Configurez l'accès client d'audit

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-116/admin/configuring-audit-clients-for-workgroup.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

Configurez l’accès client d’audit . . . 1
Configurer des clients d’audit pour CIFS . . . 1
Configurer les clients d’audit pour Workgroup . . . 1
Configurer les clients d’audit pour Active Directory . . . 4
Ajoutez un utilisateur ou un groupe à un partage d’audit CIFS . . . 7
Supprimer un utilisateur ou un groupe d’un partage d’audit CIFS . . . 9
Modifier un nom d’utilisateur ou de groupe de partage d’audit CIFS . . . 11
Vérifier l’intégration de l’audit CIFS . . . 11
Configuration du client d’audit pour NFS . . . 12
Ajouter un client d’audit NFS à un partage d’audit . . . 13
Vérifier l’intégration de l’audit NFS . . . 15
Supprimer un client d’audit NFS du partage d’audit . . . 15
Modifier l’adresse IP d’un client d’audit NFS . . . 17

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

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.