Examiner les journaux d'audit

StorageGRID software

NetApp
July 23, 2026

Sommaire

Examiner les journaux d'audit

Messages et journaux d'audit

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

Ces instructions s'adressent aux administrateurs chargés de produire des rapports sur l'activité et l'utilisation du système qui nécessitent l'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 l'utilisation d'un serveur syslog externe, consultez "Configurer la gestion des journaux et le serveur syslog externe".

Comment les messages d'audit transitent dans le système StorageGRID jusqu'au fichier audit.log pour conservation

Tous les services StorageGRID génèrent des messages d'audit lors du fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit circulent dans le système StorageGRID jusqu'au fichier `audit.log`.

Les procédures suivantes relatives aux messages d'audit et à leur conservation ne s'appliquent que si StorageGRID est configuré pour **Nœuds d'administration/nœuds locaux** ou **Nœud d'administration et serveur syslog externe**. Si StorageGRID est configuré pour « Nœuds locaux uniquement » (par défaut) ou « Serveur syslog externe », les messages d'audit sont enregistrés localement sur chaque nœud dans le fichier `/var/local/log/localaudit.log` et ne peuvent pas être traités par les nœuds d'administration ni par les nœuds de stockage.

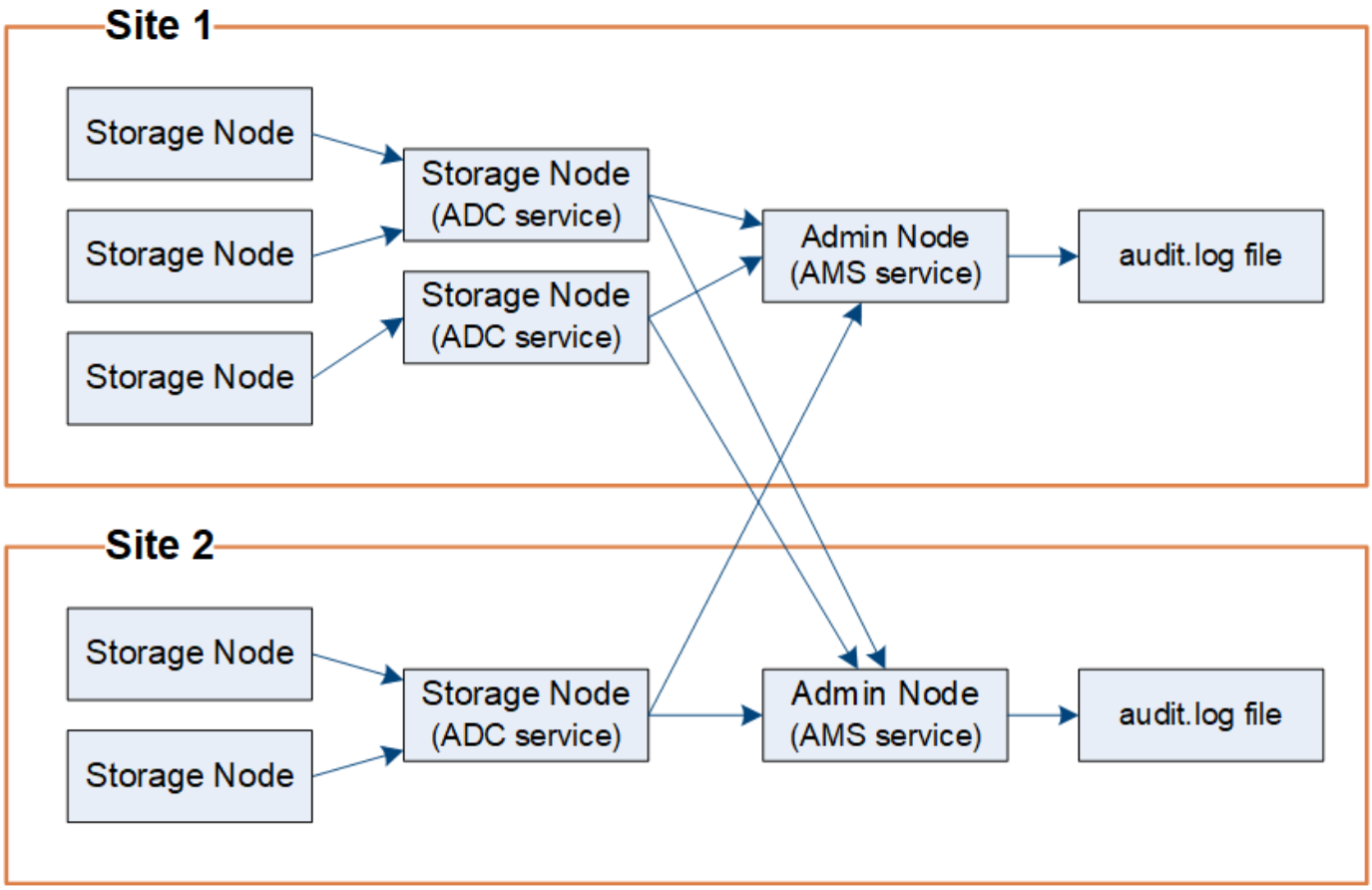
Flux de messages d'audit

Les messages d'audit sont traités par les nœuds d'administration lorsque StorageGRID est configuré pour **Nœuds d'administration/nœuds locaux** ou **Nœud d'administration et serveur syslog externe** et par les nœuds de stockage qui disposent d'un service Administrative Domain Controller (ADC).

Comme l'illustre le diagramme de flux des messages du journal des audits, chaque nœud StorageGRID envoie ses messages du journal des audits à l'un des services ADC du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

Chaque service ADC agit à son tour comme un relais et envoie sa collection de messages du journal des audits à chaque nœud d'administration dans le système StorageGRID, ce qui donne à chaque nœud d'administration un enregistrement complet de l'activité du système.

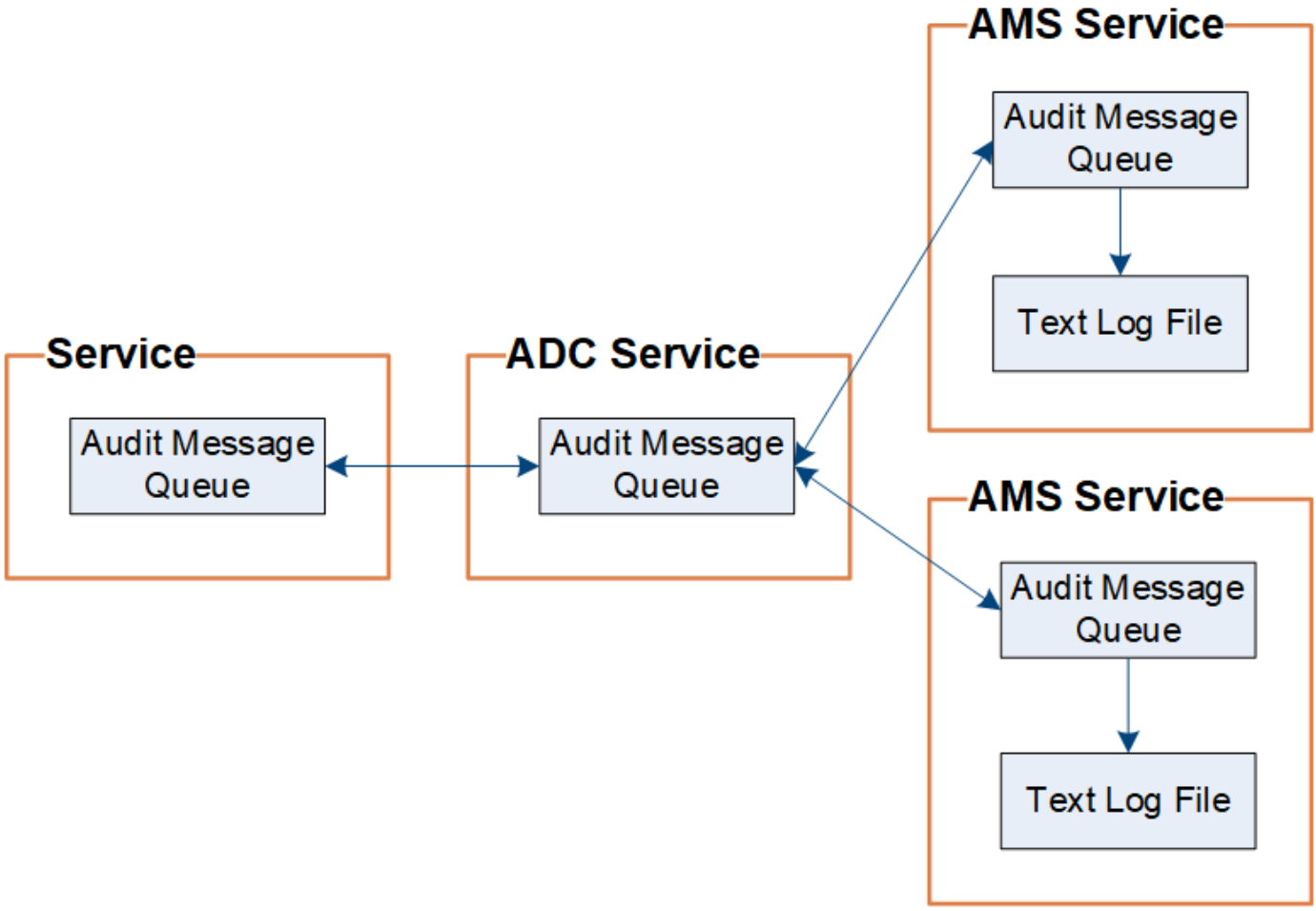
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



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 des audits.

Lorsqu'un nœud génère ou relaie un message d'audit, le message 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 des audits du répertoire `/var/local/audit/export` du nœud d'administration. Cela permet d'éviter la perte d'un message d'audit pendant le transport.



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

Plus précisément, vous pourriez observer les comportements suivants :

- Si le `/var/local/audit/export`répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration est signalé comme indisponible pour les nouveaux messages du journal des audits jusqu'à ce que le répertoire ne soit plus plein. Les requêtes client S3 ne sont pas affectées. L'alarme XAMS (Unreachable Audit Repositories) est déclenchée lorsqu'un référentiel du journal des audits est inaccessible.
- Si le `/var/local/`répertoire utilisé par un nœud de stockage avec le service ADC atteint 92 % de sa capacité, le nœud est signalé comme indisponible pour les messages du journal des audits jusqu'à ce que le répertoire ne soit rempli qu'à 87 %. Les requêtes du client S3 vers d'autres nœuds ne sont pas affectées. L'alarme NRLY (Available Audit Relays) est déclenchée lorsque les relais du journal des audits sont injoignables.

> S'il n'y a pas de nœuds de stockage disponibles avec le service ADC, les nœuds de stockage stockent les messages d'audit localement dans le fichier `/var/local/log/localaudit.log`.

- Si le `/var/local/`répertoire utilisé par un nœud de stockage atteint 85 % de sa

capacité, le nœud commence à refuser les requêtes des clients S3 avec `503 Service Unavailable.

Les types de problèmes suivants peuvent entraîner une augmentation considérable de la taille des files d'attente des messages d'audit :

- Une panne d'un nœud d'administration ou d'un nœud de stockage hébergeant le service ADC. Si l'un des nœuds du système est hors service, les nœuds restants peuvent accumuler un retard.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- L `/var/local/`espace sur un nœud de stockage ADC devient saturé pour des raisons indépendantes des messages d'audit. Dans ce cas, le nœud cesse d'accepter de nouveaux messages d'audit et donne la priorité à son arriéré actuel, ce qui peut entraîner des arriérés sur d'autres nœuds.

Alerte de grande file d'attente du journal des audits et alarme Audit Messages Queued (AMQS)

Pour vous aider à surveiller la taille des files d'attente de messages du journal des audits au fil du temps, l'alerte **File d'attente du journal des audits importante** et l'alarme AMQS héritée sont déclenchées lorsque le nombre de messages dans une file d'attente de Storage Node ou une file d'attente de Admin Node atteint certains seuils.

Si l'alerte **File d'attente d'audit importante** ou l'alarme AMQS héritée est déclenchée, commencez par vérifier la charge du système : s'il y a eu un nombre important de transactions récentes, l'alerte et l'alarme devraient se résoudre avec le temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et que sa gravité augmente, consultez un graphique de la taille de la file d'attente. Si le nombre augmente régulièrement pendant des heures ou des jours, il est probable que la charge d'audit ait dépassé la capacité d'audit du système. Réduisez le débit des opérations client ou diminuez le nombre de messages d'audit enregistrés en modifiant le niveau d'audit pour Client Writes et Client Reads sur Erreur ou Désactivé. Voir "Configurer la gestion des journaux et le serveur syslog externe".

Messages en double

Le système StorageGRID adopte une approche prudente en cas de panne de réseau ou de nœud. Pour cette raison, des messages en double peuvent figurer dans le journal des audits.

Accédez aux fichiers du journal des audits depuis la ligne de commandes du nœud d'administration StorageGRID

Le partage d'audit contient le fichier actif `audit.log` et tous les fichiers du journal des audits compressés. Vous pouvez accéder aux fichiers du journal des audits directement depuis la ligne de commandes du nœud d'administration.

Le `audit.log` fichier reste vide sauf si vous configurez StorageGRID pour **Admin Nodes/local nodes** ou **Admin Node and external syslog server**. Pour plus d'informations, consultez "Sélectionnez l'emplacement du journal".

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous devez avoir le fichier `Passwords.txt`.
- 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. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Accédez au répertoire contenant les fichiers du journal des audits :

   ```
   cd /var/local/audit/export/
   ```
3. Consultez le journal des audits actuel ou un fichier journal des audits enregistré, selon vos besoins.

Découvrez la rotation des fichiers du journal des audits dans StorageGRID

Si StorageGRID est configuré pour **Nœuds d'administration/nœuds locaux** ou **Nœud d'administration et serveur syslog externe**, les fichiers du journal des audits sont enregistrés dans le répertoire `/var/local/audit/export/` du nœud d'administration. Les fichiers actifs du journal des audits sont nommés `audit.log`.

> Vous pouvez, si vous le souhaitez, modifier la destination des journaux des audits et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements des audits continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Reportez-vous à "Configurer les messages d'audit et le serveur syslog externe".

Une fois par jour, le fichier actif `audit.log` est enregistré et un nouveau fichier `audit.log` est créé. Le nom du fichier enregistré indique le moment où il a été enregistré, au format *`yyyy-mm-dd.txt`*. Si plusieurs journaux des audits sont créés le même jour, les noms de fichiers utilisent la date à laquelle le fichier a été enregistré, suivie d'un numéro, au 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.

Au bout d'une journée, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, ce qui préserve la date d'origine. Au fil du temps, l'espace de stockage du nœud d'administration alloué aux journaux des audits est consommé. Un script surveille la consommation de l'espace du journal des audits et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le répertoire `/var/local/audit/export/`. Les journaux des audits sont supprimés en fonction de leur date de création. Les journaux les plus anciens sont supprimés en premier. Vous pouvez surveiller les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log`.

Cet exemple montre le fichier actif `audit.log`, le fichier de la veille (`2018-04-15.txt` et le fichier compressé de la veille (`2018-04-14.txt.gz`.

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

Format du fichier journal des audits

Découvrez le format des fichiers journal des audits dans StorageGRID

Les fichiers du journal des audits se trouvent sur chaque nœud d'administration et contiennent une collection de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- L'heure universelle coordonnée (UTC) de l'événement qui a déclenché le message d'audit (ATIM) au format ISO 8601, suivie d'un espace :

  YYYY-MM-DDTHH:MM:SS.UUUUUU, où *UUUUUU* sont des microsecondes.

- Le message d'audit lui-même, encadré par des crochets et commençant par `AUDT`.

L'exemple suivant présente trois messages d'audit dans un fichier journal des audits (les sauts de ligne ont été ajoutés pour plus de clarté). Ces messages ont été générés lorsqu'un locataire a créé un compartiment S3 et y a ajouté deux objets.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Dans leur format par défaut, les messages d'audit dans les fichiers du journal des audits ne sont pas faciles à lire ou à interpréter. Vous pouvez utiliser le "outil audit-explain" pour obtenir des résumés simplifiés des messages d'audit dans le journal des audits. Vous pouvez utiliser le "outil audit-sum" pour résumer combien d'opérations d'écriture, de lecture et de suppression ont été enregistrées et combien de temps ces opérations ont pris.

Utilisez l'outil audit-explain pour traduire les messages d'audit StorageGRID

Vous pouvez utiliser l' `audit-explain`outil pour traduire les messages d'audit du journal des audits dans un format facile à lire.

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous devez avoir le fichier `Passwords.txt`.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

À propos de cette tâche

L' `audit-explain`outil, disponible sur le nœud d'administration principal, fournit des résumés simplifiés des messages d'audit dans un journal des audits.

> L'`audit-explain`outil est principalement destiné à être utilisé par le support technique lors des opérations de dépannage. Le traitement des requêtes `audit-explain` peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur le fonctionnement de StorageGRID.

Cet exemple illustre un résultat typique de l' `audit-explain`outil. Ces quatre "SPUT"messages de journal des audits ont été générés lorsque le locataire S3 avec l'ID de compte 92484777680322627870 a utilisé des requêtes S3 PUT pour créer un compartiment nommé "bucket1" et y ajouter trois objets.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

L' `audit-explain`outil peut effectuer les opérations suivantes :

- Traitez les journaux des audits bruts ou compressés. Par exemple :

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Traitez plusieurs fichiers simultanément. Par exemple :

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- Acceptez les données d'entrée provenant d'un tube, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la commande `grep` ou d'autres moyens. Par exemple :

  ```
  grep SPUT audit.log | audit-explain
  ```

```
grep bucket-name audit.log | audit-explain
```

Étant donné que les journaux des audits peuvent être très volumineux et lents à analyser, vous pouvez gagner du temps en filtrant les parties que vous souhaitez examiner et en exécutant `audit-explain` sur ces parties, au lieu du fichier entier.

> ⓘ L' `audit-explain`outil n'accepte pas les fichiers compressés comme entrée via un tube. Pour traiter des fichiers compressés, fournissez leur nom de fichier comme argument en ligne de commande ou utilisez l' `zcat`outil pour les décompresser au préalable. Par exemple :
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilisez l' `help (-h)`option pour afficher les options disponibles. Par exemple :

```
$ audit-explain -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Saisissez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers que vous souhaitez analyser :

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   L' `audit-explain`outil affiche des interprétations lisibles par l'homme de tous les messages dans le ou les fichiers spécifiés.

   > ⓘ Pour réduire la longueur des lignes et améliorer la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous souhaitez voir les horodatages, utilisez l'option (`-t`timestamp.

Utilisez l'outil audit-sum pour résumer les messages d'audit de StorageGRID

Vous pouvez utiliser l' `audit-sum`outil pour compter les messages d'audit d'écriture, de lecture, d'en-tête et de suppression, ainsi que pour voir le temps (ou la taille) minimum, maximum et moyen pour chaque type d'opération.

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP du nœud d'administration principal.

À propos de cette tâche

L' `audit-sum`outil, disponible sur le nœud d'administration principal, récapitule le nombre d'opérations d'écriture, de lecture et de suppression enregistrées ainsi que la durée de ces opérations.

> L' `audit-sum`outil est principalement destiné à être utilisé par le support technique lors des opérations de dépannage. Le traitement des requêtes `audit-sum` peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur le fonctionnement de StorageGRID.

Cet exemple illustre le résultat typique de l' `audit-sum`outil. Cet exemple montre la durée des opérations de protocole.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

L' `audit-sum`outil fournit le nombre et l'heure des messages d'audit S3 et ILM suivants dans un journal des audits.

> Les codes d'audit sont supprimés du produit et de la documentation à mesure que les fonctionnalités deviennent obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour les anciennes versions de StorageGRID. Par exemple, "StorageGRID 11.8 Utilisation de l'outil de somme du journal des audits".

Code	Description	Consultez
IDEL	Suppression initiée par ILM : journalise lorsque ILM lance le processus de suppression d'un objet.	"IDEL : Suppression initiée par ILM"
SDEL	S3 DELETE : Enregistre une transaction réussie de suppression d'un objet ou d'un compartiment.	"SDEL : S3 DELETE"
SGET	S3 GET : Enregistre une transaction réussie pour récupérer un objet ou lister les objets d'un compartiment.	"SGET : S3 GET"

Code	Description	Consultez
SHEA	S3 HEAD : Enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	"SHEA : S3 HEAD"
SPUT	S3 PUT : Consigne une transaction réussie pour créer un nouvel objet ou compartiment.	"SPUT: S3 PUT"

L' `audit-sum`outil peut effectuer les opérations suivantes :

- Traitez les journaux des audits bruts ou compressés. Par exemple :

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- Acceptez les données d'entrée provenant d'un tube, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la commande `grep` ou d'autres moyens. Par exemple :

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Cet outil n'accepte pas les fichiers compressés en entrée via un tube. Pour traiter des fichiers compressés, indiquez leur nom en argument de ligne de commande ou utilisez l'outil `zcat` pour les décompresser au préalable. Par exemple :
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Vous pouvez utiliser les options de ligne de commande pour synthétiser les opérations sur les compartiments séparément de celles sur les objets, ou pour regrouper les synthèses par nom de compartiment, par période ou par type de cible. Par défaut, les synthèses affichent la durée minimale, maximale et moyenne des opérations, mais vous pouvez utiliser l' `size (-s)`option pour examiner la taille des objets à la place.

Utilisez l' `help (-h)`option pour afficher les options disponibles. Par exemple :

```
$ audit-sum -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@`*`primary_Admin_Node_IP`*

b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`

d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Si vous souhaitez analyser tous les messages relatifs aux opérations d'écriture, de lecture, de head et de suppression, suivez ces étapes :

a. Saisissez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers que vous souhaitez analyser :

```
$ audit-sum /var/local/audit/export/audit.log
```

Cet exemple illustre le résultat typique de l' `audit-sum`outil. Cet exemple montre la durée des opérations de protocole.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Dans cet exemple, les opérations SGET (S3 GET) sont les plus lentes en moyenne à 1,13 seconde, mais les opérations SGET et SPUT (S3 PUT) affichent toutes deux des temps dans le pire des cas d'environ 1 770 secondes.

b. Pour afficher les 10 opérations de récupération les plus lentes, utilisez la commande grep pour sélectionner uniquement les messages SGET et ajoutez l'option de sortie longue (`-l` pour inclure les chemins d'accès aux objets :

```
grep SGET audit.log | audit-sum -l
```

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet de rechercher dans le journal des audits d'autres messages relatifs à ces objets particuliers.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+ Cet exemple de résultat montre que les trois requêtes S3 GET les plus lentes concernaient des objets d'environ 5 Go, soit une taille bien supérieure à celle des autres objets. La grande taille explique les temps de récupération les plus lents dans le pire des cas.

3. Si vous souhaitez déterminer quelles tailles d'objets sont ingérées et récupérées depuis votre grille, utilisez l'option size (`-s` :

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

Dans cet exemple, la taille moyenne des objets pour SPUT est inférieure à 2,5 Mo, tandis que la taille moyenne pour SGET est bien plus importante. Le nombre de messages SPUT est nettement supérieur à celui des messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous souhaitez déterminer si les récupérations ont été lentes hier :

   a. Exécutez la commande sur le journal des audits approprié et utilisez l'option group-by-time (`-gt`), suivie de la période (par exemple, 15M, 1H, 10S) :

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Ces résultats montrent un pic de trafic GET S3 entre 06:00 et 07:00. Les temps maximum et moyen sont tous deux nettement plus élevés durant cette période, et ils n'ont pas augmenté progressivement à mesure que le nombre augmentait. Ces indicateurs suggèrent que la capacité a été dépassée, possiblement au niveau du réseau ou de la capacité de la grille à traiter les requêtes.

b. Pour déterminer la taille des objets récupérés chaque heure hier, ajoutez l'option size (`-s`) à la commande :

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Ces résultats indiquent que des récupérations très importantes ont eu lieu lorsque le trafic global de récupération était à son maximum.

c. Pour plus de détails, utilisez la fonction "outil audit-explain" pour consulter toutes les opérations SGET effectuées pendant cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande grep est censée comporter plusieurs lignes, ajoutez la commande `less` pour afficher le contenu du journal des audits une page (un écran) à la fois.

5. Si vous souhaitez déterminer si les opérations SPUT sur les compartiments sont plus lentes que les opérations SPUT sur les objets :

a. Commencez par utiliser l'option `-go`, qui regroupe séparément les messages pour les opérations sur les objets et les compartiments :

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Les résultats montrent que les opérations SPUT sur les compartiments présentent des caractéristiques de performance différentes de celles des opérations SPUT sur les objets.

b. Pour déterminer quels compartiments présentent les opérations SPUT les plus lentes, utilisez l'option `-gb` qui regroupe les messages par compartiment :

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Pour déterminer quels compartiments ont la plus grande taille d'objet SPUT, utilisez à la fois les options `-gb` et `-s` :

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

${post_edited_translations.segment}

Découvrez la structure des messages d'audit StorageGRID

Les messages d'audit échangés au sein du système StorageGRID comprennent des informations standard communes à tous les messages et un contenu spécifique décrivant l'événement ou l'activité signalée.

Si les informations récapitulatives fournies par les outils "audit-explain" et "somme d'audit" sont insuffisantes, reportez-vous à cette section pour comprendre le format général de tous les messages d'audit.

Voici un exemple de message d'audit tel qu'il pourrait apparaître dans le journal des audits :

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. La chaîne entière est encadrée par des parenthèses (`[ ]`, et chaque élément d'attribut possède les caractéristiques suivantes :

- Encadré par des crochets `[ ]`
- Introduit par la chaîne `AUDT`, qui indique un message d'audit
- Sans délimiteurs (ni virgules ni espaces) avant ou après
- Terminé par un caractère de saut de ligne `\n`

Chaque élément comprend un code d'attribut, un type de données et une valeur qui sont rapportés dans ce format :

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Le nombre d'éléments d'attribut dans le message dépend du type d'événement du message. Les éléments d'attribut ne sont répertoriés dans aucun ordre particulier.

La liste suivante décrit les éléments d'attribut :

- `ATTR` est un code à quatre caractères pour l'attribut signalé. Certains attributs sont communs à tous les messages de journal des audits, tandis que d'autres sont spécifiques à un événement.
- `type` est un identifiant à quatre caractères du type de données de la valeur, tel que UI64, FC32, etc. Le type est placé entre parenthèses `( )`.
- `value` est le contenu de l'attribut, généralement une valeur numérique ou textuelle. Les valeurs sont toujours suivies d'un deux-points (`:`). Les valeurs de type de données CSTR sont entourées de guillemets doubles " ".

Types de données dans les messages d'audit de StorageGRID

Différents types de données sont utilisés pour stocker les informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres de 0 à 4,294,967,295.
UI64	Entier long non signé double (64 bits) ; il peut stocker les nombres de 0 à 18,446,744,073,709,551,615.
FC32	Constante de quatre caractères ; une valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que "ABCD."
IPAD	Utilisé pour les adresses IP.
CSTR	Tableau de longueur variable de caractères UTF-8. Les caractères peuvent être échappés selon les conventions suivantes : • La barre oblique inverse est \\. • Le retour chariot est \r. • Les guillemets doubles sont \". • Le saut de ligne (nouvelle ligne) est \n. • Les caractères peuvent être remplacés par leurs équivalents hexadécimaux (au format \xHH, où HH est la valeur hexadécimale représentant le caractère).

Données spécifiques à l'événement dans les messages d'audit StorageGRID

Chaque message d'audit du journal des audits enregistre des données spécifiques à un événement système.

Après le conteneur d'ouverture `[AUDT:` qui identifie le message lui-même, l'ensemble d'attributs suivant fournit des informations sur l'événement ou l'action décrite par le message d'audit. Ces attributs sont mis en évidence dans l'exemple suivant :

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

L'élément `ATYP` (souligné dans l'exemple) identifie quel événement a généré le message. Cet exemple de message inclut le code de message "SHEA" ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une requête S3 HEAD réussie.

Éléments communs dans les messages d'audit StorageGRID

Tous les messages d'audit contiennent des éléments communs.

Code	Type	Description
AMID	FC32	ID du module : Identifiant à quatre caractères du module ID ayant généré le message. Cela indique le segment de code dans lequel le message du journal des audits a été généré.
ANID	UI32	ID du nœud : l'ID du nœud de la grille attribué au service ayant généré le message. Chaque service se voit attribuer un identifiant unique lors de la configuration et de l'installation du système StorageGRID. Cet ID ne peut pas être modifié.

Code	Type	Description
ASES	UI64	Identifiant de la session d'audit : dans les versions précédentes, cet élément indiquait l'heure à laquelle le système d'audit était initialisé après le démarrage du service. Cette valeur temporelle était mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). **Remarque :** Cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ASQN	UI64	Compteur de séquences : Dans les versions précédentes, ce compteur était incrémenté pour chaque message d'audit généré sur le nœud de grille (ANID) et remis à zéro au redémarrage du service. **Remarque :** Cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	ID de trace : Identifiant partagé par l'ensemble des messages déclenchés par un seul événement.
ATIM	UI64	Horodatage : Heure de génération de l'événement ayant déclenché le message d'audit, mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Notez que la plupart des outils disponibles pour convertir l'horodatage en date et heure locales sont basés sur les millisecondes. Il peut être nécessaire d'arrondir ou de tronquer l'horodatage enregistré. L'heure lisible par l'utilisateur qui apparaît au début du message d'audit dans le fichier `audit.log` est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées comme *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, où le `T` est un caractère littéral indiquant le début du segment horaire de la date. *`UUUUUU`* sont des microsecondes.
ATYP	FC32	Type d'événement : identifiant à quatre caractères de l'événement enregistré. Cela détermine le contenu « payload » du message : les attributs inclus.
AVER	UI32	Version : Version du message d'audit. À mesure que le logiciel StorageGRID évolue, les nouvelles versions des services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ assure la rétrocompatibilité du service AMS afin de traiter les messages provenant d'anciennes versions des services.
RSLT	FC32	Résultat : Le résultat d'un événement, d'un processus ou d'une transaction. Si ce résultat n'est pas pertinent pour un message, la valeur « AUCUN » est utilisée à la place de « SUCS » afin d'éviter tout filtrage accidentel du message.

Format et exemples des messages d'audit StorageGRID

Vous trouverez des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Voici un exemple de message d'audit tel qu'il pourrait apparaître dans le fichier `audit.log` :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Le message d'audit contient des informations sur l'événement enregistré, ainsi que des informations sur le message d'audit lui-même.

Pour identifier l'événement enregistré par le message d'audit, recherchez l'attribut ATYP (mis en évidence ci-dessous) :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

La valeur de l'attribut ATYP est SPUT. "SPUT" représente une transaction S3 PUT, qui consigne l'ingestion d'un objet dans un compartiment.

Le message de journal des audits suivant indique également le compartiment auquel l'objet est associé :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Pour découvrir quand l'événement PUT s'est produit, notez l'horodatage en Temps universel coordonné (UTC) au début du message du journal des audits. Cette valeur est une version lisible par l'humain de l'attribut ATIM du message du journal des audits lui-même :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM enregistre le temps, en microsecondes, écoulé depuis le début de l'époque UNIX. Dans cet exemple, la valeur `1405631878959669` correspond au jeudi 17 juillet 2014 à 21 h 17 min 59 s UTC.

${post_edited_translations.segment}

Lorsque des messages d'audit sont générés dans StorageGRID

Des messages d'audit sont générés à chaque ingestion, récupération ou suppression d'un objet. Vous pouvez identifier ces transactions dans le journal des audits en repérant les messages d'audit spécifiques à l'API S3.

Les messages d'audit sont liés par des identifiants spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (bucket), S3KY (key), ou les deux
Liaison des opérations internes	CBID (identifiant interne de l'objet)

Moment d'envoi des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds du grid, la taille des objets et les délais du réseau, l'ordre des messages du journal des audits générés par les différents services peut différer de celui présenté dans les exemples de cette section.

Messages d'audit pour les transactions d'ingestion d'objets dans StorageGRID

Vous pouvez identifier les transactions d'ingestion du client dans le journal des audits en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages du journal des audits générés lors d'une transaction d'ingestion ne sont pas répertoriés dans le tableau suivant. Seuls les messages nécessaires pour tracer la transaction d'ingestion sont inclus.

Messages d'audit d'ingestion S3

Code	Nom	Description	Tracer	Voir
SPUT	Transaction PUT S3	Une transaction d'ingestion S3 PUT a été effectuée avec succès.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Règles d'objet respectées	La politique ILM a été respectée pour cet objet.	CBID	"ORLM : Règles d'objet respectées"

Exemple : ingestion d'objets S3

La série de messages d'audit ci-dessous est un exemple des messages d'audit générés et enregistrés dans le journal des audits lorsqu'un client S3 ingère un objet dans un nœud de stockage (service LDR).

Dans cet exemple, la stratégie ILM active inclut la règle ILM Make 2 Copies.

> Tous les messages du journal des audits générés lors d'une transaction ne sont pas listés dans l'exemple ci-dessous. Seuls ceux relatifs à la transaction d'ingestion S3 (SPUT) sont listés.

Cet exemple suppose qu'un compartiment S3 a été créé au préalable.

SPUT: S3 PUT

Le message SPUT est généré pour indiquer qu'une transaction S3 PUT a été émise pour créer un objet dans un compartiment spécifique.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM : Règles d'objet respectées

Le message ORLM indique que la politique ILM a été respectée pour cet objet. Le message comprend l'identifiant CBID de l'objet et le nom de la règle ILM appliquée.

Pour les objets répliqués, le champ LOCS inclut l'ID du nœud LDR et l'ID du volume des emplacements de l'objet.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Pour les objets à code d'effacement, le champ LOCS comprend l'identifiant du profil de code d'effacement et l'identifiant du groupe de code d'effacement

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Le champ PATH contient les informations relatives au compartiment S3 et à la clé.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Messages d'audit pour les transactions de suppression d'objets dans StorageGRID

Vous pouvez identifier les transactions de suppression d'objets dans le journal des audits en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires pour tracer l'opération de suppression sont inclus.

Messages de journal des audits de suppression S3

Code	Nom	Description	Tracer	Voir
SDEL	Suppression S3	Demande de suppression de l'objet d'un bucket.	CBID, S3KY	"SDEL : S3 DELETE"

Exemple : suppression d'objet S3

Lorsqu'un client S3 supprime un objet d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal des audits.

> Tous les messages du journal des audits générés lors d'une transaction de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux relatifs à la transaction de suppression S3 (SDEL) sont listés.

SDEL : S3 Delete

La suppression d'un objet commence lorsque le client envoie une requête DeleteObject à un service LDR. Le message contient le compartiment à partir duquel supprimer l'objet et la clé S3 de l'objet, qui sert à l'identifier.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Messages d'audit pour les transactions de récupération d'objets dans StorageGRID

Vous pouvez identifier les transactions de récupération d'objets dans le journal des audits en localisant les messages d'audit spécifiques à l'API S3.

Le tableau suivant ne répertorie pas tous les messages d'audit générés lors d'une transaction de récupération. Seuls les messages nécessaires au suivi de la transaction de récupération y figurent.

Messages d'audit de récupération S3

Code	Nom	Description	Tracer	Voir
SGET	S3 GET	Requête effectuée pour récupérer un objet à partir d'un bucket.	CBID, S3BK, S3KY	"SGET : S3 GET"

Exemple : récupération d'objets S3

Lorsqu'un client S3 récupère un objet à partir d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal des audits.

Notez que tous les messages du journal des audits générés lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux relatifs à la transaction de récupération S3 (SGET) sont répertoriés.

SGET : S3 GET

La récupération d'un objet commence lorsque le client envoie une requête GetObject à un service LDR. Le message contient le compartiment à partir duquel récupérer l'objet et la clé S3 de l'objet, qui sert à l'identifier.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Si la politique du compartiment le permet, un client peut récupérer des objets de manière anonyme ou depuis un compartiment appartenant à un autre compte locataire. Le message du journal des audits contient des informations sur le compte locataire du propriétaire du compartiment, afin que vous puissiez suivre ces requêtes anonymes et inter-comptes.

Dans l'exemple de message suivant, le client envoie une requête GetObject pour un objet stocké dans un compartiment dont il n'est pas propriétaire. Les valeurs de SBAI et SBAC correspondent à l'identifiant et au nom du compte locataire du propriétaire du compartiment, qui diffèrent de l'identifiant et du nom du compte locataire du client enregistrés dans S3AI et SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemple : S3 Select sur un objet

Lorsqu'un client S3 émet une requête S3 Select sur un objet, des messages d'audit sont générés et

enregistrés dans le journal des audits.

Notez que tous les messages du journal des audits générés lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux relatifs à la transaction S3 Select (SelectObjectContent) sont répertoriés.

Chaque requête génère deux messages d'audit : l'un effectuant l'autorisation de la requête S3 Select (le champ S3SR est défini sur "select") et une opération GET standard ultérieure qui récupère les données du stockage pendant le traitement.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):13630097093968959 85]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messages d'audit pour les mises à jour des métadonnées des objets S3 dans StorageGRID

Des messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

Messages d'audit de mise à jour des métadonnées S3

Code	Nom	Description	Tracer	Voir
SUPD	Métadonnées S3 mises à jour	Généré lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré.	CBID, S3KY, HTRH	"SUPD : Métadonnées S3 mises à jour"

Exemple : mise à jour des métadonnées S3

L'exemple illustre une transaction réussie de mise à jour des métadonnées d'un objet S3 existant.

SUPD : Mise à jour des métadonnées S3

Le client S3 effectue une requête (SUPD) pour mettre à jour les métadonnées spécifiées (`x-amz-meta-*` pour l'objet S3 (S3KY). Dans cet exemple, les en-têtes de requête sont inclus dans le champ HTRH car il a été configuré comme en-tête de protocole d'audit (*Configuration* > **Surveillance** > **Audit and syslog server**). Voir "Configurer la gestion des journaux et le serveur syslog externe".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Messages d'audit

Découvrez les types et codes de messages d'audit dans StorageGRID

Les descriptions détaillées des messages d'audit renvoyés par le système sont présentées dans les sections suivantes. Chaque message d'audit est d'abord répertorié dans un tableau regroupant les messages apparentés par classe d'activité que le message représente. Ces regroupements sont utiles à la fois pour comprendre les types

d'activités qui sont auditées et pour sélectionner le type de filtrage des messages d'audit souhaité.

Les messages d'audit sont également classés par ordre alphabétique selon leur code à quatre caractères. Cette liste alphabétique vous permet de trouver des informations sur des messages spécifiques.

Les codes à quatre caractères utilisés tout au long de ce chapitre sont les valeurs ATYP figurant dans les messages d'audit, comme illustré dans l'exemple de message suivant :

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Pour plus d'informations sur la configuration des niveaux de messages d'audit, la modification des destinations des journaux et l'utilisation d'un serveur syslog externe pour vos informations d'audit, consultez "Configurer la gestion des journaux et le serveur syslog externe"

Catégories de messages d'audit

Messages d'audit pour les événements système dans StorageGRID

Les messages d'audit appartenant à la catégorie d'audit système sont utilisés pour les événements liés au système d'audit lui-même, aux états des nœuds de la grille, à l'activité des tâches à l'échelle du système (tâches de la grille) et aux opérations de sauvegarde de service.

Code	Titre et description du message	Voir
ECMC	Fragment de données à codage d'effacement manquant : indique qu'un fragment de données à codage d'effacement manquant a été détecté.	"ECMC : Fragment de données à codage d'effacement manquant"
ECOC	Fragment de données corrompu par effacement : indique qu'un fragment de données corrompu par effacement a été détecté.	"ECOC : Fragment de données à code d'effacement corrompu"
ETAF	Échec de l'authentification de sécurité : une tentative de connexion utilisant Transport Layer Security (TLS) a échoué.	"ETAF : Échec de l'authentification de sécurité"
GNRG	Enregistrement GNDS : Un service a mis à jour ou enregistré des informations le concernant dans le système StorageGRID.	"GNRG : Enregistrement GNDS"
GNUR	Désinscription GNDS : Un service s'est désinscrit du système StorageGRID.	"GNUR : Désinscription GNDS"

Code	Titre et description du message	Voir
GTED	Tâche de grille terminée : Le service CMN a terminé le traitement de la tâche de grille.	"GTED : Tâche Grid terminée"
GTST	Démarrage de la tâche de grille : Le service CMN a commencé à traiter la tâche de grille.	"GTST : Tâche de grille démarrée"
GTSU	Tâche de grille soumise : Une tâche de grille a été soumise au service CMN.	"GTSU : Tâche de grille soumise"
LLST	Localisation perdue : ce message de journal des audits est généré lorsqu'une localisation est perdue.	"LLST : Localisation perdue"
OLST	Objet perdu : l'objet demandé est introuvable dans le système StorageGRID.	"OLST : Le système a détecté un objet perdu"
SADD	Audit de sécurité désactivé : la journalisation des messages d'audit a été désactivée.	"SADD : Désactivation de l'audit de sécurité"
SADE	Activation de l'audit de sécurité : la journalisation des messages d'audit a été rétablie.	"SADE : Activation de l'audit de sécurité"
SVRF	Échec de la vérification du magasin d'objets : un bloc de contenu n'a pas réussi les vérifications.	"SVRF : Échec de la vérification du magasin d'objets"
SVRU	Vérification du magasin d'objets Inconnu : Des données d'objet inattendues ont été détectées dans le magasin d'objets.	"SVRU : Vérification du magasin d'objets inconnue"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : Arrêt du nœud"
SYST	Arrêt du nœud : Un service a initié un arrêt en douceur.	"SYST : Arrêt du nœud"
SYSU	Démarrage du nœud : un service a démarré ; la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : Démarrage du nœud"

Messages d'audit pour les événements de stockage d'objets dans StorageGRID

Les messages d'audit de la catégorie « audit du stockage d'objets » concernent les événements liés au stockage et à la gestion des objets au sein du système StorageGRID. Cela inclut le stockage et la récupération d'objets, les transferts de nœud de grille à nœud de grille, ainsi que les vérifications.

Les codes d'audit sont supprimés du produit et de la documentation à mesure que les fonctionnalités deviennent obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour les anciennes versions de SG. Par exemple, "Messages d'audit du stockage d'objets StorageGRID 11.8".

Code	Description	Voir
BROR	Requête de lecture seule du compartiment : Un compartiment est entré ou sorti du mode lecture seule.	"BROR : Requête en lecture seule du compartiment"
CBSE	Fin de l'envoi d'objet : L'entité source a terminé une opération de transfert de données entre nœuds de la grille.	"CBSE : Fin de l'envoi d'objet"
CBRE	Fin de réception de l'objet : L'entité de destination a terminé une opération de transfert de données entre nœuds de la grille.	"CBRE : Fin de réception d'objet"
CGRR	Demande de réplication inter-grilles : StorageGRID a tenté une opération de réplication inter-grilles pour répliquer des objets entre des compartiments dans une connexion de fédération de grilles.	"CGRR : Demande de réplication inter-grilles"
EBDL	Suppression d'un compartiment vide : le scanner ILM a supprimé un objet dans un compartiment qui supprime tous les objets (opération de vidage du compartiment).	"EBDL : Suppression du compartiment vide"
EBKR	Demande de vidage du compartiment : un utilisateur a envoyé une demande pour activer ou désactiver le vidage du compartiment (c'est-à-dire pour supprimer les objets du compartiment ou pour arrêter la suppression des objets).	"EBKR : Demande de bucket vide"
SCMT	Validation du stockage d'objets : un bloc de contenu a été entièrement stocké et vérifié, et peut maintenant être demandé.	"SCMT : Demande de validation du magasin d'objets"
SREM	Suppression d'un bloc de contenu dans le magasin d'objets : un bloc de contenu a été supprimé d'un nœud de la grille et ne peut plus être demandé directement.	"SREM : Suppression du magasin d'objets"

Messages d'audit pour les opérations de lecture client dans StorageGRID

Les messages d'audit de lecture du client sont enregistrés lorsqu'une application cliente S3 effectue une requête pour récupérer un objet.

Code	Description	Utilisé par	Voir
S3SL	Requête S3 Select : consigne la fin de l'opération après le retour d'une requête S3 Select au client. Le message S3SL peut inclure un message d'erreur et un code d'erreur. La requête a peut-être échoué.	Client S3	"S3SL : Requête S3 Select"
SGET	S3 GET : Enregistre une transaction réussie pour récupérer un objet ou lister les objets d'un compartiment. **Remarque :** Si la transaction porte sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : S3 GET"
SHEA	S3 HEAD : Enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	Client S3	"SHEA : S3 HEAD"

Messages d'audit pour les opérations d'écriture client dans StorageGRID

Les messages d'audit d'écriture côté client sont enregistrés lorsqu'une application cliente S3 effectue une requête pour créer ou modifier un objet.

Code	Description	Utilisé par	Voir
OVWR	Écrasement d'objet : consigne une transaction visant à écraser un objet par un autre objet.	Client S3	"OVWR : Écrasement d'objet"
SDEL	S3 DELETE : Enregistre une transaction réussie de suppression d'un objet ou d'un compartiment. **Remarque :** Si la transaction porte sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : S3 DELETE"
SPOS	S3 POST : Consigne une transaction réussie pour restaurer un objet du stockage AWS Glacier vers un Cloud Storage Pool.	Client S3	"SPOS: S3 POST"
SPUT	S3 PUT : Consigne une transaction réussie pour créer un nouvel objet ou compartiment. **Remarque :** Si la transaction porte sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT: S3 PUT"
SUPD	Mise à jour des métadonnées S3 : Consigne une transaction réussie de mise à jour des métadonnées d'un objet ou d'un compartiment existant.	Client S3	"SUPD : Métadonnées S3 mises à jour"

Messages d'audit de gestion StorageGRID

La catégorie Gestion enregistre les requêtes des utilisateurs adressées à l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : journal des requêtes utilisateur.	"MGAU : Message d'audit de gestion"

Messages d'audit ILM StorageGRID

Les messages d'audit appartenant à la catégorie d'audit ILM sont utilisés pour les événements liés aux opérations de gestion du cycle de vie de l'information (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée par ILM : ce message d'audit est généré lorsque ILM lance le processus de suppression d'un objet.	"IDEL : Suppression initiée par ILM"
LKCU	Nettoyage des objets écrasés. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé afin de libérer de l'espace de stockage.	"LKCU : Nettoyage des objets écrasés"
ORLM	Règles d'objet respectées : ce message d'audit est généré lorsque les données d'objet sont stockées conformément aux règles ILM.	"ORLM : Règles d'objet respectées"

Référence du message d'audit

Message d'audit BROR pour les requêtes de lecture seule sur les compartiments dans StorageGRID

Le service LDR génère ce message d'audit lorsqu'un compartiment passe en mode lecture seule ou en sort. Par exemple, un compartiment passe en mode lecture seule pendant la suppression de tous ses objets.

Code	Champ	Description
BKHD	UUID du compartiment	L'identifiant du compartiment.
BROV	Valeur de requête en lecture seule du compartiment	Que le compartiment soit rendu en lecture seule ou qu'il quitte l'état de lecture seule (1 = lecture seule, 0 = non lecture seule).

Code	Champ	Description
BROS	Raison du mode lecture seule du compartiment	La raison pour laquelle le compartiment est rendu en lecture seule ou quitte l'état de lecture seule. Par exemple, emptyBucket.
S3AI	ID du compte locataire S3	L'identifiant du compte locataire ayant envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	compartiment S3	Le nom du compartiment S3.

Message d'audit CBRB pour le début de la réception d'objet dans StorageGRID

En fonctionnement normal, les blocs de contenu sont transférés en continu entre les différents nœuds au fur et à mesure de l'accès aux données, de leur réplication et de leur conservation. Lorsqu'un transfert de bloc de contenu d'un nœud à un autre est initié, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion de nœud à nœud.
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction du transfert	Indique si le transfert CBID a été initié par une opération push ou pull : PUSH : L'opération de transfert a été demandée par l'entité expéditrice. TIRAGE : L'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	L'identifiant du nœud source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'identifiant du nœud de destination (récepteur) du transfert CBID.
CTSS	Compteur de séquence de départ	Indique le premier numéro de séquence demandé. En cas de succès, le transfert commence à partir de ce numéro de séquence.
CTES	Nombre de séquences finales attendues	Indique le dernier nombre de séquences demandé. En cas de succès, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.

Code	Champ	Description
RSLT	État de début du transfert	État au moment du lancement du transfert : SUCS : Transfert démarré avec succès.

Ce message d'audit indique qu'une opération de transfert de données entre nœuds a été initiée sur un seul élément de contenu, identifié par son identifiant de bloc de contenu. L'opération demande des données de « Start Sequence Count » à « Expected End Sequence Count ». Les nœuds émetteur et récepteur sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et, combinées aux messages d'audit de stockage, pour vérifier le nombre de réplicas.

Message d'audit CBRE pour la fin de réception d'objet dans StorageGRID

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion de nœud à nœud.
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction du transfert	Indique si le transfert CBID a été initié par une opération push ou pull : PUSH : L'opération de transfert a été demandée par l'entité expéditrice. TIRAGE : L'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	L'identifiant du nœud source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'identifiant du nœud de destination (récepteur) du transfert CBID.
CTSS	Compteur de séquence de départ	Indique le numéro de séquence à partir duquel le transfert a commencé.
CTAS	Nombre réel de séquences finales	Indique le dernier nombre de séquences transféré avec succès. Si le nombre de séquences final est identique au nombre de séquences initial, et que le résultat du transfert n'a pas été concluant, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité expéditrice) : SUCS : transfert de données effectué avec succès ; tous les comptes de séquences demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : délai de connexion dépassé lors de l'établissement ou du transfert UNRE : ID du nœud de destination inaccessible CRPT : transfert interrompu en raison de la réception de données corrompues ou invalides

Ce message d'audit indique qu'une opération de transfert de données entre nœuds a été effectuée. Si le résultat du transfert a été un succès, l'opération a transféré des données de « Start Sequence Count » à « Actual End Sequence Count ». Les nœuds émetteur et récepteur sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et pour localiser, répertorier et analyser les erreurs. Combinées aux messages d'audit de stockage, elles peuvent également être utilisées pour vérifier le nombre de réplicas.

Message d'audit CBSB pour l'objet send begin dans StorageGRID

En fonctionnement normal, les blocs de contenu sont transférés en continu entre les différents nœuds au fur et à mesure de l'accès aux données, de leur réplication et de leur conservation. Lorsqu'un transfert de bloc de contenu d'un nœud à un autre est initié, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion de nœud à nœud.
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction du transfert	Indique si le transfert CBID a été initié par une opération push ou pull : PUSH : L'opération de transfert a été demandée par l'entité expéditrice. TIRAGE : L'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	L'identifiant du nœud source (expéditeur) du transfert CBID.

Code	Champ	Description
CTDS	Entité de destination	L'identifiant du nœud de destination (récepteur) du transfert CBID.
CTSS	Compteur de séquence de départ	Indique le premier numéro de séquence demandé. En cas de succès, le transfert commence à partir de ce numéro de séquence.
CTES	Nombre de séquences finales attendues	Indique le dernier nombre de séquences demandé. En cas de succès, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	État de début du transfert	État au moment du lancement du transfert : SUCS : transfert démarré avec succès.

Ce message d'audit indique qu'une opération de transfert de données entre nœuds a été initiée sur un seul élément de contenu, identifié par son identifiant de bloc de contenu. L'opération demande des données de « Start Sequence Count » à « Expected End Sequence Count ». Les nœuds émetteur et récepteur sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et, combinées aux messages d'audit de stockage, pour vérifier le nombre de réplicas.

Message d'audit CBSE pour la fin d'envoi d'objet dans StorageGRID

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion de nœud à nœud.
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction du transfert	Indique si le transfert CBID a été initié par une opération push ou pull : PUSH : L'opération de transfert a été demandée par l'entité expéditrice. TIRAGE : L'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	L'identifiant du nœud source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'identifiant du nœud de destination (récepteur) du transfert CBID.

Code	Champ	Description
CTSS	Compteur de séquence de départ	Indique le numéro de séquence à partir duquel le transfert a commencé.
CTAS	Nombre réel de séquences finales	Indique le dernier nombre de séquences transféré avec succès. Si le nombre de séquences final est identique au nombre de séquences initial, et que le résultat du transfert n'a pas été concluant, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité expéditrice) : SUCS : Transfert effectué avec succès ; tous les décomptes de séquences demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : délai de connexion dépassé lors de l'établissement ou du transfert UNRE : ID du nœud de destination inaccessible CRPT : transfert interrompu en raison de la réception de données corrompues ou invalides

Ce message d'audit indique qu'une opération de transfert de données entre nœuds a été effectuée. Si le résultat du transfert a été un succès, l'opération a transféré des données de « Start Sequence Count » à « Actual End Sequence Count ». Les nœuds émetteur et récepteur sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et pour localiser, répertorier et analyser les erreurs. Combinées aux messages d'audit de stockage, elles peuvent également être utilisées pour vérifier le nombre de réplicas.

Message d'audit CGRR pour les demandes de réplication inter-grilles dans StorageGRID

Ce message est généré lorsque StorageGRID tente une opération de réplication inter-grilles pour répliquer des objets entre des compartiments dans une connexion de fédération de grilles.

Code	Champ	Description
CSIZ	Taille de l'objet	La taille de l'objet en octets. L'attribut CSIZ a été introduit dans StorageGRID 11.8. Par conséquent, les demandes de réplication inter-grilles couvrant une mise à niveau de StorageGRID 11.7 vers 11.8 peuvent avoir une taille totale d'objet inexacte.
S3AI	ID du compte locataire S3	L'identifiant du compte locataire qui possède le compartiment à partir duquel l'objet est répliqué.

Code	Champ	Description
GFID	ID de connexion à la fédération Grid	L'identifiant de la connexion de fédération de grilles utilisée pour la réplication inter-grilles.
OPÉRATEUR	Opération CGR	Le type d'opération de réplication inter-grilles qui a été tenté : • 0 = Répliquer l'objet • 1 = Répliquer l'objet multipartite • 2 = Répliquer le marqueur de suppression
S3BK	compartiment S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie SUCS (succès) ou GERR (erreur générale).

Message d'audit EBDL pour les suppressions d'objets de compartiment vides dans StorageGRID

Le scanner ILM a supprimé un objet dans un compartiment qui supprime tous les objets (opération de vidage du compartiment).

Code	Champ	Description
CSIZ	Taille de l'objet	La taille de l'objet en octets.
CHEMIN	Compartiment/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur de l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
RSLT	Résultat de l'opération de suppression	Le résultat d'un événement, d'un processus ou d'une transaction. Si ce résultat n'est pas pertinent pour un message, la valeur NONE est utilisée plutôt que SUCS afin que le message ne soit pas accidentellement filtré.

Message d'audit EBKR pour les requêtes de compartiment vide dans StorageGRID

Ce message indique qu'un utilisateur a envoyé une demande pour activer ou désactiver

le compartiment vide (c'est-à-dire pour supprimer des objets du compartiment ou pour arrêter la suppression d'objets).

Code	Champ	Description
BUID	UUID du compartiment	L'identifiant du compartiment.
EBJS	Configuration JSON du bucket vide	Contient le JSON représentant la configuration actuelle du compartiment vide.
S3AI	ID du compte locataire S3	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	Bucket S3	Le nom du compartiment S3.

Message d'audit ECMC pour des données à codage d'effacement manquantes dans StorageGRID

Ce message d'audit indique que le système a détecté un fragment de données à codage d'effacement manquant.

Code	Champ	Description
VCMC	ID VCS	Le nom du VCS qui contient le segment manquant.
MCID	ID du segment	L'identifiant du fragment manquant codé par effacement.
RSLT	Résultat	Ce champ a la valeur « NONE ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

Message d'audit ECOC pour des données à codage d'effacement corrompues dans StorageGRID

Ce message d'audit indique que le système a détecté un fragment de données corrompu à code d'effacement.

Code	Champ	Description
VCCO	ID VCS	Le nom du VCS qui contient le segment corrompu.
VLID	ID du volume	Le volume RangeDB qui contient le fragment codé par effacement corrompu.
CCID	ID du segment	L'identifiant du fragment corrompu codé par effacement.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur « NONE ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

Message d'audit ETAF relatif aux échecs d'authentification de sécurité dans StorageGRID

Ce message est généré lorsqu'une tentative de connexion utilisant Transport Layer Security (TLS) a échoué.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant système unique de la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Un identifiant dépendant du service représentant l'identité de l'utilisateur distant.
RSLT	Code de raison	La raison de l'échec : SCNI : Échec de l'établissement de la connexion sécurisée. CERM : Le certificat était manquant. CERT : Le certificat était invalide. CERE : Le certificat a expiré. CERR : Le certificat a été révoqué. CSGN : La signature du certificat était invalide. CSGU : Le signataire du certificat était inconnu. UCRM : Les informations d'identification de l'utilisateur étaient manquantes. UCRI : Les identifiants de l'utilisateur étaient invalides. UCRU : Les identifiants de l'utilisateur ont été refusés. TOUT : Délai d'authentification dépassé.

Lorsqu'une connexion est établie avec un service sécurisé utilisant TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et d'une logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification invalides, inattendus ou non autorisés, un message d'audit est consigné. Cela permet d'effectuer des requêtes concernant les tentatives d'accès non autorisé et d'autres problèmes de connexion liés à la sécurité.

Ce message peut provenir d'une configuration incorrecte d'une entité distante ou de tentatives de présentation

d’identifiants invalides ou non autorisés au système. Ce message de journal des audits doit être surveillé afin de détecter toute tentative d’accès non autorisé au système.

Message d’audit GNRG pour l’enregistrement GNDS dans StorageGRID

Le service CMN génère ce message d’audit lorsqu’un service a mis à jour ou enregistré des informations le concernant dans le système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la requête de mise à jour : • SUCS: Réussi • SUNV: Service indisponible • GERR: Autre défaillance
GNID	ID du nœud	L’identifiant du nœud du service qui a initié la demande de mise à jour.
GNTP	Type d’appareil	Le type de périphérique du nœud de grille (par exemple, BLDR pour un service LDR).
GNDV	Version du modèle d’appareil	La chaîne de caractères identifiant la version du modèle de périphérique du nœud de grille dans le bundle DMDL.
GNGP	Groupe	Le groupe auquel appartient le nœud de la grille (dans le contexte des coûts de liaison et du classement des requêtes de service).
GNIA	Adresse IP	Adresse IP du nœud de grille.

Ce message est généré chaque fois qu’un nœud de la grille met à jour son entrée dans le Grid Nodes Bundle.

Message d’audit GNUR pour la désinscription GNDS dans StorageGRID

Le service CMN génère ce message d’audit lorsqu’un service a supprimé les informations le concernant du système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la requête de mise à jour : • SUCS: Réussi • SUNV: Service indisponible • GERR: Autre défaillance
GNID	ID du nœud	L’identifiant du nœud du service qui a initié la demande de mise à jour.

Message d’audit GTED pour les tâches de grille terminées dans StorageGRID

Ce message d’audit indique que le service CMN a terminé le traitement de la tâche de grille spécifiée et l’a déplacée vers la table Historique. Si le résultat est SUCS, ABRT ou ROLF, un message d’audit « Grid Task Started » correspondant sera généré. Les autres résultats indiquent que le traitement de cette tâche de grille n’a jamais démarré.

Code	Champ	Description
TSID	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer cette tâche tout au long de son cycle de vie. **Remarque :** L’identifiant de tâche est attribué lors de la génération de la tâche dans la grille, et non lors de sa soumission. Il est possible qu’une même tâche de grille soit soumise plusieurs fois, et dans ce cas, le champ Identifiant de tâche ne suffit pas à lier de manière unique les messages d’audit « Soumis », « Démarré » et « Terminé ».
RSLT	Résultat	Résultat final de la tâche de grille : • SUCS : La tâche sur la grille s’est terminée avec succès. • ABRT : La tâche de grille a été terminée sans erreur de restauration. • ROLF : La tâche de grille a été interrompue et n’a pas pu terminer le processus de restauration. • ANNULÉ : La tâche de grille a été annulée par l’utilisateur avant son démarrage. • EXPR : La tâche de grille a expiré avant d’être démarrée. • IVLD : La tâche de grille était invalide. • AUTH : La tâche de la grille n’était pas autorisée. • DUPL : La tâche de grille a été rejetée comme doublon.

Message d’audit GTST pour les tâches de grille démarrées dans StorageGRID

Ce message d’audit indique que le service CMN a commencé à traiter la tâche de grille spécifiée. Le message d’audit suit immédiatement le message « Tâche de grille soumise » pour les tâches de grille initiées par le service interne de soumission de tâches de grille et sélectionnées pour une activation automatique. Pour les tâches de grille soumises dans la table « En attente », ce message est généré lorsque l’utilisateur démarre la tâche de grille.

Code	Champ	Description
TSID	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer cette tâche tout au long de son cycle de vie. **Remarque :** L'identifiant de tâche est attribué lors de la génération de la tâche dans la grille, et non lors de sa soumission. Il est possible qu'une même tâche de grille soit soumise plusieurs fois, et dans ce cas, le champ Identifiant de tâche ne suffit pas à lier de manière unique les messages d'audit « Soumis », « Démarré » et « Terminé ».
RSLT	Résultat	Le résultat. Ce champ n'a qu'une seule valeur : • SUCS : La tâche de grid a démarré avec succès.

Message d'audit GTSU pour les tâches de grille soumises dans StorageGRID

Ce message d'audit indique qu'une tâche de grille a été soumise au service CMN.

Code	Champ	Description
TSID	ID de tâche	Identifie de manière unique une tâche de grille générée et permet de gérer cette tâche tout au long de son cycle de vie. **Remarque :** L'identifiant de tâche est attribué lors de la génération de la tâche dans la grille, et non lors de sa soumission. Il est possible qu'une même tâche de grille soit soumise plusieurs fois, et dans ce cas, le champ Identifiant de tâche ne suffit pas à lier de manière unique les messages d'audit « Soumis », « Démarré » et « Terminé ».
TTYP	Type de tâche	Le type de tâche de grille.
TVER	Version de la tâche	Un numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Une description lisible par l'humain de la tâche de grille.
VATS	Valide après l'horodatage	Le moment le plus précoce (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) auquel la tâche de grille est valide.
VBTS	Horodatage de validité antérieure	La dernière heure (UINT64 microsecondes depuis le 1er janvier 1970 - heure UNIX) à laquelle la tâche de grid est valide.

Code	Champ	Description
TSRC	Source	La source de la tâche : • TXTB : La tâche de grille a été soumise via le système StorageGRID sous forme de bloc de texte signé. • GRID : La tâche de grid a été soumise via le service interne de soumission des tâches de grid.
ACTV	Type d'activation	Le type d'activation : • AUTO : La tâche de grille a été soumise pour activation automatique. • EN ATTENTE : La tâche de grille a été ajoutée à la table des tâches en attente. Il s'agit de la seule possibilité pour la source TXTB.
RSLT	Résultat	Résultat de la soumission : • SUCS : La tâche de grille a été soumise avec succès. • ÉCHEC : La tâche a été directement déplacée vers la table historique.

Message d'audit IDEL pour les suppressions initiées par ILM dans StorageGRID

Ce message est généré lorsque ILM lance le processus de suppression d'un objet.

Le message IDEL est généré dans l'une ou l'autre de ces situations :

- **Pour les objets dans les compartiments S3 conformes** : ce message est généré lorsque ILM lance le processus de suppression automatique d'un objet car sa période de rétention a expiré (en supposant que le paramètre de suppression automatique soit activé et que la conservation légale soit désactivée).
- **Pour les objets situés dans des compartiments S3 non conformes**. Ce message est généré lorsque ILM entame le processus de suppression d'un objet, car aucune instruction de placement dans les stratégies ILM actives ne s'applique actuellement à cet objet.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	L'identifiant CBID de l'objet.
CMPA	Conformité : suppression automatique	Uniquement pour les objets situés dans des compartiments S3 conformes. 0 (faux) ou 1 (vrai), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de rétention, sauf si le compartiment fait l'objet d'une conservation légale.
CMPL	Conformité : Mise sous séquestre légal	Uniquement pour les objets situés dans des compartiments S3 conformes. 0 (faux) ou 1 (vrai), indiquant si le compartiment est actuellement sous rétention légale.

Code	Champ	Description
CMPR	Conformité : Période de conservation	Uniquement pour les objets dans des compartiments S3 conformes. La durée de la période de conservation de l'objet en minutes.
CTME	Conformité : Temps d'ingestion	Uniquement pour les objets dans des compartiments S3 conformes. Heure d'ingestion de l'objet. Vous pouvez ajouter la période de rétention en minutes à cette valeur pour déterminer quand l'objet peut être supprimé du compartiment.
DMRK	Supprimer l'identifiant de version du marqueur	L'identifiant de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment versionné. Les opérations sur les compartiments n'incluent pas ce champ.
CSIZ	Taille du contenu	La taille de l'objet en octets.
LOCS	Lieux	Emplacement de stockage des données d'objet au sein du système StorageGRID. La valeur de LOCS est "" si l'objet n'a pas d'emplacement (par exemple, s'il a été supprimé). CLEC : pour les objets à code d'effacement, l'identifiant du profil de code d'effacement et l'identifiant du groupe de code d'effacement appliqués aux données de l'objet. CLDI : pour les objets répliqués, l'ID du nœud LDR et l'ID du volume de l'emplacement de l'objet. CLNL : ID du nœud ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Résultat de l'opération ILM. SUCS : L'opération ILM a réussi.
RÈGLE	Étiquette des règles	• Si un objet dans un compartiment S3 conforme est supprimé automatiquement parce que sa période de rétention a expiré, ce champ est vide. • Si l'objet est supprimé parce qu'il n'existe plus d'instructions de placement qui s'appliquent actuellement à l'objet, ce champ affiche l'étiquette lisible par l'homme de la dernière règle ILM qui s'appliquait à l'objet.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.

Code	Champ	Description
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit LKCU pour le nettoyage des objets écrasés dans StorageGRID

Ce message s'affiche lorsque StorageGRID supprime un objet écrasé qui nécessitait auparavant un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 écrit un objet dans un chemin contenant déjà un objet. La suppression s'effectue automatiquement en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	La taille de l'objet en octets.
LTYP	Type de nettoyage	*Usage interne uniquement.*
LUID	UUID de l'objet supprimé	L'identifiant de l'objet qui a été supprimé.
CHEMIN	Compartiment/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur de l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	L'identifiant de l'objet qui existe encore. Cette valeur n'est disponible que si l'objet n'a pas été supprimé.

Message d'audit LKDM pour le nettoyage des objets ayant fuité dans StorageGRID

Ce message est généré lorsqu'un fragment ayant fuité a été nettoyé ou supprimé. Un fragment peut faire partie d'un objet répliqué ou d'un objet encodé par effacement.

Code	Champ	Description
CLOC	Emplacement du segment	Le chemin d'accès du fichier de la portion de données divulguée qui a été supprimée.

Code	Champ	Description

CTYP	Type de chunk	Type de chunk :
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	Type de fuite	Les cinq types de fuites pouvant être détectées :
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Heure de création du chunk	Heure à laquelle le fragment divulgué a été créé.
UUID	Identifiant unique universel	L’identifiant de l’objet auquel appartient le fragment.
CBID	Identifiant de bloc de contenu	CBID de l’objet auquel appartient le fragment divulgué.
CSIZ	Taille du contenu	La taille du bloc en octets.

Message d’audit LLST concernant les emplacements de copies d’objets perdus dans StorageGRID

Ce message est généré lorsqu’il est impossible de trouver l’emplacement d’une copie d’objet (répliquée ou codée par effacement).

Code	Champ	Description
CBIL	CBID	Le CBID concerné.
ECPR	Profil de codage d’effacement	Pour les données d’objets codées par effacement. L’identifiant du profil de codage par effacement utilisé.

Code	Champ	Description
LTYP	Type de localisation	CLDI (en ligne) : pour les données d'objet répliquées CLEC (Online) : Pour les données d'objets codées par effacement CLNL (Nearline) : Pour les données d'objet répliqué archivées
NOID	ID du nœud source	L'identifiant du nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin vers l'objet répliqué	Chemin d'accès complet à l'emplacement disque des données de l'objet perdu. Retourné uniquement lorsque LTYP a la valeur CLDI (c'est-à-dire pour les objets répliqués). Prend la forme `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Résultat	Toujours AUCUN. RSLT est un champ obligatoire, mais n'est pas pertinent pour ce message. La valeur AUCUN est utilisée à la place de SUCS afin que ce message ne soit pas filtré.
TSRC	Source de déclenchement	UTILISATEUR : Déclenché par l'utilisateur SYST: Système déclenché
UUID	Identifiant unique universel	L'identifiant de l'objet concerné dans le système StorageGRID.

Message d'audit MGAU pour les requêtes API de gestion dans StorageGRID

La catégorie Gestion enregistre les requêtes utilisateur adressées à l'API de gestion. Chaque requête HTTP autre qu'une requête GET ou HEAD adressée à une URI d'API valide génère une réponse contenant le nom d'utilisateur, l'adresse IP et le type de requête à l'API. Les URI d'API invalides (telles que /api/v3-authorize) et les requêtes invalides adressées à des URI d'API valides ne sont pas enregistrées.

Code	Champ	Description
MDIP	Adresse IP de destination	L'adresse IP du serveur (destination).
MDNA	Nom de domaine	Le nom de domaine de l'hôte.
MPAT	Chemin de la requête	Le chemin de la requête.

Code	Champ	Description
MPQP	Paramètres de requête	Les paramètres de requête pour la demande.
MRBD	Corps de la requête	Le contenu du corps de la requête. Bien que le corps de la réponse soit enregistré par défaut, le corps de la requête est enregistré dans certains cas lorsque le corps de la réponse est vide. Comme les informations suivantes ne sont pas disponibles dans le corps de la réponse, elles sont extraites du corps de la requête pour les méthodes POST suivantes : • Nom d'utilisateur et identifiant de compte dans **POST authorize** • Nouvelle configuration des sous-réseaux dans **POST /grid/grid-networks/update** • Nouveaux serveurs NTP dans **POST /grid/ntp-servers/update** • Identifiants des serveurs mis hors service dans **POST /grid/servers/decommission** **Remarque :** Les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MRMD	Méthode de requête	La méthode de requête HTTP : • POST • PUT • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de la réponse	Le contenu de la réponse (le corps de la réponse) est enregistré par défaut. **Remarque :** Les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MSIP	Adresse IP source	L'adresse IP du client (source).
MUUN	URN utilisateur	L'URN (nom uniforme de ressource) de l'utilisateur qui a envoyé la requête.
RSLT	Résultat	Renvoie une opération réussie (SUCS) ou l'erreur signalée par le backend.

Message d'audit OLST pour les objets perdus détectés par le système dans StorageGRID

Ce message est généré lorsque le service DDS ne parvient pas à localiser une copie d'un objet dans le système StorageGRID.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	L'identifiant CBID de l'objet perdu.
NOID	ID du nœud	Si disponible, la dernière position connue, directe ou quasi directe, de l'objet perdu. Il est possible de ne disposer que de l'identifiant du nœud sans identifiant de volume si les informations relatives au volume sont indisponibles.
CHEMIN	Compartiment/clé S3	Si disponible, le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Ce champ a la valeur NONE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.
UUID	Identifiant unique universel	L'identifiant de l'objet perdu dans le système StorageGRID.
VOLUME	ID du volume	Si disponible, l'identifiant du volume du nœud de stockage pour le dernier emplacement connu de l'objet perdu.

Message d'audit ORLM pour les règles ILM respectées dans StorageGRID

Ce message est généré lorsque l'objet est correctement stocké et copié conformément aux règles ILM.

> Le message ORLM n'est pas généré lorsqu'un objet est correctement stocké par la règle par défaut « Make 2 Copies » si une autre règle de la stratégie utilise le filtre avancé « Object Size ».

Code	Champ	Description
BUID	En-tête de compartiment	Champ d'identifiant du compartiment. Utilisé pour les opérations internes. Apparaît uniquement si STAT est PRGD.
CBID	Identifiant de bloc de contenu	L'identifiant CBID de l'objet.
CSIZ	Taille du contenu	La taille de l'objet en octets.

Code	Champ	Description
LOCS	Lieux	Emplacement de stockage des données d'objet au sein du système StorageGRID. La valeur de LOCS est "" si l'objet n'a pas d'emplacement (par exemple, s'il a été supprimé). CLEC : pour les objets à code d'effacement, l'identifiant du profil de code d'effacement et l'identifiant du groupe de code d'effacement appliqués aux données de l'objet. CLDI : pour les objets répliqués, l'ID du nœud LDR et l'ID du volume de l'emplacement de l'objet. CLNL : ID du nœud ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Résultat de l'opération ILM. SUCS : L'opération ILM a réussi.
RÈGLE	Étiquette des règles	Étiquette lisible par l'homme attribuée à la règle ILM appliquée à cet objet.
SEGC	UUID du conteneur	UUID du conteneur de l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	Conteneur CBID	CBID du conteneur de l'objet segmenté. Cette valeur est disponible uniquement pour les objets segmentés et multipart.
STAT	Statut	Statut de l'opération ILM. TERMINÉ : Les opérations ILM sur l'objet sont terminées. DFER : L'objet a été marqué pour une future réévaluation ILM. PRGD : L'objet a été supprimé du système StorageGRID. NLOC : Les données de l'objet sont introuvables dans le système StorageGRID. Ce statut peut indiquer que toutes les copies des données de l'objet sont manquantes ou endommagées.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version d'un nouvel objet créé dans un compartiment versionné. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Le message d'audit ORLM peut être émis plusieurs fois pour un même objet. Par exemple, il est émis chaque fois que l'un des événements suivants se produit :

- Les règles ILM de l'objet sont satisfaites indéfiniment.
- Les règles ILM de l'objet sont satisfaites pour cette époque.
- Les règles ILM ont supprimé l'objet.
- Le processus de vérification en arrière-plan détecte qu'une copie des données d'un objet répliqué est corrompue. Le système StorageGRID effectue une évaluation ILM afin de remplacer l'objet corrompu.

Informations connexes

- "Transactions d'ingestion d'objets"
- "Transactions de suppression d'objet"

Message d'audit OVWR pour les remplacements d'objets dans StorageGRID

Ce message est généré lorsqu'une opération externe (demandée par le client) provoque le remplacement d'un objet par un autre.

Code	Champ	Description
CBID	Identifiant de bloc de contenu (nouveau)	L'identifiant CBID du nouvel objet.
CSIZ	Taille précédente de l'objet	La taille, en octets, de l'objet en cours d'écrasement.
OCBD	Identifiant du bloc de contenu (précédent)	L'identifiant CBID de l'objet précédent.
UUID	Identifiant unique universel (nouveau)	L'identifiant du nouvel objet au sein du système StorageGRID.
OUID	Identifiant unique universel (précédent)	L'identifiant de l'objet précédent au sein du système StorageGRID.
CHEMIN	Chemin d'objet S3	Le chemin d'accès à l'objet S3 utilisé à la fois pour l'objet précédent et le nouvel objet
RSLT	Code de résultat	Résultat de la transaction d'écrasement d'objet. Le résultat est toujours : SUCS: Réussi
SGRP	Site (Groupe)	Le cas échéant, l'objet écrasé a été supprimé sur le site spécifié, qui n'est pas le site où l'objet écrasé a été ingéré.

Message d’audit S3SL pour les requêtes S3 Select dans StorageGRID

Ce message signale la fin d’une requête S3 Select renvoyée au client. Le message S3SL peut inclure un message d’erreur et un code d’erreur. La requête pourrait ne pas avoir abouti.

Code	Champ	Description
BYSC	Octets analysés	Nombre d’octets analysés (reçus) en provenance des nœuds de stockage. Les valeurs de BYSC et BYPR seront probablement différentes si l’objet est compressé. Si l’objet est compressé, BYSC indiquera le nombre d’octets compressés et BYPR le nombre d’octets après décompression.
BYPR	Octets traités	Nombre d’octets traités. Indique combien d’octets des « Bytes Scanned » ont effectivement été traités ou pris en compte par une tâche S3 Select.
BYRT	Octets renvoyés	Nombre d’octets qu’une tâche S3 Select a renvoyés au client.
REPR	Enregistrements traités	Nombre d’enregistrements ou de lignes qu’une tâche S3 Select a reçus des nœuds de stockage.
RERT	Enregistrements retournés	Nombre d’enregistrements ou de lignes qu’une tâche S3 Select a renvoyés au client.
JOFI	Travail terminé	Indique si la tâche S3 Select a terminé son traitement ou non. Si cette valeur est fausse, alors la tâche n’a pas pu se terminer et les champs d’erreur contiendront probablement des données. Le client peut avoir reçu des résultats partiels, ou aucun résultat du tout.
REID	ID de la requête	Identifiant de la requête S3 Select.
EXTM	Temps d’exécution	Le temps, en secondes, qu’il a fallu pour que la tâche S3 Select se termine.
ERMG	Message d’erreur	Message d’erreur généré par le job S3 Select.
ERTY	Type d’erreur	Type d’erreur généré par la tâche S3 Select.
ERST	Trace de la pile d’erreurs	Trace de la pile d’erreurs générée par le job S3 Select.
S3BK	compartiment S3	Le nom du compartiment S3.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de la clé d'accès S3 de l'utilisateur qui a envoyé la requête.
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment.

Message d'audit SADD pour la désactivation de l'audit de sécurité dans StorageGRID

Ce message indique que le service d'origine (ID du nœud) a désactivé la journalisation des messages d'audit. StorageGRID ne collecte ni ne transmet plus de messages d'audit.

Code	Champ	Description
AETM	Méthode d'activation	La méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Le nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur NONE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.

Ce message indique que la journalisation était activée, mais qu'elle est désormais désactivée. Cette fonctionnalité est généralement utilisée uniquement lors des ingestions massives afin d'améliorer les performances du système. Après l'activité en masse, l'audit est rétabli (SADE) et la possibilité de désactiver l'audit est alors définitivement bloquée.

Message d'audit SADE pour l'activation de l'audit de sécurité dans StorageGRID

Ce message indique que le service d'origine (ID du nœud) a rétabli la journalisation des messages d'audit. StorageGRID collecte et distribue à nouveau les messages d'audit.

Code	Champ	Description
AETM	Méthode d'activation	La méthode utilisée pour activer l'audit.
AEUN	Nom d'utilisateur	Le nom d'utilisateur qui a exécuté la commande permettant d'activer la journalisation d'audit.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur NONE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.

Ce message indique que la journalisation était précédemment désactivée (SADD), mais qu'elle a été rétablie. Cette fonction est généralement utilisée uniquement lors des ingestions massives afin d'améliorer les performances du système. Après cette opération, l'audit est rétabli et la possibilité de le désactiver est alors définitivement bloquée.

Message d'audit SCMT pour les validations dans StorageGRID

Le contenu de la grille n'est pas rendu disponible ni reconnu comme stocké tant qu'il n'a pas été validé (c'est-à-dire stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a passé les contrôles d'intégrité associés. Ce message est émis lorsqu'un bloc de contenu est validé dans le stockage.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu validé pour le stockage permanent.
RSLT	Code de résultat	État au moment où l'objet a été enregistré sur le disque : SUCS: Objet enregistré avec succès.

Ce message indique qu'un bloc de contenu a été entièrement enregistré et vérifié, et qu'il peut désormais être demandé. Il permet de suivre le flux de données au sein du système.

Message d'audit SDEL pour les transactions S3 DELETE dans StorageGRID

Lorsqu'un client S3 effectue une transaction DELETE, une requête est envoyée pour supprimer l'objet ou le compartiment spécifié, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si elle est présente dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les compartiments ne comprennent pas ce champ.
DMRK	Supprimer l'identifiant de version du marqueur	L'identifiant de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment versionné. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion Grid Federation	L'identifiant de connexion de la fédération de grilles associé à une demande de suppression par réplication inter-grilles. Inclus uniquement dans les journaux d'audit de la grille de destination.
GFSA	ID du compte source de la fédération de grille	L'identifiant du compte du locataire sur la grille source pour une requête de suppression par réplication inter-grilles. Uniquement inclus dans les journaux d'audit de la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs des en-têtes de requêtes HTTP enregistrés, tels que sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus s'il est présent dans la requête et si la valeur `X-Forwarded-For` est différente de l'adresse IP de l'expéditeur de la requête (champ d'audit SAIP). `` `x-amz-bypass-governance-retention` est automatiquement inclus s'il est présent dans la requête.
MTME	Dernière heure de modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DELETE. Le résultat est toujours : SUCS: Réussi
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de clé d'accès S3 haché de l'utilisateur ayant envoyé la requête. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3BK	Bucket S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur laquelle l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la requête)	Nom du compte locataire de l'utilisateur ayant envoyé la requête. Vide pour les requêtes avec accès anonyme.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la requête.
SBAC	Nom du compte locataire S3 (propriétaire du compartiment)	Nom du compte locataire du propriétaire du compartiment. Utilisé pour identifier l'accès inter-comptes ou l'accès anonyme.
SBAI	ID du compte locataire S3 (propriétaire du compartiment)	L'identifiant du compte locataire du propriétaire du compartiment cible. Utilisé pour identifier l'accès anonyme ou inter-comptes.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'identifiant du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la requête. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les requêtes anonymes.
TEMPS	Durée	Temps de traitement total de la requête en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge de confiance	Si la requête a été acheminée par un équilibreur de charge de couche 7 de confiance, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUDM	Identifiant unique universel pour un marqueur de suppression	L'identifiant d'un marqueur de suppression. Les messages du journal d'audit spécifient soit UUDM, soit UUID, où UUDM indique un marqueur de suppression créé à la suite d'une demande de suppression d'objet et UUID indique un objet.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SGET pour les transactions S3 GET dans StorageGRID

Lorsqu'un client S3 effectue une transaction GET, une requête est envoyée pour récupérer un objet, lister les objets d'un compartiment ou supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si elle est présente dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré, exprimée en octets. Les opérations sur les compartiments ne prennent pas en compte ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs des en-têtes de requêtes HTTP enregistrés, tels que sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus s'il est présent dans la requête et si la valeur `X-Forwarded-For` est différente de l'adresse IP de l'expéditeur de la requête (champ d'audit SAIP). ``

Code	Champ	Description
LITY	ListObjectsV2	Une réponse au format *v2* a été demandée. Pour plus de détails, consultez "AWS ListObjectsV2". Pour les opérations GET sur les compartiments uniquement.
NCHD	Nombre d'enfants	Inclut les clés et les préfixes courants. Uniquement pour les opérations GET sur les compartiments.
Rang	Lecture de plage	Pour les opérations de lecture par plage uniquement. Indique la plage d'octets lue par cette requête. La valeur après la barre oblique (/) indique la taille de l'objet entier.
RSLT	Code de résultat	Résultat de la transaction GET. Résultat est toujours : SUCS: Réussi
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de clé d'accès S3 haché de l'utilisateur ayant envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	Bucket S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur laquelle l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la requête)	Nom du compte locataire de l'utilisateur ayant envoyé la requête. Vide pour les requêtes avec accès anonyme.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la requête.
SBAC	Nom du compte locataire S3 (propriétaire du compartiment)	Nom du compte locataire du propriétaire du compartiment. Utilisé pour identifier l'accès inter-comptes ou l'accès anonyme.

Code	Champ	Description
SBAI	ID du compte locataire S3 (propriétaire du compartiment)	L'identifiant du compte locataire du propriétaire du compartiment cible. Utilisé pour identifier l'accès anonyme ou inter-comptes.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'identifiant du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la requête. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les requêtes anonymes.
TEMPS	Durée	Temps de traitement total de la requête en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge de confiance	Si la requête a été acheminée par un équilibreur de charge de couche 7 de confiance, l'adresse IP de l'équilibreur de charge.
TRNC	Tronqué ou non tronqué	Définissez cette valeur sur false si tous les résultats ont été renvoyés. Définissez cette valeur sur true si d'autres résultats sont disponibles à renvoyer. Uniquement pour les opérations GET sur les compartiments.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet qui a été demandée. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SHEA pour les opérations S3 HEAD dans StorageGRID

Lorsqu'un client S3 effectue une opération HEAD, une requête est envoyée pour vérifier l'existence d'un objet ou d'un compartiment et récupérer les métadonnées sur un objet. Ce message est émis par le serveur si l'opération réussit.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.

Code	Champ	Description
CSIZ	Taille du contenu	La taille de l'objet vérifié, en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs des en-têtes de requêtes HTTP enregistrés, tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la requête et si la valeur `X-Forwarded-For` est différente de l'adresse IP de l'expéditeur de la requête (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction GET. Résultat est toujours : SUCS: Réussi
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de clé d'accès S3 haché de l'utilisateur ayant envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	Bucket S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
SACC	Nom du compte locataire S3 (expéditeur de la requête)	Nom du compte locataire de l'utilisateur ayant envoyé la requête. Vide pour les requêtes avec accès anonyme.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la requête.
SBAC	Nom du compte locataire S3 (propriétaire du compartiment)	Nom du compte locataire du propriétaire du compartiment. Utilisé pour identifier l'accès inter-comptes ou l'accès anonyme.

Code	Champ	Description
SBAI	ID du compte locataire S3 (propriétaire du compartiment)	L'identifiant du compte locataire du propriétaire du compartiment cible. Utilisé pour identifier l'accès anonyme ou inter-comptes.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'identifiant du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la requête. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les requêtes anonymes.
TEMPS	Durée	Temps de traitement total de la requête en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge de confiance	Si la requête a été acheminée par un équilibreur de charge de couche 7 de confiance, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet qui a été demandée. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SPOS pour les transactions S3 POST dans StorageGRID

Lorsqu'un client S3 envoie une requête POST Object, ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si elle est présente dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs des en-têtes de requêtes HTTP enregistrés, tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la requête et si la valeur `X-Forwarded-For` est différente de l'adresse IP de l'expéditeur de la requête (champ d'audit SAIP). (Non prévu pour SPOS).
RSLT	Code de résultat	Résultat de la requête RestoreObject. Le résultat est toujours : SUCS: Réussi
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de clé d'accès S3 haché de l'utilisateur ayant envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	Bucket S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur laquelle l'opération est effectuée, le cas échéant. Définissez sur « select » pour une opération S3 Select.
SACC	Nom du compte locataire S3 (expéditeur de la requête)	Nom du compte locataire de l'utilisateur ayant envoyé la requête. Vide pour les requêtes avec accès anonyme.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la requête.

Code	Champ	Description
SBAC	Nom du compte locataire S3 (propriétaire du compartiment)	Nom du compte locataire du propriétaire du compartiment. Utilisé pour identifier l'accès inter-comptes ou l'accès anonyme.
SBAI	ID du compte locataire S3 (propriétaire du compartiment)	L'identifiant du compte locataire du propriétaire du compartiment cible. Utilisé pour identifier l'accès anonyme ou inter-comptes.
SRCF	Configuration des sous-ressources	Restaurer les informations.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'identifiant du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la requête. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les requêtes anonymes.
TEMPS	Durée	Temps de traitement total de la requête en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge de confiance	Si la requête a été acheminée par un équilibreur de charge de couche 7 de confiance, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet qui a été demandée. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SPUT pour les transactions S3 PUT dans StorageGRID

Lorsqu'un client S3 effectue une opération PUT, une requête est envoyée pour créer un nouvel objet ou compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du compartiment, s'ils sont présents dans la requête (tronqués aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si elle est présente dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré, exprimée en octets. Les opérations sur les compartiments ne prennent pas en compte ce champ.
GFID	ID de connexion Grid Federation	L'identifiant de connexion de la fédération de grilles associé à une requête PUT de réplication inter-grilles. Inclus uniquement dans les journaux d'audit de la grille de destination.
GFSA	ID du compte source de la fédération de grille	L'identifiant du compte du locataire sur la grille source pour une requête PUT de réplication inter-grilles. Uniquement inclus dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs des en-têtes de requêtes HTTP enregistrés, tels que sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus s'il est présent dans la requête et si la valeur `X-Forwarded-For` est différente de l'adresse IP de l'expéditeur de la requête (champ d'audit SAIP). `` `x-amz-bypass-governance-retention` est automatiquement inclus s'il est présent dans la requête.
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête de requête `x-amz-bucket-object-lock-enabled`, si elle est présente dans la requête.
LKLH	Conservation légale du verrouillage d'objet	Valeur de l'en-tête de requête `x-amz-object-lock-legal-hold`, si elle est présente dans la requête PutObject.

Code	Champ	Description
LKMD	Mode de rétention du verrouillage d'objet	Valeur de l'en-tête de requête `x-amz-object-lock-mode`, si elle est présente dans la requête PutObject.
LKRU	Date de conservation du verrouillage d'objet	Valeur de l'en-tête de requête `x-amz-object-lock-retain-until-date`, si elle est présente dans la requête PutObject. Les valeurs sont limitées à 100 ans à compter de la date d'ingestion de l'objet.
MTME	Dernière heure de modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction PUT. Résultat est toujours : SUCS: Réussi
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de clé d'accès S3 haché de l'utilisateur ayant envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	Bucket S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur laquelle l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la requête)	Nom du compte locataire de l'utilisateur ayant envoyé la requête. Vide pour les requêtes avec accès anonyme.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la requête.
SBAC	Nom du compte locataire S3 (propriétaire du compartiment)	Nom du compte locataire du propriétaire du compartiment. Utilisé pour identifier l'accès inter-comptes ou l'accès anonyme.

Code	Champ	Description
SBAI	ID du compte locataire S3 (propriétaire du compartiment)	L'identifiant du compte locataire du propriétaire du compartiment cible. Utilisé pour identifier l'accès anonyme ou inter-comptes.
SRCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1 024 premiers caractères).
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'identifiant du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la requête. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les requêtes anonymes.
TEMPS	Durée	Temps de traitement total de la requête en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge de confiance	Si la requête a été acheminée par un équilibreur de charge de couche 7 de confiance, l'adresse IP de l'équilibreur de charge.
ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations CompleteMultipartUpload. Indique que toutes les parties ont été téléchargées et assemblées.
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version d'un nouvel objet créé dans un compartiment versionné. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.
VSST	État de version	Le nouvel état de versionnage d'un compartiment. Deux états sont utilisés : « activé » ou « suspendu ». Les opérations sur les objets n'incluent pas ce champ.

Message d'audit SREM pour la suppression d'un object store dans StorageGRID

Ce message est émis lorsque du contenu est supprimé du stockage persistant et n'est plus accessible via les API classiques.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu supprimé du stockage permanent.

Code	Champ	Description
RSLT	Code de résultat	Indique le résultat des opérations de suppression de contenu. La seule valeur définie est : SUCS : Contenu supprimé du stockage persistant

Ce message d'audit indique qu'un bloc de contenu a été supprimé d'un nœud et ne peut plus être demandé directement. Ce message peut être utilisé pour suivre le flux de contenu supprimé au sein du système.

Message d'audit SUPD pour les mises à jour des métadonnées S3 dans StorageGRID

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées réussit.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si elle est présente dans la requête, lors de la mise à jour des paramètres de conformité d'un compartiment.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré, exprimée en octets. Les opérations sur les compartiments ne prennent pas en compte ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs des en-têtes de requêtes HTTP enregistrés, tels que sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus s'il est présent dans la requête et si la valeur `X-Forwarded-For` est différente de l'adresse IP de l'expéditeur de la requête (champ d'audit SAIP). ``
RSLT	Code de résultat	Résultat de la transaction GET. Résultat est toujours : SUCS: succès

Code	Champ	Description
S3AI	ID du compte locataire S3 (expéditeur de la requête)	L'identifiant du compte locataire de l'utilisateur qui a envoyé la requête. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la requête)	L'identifiant de clé d'accès S3 haché de l'utilisateur ayant envoyé la requête. Une valeur vide indique un accès anonyme.
S3BK	Bucket S3	Le nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3, sans le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
SACC	Nom du compte locataire S3 (expéditeur de la requête)	Nom du compte locataire de l'utilisateur ayant envoyé la requête. Vide pour les requêtes avec accès anonyme.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la requête.
SBAC	Nom du compte locataire S3 (propriétaire du compartiment)	Nom du compte locataire du propriétaire du compartiment. Utilisé pour identifier l'accès inter-comptes ou l'accès anonyme.
SBAI	ID du compte locataire S3 (propriétaire du compartiment)	L'identifiant du compte locataire du propriétaire du compartiment cible. Utilisé pour identifier l'accès anonyme ou inter-comptes.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'identifiant du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la requête. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les requêtes anonymes.
TEMPS	Durée	Temps de traitement total de la requête en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge de confiance	Si la requête a été acheminée par un équilibreur de charge de couche 7 de confiance, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	L'identifiant de l'objet au sein du système StorageGRID.
VSID	ID de version	L'identifiant de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Message d'audit SVRF pour les échecs de vérification du stockage d'objets dans StorageGRID

Ce message s'affiche lorsqu'un bloc de contenu échoue au processus de vérification. À chaque lecture ou écriture de données d'objet répliquées sur disque, plusieurs contrôles de vérification et d'intégrité sont effectués afin de garantir que les données envoyées à l'utilisateur demandeur sont identiques aux données initialement ingérées dans le système. Si l'un de ces contrôles échoue, le système met automatiquement en quarantaine les données d'objet répliquées corrompues pour empêcher qu'elles ne soient récupérées à nouveau.

Code	Champ	Description
CBID	Identifiant de bloc de contenu	L'identifiant unique du bloc de contenu dont la vérification a échoué.
RSLT	Code de résultat	Type d'échec de vérification : CRCF : Échec du contrôle de redondance cyclique (CRC). HMAC : Échec du contrôle du code d'authentification de message basé sur le hachage (HMAC). EHSH : Hachage de contenu chiffré inattendu. PHSH : Hachage de contenu d'origine inattendu. SEQC : Séquence de données incorrecte sur le disque. PERR : Structure de fichier disque invalide. DERR : Erreur de disque. FNAM : Nom de fichier incorrect.

Ce message doit être surveillé de près. Les échecs de vérification du contenu peuvent indiquer des défaillances matérielles imminentes.

Pour déterminer l'opération à l'origine du message, consultez la valeur du champ AMID (ID du module). Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire la vérification en arrière-plan, et STOR indique que le message a été déclenché par la récupération de contenu.

Message d'audit SVRU pour un contenu de magasin d'objets inconnu dans StorageGRID

Le composant de stockage du service LDR analyse en continu toutes les copies des données d'objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue de données d'objet répliquées est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Le chemin d'accès du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. « AUCUN » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

Le message d'audit SVRU : Object Store Verify Unknown doit être surveillé de près. Il indique que des copies inattendues de données d'objets ont été détectées dans le magasin d'objets. Vous devez enquêter immédiatement sur cette situation afin de déterminer comment ces copies ont été créées, car cela peut indiquer des défaillances matérielles imminentes.

Message d'audit SYSD pour les arrêts de nœuds en douceur dans StorageGRID

Lorsqu'un service s'arrête correctement, ce message est généré pour indiquer que l'arrêt a été demandé. Généralement, ce message n'est envoyé qu'après un redémarrage ultérieur, car la file d'attente des messages du journal des audits n'est pas vidée avant l'arrêt. Si le service n'a pas redémarré, recherchez le message SYST, envoyé au début de la séquence d'arrêt.

Code	Champ	Description
RSLT	Arrêt propre	Nature de la fermeture : SUCS : Le système a été arrêté proprement.

Le message n'indique pas si le serveur hôte est en cours d'arrêt, uniquement le service de signalement. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « dirty », car le message est généré uniquement lors d'arrêts « clean ».

Message d'audit SYST pour l'arrêt d'un nœud dans StorageGRID

Lorsqu'un service est arrêté correctement, ce message est généré pour indiquer que l'arrêt a été demandé et que le service a entamé sa séquence d'arrêt. SYST peut être utilisé pour déterminer si l'arrêt a été demandé, avant que le service ne soit redémarré (contrairement à SYSD, qui est généralement envoyé après le redémarrage du service).

Code	Champ	Description
RSLT	Arrêt propre	Nature de la fermeture : SUCS : Le système a été arrêté proprement.

Le message n'indique pas si le serveur hôte est en cours d'arrêt, uniquement le service de signalement. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « dirty », car ce message est généré uniquement lors d'arrêts « clean ».

Message d'audit SYSU pour le nœud démarre dans StorageGRID

Lorsqu'un service est redémarré, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Arrêt propre	Nature de la fermeture : SUCS : Le système a été arrêté proprement. DSDN : Le système n'a pas été arrêté correctement. VRGN : Le système a été démarré pour la première fois après l'installation (ou la réinstallation) du serveur.

Ce message n'indique pas si le serveur hôte a été démarré, mais uniquement le service de rapports. Ce message peut servir à :

- Détectez toute discontinuité dans le journal des audits.
- Déterminez si un service présente une défaillance en cours de fonctionnement (la nature distribuée du système StorageGRID pouvant masquer ces défaillances). Server Manager redémarre automatiquement tout service défaillant.