稽核訊息格式
StorageGRID 11.7

NetApp
April 12, 2024

目錄

稽核訊息格式

稽核訊息格式：總覽

在這個系統內交換的稽核訊息StorageGRID 包括所有訊息通用的標準資訊、以及說明所報告事件或活動的特定內容。

如果摘要資訊是由所提供 "稽核說明" 和 "稽核總和" 工具不足、請參閱本節以瞭解所有稽核訊息的一般格式。

以下是稽核記錄檔中可能出現的稽核訊息範例：

```
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]]
```

每個稽核訊息都包含一串屬性元素。整個字串都以方括弧括住（`[ ]`）、且字串中的每個屬性元素具有下列特性：

- 附在支架中 `[ ]`
- 由字串引進 `AUDT`，表示稽核訊息
- 不含分隔符號（不含逗號或空格）
- 以換行字元終止 `\n`

每個元素都包含屬性代碼、資料類型及以下列格式報告的值：

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

訊息中的屬性元素數目取決於訊息的事件類型。屬性元素不會以任何特定順序列出。

下列清單說明屬性元素：

- `ATTR` 為所報告屬性的四個字元代碼。有些屬性是所有稽核訊息和其他特定事件的常見屬性。
- `type` 為值的程式設計資料類型的四個字元識別碼、例如UI64、FC32等。此類型以括弧括住 `( )`。
- `value` 是屬性的內容、通常是數值或文字值。值一律會跟在一個分號之後 (`:`）。資料類型CStr的值會以雙引號括住 `" "`。

資料類型

不同的資料類型可用來將資訊儲存在稽核訊息中。

類型	說明
UI32	無符號長整數（32位元）；可儲存0至4、294、967、295的數字。
UI64	無符號雙長整數（64位元）；可儲存0至18、446,744,073,709,551615的數字。
FC32	四個字元常量； 32 位元無符號整數值、表示為四個 ASCII 字元、例如「 ABCD 」。
iPad	用於IP位址。
CStr	UTF-8 字元的可變長度陣列。可以使用下列慣例來轉義字元： • 反斜槓是\。 • 回車是\r • 雙引號是\ • 換行（新行）為 • 字元可以用其十六進位等效字元來取代（格式為\xhh、其中hh是代表字元的十六進位值）。

事件特定資料

稽核日誌中的每個稽核訊息都會記錄特定於系統事件的資料。

開啟後 `[AUDT:` 識別訊息本身的容器、下一組屬性會提供稽核訊息所述事件或動作的相關資訊。這些屬性會在下列範例中反白顯示：

```
2018-12-05T08：24：45.921845 [AUDT：\[RSALT\]（FC32\）：SUCS\*\[Time（UI64\）：11454\[SAIP\（ipad\）："10.224.0.100"\[S3AI（CStr\）："4196920499*
Stls6400c64T64"S=Cs=S64T64T1T64"S=Cs=Cs=S64T64T1T1T64T64T64"1T64T1T1"S=S="S64T64"S=Cs=Cs=S64"S64T1=Cs=Cs=C64T64T64T64T1T1T1T1T1T1="S64T1=Cs=C64T64T64T1=C64"S=Cs="S64T1=C64T1="S64T64T1=C64T64T64T1"S="S
```

。 `ATYP` 元素（在範例中加上底線）可識別產生訊息的事件。此範例訊息包括 "Shea" 訊息代碼（ [ATYP（ FC32 ）： Shea ）、表示它是由成功的 S3 標頭要求所產生。

稽核訊息中的一般元素

所有稽核訊息都包含通用元素。

程式碼	類型	說明
在	FC32	模組 ID ：產生訊息之模組 ID 的四個字元識別碼。這表示產生稽核訊息的程式碼區段。

程式碼	類型	說明
ANID	UI32	節點ID：指派給產生訊息之服務的網格節點ID。每項服務在StorageGRID設定和安裝完整套系統時、都會分配一個唯一的識別碼。此 ID 無法變更。
。	UI64	稽核工作階段識別碼：在舊版中、此元素指出在服務啟動後、稽核系統初始化的時間。此時間值的測量單位為自作業系統時代（1970年1月1日為00：00：00 UTC）以來的微秒。 *注意：*此元素已過時、不再出現在稽核訊息中。
ASQN	UI64	連續數：在先前版本中、此計數器會針對網格節點（ANID）上每個產生的稽核訊息遞增、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。
ATID	UI64	追蹤ID：由單一事件觸發的一組訊息所共用的識別碼。
ATIM	UI64	時間戳記：觸發稽核訊息的事件產生時間、以微秒為單位、自作業系統時期（00：00：00 UTC於70年1月1日）以來計算。請注意、將時間戳記轉換為本機日期和時間的大多數可用工具都是以毫秒為基礎。 可能需要捨入或捨去記錄的時間戳記。顯示在中稽核訊息開頭的人類可讀時間 `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` 為文字字串字元、表示日期時間區段的開頭。 *`UUUUUU`* 為微秒。
ATYP	FC32	事件類型：所記錄事件的四個字元識別碼。這會規範訊息的「有效負載」內容：包含的屬性。
離職者	UI32	版本：稽核訊息的版本。隨著更新版的支援軟體、新版的服務可能會在稽核報告中加入新功能。StorageGRID此欄位可在AMS服務中啟用向下相容性、以處理舊版服務的訊息。
RSRLT	FC32	結果：事件、程序或交易的結果。如果與訊息無關、則不會使用任何訊息、而不會使用SUCS、因此不會意外篩選訊息。

稽核訊息範例

您可以在每個稽核訊息中找到詳細資訊。所有稽核訊息都使用相同的格式。

以下是可能出現在中的範例稽核訊息 `audit.log` 檔案：

```
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]]
```

稽核訊息包含所記錄事件的相關資訊、以及稽核訊息本身的相關資訊。

若要識別稽核訊息所記錄的事件、請尋找ATYP屬性（反白顯示如下）：

```
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。 "SPUT" 代表 S3 Put 交易、將物件的擷取記錄到儲存區。

下列稽核訊息也會顯示物件關聯的儲存區：

```
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]]
```

若要瞭解放置事件發生的時間、請在稽核訊息開頭記下通用協調時間（UTC）時間戳記。此值是稽核訊息本身的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會記錄UNIX時代開始以來的時間（以微秒為單位）。範例中的值 `1405631878959669` 轉譯為2014年7月17日星期四21：17：59 UTC。