



# Présentation

## StorageGRID

NetApp  
October 03, 2025

# Sommaire

Examiner les journaux d'audit : présentation . . . . .	1
Flux et conservation des messages d'audit . . . . .	1
Flux de message d'audit . . . . .	1
Accéder au fichier journal d'audit . . . . .	4
Rotation du fichier journal d'audit . . . . .	5

# Examiner les journaux d'audit : présentation

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.

Pour utiliser le fichier journal texte, vous devez avoir accès au partage d'audit configuré sur le nœud d'administration.

Pour plus d'informations sur la configuration des niveaux de messages d'audit et sur l'utilisation d'un serveur syslog externe, reportez-vous à la section [Configurez les messages d'audit et les destinations des journaux](#).

## Informations associées

- [Administre 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.

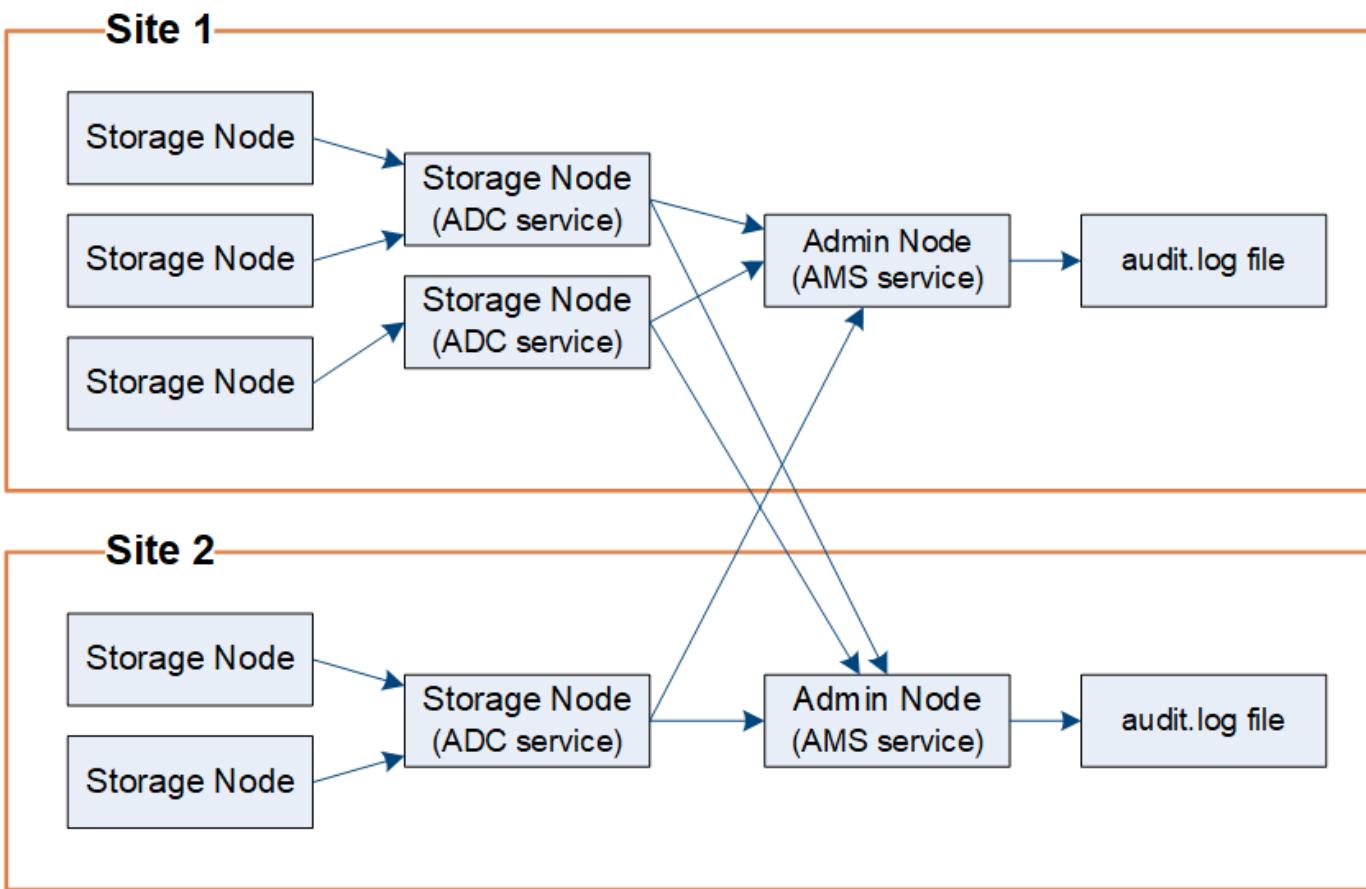
### Flux de message d'audit

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.

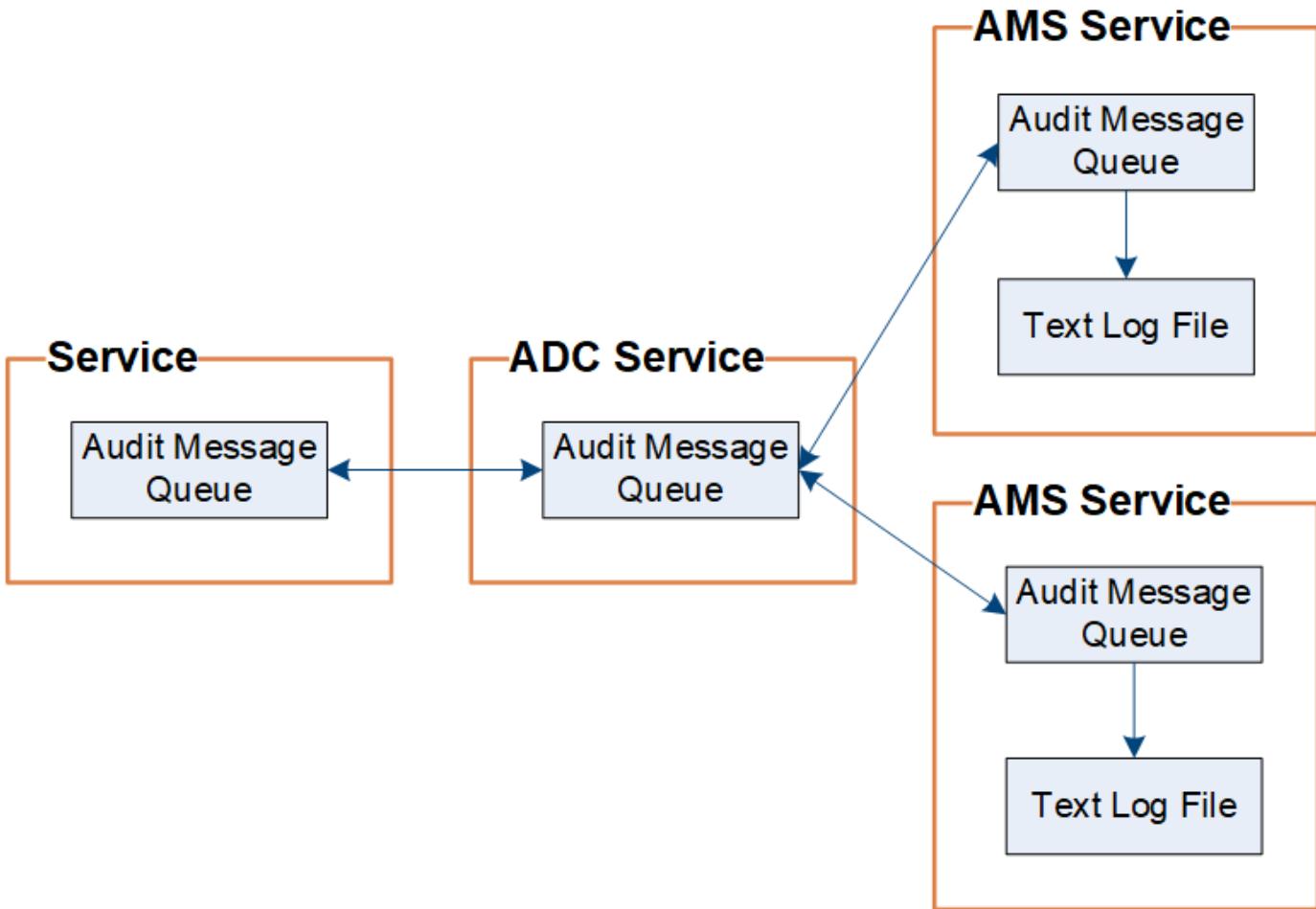
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé audit.log.



### 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 dans le /var/local/log/localaudit.log fichier.

- 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 «[Configurez les messages d'audit et les destinations des journaux](#).”

### **Duplicer 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.

## **Accéder 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 (le protocole CIFS est obsolète). 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.



Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir [Configurez les messages d'audit et les destinations des journaux](#).

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
```

## **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 JOUSSANCE, 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.