Installation du plug-in SnapCenter pour la base de données Oracle

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-49/protect-sco/install-snapcenter-plug-in-for-oracle-workflow.html on September 26, 2025. Always check docs.netapp.com for the latest.

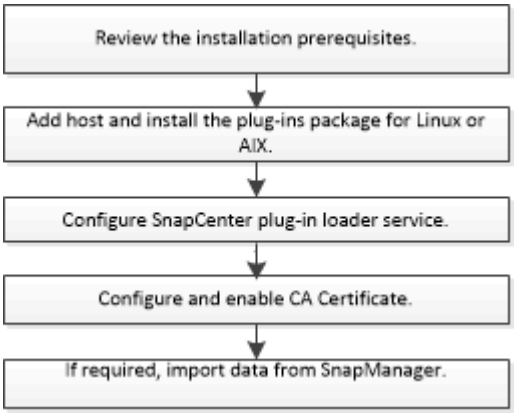
Sommaire

Installation du plug-in SnapCenter pour la base de données Oracle . . . 1
Workflow d'installation du plug-in SnapCenter pour Oracle Database . . . 1
Conditions préalables pour l'ajout d'hôtes et l'installation de Plug-ins Package pour Linux ou AIX . . . 1
Configuration requise pour l'hôte Linux . . . 2
Configuration requise pour l'hôte AIX . . . 5
Configurez les informations d'identification . . . 7
Configurer les informations d'identification d'une base de données Oracle . . . 9
Ajoutez des hôtes et installez Plug-ins Package pour Linux ou AIX à l'aide de l'interface utilisateur graphique . . . 10
Surveiller l'état de l'installation . . . 14
Autres méthodes d'installation de Plug-ins Package pour Linux ou AIX . . . 14
Installation sur plusieurs hôtes distants à l'aide d'applets de commande . . . 15
Installez-le sur l'hôte du cluster . . . 15
Installez Plug-ins Package pour Linux en mode silencieux . . . 16
Installez le module plug-ins pour AIX en mode silencieux . . . 17
Configurer le service du chargeur enfichable SnapCenter . . . 18
Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux . . . 21
Gérer le mot de passe pour le magasin de clés SPL et l'alias de la paire de clés signée CA utilisée . . . 21
Configurez les certificats racine ou intermédiaire sur le magasin de confiance SPL . . . 22
Configurez la paire de clés signée CA sur le magasin de confiance SPL . . . 22
Configurer la liste de révocation de certificats (CRL) pour SPL . . . 23
Activez les certificats CA pour les plug-ins . . . 24
Importation des données depuis SnapManager for Oracle et SnapManager for SAP vers SnapCenter . . . 24
Configurations prises en charge pour l'importation de données . . . 25
Ce qui est importé dans SnapCenter . . . 25
Ce qui n'est pas importé dans SnapCenter . . . 28
Préparez-vous à importer des données . . . 28
Importer des données . . . 29

Installation du plug-in SnapCenter pour la base de données Oracle

Workflow d'installation du plug-in SnapCenter pour Oracle Database

Vous devez installer et configurer le plug-in SnapCenter pour la base de données Oracle si vous souhaitez protéger les bases de données Oracle.



Conditions préalables pour l'ajout d'hôtes et l'installation de Plug-ins Package pour Linux ou AIX

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 avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.

  Le plug-in SnapCenter pour base de données Oracle peut être installé par un utilisateur non root. Cependant, vous devez configurer les privilèges sudo pour que l'utilisateur non-root installe et démarre le processus de plug-in. Après l'installation du plug-in, les processus s'exécutent en tant qu'utilisateur non-racine efficace.

- Si vous installez le module de plug-ins SnapCenter pour AIX sur un hôte AIX, vous devez avoir résolu manuellement les liens symboliques au niveau du répertoire.

  Le module de plug-ins SnapCenter pour AIX résout automatiquement le lien symbolique au niveau du fichier, mais pas les liens symboliques au niveau du répertoire pour obtenir le chemin absolu JAVA_HOME.

- Créez des informations d'identification avec le mode d'authentification sous Linux ou AIX pour l'utilisateur d'installation.
- Vous devez avoir installé Java 1.8.x ou Java 11, 64 bits, sur votre hôte Linux ou AIX.

  Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux.

Pour plus d'informations sur le téléchargement DE JAVA, voir :

- "Téléchargements Java pour tous les systèmes d'exploitation"
- "IBM Java pour AIX"

- Pour les bases de données Oracle qui s'exécutent sur un hôte Linux ou AIX, installez le plug-in SnapCenter pour base de données Oracle et le plug-in SnapCenter pour UNIX.

> Vous pouvez utiliser le plug-in pour Oracle Database afin de gérer également les bases de données Oracle pour SAP. Cependant, l'intégration de SAP BR*Tools n'est pas prise en charge.

- Si vous utilisez Oracle Database 11.2.0.3 ou une version ultérieure, vous devez installer le correctif Oracle 13366202.

> Le mappage UUID dans le fichier /etc/fstab n'est pas pris en charge par SnapCenter.

- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

Configuration requise pour l'hôte Linux

Vous devez vous assurer que l'hôte répond à la configuration requise avant d'installer le module de plug-ins SnapCenter pour Linux.

Élément	De formation
Systèmes d'exploitation	• Red Hat Enterprise Linux • Oracle Linux Si vous utilisez une base de données Oracle sur LVM sous Oracle Linux ou Red Hat Enterprise Linux 6.6 ou 7.0, vous devez installer la dernière version de Logical Volume Manager (LVM). • SUSE Linux Enterprise Server (SLES)
RAM minimale pour le plug-in SnapCenter sur l'hôte	2 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) Oracle Java et OpenJDK Flavors • Java 11 (64 bits) Oracle Java et OpenJDK Flavors Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux. 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".

Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux

Les versions SnapCenter 2.0 et ultérieures permettent à un utilisateur non-root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Modifiez le fichier */etc/ssh/sshd_config* pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

  Redémarrez le service sshd après la mise à jour du fichier de configuration.

  Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier /etc/sudoers : '/<crs_home>/bin/olsnodes'

Vous pouvez obtenir la valeur de *crs_Home* à partir du fichier */etc/oracle/olr.loc*.

LINUX_USER est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir le *checksum_Value* à partir du fichier **oracle_checksum.txt**, qui se trouve dans la page *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Si vous avez spécifié un emplacement personnalisé, l'emplacement sera *Custom_path\NetApp\SnapCenter\Package Repository*.

Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

Configuration requise pour l'hôte AIX

Vous devez vous assurer que l'hôte répond aux exigences requises avant d'installer le module de plug-ins SnapCenter pour AIX.

Le plug-in SnapCenter pour UNIX qui fait partie du package de plug-ins SnapCenter pour AIX ne prend pas en charge les groupes de volumes simultanés.

Élément	De formation
Systèmes d'exploitation	AIX 7.1 ou version ultérieure
RAM minimale pour le plug-in SnapCenter sur l'hôte	4 GO
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.

Élément	De formation
Packs logiciels requis	• Java 1.8.x (64 bits) IBM Java • Java 11 (64 bits) IBM Java 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".

Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte AIX

SnapCenter 4.4 et version ultérieure permet à un utilisateur non-root d'installer le module de plug-ins SnapCenter pour AIX et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Modifiez le fichier */etc/ssh/sshd_config* pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

  Redémarrez le service sshd après la mise à jour du fichier de configuration.

  Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx

- /Custom_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Étapes

1. Connectez-vous à l'hôte AIX sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour AIX.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier /etc/sudoers : '/<crs_home>/bin/olsnodes'

Vous pouvez obtenir la valeur de *crs_Home* à partir du fichier */etc/oracle/olr.loc*.

AIX_USER est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir le *checksum_Value* à partir du fichier **oracle_checksum.txt**, qui se trouve dans la page *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Si vous avez spécifié un emplacement personnalisé, l'emplacement sera *Custom_path\NetApp\SnapCenter\Package Repository*.

Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

Configurez les informations d'identification

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 sur des hôtes Linux ou AIX.

À propos de cette tâche

Les informations d'identification sont créées pour l'utilisateur root ou pour un utilisateur non-root disposant de

privilèges sudo pour installer et démarrer le processus de plug-in.

Pour plus d'informations, voir : Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux ou Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte AIX

Meilleure pratique : bien que vous soyez autorisé à créer des informations d'identification 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.

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, entrez les informations d'identification :

Pour ce champ…	Procédez comme ça…
Nom d'identification	Saisissez un nom pour les informations d'identification.
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 du champ Nom d'utilisateur est : *username*

Pour ce champ…	Procédez comme ça…
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser. En fonction du système d'exploitation de l'hôte du plug-in, sélectionnez Linux ou AIX.
Utilisez les privilèges sudo	Cochez la case **utiliser privilèges sudo** si vous créez des informations d'identification pour un utilisateur non-root.

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 sur la page **utilisateur et accès**.

Configurer les informations d'identification d'une base de données Oracle

Vous devez configurer les informations d'identification utilisées pour effectuer des opérations de protection des données sur les bases de données Oracle.

À propos de cette tâche

Consultez les différentes méthodes d'authentification prises en charge pour la base de données Oracle. Pour plus d'informations, reportez-vous à la section "Méthodes d'authentification pour vos informations d'identification".

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, le nom d'utilisateur doit au moins disposer de privilèges de groupe de ressources et de sauvegarde.

Si vous avez activé l'authentification de la base de données Oracle, une icône de cadenas rouge s'affiche dans la vue Ressources. Vous devez configurer les informations d'identification de la base de données pour pouvoir protéger la base de données ou l'ajouter au groupe de ressources pour effectuer des opérations de protection des données.

Si vous spécifiez des détails incorrects lors de la création d'informations d'identification, un message d'erreur s'affiche. Vous devez cliquer sur **Annuler**, puis réessayer.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.
3. Cliquez sur , puis sélectionnez le nom d'hôte et le type de base de données pour filtrer les ressources.

   Vous pouvez ensuite cliquer sur pour fermer le volet de filtre.
4. Sélectionnez la base de données, puis cliquez sur **Paramètres de base de données** > **configurer la base de données**.

5. Dans la section configurer les paramètres de la base de données, dans la liste déroulante **utiliser les informations d'identification existantes**, sélectionnez les informations d'identification qui doivent être utilisées pour effectuer des tâches de protection des données sur la base de données Oracle.

   L'utilisateur Oracle doit disposer des privilèges sysdba.

   Vous pouvez également créer des informations d'identification en cliquant sur .

6. Dans la section configurer les paramètres ASM, dans la liste déroulante **utiliser les informations d'identification existantes**, sélectionnez les informations d'identification qui doivent être utilisées pour exécuter des tâches de protection des données sur l'instance ASM.

   L'utilisateur ASM doit disposer du privilège sysasm.

   Vous pouvez également créer des informations d'identification en cliquant sur .

7. Dans la section configurer les paramètres du catalogue RMAN, dans la liste déroulante **utiliser les informations d'identification existantes**, sélectionnez les informations d'identification qui doivent être utilisées pour effectuer des tâches de protection des données sur la base de données du catalogue Oracle Recovery Manager (RMAN).

   Vous pouvez également créer des informations d'identification en cliquant sur .

   Dans le champ **TNSName**, entrez le nom du fichier TNS (transparent Network Substrand) qui sera utilisé par le serveur SnapCenter pour communiquer avec la base de données.

8. Dans le champ **Preferred RAC Nodes**, indiquez les nœuds RAC (Real application Cluster) préférés pour la sauvegarde.

   Les nœuds préférés peuvent être un ou tous les nœuds de cluster où sont présentes les instances de base de données RAC. L'opération de sauvegarde est déclenchée uniquement sur ces nœuds préférés, par ordre de préférence.

   Dans RAC One Node, un seul nœud est répertorié dans les nœuds préférés, et ce nœud préféré est le nœud où la base de données est actuellement hébergée.

   Après le basculement ou le déplacement de la base de données RAC One Node, l'actualisation des ressources de la page Ressources SnapCenter supprimera l'hôte de la liste **Preferred RAC Nodes** où la base de données était hébergée précédemment. Le nœud RAC où la base de données est déplacée sera répertorié dans **RAC Nodes** et devra être configuré manuellement comme nœud RAC préféré.

   Pour plus d'informations, voir "Nœuds préférés dans la configuration RAC".

9. Cliquez sur **OK**.

Ajoutez des hôtes et installez Plug-ins Package pour Linux ou AIX à l'aide de l'interface utilisateur graphique

Vous pouvez utiliser la page Ajouter un hôte pour ajouter des hôtes, puis installer le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX. Les plug-ins sont automatiquement installés sur les hôtes distants.

À propos de cette tâche

Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour un cluster. Si vous installez le plug-in sur un cluster (Oracle RAC), le plug-in est installé sur tous les nœuds du cluster. Pour Oracle RAC One Node, vous devez installer le plug-in sur les nœuds actif et passif.

Vous devez être affecté à un rôle doté des autorisations d'installation et de désinstallation du plug-in, telles que le rôle d'administrateur SnapCenter.

Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.

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 **Linux** ou **AIX** comme type d'hôte. Le serveur SnapCenter ajoute l'hôte, puis installe le plug-in pour Oracle Database et le plug-in pour UNIX si les plug-ins ne sont pas déjà installés sur l'hôte.
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 FQDN. Vous pouvez entrer les adresses IP ou FQDN de l'un des éléments suivants : • Hôte autonome • N'importe quel nœud dans l'environnement Oracle Real application clusters (RAC) Le nœud VIP ou l'analyse IP n'est pas pris en charge 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 des informations 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.
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 chemin par défaut est */opt/NetApp/snapcenter*. Vous pouvez éventuellement personnaliser le chemin.

Pour ce champ…	Procédez comme ça…
Ajoutez tous les hôtes dans Oracle RAC	Cochez cette case pour ajouter tous les nœuds du cluster dans un RAC Oracle. Dans une configuration Flex ASM, tous les nœuds, qu'il s'agisse d'un nœud Hub ou Leaf, seront ajoutés.
Ignorer les vérifications de préinstallation facultatives	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.

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.

   Le script de vérification préalable ne valide pas l'état du pare-feu du port du plug-in s'il est spécifié dans les règles de rejet du pare-feu.

   Les messages d'erreur ou d'avertissement appropriés s'affichent si les exigences minimales ne sont pas respectées. 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. 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.

   SnapCenter ne prend pas en charge l'algorithme ECDSA.

   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 à l'adresse */Custom_location/snapcenter/logs*.

Résultat

Toutes les bases de données de l'hôte sont automatiquement découvertes et affichées dans la page Ressources. Si rien ne s'affiche, cliquez sur **Actualiser les ressources**.

Surveiller l'état de l'installation

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 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 **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**.

Autres méthodes d'installation de Plug-ins Package pour Linux ou AIX

Vous pouvez également installer manuellement le module Plug-ins pour Linux ou AIX en utilisant les applets de commande ou les interfaces de ligne de commande.

Avant d'installer le plug-in manuellement, vous devez valider la signature du package binaire à l'aide de la clé **snapcenter_public_key.pub** et **snapcenter_linux_host_plugin.bin.bin** située à la position *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Assurez-vous que **OpenSSL 1.0.2g** est installé sur l'hôte sur lequel vous souhaitez installer le plug-in.

Valider la signature du package binaire en exécutant la commande :

- Pour hôte Linux : `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature`

`snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`

- Pour l'hôte AIX : `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

Installation sur plusieurs hôtes distants à l'aide d'applets de commande

Vous devez utiliser l'applet de commande *Install-SmHostPackage* PowerShell pour installer le module de plug-ins SnapCenter pour Linux ou le module de plug-ins SnapCenter pour AIX sur plusieurs hôtes.

Ce dont vous aurez besoin

Vous devez être connecté 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 package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX à l'aide de l'applet de commande *Install-SmHostPackage* et des paramètres requis.

   Vous pouvez utiliser l'option *-skipprecheck* lorsque vous avez déjà installé les plug-ins manuellement et ne voulez pas vérifier si l'hôte répond aux exigences requises pour installer le plug-in.

   Le script de vérification préalable ne valide pas l'état du pare-feu du port du plug-in s'il est spécifié dans les règles de rejet du pare-feu.

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

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".

Installez-le sur l'hôte du cluster

Vous devez installer SnapCenter Plug-ins Package pour Linux ou SnapCenter Plug-ins Package pour AIX sur les deux nœuds de l'hôte cluster.

Chacun des nœuds de l'hôte de cluster a deux adresses IP. L'une des adresses IP sera l'adresse IP publique des nœuds respectifs et la seconde sera l'adresse IP du cluster partagée entre les deux nœuds.

Étapes

1. Installez le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX sur les deux nœuds de l'hôte de cluster.
2. Vérifiez que les valeurs correctes pour les paramètres SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT et SPL_ENABLED_PLUGINS sont spécifiées dans le fichier spl.properties situé à */var/opt/snapcenter/SPL/etc/*.

   Si SPL_ENABLED_PLUGINS n'est pas spécifié dans spl.properties, vous pouvez l'ajouter et attribuer la valeur SCO,SCU.

3. 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.
4. Dans chacun des nœuds, définissez les adresses IP préférées du nœud à l'aide de la commande *set-PreferredHostIPsInStorageExportPolicy* sccli et des paramètres requis.
5. Dans l'hôte SnapCenter Server, ajoutez une entrée pour l'adresse IP du cluster et le nom DNS correspondant dans *C:\Windows\System32\drivers\etc\hosts*.
6. Ajoutez le nœud au serveur SnapCenter à l'aide de l'applet de commande *Add-SmHost* en spécifiant l'adresse IP du cluster pour le nom d'hôte.

Découvrez la base de données Oracle sur le nœud 1 (en supposant que l'adresse IP du cluster est hébergée sur le nœud 1) et créez une sauvegarde de la base de données. En cas de basculement, vous pouvez utiliser la sauvegarde créée sur le nœud 1 pour restaurer la base de données sur le nœud 2. Vous pouvez également utiliser la sauvegarde créée sur le nœud 1 pour créer un clone sur le nœud 2.

En cas de basculement, des volumes, des répertoires et des fichiers seront obsolètes, lorsque d'autres opérations SnapCenter sont en cours d'exécution.

Installez Plug-ins Package pour Linux en mode silencieux

Vous pouvez installer le module de plug-ins SnapCenter pour Linux en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

Ce dont vous aurez besoin

- Vous devez passer en revue les conditions préalables à l'installation du package de plug-ins.
- Vous devez vous assurer que la variable d'environnement D'AFFICHAGE n'est pas définie.

  Si la variable d'environnement D'AFFICHAGE est définie, vous devez annuler l'AFFICHAGE, puis essayer d'installer manuellement le plug-in.

À propos de cette tâche

Vous devez fournir les informations nécessaires à l'installation lors de l'installation en mode console, alors qu'en mode silencieux, vous n'avez pas à fournir d'informations d'installation.

Étapes

1. Téléchargez le module de plug-ins SnapCenter pour Linux à partir de l'emplacement d'installation du serveur SnapCenter.

   Le chemin d'installation par défaut est *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Ce chemin est accessible 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 téléchargé le fichier d'installation.
3. Courez

   ```
   ./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-
   DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
   DUSER_INSTALL_DIR==/opt/custom_path
   ```

4. Modifiez le fichier spl.properties situé à l'adresse */var/opt/snapcenter/spl/etc/* pour ajouter SPL_ENABLED_PLUGINS=SCO,SCU, puis redémarrez le service de chargeur de plug-in SnapCenter.

> L'installation du package plug-ins enregistre les plug-ins sur l'hôte et non sur le serveur SnapCenter. Vous devez enregistrer les plug-ins sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Lors de l'ajout de l'hôte, sélectionnez « aucun » comme identifiant. Une fois l'hôte ajouté, les plug-ins installés sont automatiquement découverts.

Installez le module plug-ins pour AIX en mode silencieux

Vous pouvez installer le module de plug-ins SnapCenter pour AIX en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

Ce dont vous aurez besoin

- Vous devez passer en revue les conditions préalables à l'installation du package de plug-ins.
- Vous devez vous assurer que la variable d'environnement D'AFFICHAGE n'est pas définie.

  Si la variable d'environnement D'AFFICHAGE est définie, vous devez annuler l'AFFICHAGE, puis essayer d'installer manuellement le plug-in.

Étapes

1. Téléchargez le module de plug-ins SnapCenter pour AIX à partir de l'emplacement d'installation du serveur SnapCenter.

   Le chemin d'installation par défaut est *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Ce chemin est accessible 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 téléchargé le fichier d'installation.
3. Courez

   ```
   ./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
   DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
   DUSER_INSTALL_DIR==/opt/custom_path-
   DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
   DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
   ```

4. Modifiez le fichier spl.properties situé à l'adresse */var/opt/snapcenter/spl/etc/* pour ajouter SPL_ENABLED_PLUGINS=SCO,SCU, puis redémarrez le service de chargeur de plug-in SnapCenter.

> L'installation du package plug-ins enregistre les plug-ins sur l'hôte et non sur le serveur SnapCenter. Vous devez enregistrer les plug-ins sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Lors de l'ajout de l'hôte, sélectionnez « aucun » comme identifiant. Une fois l'hôte ajouté, les plug-ins installés sont automatiquement découverts.

Configurer le service du chargeur enfichable SnapCenter

Le service de chargeur de plug-in SnapCenter charge le package de plug-in pour Linux ou AIX afin d'interagir avec le serveur SnapCenter. Le service de chargeur de plug-in SnapCenter est installé lorsque vous installez le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX.

À propos de cette tâche

Après avoir installé le progiciel de plug-ins SnapCenter pour Linux ou le progiciel de plug-ins SnapCenter pour AIX, le service chargeur de plug-in SnapCenter démarre automatiquement. Si le service du chargeur enfichable SnapCenter ne démarre pas automatiquement, vous devez :

- Assurez-vous que le répertoire dans lequel le plug-in fonctionne n'est pas supprimé
- Augmentez l'espace mémoire alloué à la machine virtuelle Java

Le fichier spl.properties, qui se trouve à */Custom_location/NetApp/snapcenter/spl/etc/*, contient les paramètres suivants. Les valeurs par défaut sont attribuées à ces paramètres.

Nom du paramètre	Description
NIVEAU_JOURNAL	Affiche les niveaux de journaux pris en charge. Les valeurs possibles sont TRACE, DEBUG, INFO, WARN, ERROR, ET FATAL.
SPL_PROTOCOL	Affiche le protocole pris en charge par le chargeur SnapCenter Plug-in. Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.
SNAPCENTER_SERVER_PROTOCOL	Affiche le protocole pris en charge par le serveur SnapCenter. Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.
SKIP_JAVAHOME_UPDATE	Par défaut, le service SPL détecte le chemin Java et met à jour LE paramètre JAVA_HOME. Par conséquent, la valeur par défaut est DÉFINIE sur FALSE. Vous pouvez définir LA valeur TRUE si vous souhaitez désactiver le comportement par défaut et corriger manuellement le chemin Java.

Nom du paramètre	Description
SPL_KEYSTORE_PASS	Affiche le mot de passe du fichier keystore. Vous ne pouvez modifier cette valeur que si vous modifiez le mot de passe ou si vous créez un nouveau fichier de magasin de clés.
SPL_PORT	Affiche le numéro de port sur lequel le service du chargeur enfichable SnapCenter est exécuté. Vous pouvez ajouter la valeur si la valeur par défaut est manquante. Vous ne devez pas modifier la valeur après l'installation des modules externes.
SNAPCENTER_SERVER_HOST	Affiche l'adresse IP ou le nom d'hôte du serveur SnapCenter.
CHEMIN_DU_MAGASIN_DE_CLÉS SPL	Affiche le chemin absolu du fichier de magasin de clés.
SNAPCENTER_SERVER_PORT	Affiche le numéro de port sur lequel le serveur SnapCenter s'exécute.
LOGS_MAX_COUNT	Affiche le nombre de fichiers journaux du chargeur de plug-in SnapCenter qui sont conservés dans le dossier */Custom_location/snapcenter/spl/logs*. La valeur par défaut est 5000. Si le nombre est supérieur à la valeur spécifiée, les 5000 derniers fichiers modifiés sont conservés. La vérification du nombre de fichiers est effectuée automatiquement toutes les 24 heures à partir du démarrage du service du chargeur de plug-in SnapCenter. Si vous supprimez manuellement le fichier spl.properties, le nombre de fichiers à conserver est défini sur 9999.
JAVA_HOME	Affiche le chemin absolu du répertoire Java_HOME utilisé pour démarrer le service SPL. Ce chemin est déterminé lors de l'installation et dans le cadre du démarrage de SPL.

Nom du paramètre	Description
LOG_MAX_SIZE	Affiche la taille maximale du fichier journal des travaux. Une fois la taille maximale atteinte, le fichier journal est compressé et les journaux sont écrits dans le nouveau fichier de ce travail.
RETAIN_LOGS_OF_LAST_DAYS	Affiche le nombre de jours jusqu'à lesquels les journaux sont conservés.
ACTIVER_CERTIFICAT_VALIDATION	Affiche TRUE lorsque la validation du certificat CA est activée pour l'hôte. Vous pouvez activer ou désactiver ce paramètre en modifiant le fichier spl.properties ou en utilisant l'interface graphique ou l'applet de commande SnapCenter.

Si l'un de ces paramètres n'est pas affecté à la valeur par défaut ou si vous souhaitez attribuer ou modifier la valeur, vous pouvez modifier le fichier spl.properties. Vous pouvez également vérifier le fichier spl.properties et le modifier pour résoudre tous les problèmes liés aux valeurs qui sont affectées aux paramètres. Après avoir modifié le fichier spl.properties, vous devez redémarrer le service de chargeur de plug-in SnapCenter.

Étapes

1. Effectuez l'une des opérations suivantes, si nécessaire :
   - Démarrer le service du chargeur enfichable SnapCenter en tant qu'utilisateur root :

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl start`
** Arrêtez le service du chargeur enfichable SnapCenter :
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```

     Vous pouvez utiliser l'option -force avec la commande stop pour arrêter le service SnapCenter Plug-in Loader avec force. Cependant, vous devez faire preuve de prudence avant de le faire car il met également fin aux opérations existantes.

   - Redémarrez le service du chargeur Plug-in SnapCenter :

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
** Rechercher l'état du service du chargeur enfichable SnapCenter :
```

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl status`
** Trouver le changement dans le service du chargeur Plug-in
SnapCenter :
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux

Vous devez gérer le mot de passe de la base de stockage de clés SPL et de son certificat, configurer le certificat de l'autorité de certification, configurer les certificats racine ou intermédiaires dans la base de stockage sécurisée SPL et configurer la paire de clés signée de l'autorité de certification dans la base de stockage sécurisée avec le service chargeur de plug-in SnapCenter pour activer le certificat numérique installé.

SPL utilise le fichier « keystore.jks », qui se trouve dans '/var/opt/snapcenter/spl/etc.' en tant que magasin de confiance et clé.

Gérer le mot de passe pour le magasin de clés SPL et l'alias de la paire de clés signée CA utilisée

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés SPL dans le fichier de propriétés SPL.

   C'est la valeur correspondant à la clé 'PL_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>" -keystore keystore.jks
   ```

   Mettez à jour la même chose pour la clé SPL_KEYSTORE_PASS dans le fichier spl.properties.

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

Le mot de passe du magasin de clés SPL 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 SPL

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée dans le stockage de confiance SPL.

Étapes

1. Accédez au dossier contenant le magasin de clés SPL : */var/opt/snapcenter/spl/etc*.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
 keytool -list -v -keystore keystore.jks
. Ajouter un certificat racine ou intermédiaire :
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaire sur le stockage de confiance SPL.
```

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 le magasin de confiance SPL

Vous devez configurer la paire de clés signée CA dans le magasin de confiance SPL.

Étapes

1. Accédez au dossier contenant le magasin de clés de la SPL /var/opt/snapcenter/spl/etc
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
 keytool -list -v -keystore keystore.jks
. Ajoutez le certificat de l'autorité de certification ayant une clé
privée et une clé publique.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Répertorier les certificats ajoutés dans le magasin de clés.
```

```
 keytool -list -v -keystore keystore.jks
. 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.
. 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 du magasin de clés SPL par défaut est la valeur de la clé SPL_KEYSTORE_PASS dans le fichier spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -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 "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurez le nom d'alias à partir du magasin de clés situé dans le
fichier spl.properties.
```

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

4. Redémarrez le service après avoir configuré la paire de clés signée CA dans la boutique de confiance SPL.

Configurer la liste de révocation de certificats (CRL) pour SPL

Vous devez configurer la CRL pour SPL

À propos de cette tâche

- SPL recherche les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour SPL est */var/opt/snapcenter/spl/etc/crl*.

Étapes

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

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 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.

Importation des données depuis SnapManager for Oracle et SnapManager for SAP vers SnapCenter

Importer des données à partir de SnapManager pour Oracle et de SnapManager pour SAP vers SnapCenter vous permet de continuer à utiliser vos données des versions précédentes.

Vous pouvez importer des données de SnapManager for Oracle et de SnapManager for SAP vers SnapCenter

en exécutant l'outil d'importation à partir de l'interface de ligne de commande (interface de ligne de commande hôte Linux).

L'outil d'importation crée des stratégies et des groupes de ressources dans SnapCenter. Les stratégies et les groupes de ressources créés dans SnapCenter correspondent aux profils et opérations effectués à l'aide de ces profils dans SnapManager for Oracle et SnapManager for SAP. L'outil d'importation SnapCenter interagit avec les bases de données du référentiel SnapManager pour Oracle et SnapManager pour SAP et avec la base de données que vous souhaitez importer.

- Récupère tous les profils, plannings et opérations effectués à l'aide des profils.
- Crée une politique de sauvegarde SnapCenter pour chaque opération et chaque planification attachée à un profil.
- Crée un groupe de ressources pour chaque base de données cible.

Vous pouvez exécuter l'outil d'importation en exécutant le script sc-migration situé à l'adresse */opt/NetApp/snapcenter/spl/bin*. Lorsque vous installez le package de plug-ins SnapCenter pour Linux sur l'hôte de base de données que vous souhaitez importer, le script sc-migration est copié dans */opt/NetApp/snapcenter/spl/bin*.

L'importation de données n'est pas prise en charge à partir de l'interface utilisateur graphique SnapCenter.

SnapCenter ne prend pas en charge Data ONTAP fonctionnant en 7-mode. Vous pouvez utiliser l'outil 7-mode transition Tool pour migrer vers un système ONTAP les données et les configurations stockées sur un système exécutant Data ONTAP 7-mode.

Configurations prises en charge pour l'importation de données

Avant d'importer les données de SnapManager 3.4.x pour Oracle et de SnapManager 3.4.x pour SAP vers SnapCenter, nous vous recommandons de connaître les configurations prises en charge par le plug-in SnapCenter pour base de données Oracle.

Les configurations prises en charge par le plug-in SnapCenter pour base de données Oracle sont répertoriées dans le "Matrice d'interopérabilité NetApp".

Ce qui est importé dans SnapCenter

Vous pouvez importer des profils, des plannings et des opérations effectués à l'aide des profils.

Grâce à SnapManager for Oracle et SnapManager for SAP	À SnapCenter
Profils sans opération ni planification	Une stratégie est créée avec le type de sauvegarde par défaut en ligne et le champ d'application de sauvegarde complet.

Grâce à SnapManager for Oracle et SnapManager for SAP	À SnapCenter
Profils avec une ou plusieurs opérations	Plusieurs règles sont créées en fonction d'une combinaison unique d'un profil et d'opérations réalisées à l'aide de ce profil. Les stratégies créées dans SnapCenter contiennent les détails d'élagage et de conservation du journal d'archivage extraits du profil et des opérations correspondantes.
Profils avec configuration Oracle Recovery Manager (RMAN)	Les stratégies sont créées avec l'option **sauvegarde catalogue avec Oracle Recovery Manager** activée. Si le catalogage RMAN externe a été utilisé dans SnapManager, vous devez configurer les paramètres du catalogue RMAN dans SnapCenter. Vous pouvez sélectionner les informations d'identification existantes ou créer une nouvelle information d'identification. Si RMAN a été configuré par le biais du fichier de contrôle dans SnapManager, vous n'avez pas besoin de configurer RMAN dans SnapCenter.
Calendrier joint à un profil	Une règle est créée uniquement pour le planning.
Base de données	Un groupe de ressources est créé pour chaque base de données importée. Dans une configuration RAC (Real application clusters), le nœud sur lequel vous exécutez l'outil d'importation devient le nœud préféré après l'importation et le groupe de ressources est créé pour ce nœud.

Lorsqu'un profil est importé, une stratégie de vérification est créée avec la stratégie de sauvegarde.

Lorsque SnapManager pour Oracle et SnapManager pour SAP profils, planifications et toutes les opérations effectuées à l'aide des profils sont importées dans SnapCenter, les différentes valeurs de paramètres sont également importées.

SnapManager for Oracle et SnapManager for SAP : paramètres et valeurs	Paramètre et valeurs de SnapCenter	Remarques
Étendue de la sauvegarde • Pleine • Les données • Journal	Étendue de la sauvegarde • Pleine • Les données • Journal	
Mode de sauvegarde • Auto • En ligne • Hors ligne	Type de sauvegarde • En ligne • Arrêt hors ligne	Si le mode de sauvegarde est Auto, l'outil d'importation vérifie alors l'état de la base de données lorsque l'opération a été effectuée et définit de manière appropriée le type de sauvegarde comme Arrêt en ligne ou hors ligne.
La conservation • Jours • Compte	La conservation • Jours • Compte	SnapManager pour Oracle et SnapManager pour SAP utilise à la fois des jours et des nombres pour définir les paramètres de conservation. Dans SnapCenter, il y a soit des jours *OU* comptes. La conservation est donc définie sur des jours car les jours de préférence ne sont plus nombreux dans SnapManager pour Oracle et SnapManager pour SAP.
Élagage pour les plannings • Tout • Numéro de changement du système (SCN) • Date • Journaux créés avant les heures, les jours, les semaines et les mois spécifiés	Élagage pour les plannings • Tout • Journaux créés avant les heures et les jours spécifiés	SnapCenter ne prend pas en charge l'élagage selon SCN, date, semaines et mois.

SnapManager for Oracle et SnapManager for SAP : paramètres et valeurs	Paramètre et valeurs de SnapCenter	Remarques
Notification • E-mails envoyés uniquement pour assurer la réussite des opérations • E-mails envoyés uniquement en cas d'échec • E-mails envoyés pour succès et échecs	Notification • Toujours • En cas de défaillance • Avertissement • Erreur	Les notifications par e-mail sont importées. Cependant, vous devez mettre à jour manuellement le serveur SMTP à l'aide de l'interface graphique SnapCenter. L'objet de l'e-mail reste vide pour que vous puissiez le configurer.

Ce qui n'est pas importé dans SnapCenter

L'outil d'importation n'importe pas tout dans SnapCenter.

Vous ne pouvez pas importer les éléments suivants dans SnapCenter :

- Les métadonnées de sauvegarde
- Sauvegardes partielles
- Sauvegardes relatives à Raw Device Mapping (RDM) et Virtual Storage Console (VSC)
- Rôles ou informations d'identification disponibles dans le référentiel SnapManager pour Oracle et SnapManager pour SAP
- Données liées aux opérations de vérification, de restauration et de clonage
- Des opérations de suppression
- Détails de réplication spécifiés dans le profil SnapManager pour Oracle et SnapManager pour SAP

  Après l'importation, vous devez modifier manuellement la stratégie correspondante créée dans SnapCenter pour inclure les détails de la réplication.

- Informations de sauvegarde cataloguées

Préparez-vous à importer des données

Avant d'importer des données dans SnapCenter, vous devez effectuer certaines tâches pour que l'opération d'importation puisse réussir.

Étapes

1. Identifiez la base de données à importer.
2. À l'aide de SnapCenter, ajoutez l'hôte de base de données et installez SnapCenter Plug-ins Package pour Linux.
3. SnapCenter permet de configurer les connexions des SVM utilisées par les bases de données sur l'hôte.
4. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
5. Dans la page Ressources, assurez-vous que la base de données à importer est découverte et affichée.

Lorsque vous souhaitez exécuter l'outil d'importation, la base de données doit être accessible ou la création du groupe de ressources échoue.

Si les informations d'identification de la base de données sont configurées, vous devez créer les informations d'identification correspondantes dans SnapCenter, attribuer les informations d'identification à la base de données, puis relancer la découverte de la base de données. Si la base de données réside dans ASM (Automatic Storage Management), vous devez créer des informations d'identification pour l'instance ASM et affecter ces informations d'identification à la base de données.

6. Assurez-vous que l'utilisateur exécutant l'outil d'importation dispose de privilèges suffisants pour exécuter des commandes CLI SnapManager pour Oracle ou SnapManager pour SAP (telles que la commande pour suspendre les planifications) à partir de l'hôte SnapManager pour Oracle ou SnapManager pour SAP.
7. Exécutez les commandes suivantes sur l'hôte SnapManager pour Oracle ou SnapManager pour SAP pour suspendre les planifications :
   a. Si vous souhaitez suspendre les planifications sur l'hôte SnapManager pour Oracle, exécutez :
      - `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smo credential set -profile -name profile_name`

      Vous devez exécuter la commande d'ensemble d'informations d'identification smo pour chaque profil de l'hôte.

   b. Si vous souhaitez suspendre les planifications sur l'hôte SnapManager pour SAP, exécutez :
      - `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smsap credential set -profile -name profile_name`

      Vous devez exécuter la commande smsap Credential set pour chaque profil de l'hôte.

8. Assurez-vous que le nom de domaine complet (FQDN) de l'hôte de la base de données s'affiche lorsque vous exécutez hostname -F.

   Si le FQDN n'est pas affiché, vous devez modifier /etc/hosts pour spécifier le FQDN de l'hôte.

Importer des données

Vous pouvez importer des données en exécutant l'outil d'importation à partir de l'hôte de la base de données.

À propos de cette tâche

Les règles de sauvegarde SnapCenter créées après l'importation ont des formats de nommage différents :

- Les règles créées pour les profils sans opération ni planification ont le format SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRÉE.

  Lorsqu'aucune opération n'est effectuée à l'aide d'un profil, la règle correspondante est créée avec le type de sauvegarde par défaut en tant qu'étendue en ligne et la sauvegarde complète.

- Les règles créées pour les profils avec une ou plusieurs opérations ont le format SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRÉ.
- Les règles créées pour les planifications attachées aux profils ont le format SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRÉ.

Étapes

1. Connectez-vous à l'hôte de base de données que vous souhaitez importer.
2. Exécutez l'outil d'importation en exécutant le script sc-migrate situé à */opt/NetApp/snapcenter/spl/bin*.
3. Entrez le nom d'utilisateur et le mot de passe du serveur SnapCenter.

   Une fois les informations d'identification valides, une connexion est établie avec SnapCenter.

4. Entrez les détails de la base de données du référentiel SnapManager pour Oracle ou SnapManager pour SAP.

   La base de données du référentiel répertorie les bases de données disponibles sur l'hôte.

5. Entrez les détails de la base de données cible.

   Si vous souhaitez importer toutes les bases de données de l'hôte, entrez tout.

6. Si vous souhaitez générer un journal système ou envoyer des messages ASUP pour les opérations ayant échoué, vous devez les activer soit en exécutant la commande *Add-SmStorageConnection* soit *set-SmStorageConnection*.

> Si vous souhaitez annuler une opération d'importation, soit lors de l'exécution de l'outil d'importation, soit après l'importation, vous devez supprimer manuellement les stratégies SnapCenter, les informations d'identification et les groupes de ressources créés dans le cadre de l'opération d'importation.

Résultats

Les stratégies de sauvegarde SnapCenter sont créées pour les profils, les planifications et les opérations effectuées à l'aide des profils. Des groupes de ressources sont également créés pour chaque base de données cible.

Une fois les données importées avec succès, les planifications associées à la base de données importée sont suspendues dans SnapManager pour Oracle et SnapManager pour SAP.

> Après l'importation, vous devez gérer la base de données ou le système de fichiers importés à l'aide de SnapCenter.

Les journaux de chaque exécution de l'outil d'importation sont stockés dans le répertoire

/var/opt/snapcenter/spl/logs sous le nom spl_migration_timestamp.log. Vous pouvez consulter ce journal pour consulter les erreurs d'importation et les résoudre.

Informations sur le copyright

Copyright © 2025 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.