



Configurer XCP

XCP

NetApp
January 22, 2026

Sommaire

Configurer XCP	1
Configurez le fichier INI pour XCP NFS	1
Configurez le fichier INI pour un utilisateur racine	1
Configurez le fichier INI pour un utilisateur non-root	1
Réglage des performances	2
Variable d'environnement	2
Configurez le connecteur POSIX	3
Fonctionnalités prises en charge	3
Syntaxe du chemin	3
Configurez un connecteur POSIX	3
Propriété (UID et GID)	4
Augmentez le nombre maximal de descripteurs de fichier ouverts	5
Configurer le connecteur HDFS	5
Configurer l'évolutivité horizontale sur plusieurs nœuds	6
Configurer le connecteur S3	8
Configurez un connecteur S3	8

Configurer XCP

Configurez le fichier INI pour XCP NFS

Étapes de configuration du fichier INI pour XCP.



Le fichier INI XCP n'est pas requis dans le SMB XCP.

Configurez le fichier INI pour un utilisateur racine

Vous pouvez utiliser la procédure suivante pour configurer le fichier INI pour un utilisateur racine XCP NFS.

Étapes

1. Ajoutez l'emplacement du catalogue pour le serveur XCP dans le fichier de configuration hôte en utilisant le `vi` rédacteur :



L'emplacement du catalogue doit être exporté avant de modifier les détails dans `xcp.ini`. Fichier de configuration XCP. L'emplacement du catalogue (NFSv3) doit être montable par l'hôte XCP Linux mais pas nécessairement monté.

```
[root@localhost /]# vi /opt/NetApp/xFiles/xcp/xcp.ini
```

2. Vérifier que les entrées du fichier de configuration hôte du client XCP Linux pour le catalogue ont été modifiées :

```
[root@localhost /]# cat /opt/NetApp/xFiles/xcp/xcp.ini
# Sample xcp config
[xcp]
catalog = 10.61.82.210:/vol/xcpvol/
```

Configurez le fichier INI pour un utilisateur non-root

En tant qu'utilisateur non root, vous n'êtes pas autorisé à monter le système de fichiers NFS. Un utilisateur root est requis pour monter d'abord le volume du catalogue, puis, en tant qu'utilisateur non root exécutant XCP, si vous avez l'autorisation de lecture/écriture au volume du catalogue, vous pouvez accéder au volume du catalogue monté en utilisant un connecteur POSIX. Une fois le volume monté, vous pouvez ajouter le chemin d'accès au catalogue :

```
(t/10.237.170.53_catalog_vol - This is the path where catalog volume is  
mounted) as follows.
```

```
[user1@scspr2474004001 xcp]$ ls -ltr  
total 8  
drwxrwxr-x 2 user1 user1 21 Sep 20 02:04 xcplogs  
-rw-rw-r-- 1 user1 user1 71 Sep 20 02:04 xcp.ini  
-rwxr-xr-x 1 user1 user1 352 Sep 20 02:10 license  
[user1@scspr2474004001 xcp]$ cat /home/user1/NetApp/xFiles/xcp/xcp.ini  
  
Sample xcp config [xcp]  
catalog = file:///t/10.237.170.53_catalog_vol
```

Réglage des performances

Pour XCP NFS, après planification de la migration à l'aide du `show` et `scan` vous pouvez migrer des données.



Lorsque vous effectuez la migration des données en tant qu'utilisateur non racine, un utilisateur root peut effectuer l'étape suivante.

Pour des performances et une fiabilité optimales, NetApp recommande de définir les paramètres de performance TCP du noyau Linux suivants dans `/etc/sysctl.conf`. Sur l'hôte client XCP Linux. Courez `sysctl -p` ou le `reboot` commande pour valider les modifications :

```
net.core.rmem_default = 1342177  
net.core.rmem_max = 16777216  
net.core.rmem_max = 16777216  
net.core.wmem_default = 1342177  
net.core.wmem_max = 16777216  
net.ipv4.tcp_rmem = 4096 1342177 16777216  
net.ipv4.tcp_wmem = 4096 1342177 16777216  
net.core.netdev_max_backlog = 300000  
net.ipv4.tcp_fin_timeout = 10
```



Pour un utilisateur non-racine, le paramètre doit être exécuté par un utilisateur root.

Variable d'environnement

Configuration de variable d'environnement facultative pour les systèmes XCP NFS.



Un utilisateur non-root peut également utiliser les variables suivantes.

Variable d'environnement XCP_CONFIG_DIR remplace l'emplacement par défaut, /opt/NetApp/xFiles/xcp. Si elle est définie, la valeur doit correspondre à un chemin du système de fichiers du système d'exploitation, éventuellement à un répertoire NFS monté. Lorsque le XCP_CONFIG_DIR variable est défini, un nouveau répertoire portant le même nom que le nom d'hôte est créé dans le chemin du répertoire de configuration personnalisé, les nouveaux journaux sont stockés à cet emplacement.

```
[root@localhost /]# export XCP_CONFIG_DIR ='/tmp/xcp_config_dir_path'
```

Variable d'environnement XCP_LOG_DIR Remplace l'emplacement par défaut qui stocke le journal XCP dans le répertoire de configuration. Si elle est définie, la valeur doit correspondre à un chemin du système de fichiers du système d'exploitation, éventuellement à un répertoire NFS monté. Lorsque le XCP_LOG_DIR variable est défini, un nouveau répertoire avec le même nom que l'hôte est créé dans le chemin du répertoire de journaux personnalisé, les nouveaux journaux sont stockés à cet emplacement.

```
[root@localhost /]# export XCP_LOG_DIR='/tmp/xcp_log_dir_path'
```

Variable d'environnement XCP_CATALOG_PATH remplace le paramètre dans xcp.ini. Si elle est définie, la valeur doit être au format de chemin xcp, server:export[:subdirectory].

```
[root@localhost /]# export XCP_CATALOG_PATH='10.61.82.210:/vol/xcpvol/'
```



Pour un utilisateur non-racine, vous devez remplacer XCP_CATALOG_PATH À partir du chemin exporté avec le chemin POSIX.

Configurez le connecteur POSIX

XCP NFS prend désormais en charge l'utilisation de connecteurs POSIX pour fournir des chemins source et de destination pour la migration des données.

Fonctionnalités prises en charge

Les fonctions suivantes sont prises en charge pour les connecteurs POSIX :

- Pour les systèmes de fichiers POSIX prenant en charge la nanoseconde atime, mtime, et ctime, le scan la commande obtient les valeurs complètes (secondes et nanosecondes) et le copy les définit par commande
- Les connecteurs POSIX sont plus sûrs que XCP avec des sockets TCP NFSv3.

Syntaxe du chemin

La syntaxe de chemin d'un connecteur POSIX est file://<mounted path on linux>.

Configurez un connecteur POSIX

Pour configurer un connecteur POSIX, vous devez effectuer les tâches suivantes :

- Monter un volume source et un volume de destination
- Vérifiez que le chemin de destination dispose de l'autorisation nécessaire pour écrire les données

Une destination et un catalogue sont montés dans l'exemple suivant :

```
root@scspr2395903001 ~]# findmnt -t nfs4
TARGET SOURCE FSTYPE OPTIONS
/t/10.237.170.39_src_vol 10.237.170.39:/source_vol nfs4
rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=t
cp,timeo=600,retrans=2,sec=sys,clien
/t/10.237.170.53_dest_vol 10.237.170.53:/dest_vol nfs4
rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=t
cp,timeo=600,retrans=2,sec=sys,clien
/t/10.237.170.53_catalog_vol 10.237.170.53:/xcp_catalog nfs4
rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=t
cp,timeo=600,retrans=2,sec=sys,clien
[root@scspr2395903001 ~]#
```

Les connecteurs POSIX accèdent à un volume source et de destination en utilisant la syntaxe POSIX `file://`. Dans l'exemple ci-dessus, le chemin source est `file:///t/10.237.170.39_src_vol` et le chemin de destination est `file:///t/10.237.170.53_dest_vol`.

Vous pouvez gérer l'exemple de configuration d'un catalogue XCP partagé par des utilisateurs non-root en créant un groupe Linux pour les utilisateurs XCP. Pour les utilisateurs non-racines, les autorisations suivantes sont requises pour que les utilisateurs du groupe Linux effectuent des migrations.

Dans l'exemple de sortie suivant, `demo` est l'utilisateur non-racine et `/mnt/xcp-catalog` est le chemin d'accès où le volume du catalogue est monté :

```
sudo groupadd -g 7711 xcp_users
sudo usermod -G xcp_users -a demo
sudo chown -R :xcp_users /mnt/xcp-catalog
sudo chmod -R g+w /mnt/xcp-catalog
```

Le catalogue XCP ne stocke pas les données mais il stocke les noms de fichiers de numérisation et de copie, les noms de répertoires et d'autres métadonnées. Par conséquent, il est recommandé de configurer les autorisations de système de fichiers de catalogue pour les utilisateurs autorisés afin de leur donner la possibilité de sécuriser les métadonnées stockées.

Propriété (UID et GID)

Lorsque vous êtes configuré comme utilisateur normal, par défaut, un `copy` Une commande vers une destination POSIX ou NFS3 ne tente pas de définir la propriété (ID utilisateur (UID) et ID de groupe (GID). La définition de la propriété est généralement effectuée par un administrateur. Lorsque l'utilisateur A copie des fichiers de l'utilisateur B, l'utilisateur A s'attend à posséder la destination. Cependant, ce n'est pas le cas lorsqu'un utilisateur root copie les fichiers. Lorsqu'un utilisateur root copie les fichiers, le `-chown` l'option modifie le comportement de sorte qu'un comportement non-racine soit modifié `copy` commande avec `-chown`

Tentatives de définition de l'UID et du GID.

Augmentez le nombre maximal de descripteurs de fichier ouverts

Pour des performances et une fiabilité optimales, vous pouvez augmenter le nombre maximal de descripteurs de fichier ouverts pour l'utilisateur XCP sur tous les nœuds.

Étapes

1. Ouvrez le fichier à l'aide de la commande suivante :
`vi /etc/security/limits.conf`
2. Ajoutez la ligne suivante au fichier :
`<username> - nofile 999999`

Exemple

```
root - nofile 999999
```

Voir "[Solutions Red Hat](#)" pour en savoir plus.

Configurer le connecteur HDFS

Pour XCP NFS, le connecteur HDFS (Hadoop Distributed File System) (`hdfs://`) permet à XCP d'accéder à tout système de fichiers HDFS disponible avec différents fournisseurs.

Fonctionnalités prises en charge

Le `copy` Les opérations de commande de HDFS à NFS sont prises en charge pour les connecteurs HDFS.

Syntaxe du chemin

La syntaxe de chemin d'un connecteur HDFS est `hdfs://[user@host:port]/full-path`.



Si vous ne spécifiez pas d'utilisateur, d'hôte et de port, les appels XCP `hdfsConnect` avec l'hôte défini sur `default` et le port défini sur `0`.

Configurez un connecteur HDFS

Pour exécuter HDFS `copy` Vous devez configurer le client HDFS sur le système Linux et, en fonction du fournisseur Hadoop, suivre la configuration d'installation disponible sur Internet. Par exemple, vous pouvez définir le client d'un cluster MapR à l'aide de <https://docs.datafabric.hpe.com/60/AdvancedInstallation/SettingUpTheClient-redhat.html>.

Une fois la configuration du client HDFS terminée, vous devez terminer la configuration sur le client. Pour utiliser les chemins HDFS avec des commandes XCP, vous devez disposer des variables d'environnement suivantes :

- `CHEMIN_NHDFS_LIBHDFS_NHDFS`
- `CHEMIN_NHDFS_LIBJVM`

Dans les exemples suivants, les paramètres fonctionnent avec MapR et Java-1.8.0-openjdk-devel sur CentOS:

```

export JAVA_HOME=$(dirname $(dirname $(readlink $(readlink $(
which javac)))) )
export NHDFS_LIBJVM_PATH=`find $JAVA_HOME -name "libjvm.so"` export
NHDFS_LIBHDFS_PATH=/opt/mapr/lib/libMapRClient.so

```

```

[demo@mapr0 ~]$ hadoop fs -ls Found 3 items
drwxr-xr-x - demo mapr 0 2021-01-14 00:02 d1
drwxr-xr-x - demo mapr 0 2021-01-14 00:02 d2
drwxr-xr-x - demo mapr 0 2021-01-14 00:02 d3

```

Configurer l'évolutivité horizontale sur plusieurs nœuds

Pour XCP NFS, vous pouvez surmonter les limites de performance d'un nœud unique en utilisant un seul copy (ou scan -md5) Commande permettant d'exécuter des travailleurs sur plusieurs systèmes Linux ou nœuds de cluster.

Fonctionnalités prises en charge

Le scale-out multi-nœuds est utile dans n'importe quel environnement où la performance d'un seul système n'est pas suffisante, par exemple dans les scénarios suivants :

- Il faut plusieurs mois pour qu'un seul nœud copie des pétaoctets de données
- Lorsque les connexions à latence élevée vers les magasins d'objets cloud ralentissent un nœud individuel
- Dans les grandes batteries de clusters HDFS où vous exécutez un très grand nombre d'opérations d'E/S.

Syntaxe du chemin

La syntaxe de chemin pour l'évolutivité scale-out multi-nœuds est --nodes worker1,worker2,worker3.

Configurer l'évolutivité horizontale multi-nœuds

Envisagez une configuration avec quatre hôtes Linux aux configurations CPU et RAM similaires. Vous pouvez utiliser les quatre hôtes pour la migration, car XCP peut coordonner les opérations de copie sur tous les nœuds hôtes. Pour utiliser ces nœuds dans un environnement scale-out, vous devez identifier l'un des quatre nœuds en tant que nœud principal et les autres nœuds en tant que nœuds worker. Par exemple, pour une configuration Linux à quatre noeuds, nommez les noeuds comme "maître", "worker1", "worker2" et "worker3", puis configurez la configuration sur le noeud maître :

1. Copier XCP dans le répertoire de base.
2. Installer et activer la licence XCP.
3. Modifiez le xcp.ini et ajoutez le chemin du catalogue.
4. Définissez SSH (Passwordless Secure Shell) du nœud maître vers les nœuds worker :
 - a. Générer la clé sur le nœud maître :

```
ssh-keygen -b 2048 -t rsa -f /root/.ssh/id_rsa -q -N ''
```

- b. Copiez la clé sur tous les nœuds worker :

```
ssh-copy-id -i /root/.ssh/id_rsa.pub root@worker1
```

Le nœud maître XCP utilise SSH pour exécuter des travailleurs sur d'autres nœuds. Vous devez configurer les nœuds worker pour activer un accès SSH sans mot de passe pour l'utilisateur exécutant XCP sur le noeud maître. Par exemple, pour permettre à un utilisateur de démonstration sur un noeud maître d'utiliser le noeud "worker1" comme nœud de travail XCP, vous devez copier le binaire XCP du noeud maître vers tous les nœuds de travail dans le répertoire de base.

MaxStartups

Lorsque vous démarrez plusieurs travailleurs XCP simultanément, pour éviter les erreurs, vous devez augmenter le sshd MaxStartups paramètre sur chaque nœud de travail comme indiqué dans l'exemple suivant :

```
echo "MaxStartups 100" | sudo tee -a /etc/ssh/sshd_config  
sudo systemctl restart sshd
```

Le fichier nodes.ini"

Lorsque XCP exécute un worker sur un nœud de cluster, le processus worker hérite des variables d'environnement du processus XCP principal sur le nœud maître. Pour personnaliser un environnement de nœud particulier, vous devez définir les variables dans le nodes.ini fichier dans le répertoire de configuration uniquement sur le nœud maître (les nœuds de travail ne disposent pas d'un répertoire de configuration ou d'un catalogue). Par exemple, pour un serveur ubuntu mars qui a son libjvm.so Dans un autre emplacement du nœud maître, tel que Wave (qui est CentOS), il faut un répertoire de configuration pour permettre à un employé sur mars d'utiliser le connecteur HDFS. Cette configuration est illustrée dans l'exemple suivant :

```
[schay@wave ~]$ cat /opt/NetApp/xFiles/xcp/nodes.ini [mars]  
NHDFS_LIBJVM_PATH=/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/  
amd64/server/libjvm.so
```

Si vous utilisez une multisession avec des chemins de fichiers POSIX et HDFS, vous devez monter le système de fichiers et le système de fichiers exporté source et destination sur le nœud principal et tous les nœuds worker.

Lorsque XCP s'exécute sur un nœud de travail, le nœud de travail n'a pas de configuration locale (pas de licence, de fichiers journaux ou de catalogue). XCP binaire uniquement est requis sur le système de votre répertoire personnel. Par exemple, pour exécuter l' copy commande, le nœud maître et tous les nœuds workers doivent avoir accès à la source et à la destination. Pour xcp copy --nodes linux1,linux2 hdfs:///user/demo/test file:///mnt/ontap, le linux1 et linux2 Les hôtes doivent avoir le logiciel client HDFS configuré et l'exportation NFS montée sur /mnt/ontap, et, comme mentionné précédemment, une copie du binaire XCP dans le répertoire local.

Combinaison de connecteurs POSIX et HDFS, d'une évolutivité scale-out multi-nœuds et de fonctions de sécurité

Vous pouvez combiner les connecteurs POSIX et HDFS, l'évolutivité horizontale multinode et les fonctions de sécurité. Par exemple copy et verify Les commandes combinent des connecteurs POSIX et HDFS avec la sécurité et les fonctionnalités scale-out :

- copy exemple de commande :

```
./xcp copy hdfs:///user/demo/d1 file:///mnt/nfs-server0/d3  
./xcp copy -match "'USER1 in name'" file:///mnt/nfs-server0/d3  
hdfs:///user/demo/d1  
./xcp copy -node worker1,worker2,worker3 hdfs:///user/demo/d1  
file:///mnt/nfs-server0/d3
```

- verify exemple de commande :

```
./xcp verify hdfs:///user/demo/d2 file:///mnt/nfs-server0/d3
```

Configurer le connecteur S3

À partir de XCP 1.9.2, le connecteur simple Storage Service (S3) renforce le périmètre de la migration des données XCP en permettant la migration des données à partir des systèmes de fichiers Hadoop Distributed File System (HDFS) vers le stockage objet S3.

Cas d'utilisation de la migration pris en charge

Les cas d'usage suivants sont pris en charge pour les connecteurs S3 :

- Migration de HDFS vers NetApp StorageGRID
- Migration de HDFS vers Amazon S3
- Migration de HDFS à NetApp ONTAP S3



Actuellement, MapR est uniquement qualifié et pris en charge pour HDFS.

Fonctionnalités prises en charge

Prise en charge du `scan`, `copy`, `verify`, `resume` et `delete`. Des commandes sont disponibles pour les connecteurs S3.

Fonctions non prises en charge

Prise en charge du `sync`. La commande n'est pas disponible pour les connecteurs S3.

Syntaxe du chemin

La syntaxe du chemin pour le connecteur S3 est `s3://<bucket in S3>`.

- Vous pouvez fournir un profil S3 spécifique pour les commandes XCP à l'aide de `-s3.profile` option.
- Vous pouvez utiliser le `s3.endpoint` Option permettant de modifier la valeur du noeud final pour communiquer avec S3



L'utilisation du terminal est obligatoire pour StorageGRID et ONTAP S3.

Configurez un connecteur S3

Étapes

- Pour exécuter la commande XCP avec le connecteur S3, créez un compartiment dans S3 en suivant la documentation en ligne de chaque plateforme :
 - "Gestion du stockage objet ONTAP S3"
 - "StorageGRID : présentation du compte de locataire"

 Avant de continuer, vous devez avoir le access key, secret key, L'ensemble de certificats de l'autorité de certification (CA) et endpoint url informations. XCP identifie le compartiment S3 et se connecte à l'aide de ces paramètres avant de lancer une opération.
- Installez les packages CLI d'Amazon Web Services (AWS) et exécutez les commandes CLI d'AWS pour configurer les clés et les certificats SSL (Secure Sockets Layer) pour les comptes S3 :
 - Voir "[Installation ou mise à jour de la dernière version de l'interface de ligne de commande AWS](#)" Pour installer les packages AWS.
 - Voir la "[Référence des commandes de la CLI AWS](#)" pour en savoir plus.
- Utilisez le aws configure pour configurer votre fichier d'informations d'identification. Par défaut, l'emplacement du fichier est /root/.aws/credentials. Le fichier d'informations d'identification doit spécifier la clé d'accès et la clé d'accès secrète.
- Utilisez le aws configure set Commande permettant de spécifier un bundle de certificats d'autorité de certification, qui est un fichier contenant le .pem Extension utilisée lors de la vérification des certificats SSL. Par défaut, l'emplacement du fichier est /root/.aws/config.

Exemple:

```
[root@client1 ~]# aws configure
AWS Access Key ID [None]: <access_key>
AWS Secret Access Key [None]: <secret_key>
Default region name [None]:
Default output format [None]:
[root@client1 ~]# cat /root/.aws/credentials
[default]
aws_access_key_id = <access_key>
aws_secret_access_key = <secret_key>
[root@client1 ~]#
[root@client1 ~]# aws configure set default.ca_bundle
/u/xxxx/s3/ca/aws_cacert.pem
[root@client1 ~]# cat /root/.aws/config
[default]
ca_bundle = /u/xxxx/s3/ca/aws_cacert.pem
```

- Une fois la configuration d'installation requise terminée, vérifier que les commandes de l'interface de ligne de commande AWS peuvent accéder aux compartiments S3 à partir du client Linux avant d'exécuter les commandes XCP :

```
aws s3 ls --endpoint-url <endpoint_url> s3://bucket-name/
aws s3 ls --profile <profile> --endpoint-url <endpoint_url> s3://bucket-name
```

Exemple:

```
[root@client1 linux]# aws s3 ls --profile <profile> --endpoint
<endpoint_url>  s3://<bucket-name>
                  PRE 1G/
                  PRE aws_files/
                  PRE copied_folders/
                  PRE d1/
                  PRE d2/
                  PRE giant_size_dirs/
                  PRE medium_size_dirs/
                  PRE small_size_dirs/
[root@client1 l
```

Informations sur le copyright

Copyright © 2026 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 JOUSSANCE, 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.