



Installez le plug-in SnapCenter pour les systèmes de fichiers Unix

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommaire

- Installez le plug-in SnapCenter pour les systèmes de fichiers Unix. 1
 - Conditions préalables à l'ajout d'hôtes et à l'installation de Plug-ins Package pour Linux 1
 - Ajoutez des hôtes et installez Plug-ins Package pour Linux à l'aide de l'interface graphique. 2
 - Configurer le service du chargeur enfichable SnapCenter 5
 - Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux 9
 - Activez les certificats CA pour les plug-ins. 12

Installez le plug-in SnapCenter pour les systèmes de fichiers Unix

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

Avant d'ajouter un hôte et d'installer le package de plug-ins pour Linux, vous devez remplir toutes les conditions requises.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous pouvez utiliser l'authentification basée sur un mot de passe pour l'utilisateur root ou non root ou l'authentification basée sur une clé SSH.

Le plug-in SnapCenter pour systèmes de fichiers Unix 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.

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



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](#)"

- 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
Systemes d'exploitation	<ul style="list-style-type: none">• Red Hat Enterprise Linux• Oracle Linux• 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	<p>2 GO</p> <p> 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.</p>
Packs logiciels requis	<ul style="list-style-type: none"> • Java 1.8.x (64 bits) Oracle Java et OpenJDK • Java 11 (64 bits) Oracle Java et OpenJDK <p> Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux.</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p>

Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp](#)".

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

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


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 comme type d'hôte.
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p> <p>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.</p>
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification.</p> <p>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.</p> <p>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.</p> <div data-bbox="873 1163 928 1222" style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> i </div> <p style="margin-left: 20px;">Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p>

5. Dans la section Select Plug-ins to Install, sélectionnez **Unix File Systems**.

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

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port.</p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  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. </div>
Chemin d'installation	<p>Le chemin par défaut est <code>/opt/NetApp/snapcenter</code>.</p> <p>Vous pouvez éventuellement personnaliser le chemin. Si vous utilisez le chemin personnalisé, assurez-vous que le contenu par défaut des sudoers est mis à jour avec le chemin personnalisé.</p>
Ignorer les vérifications de préinstallation facultatives	<p>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.</p>

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**.



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






Tous les systèmes de fichiers montés sur l'hôte sont automatiquement découverts et affichés sous 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 n'a pas pu démarrer en raison d'avertissements
-  En file d'

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
 - a. Cliquez sur **Filtrer**.
 - b. Facultatif : spécifiez les dates de début et de fin.
 - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
 - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
 - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Configurer le service du chargeur enfichable SnapCenter

Le service chargeur de plug-in SnapCenter charge le package de plug-in pour Linux afin qu'il interagisse avec le serveur SnapCenter. Le service chargeur de plug-in SnapCenter est installé lorsque vous installez le module de plug-ins SnapCenter pour Linux.

À propos de cette tâche

Après avoir installé le pack de plug-ins SnapCenter pour Linux, le service de 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.
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.

Nom du paramètre	Description
SPL_PORT	<p>Affiche le numéro de port sur lequel le service du chargeur enfichable SnapCenter est exécuté.</p> <p>Vous pouvez ajouter la valeur si la valeur par défaut est manquante.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Vous ne devez pas modifier la valeur après l'installation des modules externes. </div>
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	<p>Affiche le nombre de fichiers journaux du chargeur de plug-in SnapCenter qui sont conservés dans le dossier <i>/Custom_location/snapcenter/spl/logs</i>.</p> <p>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.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Si vous supprimez manuellement le fichier <i>spl.properties</i>, le nombre de fichiers à conserver est défini sur 9999. </div>
JAVA_HOME	<p>Affiche le chemin absolu du répertoire <i>Java_HOME</i> utilisé pour démarrer le service SPL.</p> <p>Ce chemin est déterminé lors de l'installation et dans le cadre du démarrage de SPL.</p>
LOG_MAX_SIZE	<p>Affiche la taille maximale du fichier journal des travaux.</p> <p>Une fois la taille maximale atteinte, le fichier journal est compressé et les journaux sont écrits dans le nouveau fichier de ce travail.</p>

Nom du paramètre	Description
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 :

- Démarrez le service du chargeur de plug-in SnapCenter :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
 - En tant qu'utilisateur non root, exécutez : `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- Arrêtez le service du chargeur enfichable SnapCenter :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - En tant qu'utilisateur non root, exécutez : `sudo /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 :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - En tant qu'utilisateur non root, exécutez : `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Recherchez l'état du service du chargeur enfichable SnapCenter :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - En tant qu'utilisateur non root, exécutez : `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

- Trouver le changement dans le service du chargeur Plug-in SnapCenter :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - En tant qu'utilisateur non root, exécutez : `sudo`
`/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 du magasin de clés SPL et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaire pour le magasin de confiance SPL et configurer la paire de clés signée CA pour le magasin de confiance SPL avec le service de 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
<AliasNameForCertificateToBeImported> -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
. Répertoriez 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 "<OriginalAliasName>" -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 de l'autorité de certification n'est ni activé ni attribué à l'hôte du plug-in.
- * *  Indique que le certificat de l'autorité de certification a été validé avec succès.
- * *  Indique que le certificat de l'autorité de certification n'a pas pu être validé.
- *  indique que les informations de connexion n'ont pas pu être récupérées.



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

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 DÉLICTEUELLE (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.