Restaurez vos données après une panne de nœud d'administration

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-118/maintain/recovering-from-admin-node-failures.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommaire

Restaurez vos données après une panne de nœud d'administration . . . 1
Échec de la restauration à partir d'un nœud d'administration : workflow . . . 1
Restaurez vos données après une panne de nœud d'administration principal . . . 1
Restauration après les pannes de nœud d'administration principal : présentation . . . 1
La copie des journaux d'audit à partir d'un nœud d'administration principal a échoué . . . 1
Remplacez le nœud d'administration principal . . . 3
Configurez le nœud d'administration principal de remplacement . . . 3
Restaurez le journal d'audit sur le nœud d'administration principal restauré . . . 5
Restaurez la base de données du nœud d'administration lors de la récupération du nœud d'administration principal . . . 6
Restaurez les metrics Prometheus lors de la récupération du nœud d'administration principal . . . 8
Restaurez vos données en cas de défaillance d'un nœud d'administration non principal . . . 9
Restauration après des pannes de nœud d'administration non principal : présentation . . . 9
Copie des journaux d'audit à partir d'un nœud d'administration non primaire ayant échoué . . . 9
Remplacez un nœud d'administration non primaire . . . 10
Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire . . . 11
Restaurez le journal d'audit sur un nœud d'administration non primaire restauré . . . 13
Restaurez la base de données du nœud d'administration lors de la restauration d'un nœud d'administration non primaire . . . 14
Restaurez des metrics Prometheus lors de la récupération d'un nœud d'administration non primaire . . . 16

Restaurez vos données après une panne de nœud d'administration

Échec de la restauration à partir d'un nœud d'administration : workflow

Le processus de restauration d'un noeud d'administration dépend du noeud d'administration principal ou non primaire.

Les étapes générales de restauration d'un nœud d'administration principal ou non primaire sont les mêmes, bien que les détails de la procédure diffèrent.

Suivez toujours la procédure de récupération correcte pour le nœud d'administration que vous restaurez. Les procédures semblent identiques à un niveau élevé, mais diffèrent dans les détails.

Choix

- "Restaurez vos données après une panne de nœud d'administration principal"
- "Restaurez vos données en cas de défaillance d'un nœud d'administration non principal"

Restaurez vos données après une panne de nœud d'administration principal

Restauration après les pannes de nœud d'administration principal : présentation

Vous devez effectuer un ensemble spécifique de tâches pour effectuer une restauration suite à une défaillance d'un nœud d'administration principal. Le nœud d'administration principal héberge le service de nœud de gestion de la configuration (CMN) pour la grille.

Un nœud d'administration principal défectueux doit être remplacé rapidement. Le service de nœud de gestion de la configuration (CMN) sur le nœud d'administration principal est responsable de l'émission de blocs d'identifiants d'objets pour la grille. Ces identificateurs sont attribués aux objets lors de leur ingestion. Les nouveaux objets ne peuvent pas être ingérés à moins que des identifiants soient disponibles. L'ingestion d'objet peut se poursuivre pendant que le CMN n'est pas disponible car la quantité d'identifiants d'un mois environ est mise en cache dans la grille. Cependant, une fois les identificateurs mis en cache épuisés, aucun nouvel objet ne peut être ajouté.

> Vous devez réparer ou remplacer un nœud d'administration principal défectueux dans un délai d'environ un mois. Dans ce cas, la grille risque de perdre sa capacité à ingérer de nouveaux objets. La période exacte dépend de votre taux d'acquisition de l'objet : si vous avez besoin d'une évaluation plus précise de la durée de votre grille, contactez le support technique.

La copie des journaux d'audit à partir d'un nœud d'administration principal a échoué

Si vous pouvez copier les journaux d'audit à partir du nœud d'administration principal défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud

d'administration principal restauré une fois qu'il est en cours d'exécution.

Description de la tâche

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.

> Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

Étapes

1. Si possible, connectez-vous au nœud d'administration défaillant. Sinon, connectez-vous au nœud d'administration principal ou à un autre nœud d'administration, le cas échéant.
   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.

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

2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal :`service ams stop`
3. Accédez au répertoire d'exportation d'audit :

   ```
   cd /var/local/log
   ```

4. Renommez la source `audit.log` dans un nom de fichier numéroté unique. Par exemple, renommez le fichier audit.log en `2023-10-25.txt.1`.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

5. Redémarrez le service AMS : `service ams start`
6. Créez le répertoire pour copier tous les fichiers journaux d'audit vers un emplacement temporaire sur un nœud de grille distinct : `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

7. Copiez tous les fichiers journaux d'audit à l'emplacement temporaire : `scp -p * admin@`

`grid_node_IP`:/var/local/tmp/saved-audit-logs

Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

8. Se déconnecter en tant que racine : `exit`

Remplacez le nœud d'administration principal

Pour restaurer un noeud d'administration principal, vous devez d'abord remplacer le matériel physique ou virtuel.

Vous pouvez remplacer un nœud d'administration principal défectueux par un nœud d'administration principal s'exécutant sur la même plate-forme, ou remplacer un nœud d'administration principal s'exécutant sur VMware ou un hôte Linux par un nœud d'administration principal hébergé sur une appliance de services.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement des nœuds (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration du nœud d'administration principal.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appliances de services	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Configurez le nœud d'administration principal de remplacement

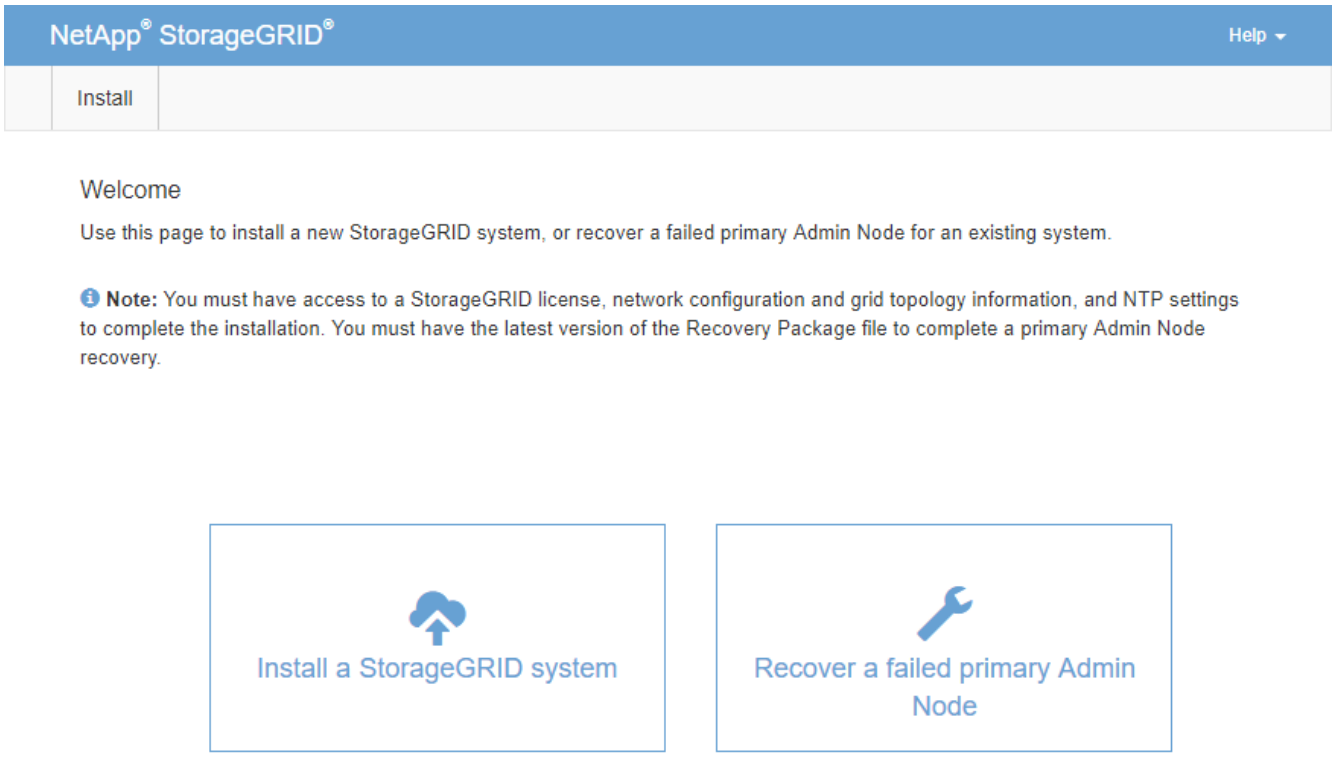
Le nœud de remplacement doit être configuré en tant que nœud d'administration principal de votre système StorageGRID.

Avant de commencer

- Pour les nœuds d'administration principaux hébergés sur des machines virtuelles, la machine virtuelle a été déployée, mise sous tension et initialisée.
- Pour les nœuds d'administration primaires hébergés sur une appliance de services, vous avez remplacé l'appliance et installé le logiciel. Voir la "instructions d'installation de votre appareil".
- Vous disposez de la dernière sauvegarde du fichier du progiciel de récupération (`sgws-recovery-package-id-revision.zip`).
- Vous avez la phrase secrète pour le provisionnement.

Étapes

1. Ouvrez votre navigateur Web et accédez à `https://primary_admin_node_ip`.



2. Cliquez sur **récupérer un noeud d'administration principal ayant échoué**.
3. Téléchargez la sauvegarde la plus récente du progiciel de restauration :
   a. Cliquez sur **Parcourir**.
   b. Recherchez le fichier de progiciel de récupération le plus récent pour votre système StorageGRID et cliquez sur **Ouvrir**.
4. Saisissez la phrase secrète pour le provisionnement.
5. Cliquez sur **Démarrer la récupération**.

   Le processus de récupération commence. Le Grid Manager peut devenir indisponible pendant quelques minutes lorsque les services requis démarrent. Une fois la récupération terminée, la page de connexion s'affiche.

6. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du noeud d'administration.

   > Pour configurer une confiance de partie utilisatrice, reportez-vous à la section "Configurer l'authentification unique". Pour accéder au certificat de serveur par défaut, connectez-vous au shell de commande du noeud d'administration. Accédez au `/var/local/mgmt-api` et sélectionnez `server.crt` fichier.

7. Déterminez si vous devez appliquer un correctif.

a. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
b. Sélectionnez **NOEUDS**.
c. Dans la liste de gauche, sélectionnez le nœud d'administration principal.
d. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.
e. Sélectionnez un autre nœud de grille.
f. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.
   - Si les versions affichées dans les champs **version du logiciel** sont identiques, vous n'avez pas besoin d'appliquer un correctif.
   - Si les versions affichées dans les champs **version du logiciel** sont différentes, vous devez le faire "appliquer un correctif" Pour mettre à jour le nœud d'administration principal restauré vers la même version.

Restaurez le journal d'audit sur le nœud d'administration principal restauré

Si vous avez pu conserver le journal d'audit à partir du nœud d'administration principal défaillant, vous pouvez le copier sur le nœud d'administration principal en cours de restauration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un noeud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

> Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :
>
> - Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
> - Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.
>
> Voir "Configurez les messages d'audit et les destinations des journaux" pour plus d'informations.

Étapes

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

   a. Saisissez la commande suivante : `ssh admin@recovery_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.

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

2. Vérifiez quels fichiers d'audit ont été conservés : `cd /var/local/log`

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration restauré : `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.

5. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration restauré : `chown ams-user: bycast *`

6. Se déconnecter en tant que racine : `exit`

Vous devez également restaurer tout accès client existant au partage d'audit. Pour plus d'informations, voir "Configurez l'accès client d'audit".

Restaurez la base de données du nœud d'administration lors de la récupération du nœud d'administration principal

Si vous souhaitez conserver les informations historiques sur les attributs, les alarmes et les alertes sur un noeud d'administration principal ayant échoué, vous pouvez restaurer la base de données du noeud d'administration. Vous ne pouvez restaurer cette base de données que si votre système StorageGRID inclut un autre noeud d'administration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de défaillance d'un nœud d'administration, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données contient les informations suivantes :

- Historique des alertes
- Historique des alarmes
- Les données d'attributs historiques, qui sont utilisées dans les graphiques et les rapports texte disponibles à partir de la page **SUPPORT** > **Outils** > **topologie de grille**.

Lorsque vous restaurez un noeud d'administration, le processus d'installation du logiciel crée une base de données de noeud d'administration vide sur le noeud récupéré. Toutefois, la nouvelle base de données comprend uniquement les informations pour les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement.

Si vous avez restauré un noeud d'administration principal et que votre système StorageGRID dispose d'un autre noeud d'administration, vous pouvez restaurer les informations historiques en copiant la base de données du noeud d'administration d'un noeud d'administration non primaire (le *source Admin Node*) vers le noeud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données du nœud d'administration.

> La copie de la base de données du nœud d'administration peut prendre plusieurs heures. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   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.
2. Depuis le nœud d'administration source, arrêtez le service MI : `service mi stop`
3. Depuis le nœud d'administration source, arrêtez le service Management application Program interface (mgapi) : `service mgmt-api stop`
4. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :
      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. Arrêtez le service MI : `service mi stop`
   c. Arrêt du service mgmt-api : `service mgmt-api stop`
   d. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`
   e. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.
   f. Copiez la base de données du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Lorsque vous y êtes invité, confirmez que vous souhaitez remplacer la base DE données MI sur le nœud d'administration restauré.

      La base de données et ses données historiques sont copiées dans le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré.

   h. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé

privée de l'agent SSH. Entrez :`ssh-add -D`

5. Redémarrez les services sur le nœud d'administration source : `service servermanager start`

Restaurez les metrics Prometheus lors de la récupération du nœud d'administration principal

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration principal défaillant. Les metrics de Prometheus ne peuvent être restaurés que si votre système StorageGRID inclut un autre nœud d'administration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un nœud d'administration principal et que votre système StorageGRID dispose d'un autre nœud d'administration, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus à partir d'un nœud d'administration non primaire (le *source Admin Node*) vers le nœud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données Prometheus.

> La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   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.
2. Depuis le nœud d'administration source, arrêter le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :
      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. Arrêtez le service Prometheus : `service prometheus stop`

c. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`

d. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

e. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Lorsque vous y êtes invité, appuyez sur **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le noeud d'administration restauré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :`ssh-add -D`

4. Redémarrez le service Prometheus sur le nœud d'administration source.`service prometheus start`

Restaurez vos données en cas de défaillance d'un nœud d'administration non principal

Restauration après des pannes de nœud d'administration non principal : présentation

Vous devez effectuer les tâches suivantes pour effectuer une restauration à partir d'une panne de nœud d'administration non primaire. Un nœud d'administration héberge le service de nœud de gestion de la configuration (CMN) et est appelé nœud d'administration principal. Bien que vous puissiez avoir plusieurs nœuds d'administration, chaque système StorageGRID n'inclut qu'un seul nœud d'administration principal. Tous les autres nœuds d'administration sont des nœuds d'administration non primaires.

Copie des journaux d'audit à partir d'un nœud d'administration non primaire ayant échoué

Si vous pouvez copier les journaux d'audit depuis le nœud d'administration défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration non primaire restauré après son exécution.

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.

> Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

1. Si possible, connectez-vous au nœud d'administration défaillant. Sinon, connectez-vous au nœud d'administration principal ou à un autre nœud d'administration, le cas échéant.
   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.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal :`service ams stop`
3. Accédez au répertoire d'exportation d'audit :

   ```
   cd /var/local/log
   ```
4. Renommez le fichier source audit.log en un nom de fichier numéroté unique. Par exemple, renommez le fichier audit.log en `2023-10-25.txt.1`.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
5. Redémarrez le service AMS : `service ams start`
6. Créez le répertoire pour copier tous les fichiers journaux d'audit vers un emplacement temporaire sur un nœud de grille distinct : `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.
7. Copiez tous les fichiers journaux d'audit à l'emplacement temporaire : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.
8. Se déconnecter en tant que racine : `exit`

Remplacez un nœud d'administration non primaire

Pour restaurer un noeud d'administration non primaire, vous devez d'abord remplacer le

matériel physique ou virtuel.

Vous pouvez remplacer un noeud d'administration non primaire défaillant par un noeud d'administration non primaire exécuté sur la même plate-forme, ou remplacer un noeud d'administration non primaire exécuté sur VMware ou un hôte Linux par un noeud d'administration non primaire hébergé sur une appliance de services.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement de nœud (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration de nœud d'administration non primaire.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appliances de services	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire

Après avoir remplacé un noeud d'administration non primaire, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

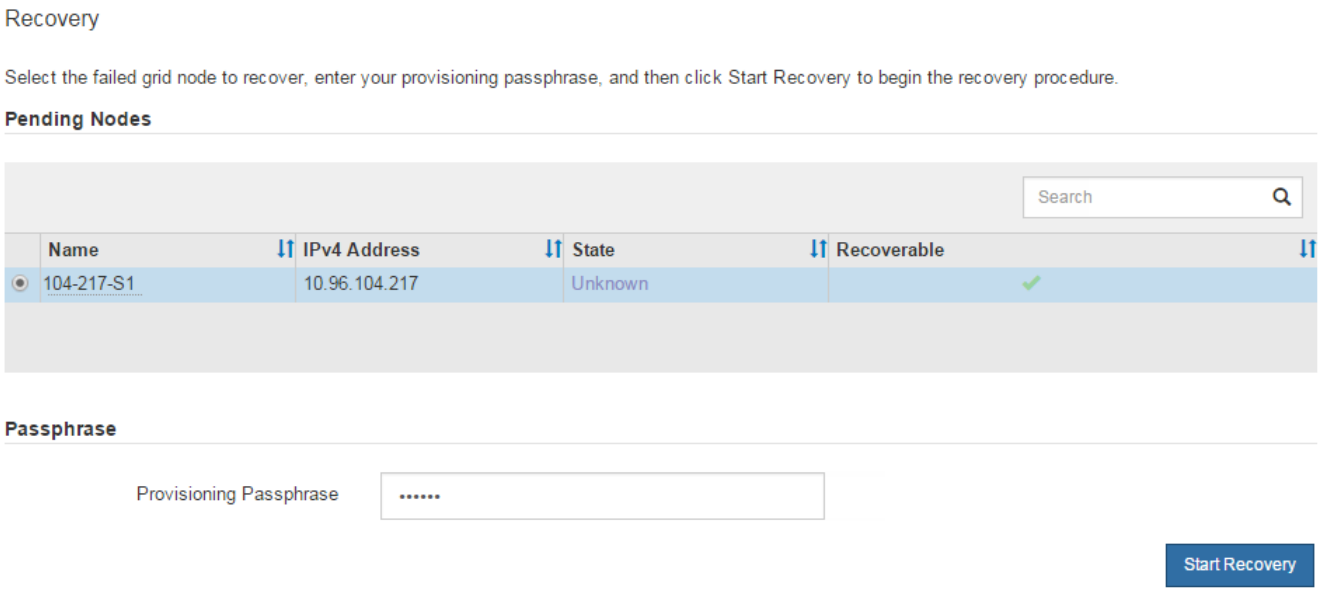
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **récupération**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

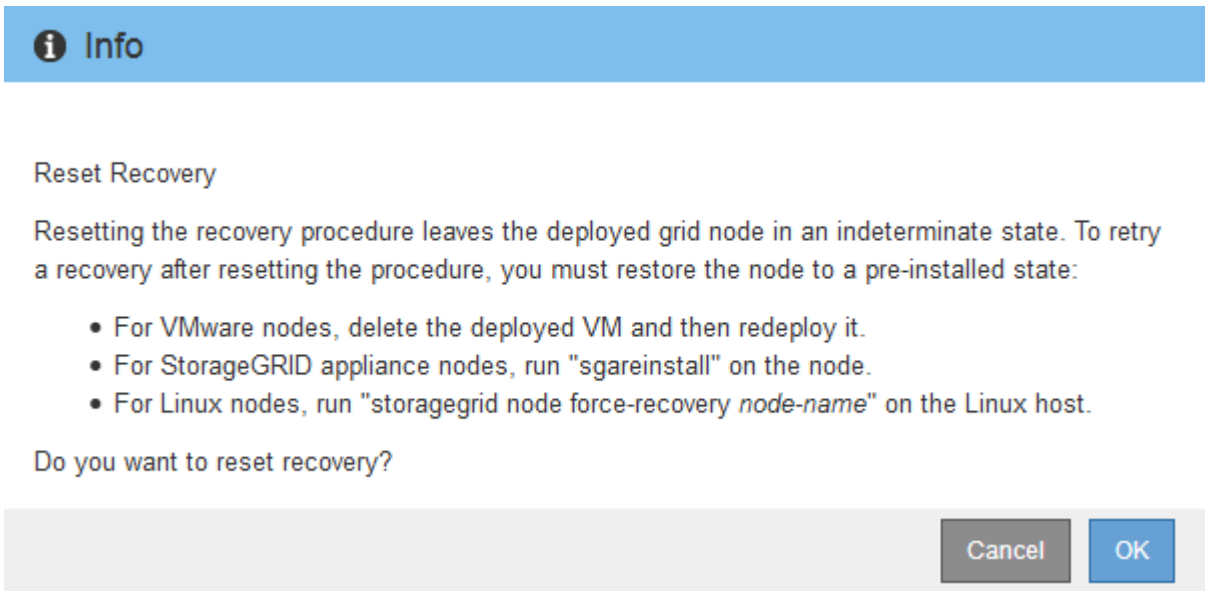
   Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la phrase de passe de provisionnement *.
4. Cliquez sur **Démarrer la récupération**.



5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.

> Pendant l'exécution de la procédure de récupération, vous pouvez cliquer sur **Réinitialiser** pour lancer une nouvelle restauration. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.



Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appliance** : si vous souhaitez réessayer la récupération après la réinitialisation de la procédure, vous devez restaurer le nœud de l'appliance à un état préinstallé en cours d'exécution `sgareinstall` sur le nœud. Voir "Préparez l'appareil pour la réinstallation (remplacement de la plate-forme uniquement)".

6. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du noeud d'administration.

> Pour configurer une confiance de partie utilisatrice, reportez-vous à la section "Configurer l'authentification unique". Pour accéder au certificat de serveur par défaut, connectez-vous au shell de commande du noeud d'administration. Accédez au `/var/local/mgmt-api` et sélectionnez `server.crt` fichier.

Restaurez le journal d'audit sur un nœud d'administration non primaire restauré

Si vous avez pu conserver le journal d'audit à partir du noeud d'administration non primaire défaillant, de sorte que les informations du journal d'audit historique soient conservées, vous pouvez le copier sur le noeud d'administration non primaire que vous êtes en train de récupérer.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un noeud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

> Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :
>
> - Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
> - Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.
>
> Voir "Configurez les messages d'audit et les destinations des journaux" pour plus d'informations.

Étapes

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

   a. Saisissez la commande suivante :

      `ssh admin@recovery_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.

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

2. Vérifiez quels fichiers d'audit ont été conservés :

   ```
   cd /var/local/log
   ```

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration restauré :

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.
5. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration restauré :

   ```
   chown ams-user:bycast *
   ```

6. Se déconnecter en tant que racine : `exit`

Vous devez également restaurer tout accès client existant au partage d'audit. Pour plus d'informations, voir "Configurez l'accès client d'audit".

Restaurez la base de données du nœud d'administration lors de la restauration d'un nœud d'administration non primaire

Si vous souhaitez conserver les informations historiques relatives aux attributs, aux alarmes et aux alertes sur un nœud d'administration non primaire qui a échoué, vous pouvez restaurer la base de données du nœud d'administration à partir du nœud d'administration principal.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de défaillance d'un nœud d'administration, les informations historiques stockées dans sa base de

données de nœud d'administration sont perdues. Cette base de données contient les informations suivantes :

- Historique des alertes
- Historique des alarmes
- Les données d'attributs historiques, qui sont utilisées dans les graphiques et les rapports texte disponibles à partir de la page **SUPPORT** > **Outils** > **topologie de grille**.

Lorsque vous restaurez un noeud d'administration, le processus d'installation du logiciel crée une base de données de noeud d'administration vide sur le noeud récupéré. Toutefois, la nouvelle base de données comprend uniquement les informations pour les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement.

Si vous avez restauré un noeud d'administration non primaire, vous pouvez restaurer les informations d'historique en copiant la base de données du noeud d'administration principal (le noeud d'administration *source*) vers le noeud récupéré.

> La copie de la base de données du nœud d'administration peut prendre plusieurs heures. Certaines fonctions de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud source.

Étapes

1. Connectez-vous au nœud d'administration source :
   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.
2. Exécutez la commande suivante depuis le nœud d'administration source. Saisissez ensuite la phrase de passe de provisionnement si vous y êtes invité. `recover-access-points`
3. Depuis le nœud d'administration source, arrêtez le service MI : `service mi stop`
4. Depuis le nœud d'administration source, arrêtez le service Management application Program interface (mgapi) : `service mgmt-api stop`
5. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :
      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. Arrêtez le service MI : `service mi stop`
   c. Arrêt du service mgmt-api : `service mgmt-api stop`
   d. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`
   e. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.
   f. Copiez la base de données du nœud d'administration source vers le nœud d'administration restauré :

`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Lorsque vous y êtes invité, confirmez que vous souhaitez remplacer la base DE données MI sur le nœud d'administration restauré.

   La base de données et ses données historiques sont copiées dans le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré.

h. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :`ssh-add -D`

6. Redémarrez les services sur le nœud d'administration source : `service servermanager start`

Restaurez des metrics Prometheus lors de la récupération d'un nœud d'administration non primaire

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration non primaire qui a échoué.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un noeud d'administration non primaire, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus du noeud d'administration principal (le *source Admin Node*) vers le noeud d'administration récupéré.

> La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   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.
2. Depuis le nœud d'administration source, arrêter le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :

a. Connectez-vous au nœud d'administration restauré :

   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. Arrêtez le service Prometheus : `service prometheus stop`

c. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`

d. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

e. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Lorsque vous y êtes invité, appuyez sur **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le noeud d'administration restauré.

   La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :`ssh-add -D`

4. Redémarrez le service Prometheus sur le nœud d'administration source.`service prometheus start`

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.