Configurez l'accès client d'audit

StorageGRID 11.7

NetApp
April 12, 2024

Sommaire

Configurez l’accès client d’audit

Configurer l’accès client d’audit pour NFS

Le nœud d’administration, via le service AMS (Audit Management System), consigne tous les événements système vérifiés dans un fichier journal disponible via le partage d’audit, qui est ajouté à chaque nœud d’administration lors de l’installation. Le partage d’audit est automatiquement activé en tant que partage en lecture seule.

Pour accéder aux journaux d’audit, vous pouvez configurer l’accès client aux partages d’audit pour NFS. Ou bien, c’est possible "utilisez un serveur syslog externe".

Le système StorageGRID utilise une reconnaissance positive pour éviter toute perte de messages d’audit avant qu’ils ne soient écrits dans le fichier journal. Un message reste placé dans la file d’attente d’un service jusqu’à ce que le service AMS ou un service de relais d’audit intermédiaire en ait reconnu le contrôle. Pour plus d’informations, voir "Examiner les journaux d’audit".

Avant de commencer

- Vous avez le `Passwords.txt` avec le mot de passe root/admin.
- Vous avez le `Configuration.txt` Fichier (disponible dans le progiciel de récupération).
- Le client d’audit utilise NFS version 3 (NFSv3).

Description de la tâche

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

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 certains services ne sont pas répertoriés comme étant 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 NFS. Entrez : `config_nfs.rb`

```
-----------------------------------------------------------------
| Shares                | Clients              | Config          |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
-----------------------------------------------------------------
```

5. Ajouter le client d'audit : `add-audit-share`
   a. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : `client_IP_address`
   b. Lorsque vous y êtes invité, appuyez sur **entrée**.
6. Si plusieurs clients d'audit sont autorisés à accéder au partage d'audit, ajoutez l'adresse IP de l'utilisateur supplémentaire : `add-ip-to-share`
   a. Entrez le numéro du partage d'audit : *`audit_share_number`*
   b. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : *`client_IP_address`*
   c. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration NFS s'affiche.

   d. Répétez ces sous-étapes pour chaque client d'audit supplémentaire ayant accès au partage d'audit.
7. Vérifiez éventuellement votre configuration.
   a. Saisissez les informations suivantes : `validate-config`

      Les services sont vérifiés et affichés.

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

      L'utilitaire de configuration NFS s'affiche.

   c. Fermez l'utilitaire de configuration NFS : `exit`
8. Déterminez si vous devez activer des partages d'audit sur d'autres sites.
   - 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 du 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 supplémentaire.

iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant. Entrez : `exit`

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

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accordez l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage ou supprimez un client d'audit existant en supprimant son adresse IP.

Ajouter un client d'audit NFS à un partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accorder l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage d'audit.

Avant de commencer

- Vous avez le `Passwords.txt` avec le mot de passe du compte root/admin.
- Vous avez le `Configuration.txt` Fichier (disponible dans le progiciel de récupération).
- Le client d'audit utilise NFS version 3 (NFSv3).

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 NFS : `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Entrez : `add-ip-to-share`

La liste des partages d'audit NFS activés sur le nœud d'administration s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Entrez le numéro du partage d'audit : *audit_share_number*
5. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : *client_IP_address*

   Le client d'audit est ajouté au partage d'audit.

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

   L'utilitaire de configuration NFS s'affiche.

7. Répétez les étapes pour chaque client d'audit qui doit être ajouté au partage d'audit.
8. Vérifiez éventuellement votre configuration : `validate-config`

   Les services sont vérifiés et affichés.

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

      L'utilitaire de configuration NFS s'affiche.

9. Fermez l'utilitaire de configuration NFS : `exit`
10. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

    Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, activez éventuellement ces partages d'audit si nécessaire :

    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 cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
    c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
11. Déconnectez-vous du shell de commande : `exit`

Vérifier l'intégration de l'audit NFS

Après avoir configuré un partage d'audit et ajouté un client d'audit NFS, vous pouvez monter le partage client d'audit et vérifier que les fichiers sont disponibles à partir du partage d'audit.

Étapes

1. Vérifiez la connectivité (ou la variante du système client) à l'aide de l'adresse IP côté client du nœud d'administration hébergeant le service AMS. Entrez : `ping IP_address`

   Vérifiez que le serveur répond, indiquant la connectivité.

2. Montez le partage d'audit en lecture seule à l'aide d'une commande appropriée au système d'exploitation

client. Un exemple de commande Linux est (entrez sur une ligne) :

`mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

Utilisez l'adresse IP du nœud d'administration hébergeant le service AMS et le nom de partage prédéfini pour le système d'audit. Le point de montage peut être n'importe quel nom sélectionné par le client (par exemple, `myAudit` dans la commande précédente).

3. Vérifiez que les fichiers sont disponibles à partir du partage d'audit. Entrez : `ls myAudit /*`

   où `myAudit` est le point de montage du partage d'audit. Au moins un fichier journal doit être répertorié.

Supprimer un client d'audit NFS du partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Vous pouvez supprimer un client d'audit existant en supprimant son adresse IP.

Avant de commencer

- Vous avez le `Passwords.txt` avec le mot de passe du compte root/admin.
- Vous avez le `Configuration.txt` Fichier (disponible dans le progiciel de récupération).

Description de la tâche

Vous ne pouvez pas supprimer la dernière adresse IP autorisée pour accéder au partage d'audit.

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 NFS : `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Supprimez l'adresse IP du partage d'audit : `remove-ip-from-share`

   Une liste numérotée de partages d'audit configurés sur le serveur s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Saisissez le numéro correspondant au partage d'audit : *`audit_share_number`*

   Une liste numérotée d'adresses IP autorisées à accéder au partage d'audit s'affiche.

5. Saisissez le numéro correspondant à l'adresse IP que vous souhaitez supprimer.

   Le partage d'audit est mis à jour et l'accès n'est plus autorisé à partir d'un client d'audit possédant cette adresse IP.

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

   L'utilitaire de configuration NFS s'affiche.

7. Fermez l'utilitaire de configuration NFS : `exit`
8. Si votre déploiement StorageGRID est un déploiement de plusieurs sites de data Center avec des nœuds d'administration supplémentaires sur les autres sites, désactivez les partages d'audit suivants :
   a. Connectez-vous à distance au nœud d'administration de chaque 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 cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.
   c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
9. Déconnectez-vous du shell de commande : `exit`

Modifier l'adresse IP d'un client d'audit NFS

Procédez comme suit si vous devez modifier l'adresse IP d'un client d'audit NFS.

Étapes

1. Ajouter une nouvelle adresse IP à un partage d'audit NFS existant.
2. Supprimez l'adresse IP d'origine.

Informations associées

- "Ajouter un client d'audit NFS à un partage d'audit"
- "Supprimer un client d'audit NFS du partage d'audit"

Informations sur le copyright

Informations sur les marques commerciales