



Configuration des clients d'audit pour CIFS

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

- Configuration des clients d'audit pour CIFS 1
 - Configuration des clients d'audit pour Workgroup 1
 - Configuration des clients d'audit pour Active Directory 4
 - Ajout d'un utilisateur ou d'un groupe à un partage d'audit CIFS 7
 - Suppression d'un utilisateur ou d'un groupe d'un partage d'audit CIFS 9
 - Modification du nom d'utilisateur ou de groupe d'un audit CIFS 11
 - Vérification de l'intégration d'un audit CIFS 11

Configuration des clients d'audit pour CIFS

La procédure utilisée pour configurer un client d'audit dépend de la méthode d'authentification Windows Workgroup ou Windows Active Directory (AD). Lorsqu'il est ajouté, le partage d'audit est automatiquement activé en tant que partage en lecture seule.



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Informations associées

["Mise à niveau du logiciel"](#)

Configuration des clients d'audit pour Workgroup

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Définissez l'authentification pour le groupe de travail Windows :

Si l'authentification a déjà été définie, un message d'avertissement s'affiche. Si l'authentification a déjà été définie, passez à l'étape suivante.

- Entrez : `set-authentication`
- Lorsque vous êtes invité à installer Windows Workgroup ou Active Directory, entrez : `workgroup`
- Lorsque vous y êtes invité, entrez le nom du groupe de travail : `workgroup_name`
- Lorsque vous y êtes invité, créez un nom NetBIOS significatif : `netbios_name`

ou

Appuyez sur **entrée** pour utiliser le nom d'hôte du noeud d'administration comme nom NetBIOS.

Le script redémarre le serveur Samba et des modifications sont appliquées. Cela devrait prendre moins d'une minute. Une fois l'authentification définie, ajoutez un client d'audit.

- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

6. Ajouter un client d'audit :

- Entrez : `add-audit-share`



Le partage est automatiquement ajouté en lecture seule.

- Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user`
- Lorsque vous y êtes invité, entrez le nom d'utilisateur de l'audit : `audit_user_name`
- Lorsque vous y êtes invité, entrez un mot de passe pour l'utilisateur d'audit : `password`
- Lorsque vous y êtes invité, saisissez à nouveau le même mot de passe pour le confirmer : `password`
- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.



Il n'est pas nécessaire d'entrer un répertoire. Le nom du répertoire d'audit est prédéfini.

7. Si plusieurs utilisateurs ou groupes sont autorisés à accéder au partage d'audit, ajoutez-les :

a. Entrez : `add-user-to-share`

Une liste numérotée des partages activés s'affiche.

b. Lorsque vous y êtes invité, entrez le numéro du partage audit-exportation : `share_number`

c. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user`

ou `group`

d. Lorsque vous y êtes invité, entrez le nom de l'utilisateur ou du groupe d'audit : `audit_user` or `audit_group`

e. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

f. Répétez ces sous-étapes pour chaque utilisateur ou groupe supplémentaire ayant accès au partage d'audit.

8. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Lorsque vous y êtes invité, appuyez sur **entrée**.

La configuration du client d'audit s'affiche.

b. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

9. Fermez l'utilitaire de configuration CIFS : `exit`

10. Démarrez le service Samba : `service smb start`

11. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

ou

Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ce partage d'audit comme requis :

- a. Connectez-vous à distance au nœud d'administration d'un site :
 - i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - iii. Entrez la commande suivante pour passer à la racine : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- b. Répétez les étapes pour configurer le partage d'audit pour chaque nœud d'administration supplémentaire.
- c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`

12. Déconnectez-vous du shell de commande : `exit`

Informations associées

"Mise à niveau du logiciel"

Configuration des clients d'audit pour Active Directory

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez disposer du nom d'utilisateur et du mot de passe CIFS Active Directory.
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Définissez l'authentification pour Active Directory : `set-authentication`

Dans la plupart des déploiements, vous devez définir l'authentification avant d'ajouter le client d'audit. Si l'authentification a déjà été définie, un message d'avertissement s'affiche. Si l'authentification a déjà été définie, passez à l'étape suivante.

- Lorsque vous êtes invité à installer Workgroup ou Active Directory : `ad`
- À l'invite, entrez le nom du domaine AD (nom de domaine court).
- Indiquez l'adresse IP ou le nom d'hôte DNS du contrôleur de domaine.
- Lorsque vous y êtes invité, entrez le nom de domaine de domaine complet.

Utilisez des lettres majuscules.

- Lorsque vous êtes invité à activer la prise en charge de winbind, tapez **y**.

Winbind est utilisé pour résoudre les informations utilisateur et de groupe à partir des serveurs AD.

- Lorsque vous y êtes invité, entrez le nom NetBIOS.
- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

6. Rejoindre le domaine :

- Si ce n'est pas déjà fait, démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`
- Rejoindre le domaine : `join-domain`
- Vous êtes invité à tester si le nœud d'administration est actuellement un membre valide du domaine. Si ce nœud d'administration n'a pas déjà rejoint le domaine, entrez : `no`
- Indiquez le nom d'utilisateur de l'administrateur lorsque vous y êtes invité :
`administrator_username`

où `administrator_username` Est le nom d'utilisateur CIFS Active Directory, pas le nom d'utilisateur StorageGRID.

- Lorsque vous y êtes invité, indiquez le mot de passe de l'administrateur : `administrator_password`

l'ont été `administrator_password` Est le nom d'utilisateur CIFS Active Directory, et non le mot de passe StorageGRID.

- f. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

7. Vérifiez que vous avez correctement joint le domaine :

- a. Rejoindre le domaine : `join-domain`

- b. Lorsque vous êtes invité à tester si le serveur est actuellement un membre valide du domaine, entrez :
`y`

Si vous recevez le message « rejoindre est OK », vous avez rejoint le domaine avec succès. Si vous n'obtenez pas cette réponse, essayez de définir l'authentification et de rejoindre à nouveau le domaine.

- c. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

8. Ajouter un client d'audit : `add-audit-share`

- a. Lorsque vous êtes invité à ajouter un utilisateur ou un groupe, entrez : `user`

- b. Lorsque vous êtes invité à saisir le nom d'utilisateur de l'audit, entrez le nom d'utilisateur de l'audit.

- c. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

9. Si plusieurs utilisateurs ou groupes sont autorisés à accéder au partage d'audit, ajoutez des utilisateurs supplémentaires : `add-user-to-share`

Une liste numérotée des partages activés s'affiche.

- a. Entrez le numéro du partage audit-exportation.

- b. Lorsque vous êtes invité à ajouter un utilisateur ou un groupe, entrez : `group`

Vous êtes invité à entrer le nom du groupe d'audit.

- c. Lorsque vous êtes invité à entrer le nom du groupe d'audit, entrez le nom du groupe d'utilisateurs d'audit.

- d. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

- e. Répétez cette étape pour chaque utilisateur ou groupe supplémentaire ayant accès au partage d'audit.

10. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-interfaces.inc`
- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-filesystem.inc`

- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-interfaces.inc`
- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-custom-config.inc`
- Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-shares.inc`
- `rlimit_max` : augmentation de `rlimit_max` (1024) à la limite Windows minimale (16384)



Ne pas combiner le paramètre 'Security=ADS' avec le paramètre 'Password Server'.
(Par défaut, Samba détecte le bon DC à contacter automatiquement).

- Lorsque vous y êtes invité, appuyez sur **entrée** pour afficher la configuration du client d'audit.
- Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

11. Fermez l'utilitaire de configuration CIFS : `exit`

12. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

ou

Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit comme requis :

- Connectez-vous à distance au nœud d'administration d'un site :
 - Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - Entrez la commande suivante pour passer à la racine : `su -`
 - Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
- Fermez la connexion du shell sécurisé distant au nœud d'administration : `exit`

13. Déconnectez-vous du shell de commande : `exit`

Informations associées

["Mise à niveau du logiciel"](#)

Ajout d'un utilisateur ou d'un groupe à un partage d'audit CIFS

Vous pouvez ajouter un utilisateur ou un groupe à un partage d'audit CIFS intégré à l'authentification AD.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

La procédure suivante concerne un partage d'audit intégré à l'authentification AD.



L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés. Entrez : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config	

add-audit-share	set-authentication	validate-config	
enable-disable-share	set-netbios-name	help	
add-user-to-share	join-domain	exit	
remove-user-from-share	add-password-server		
modify-group	remove-password-server		
	add-wins-server		
	remove-wins-server		

5. Commencez à ajouter un utilisateur ou un groupe : `add-user-to-share`

Une liste numérotée de partages d'audit qui ont été configurés s'affiche.

6. Lorsque vous y êtes invité, entrez le numéro du partage d'audit (audit-export) : `audit_share_number`

On vous demande si vous souhaitez donner un accès à ce partage d'audit à un utilisateur ou à un groupe.

7. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user` ou `group`
8. Lorsque vous êtes invité à entrer le nom de l'utilisateur ou du groupe pour ce partage d'audit AD, entrez le nom.

L'utilisateur ou le groupe est ajouté en lecture seule pour le partage d'audit à la fois dans le système d'exploitation du serveur et dans le service CIFS. La configuration Samba est rechargée pour permettre à l'utilisateur ou au groupe d'accéder au partage du client d'audit.

9. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

10. Répétez ces étapes pour chaque utilisateur ou groupe ayant accès au partage d'audit.

11. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

- Impossible de trouver le fichier `/etc/samba/include/cifs-interfaces.inc`
- Impossible de trouver le fichier `/etc/samba/include/cifs-filesystem.inc`
- Impossible de trouver le fichier `/etc/samba/include/cifs-custom-config.inc`
- Impossible de trouver le fichier `/etc/samba/include/cifs-shares.inc`
 - i. Lorsque vous y êtes invité, appuyez sur **entrée** pour afficher la configuration du client d'audit.
 - ii. Lorsque vous y êtes invité, appuyez sur **entrée**.

12. Fermez l'utilitaire de configuration CIFS : `exit`

13. Déterminez si vous devez activer des partages d'audit supplémentaires, comme suit :

- Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.
- Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit si nécessaire :
 - i. Connectez-vous à distance au nœud d'administration d'un site :
 - A. Saisissez la commande suivante : `ssh admin@grid_node_IP`
 - B. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - C. Entrez la commande suivante pour passer à la racine : `su -`
 - D. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - ii. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
 - iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`

14. Déconnectez-vous du shell de commande : `exit`

Suppression d'un utilisateur ou d'un groupe d'un partage d'audit CIFS

Vous ne pouvez pas supprimer le dernier utilisateur ou groupe autorisé à accéder au partage d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec les mots de passe du compte racine (disponible dans LEDIT package).

- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

3. Commencez à supprimer un utilisateur ou un groupe : `remove-user-from-share`

Une liste numérotée des partages d'audit disponibles pour le nœud d'administration s'affiche. Le partage d'audit est étiqueté audit-export.

4. Entrez le numéro du partage d'audit : `audit_share_number`

5. Lorsque vous êtes invité à supprimer un utilisateur ou un groupe : `user` ou `group`

Une liste numérotée d'utilisateurs ou de groupes pour le partage d'audit s'affiche.

6. Entrez le numéro correspondant à l'utilisateur ou au groupe que vous souhaitez supprimer : `number`

Le partage d'audit est mis à jour et l'utilisateur ou le groupe n'est plus autorisé à accéder au partage d'audit. Par exemple :

```
Enabled shares
  1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
  1. audituser
  2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Fermez l'utilitaire de configuration CIFS : `exit`
8. Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, désactivez le partage d'audit sur chaque site selon les besoins.
9. Déconnectez-vous de chaque shell de commande une fois la configuration terminée : `exit`

Informations associées

["Mise à niveau du logiciel"](#)

Modification du nom d'utilisateur ou de groupe d'un audit CIFS

Vous pouvez modifier le nom d'un utilisateur ou d'un groupe pour un partage d'audit CIFS en ajoutant un nouvel utilisateur ou un nouveau groupe, puis en supprimant l'ancien.

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Ajoutez un nouvel utilisateur ou un nouveau groupe portant le nom mis à jour au partage d'audit.
2. Supprimez l'ancien nom d'utilisateur ou de groupe.

Informations associées

["Mise à niveau du logiciel"](#)

["Ajout d'un utilisateur ou d'un groupe à un partage d'audit CIFS"](#)

["Suppression d'un utilisateur ou d'un groupe d'un partage d'audit CIFS"](#)

Vérification de l'intégration d'un audit CIFS

Le partage d'audit est en lecture seule. Les fichiers journaux sont destinés à être lus par des applications informatiques et la vérification ne comprend pas l'ouverture d'un fichier.

Il est considéré comme suffisant de vérifier que les fichiers journaux d'audit apparaissent dans une fenêtre de l'Explorateur Windows. Après vérification de la connexion, fermez toutes les fenêtres.

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 DÉLICTELLE (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.