Formatos de archivo y mensaje de registro de auditoría

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-116/audit/using-audit-explain-tool.html on October 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Formatos de archivo y mensaje de registro de auditoría . . . 1
Formato del archivo de registro de auditoría . . . 1
Utilice la herramienta de explicación de auditoría . . . 3
Utilice la herramienta de suma de auditoría . . . 5
Formato de mensaje de auditoría . . . 14
Tipos de datos . . . 15
Datos específicos de un evento . . . 16
Elementos comunes de los mensajes de auditoría . . . 16
Ejemplos de mensajes de auditoría . . . 18

Formatos de archivo y mensaje de registro de auditoría

Puede usar los registros de auditoría para recopilar información sobre el sistema y solucionar problemas. Debe comprender el formato del archivo de registro de auditoría y el formato general que se utiliza para los mensajes de auditoría.

Formato del archivo de registro de auditoría

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

Cada mensaje de auditoría contiene lo siguiente:

- Hora universal coordinada (UTC) del evento que activó el mensaje de auditoría (ATIM) en formato ISO 8601, seguido de un espacio:

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

- El mensaje de auditoría mismo, entre corchetes y empezando por `AUDT`.

En el siguiente ejemplo se muestran tres mensajes de auditoría en un archivo de registro de auditoría (se han agregado saltos de línea para facilitar la lectura). Estos mensajes se generaron cuando un inquilino creó un bloque de S3 y se añadieron dos objetos a ese bloque.

```
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]]
```

Con su formato predeterminado, los mensajes de auditoría de los archivos de registro de auditoría no son fáciles de leer ni interpretar. Puede utilizar el `audit-explain` herramienta para obtener resúmenes simplificados de los mensajes de auditoría en el registro de auditoría. Puede utilizar el `audit-sum` herramienta para resumir cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo duraron estas operaciones.

Información relacionada

Utilice la herramienta de explicación de auditoría

Utilice la herramienta de explicación de auditoría

Puede utilizar el `audit-explain` herramienta para traducir los mensajes de auditoría del registro de auditoría a un formato de fácil lectura.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

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

> La `audit-explain` la herramienta está diseñada principalmente para su uso por parte del soporte técnico durante operaciones de solución de problemas. Procesamiento `audit-explain` Las consultas pueden consumir una gran cantidad de energía de CPU, lo que puede afectar a las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de `audit-explain` herramienta. Estos cuatro mensajes de auditoría SPUT se generaron cuando el inquilino S3 con ID de cuenta 92484777680322627870 utilizó solicitudes PUT de S3 para crear un bloque llamado "bucket1" y añadió tres objetos a ese bloque.

```
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
```

La `audit-explain` la herramienta puede procesar registros de auditoría sencillos o comprimidos. Por ejemplo:

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

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

La `audit-explain` la herramienta también puede procesar varios archivos a la vez. Por ejemplo:

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

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

Por último, la `audit-explain` la herramienta puede aceptar la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada mediante `grep` comando u otros medios. Por ejemplo:

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

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

Como los registros de auditoría pueden ser muy grandes y lentos de análisis, puede ahorrar tiempo al filtrar las partes que desea ver y ejecutar `audit-explain` en las partes, en lugar del archivo completo.

> La `audit-explain` la herramienta no acepta archivos comprimidos como entrada con hilo. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comandos o utilice `zcat` herramienta para descomprimir primero los archivos. Por ejemplo:

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

Utilice la `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 `Passwords.txt` archivo.
2. Introduzca el comando siguiente, donde `/var/local/audit/export/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

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

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

   > Para reducir las longitudes de línea y facilitar la legibilidad, las marcas de tiempo no se muestran de forma predeterminada. Si desea ver las marcas de tiempo, use la Marca de hora (`-t`) opción.

Información relacionada

SPUT: S3 PUT

Utilice la herramienta de suma de auditoría

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

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

La `audit-sum` Herramienta, disponible en el nodo de administración principal, resume cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo han tardado estas operaciones.

> La `audit-sum` la herramienta está diseñada principalmente para su uso por parte del soporte técnico durante operaciones de solución de problemas. Procesamiento `audit-sum` Las consultas pueden consumir una gran cantidad de energía de CPU, lo que puede afectar a las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de `audit-sum` herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de 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
```

La `audit-sum` La herramienta proporciona recuentos y horas para los siguientes mensajes de auditoría de S3, Swift y ILM en un registro de auditoría:

Codificación	Descripción	Consulte
ARCT	Archive recupere desde Cloud-Tier	ARCT: Recuperación de archivos a partir de nivel de cloud
ASCT	Almacenamiento de datos para el nivel cloud	ASCT: Archive Store Cloud-Tier

Codificación	Descripción	Consulte
IDEL	ILM Initiated Delete: Registra cuando ILM inicia el proceso de eliminación de un objeto.	IDEL: Eliminación de ILM iniciada
SDEL	S3 DELETE: Registra una transacción realizada correctamente para eliminar un objeto o bloque.	SDEL: ELIMINACIÓN DE S3
SGET	S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque.	SGET: S3 GET
SHEA	S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque.	SHEA: CABEZA S3
SPUT	S3 PUT: Registra una transacción realizada correctamente para crear un nuevo objeto o bloque.	SPUT: S3 PUT
¡WDEL	Swift DELETE: Registra una transacción realizada correctamente para eliminar un objeto o un contenedor.	WDEL: ELIMINACIÓN de Swift
CONSIGA	Swift GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un contenedor.	WGET: Swift GET
WHEA	Swift HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o contenedor.	WHEA: CABEZA de Swift
WPUT	Swift PUT: Registra una transacción correcta para crear un nuevo objeto o contenedor.	WPUT: SWIFT PUT

La `audit-sum` la herramienta puede procesar registros de auditoría sencillos o comprimidos. Por ejemplo:

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

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

La `audit-sum` la herramienta también puede procesar varios archivos a la vez. Por ejemplo:

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

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

Por último, la `audit-sum` la herramienta también puede aceptar la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada mediante la `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 con hilo. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comandos o utilice `zcat` herramienta para descomprimir primero los archivos. Por ejemplo:

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

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

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

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

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

Este ejemplo muestra el resultado típico de `audit-sum` herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de 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 a 1.13 segundos, pero las operaciones SGET y SPUT (S3 PUT) muestran tiempos largos en el peor de los casos de aproximadamente 1,770 segundos.

b. Para mostrar las operaciones de recuperación 10 más lentas, utilice el comando grep para seleccionar sólo los mensajes SGET y agregar la opción Long OUTPUT (`-l`) para incluir rutas de objetos: `grep SGET audit.log | audit-sum -l`

   Los resultados incluyen el tipo (objeto o bloque) y la ruta de acceso, que le permite obtener el registro de auditoría de otros mensajes relacionados con estos objetos en particular.

```
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
```

+ Desde este ejemplo, puede ver que las tres solicitudes DE OBTENER S3 más lentas eran para objetos de un tamaño de 5 GB, mucho mayor que el de los otros objetos. El gran tamaño representa los lentos tiempos de recuperación en el peor de los casos.

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

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

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

En este ejemplo, el tamaño medio del objeto para SPUT es inferior a 2.5 MB, pero el tamaño medio para SGET es mucho mayor. El número de mensajes SPUT es mucho mayor que el número de mensajes SGET, lo que indica que la mayoría de los objetos nunca se recuperan.

4. Si quieres determinar si las recuperaciones eran lentas ayer:
   a. Emita el comando en el registro de auditoría correspondiente y use la opción group-by-Time (`-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 S3 CONSIGUE tráfico pico entre 06:00 y 07:00. Los tiempos máximo y promedio son considerablemente más altos en estos tiempos también, y no subieron gradualmente a medida que el recuento aumentó. Esto sugiere que se ha superado la capacidad en algún lugar, quizás en la red o en la capacidad del grid para procesar solicitudes.

b. Para determinar el tamaño de los objetos recuperados ayer cada hora, agregue la opción size (`-s`) para el mando:

```
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 se han producido recuperaciones de gran tamaño cuando se alcanzó el máximo tráfico de recuperación total.

c. Para ver más detalles, utilice `audit-explain` Herramienta 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 sea de muchas líneas, agregue `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 los segmentos son más lentas que las operaciones SPUT para los objetos:

a. Comience por utilizar el `-go` opción, que agrupa mensajes para operaciones de objeto y bloque 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 los cubos tienen características de rendimiento diferentes a las operaciones SPUT para los objetos.

b. Para determinar qué cucharones tienen las operaciones de SPUT más lentas, utilice `-gb` opción, que agrupa mensajes por bloque:

```
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 cucharones tienen el tamaño de objeto SPUT más grande, utilice ambos `-gb` y la `-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 relacionada

Utilice la herramienta de explicación de auditoría

Formato de mensaje de auditoría

Los mensajes de auditoría intercambiados dentro del sistema StorageGRID incluyen información estándar común a todos los mensajes y contenido específico que describe el evento o la actividad que se está reportando.

Si la información resumida proporcionada por el `audit-explain` y.. `audit-sum` las herramientas son insuficientes; consulte esta sección para comprender el formato general de todos los mensajes de auditoría.

El siguiente es un mensaje de auditoría de ejemplo que puede aparecer en el archivo de registro de auditoría:

```
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]]
```

Cada mensaje de auditoría contiene una cadena de elementos de atributo. Toda la cadena se encuentra entre paréntesis (`[ ]`), y cada elemento de atributo de la cadena tiene las siguientes características:

- Entre paréntesis `[ ]`
- Introducido por la cadena `AUDT`, que indica un mensaje de auditoría
- Sin delimitadores (sin comas o espacios) antes o después
- Terminado por un carácter de avance de línea `\n`

Cada elemento incluye un código de atributo, un tipo de datos y un valor que se informa en este formato:

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

El número de elementos de atributo del mensaje depende del tipo de evento del mensaje. Los elementos de atributo no aparecen en ningún orden en particular.

En la siguiente lista se describen los elementos del atributo:

- `ATTR` es un código de cuatro caracteres para el atributo que se informa. Hay algunos atributos que son comunes a todos los mensajes de auditoría y a otros que son específicos de eventos.
- `type` Es un identificador de cuatro caracteres del tipo de datos de programación del valor, como UI64, FC32, etc. El tipo está entre paréntesis `( )`.
- `value` es el contenido del atributo, normalmente un valor numérico o de texto. Los valores siempre siguen dos puntos (`:`). Los valores del tipo de datos CSTR están rodeados por comillas dobles `" "`.

Información relacionada

Utilice la herramienta de explicación de auditoría

Utilice la herramienta de suma de auditoría

Auditar mensajes

Elementos comunes de los mensajes de auditoría

Tipos de datos

Ejemplos de mensajes de auditoría

Tipos de datos

Se utilizan diferentes tipos de datos para almacenar información en mensajes de auditoría.

Tipo	Descripción
UI32	Entero largo sin signo (32 bits); puede almacenar los números de 0 a 4,294,967,295.
UI64	Entero doble largo sin signo (64 bits); puede almacenar los números de 0 a 18,446,744,073,709,551,615.
FC32	Constante de cuatro caracteres; un valor entero de 32-bits sin signo que se representa como cuatro caracteres ASCII, como "ABCD".
IPAD	Se usa para direcciones IP.

Tipo	Descripción
CSTR	Matriz de longitud variable de caracteres UTF-8. Los caracteres se pueden escapar con las siguientes convenciones: • La barra invertida es \\. • El retorno del carro es \r. • Las comillas dobles son \". • La alimentación de línea (nueva línea) es \n. • Los caracteres se pueden sustituir por sus equivalentes hexadecimales (en el formato \xHH, donde HH es el valor hexadecimal que representa el carácter).

Datos específicos de un evento

Cada mensaje de auditoría del registro de auditoría registra datos específicos de un evento del sistema.

Siguiendo la abertura `[AUDT:` contenedor que identifica el mensaje en sí, el siguiente conjunto de atributos proporciona información acerca del evento o la acción descrita por el mensaje de auditoría. Estos atributos se resaltan en el siguiente ejemplo:

```
2018-12-SUST08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]* *\[TIME\(UI64\):11454
60025621595611246499\[SUST08\[SAIP\(IPAD\):"10.224.0 60025621595611246499.100
60025621595611246499"\[S3AI\(ECSTR\):"CSTR\\\\"[CSTR\][CSTR\\][CSTR]\\\\[CSTR][CSTR]\\\\[CSTR][
CSTR][CSTR\\\\\\\\"[CSTR][CSTR][CSTR][CSTR\\\\\\\\\\[CSTR][CSTR][CSTR][CSTR][CSTR][CSTR\\\\\\\\\
\[CSTR][CSTR][CSTR][CSTR][CSTR][CSTR][CSTR][CSTR\\\\\\\\\\\\\[KJC][KJC\\\
15552417629170647261 12281045 1543998285921845 10 30720
```

La `ATYP` elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el código DE mensaje SHEA ([ATYP(FC32):SHEA]), que indica que se generó mediante una solicitud de ENCABEZADO S3 correcta.

Información relacionada

Elementos comunes de los mensajes de auditoría

Auditar mensajes

Elementos comunes de los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

Codificación	Tipo	Descripción
EN MEDIO	FC32	ID de módulo: Identificador de cuatro-caracteres del ID de módulo que generó el mensaje. Indica el segmento de código en el que se generó el mensaje de auditoría.
ANID	UI32	Node ID: El ID del nodo de grid asignado al servicio que generó el mensaje. A cada servicio se le asigna un identificador único en el momento en que se configura e instala el sistema StorageGRID. Este ID no se puede cambiar.
ASES	UI64	Identificador de sesión de auditoría: En versiones anteriores, este elemento indicó la hora a la que se inicializó el sistema de auditoría después de que se iniciara el servicio. Este valor de tiempo se midió en microsegundos desde la época del sistema operativo (00:00:00 UTC el 1 de enero de 1970). **Nota:** este elemento es obsoleto y ya no aparece en los mensajes de auditoría.
ASQN	UI64	Recuento de secuencias: En versiones anteriores, este contador se ha incrementado para cada mensaje de auditoría generado en el nodo de cuadrícula (ANID) y se ha restablecido a cero en el reinicio del servicio. **Nota:** este elemento es obsoleto y ya no aparece en los mensajes de auditoría.
AID	UI64	ID de seguimiento: Identificador que comparte el conjunto de mensajes activados por un solo evento.
ATIM	UI64	Marca de hora: Hora en la que se generó el evento que activó el mensaje de auditoría, medida en microsegundos desde la época del sistema operativo (00:00:00 UTC el 1 de enero de 1970). Tenga en cuenta que la mayoría de las herramientas disponibles para convertir la Marca de tiempo a fecha y hora local se basan en milisegundos. Es posible que sea necesario redondear o truncar la Marca de tiempo registrada. El tiempo legible-humano que aparece al principio del mensaje de auditoría en la `audit.log` File es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan como *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, donde `T` es un carácter literal de cadena que indica el comienzo del segmento de tiempo de la fecha. *`UUUUUU`* son microsegundos.
ATYP	FC32	Tipo de evento: Un identificador de cuatro-caracteres del evento que se está registrando. Esto rige el contenido de "carga útil" del mensaje: Los atributos que se incluyen.
PROTECTOR	UI32	Versión: Versión del mensaje de auditoría. A medida que el software StorageGRID evoluciona, las nuevas versiones de los servicios podrían incorporar nuevas funciones en los informes de auditorías. Este campo permite la compatibilidad con versiones anteriores del servicio AMS para procesar mensajes de versiones anteriores de servicios.

Codificación	Tipo	Descripción
TRANSFORMACIÓN DIGITAL	FC32	Resultado: Resultado del evento, proceso o transacción. Si no es relevante para un mensaje, NO SE utiliza NINGUNO en lugar de SUCS para que el mensaje no se filtre accidentalmente.

Ejemplos de mensajes de auditoría

Puede encontrar información detallada en cada mensaje de auditoría. Todos los mensajes de auditoría tienen el mismo formato.

A continuación se muestra un mensaje de auditoría de ejemplo, que puede aparecer en la `audit.log` archivo:

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

El mensaje de auditoría contiene información sobre el evento que se está grabando, así como información sobre el propio mensaje de auditoría.

Para identificar qué evento se registra en el mensaje de auditoría, busque el atributo ATYP (destacado a continuación):

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

El valor del atributo ATYP es SPUT. SPUT representa una transacción PUT de S3, que registra la ingesta de un objeto en un bloque.

El siguiente mensaje de auditoría también muestra el bloque al que está asociado el objeto:

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

Para detectar cuándo se produjo el evento PUT, anote la Marca de hora de hora universal coordinada (UTC) al comienzo del mensaje de auditoría. Este valor es una versión legible-humano del atributo ATIM del mensaje de auditoría:

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

ATIM registra el tiempo, en microsegundos, desde el comienzo de la época UNIX. En el ejemplo, el valor `1405631878959669` Se traduce al jueves 17-Jul-2014 21:17:59 UTC.

Información relacionada

SPUT: S3 PUT

Elementos comunes de los mensajes de auditoría

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.