Formato de archivo de registro de auditoría

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Formato de archivo de registro de auditoría 1
Formato de archivo de registro de auditoría 1
Utilice la herramienta de auditoría y explicación 3
Utilice la herramienta de suma de auditoría 4

Formato de archivo de registro de auditoría

Formato de archivo de registro de auditoría

Los archivos de registro de auditoría se encuentran en cada nodo de administración y contienen una colección de mensajes de auditoría individuales.

Cada mensaje de auditoría contiene lo siguiente:

- El Tiempo Universal Coordinado (UTC) del evento que activó el mensaje de auditoría (ATIM) en formato ISO 8601, seguido de un espacio:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, dónde *UUUUUU* son microsegundos.

- El mensaje de auditoría en sí, encerrado entre corchetes y comenzando con `AUDT` .

El siguiente ejemplo muestra tres mensajes de auditoría en un archivo de registro de auditoría (se agregan saltos de línea para facilitar la lectura). Estos mensajes se generaron cuando un inquilino creó un depósito S3 y agregó dos objetos a ese depósito.

```
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]]
```

En su formato predeterminado, los mensajes de auditoría en los archivos de registro de auditoría no son fáciles de leer ni interpretar. Puedes utilizar el"herramienta de auditoría y explicación" para obtener resúmenes simplificados de los mensajes de auditoría en el registro de auditoría. Puedes utilizar el"herramienta de suma de auditoría" para resumir cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tomaron estas operaciones.

Utilice la herramienta de auditoría y explicación

Puedes utilizar el `audit-explain` herramienta para traducir los mensajes de auditoría en el registro de auditoría a un formato fácil de leer.

Antes de empezar

- Tienes"permisos de acceso específicos" .
- Debes tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

El `audit-explain` La herramienta, disponible en el nodo de administración principal, proporciona resúmenes simplificados de los mensajes de auditoría en un registro de auditoría.

> El `audit-explain` La herramienta está destinada principalmente a ser utilizada por el soporte técnico durante operaciones de resolución de problemas. Tratamiento `audit-explain` Las consultas pueden consumir una gran cantidad de energía de la CPU, lo que podría afectar las operaciones de StorageGRID .

Este ejemplo muestra una salida típica del `audit-explain` herramienta. Estos cuatro"ESPOLVO" Se generaron mensajes de auditoría cuando el inquilino S3 con ID de cuenta 92484777680322627870 utilizó solicitudes S3 PUT para crear un depósito llamado "bucket1" y agregar tres objetos a ese depósito.

```
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
```

El `audit-explain` La herramienta puede hacer lo siguiente:

- Procesar registros de auditoría simples o comprimidos. Por ejemplo:

  ```
  audit-explain audit.log

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

- Procesar múltiples archivos simultáneamente. Por ejemplo:

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

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

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada utilizando el `grep` comando u otros medios. Por ejemplo:

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

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

Debido a que los registros de auditoría pueden ser muy grandes y lentos de analizar, puede ahorrar tiempo filtrando las partes que desea ver y ejecutando `audit-explain` en las partes, en lugar de en todo el archivo.

> El `audit-explain` La herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el `zcat` herramienta para descomprimir los archivos primero. Por ejemplo:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilice el `help (-h)` Opción para ver las opciones disponibles. Por ejemplo:

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

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .
2. Introduzca el siguiente comando, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

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

   El `audit-explain` La herramienta imprime interpretaciones legibles por humanos de todos los mensajes en el archivo o archivos especificados.

   > Para reducir la longitud de las líneas y facilitar la legibilidad, las marcas de tiempo no se muestran de forma predeterminada. Si desea ver las marcas de tiempo, utilice la marca de tiempo(`-t`) opción.

Utilice la herramienta de suma de auditoría

Puedes utilizar el `audit-sum` herramienta para contar los mensajes de auditoría de escritura, lectura, encabezado y eliminación y para ver el tiempo mínimo, máximo y promedio (o tamaño) para cada tipo de operación.

Antes de empezar

- Tienes"permisos de acceso específicos" .

- Debes tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

El `audit-sum` La herramienta, disponible en el nodo de administración principal, resume cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tomaron estas operaciones.

> El `audit-sum` La herramienta está destinada principalmente a ser utilizada por el soporte técnico durante operaciones de resolución de problemas. Tratamiento `audit-sum` Las consultas pueden consumir una gran cantidad de energía de la CPU, lo que podría afectar las operaciones de StorageGRID .

Este ejemplo muestra una salida típica del `audit-sum` herramienta. Este ejemplo muestra cuánto tiempo tomaron las operaciones del protocolo.

```
  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
```

El `audit-sum` La herramienta proporciona recuentos y tiempos para los siguientes mensajes de auditoría de S3, Swift e ILM en un registro de auditoría.

> Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentra un código de auditoría que no aparece aquí, consulte las versiones anteriores de este tema para ver versiones anteriores de SG. Por ejemplo, "Documentación sobre el uso de la herramienta de suma de auditoría de StorageGRID 11.8" .

Código	Descripción	Referirse a
IDEL	Eliminación iniciada por ILM: registra cuándo ILM inicia el proceso de eliminación de un objeto.	"IDEL: Eliminación iniciada por ILM"
SDEL	S3 ELIMINAR: registra una transacción exitosa para eliminar un objeto o depósito.	"SDEL: S3 ELIMINAR"
SGET	S3 GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un depósito.	"SGET: S3 OBTENER"

Código	Descripción	Referirse a
KARITÉ	S3 HEAD: Registra una transacción exitosa para verificar la existencia de un objeto o depósito.	"SHEA: CABEZA T3"
ESPOLVO	S3 PUT: Registra una transacción exitosa para crear un nuevo objeto o depósito.	"SPUT: S3 PONER"
WDEL	Swift DELETE: registra una transacción exitosa para eliminar un objeto o contenedor.	"WDEL: Eliminación rápida"
WGET	Swift GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un contenedor.	"WGET: Obtención rápida"
TRIGO	Swift HEAD: registra una transacción exitosa para verificar la existencia de un objeto o contenedor.	"WHEA: CABEZA Veloz"
WPUT	Swift PUT: registra una transacción exitosa para crear un nuevo objeto o contenedor.	"WPUT: PUT rápido"

El `audit-sum` La herramienta puede hacer lo siguiente:

- Procesar registros de auditoría simples o comprimidos. Por ejemplo:

```
audit-sum audit.log

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

- Procesar múltiples archivos simultáneamente. Por ejemplo:

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

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

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada utilizando el `grep` comando u otros medios. Por ejemplo:

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

grep bucket1 audit.log | audit-sum

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

> Esta herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el `zcat` herramienta para descomprimir los archivos primero. Por ejemplo:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Puede utilizar las opciones de la línea de comandos para resumir las operaciones en los depósitos por separado de las operaciones en los objetos o para agrupar resúmenes de mensajes por nombre de depósito, por período de tiempo o por tipo de destino. De forma predeterminada, los resúmenes muestran el tiempo de operación mínimo, máximo y promedio, pero puede utilizar el `size (-s)` Opción para mirar el tamaño del objeto en su lugar.

Utilice el `help (-h)` Opción para ver las opciones disponibles. Por ejemplo:

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

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

      Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Si desea analizar todos los mensajes relacionados con las operaciones de escritura, lectura, encabezado y eliminación, siga estos pasos:
   a. Introduzca el siguiente comando, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

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

      Este ejemplo muestra una salida típica del `audit-sum` herramienta. Este ejemplo muestra cuánto tiempo tomaron las operaciones del protocolo.

      ```
        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
      ```

      En este ejemplo, las operaciones SGET (S3 GET) son las más lentas en promedio, con 1,13 segundos, pero las operaciones SGET y SPUT (S3 PUT) muestran tiempos de peor caso prolongados de aproximadamente 1770 segundos.

b. Para mostrar las 10 operaciones de recuperación más lentas, utilice el comando grep para seleccionar solo mensajes SGET y agregar la opción de salida larga(`-l`) para incluir rutas de objetos:

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

Los resultados incluyen el tipo (objeto o depósito) y la ruta, lo que le permite buscar en el registro de auditoría otros mensajes relacionados con estos objetos particulares.

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

+ En este ejemplo de salida, puede ver que las tres solicitudes GET de S3 más lentas fueron para objetos de aproximadamente 5 GB de tamaño, lo cual es mucho más grande que los otros objetos. El gran tamaño explica los tiempos de recuperación lentos en el peor de los casos.

3. Si desea determinar qué tamaños de objetos se están ingiriendo y recuperando de su cuadrícula, utilice la opción de tamaño(`-s`):

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

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

En este ejemplo, el tamaño de objeto promedio para SPUT es inferior a 2,5 MB, pero el tamaño promedio para SGET es mucho mayor. La cantidad de mensajes SPUT es mucho mayor que la cantidad de mensajes SGET, lo que indica que la mayoría de los objetos nunca se recuperan.

4. Si desea determinar si las recuperaciones fueron lentas ayer:

   a. Emita el comando en el registro de auditoría apropiado y utilice la opción agrupar por tiempo(`-gt`), seguido del período de tiempo (por ejemplo, 15M, 1H, 10S):

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

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

Estos resultados muestran que el tráfico GET de S3 aumentó entre las 06:00 y las 07:00. Los tiempos máximos y promedio también son considerablemente más altos en estos momentos y no aumentan gradualmente a medida que aumenta el recuento. Esto sugiere que se excedió la capacidad en algún lugar, quizás en la red o en la capacidad de la red para procesar solicitudes.

b. Para determinar qué tamaño de objetos se recuperaron cada hora ayer, agregue la opción de tamaño(`-s`) al comando:

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

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

Estos resultados indican que algunas recuperaciones muy grandes ocurrieron cuando el tráfico de recuperación general estaba en su máximo.

c. Para ver más detalles, utilice el"herramienta de auditoría y explicación" para revisar todas las operaciones de SGET durante esa hora:

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

Si se espera que la salida del comando grep tenga muchas líneas, agregue el `less` comando para mostrar el contenido del archivo de registro de auditoría una página (una pantalla) a la vez.

5. Si desea determinar si las operaciones SPUT en depósitos son más lentas que las operaciones SPUT en objetos:

a. Comience usando el `-go` opción, que agrupa los mensajes para operaciones de objetos y depósitos por separado:

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

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

Los resultados muestran que las operaciones SPUT para contenedores tienen características de rendimiento diferentes a las de las operaciones SPUT para objetos.

b. Para determinar qué buckets tienen las operaciones SPUT más lentas, utilice el `-gb` opción, que agrupa los mensajes por contenedor:

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

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

c. Para determinar qué depósitos tienen el tamaño de objeto SPUT más grande, utilice ambos `-gb` y el `-s` opciones:

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

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

Información de copyright

Información de la marca comercial