre hôte Windows.

  "Téléchargements Java pour tous les systèmes d'exploitation"

  "Matrice d'interopérabilité NetApp"

Hôtes Linux

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 1.8 64 bits sur votre hôte Linux.

  "Téléchargements Java pour tous les systèmes d'exploitation"

  "Matrice d'interopérabilité NetApp"

- Pour les bases de données SAP HANA qui s'exécutent sur un hôte Linux, lors de l'installation du plug-in pour base de données SAP HANA, le plug-in SnapCenter pour UNIX est installé automatiquement.

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".

Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux

Avant d'installer le module de plug-ins SnapCenter pour Linux, vous devez connaître certains besoins en espace système hôte de base et en dimensionnement.

Élément	De formation
Systèmes d'exploitation	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) 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	2 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	Java 1.8.x (64 bits)Java Oracle et OpenJDK Flavors Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans /var/opt/snapcenter/spl/etc/spl.properties est définie sur la version JAVA correcte et le chemin correct. Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".

Configurer les identifiants du plug-in SnapCenter pour la base de données SAP HANA

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.

À propos de cette tâche

- Hôtes Linux

  Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

  Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

  Meilleure pratique: bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

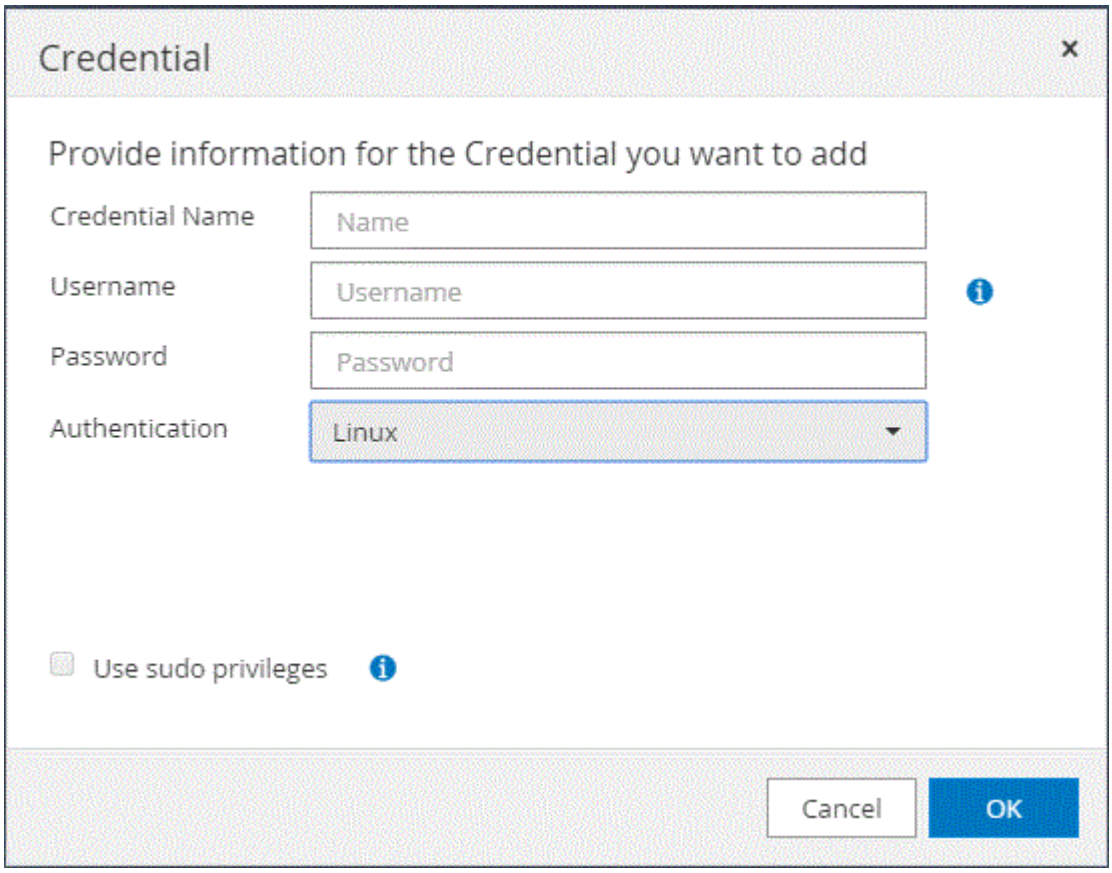
  Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

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

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**.



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	Saisissez un nom pour les informations d'identification.

Pour ce champ…	Procédez comme ça…
Nom d'utilisateur	Entrez le nom d'utilisateur et le mot de passe à utiliser 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* 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.
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utilisez les privilèges sudo	Cochez la case **utiliser privilèges sudo** si vous créez des informations d'identification pour un utilisateur non-root. Applicable uniquement aux utilisateurs Linux.

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.

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.

Installez le plug-in SnapCenter pour les bases de données SAP HANA

Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour 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, 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 ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.

- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- 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 SAP HANA"

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.
- Pour la réplication système SAP HANA afin de détecter les ressources sur les systèmes principal et secondaire, il est recommandé d'ajouter à la fois les systèmes principal et secondaire à l'aide de l'utilisateur root ou sudo.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ…	Procédez comme ça…
Type d'hôte	Sélectionnez le type d'hôte : • Répertoires de base • Linux Le plug-in pour SAP HANA est installé sur l'hôte client HDBSQL et cet hôte peut se trouver sur un système Windows ou Linux.
Nom d'hôte	Entrez le nom d'hôte de communication. 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 FQDN. Vous devez configurer le client HDBSQL et HDBUserStore sur cet hôte.

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 des informations d'identification que vous avez fourni. 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.
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.
Chemin d'installation	Le plug-in pour SAP HANA est installé sur l'hôte client HDBSQL et cet hôte peut se trouver sur un système Windows ou Linux. • Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin. • Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.

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	Pour l'hôte Windows, 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$. 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 vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à 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.

8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

   Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.

   La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

9. Surveillez la progression de l'installation.

   Les fichiers journaux spécifiques à l'installation se trouvent dans /custom_location/snapcenter/logs.

Installez les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer simultanément les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes à l'aide de l'applet de commande Install-SmHostPackage PowerShell.

Ce dont vous aurez besoin

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 sur plusieurs hôtes 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 au "Guide de référence de l'applet de commande du logiciel SnapCenter".

   Vous pouvez utiliser l'option -skipprecheck lorsque vous avez installé les plug-ins manuellement et 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 SAP HANA Database sur des hôtes Linux à l'aide de l'interface de ligne de commandes

Vous devez installer le plug-in SnapCenter pour la base de données SAP HANA à l'aide de l'interface utilisateur de SnapCenter. Si votre environnement n'autorise pas l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter, vous pouvez installer le plug-in pour base de données SAP HANA en mode console ou en mode silencieux à l'aide de l'interface de ligne de commandes.

Ce dont vous aurez besoin

- Vous devez installer le plug-in pour la base de données SAP HANA sur chacun des hôtes Linux sur lesquels réside le client HDBSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour la base de données SAP HANA doit répondre aux exigences des logiciels, bases de données et systèmes d'exploitation qui en dépendent.

  La matrice d'interopérabilité (IMT) contient les dernières informations sur les configurations prises en charge.

  "Matrice d'interopérabilité NetApp"

- Le plug-in SnapCenter pour base de données SAP HANA fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé

SnapCenter sur un hôte Windows.

Étapes

1. Copiez le fichier d'installation du package de plug-ins SnapCenter pour Linux (snapcenter_linux_host_plugin.bin) depuis C:\ProgramData\NetApp\SnapCenter\Package Repository vers l'hôte où vous souhaitez installer le plug-in pour la base de données SAP HANA.

   Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in : `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT spécifie le port de communication SMCore HTTPS.
   - -DSERVER_IP spécifie l'adresse IP du serveur SnapCenter.
   - -DSERVER_HTTPS_PORT spécifie le port HTTPS du serveur SnapCenter.
   - -DUSER_INSTALL_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
   - DINSTALL_LOG_NAME indique le nom du fichier journal.

   ```
   /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
   -DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
   -DUSER_INSTALL_DIR=/opt
   -DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
   -DCHOSEN_FEATURE_LIST=CUSTOM
   ```

4. Modifiez le fichier /<répertoire d'installation>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, puis ajoutez le paramètre PLUGINS_ENABLED = hana:3.0.
5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres requis.

   Les informations relatives aux paramètres pouvant être utilisés avec la commande 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".

Contrôler l'état de l'installation du plug-in pour SAP HANA

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"
   ```

Configurez le certificat d'autorité de certification pour le service de plug-ins SnapCenter SAP HANA sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés de plug-ins personnalisé et de son certificat, configurer le certificat de l'autorité de certification, configurer les certificats racine ou intermédiaires sur le magasin de confiance des plug-ins personnalisés et configurer la paire de clés signée par l'autorité de certification sur le magasin de confiance des plug-ins personnalisés avec le service des plug-ins personnalisés SnapCenter pour activer le certificat numérique installé.

Les plug-ins personnalisés utilisent le fichier « keystore.jks », qui se trouve à l'adresse */opt/NetApp/snapcenter/scc/etc* comme magasin de confiance et comme magasin de clés.

Gérer le mot de passe pour le magasin de clés de plug-in personnalisé et l'alias de la paire de clés signée par l'autorité de certification utilisée

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés enfichable personnalisé à partir du fichier de propriétés de l'agent du plug-in personnalisé.

   C'est la valeur correspondant à la clé 'KEYSTORE_PASS'.

2. Modifiez le mot de passe du magasin de clés :

   ```
    keytool -storepasswd -keystore keystore.jks
   . Remplacez le mot de passe de tous les alias des entrées de clé privée
   du magasin de clés par le même mot de passe que celui utilisé pour le
   magasin de clés :
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Procédez de même pour la clé KEYSTORE_PASS dans le fichier *agent.properties*.

3. Redémarrez le service après avoir modifié le mot de passe.

> Le mot de passe du magasin de clés de plug-in personnalisé et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurez les certificats racine ou intermédiaire sur le magasin de confiance du plug-in personnalisé

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée sur le magasin de confiance du plug-in personnalisé.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in : /opt/NetApp/snapcenter/scc/etc
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaire sur le magasin de confiance personnalisé du plug-in.
```

> Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

Configurez la paire de clés signée CA sur un plug-in de stockage en fiducie personnalisé

Vous devez configurer la paire de clés signées CA dans le magasin de confiance personnalisé du plug-in.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in /opt/NetApp/snapcenter/scc/etc
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Répertorier les certificats ajoutés dans le magasin de clés.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

   Le mot de passe de magasin de clés personnalisé par défaut est la valeur du FICHIER KEYSTORE_PASS dans le fichier agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Si le nom d'alias du certificat de l'autorité de certification est
   long et contient de l'espace ou des caractères spéciaux ("*",","),
   remplacez le nom d'alias par un nom simple :
   ```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurez le nom d'alias à partir du certificat CA dans le fichier
agent.properties.
```

Mettez cette valeur à jour par rapport à la clé SCC_CERTIFICATE_ALIAS.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification dans le magasin de confiance personnalisé du plug-in.

Configurez la liste de révocation de certificats (CRL) pour les plug-ins personnalisés SnapCenter

À propos de cette tâche

- Les plug-ins personnalisés SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins personnalisés SnapCenter est opt/NetApp/snapcenter/etc/crl.

Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier agent.properties par rapport à la clé CRL_PATH.

   Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

Configurez le certificat d'autorité de certification pour le service de plug-ins SnapCenter SAP HANA sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés de plug-ins personnalisé et de son certificat, configurer le certificat de l'autorité de certification, configurer les certificats racine ou intermédiaires sur le magasin de confiance des plug-ins personnalisés et configurer la paire de clés signée par l'autorité de certification sur le magasin de confiance des plug-ins personnalisés avec le service des plug-ins personnalisés SnapCenter pour activer le certificat numérique installé.

Les plug-ins personnalisés utilisent le fichier *keystore.jks*, qui se trouve à l'adresse *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* comme magasin de confiance et magasin de clés.

Gérer le mot de passe pour le magasin de clés de plug-in personnalisé et l'alias de la paire de clés signée par l'autorité de certification utilisée

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés enfichable personnalisé à partir du fichier de propriétés de l'agent du plug-in personnalisé.

   C'est la valeur correspondant à la clé *KEYSTORE_PASS*.

2. Modifiez le mot de passe du magasin de clés :

   keytool -storepasswd -keystore keystore.jks

> Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

   keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks

   Procédez de même pour la clé KEYSTORE_PASS dans le fichier *agent.properties*.

4. Redémarrez le service après avoir modifié le mot de passe.

> Le mot de passe du magasin de clés de plug-in personnalisé et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurez les certificats racine ou intermédiaire sur le magasin de confiance du plug-in personnalisé

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée sur le magasin de confiance du plug-in personnalisé.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

   keytool -list -v -keystore keystore.jks

4. Ajouter un certificat racine ou intermédiaire :

   Keytool -import -trucacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaire sur le magasin de confiance personnalisé du plug-in.

> Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

Configurez la paire de clés signée CA sur un plug-in de stockage en fiducie personnalisé

Vous devez configurer la paire de clés signées CA dans le magasin de confiance personnalisé du plug-in.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Localisez le fichier *keystore.jks*.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

keytool -list -v -keystore keystore.jks

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

   Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS

5. Répertorier les certificats ajoutés dans le magasin de clés.

   keytool -list -v -keystore keystore.jks

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

   Le mot de passe de magasin de clés personnalisé par défaut est la valeur du FICHIER KEYSTORE_PASS dans le fichier agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configurez le nom d'alias à partir du certificat CA dans le fichier *agent.properties*.

   Mettez cette valeur à jour par rapport à la clé SCC_CERTIFICATE_ALIAS.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification dans le magasin de confiance personnalisé du plug-in.

Configurez la liste de révocation de certificats (CRL) pour les plug-ins personnalisés SnapCenter

À propos de cette tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section "Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter".
- Les plug-ins personnalisés SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins personnalisés SnapCenter est *'C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\crl'*.

Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier *agent.properties* par rapport à la clé CRL_PATH.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

   Les certificats entrants seront vérifiés pour chaque CRL.

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.

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.