Formato de mensaje de auditoría

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Formato de mensaje de auditoría

Formato del mensaje de auditoría: Información general

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 "auditoría-explicar" y.. "suma de auditoría" 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 dato CSTR están rodeados por comillas dobles.

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 sin signo de 32 bits representado como cuatro caracteres ASCII como ABCD.
IPAD	Se usa para direcciones IP.
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:

2018-12-05T08:24:45,921845 [AUDT:*\[RSLT\(FC32\):SUCS\]* **\[TIME\(UI64\):11454\]\[SAIP\(IPAD\): «10.224.0.100»\]\[S3AI\(CSTR\): «60025621595611246499»\] \[SACC\(CSTR\): “Cuenta”\]\[S3AK\(CSTR\): “SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=”\] \[SUSR\(CSTR\): “Urn:sgws:identity::60025621595611246499:root”\] \[SBAI\(CSTR\): “60025621595611246499”\]\[SBAC\(CSTR\): “CUENTA”\]\[S3BK\(CSTR\): “CUBO”\] \[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]]

La `ATYP` elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el "SHEA" Código de mensaje ([ATYP(FC32):SHEA]), que indica que fue generado por una solicitud correcta de S3 CABEZA.

Elementos comunes de los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

Codificación	Tipo	Descripción
EN MEDIO	FC32	ID del módulo: Identificador de cuatro caracteres del ID del 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 por el usuario que aparece al principio del mensaje de auditoría en `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.

Codificación	Tipo	Descripción
ATYP	FC32	Tipo de evento: 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.
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, tal y como podría 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 S3, que registra la ingesta de un objeto en un depósito.

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 por 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-Jul-2014 21:17:59 UTC.

Información de copyright

Información de la marca comercial