



Examiner les journaux d'audit

StorageGRID software

NetApp
February 12, 2026

Sommaire

Examiner les journaux d'audit	1
Journaux et messages d'audit	1
Flux et conservation des messages d'audit	1
Flux de message d'audit	1
Accéder au fichier journal d'audit	4
Rotation du fichier journal d'audit	5
Format du fichier journal d'audit	6
Format du fichier journal d'audit	6
Utiliser l'outil d'explication d'audit	7
Utiliser l'outil audit-sum	9
Format du message d'audit	18
Format du message d'audit	18
Types de données	19
Données spécifiques à un événement	19
Éléments communs dans les messages d'audit	20
Exemples de messages d'audit	21
Messages d'audit et cycle de vie de l'objet	23
Quand un message d'audit est-il généré ?	23
Transactions d'ingestion d'objets	23
Transactions de suppression d'objet	25
Transactions de récupération d'objet	26
Messages de mise à jour des métadonnées	28
Messages d'audit	29
Descriptions des messages d'audit	29
Catégories de messages d'audit	30
Référence du message d'audit	34

Examiner les journaux d'audit

Journaux et messages d'audit

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

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

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"](#) .

Flux et conservation des messages d'audit

Tous les services StorageGRID génèrent des messages d'audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit se déplacent dans le fichier via le système StorageGRID `audit.log`.

Les flux de travail suivants pour les messages d'audit et la conservation des messages d'audit ne s'appliquent que si StorageGRID est configuré pour les **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 du `/var/local/log/localaudit.log` fichier et ne peut pas être traité par les nœuds d'administration ou les nœuds de stockage.

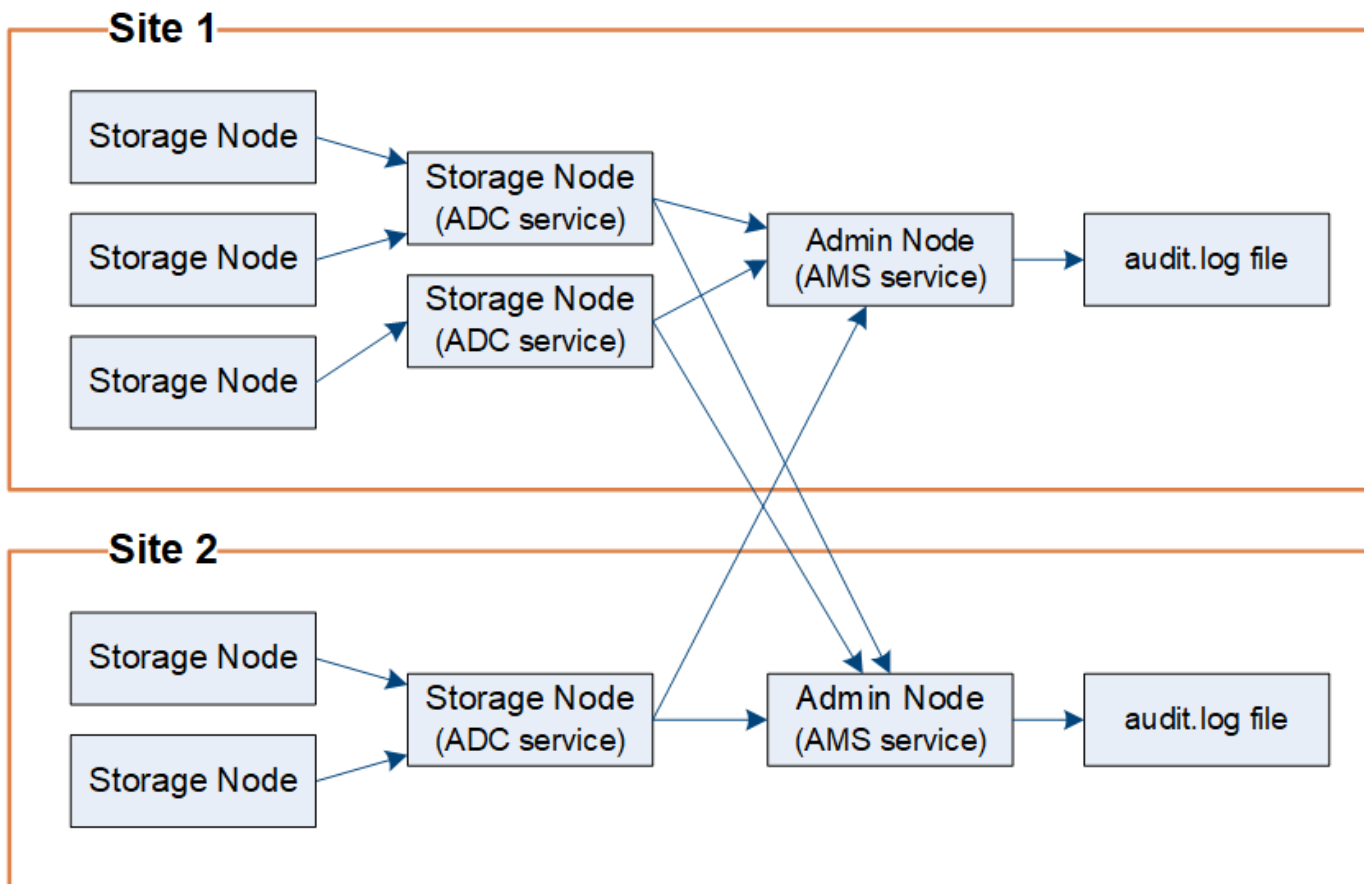
Flux de message d'audit

Les messages d'audit sont traités par les nœuds d'administration lorsque StorageGRID est configuré pour les **nœuds d'administration/nœuds locaux** ou **nœud d'administration et serveur syslog externe** et par les nœuds de stockage qui disposent d'un service de contrôleur de domaine administratif (ADC).

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

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

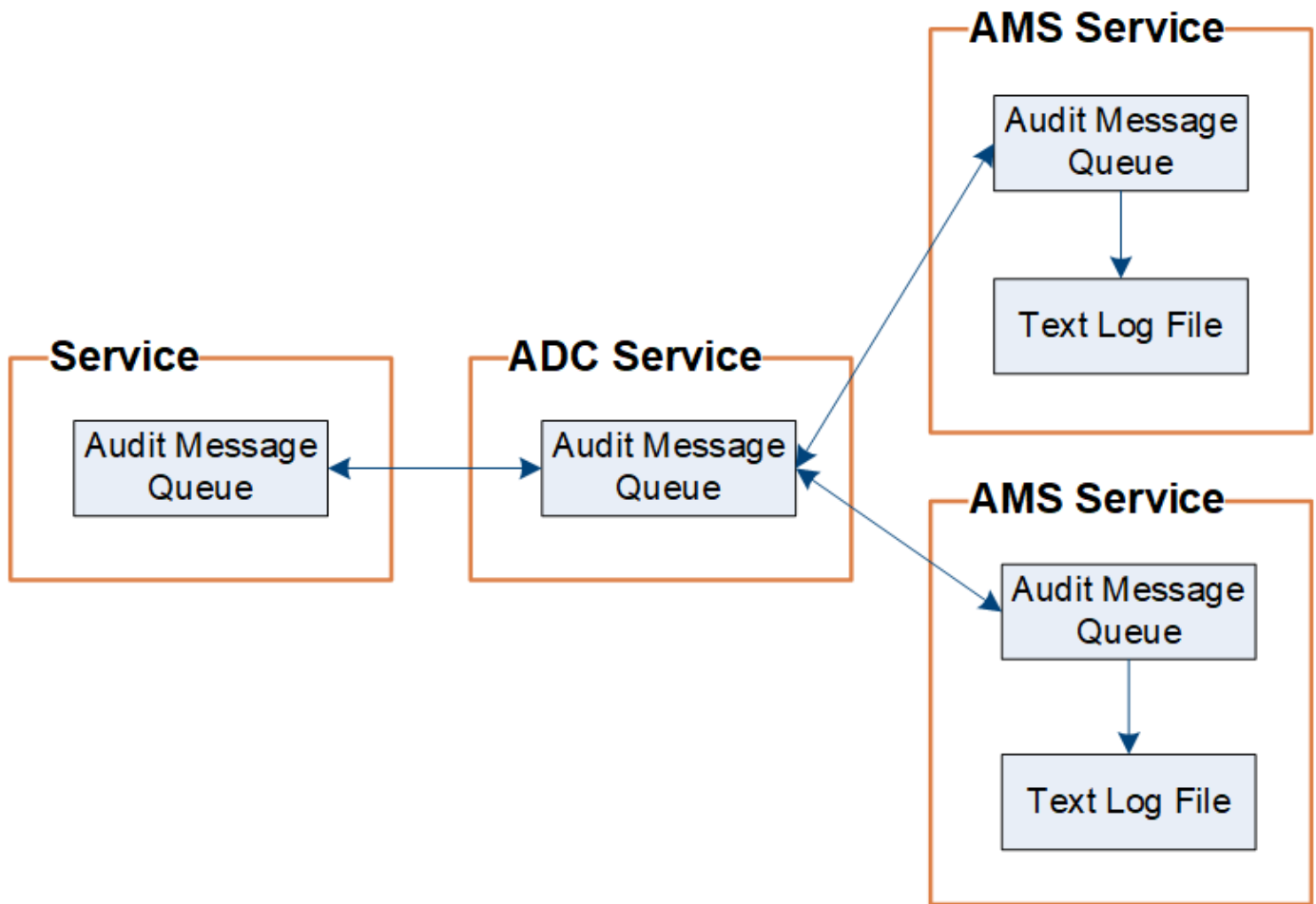
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



Conservation des messages d'audit

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

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



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

Plus précisément, vous pouvez voir les comportements suivants :

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



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 `/var/local/log/localaudit.log` le fichier.

- Si le `/var/local/` le répertoire utilisé par un nœud de stockage devient plein à 85 %, le nœud

commence à refuser les demandes des clients S3 avec 503 Service Unavailable .

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

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

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

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

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

Si l'alerte ou l'alarme persiste et augmente en gravité, affichez un graphique de la taille de la file d'attente. Si le nombre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit enregistrés en modifiant le niveau d'audit pour les écritures et les lectures du client sur Erreur ou Désactivé. Voir ["Configurer la gestion des journaux et le serveur syslog externe"](#) .

Dupliquer les messages

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

Accéder au fichier journal d'audit

Le partage d'audit contient le fichier actif `audit.log` et tous les fichiers journaux d'audit compressés. Vous pouvez accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Le `audit.log` le fichier reste vide sauf si vous configurez StorageGRID pour **Nœuds d'administration/nœuds locaux** ou **Nœud d'administration et serveur syslog externe**. Pour plus d'informations, reportez-vous à ["Sélectionnez l'emplacement du journal"](#) .

Avant de commencer

- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Étapes

1. Connectez-vous à un nœud d'administration :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Accédez au répertoire contenant les fichiers journaux d'audit :

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

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

Rotation du fichier journal d'audit

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



En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. "[Configurer les messages d'audit et le serveur syslog externe](#)".

Une fois par jour, le fichier actif `audit.log` est enregistré et un nouveau `audit.log` fichier démarre. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`. Si plusieurs journaux d'audit sont créés en une seule journée, les noms de fichier utilisent la date à laquelle le fichier a été enregistré, ajoutée par un nombre, 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.

Après une journée, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui préserve la date originale. Au fil du temps, le stockage du nœud d'administration alloué aux journaux d'audit est consommé. Un script surveille la consommation d'espace du journal d'audit et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le `/var/local/audit/export/ annuaire`. Les journaux d'audit sont supprimés en fonction de la date de leur 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 du jour précédent (`2018-04-15.txt`) et le fichier compressé du jour précédent (`2018-04-14.txt.gz`).

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

Format du fichier journal d'audit

Format du fichier journal d'audit

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent un ensemble de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Temps universel coordonné (UTC) de l'événement qui a déclenché le message d'audit (ATIM) au format ISO 8601, suivi d'un espace :

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

- Le message d'audit lui-même, entre crochets et commençant par AUDT.

L'exemple suivant montre trois messages d'audit dans un fichier journal d'audit (sauts de ligne ajoutés pour la lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un compartiment S3 et a ajouté deux objets dans ce compartiment.

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 journaux d’audit ne sont pas faciles à lire ou à interpréter. Vous pouvez utiliser le ["outil d'audit-explication"](#) pour obtenir des résumés simplifiés des messages d’audit dans le journal d’audit. Vous pouvez utiliser le ["outil de somme d'audit"](#) pour résumer le nombre d’opérations d’écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.

Utiliser l’outil d’explication d’audit

Vous pouvez utiliser `audit-explain` l’outil pour traduire les messages d’audit dans le journal d’audit dans un format facile à lire.

Avant de commencer

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

Description de la tâche

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



Cet `audit-explain` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-explain` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l'`audit-explain`outil. Ces quatre "SPUT" messages d'audit ont été générés lorsque le locataire S3 associé à l'ID de compte 92484777680322627870 a utilisé des demandes PUT S3 pour créer un compartiment nommé « bucket1 » et ajouter trois objets à ce compartiment.

```
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 :

- Traiter les journaux d'audit 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 l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'autres moyens. Par exemple :

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

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

Comme les journaux d'audit peuvent être très volumineux et lents à analyser, vous gagnez du temps en filtrant les parties que vous souhaitez consulter et exécuter `audit-explain` sur les pièces, au lieu du fichier entier.



`audit-explain` L'outil n'accepte pas les fichiers compressés en tant qu'entrée de tuyauterie. Pour traiter des fichiers compressés, indiquez leurs noms de fichiers en tant qu'arguments de ligne de commande ou utilisez l'`zcat` outil pour décompresser d'abord les fichiers. Par exemple :

```
zcat audit.log.gz | audit-explain
```

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

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

Étapes

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Entrez 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 imprime des interprétations lisibles de tous les messages du ou des fichiers spécifiés.



Pour réduire la longueur des lignes et faciliter la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous voulez voir les horodatages, utilisez l'`-t` option horodatage).

Utiliser l'outil audit-sum

Vous pouvez utiliser `audit-sum` l'outil pour compter les messages d'audit d'écriture, de lecture, de tête et de suppression et pour afficher le temps minimal, maximal et moyen (ou la taille) 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.

Description de la tâche

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



Cet `audit-sum` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-sum` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l'`audit-sum`outil. Cet exemple montre la durée des opérations de protocoles.

```

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

```

Le `audit-sum` L'outil fournit les décomptes et les heures des messages d'audit S3 et ILM suivants dans un journal d'audit.



Les codes d'audit sont supprimés du produit et de la documentation à mesure que les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, vérifiez les versions précédentes de cette rubrique pour les anciennes versions de StorageGRID . Par exemple : ["StorageGRID 11.8 Utilisation de l'outil de somme d'audit"](#) .

Code	Description	Reportez-vous à la section
IDEL	ILM initialisée – journaux lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.	"SDEL : SUPPRESSION S3"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	"SHEA : TÊTE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.	"SPUT : PUT S3"

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

- Traiter les journaux d'audit 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 l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande 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 comme entrée canalisée. Pour traiter les fichiers compressés, fournissez leurs noms de fichiers comme arguments de ligne de commande ou utilisez le `zcat` outil pour décompresser les fichiers en premier. Par exemple:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Vous pouvez utiliser les options de ligne de commande pour résumer les opérations sur des compartiments séparément des opérations sur des objets ou pour regrouper les résumés de messages par nom de compartiment, par période ou par type de cible. Par défaut, les résumés affichent le temps de fonctionnement minimal, maximal et moyen, mais vous pouvez utiliser l' `size (-s)` option pour examiner la taille de l'objet à la place.

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

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

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour basculer en root : `su -`
- d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Pour analyser tous les messages liés aux opérations d'écriture, de lecture, de tête et de suppression, procédez comme suit :

- a. Entrez 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 montre les résultats typiques de l'`audit-sum`outil. Cet exemple montre la durée des opérations de protocoles.

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 opérations les plus lentes en moyenne à 1.13 secondes, mais les opérations SGET et SPUT (S3 PUT) affichent toutes les deux de longues périodes de pire des cas d'environ 1,770 secondes.

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

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

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet d'afficher le journal d'audit pour les 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/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
      backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
      backup/r90l0aQ8JB-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

```

+ Dans cet exemple de sortie, vous pouvez constater que les trois demandes GET S3 les plus lentes étaient celles des objets d'une taille d'environ 5 Go (ce qui est beaucoup plus important que les autres objets). La grande taille tient compte des délais de récupération lents les moins importants.

3. Si vous voulez déterminer la taille des objets qui sont ingérés et récupérés à partir de votre grille, utilisez l'option taille (-s) :

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

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

Dans cet exemple, la taille moyenne des objets pour SPUT est inférieure à 2.5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est beaucoup plus élevé que le nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous voulez déterminer si les récupérations étaient lentes hier :
 - a. Exécutez la commande dans le journal d'audit approprié et utilisez l'option Group-by-time (`-gt`(groupe par heure), suivie de la période (par exemple, 15M, 1H, 10S) :

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


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

Ces résultats montrent que le trafic S3 GET a augmenté entre 06h00 et 07h00. Les temps maximum et moyen sont tous deux considérablement plus élevés au cours de cette période, et ils n'ont pas augmenté progressivement à mesure que le nombre augmentait. Ces mesures suggèrent que la capacité a été dépassée, peut-être dans le réseau ou dans la capacité du réseau à traiter les demandes.

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

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

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

Ces résultats indiquent que des récupérations très importantes se sont produites lorsque le trafic global de récupération était à son maximum.

- c. Pour plus de détails, utilisez le ["outil d'audit-explication"](#) pour revoir toutes les opérations SGET pendant cette heure :

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

Si la sortie de la commande `grep` doit être de plusieurs lignes, ajoutez la `less` commande pour afficher le contenu du fichier journal d'audit, une page (un écran) à la fois.

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

- a. Commencez par utiliser l' ``-go`` option, qui regroupe les messages pour les opérations d'objet et de compartiment séparément :

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

message group average(sec)	count	min(sec)	max(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 pour les compartiments ont des caractéristiques de performances différentes de celles des opérations SPUT pour les objets.

- b. Pour déterminer les compartiments ayant 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 average(sec)	count	min(sec)	max(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 taille d'objet SPUT la plus élevée, utilisez les options `-gb` et `-s` :

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

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

Format du message d'audit

Format du message d'audit

Les messages d'audit échangés dans le système StorageGRID incluent des informations standard communes à tous les messages et du contenu spécifique décrivant l'événement ou l'activité signalé.

Si les informations récapitulatives fournies par les ["audit - expliquer"](#) outils et ["somme-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 peut apparaître dans le fichier journal d'audit :

```
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 entre parenthèses ([]) et chaque élément d'attribut de la chaîne possède les caractéristiques suivantes :

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

Chaque élément inclut un code d'attribut, un type de données et une valeur qui sont rapportées 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 pas répertoriés dans un 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 d'audit et à d'autres, qui sont spécifiques à un événement.
- `type` Est un identificateur à quatre caractères du type de données de programmation de la valeur, comme `UI64`, `FC32`, etc. Le type est entre parenthèses ().
- `value` est le contenu de l'attribut, généralement une valeur numérique ou textuelle. Les valeurs suivent toujours deux points (:). Les valeurs du type de données `CSTR` sont entourées de guillemets doubles " ".

Types de données

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 0 à 4,294,967,295.
UI64	Entier double non signé (64 bits) ; il peut stocker les nombres 0 à 18,446,744,073,709,551,615.
FC32	Constante de quatre caractères ; valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
IPAD	Utilisé pour les adresses IP.
REST	Tableau de caractères UTF-8 de longueur variable. Les caractères peuvent être échappé avec les conventions suivantes : <ul style="list-style-type: none">• La barre oblique inverse est \.• Le retour chariot est \r.• Les guillemets sont \".• La ligne d'alimentation (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 un événement

Chaque message d'audit du journal d'audit enregistre les 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 décrit par le message d'audit. Ces attributs sont mis en évidence dans l'exemple suivant :

2018-12-05T08:24 10.224.0 60025621595611246499:45.921845 100 60025621595611246499
[AUDT:*\[RSLT(FC32\):SUCS\ \[TIME\(\UI64\):11454\]\[SAIP\(\IPAD\)\]\[S3AI\(\CSTR\)\](CSTR\ \

60025621595611246499\« STU3S\ \»\« STC\ \»\« STC\ \»\[STC\ \» :\[S6S\]\[STC\|STC\|STC\]\« STC\ \»
:\[STE\]\[STC\|STC\|STC\|STE\]\[STC*\[STC\|STC\|STC\|STC*\[STC\]\« S\ \» :\[STC\]\« STE\ \» :\[STC\]\« STE\

\« :\[STE\]\« S\ \» :\[STE\]\ \» :\[STE\]\[S3S\ \» :*\[STC\|STC\|STC\|S37 30720 10 1543998285921845

12281045 15552417629170647261

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

Éléments communs dans les messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU	FC32	ID de module : identificateur à quatre caractères de l'ID de module qui a généré le message. Ceci indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : ID de nœud de la grille attribué au service qui a généré le message. Un identifiant unique est attribué à chaque service au moment de la configuration et de l'installation du système StorageGRID. Cet ID ne peut pas être modifié.
ASE	UI64	<p>Identifiant de session d'audit : dans les versions précédentes, cet élément indique l'heure à laquelle le système d'audit a été initialisé après le démarrage du service. Cette valeur temporelle a été mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970).</p> <p>Remarque : cet élément est obsolète et n'apparaît plus dans les messages d'audit.</p>
ASQN	UI64	<p>Nombre de séquences : dans les versions précédentes, ce compteur a été incrémenté pour chaque message d'audit généré sur le nœud de la grille (ANID) et remis à zéro au redémarrage du service.</p> <p>Remarque : cet élément est obsolète et n'apparaît plus dans les messages d'audit.</p>
ATID	UI64	Trace ID : identifiant partagé par l'ensemble de messages déclenchés par un seul événement.

Code	Type	Description
ATIM	UI64	<p>Timestamp: Heure à laquelle l'événement a été généré le message d'audit, mesuré 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 des millisecondes.</p> <p>Il peut être nécessaire d'arrondir ou de tronquer l'horodatage enregistré. Le temps lisible par l'utilisateur qui apparaît au début du message d'audit dans le <code>audit.log</code> fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées par <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, où le T est un caractère de chaîne littérale indiquant le début du segment de temps de la date. <code>UUUUUU</code> sont des microsecondes.</p>
ATYP	FC32	Type d'événement : identificateur à quatre caractères de l'événement en cours de consignation. Cela régit le contenu « charge utile » du message : les attributs inclus.
FINISSEUR	UI32	Version : version du message d'audit. À mesure que le logiciel StorageGRID évolue, les nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet une rétrocompatibilité dans le service AMS pour traiter les messages provenant de versions antérieures de services.
RSLT	FC32	Résultat : résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

Exemples de messages d'audit

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 peut apparaître dans `audit.log` le fichier :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][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 en cours d'enregistrement, 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):"s3small11"] [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 PUT S3, qui consigne l'ingestion d'un objet dans un compartiment.

Le message d'audit suivant indique également le compartiment à partir duquel 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\): "s3small11"] [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 savoir quand l'événement PUT s'est produit, notez l'horodatage universel coordonné (UTC) au début du message d'audit. Cette valeur est une version lisible par l'utilisateur de l'attribut ATIM du message d'audit lui-même :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [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, depuis le début de l'époque UNIX. Dans l'exemple, la valeur 1405631878959669 se traduit par jeudi, 17-Jul-2014 21:17:59 UTC.

Messages d'audit et cycle de vie de l'objet

Quand un message d'audit est-il généré ?

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

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

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

Calendrier des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de la grille, la taille de l'objet et les retards réseau, l'ordre des messages d'audit générés par les différents services peut varier de celui présenté dans les exemples de cette section.

Transactions d'ingestion d'objets

Vous pouvez identifier les transactions d'ingestion de clients dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une transaction d'ingestion ne sont pas répertoriés dans le tableau suivant. Seuls les messages nécessaires au suivi de la transaction d'ingestion sont inclus.

Ingestion des messages d'audit S3

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

Exemple : ingestion d'objet S3

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

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



Tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de transfert S3 (SPUT) sont répertoriées.

Dans cet exemple, un compartiment S3 a déjà été créé.

SPUT : PUT S3

Le message SPUT est généré pour indiquer qu'une transaction PUT S3 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 satisfaite pour cet objet. Le message inclut le CBID de l'objet et le nom de la règle ILM appliquée.

Pour les objets répliqués, le champ EMBLEMENTS inclut l'ID de nœud LDR et l'ID de volume des emplacements d'objets.

```
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 avec code d'effacement, le champ EMBLEMENTS inclut l'ID du profil de code d'effacement et l'ID du groupe de codes 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):4168559046473725560]]
```

Le champ PATH inclut les informations sur le bucket S3 et 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):344833886538369336]]
```

Transactions de suppression d'objet

Vous pouvez identifier les transactions de suppression d'objets dans le journal d'audit 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 requis pour suivre la transaction de suppression sont inclus.

S3 supprime les messages d'audit

Code	Nom	Description	Tracé	Voir
SDEL	Suppression S3	Demande de suppression de l'objet d'un compartiment.	CBID, S3KY	"SDEL : SUPPRESSION S3"

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 d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de suppression S3 (SDEL) sont répertoriées.

SDEL : suppression S3

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

```
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):"SGKHya1RU_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]]
```

Transactions de récupération d'objet

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

Tous les messages d'audit générés lors d'une transaction de récupération ne sont pas répertoriés dans le tableau suivant. Seuls les messages nécessaires au suivi de la transaction de récupération sont inclus.

Messages d'audit de récupération S3

Code	Nom	Description	Tracé	Voir
SGET	OBTENTION S3	Demande de récupération d'un objet à partir d'un compartiment.	CBID, S3BK, S3KY	"SGET : OBTENEZ S3"

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 d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction de récupération S3 (SGET) sont répertoriées.

SGET : OBTENEZ S3

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

```

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 règle de compartiment le permet, un client peut récupérer des objets de façon anonyme ou récupérer des objets à partir d'un compartiment qui est détenu par un autre compte de locataire. Le message d'audit contient des informations sur le compte du propriétaire du compartiment afin que vous puissiez suivre ces demandes 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` enregistrent l'ID et le nom de compte du propriétaire du compartiment, qui diffèrent de l'ID et du nom du compte du locataire enregistré 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 d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction `S3 Select (SelectObjectContent)` sont répertoriées.

Chaque requête génère deux messages d'audit : un qui effectue l'autorisation de la requête `S3 Select` (le champ `S3SR` est défini sur « `SELECT` ») et une opération `GET` standard 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][SAIP(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(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):1363009709396895985]]
```

2021-11-08T15:35:32.604886

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SAIP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-for\":\"unix:\"}"]][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(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):10185581][MTME(UI64):1636380348695262][AVER(UI32):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][AMID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messages de mise à jour des métadonnées

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

Messages d'audit de la mise à jour des métadonnées S3

Code	Nom	Description	Tracé	Voir
SUPD	Métadonnées S3 mises à jour	Générées 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 la réussite d'une transaction permettant de mettre à jour les métadonnées d'un objet S3 existant.

SUPD : mise à jour des métadonnées S3

Le client S3 fait une demande (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 > Serveur d'audit et syslog`). 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

Descriptions des messages d'audit

Les descriptions détaillées des messages d'audit renvoyés par le système sont répertoriées dans les sections suivantes. Chaque message d'audit est d'abord répertorié dans un tableau qui regroupe les messages associés en fonction de la classe d'activité que le message représente. Ces regroupements sont utiles à la fois pour comprendre les types d'activités auditées et pour sélectionner le type souhaité de filtrage des messages d'audit.

Les messages d'audit sont également répertoriés par ordre alphabétique par 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 trouvées dans les messages d'audit, comme indiqué 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 définition 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 système

Les messages d'audit appartenant à la catégorie d'audit du 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 des services.

Code	Titre et description du message	Voir
ECMC	Fragment de données manquant avec code d'effacement : indique qu'un fragment de données manquant avec code d'effacement a été détecté.	"ECMC : fragment de données avec code d'effacement manquant"
ECOC	Fragment de données avec code d'effacement corrompu : indique qu'un fragment de données avec code d'effacement corrompu a été détecté.	"ECOC : fragment de données avec code d'effacement corrompu"
EN	Échec de l'authentification de sécurité : une tentative de connexion à l'aide du protocole TLS (transport Layer Security) a échoué.	"ETAF : échec de l'authentification de sécurité"
GNRG	Enregistrement GNDS : service mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.	"GNRG : enregistrement GNDS"
GNUR	Annulation de l'enregistrement du GNDS : un service s'est désinscrit du système StorageGRID.	"GNUR : non-inscription du GNDS"
GTED	Tâche de grille terminée : le service CMN a terminé le traitement de la tâche de grille.	"GTED : tâche de grille terminée"
GTST	Tâche de grille démarrée : 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 envoyée au service CMN.	"GTSU : tâche de grille soumise"

Code	Titre et description du message	Voir
LLST	Emplacement perdu : ce message d'audit est généré en cas de perte d'un emplacement.	"LLST : emplacement perdu"
OLST	Objet perdu : un objet demandé ne peut pas se trouver dans le système StorageGRID.	"OLST : le système a détecté un objet perdu"
AJOUTER	Désactivation de l'audit de sécurité : l'enregistrement des messages d'audit a été désactivé.	"SADD : désactivation de l'audit de sécurité"
SADE	Activation de l'audit de sécurité : la journalisation des messages d'audit a été restaurée.	"SADE : activation de l'audit de sécurité"
SVRF	Échec de la vérification du magasin d'objets : échec de la vérification d'un bloc de contenu.	"SVRF : échec de la vérification du magasin d'objets"
SVRU	Vérification du magasin d'objets Inconnu : données d'objet inattendues 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 démarré un arrêt normal.	"SYST : arrêt du nœud"
SYSU	Node Start : service démarré, la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"

Messages d'audit du stockage objet

Les messages d'audit appartenant à la catégorie d'audit du stockage objet sont utilisés pour les événements liés au stockage et à la gestion d'objets au sein du système StorageGRID. Il s'agit notamment du stockage objet et des récupérations, des transferts entre nœuds grid et nœuds.



Les codes d'audit sont supprimés du produit et de la documentation, car les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour connaître les versions antérieures de SG. Par exemple ["Messages d'audit du stockage objet StorageGRID 11.8"](#), .

Code	Description	Voir
BROR	Demande de lecture seule du compartiment : un compartiment est entré ou a quitté le mode lecture seule.	"BROR : demande en lecture seule du compartiment"

Code	Description	Voir
CBSE	Objet Envoyer fin : l'entité source a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBSE : fin de l'envoi de l'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBRE : fin de la réception de l'objet"
CGRR	Demande de réplication multigrille : StorageGRID a tenté une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille.	"CGRR : demande de réplication croisée"
EBDL	Suppression d'un compartiment vide : l'analyse ILM a supprimé un objet d'un compartiment qui supprime tous les objets (opération de compartiment vide).	"EBDL : suppression du compartiment vide"
EBKR	Demande de compartiment vide : un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter la suppression d'objets).	"EBKR : demande de godet vide"
BALAYAGE	Validation d'un magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié, et peut désormais être demandé.	"SCMT : demande de validation de magasin d'objets"
SREM	Suppression du magasin d'objets : un bloc de contenu a été supprimé d'un nœud de grille et ne peut plus être demandé directement.	"SREM : Suppression du magasin d'objets"

Messages d'audit de lecture du client

Les messages d'audit de lecture du client sont consignés lorsqu'une application client S3 demande la récupération d'un objet.

Code	Description	Utilisé par	Voir
S3SL	Demande S3 Select : enregistre une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.	Client S3	"S3SL: Demande S3 Select"

Code	Description	Utilisé par	Voir
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	Client S3	"SHEA : TÊTE S3"

Écrire des messages d'audit client

Les messages d'audit d'écriture du client sont consignés lorsqu'une application client S3 demande de créer ou de modifier un objet.

Code	Description	Utilisé par	Voir
OVWR	Remplacement d'objet : consigne une transaction afin de remplacer un objet par un autre.	Client S3	"OVWR : remplacement d'objet"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPR	POST S3 : consigne une transaction réussie pour restaurer un objet à partir du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPO : BORNE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : PUT S3"
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment.	Client S3	"SUPD : métadonnées S3 mises à jour"

Message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion.

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

Messages d'audit ILM

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 des informations (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée de l'ILM : ce message d'audit est généré lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
LKCU	Nettoyage d'objet écrasé. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : nettoyage d'objet écrasé"
ORLM	Règles objet respectées : ce message d'audit est généré lorsque les données objet sont stockées comme spécifié par les règles ILM.	"ORLM : règles d'objet respectées"

Référence du message d'audit

BROR : demande en lecture seule du compartiment

Le service LDR génère ce message d'audit lorsqu'un compartiment passe en mode lecture seule ou quitte ce mode. Par exemple, un compartiment passe en mode lecture seule tandis que tous les objets sont en cours de suppression.

Code	Champ	Description
BKHD	UUID de compartiment	ID du compartiment.
BROV	Valeur de demande de lecture seule du compartiment	Que le compartiment soit en lecture seule ou qu'il quitte l'état en lecture seule (1 = lecture seule, 0 = non-lecture seule).
BROS	Motif de compartiment en lecture seule	Raison pour laquelle le compartiment est en lecture seule ou quitte l'état en lecture seule. Par exemple, emptyBucket.
S3AI	ID de compte locataire S3	ID du compte de locataire qui a envoyé la demande. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3BK	Compartiment S3	Nom du compartiment S3.

CBRB : début de la réception de l'objet

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour

vérifier le nombre de répliques.

CBRE : fin de la réception de l'objet

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	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

CBSB : début de l'envoi de l'objet

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour

suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

CBSE : fin de l'envoi de l'objet

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	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	<p>Résultat de l'opération de transfert (du point de vue de l'entité émettrice) :</p> <p>SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés.</p> <p>CONL : connexion perdue pendant le transfert</p> <p>CTMO : expiration de la connexion pendant l'établissement ou le transfert</p> <p>UNRE : ID de nœud de destination inaccessible</p> <p>CRPT : transfert terminé en raison de la réception de données corrompues ou non valides</p>

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

CGRR : demande de réplication croisée

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

Code	Champ	Description
CSIZ	Taille de l'objet	<p>Taille de l'objet en octets.</p> <p>L'attribut CSIZ a été introduit dans StorageGRID 11.8. Par conséquent, les requêtes de réplication multigrille couvrant une mise à niveau StorageGRID 11.7 à 11.8 peuvent avoir une taille d'objet totale inexacte.</p>
S3AI	ID de compte locataire S3	ID du compte de locataire qui détient le compartiment à partir duquel l'objet est répliqué.
GFID	ID de connexion de fédération de grille	ID de la connexion de fédération de grille utilisée pour la réplication inter-grille.

Code	Champ	Description
OPER	Opération CGR	Type d'opération de réplication inter-grille qui a été tentée : <ul style="list-style-type: none"> • 0 = objet répliqué • 1 = objet multi pièce répliqué • 2 = marqueur de suppression répliqué
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.
VSID	ID de version	ID de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie réussi (SUCS) ou erreur générale (GERR).

EBDL : suppression du compartiment vide

Le scanner ILM a supprimé un objet d'un compartiment qui supprime tous les objets (en cours d'exécution d'une opération de compartiment vide).

Code	Champ	Description
CSIZ	Taille de l'objet	Taille de l'objet en octets.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
RSLT	Résultat de l'opération de suppression	Résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

EBKR : demande de godet vide

Ce message indique qu'un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter de supprimer des objets).

Code	Champ	Description
BUID	UUID de compartiment	ID du compartiment.
EBJS	Configuration JSON de compartiment vide	Contient le fichier JSON représentant la configuration de compartiment vide actuelle.
S3AI	ID de compte locataire S3	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

ECMC : fragment de données avec code d'effacement manquant

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

Code	Champ	Description
VCMC	ID VCS	Nom du VCS contenant le bloc manquant.
CODE DE DIAGNOSTIC	ID de bloc	Identifiant du fragment avec code d'effacement manquant.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

ECOC : fragment de données avec code d'effacement corrompu

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

Code	Champ	Description
VCCO	ID VCS	Nom du VCS contenant le bloc corrompu.
VLID	ID du volume	Volume RangeDB contenant le fragment codé d'effacement corrompu.
CCID	ID de bloc	Identificateur du fragment codé d'effacement corrompu.

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. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

ETAF : échec de l'authentification de sécurité

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

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Identifiant dépendant du service représentant l'identité de l'utilisateur distant.
RSLT	Code de motif	<p>La raison de l'échec :</p> <p>SCNI : échec de l'établissement de connexion sécurisée.</p> <p>CERM : certificat manquant.</p> <p>CERT : le certificat n'était pas valide.</p> <p>CERE: Le certificat a expiré.</p> <p>CERR : le certificat a été révoqué.</p> <p>CSGN : la signature du certificat n'est pas valide.</p> <p>CSGU : le signataire de certificat était inconnu.</p> <p>UCRM : les informations d'identification de l'utilisateur étaient manquantes.</p> <p>UCRI : les informations d'identification de l'utilisateur étaient incorrectes.</p> <p>UCRU : les informations d'identification de l'utilisateur ont été interdites.</p> <p>TOUT : expiration du délai d'authentification.</p>

Lorsqu'une connexion est établie à un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et de la logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou interdits, un message d'audit est consigné. Cela permet de rechercher des tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut être dû à une entité distante ayant une configuration incorrecte ou à des tentatives de

présentation d'informations d'identification non valides ou interdites au système. Ce message d'audit doit être surveillé pour détecter les tentatives d'accès non autorisé au système.

GNRG : enregistrement GNDS

Le service CMN génère ce message d'audit lorsqu'un service a mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : <ul style="list-style-type: none">• CMC : réussi• SUNV : service non disponible• GERR : autre panne
GNID	ID du nœud	ID de nœud du service qui a lancé la demande de mise à jour.
GNTTP	Type de périphérique	Type de périphérique du nœud de grid (par exemple BLDR pour un service LDR).
GNDV	Version du modèle de périphérique	Chaîne identifiant la version du modèle de terminal du nœud de grille dans le bundle DMDL.
GNP	Groupe	Groupe auquel appartient le nœud de la grille (dans le contexte des coûts de lien et du classement des requêtes de service).
GNIA	Adresse IP	Adresse IP du nœud de la grille.

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

GNUR : non-inscription du GNDS

Le service CMN génère ce message d'audit lorsqu'un service a des informations non enregistrées sur lui-même à partir du système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : <ul style="list-style-type: none">• CMC : réussi• SUNV : service non disponible• GERR : autre panne
GNID	ID du nœud	ID de nœud du service qui a lancé la demande de mise à jour.

GTED : tâche de grille terminée

Ce message d'audit indique que le service CMN a terminé le traitement de la tâche de grille spécifiée et a déplacé la tâche vers la table Historique. Si le résultat est SUC, ABRT ou ROLF, un message d'audit correspondant à la tâche de grille démarrée sera affiché. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais démarré.

Code	Champ	Description
2	ID de tâche	<p>Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche de grille tout au long de son cycle de vie.</p> <p>Remarque : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.</p>
RSLT	Résultat	<p>Résultat de l'état final de la tâche de grille :</p> <ul style="list-style-type: none">• SUC : la tâche de grille s'est terminée avec succès.• ABRT : la tâche de grille a été interrompue sans erreur de retour arrière.• ROLF : la tâche de grille a été interrompue et n'a pas pu terminer le processus de restauration.• ANNUL : la tâche de grille a été annulée par l'utilisateur avant son démarrage.• EXPR : la tâche de grille a expiré avant son démarrage.• IVLD : la tâche de grille n'était pas valide.• AUTH : la tâche de grille n'était pas autorisée.• DUPL : la tâche de grille a été rejetée en double.

GTST : tâche de grille démarrée

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 de la tâche de grille soumise pour les tâches de grille initiées par le service interne Grid Task Submission et sélectionnées pour l'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
2	ID de tâche	<p>Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie.</p> <p>Remarque : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.</p>
RSLT	Résultat	<p>Résultat. Ce champ n'a qu'une seule valeur :</p> <ul style="list-style-type: none"> • SUC : la tâche de grille a été démarrée avec succès.

GTSU : tâche de grille soumise

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

Code	Champ	Description
2	ID de tâche	<p>Identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie.</p> <p>Remarque : l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.</p>
TTYP	Type de tâche	Type de tâche de grille.
VER	Version de la tâche	Numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Description lisible par l'homme de la tâche de grille.
CUVES	Valide après horodatage	La première fois (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant horodatage	Dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.

Code	Champ	Description
TSRC	Source	Source de la tâche : <ul style="list-style-type: none"> • TXTB : la tâche de grille a été soumise via le système StorageGRID sous forme de bloc de texte signé. • GRILLE : la tâche de grille a été soumise via le service de soumission de tâches Grid interne.
ACTV	Type d'activation	Type d'activation : <ul style="list-style-type: none"> • AUTO : la tâche de grille a été soumise pour l'activation automatique. • PEND : la tâche de grille a été envoyée dans la table en attente. C'est la seule possibilité pour la source TXTB.
RSLT	Résultat	Résultat de la soumission : <ul style="list-style-type: none"> • SUC : la tâche de grille a été envoyée avec succès. • ECHEC : la tâche a été déplacée directement vers la table historique.

IDEL : suppression initiée ILM

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

Le message IDEL est généré dans l'une ou l'autre des situations suivantes :

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

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CMPA	Conformité : suppression automatique	Pour les objets des compartiments S3 uniquement. 0 (false) ou 1 (true), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le compartiment ne soit soumis à une conservation légale.
CMPL	Conformité : obligation légale	Pour les objets des compartiments S3 uniquement. 0 (faux) ou 1 (vrai), indiquant si le godet est actuellement en attente légale.

Code	Champ	Description
CMPR	Conformité : période de conservation	Pour les objets des compartiments S3 uniquement. Durée de conservation de l'objet en minutes.
CTME	Conformité : temps d'entrée	Pour les objets des compartiments S3 uniquement. Temps d'ingestion de l'objet. Vous pouvez ajouter la période de conservation en minutes à cette valeur pour déterminer quand l'objet peut être supprimé du compartiment.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet en octets.
EMPLACEMENT S	Emplacements	<p>L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMPLACEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé).</p> <p>CLEC : pour les objets avec code d'effacement, l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement appliqués aux données de l'objet.</p> <p>CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet.</p> <p>CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.</p>
CHEMIN	Compartiment/cl é S3	Nom du compartiment S3 et nom de la clé S3.
RSLT	Résultat	<p>Résultat de l'opération ILM.</p> <p>SUC : l'opération ILM a réussi.</p>
RÈGLE	Libellé de règles	<ul style="list-style-type: none"> • Si un objet d'un compartiment S3 conforme est supprimé automatiquement car sa période de conservation a expiré, ce champ est vide. • Si l'objet est supprimé car il n'y a 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 appliquée à l'objet.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Code	Champ	Description
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

LKCU : nettoyage d'objet écrasé

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui auparavant requiert un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 écrit un objet dans un chemin qui contient déjà un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet en octets.
LTYP	Type de nettoyage	<i>Usage interne uniquement.</i>
LUID	UUID d'objet supprimé	Identifiant de l'objet qui a été supprimé.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet qui existe toujours. Cette valeur est disponible uniquement si l'objet n'a pas été supprimé.

LKDM : nettoyage d'objets fuyée

Ce message est généré lorsqu'un morceau qui fuit a été nettoyé ou supprimé. Un bloc peut faire partie d'un objet répliqué ou d'un objet avec code d'effacement.

Code	Champ	Description
CLOC	Emplacement des blocs	Le chemin du fichier du morceau qui a fui et qui a été supprimé.
CTYP	Type de bloc	Type de bloc : ec: Erasure-coded object chunk repl: Replicated object chunk

Code	Champ	Description
LTyp	Type de fuite	<p>Les cinq types de fuites pouvant être détectés :</p> <p><code>object_leaked</code>: Object doesn't exist in the grid</p> <p><code>location_leaked</code>: Object exists in the grid, but found location doesn't belong to object</p> <p><code>mup_seg_leaked</code>: Multipart upload was stopped or not completed, and the segment/part was left out</p> <p><code>segment_leaked</code>: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment</p> <p><code>no_parent</code>: Container object is deleted, but object segment was left out and not deleted</p>
CTIM	Temps de création des blocs	Heure à laquelle le morceau de fuite a été créé.
UUID	Identifiant unique universel	Identifiant de l'objet auquel appartient le bloc.
CBID	Identificateur du bloc de contenu	CBID de l'objet auquel appartient le segment divulgué.
CSIZ	Taille du contenu	Taille du bloc en octets.

LLST : emplacement perdu

Ce message est généré chaque fois qu'un emplacement pour une copie d'objet (répliquée ou avec code d'effacement) est introuvable.

Code	Champ	Description
BIL	CBID	CBID affecté.
ECPR	Profil de codage d'effacement	Pour les données d'objet avec code d'effacement. ID du profil de code d'effacement utilisé.
LTyp	Type d'emplacement	<p>CLDI (Online) : pour les données d'objet répliquées</p> <p>CLEC (en ligne) : pour les données d'objet avec code d'effacement</p> <p>CLNL (Nearline) : pour les données d'objets répliqués archivés</p>

Code	Champ	Description
NON	ID de nœud source	ID de nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin d'accès à l'objet répliqué	Chemin complet vers l'emplacement du disque des données de l'objet perdu. Renvoyé uniquement lorsque LTYP a une valeur CLDI (c'est-à-dire pour les objets répliqués). Prend le formulaire <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Résultat	Toujours AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
TSRC	Déclenchement de la source	UTILISATEUR : utilisateur déclenché SYST : déclenchement du système
UUID	ID universel unique	Identifiant de l'objet affecté dans le système StorageGRID.

MG AU : message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion. Chaque requête HTTP qui n'est pas une requête GET ou HEAD à un URI d'API valide consigne une réponse contenant le nom d'utilisateur, l'adresse IP et le type de requête à l'API. Les URI d'API non valides (tels que /api/v3-Authorise) et les demandes non valides d'URI d'API valides ne sont pas consignés.

Code	Champ	Description
MDIP	Adresse IP de destination	Adresse IP du serveur (destination).
ADNM	Nom de domaine	Nom du domaine hôte.
MPAT	CHEMIN de la demande	Le chemin de la demande.
MPQP	Paramètres de requête	Paramètres de requête pour la demande.

Code	Champ	Description
MBD	Corps de la demande	<p>Le contenu de l'organisme de demande. Lorsque le corps de réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de réponse est vide. Comme les informations suivantes ne sont pas disponibles dans le corps de réponse, elles sont extraites du corps de la demande pour les méthodes SUIVANTES :</p> <ul style="list-style-type: none"> • Nom d'utilisateur et ID de compte dans POST Authorise • Nouvelle configuration de sous-réseaux dans POST /grid/grid-Networks/update • Nouveaux serveurs NTP dans POST /grid/ntp-servers/update • ID de serveur déclassés dans POST /grid/serveurs/désaffecter <p>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).</p>
MMD	Méthode de demande	<p>La méthode de requête HTTP :</p> <ul style="list-style-type: none"> • POST • EN • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de réponse	<p>Le contenu de la réponse (le corps de réponse) est consigné par défaut.</p> <p>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).</p>
MSIP	Adresse IP source	Adresse IP du client (source).
UUUN	URN utilisateur	URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.

OLST : le système a détecté un objet perdu

Ce message est généré lorsque le service DDS ne trouve aucune copie d'un objet dans le système StorageGRID.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet perdu.
NON	ID du nœud	S'il est disponible, dernier emplacement direct ou proche de la ligne connue de l'objet perdu. Il est possible d'avoir uniquement l'ID de nœud sans ID de volume si les informations sur le volume ne sont pas disponibles.
CHEMIN	Compartiment/clé S3	S'il est disponible, le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
UUID	ID universel unique	Identificateur de l'objet perdu dans le système StorageGRID.
VOLI	ID du volume	S'il est disponible, l'ID de volume du nœud de stockage pour le dernier emplacement connu de l'objet perdu.

ORLM : règles d'objet respectées

Ce message est généré lorsque l'objet est stocké et copié comme spécifié par les règles ILM.



Le message ORLM n'est pas généré lorsqu'un objet est stocké avec succès par la règle de création de 2 copies par défaut si une autre règle de la stratégie utilise le filtre avancé taille d'objet.

Code	Champ	Description
BUID	Cueilleur de godet	Champ ID de compartiment. Utilisé pour les opérations internes. S'affiche uniquement si STAT est PRGD.
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CSIZ	Taille du contenu	Taille de l'objet en octets.

Code	Champ	Description
EMPLACEMENT S	Emplacements	<p>L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMBLEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé).</p> <p>CLEC : pour les objets avec code d'effacement, l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement appliqués aux données de l'objet.</p> <p>CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet.</p> <p>CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.</p>
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
RSLT	Résultat	<p>Résultat de l'opération ILM.</p> <p>SUC : l'opération ILM a réussi.</p>
RÈGLE	Libellé de règles	Étiquette lisible par l'homme donnée à la règle ILM appliquée à cet objet.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	CBID du conteneur	CBID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que pour les objets segmentés et partitionnés.
URGENCE	État	<p>État de l'opération ILM.</p> <p>L'OPÉRATION ILM est terminée pour l'objet.</p> <p>DFER: L'objet a été marqué pour une future réévaluation ILM.</p> <p>PRGD : l'objet a été supprimé du système StorageGRID.</p> <p>NLOC : les données d'objet ne sont plus disponibles dans le système StorageGRID. Cet état peut indiquer que toutes les copies des données d'objet sont manquantes ou endommagées.</p>
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. 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 seul objet. Par exemple, il est émis chaque fois que l'un des événements suivants se produit :

- Les règles ILM de l'objet sont satisfaites à jamais.
- 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'objet répliqué est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

Informations associées

- ["Transactions d'ingestion d'objets"](#)
- ["Transactions de suppression d'objet"](#)

OVWR : remplacement d'objet

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

Code	Champ	Description
CBID	Identifiant de bloc de contenu (nouveau)	CBID du nouvel objet.
CSIZ	Taille d'objet précédente	Taille, en octets, de l'objet à remplacer.
OCBD	Identifiant de bloc de contenu (précédent)	CBID de l'objet précédent.
UUID	ID universel unique (nouveau)	Identifiant du nouvel objet dans le système StorageGRID.
OUID	ID universel unique (précédent)	Identifiant de l'objet précédent dans le système StorageGRID.
CHEMIN	Chemin d'objet S3	Chemin d'accès à l'objet S3 utilisé pour l'objet précédent et le nouvel objet
RSLT	Code de résultat	Résultat de la transaction de remplacement d'objet. Le résultat est toujours : CMC : réussi

Code	Champ	Description
SGRP	Site (groupe)	S'il est présent, l'objet écrasé a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet écrasé a été ingéré.

S3SL: Demande S3 Select

Ce message consigne une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.

Code	Champ	Description
BYSC	Octets analysés	Nombre d'octets analysés (reçus) à partir des nœuds de stockage. BYSC et BYPR sont susceptibles d'être différents si l'objet est compressé. Si l'objet est compressé, BYSC aura le nombre d'octets compressés et BYPR les octets après décompression.
MODÈLE BYPR	Octets traités	Nombre d'octets traités. Indique le nombre d'octets analysés ou traités par un travail S3 Select.
MODÈLE BYRT	Octets renvoyés	Nombre d'octets renvoyés par une tâche S3 Select au client.
RÉFÉRENTIEL	Enregistrements traités	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a reçus des nœuds de stockage.
REIU	Documents renvoyés	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a renvoyé au client.
JOFI	Travail terminé	Indique si le traitement du travail S3 Select est terminé ou non. Si cette valeur est faux, le travail n'a pas pu se terminer et les champs d'erreur contiennent probablement des données. Le client a peut-être reçu des résultats partiels ou aucun résultat.
REID	ID de la demande	Identifiant de la demande S3 Select.
EXTM	Heure d'exécution	Temps, en secondes, nécessaire à la réalisation de S3 Select Job.
GROUPE DE GESTION	Message d'erreur	Message d'erreur généré par le travail S3 Select.
QTÉ	Type d'erreur	Type d'erreur généré par le travail S3 Select.
ERST	Erreur Stacktrace	Erreur Stacktrace générée par le travail S3 Select.

Code	Champ	Description
S3BK	Compartiment S3	Nom du compartiment S3.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 pour l'utilisateur qui a envoyé la demande.
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.

SADD : désactivation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a désactivé la journalisation des messages d'audit ; les messages d'audit ne sont plus collectés ou livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la journalisation était déjà activée, mais qu'elle a été désactivée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré (SADE) et la capacité de désactivation de l'audit est ensuite bloquée de manière permanente.

SADE : activation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a restauré la journalisation des messages d'audit ; les messages d'audit sont de nouveau collectés et livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour activer l'audit.

Code	Champ	Description
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la consignation a été précédemment désactivée (SADD), mais qu'elle a maintenant été restaurée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré et la fonctionnalité de désactivation de l'audit est bloquée définitivement.

SCMT : validation du magasin d'objets

Le contenu de la grille n'est pas disponible ou reconnu comme stocké tant qu'il n'a pas été engagé (c'est-à-dire qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a transmis des contrôles d'intégrité liés. Ce message est émis lorsqu'un bloc de contenu est attribué au stockage.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu engagé dans le stockage permanent.
RSLT	Code de résultat	Statut au moment où l'objet était stocké sur le disque : SUCS : objet enregistré avec succès.

Ce message signifie qu'un bloc de contenu donné a été complètement stocké et vérifié, et qu'il peut maintenant être demandé. Il peut être utilisé pour suivre le flux de données dans le système.

SDEL : SUPPRESSION S3

Lorsqu'un client S3 émet une transaction DE SUPPRESSION, une demande de suppression de l'objet ou du compartiment spécifié ou de suppression d'une sous-ressource de compartiment/objet est formulée. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du 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	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les compartiments n'incluent pas ce champ.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande de suppression de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande de suppression de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div> <p>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</p> <p>x-amz-bypass-governance-retention est automatiquement inclus s'il est présent dans la demande.</p> </div>
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RLST	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UDM	Identificateur unique universel pour un marqueur de suppression	Identifiant d'un marqueur de suppression. Les messages du journal d'audit indiquent UUDM ou UUID : 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	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SGET : OBTENEZ S3

Lorsqu'un client S3 émet une transaction GET, une demande est formulée pour extraire un objet ou répertorier les objets dans un compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du 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	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div> <p><code>`X-Forwarded-For`</code> Est automatiquement inclus s'il est présent dans la demande et si la <code>`X-Forwarded-For`</code> valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</p> </div>

Code	Champ	Description
NULLITÉ	ListObjectsV2	Une réponse <i>v2 format</i> a été demandée. Pour plus de détails, voir " AWS ListObjectsV2 ". Uniquement pour les opérations GET bucket.
NHD	Nombre d'enfants	Inclut des clés et des préfixes courants. Uniquement pour les opérations GET bucket.
AU RANG	Plage lue	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette demande. La valeur après la barre oblique (/) indique la taille de l'objet entier.
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
TRNC	Tronqué ou non tronqué	Définissez sur FALSE si tous les résultats ont été renvoyés. Réglez sur vrai si d'autres résultats sont disponibles pour revenir. Uniquement pour les opérations GET bucket.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SHEA : TÊTE S3

Lorsqu'un client S3 émet une opération HEAD, une demande est effectuée pour vérifier l'existence d'un objet ou d'un bucket et récupérer les métadonnées relatives à un objet. Ce message est émis par le serveur si l'opération réussit.

Code	Champ	Description
CBID	Identificateur du 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	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet vérifié en octets. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div> <p>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</p> </div>
RSLT	Code de résultat	<p>Résultat de la transaction GET. Le résultat est toujours :</p> <p>CMC : réussi</p>
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SPO : BORNE S3

Lorsqu'un client S3 émet une requête POST-objet, ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du 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	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets.

Code	Champ	Description
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div> <p>`X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</p> </div> <p>(Non prévu pour SPOS).</p>
RSLT	Code de résultat	<p>Résultat de la demande RestoreObject. Le résultat est toujours :</p> <p>CMC : réussi</p>
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	<p>Le godet ou la sous-ressource d'objet utilisé, le cas échéant.</p> <p>Réglez sur « SELECT » pour une opération S3 Select.</p>
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	Informations sur la restauration.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SPUT : PUT S3

Lorsqu'un client S3 émet une transaction PUT, une demande est formulée pour créer un nouvel objet ou un nouveau compartiment, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du 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 demande (tronqués aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande PUT de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande PUT de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	<p>Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration.</p> <div> <p><code>`X-Forwarded-For`</code> Est automatiquement inclus s'il est présent dans la demande et si la <code>`X-Forwarded-For`</code> valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</p> </div> <p><code>x-amz-bypass-governance-retention</code> est automatiquement inclus s'il est présent dans la demande.</p>
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête <code>`x-amz-bucket-object-lock-enabled`</code> de la demande , s'il est présent dans la demande.
LKLH	Verrouillage de l'objet en attente légale	Valeur de l'en-tête de requête <code>x-amz-object-lock-legal-hold</code> , s'il est présent dans la demande PutObject.

Code	Champ	Description
LKMD	Mode de conservation du verrouillage d'objet	Valeur de l'en-tête de requête <code>x-amz-object-lock-mode</code> , s'il est présent dans la demande PutObject.
LKRU	Conservation de l'objet jusqu'à la date	Valeur de l'en-tête de requête <code>x-amz-object-lock-retain-until-date</code> , s'il est présent dans la demande PutObject. Les valeurs sont limitées à 100 ans après la date d'ingestion de l'objet.
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
ID ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations CompleteMultipartUpload. Indique que toutes les pièces ont été téléchargées et assemblées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.
VSST	Etat de gestion des versions	Nouvel état de gestion des versions d'un compartiment. Deux États sont utilisés : « activé » ou « suspendu ». Les opérations sur les objets n'incluent pas ce champ.

SREM : Suppression du magasin d'objets

Ce message est émis lorsque le contenu est supprimé du stockage persistant et n'est plus accessible via des API régulières.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu supprimé du stockage permanent.
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 signifie qu'un bloc de contenu donné a été supprimé d'un nœud et ne peut plus être demandé directement. Le message peut être utilisé pour suivre le flux de contenu supprimé dans le système.

SUPD : métadonnées S3 mises à jour

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

Code	Champ	Description
CBID	Identificateur du 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	Valeur de l'en-tête de requête HTTP de contrôle de cohérence, s'il est présent dans la demande, lors de la mise à jour des paramètres de conformité d'un compartiment.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. <div> `X-Forwarded-For` Est automatiquement inclus s'il est présent dans la demande et si la `X-Forwarded-For` valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). </div>
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi

Code	Champ	Description
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Heure	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID 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.

SVRF : échec de la vérification du magasin d'objets

Ce message est émis chaque fois qu'un bloc de contenu échoue au processus de vérification. Chaque fois que les données d'objet répliqué sont lues ou écrites sur le disque, plusieurs vérifications et vérifications d'intégrité sont effectuées pour s'assurer que les données envoyées à l'utilisateur requérant sont identiques aux données initialement ingérées sur le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données d'objet répliqué corrompues pour les empêcher d'être récupérées à nouveau.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu qui a échoué à la vérification.
RSLT	Code de résultat	Type d'échec de vérification : CRCF : échec du contrôle de redondance cyclique (CRC). HMAC : échec de la vérification du code d'authentification du message basé sur le hachage (HMAC). EHSR : hachage de contenu crypté inattendu. PHSR : hachage de contenu original inattendu. SEQC : séquence de données incorrecte sur le disque. PERR : structure non valide du fichier de disque. DERR : erreur disque. FNAM : nom de fichier incorrect.



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

Pour déterminer quelle opération a déclenché le message, reportez-vous à la valeur du champ 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 du contenu.

SVRU : Vérification du magasin d'objets inconnue

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

Code	Champ	Description
FPTH	Chemin du fichier	Chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.



Le message d'audit SVRU: Object Store Verify Unknown doit être suivi de près. Cela signifie que des copies inattendues de données objet ont été détectées dans le magasin d'objets. Cette situation doit être examinée immédiatement pour déterminer comment ces copies ont été créées, car elle peut indiquer des défaillances matérielles imminentes.

SYSD : arrêt du nœud

Lorsqu'un service est arrêté avec élégance, ce message est généré pour indiquer que l'arrêt a été demandé. Généralement, ce message est envoyé uniquement après un redémarrage ultérieur, car la file d'attente des messages d'audit n'est pas effacée avant l'arrêt. Recherchez le message SYST, envoyé au début de la séquence d'arrêt, si le service n'a pas redémarré.

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

SYST : arrêt du nœud

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

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

SYSU : démarrage du nœud

Lors du redémarrage d'un service, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système a été arrêté proprement. DSDN : le système n'a pas été arrêté complètement. VRGN : le système a été démarré pour la première fois après l'installation du serveur (ou la réinstallation).

Le message n'indique pas si le serveur hôte a été démarré, seul le service de génération de rapports. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant le fonctionnement (étant donné que la nature distribuée du système StorageGRID peut masquer ces défaillances). Server Manager redémarre automatiquement un service en panne.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.