Formato del mensaje de auditoría

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Formato del mensaje de auditoría

Formato del 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 informa.

Si la información resumida proporcionada por el"auditoría-explicación" y"suma de auditoría" Si las herramientas son insuficientes, consulte esta sección para comprender el formato general de todos los mensajes de auditoría.

El siguiente es un ejemplo de mensaje de auditoría tal como podría 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 atributos. La cadena completa está entre corchetes.(`[ ]`), y cada elemento de atributo en la cadena tiene las siguientes características:

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

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

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

La cantidad de elementos de atributo en el mensaje depende del tipo de evento del mensaje. Los elementos de atributo no se enumeran en ningún orden particular.

La siguiente lista describe los elementos de 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 otros que son específicos del evento.
- `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 a dos puntos(:`). Los valores del tipo de datos CSTR están

rodeados por comillas dobles " ".

Tipos de datos

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

Tipo	Descripción
UI32	Entero largo sin signo (32 bits); puede almacenar los números del 0 al 4.294.967.295.
UI64	Entero doble largo sin signo (64 bits); puede almacenar los números del 0 al 18.446.744.073.709.551.615.
FC32	Constante de cuatro caracteres; un valor entero sin signo de 32 bits representado como cuatro caracteres ASCII como "ABCD".
iPad	Se utiliza para direcciones IP.
CSTR	Una matriz de longitud variable de caracteres UTF-8. Los caracteres se pueden escapar con las siguientes convenciones: • La barra invertida es \\. • El retorno de carro es \r. • Las comillas dobles son \". • El salto de línea (nueva línea) es \n. • Los caracteres se pueden reemplazar por sus equivalentes hexadecimales (en el formato \xHH, donde HH es el valor hexadecimal que representa el carácter).

Datos específicos del evento

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

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

2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]* **\[TIEMPO\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\] \[SACC\(CSTR\):"cuenta"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsK JA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\] \[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"cuenta"\]\[S3BK\(CSTR\):"depósito"\] \[S3KY\(CSTR\):"objeto"\]\[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]]

El `ATYP` El elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el"KARITÉ" código de mensaje ([ATYP(FC32):SHEA]), que indica que fue generado por una solicitud S3 HEAD exitosa.

Elementos comunes en los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

Código	Tipo	Descripción
EN MEDIO DE	FC32	ID del módulo: un identificador de cuatro caracteres del ID del módulo que generó el mensaje. Esto indica el segmento de código dentro del cual se generó el mensaje de auditoría.
ANID	UI32	ID de nodo: el ID del nodo de la red 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 . Esta identificación no se puede cambiar.
ASES	UI64	Identificador de sesión de auditoría: en versiones anteriores, este elemento indicaba el momento en el que se inicializaba el sistema de auditoría después de iniciarse el servicio. Este valor de tiempo se midió en microsegundos desde la época del sistema operativo (00:00:00 UTC del 1 de enero de 1970). **Nota:** Este elemento está obsoleto y ya no aparece en los mensajes de auditoría.
ASQN	UI64	Recuento de secuencia: en versiones anteriores, este contador se incrementaba para cada mensaje de auditoría generado en el nodo de la red (ANID) y se restablecía a cero al reiniciar el servicio. **Nota:** Este elemento está obsoleto y ya no aparece en los mensajes de auditoría.
ATID	UI64	ID de seguimiento: un identificador que comparte el conjunto de mensajes que se activaron mediante un solo evento.

Código	Tipo	Descripción
ATIM	UI64	Marca de tiempo: la hora en que se generó el evento que activó el mensaje de auditoría, medido en microsegundos desde la época del sistema operativo (00:00:00 UTC del 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 locales se basan en milisegundos. Podría ser necesario redondear o truncar la marca de tiempo registrada. La hora legible por humanos que aparece al comienzo del mensaje de auditoría en el `audit.log` El archivo es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan como *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , donde el `T` es un carácter de cadena literal 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 regula el contenido de "carga útil" del mensaje: los atributos que se incluyen.
AFIRMAR	UI32	Versión: La 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 auditoría. Este campo permite la compatibilidad con versiones anteriores del servicio AMS para procesar mensajes de versiones anteriores de los servicios.
RSLT	FC32	Resultado: El resultado de un evento, proceso o transacción. Si no es relevante para un mensaje, se utiliza NONE 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 utilizan el mismo formato.

El siguiente es un ejemplo de mensaje de auditoría tal como podría aparecer en el `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 registrando, así como información sobre el mensaje de auditoría en sí.

Para identificar qué evento registra el mensaje de auditoría, busque el atributo ATYP (resaltado 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. "ESPOLVO" representa una transacción S3 PUT, que registra la ingesta de un objeto en un depósito.

El siguiente mensaje de auditoría también muestra el depósito 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 descubrir cuándo ocurrió el evento PUT, observe la marca de tiempo del Tiempo Universal Coordinado (UTC) al comienzo del mensaje de auditoría. Este valor es una versión legible para humanos del atributo ATIM del mensaje de auditoría en sí:

```
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 de julio de 2014 21:17:59 UTC.