Présentation du message d'audit

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

Présentation du message d’audit

Ces instructions contiennent des informations sur la structure et le contenu des messages d’audit StorageGRID et des journaux d’audit. Vous pouvez utiliser ces informations pour lire et analyser la piste d’audit de l’activité du système.

Ces instructions s’adresse aux administrateurs responsables de la production de rapports d’activité et d’utilisation du système qui nécessitent une analyse des messages d’audit du système StorageGRID.

Vous êtes supposé avoir une bonne compréhension de la nature des activités vérifiées dans le système StorageGRID. Pour utiliser le fichier journal texte, vous devez avoir accès au partage d’audit configuré sur le nœud d’administration.

Informations associées

"Administrer StorageGRID"

Flux et conservation des messages d’audit

Tous les services StorageGRID génèrent des messages d’audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d’audit passent du système StorageGRID au système `audit.log` fichier.

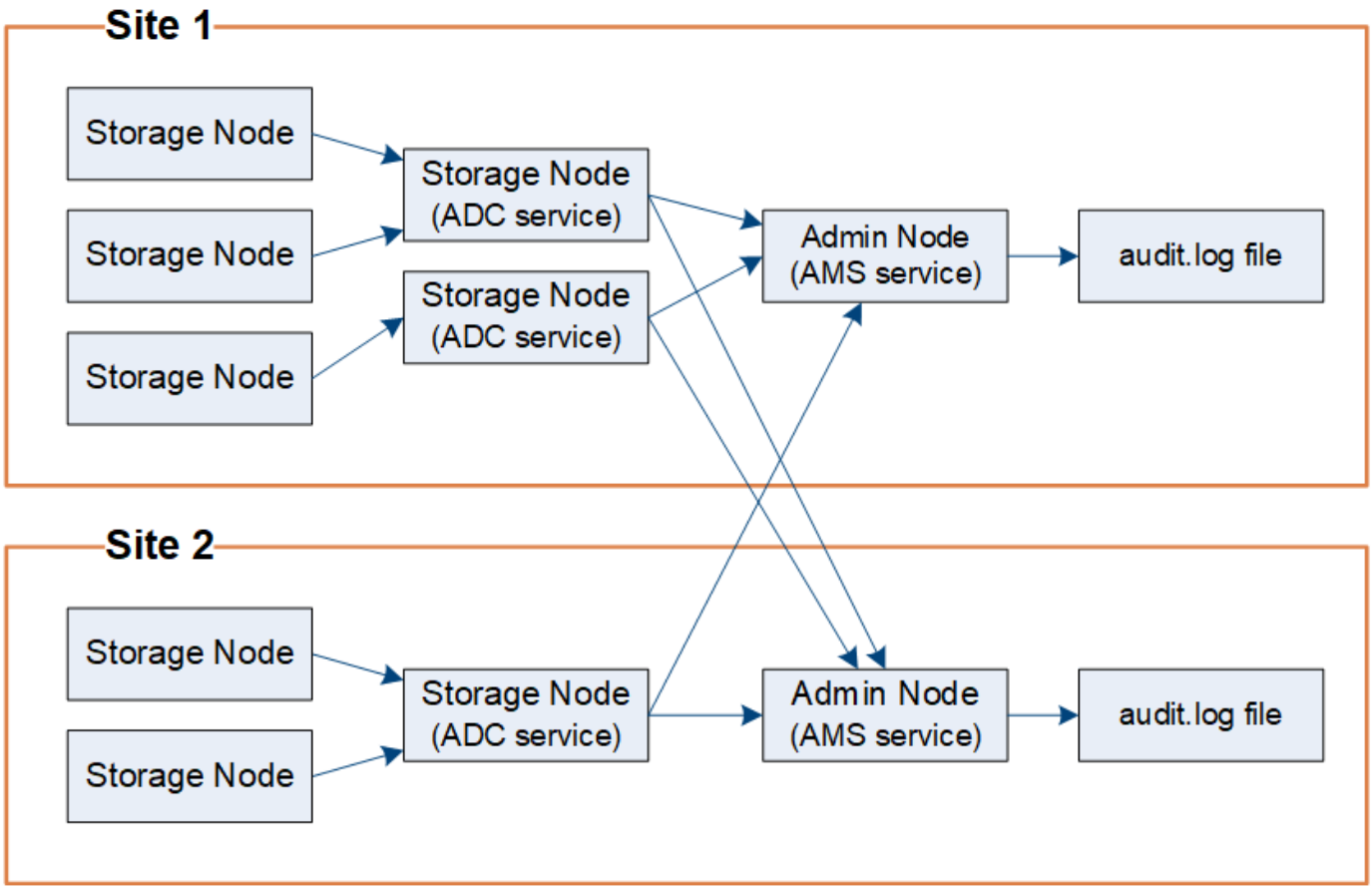
Flux de message d’audit

Les messages d’audit sont traités par des nœuds d’administration et par les nœuds de stockage disposant d’un service ADC (administrative Domain Controller).

Comme indiqué dans le schéma de flux des messages d’audit, chaque nœud StorageGRID envoie ses messages d’audit à l’un des services ADC du site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

De son tour, chaque service ADC agit comme un relais et envoie sa collection de messages d’audit à chaque nœud d’administration du système StorageGRID, ce qui donne à chaque nœud d’administration un enregistrement complet de l’activité du système.

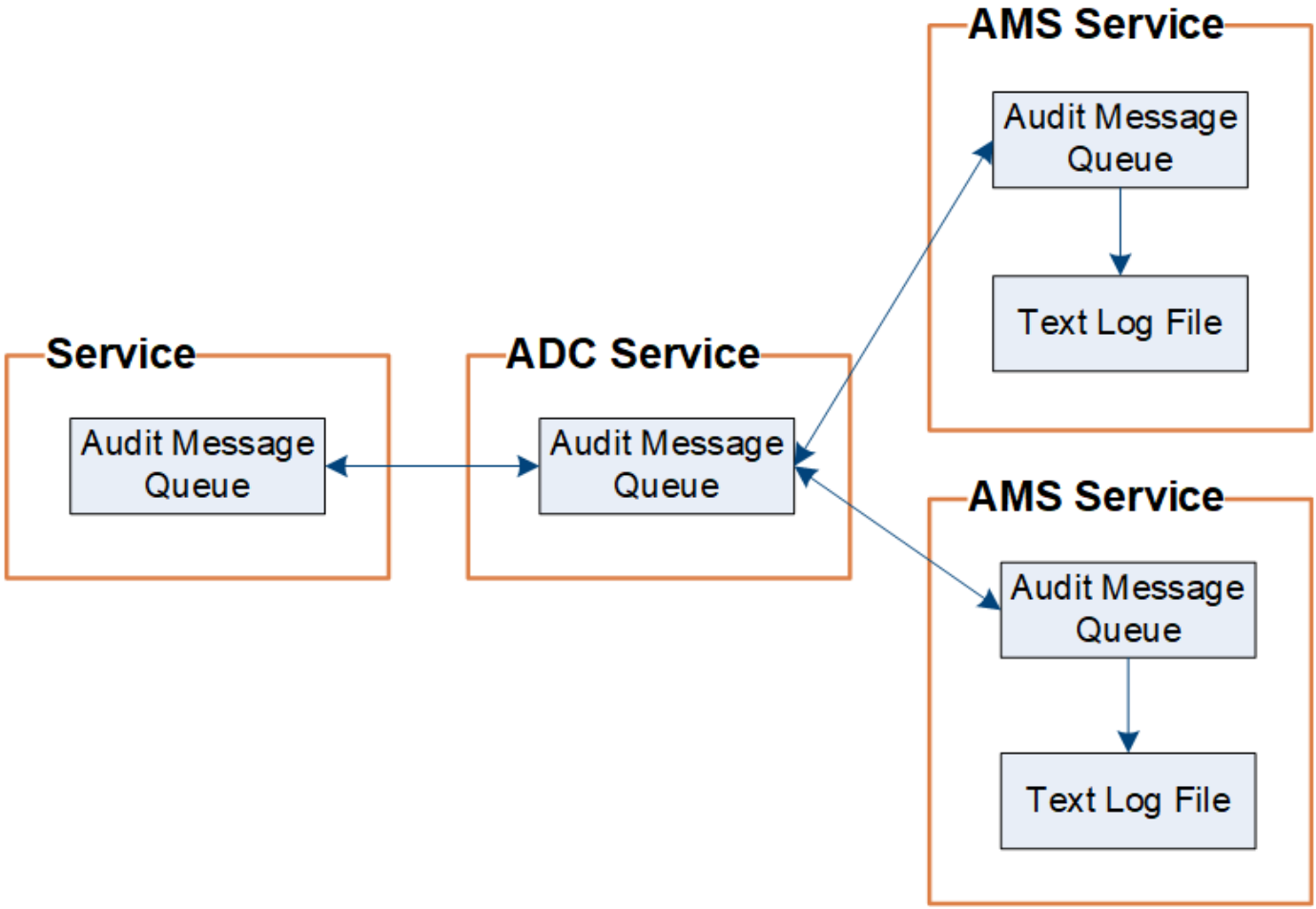
Chaque nœud d’administration stocke les messages d’audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



Conservation des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit ne soit perdu avant d'être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou transmet un message d'audit, celui-ci est stocké dans une file d'attente de messages d'audit sur le disque système du nœud de la grille. Une copie du message est toujours conservée dans une file d'attente de messages d'audit jusqu'à ce que le message soit écrit dans le fichier journal d'audit du nœud d'administration `/var/local/audit/export` répertoire. Cela permet d'éviter la perte d'un message d'audit pendant le transport.



La file d'attente des messages d'audit peut augmenter temporairement en raison de problèmes de connectivité réseau ou d'une capacité d'audit insuffisante. Au fur et à mesure que les files d'attente augmentent, elles consomment davantage d'espace disponible dans chaque nœud `/var/local/` répertoire. Si le problème persiste et que le répertoire des messages d'audit d'un nœud devient trop plein, les nœuds individuels priorisent le traitement de leur carnet de commandes et deviennent temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pouvez voir les comportements suivants :

- Si le `/var/local/audit/export` Le répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration sera signalé comme indisponible pour les nouveaux messages d'audit jusqu'à ce que le répertoire ne soit plus plein. Les demandes des clients S3 et Swift ne sont pas affectées. L'alarme XAMS (Unreable Audit Revers) est déclenchée lorsqu'un référentiel d'audit est inaccessible.
- Si le `/var/local/` Le répertoire utilisé par un nœud de stockage avec le service ADC devient plein à 92 %, le nœud sera signalé comme indisponible pour les messages d'audit jusqu'à ce que le répertoire soit plein à seulement 87 %. Les demandes des clients S3 et Swift vers d'autres nœuds ne sont pas affectées. L'alarme NRLY (relais d'audit disponibles) est déclenchée lorsque les relais d'audit sont inaccessibles.

  > Si aucun nœud de stockage n'est disponible avec le service ADC, les nœuds de stockage stockent les messages d'audit localement.

- Si le `/var/local/` Le répertoire utilisé par un nœud de stockage devient plein à 85 %. Le nœud refuse les demandes des clients S3 et Swift avec `503 Service Unavailable`.

Les types de problèmes suivants peuvent entraîner une augmentation très importante des files d'attente de messages d'audit :

- Panne d'un nœud d'administration ou d'un nœud de stockage avec le service ADC. Si l'un des nœuds du système est en panne, les nœuds restants peuvent devenir connectés à un nœud défaillant.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- Le `/var/local/` L'espace sur un nœud de stockage ADC est saturé pour des raisons sans rapport avec les messages d'audit. Dans ce cas, le nœud n'accepte plus de nouveaux messages d'audit et hiérarchise son carnet de commandes actuel, ce qui peut entraîner des arriérés sur les autres nœuds.

Alerte de file d'attente d'audit et alarme de messages d'audit en file d'attente (AMQS)

Pour vous aider à surveiller la taille des files d'attente de messages d'audit dans le temps, l'alerte **grande file d'attente d'audit** et l'alarme AMQS héritée sont déclenchées lorsque le nombre de messages dans une file d'attente de nœud de stockage ou une file d'attente de nœud d'administration atteint certains seuils.

Si l'alerte **grande file d'attente d'audit** ou l'alarme AMQS héritée est déclenchée, commencez par vérifier la charge sur le système—s'il y a eu un nombre important de transactions récentes, l'alerte et l'alarme doivent être résolus au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente la gravité, affichez un graphique de la taille de la file d'attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit consignés en modifiant le niveau d'audit pour les écritures du client et les lectures du client sur erreur ou Désactivé. Voir «"Modification des niveaux de messages d'audit"."

Dupliquer les messages

Le système StorageGRID adopte une approche prudente en cas de panne sur un réseau ou un nœud. Pour cette raison, des messages en double peuvent exister dans le journal d'audit.

Modification des niveaux de messages d'audit

Vous pouvez ajuster les niveaux d'audit pour augmenter ou diminuer le nombre de messages d'audit enregistrés dans le journal d'audit pour chaque catégorie de messages d'audit.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Les messages d'audit enregistrés dans le journal d'audit sont filtrés en fonction des paramètres de la page **Configuration** > **surveillance** > **Audit**.

Vous pouvez définir un niveau d'audit différent pour chacune des catégories de messages suivantes :

- **Système** : par défaut, ce niveau est défini sur Normal.
- **Stockage** : par défaut, ce niveau est défini sur erreur.
- **Gestion** : par défaut, ce niveau est défini sur Normal.

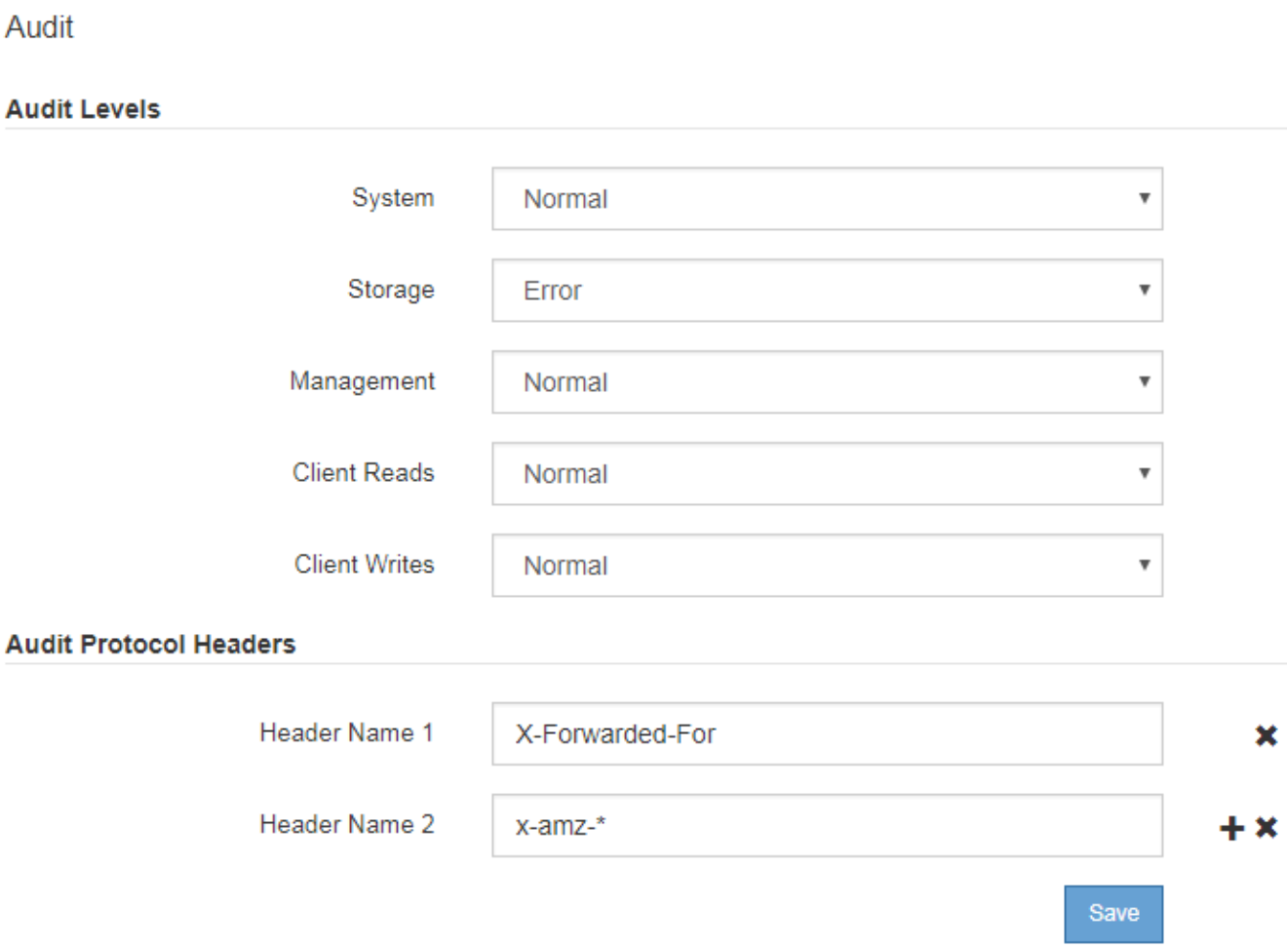
- **Lecture client** : par défaut, ce niveau est défini sur Normal.
- **Écrit client** : par défaut, ce niveau est défini sur Normal.

> Ces valeurs par défaut s'appliquent si vous avez installé StorageGRID à l'origine à l'aide de la version 10.3 ou ultérieure. Si vous avez mis à niveau à partir d'une version antérieure de StorageGRID, la valeur par défaut pour toutes les catégories est Normal.

> Durant les mises à niveau, les configurations des niveaux d'audit ne seront pas effectives immédiatement.

Étapes

1. Sélectionnez **Configuration** > **surveillance** > **Audit**.



2. Pour chaque catégorie de message d'audit, sélectionnez un niveau d'audit dans la liste déroulante :

Niveau d'audit	Description
Éteint	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont consignés—les messages d'audit pour lesquels le code de résultat n'a pas été « réussi » (CMC).

Niveau d'audit	Description
Normale	Les messages transactionnels standard sont consignés—les messages répertoriés dans ces instructions pour la catégorie.
Débogage	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit normal.

Les messages inclus pour tout niveau particulier incluent ceux qui seraient consignés aux niveaux supérieurs. Par exemple, le niveau Normal inclut tous les messages d'erreur.

3. Sous **en-têtes de protocole d'audit**, entrez le nom des en-têtes de requête HTTP à inclure dans les messages d'audit lecture client et écriture client. Utilisez un astérisque (*) comme caractère générique ou utilisez la séquence d'échappement (*) comme astérisque littéral. Cliquez sur le signe plus pour créer une liste de champs de nom d'en-tête.

   Les en-têtes de protocole d'audit ne s'appliquent qu'aux demandes S3 et Swift.

   Lorsque de tels en-têtes HTTP sont trouvés dans une requête, ils sont inclus dans le message d'audit sous le champ HTRH.

   Les en-têtes de requête de protocole d'audit ne sont consignés que si le niveau d'audit pour **lecture client** ou **écriture client** n'est pas **off**.

4. Cliquez sur **Enregistrer**.

Informations associées

"Messages d'audit système"

"Messages d'audit du stockage objet"

"Message d'audit de gestion"

"Messages d'audit de lecture du client"

"Administrer StorageGRID"

Accès au fichier journal d'audit

Le partage d'audit contient le partage actif `audit.log` fichier et tous les fichiers journaux d'audit compressés. Pour accéder facilement aux journaux d'audit, vous pouvez configurer l'accès des clients aux partages d'audit pour NFS et CIFS (obsolètes). Vous pouvez également accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Accédez au répertoire contenant les fichiers journaux d'audit :

```
cd /var/local/audit/export
```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Informations associées

"Administrer StorageGRID"

Rotation du fichier journal d'audit

Les fichiers journaux d'audit sont enregistrés sur un nœud d'administration `/var/local/audit/export` répertoire. Les fichiers journaux d'audit actifs sont nommés `audit.log`.

Une fois par jour, le actif `audit.log` le fichier est enregistré et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format *`yyyy-mm-dd.txt`*. Si plusieurs journaux d'audit sont créés dans un seul jour, les noms de fichiers utilisent la date d'enregistrement du fichier, ajoutée par un nombre, dans le format *`yyyy-mm-dd.txt.n`*. Par exemple : `2018-04-15.txt` et `2018-04-15.txt.1` Sont les premier et deuxième fichiers journaux créés et enregistrés le 15 avril 2018.

Après un jour, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, qui conserve la date originale. Avec le temps, cela entraîne la consommation du stockage alloué aux journaux d'audit sur le nœud d'administration. Un script surveille la consommation d'espace du journal d'audit et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le `/var/local/audit/export` répertoire. Les journaux d'audit sont supprimés en fonction de la date de création, le plus ancien étant supprimé en premier. Vous pouvez contrôler les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log`.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```