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

StorageGRID 11.8

NetApp
May 17, 2024

Sommaire

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 2
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 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

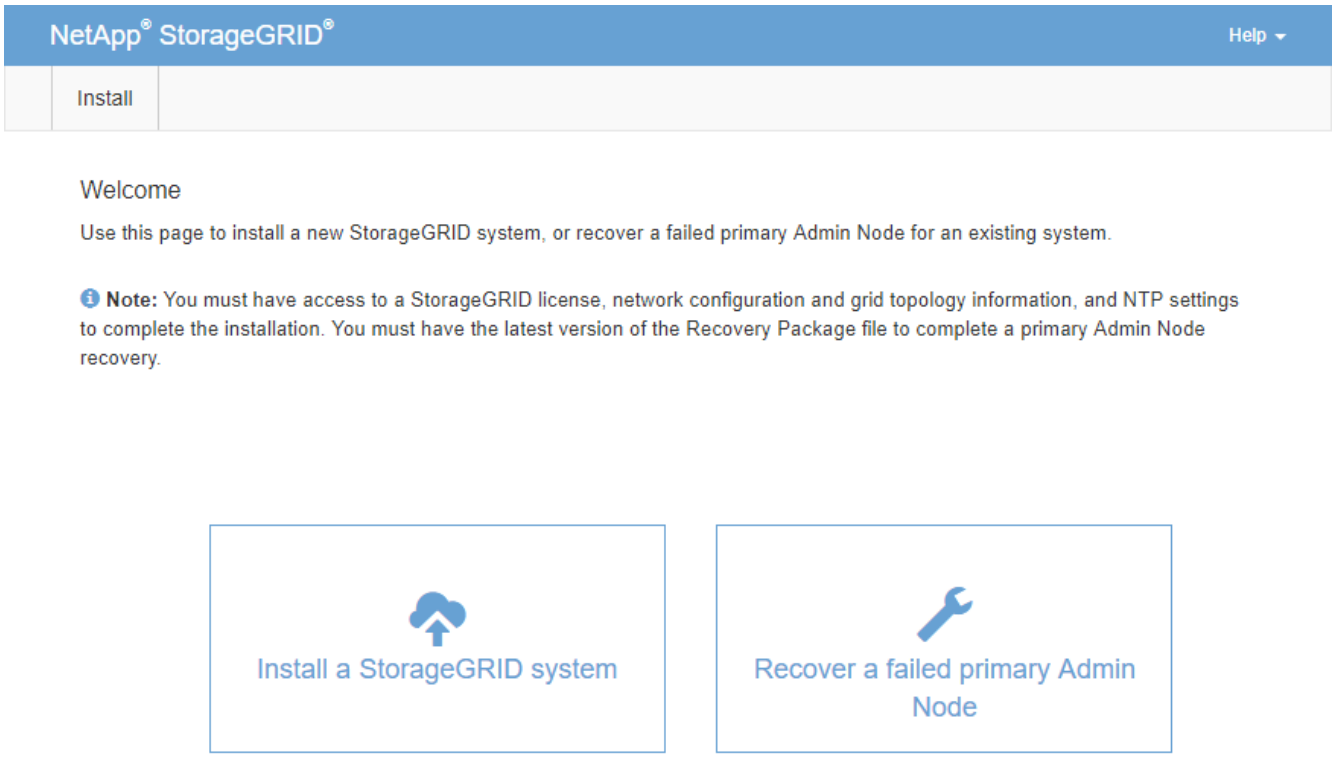
Le nœud de remplacement doit être configuré en tant que nœud d'administration principal de votre système StorageGRID.

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`