

Configuration NDMP ONTAP 9

NetApp September 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/ndmp/index.html on September 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Configuration NDMP
Présentation de la configuration NDMP 1
Workflow de configuration NDMP
Préparation à la configuration NDMP 2
Vérifiez les connexions du lecteur de bande 4
Activer les réservations sur bande
Configurer SVM-scoped NDMP
Configurer node-scoped NDMP
Configurez l'application de sauvegarde

Configuration NDMP

Présentation de la configuration NDMP

Vous pouvez rapidement configurer un cluster ONTAP 9 de sorte qu'il utilise le protocole NDMP (Network Data Management Protocol) pour sauvegarder les données directement sur bande à l'aide d'une application de sauvegarde tierce.

Si l'application de backup supporte Cluster Aware Backup (CAB), vous pouvez configurer NDMP sous la forme *SVM-scoped* ou *node-scoped* :

- SVM-scoped au niveau du cluster (admin SVM) permet de sauvegarder tous les volumes hébergés sur différents nœuds du cluster. SVM-scoped NDMP est recommandé si possible.
- Node-scoped NDMP vous permet de sauvegarder tous les volumes hébergés sur ce nœud.

Si l'application de backup ne prend pas en charge CAB, il faut utiliser node-scoped NDMP.

SVM-scoped et node-scoped NDMP sont mutuellement exclusifs ; ils ne peuvent pas être configurés sur le même cluster.



Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

En savoir plus sur "Sauvegarde « cluster Aware Backup » (CAB)".

Avant de configurer NDMP, vérifiez les points suivants :

- Vous disposez d'une application de sauvegarde tierce (également appelée Data Management application ou DMA).
- Vous êtes un administrateur de cluster.
- · Les périphériques de bande et un serveur multimédia en option sont installés.
- Les périphériques de bande sont connectés au cluster via un commutateur Fibre Channel (FC) et ne sont pas directement connectés.
- Au moins une unité de bande a un numéro d'unité logique (LUN) de 0.

Workflow de configuration NDMP

La configuration de la sauvegarde sur bande sur NDMP implique la préparation de la configuration NDMP, la vérification des connexions du périphérique de bande, l'activation des réservations sur bande, la configuration de NDMP au niveau SVM ou node, l'activation de NDMP sur le cluster, la configuration d'un utilisateur de sauvegarde, la configuration des LIFs et la configuration de l'application de sauvegarde.



Préparation à la configuration NDMP

Avant de configurer l'accès de sauvegarde sur bande via le protocole NDMP (Network Data Management Protocol), vous devez vérifier que la configuration planifiée est prise en charge. Vérifier que vos lecteurs de bande sont répertoriés comme disques qualifiés sur chaque nœud, vérifier que tous les nœuds disposent des LIF intercluster, Et déterminer si l'application de sauvegarde prend en charge l'extension CLUSTER Aware Backup (CAB).

Étapes

 Consultez le tableau de compatibilité de votre fournisseur d'applications de sauvegarde pour la prise en charge du protocole ONTAP (NetApp ne qualifier pas les applications de sauvegarde tierces avec ONTAP ou NDMP).

Vérifiez que les composants NetApp suivants sont compatibles :

• Version de ONTAP 9 qui s'exécute sur le cluster.

- Le fournisseur et la version de l'application de sauvegarde, par exemple Veritas NetBackup 8.2 ou CommVault.
- Les lecteurs de bande décrivent en détail le fabricant, le modèle et l'interface des lecteurs de bande, par exemple IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- $\circ\,$ Plateformes des nœuds du cluster : par exemple, FAS8700 ou A400



Vous trouverez des matrices de support de compatibilité ONTAP existantes pour les applications de sauvegarde dans le "Matrice d'interopérabilité NetApp".

- 2. Vérifiez que vos lecteurs de bande sont répertoriés comme lecteurs qualifiés dans le fichier de configuration de bande intégré de chaque nœud :
 - a. Sur l'interface de ligne de commande, affichez le fichier de configuration de bande intégré à l'aide du storage tape show-supported-status commande.

cluster1::> storage tape show-supported-status				
Node: cluster1-1				
	Is			
Tape Drives	Supported	Support Status		
Certance Ultrium 2	true	Dynamically Qualified		
Certance Ultrium 3	true	Dynamically Qualified		
Digital DLT2000	true	Qualified		

b. Comparez vos lecteurs de bande à la liste des lecteurs qualifiés dans la sortie.



Les noms des périphériques de bande dans la sortie peuvent varier légèrement par rapport aux noms figurant sur l'étiquette du périphérique ou dans la matrice d'interopérabilité. Par exemple, le DLT2000 numérique peut également être appelé DL2k. Vous pouvez ignorer ces différences mineures de dénomination.

c. Si un périphérique ne figure pas dans la liste comme indiqué dans le résultat, même si celui-ci est qualifié conformément à la matrice d'interopérabilité, téléchargez et installez un fichier de configuration mis à jour pour le périphérique, en suivant les instructions du site du support NetApp.

"Téléchargements NetApp : fichiers de configuration des lecteurs de bande"

Il se peut qu'un périphérique qualifié ne figure pas dans le fichier de configuration de bande intégré si le périphérique de bande a été qualifié après l'expédition du nœud.

- 3. Vérifier que chaque nœud du cluster dispose d'un LIF intercluster :
 - a. Afficher les LIFs intercluster sur les nœuds en utilisant le network interface show -role intercluster commande.

b. Si aucune LIF intercluster n'existe sur un nœud, créer une LIF intercluster en utilisant le network interface create commande.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
cluster1::> network interface show -role intercluster
         Logical Status Network Current
Current Is
Vserver Interface Admin/Oper Address/Mask Node
Port Home
_____ _____
_____ ___
cluster1 IC1 up/up 192.0.2.65/24 cluster1-1
e0a true
                 up/up 192.0.2.68/24 cluster1-2
cluster1 IC2
e0b true
```

"Gestion du réseau"

4. Déterminez si l'application de sauvegarde prend en charge Cluster Aware Backup (CAB) à l'aide de la documentation fournie avec l'application de sauvegarde.

Le support CAB est un facteur clé pour déterminer le type de sauvegarde que vous pouvez effectuer.

Vérifiez les connexions du lecteur de bande

Vous devez vous assurer que tous les lecteurs et changeurs de supports sont visibles

dans ONTAP en tant que périphériques.

Étapes

1. Affichez des informations sur tous les lecteurs et changeurs de supports à l'aide du storage tape show commande.

```
cluster1::> storage tape show
Node: cluster1-01
Device ID
                   Device Type Description
Status
_____
                   _____
                                _____
_____
sw4:10.11
                   tape drive HP LTO-3
normal
0b.125L1
                  media changer HP MSL G3 Series
normal
0d.4
                   tape drive IBM LTO 5 ULT3580
normal
0d.4L1
                   media changer IBM 3573-TL
normal
. . .
```

- 2. Si aucun lecteur de bande n'est affiché, résolvez le problème.
- 3. Si un changeur de supports n'est pas affiché, affichez les informations relatives aux changeurs de supports à l'aide du storage tape show-media-changer commande, puis résolution du problème.

```
cluster1::> storage tape show-media-changer
Media Changer: sw4:10.11L1
 Description: PX70-TL
        WWNN: 2:00a:000e11:10b919
        WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000 LL1
      Errors: -
Paths:
                      Initiator Alias Device State
Node
Status
____
                                        _____
_____
cluster1-01
                      2b mc0 in-use
normal
. . .
```

Activer les réservations sur bande

Vous devez vous assurer que les lecteurs de bande sont réservés à l'utilisation par les applications de sauvegarde pour les opérations de sauvegarde NDMP.

Description de la tâche

Les paramètres de réservation varient selon les applications de sauvegarde et ces paramètres doivent correspondre à l'application de sauvegarde et aux nœuds ou serveurs utilisant les mêmes lecteurs. Consultez la documentation fournisseur de l'application de sauvegarde pour connaître les paramètres de réservation corrects.

Étapes

1. Activer les réservations à l'aide de options -option-name tape.reservations -option-value persistent commande.

La commande suivante active les réservations avec le persistent valeur :

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. Vérifiez que les réservations sont activées sur tous les nœuds à l'aide de l'options tape.reservations commande, puis vérifiez la sortie.

```
cluster1::> options tape.reservations
cluster1-1
  tape.reservations persistent
cluster1-2
  tape.reservations persistent
2 entries were displayed.
```

Configurer SVM-scoped NDMP

Activer SVM-scoped NDMP sur le cluster

Si le DMA prend en charge l'extension Cluster Aware Backup (CAB), vous pouvez sauvegarder tous les volumes hébergés sur différents nœuds d'un cluster en activant SVM-scoped NDMP, en activant le service NDMP sur le cluster (admin SVM) et en configurant les LIF de données et de contrôle.

Ce dont vous avez besoin

L'extension CAB doit être prise en charge par le DMA.

Description de la tâche

La désactivation du mode node-scoped NDMP permet d'activer le mode SVM-scoped NDMP sur le cluster.

Étapes

1. Activer le mode NDMP SVM-scoped :

cluster1::> system services ndmp node-scope-mode off

Le mode NDMP SVM-scoped est activé.

2. Activer le service NDMP sur le SVM d'admin:

cluster1::> vserver services ndmp on -vserver cluster1

Le type d'authentification est défini sur challenge par défaut, l'authentification en texte brut est désactivée.



Pour des communications sécurisées, vous devez maintenir l'authentification en texte brut désactivée.

3. Vérifier que le service NDMP est activé :

cluster1::> vserver services ndmp show

Vserver	Enabled	Authentication	type
cluster1	true	challenge	
VSI	laise	chartenge	

Activez un utilisateur de sauvegarde pour l'authentification NDMP

Pour authentifier SVM-scoped NDMP depuis l'application de backup, un utilisateur administratif doit disposer des privilèges suffisants et d'un mot de passe NDMP.

Description de la tâche

Vous devez générer un mot de passe NDMP pour les utilisateurs admin de sauvegarde. Vous pouvez activer les utilisateurs admin de sauvegarde au niveau du cluster ou de la SVM et, si nécessaire, vous pouvez créer un nouvel utilisateur. Par défaut, les utilisateurs disposant des rôles suivants peuvent s'authentifier pour la sauvegarde NDMP :

- Au niveau du cluster : admin ou backup
- SVM individuels : vsadmin ou vsadmin-backup

Si vous utilisez un utilisateur NIS ou LDAP, l'utilisateur doit exister sur le serveur respectif. Vous ne pouvez pas utiliser un utilisateur Active Directory.

Étapes

1. Afficher les utilisateurs et autorisations admin actuels :

```
security login show
```

2. Si nécessaire, créez un nouvel utilisateur de sauvegarde NDMP avec le security login create Commande et le rôle approprié pour les privilèges des SVM au niveau du cluster ou individuels.

Vous pouvez spécifier un nom d'utilisateur de sauvegarde locale ou un nom d'utilisateur NIS ou LDAP pour l'-user-or-group-name paramètre.

La commande suivante crée l'utilisateur de sauvegarde backup_admin1 avec le backup rôle pour l'ensemble du cluster :

```
cluster1::> security login create -user-or-group-name backup_admin1
-application ssh -authmethod password -role backup
```

La commande suivante crée l'utilisateur de sauvegarde <code>vsbackup_admin1</code> avec le <code>vsadmin-backup</code> Rôle d'un SVM individuel :

```
cluster1::> security login create -user-or-group-name vsbackup_admin1
-application ssh -authmethod password -role vsadmin-backup
```

Entrez un mot de passe pour le nouvel utilisateur et confirmez.

3. Générer un mot de passe pour la SVM d'admin via le vserver services ndmp generate password commande.

Le mot de passe généré doit être utilisé pour authentifier la connexion NDMP par l'application de sauvegarde.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1
Vserver: cluster1
   User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configurez les LIF

Vous devez identifier les LIF qui seront utilisées pour établir une connexion de données entre les données et les ressources sur bande, et pour contrôler la connexion entre la SVM d'administration et l'application de sauvegarde. Une fois les LIF définies, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour les LIF et spécifier le rôle d'interface privilégié.

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Étapes

1. Identifier les LIF intercluster, cluster-management et node-management en utilisant le network interface show commande avec -role paramètre.

La commande suivante affiche les LIFs intercluster :

<pre>cluster1::></pre>	network interface	show -role	intercluster	
Current Is	Logical	Status	Network	Current
Vserver Port Home	Interface e	Admin/Oper	Address/Mask	Node
cluster1 e0a true	IC1	up/up	192.0.2.65/24	cluster1-1
cluster1 e0b true	IC2 e	up/up	192.0.2.68/24	cluster1-2

La commande suivante affiche la LIF cluster-management :

La commande suivante affiche les LIFs de node-management :

clusterl::> network interface show -role node-mgmt Logical Status Network Current Current Is Vserver Interface Admin/Oper Address/Mask Node Port Home Interface Interface Interface Interface Port Home Interface Interf

- 2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIF intercluster, cluster-management (cluster-mgmt) et node-management (node-mgmt) :
 - a. Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de system services firewall policy show commande.

La commande suivante affiche la politique de pare-feu pour la LIF cluster-management :

<pre>cluster1::> system services firewall policy show -policy cluster</pre>			
Vserver	Policy	Service	Allowed
cluster	cluster	dns http https ** ndmp ndmps ntp rsh snmp ssh	0.0.0.0/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0** 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0
10 entries	were displaye	telnet d.	0.0.0/0

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster
Vserver Policy Service Allowed
_____
                       _____ ___
                                    _____
cluster1 intercluster dns
                             _
                     http -
                    https -
**ndmp 0.0.0.0/0, ::/0**
                     ndmps
                              _
                     ntp
                              _
                     rsh
                             _
                     ssh
                              _
                     telnet -
9 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour la LIF node-management :

cluster1::> system services firewall policy show -policy mgmt			
Vserver	Policy	Service	Allowed
 cluster1-1	mgmt	dns http https **ndmp ndmps ntp rsh snmp	0.0.0.0/0, ::/0 0.0.0.0/0, ::/0 0.0.0.0/0, ::/0 0.0.0.0/0, ::/0** 0.0.0.0/0, ::/0 - 0.0.0.0/0, ::/0
		ssh	0.0.0/0, ::/0
10 entries were displayed.			

b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du system services firewall policy modify commande avec -service paramètre.

La commande suivante active la politique de pare-feu pour le LIF intercluster :

cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0

- 3. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :
 - a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur broadcastdomain-wide, Et la policy pour les LIFs intercluster et node-management est définie sur localonly à l'aide du network interface show -failover commande.

La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```
cluster1::> network interface show -failover
          Logical
                           Home
                                           Failover
Failover
Vserver
         Interface
                         Node:Port
                                           Policy
Group
_____
cluster cluster1 clus1 cluster1-1:e0a local-only
cluster
                                                Failover Targets:
                                                . . . . . . .
**cluster1 cluster mgmt cluster1-1:e0m broadcast-domain-wide
Default**
                                                Failover Targets:
                                                . . . . . . .
          **IC1
                            cluster1-1:e0a
                                              local-only
Default**
                                                Failover Targets:
                            cluster1-1:e0b
          **IC2
                                              local-only
Default**
                                                Failover Targets:
                                                . . . . . . .
**cluster1-1 cluster1-1 mgmt1 cluster1-1:e0m
                                             local-only
Default**
                                                Failover Targets:
                                                . . . . . .
**cluster1-2 cluster1-2 mgmt1 cluster1-2:e0m
                                             local-only
Default**
                                                Failover Targets:
                                                . . . . . .
```

a. Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant le network interface modify commande avec -failover-policy paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Spécifier les LIFs requises pour la connexion de données à l'aide de vserver services ndmp modify commande avec preferred-interface-role paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de vserver services ndmp show commande.

```
cluster1::> vserver services ndmp show -vserver cluster1
Vserver: cluster1
NDMP Version: 4
.....
Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

Configurer node-scoped NDMP

Activez NDMP node-scoped sur le cluster

Vous pouvez sauvegarder des volumes hébergés sur un seul nœud en activant NDMP node-scoped, en activant le service NDMP et en configurant une LIF pour la connexion data et contrôle. Cela peut être effectué pour tous les nœuds du cluster.



Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

Description de la tâche

Si vous utilisez NDMP en mode node-scope, l'authentification doit être configurée sur la base de chaque nœud. Pour plus d'informations, voir "L'article de la base de connaissances "Comment configurer l'authentification NDMP en mode 'node-scope'".

Étapes

1. Activer le mode NDMP node-scoped :

cluster1::> system services ndmp node-scope-mode on

NDMP node-scope-mode est activé.

2. Activer le service NDMP sur tous les nœuds du cluster :

L'utilisation du caractère générique "*" permet le service NDMP sur tous les nœuds en même temps.

Vous devez spécifier un mot de passe pour l'authentification de la connexion NDMP par l'application de backup.

cluster1::> system services ndmp on -node *

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Désactivez le -clear-text Option pour la communication sécurisée du mot de passe NDMP :

Utilisation du caractère générique "*" disables the -clear-text option sur tous les nœuds simultanément.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Vérifiez que le service NDMP est activé et que -clear-text l'option est désactivée :

cluster1::> system services ndmp show

Node	Enabled	Clear text	User Id
cluster1-1	true	false	root
cluster1-2	true	false	root
2 entries were displayed.			

Configurer une LIF

Vous devez identifier une LIF qui sera utilisée pour établir une connexion de données et une connexion de contrôle entre le nœud et l'application de sauvegarde. Après avoir identifié le LIF, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour le LIF.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

Étapes

1. Identifier le LIF intercluster hébergé sur les nœuds en utilisant le network interface show commande avec -role paramètre.

- 2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIFs intercluster :
 - a. Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de system services firewall policy show commande.

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster
Vserver Policy Service Allowed
_____
        cluster1
        intercluster dns
                  http
                         _
                  https
                          0.0.0.0/0, ::/0**
                  **ndmp
                  ndmps
                  ntp
                          _
                  rsh
                  ssh
                  telnet
                          _
9 entries were displayed.
```

b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du system services firewall policy modify commande avec -service paramètre.

La commande suivante active la politique de pare-feu pour le LIF intercluster :

cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0

3. S'assurer que la politique de basculement est correctement définie pour les LIFs intercluster :

a. Vérifier que la policy de basculement pour les LIFs intercluster est définie sur local-only à l'aide du network interface show -failover commande.

```
cluster1::> network interface show -failover
           Logical
                          Home
                                           Failover
                                                       Failover
           Interface
Vserver
                         Node:Port
                                           Policy
                                                       Group
                          ----- -----
_____
           _____
           **IC1
cluster1
                             cluster1-1:e0a local-only
Default**
                                                Failover Targets:
                                                . . . . . . .
           **IC2
                            cluster1-2:e0b
                                              local-only
Default**
                                                Failover Targets:
                                                . . . . . . .
cluster1-1 cluster1-1 mgmt1 cluster1-1:e0m
                                           local-only Default
                                                Failover Targets:
                                                . . . . . . .
```

b. Si la stratégie de basculement n'est pas définie de manière appropriée, modifiez la stratégie de basculement en utilisant le network interface modify commande avec -failover-policy paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configurez l'application de sauvegarde

Une fois le cluster configuré pour l'accès NDMP, vous devez collecter les informations de la configuration du cluster, puis configurer le reste du processus de sauvegarde dans l'application de sauvegarde.

Étapes

- 1. Collectez les informations suivantes que vous avez configurées précédemment dans ONTAP :
 - Nom d'utilisateur et mot de passe requis par l'application de sauvegarde pour créer la connexion NDMP
 - Les adresses IP des LIFs intercluster que l'application de sauvegarde nécessite pour se connecter au cluster
- 2. Dans ONTAP, affichez les alias attribués par ONTAP à chaque périphérique en utilisant le storage tape alias show commande.

Les alias sont souvent utiles pour configurer l'application de sauvegarde.

cluster1::> storage tape show -alias			
Device ID: 2a.0 Device Type: tape drive Description: Hewlett-Packard LTO-5			
Node	Alias	Mapping	
stsw-3220-4a-4b-02	st2	SN[HU19497WVR]	

3. Dans l'application de sauvegarde, configurez le reste du processus de sauvegarde à l'aide de la documentation de l'application de sauvegarde.

Une fois que vous avez terminé

En cas de mobilité des données, comme un déplacement de volume ou une migration LIF, vous devez être prêt à réinitialiser les opérations de sauvegarde interrompues.

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 nonresponsabilité 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.