



Formats du fichier journal d'audit et des messages

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

- Formats du fichier journal d’audit et des messages..... 1
 - Format du fichier journal d’audit..... 1
 - Format du message d’audit 14

Formats du fichier journal d'audit et des messages

Les journaux d'audit permettent de collecter les informations sur votre système et de résoudre les problèmes. Vous devez comprendre le format du fichier journal d'audit et le format général utilisé pour les messages 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][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):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 `audit-explain` outil pour obtenir des résumés simplifiés des messages d'audit dans le journal d'audit. Vous pouvez utiliser le `audit-sum` outil pour résumer le nombre d'opérations d'écriture, de lecture et de suppression enregistrées, ainsi que la durée nécessaire à ces opérations.

Informations associées

["Utilisation de l'outil d'explication d'audit"](#)

Utilisation de l'outil d'explication d'audit

Vous pouvez utiliser le `audit-explain` outil permettant de traduire les messages d'audit du journal d'audit dans un format facile à lire.

Ce dont vous avez besoin

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

Description de la tâche

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



Le `audit-explain` l'outil est principalement destiné au support technique lors des opérations de dépannage. En cours de traitement `audit-explain` Les requêtes peuvent consommer une très grande quantité d'énergie dans le processeur, ce qui peut affecter les opérations de StorageGRID.

Cet exemple montre une sortie type de l' `audit-explain` outil. Ces quatre messages d'audit SPUT ont été générés lorsque le locataire S3 avec l'ID de compte 92484777680322627870 a UTILISÉ les demandes S3 POUR créer un compartiment nommé « bucket1 » et ajouter trois objets dans 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
```

Le `audit-explain` l'outil peut traiter des journaux d'audit simples ou compressés. Par exemple :

```
audit-explain audit.log
```

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

Le `audit-explain` l'outil peut également traiter plusieurs fichiers en même temps. Par exemple :

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

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

Enfin, le `audit-explain` l'outil peut accepter les entrées d'un tuyau, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide de l' `grep` commande ou autre moyen. Par exemple :

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

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

Puisque les journaux d'audit peuvent être très volumineux et lents à analyser, vous pouvez gagner du temps en filtrant les pièces que vous voulez regarder et exécuter `audit-explain` sur les pièces, au lieu du fichier entier.



Le `audit-explain` l'outil n'accepte pas les fichiers compressés comme entrée de canalisation. Pour traiter des fichiers compressés, indiquez leurs noms de fichier comme arguments de ligne de commande ou utilisez le `zcat` outil de décompression des fichiers en premier. Par exemple :

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

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

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

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

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

Le `audit-explain` l'outil imprime les interprétations lisibles par l'homme de tous les messages du ou des fichiers spécifiés.



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

Informations associées

"SPUT : PUT S3"

À l'aide de l'outil audit-sum


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

Ce dont vous avez besoin

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

Description de la tâche

Le `audit-sum` Disponible sur le nœud d'administration principal, cet outil récapitule le nombre d'opérations d'écriture, de lecture et de suppression enregistrées et la durée de ces opérations.



Le `audit-sum` l'outil est principalement destiné au support technique lors des opérations de dépannage. En cours de traitement `audit-sum` Les requêtes peuvent consommer une très grande quantité d'énergie dans le processeur, ce qui peut affecter les opérations de StorageGRID.

Cet exemple montre une sortie type 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` Dans un journal d'audit, l'outil indique le nombre et la durée des messages d'audit S3, Swift et ILM suivants :

| Code | Description | Reportez-vous à la section |
|------|-----------------------------------|--|
| ARCT | Archivage depuis le Tier cloud | "ARCT : récupération d'archives depuis Cloud-Tier" |
| ASCT | Tier cloud du magasin d'archivage | "ASCT : magasin d'archives, niveau du cloud" |

| 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" |
| WDEL | SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur. | "WDEL : SUPPRESSION rapide" |
| C'EST PARTI | SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur. | "WGET: SWIFT GET" |
| WHEA | SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur. | "WHEA: TÊTE SWIFT" |
| WPUT | SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur. | "WPUT : PUT SWIFT" |

Le `audit-sum` l'outil peut traiter des journaux d'audit simples ou compressés. Par exemple :

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

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

Le `audit-sum` l'outil peut également traiter plusieurs fichiers en même temps. Par exemple :


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

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

Enfin, le `audit-sum` l'outil peut également accepter l'entrée d'un tuyau, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide de l' `grep` commande ou autre moyen. 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 de pipettes. Pour traiter des fichiers compressés, indiquez leurs noms de fichier comme arguments de ligne de commande ou utilisez le `zcat` outil de décompression des 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 indiquent le temps de fonctionnement minimum, maximum et moyen, mais vous pouvez utiliser le `size` (`-s`) option pour regarder la taille de l'objet.

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

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

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
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 à analyser :

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

Cet exemple montre une sortie type de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

| message group average (sec) | count | min (sec) | max (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'accès aux objets : `grep SGET audit.log | audit-sum -l`

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet 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/r9010aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r9010aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r9010aQ8JB-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. Pour déterminer la taille des objets en cours d'ingestion et d'extraction à partir de votre grille, utilisez l'option size (-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 sur le journal d'audit approprié et utilisez l'option group-by-time (-gt), suivi 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 S3 GÉNÈRE un trafic entre 06:00 et 07:00. Les temps maximum et moyen sont à la fois considérablement plus élevés à ces moments aussi, et ils n'ont pas augmenté progressivement à mesure que le comptage a augmenté. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou que la grille peut traiter les demandes.

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

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

| message group 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 `audit-explain` Outil pour passer en revue toutes les opérations du SGET au cours de cette heure :

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

Si la sortie de la commande `grep` est censée être de nombreuses lignes, ajoutez le `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 le `-go` option, qui regroupe les messages pour les opérations liées aux objets et aux compartiments 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 godets dont les opérations SPUT sont les plus lentes, utiliser le `-gb` option, 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 plus grande taille d'objet SPUT, utilisez les deux `-gb` et le `-s` options :

```
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.ldt002 0.352 | 1564563 | 0.000 | 999.972 |

Informations associées

["Utilisation de l'outil d'explication 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 le résumé fourni par le `audit-explain` et `audit-sum` les outils sont insuffisants, reportez-vous à cette section pour comprendre le format général de tous les messages de vérification.

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(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. L'ensemble de la chaîne est entre crochets ([]), et chaque élément d'attribut de la chaîne possède les caractéristiques suivantes :

- Entre crochets []
- 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 flux 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 en cours de signalement. 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 de texte. Les valeurs suivent toujours deux-points (:). Les valeurs du type de données CSTR sont entourées de guillemets doubles " ".

Informations associées

["Utilisation de l'outil d'explication d'audit"](#)

["À l'aide de l'outil audit-sum"](#)

["Messages d'audit"](#)

["Éléments communs dans les messages d'audit"](#)

["Types de données"](#)

["Exemples de messages d'audit"](#)

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 sous la forme de quatre caractères ASCII tels que « ABCD ». |
| IPAD | Utilisé pour les adresses IP. |

| Type | Description |
|------|---|
| REST | <p>Un tableau de caractères UTF-8 à longueur variable. Les caractères peuvent être échappé avec les conventions suivantes :</p> <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 l'ouverture [AUDT: conteneur 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 :

```
2018-12-05T08:24:45.921845 [AUDT:[RSLT(FC32):SUCS]
[TIME(UI64):11454] [SAIP(IPAD):"10.224.0.100"]
[S3AI(CSTR):"60025621595611246499"] [SACC(CSTR):"account"]
[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk_E6dYzKlumRsKJA=="]
[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]
[SBAI(CSTR):"60025621595611246499"] [SBAC(CSTR):"account"] [S3BK(CSTR):"bucket"]
[S3KY(CSTR):"object"] [CBID(UI64):0xCC128B9B9E428347]
[UUID(CSTR):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"] [CSIZ(UI64):30720]
[AVER(UI32):10] [ATIM(UI64):1543998285921845] [ATYP(FC32):SHEA]
[ANID(UI32):12281045] [AMID(FC32):S3RQ] [ATID(UI64):15552417629170647261]]
```

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

Informations associées

["Éléments communs dans les messages d'audit"](#)

["Messages d'audit"](#)

Éléments communs dans les messages d'audit

Tous les messages d'audit contiennent les éléments communs.

| Code | Type | Description |
|-----------|------|---|
| AU MILIEU | FC32 | ID du module : identifiant à quatre caractères de l'ID du 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. |
| 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. Temps lisible par l'homme 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 sous la forme <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, où 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 d'enregistrement. 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. |

| Code | Type | Description |
|------|------|--|
| 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 le `audit.log` 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, dans laquelle il consigne l'entrée 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 Traduit au jeudi 17 juillet 2014 21:17:59 UTC.

Informations associées

["SPUT : PUT S3"](#)

["Éléments communs dans les messages d'audit"](#)

Informations sur le copyright

Copyright © 2024 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.