審計訊息格式
StorageGRID software

NetApp
May 29, 2026

目錄

審計訊息格式 1
- 審計訊息格式 1
- 資料類型 1
- 事件特定數據 2
- 審計訊息中的常見元素 2
- 審計訊息範例 3

審計訊息格式

審計訊息格式

StorageGRID系統內交換的稽核訊息包括所有訊息共有的標準資訊以及描述所報告事件或活動的具體內容。

如果"審計解釋"和"審計總額"工具不足，請參閱本節以了解所有稽核訊息的一般格式。

以下是審計日誌檔案中可能出現的範例審計訊息：

```
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]]
```

每條審計訊息都包含一串屬性元素。整個字串括在括號中(`[ ]`)，字串中每個屬性元素具有以下特點：

- 括在括號中 `[ ]`
- 由字串引入 `AUDT`，表示審計消息
- 前後沒有分隔符號（沒有逗號或空格）
- 以換行符終止 `\n`

每個元素都包含一個屬性代碼、一個資料類型和一個值，並以以下格式報告：

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

訊息中的屬性元素的數量取決於訊息的事件類型。實體元素沒有按照任何特定順序列出。

以下列表描述了屬性元素：

- `ATTR`是所報告屬性的四字元代碼。有些屬性是所有審計訊息所共有的，而其他屬性則是特定於事件的。
- `type`是值的程式資料類型的四個字元的標識符，例如 `UI64`、`FC32` 等。類型用括號括起來 `( )`。
- `value`是屬性的內容，通常是數字或文字值。值總是跟在冒號後面 (`:`) 。資料型別 CSTR 的值用雙引號「」括起來。

資料類型

不同的資料類型用於儲存審計訊息中的資訊。

類型	描述
UI32	無符號長整數（32 位元）；可儲存 0 到 4,294,967,295 的數字。
UI64	無符號雙精確度長整數（64 位元）；它可以儲存 0 到 18,446,744,073,709,551,615 的數字。
FC32	四字符常數；一個 32 位元無符號整數值，表示為四個 ASCII 字符，例如“ABCD”。
IPAD	用於 IP 位址。
連續應力試驗	UTF-8 字元的可變長度數組。字元可以按照以下約定進行轉義： • 反斜杠是 \\。 • 回車符是 \r。 • 雙引號是\"。 • 換行符（新行）是 \n。 • 字元可以用其十六進位等效值替換（格式為 \xHH，其中 HH 是表示字元的十六進位值）。

事件特定數據

審計日誌中的每個審計訊息都記錄特定於系統事件的資料。

開幕後 `[AUDT:`標識訊息本身的容器，下一組屬性提供有關審計訊息所描述的事件或操作的資訊。以下範例中突出顯示了這些屬性：

```
2018-12-05T08：24：45.921845 [AUDT：\[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]\):"60
025621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRs
KJA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"帳號"\]\[S3BK\(CSTR\):"儲存桶"\]
\[S3KY\(CSTR\):"物件"\]\[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):1552417626174176267]
```

這 `ATYP`元素（範例中帶下劃線）標識產生該訊息的事件。此範例訊息包括"乳木果"訊息代碼（[ATYP(FC32):SHEA]），表示它是由成功的 S3 HEAD 請求產生的。

審計訊息中的常見元素

所有審計訊息都包含共同的元素。

程式碼	類型	描述
之中	FC32	模組 ID：產生訊息的模組 ID 的四個字元識別碼。這表示產生審計訊息的代碼段。
安尼德	UI32	節點 ID：指派給產生訊息的服務的網格節點 ID。在設定和安裝StorageGRID系統時，每個服務都會指派一個唯一的識別碼。此 ID 無法變更。
東南大學	UI64	審計會話標識符：在先前的版本中，此元素指示服務啟動後審計系統初始化的時間。此時間值以作業系統紀元（1970 年 1 月 1 日 00:00:00 UTC）以來的微秒為單位進行測量。 *注意：*此元素已過時，不再出現在稽核訊息中。
美國品質協會	UI64	序列計數：在先前的版本中，此計數器會隨著網格節點（ANID）上產生的每個稽核訊息而遞增，並在服務重新啟動時重設為零。 *注意：*此元素已過時，不再出現在稽核訊息中。
急性胰臟炎	UI64	追蹤 ID：由單一事件觸發的一組訊息共享的識別碼。
ATIM	UI64	時間戳記：觸發稽核訊息的事件的產生時間，以自作業系統紀元（1970 年 1 月 1 日 00:00:00 UTC）以來的微秒為單位。請注意，大多數用於將時間戳轉換為本地日期和時間的工具都是基於毫秒的。 可能需要對記錄的時間戳進行四捨五入或截斷。審計訊息開頭出現的可讀時間 `audit.log`檔案是 `ISO 8601` 格式的 `ATIM` 屬性。日期和時間表示為 `*YYYY-MMDDTHH:MM:SS.UUUUUU*`，其中 `T`是一個文字字串字符，表示日期時間段的開始。`*UUUUUU*`是微秒。
典型蛋白	FC32	事件類型：正在記錄的事件的四個字元的識別碼。這決定了訊息的「有效負載」內容：所包含的屬性。
斷言	UI32	版本：審計訊息的版本。隨著StorageGRID軟體的發展，新版本的服務可能會在審計報告中加入新功能。此欄位使 AMS 服務能夠向後相容，以處理來自舊版本服務的訊息。
放射學研究實驗室	FC32	結果：事件、過程或交易的結果。如果與訊息無關，則使用 NONE 而不是 SUCS，以免訊息被意外過濾。

審計訊息範例

您可以在每個審計訊息中找到詳細資訊。所有審計訊息都使用相同的格式。

以下是可能出現在 `audit.log`文件：

```
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]]
```

審計訊息包含有關正在記錄的事件的信息，以及有關審計訊息本身的資訊。

若要確定審計訊息記錄了哪個事件，請尋找 ATYP 屬性（如下所示）：

```
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]]
```

ATYP屬性的值為SPUT。"噴管"表示 S3 PUT 事務，它將物件的攝取記錄到儲存桶中。

以下審計訊息也顯示了該物件所關聯的儲存桶：

```
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]]
```

若要了解 PUT 事件發生的時間，請注意審計訊息開頭的協調世界時 (UTC) 時間戳記。該值是審計訊息本身的 ATIM 屬性的人類可讀版本：

```
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 記錄自 UNIX 紀元開始以來的時間（以微秒為單位）。在範例中，值 `1405631878959669`轉換為 2014 年 7 月 17 日星期四 21:17:59 UTC。

版權資訊

商標資訊