Gérer les nœuds d'administration

StorageGRID

NetApp
October 03, 2025

Sommaire

Gérer les nœuds d’administration

Qu’est-ce qu’un nœud d’administration

Des nœuds d’administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Chaque grid doit être connecté à un nœud d’administration principal et doit comporter un nombre quelconque de nœuds d’administration non primaires pour assurer la redondance.

Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un noeud d’administration. Vous pouvez vous connecter à n’importe quel nœud d’administration et chaque nœud d’administration affiche une vue similaire du système StorageGRID. Cependant, les procédures de maintenance doivent être effectuées à l’aide du nœud d’administration principal.

Les nœuds d’administration peuvent également être utilisés pour équilibrer la charge du trafic des clients S3 et Swift.

Les nœuds d’administration hébergent les services suivants :

- Service AMS
- Service CMN
- Service NMS
- Service Prometheus
- Services d’équilibrage de la charge et haute disponibilité (pour prendre en charge le trafic des clients S3 et Swift)

Les nœuds d’administration prennent également en charge l’API de gestion (Management application Program interface) pour traiter les requêtes depuis l’API de gestion du grid et l’API de gestion des locataires. Voir Utilisez l’API de gestion du grid.

Qu’est-ce que le service AMS

Le service du système de gestion de la vérification (AMS) suit l’activité et les événements du système.

Qu’est-ce que le service CMN

Le service de nœud de gestion de la configuration (CMN) gère les configurations de connectivité et de protocoles à l’échelle du système nécessaires à tous les services. De plus, le service CMN est utilisé pour exécuter et surveiller les tâches de la grille. Il n’y a qu’un seul service CMN par déploiement StorageGRID. Le nœud d’administration qui héberge le service CMN est appelé nœud d’administration principal.

En quoi consiste le service NMS

Le service Network Management System (NMS) alimente les options de surveillance, de rapport et de configuration affichées via le gestionnaire de grille, l’interface navigateur du système StorageGRID.

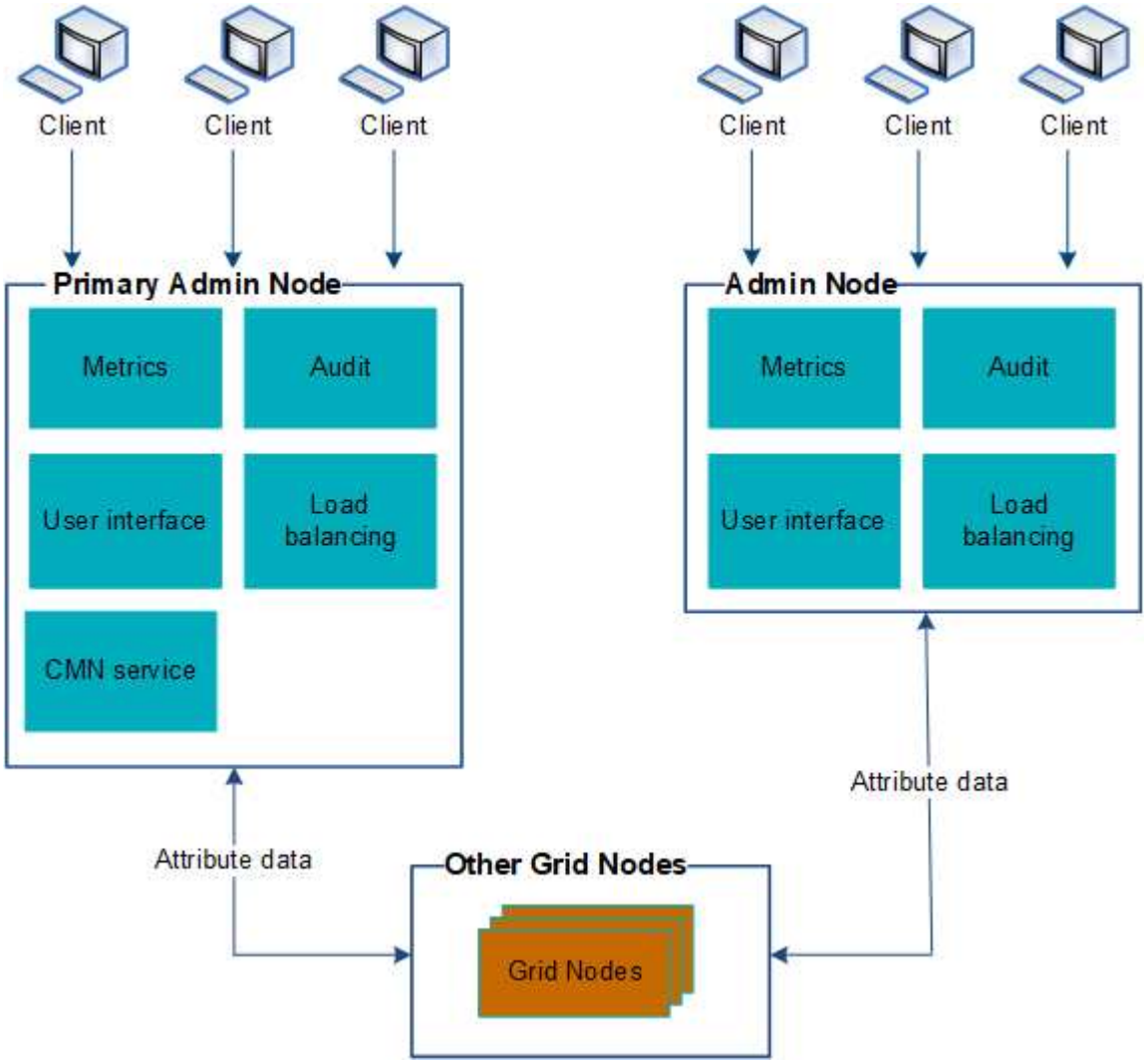
Définition du service Prometheus

Le service Prometheus collecte les metrics de séries chronologiques des services sur tous les nœuds.

Utiliser plusieurs nœuds d'administration

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de contrôler et de configurer en continu votre système StorageGRID, même en cas de panne d'un nœud d'administration.

Si un nœud d'administration devient indisponible, le traitement des attributs continue, les alertes et les alarmes (système hérité) sont toujours déclenchées et les notifications par e-mail et les messages AutoSupport sont toujours envoyés. Toutefois, plusieurs nœuds d'administration n'assurent pas la protection du basculement, à l'exception des notifications et des messages AutoSupport. En particulier, les accusés de réception d'alarme d'un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration.



Deux options s'offrent à vous pour continuer à afficher et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à tout autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration haute disponibilité, les clients Web peuvent continuer à accéder à Grid Manager ou au Gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA. Voir Gérez les groupes haute disponibilité.

Lors de l'utilisation d'un groupe haute disponibilité, l'accès est interrompu en cas de défaillance du nœud d'administration principal. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA bascule vers un autre noeud d'administration du groupe.

Certaines tâches de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration principal. En cas de panne du nœud d'administration principal, celui-ci doit être restauré avant que le système StorageGRID ne fonctionne à nouveau entièrement.

Identifiez le nœud d'administration principal

Le nœud d'administration principal héberge le service CMN. Certaines procédures de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration principal.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site* nœud d'administration**, puis sélectionnez ➕ Pour développer l'arborescence de la topologie et afficher les services hébergés sur ce nœud d'administration.

   Le nœud d'administration principal héberge le service CMN.

3. Si ce nœud d'administration n'héberge pas le service CMN, vérifiez les autres nœuds d'administration.

Sélectionnez un expéditeur préféré

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, vous pouvez sélectionner le nœud d'administration qui doit être l'expéditeur préféré des notifications. Par défaut, le nœud d'administration principal est sélectionné, mais n'importe quel nœud d'administration peut être l'expéditeur préféré.

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

La page **CONFIGURATION système Options d'affichage** indique quel nœud d'administration est actuellement sélectionné comme expéditeur préféré. Le nœud d'administration principal est sélectionné par défaut.

Dans des conditions normales de fonctionnement du système, seul l'expéditeur préféré envoie les notifications suivantes :

- Messages AutoSupport

- Notifications SNMP
- E-mails d'alerte
- E-mails d'alarme (système hérité)

Cependant, tous les autres nœuds d'administration (expéditeurs de secours) surveillent l'expéditeur préféré. Si un problème est détecté, un expéditeur en attente peut également envoyer ces notifications.

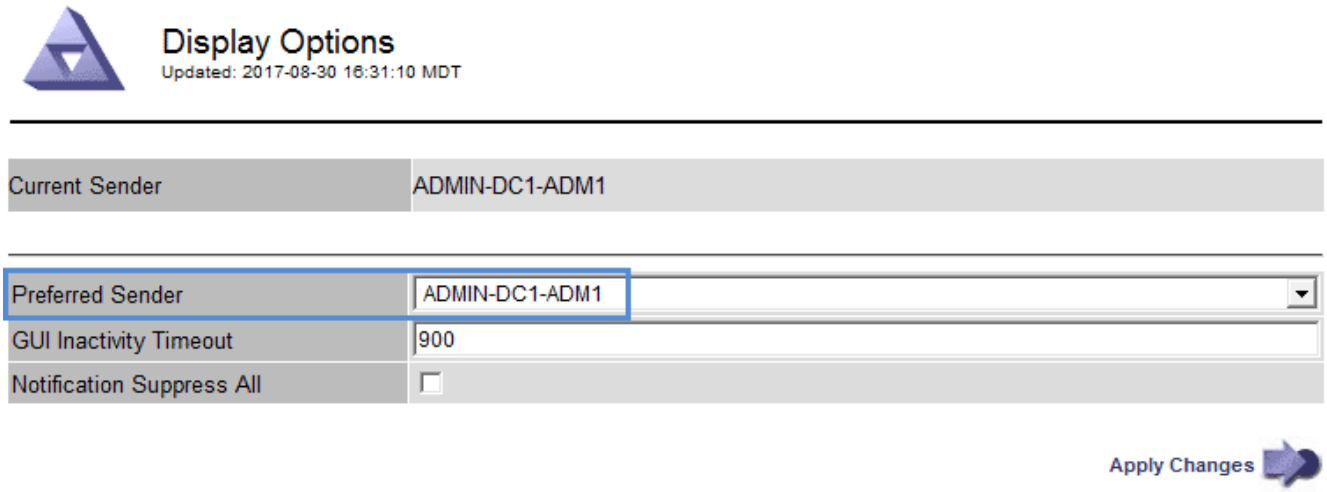
Dans les cas suivants, l'expéditeur préféré et l'expéditeur de secours peuvent envoyer des notifications :

- Si les nœuds d'administration deviennent « en attente » les uns des autres, l'expéditeur préféré et les expéditeurs de secours tenteront d'envoyer des notifications, et plusieurs copies de notifications peuvent être reçues.
- Lorsqu'un expéditeur en veille détecte des problèmes avec l'expéditeur préféré et commence à envoyer des notifications, il est possible que l'expéditeur préféré puisse récupérer sa capacité à envoyer des notifications. Dans ce cas, des notifications en double peuvent être envoyées. L'expéditeur en attente interrompt l'envoi des notifications lorsqu'il ne détecte plus d'erreurs sur l'expéditeur préféré.

> Lorsque vous testez les notifications d'alarme et les messages AutoSupport, tous les nœuds Admin envoient l'e-mail de test. Lorsque vous testez les notifications d'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité.

Étapes

1. Sélectionnez **CONFIGURATION système Options d'affichage**.
2. Dans le menu Options d'affichage, sélectionnez **Options**.
3. Sélectionnez le noeud d'administration que vous souhaitez définir comme expéditeur préféré dans la liste déroulante.



4. Sélectionnez **appliquer les modifications**.

   Le nœud d'administration est défini comme l'expéditeur préféré des notifications.

Afficher l’état des notifications et les files d’attente

Le service Network Management System (NMS) sur les nœuds Admin envoie des notifications au serveur de messagerie. Vous pouvez afficher l’état actuel du service NMS ainsi que la taille de sa file d’attente de notifications sur la page moteur d’interface.

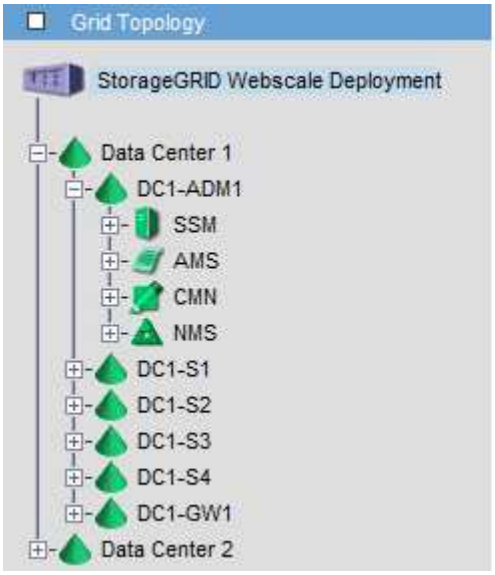
Pour accéder à la page moteur d’interface, sélectionnez **SUPPORT Outils topologie de grille**. Enfin, sélectionnez ***site Admin Node* NMS interface Engine**.

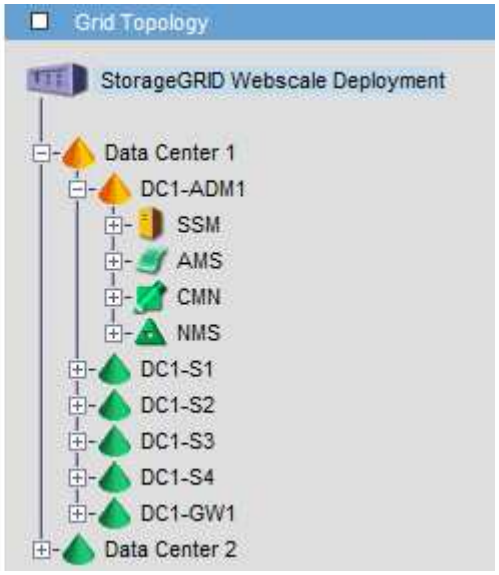
Les notifications sont traitées via la file d’attente de notifications par e-mail et sont envoyées au serveur de messagerie l’une après l’autre dans l’ordre dans lequel elles sont déclenchées. En cas de problème (par exemple, une erreur de connexion réseau) et si le serveur de messagerie n’est pas disponible lors de la tentative d’envoi de la notification, une tentative de renvoi de la notification au serveur de messagerie se poursuit pendant une période de 60 secondes. Si la notification n’est pas envoyée au serveur de messagerie après 60 secondes, elle est supprimée de la file d’attente de notifications et une tentative d’envoi de la notification suivante dans la file d’attente est effectuée. Comme les notifications peuvent être supprimées de la file d’attente de notifications sans être envoyées, il est possible qu’une alarme puisse être déclenchée sans qu’une notification soit envoyée. Dans le cas où une notification est supprimée de la file d’attente sans être envoyée, l’alarme mineure EN MINUTES (état de notification par e-mail) est déclenchée.

Affichage des alarmes acquittées par les nœuds d’administration (système hérité)

Lorsque vous accusez réception d’une alarme sur un nœud d’administration, l’alarme acquittée n’est copiée sur aucun autre nœud d’administration. Comme les accusés de réception ne sont pas copiés sur d’autres nœuds d’administration, il est possible que l’arborescence de la topologie de grille ne soit pas identique pour chaque nœud d’administration.

Cette différence peut être utile lors de la connexion de clients Web. Les clients Web peuvent avoir différentes vues du système StorageGRID selon les besoins de l’administrateur.





Notez que les notifications sont envoyées depuis le nœud d’administration où l’accusé de réception a lieu.

Configurez l'accès client d'audit

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. Pour faciliter l'accès aux journaux d'audit, vous pouvez configurer l'accès des clients aux partages d'audit pour CIFS et NFS.

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.

> L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID. Si vous avez la possibilité d'utiliser CIFS ou NFS, choisissez NFS.

Configurer 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.

Configurer les 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 avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous avez 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.

   a. Entrez : `set-authentication`
   b. Lorsque vous êtes invité à installer Windows Workgroup ou Active Directory, entrez : `workgroup`
   c. Lorsque vous y êtes invité, entrez le nom du groupe de travail : *`workgroup_name`*
   d. 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.

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

      L'utilitaire de configuration CIFS s'affiche.

6. Ajouter un client d'audit :

   a. Entrez : `add-audit-share`

Le partage est automatiquement ajouté en lecture seule.

b. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : *user*

c. Lorsque vous y êtes invité, entrez le nom d'utilisateur de l'audit : *audit_user_name*

d. Lorsque vous y êtes invité, entrez un mot de passe pour l'utilisateur d'audit : *password*

e. Lorsque vous y êtes invité, saisissez à nouveau le même mot de passe pour le confirmer : *password*

f. 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 smbd 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`

Configurer les 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 avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous disposez du nom d'utilisateur et du mot de passe CIFS Active Directory.
- Vous avez 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.

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

      Utilisez des lettres majuscules.

   e. 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.

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

      L'utilitaire de configuration CIFS s'affiche.

6. Rejoindre le domaine :
   a. Si ce n'est pas déjà fait, démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`
   b. Rejoindre le domaine : `join-domain`
   c. 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`

d. 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.

e. 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`
    - rlimiit_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).

    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**.

    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 :

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

Ajoutez un utilisateur ou 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 avez le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).

- Vous avez 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`

Supprimer un utilisateur ou 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 avez le `Passwords.txt` Fichier avec les mots de passe du compte racine (disponible dans LEDIT package).

- Vous avez 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`

Modifier un nom d'utilisateur ou de groupe de partage d'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

- Ajoutez un utilisateur ou un groupe à un partage d'audit CIFS
- Supprimer un utilisateur ou un groupe d'un partage d'audit CIFS

Vérifier l'intégration de l'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.

Configuration du client d'audit pour NFS

Le partage d'audit est automatiquement activé en tant que partage en lecture seule.

Ce dont vous avez besoin

- Vous avez le `Passwords.txt` Fichier avec le mot de passe root/admin (disponible dans LEDIT paquet).
- Vous avez le `Configuration.txt` Fichier (disponible dans LEDIT paquet).
- 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 des services ne sont pas répertoriés comme 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.

Ce dont vous avez besoin

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

- 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.

Ce dont vous avez besoin

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

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

Description de la tâche

Vous ne pouvez pas supprimer la dernière adresse IP autorisée à 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