



稽核記錄檔和訊息格式 StorageGRID

NetApp
October 03, 2025

目錄

稽核記錄檔和訊息格式	1
稽核記錄檔格式	1
使用稽核說明工具	3
使用稽核加總工具	4
稽核訊息格式	14
資料類型	15
事件特定資料	16
稽核訊息中的一般元素	16
稽核訊息範例	17

稽核記錄檔和訊息格式

您可以使用稽核記錄來收集系統相關資訊、並疑難排解問題。您應該瞭解稽核記錄檔的格式、以及稽核訊息所使用的一般格式。

稽核記錄檔格式

稽核記錄檔位於每個管理節點、並包含個別稽核訊息的集合。

每個稽核訊息都包含下列項目：

- 觸發ISO 8601格式稽核訊息（ATIM）的事件協調世界時間（UTC）、後面接著空格：

YYYY-MM-DDTHH:MM:SS.UUUUUU、其中 *UUUUUU* 為微秒。

- 稽核訊息本身、以方括弧括住、開頭為 `AUDT`。

下列範例顯示稽核記錄檔中的三個稽核訊息（換行符號會新增以方便閱讀）。當租戶建立S3儲存區並將兩個物件新增至該儲存區時、就會產生這些訊息。

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]]
```

以預設格式、稽核記錄檔中的稽核訊息不易讀取或解讀。您可以使用 `audit-explain` 工具、可在稽核記錄中取得稽核訊息的簡化摘要。您可以使用 `audit-sum` 此工具可摘要記錄寫入、讀取及刪除作業的數量、以及這些作業所需的時間。

相關資訊

["使用稽核說明工具"](#)

["使用稽核加總工具"](#)

使用稽核說明工具

您可以使用 `audit-explain` 將稽核記錄中的稽核訊息轉譯為易於讀取的格式的工具。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須擁有 `Passwords.txt` 檔案：
- 您必須知道主管理節點的IP位址。

關於這項工作

- `audit-explain` 此工具可在主要管理節點上使用、可在稽核記錄中提供稽核訊息的簡化摘要。



◦ `audit-explain` 此工具主要供疑難排解作業期間的技術支援人員使用。處理中 `audit-explain` 查詢可能會耗用大量的CPU電力、這可能會影響StorageGRID 到整個過程。

此範例顯示的一般輸出 `audit-explain` 工具：當帳戶ID為92484777680322627870的S3租戶提出建立名為「Bucket1」的儲存區要求、並將三個物件新增至該儲存區時、就會產生這四個SPUT稽核訊息。

```
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
```

- `audit-explain` 工具可以處理純文字或壓縮的稽核記錄。例如：

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

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

- `audit-explain` 工具也可以一次處理多個檔案。例如：

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

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

最後 `audit-explain` 工具可以接受來自管路的輸入、讓您使用篩選及預先處理輸入 `grep` 命令或其他方法。例如：

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

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

由於稽核記錄的剖析速度可能非常龐大且緩慢、因此您可以篩選要查看及執行的部分、藉此節省時間 `audit-explain` 在零件上、而非整個檔案。



◦ `audit-explain` 工具不接受壓縮檔案做為管道輸入。若要處理壓縮檔案、請將檔案名稱提供為命令列引數、或使用 `zcat` 先解壓縮檔案的工具。例如：

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

使用 `help (-h)` 選項以查看可用的選項。例如：

```
$ audit-explain -h
```

步驟

1. 登入主要管理節點：

- a. 輸入下列命令：`ssh admin@primary_Admin_Node_IP`
- b. 輸入中所列的密碼 `Passwords.txt` 檔案：

2. 輸入下列命令、其中 `/var/local/audit/export/audit.log` 代表您要分析的檔案名稱和位置：

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

◦ `audit-explain` 工具會針對指定檔案或檔案中的所有訊息、列印人類可讀的解析。



為了縮短行長並提高讀取能力、預設不會顯示時間戳記。如果您想要查看時間戳記、請使用時間戳記 (`-t`) 選項。

相關資訊

["SPUT : S3"](#)

使用稽核加總工具

您可以使用 `audit-sum` 用於計算寫入、讀取、顯示及刪除稽核訊息的工具、以及查看每種作業類型的最小、最大和平均時間（或大小）。

您需要的產品

- 您必須擁有特定的存取權限。

- 您必須擁有 Passwords.txt 檔案：
- 您必須知道主管理節點的IP位址。

關於這項工作

◦ audit-sum 工具（可在主要管理節點上使用）摘要說明記錄了多少寫入、讀取和刪除作業、以及這些作業需要多長時間。



◦ audit-sum 此工具主要供疑難排解作業期間的技術支援人員使用。處理中 audit-sum 查詢可能會耗用大量的CPU電力、這可能會影響StorageGRID 到整個過程。

此範例顯示的一般輸出 audit-sum 工具：此範例顯示傳輸協定作業所需的時間。

```

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

```

◦ audit-sum 此工具可在稽核記錄中提供下列S3、Swift和ILM稽核訊息的計數和時間：

程式碼	說明	請參閱
ARCT	歸檔從雲端層擷取	"ARCT：歸檔從雲端層擷取"
ASCT	歸檔儲存雲端層	"ASCT：歸檔儲存雲端層"
理想	ILM初始化刪除：ILM開始刪除物件的程序時記錄。	"表意：ILM啟動刪除"
SDEL	S3刪除：記錄成功的交易以刪除物件或儲存區。	"SDEL：S3刪除"
SGET	S3 Get：記錄成功的交易、以擷取物件或列出儲存區中的物件。	"SGET：S3取得"
Shea	S3標頭：記錄成功的交易、以檢查物件或儲存區是否存在。	"Shea：S3負責人"

程式碼	說明	請參閱
SPUT	S3 PUT：記錄成功的交易、以建立新的物件或儲存區。	"SPUT：S3"
WDEL	Swift刪除：記錄成功的交易以刪除物件或容器。	"WDEL：Swift刪除"
WGet	Swift Get：記錄成功的交易、以擷取物件或列出容器中的物件。	"WGet：Swift Get"
WHA	Swift標頭：記錄成功的交易、以檢查物件或容器是否存在。	"WHA：Swift刀頭"
WUT	Swift PUT：記錄成功的交易、以建立新的物件或容器。	"WUTT：Swift Put"

◦ `audit-sum` 工具可以處理純文字或壓縮的稽核記錄。例如：

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

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

◦ `audit-sum` 工具也可以一次處理多個檔案。例如：

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

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

最後 `audit-sum` 工具也可以接受來自管路的輸入、讓您使用篩選和預先處理輸入 `grep` 命令或其他方法。例如：

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



此工具不接受壓縮檔案做為管道輸入。若要處理壓縮檔案、請將檔案名稱提供為命令列引數、或使用 `zcat` 先解壓縮檔案的工具。例如：

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

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

您可以使用命令列選項、將儲存區上的作業與物件上的作業分開彙總、或依儲存區名稱、時間期間或目標類型將訊息摘要分組。根據預設、摘要會顯示最小、最大和平均操作時間、但您可以使用 `size (-s)` 選項、改為查看物件大小。

使用 `help (-h)` 選項以查看可用的選項。例如：

```
$ audit-sum -h
```

步驟

1. 登入主要管理節點：

- a. 輸入下列命令：`ssh admin@primary_Admin_Node_IP`
- b. 輸入中所列的密碼 `Passwords.txt` 檔案：

2. 如果您要分析與寫入、讀取、標頭及刪除作業相關的所有訊息、請依照下列步驟操作：

- a. 輸入下列命令、其中 `/var/local/audit/export/audit.log` 代表您要分析的檔案名稱和位置：

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

此範例顯示的一般輸出 `audit-sum` 工具：此範例顯示傳輸協定作業所需的時間。

message group average(sec)	count	min(sec)	max(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			

在此範例中、SGET (S3 Get) 作業平均速度最慢、僅1.13秒、但SGET和SPUT (S3 PUT) 作業都顯示出約1、730秒的長時間最差時間。

- b. 若要顯示最慢的10個擷取作業、請使用Grep命令僅選取SGET訊息、然後新增長輸出選項 (-l) 若要包含物件路徑：`grep SGET audit.log | audit-sum -l`

結果包括類型 (物件或儲存區) 和路徑、可讓您為稽核日誌中與這些特定物件相關的其他訊息進行Grep。

```

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/r9010aQ8JB-1566861764-4519.iso
1624414429  10.96.101.125      object  5375001556
backup/r9010aQ8JB-1566861764-6618.iso
1533143793  10.96.101.125      object  5183661466
backup/r9010aQ8JB-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

```

+ 在此範例輸出中、您可以看到三個最慢的S3「Get（取得）」要求是針對大小約5 GB的物件、比其他物件大得多。大容量則是最差擷取時間緩慢的問題。

3. 如果您想要判斷要從網格擷取和擷取的物件大小、請使用「大小」選項 (-s) :

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

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

在此範例中、SPUT的平均物件大小低於2.5 MB、但SGET的平均大小卻大得多。SPUT訊息的數量遠高於SGET訊息的數量、表示大部分的物件永遠不會擷取。

- 4. 如果您想要判斷昨天擷取的速度是否緩慢：
 - a. 在適當的稽核記錄上發出命令、然後使用「依時間分組」選項 (-gt)、接著是期間 (例如、15M、1H、10S)：

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

這些結果顯示S3在06:00到07:00之間尖峰流量。在這些時間、最大和平均時間都會大幅增加、而且不會隨著計數增加而逐漸增加。這表示容量已超過某個位置、可能是網路或網格處理要求的能力。

b. 若要判斷昨天每小時擷取的物件大小、請新增「大小」選項 (-s) 命令：

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

這些結果顯示、當整體擷取流量達到最大值時、會發生一些非常大的擷取。

- c. 若要查看更多詳細資料、請使用 `audit-explain` 檢閱該時段所有SGET作業的工具：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

如果應該輸出許多行的Grep命令、請新增 `less` 命令、一次顯示一頁（一個畫面）的稽核記錄檔內容。

5. 如果您想要判斷儲存區上的SPUT作業是否比物件的SPUT作業慢：

- a. 從使用開始 `-go` 選項、可分別將物件和儲存區作業的訊息分組：

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

結果顯示、適用於貯體的SPUT作業與物件的SPUT作業具有不同的效能特性。

b. 若要判斷哪些儲存區的SPUT作業速度最慢、請使用 -gb 選項、可依儲存區將訊息分組：

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ltd002 0.361	1564563	0.011	51.569

c. 若要判斷哪些儲存區具有最大的SPUT物件大小、請同時使用 -gb 和 -s 選項：

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ldt002 0.352	1564563	0.000	999.972

相關資訊

["使用稽核說明工具"](#)

稽核訊息格式

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 audit-explain 和 audit-sum 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 (FC32) :SYSU] [ANID (UI32) :11627225] [AMID (FC32) :ARNI] [ATID (UI64) :9445736326500603516]]
```

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 " "。

相關資訊

["使用稽核說明工具"](#)

["使用稽核加總工具"](#)

["稽核訊息"](#)

["稽核訊息中的一般元素"](#)

["資料類型"](#)

["稽核訊息範例"](#)

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	四個字元的常量 ; 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。

類型	說明
CStr	<p>長度可變的UTF - 8字元陣列。可以使用下列慣例來轉義字元：</p> <ul style="list-style-type: none"> • 反斜槓是\ • 回車是\ • 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\

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: [RSLT (FC32) :SUCS]
[TIME (UI64) :11454] [SAIP (IPAD) : "10.224.0.100"]
[S3AI (CSTR) : "60025621595611246499"] [SACC (CSTR) : "account"]
[S3AK (CSTR) : "SGKH4_Nc8S01H6w3w0nCOFCGgk_E6dYzKlumRsKJA=="]
[SUSR (CSTR) : "urn:sgws:identity::60025621595611246499:root"]
[SBAI (CSTR) : "60025621595611246499"] [SBAC (CSTR) : "account"] [S3BK (CSTR) : "bucket"]
[S3KY (CSTR) : "object"] [CBID (UI64) :0xCC128B9B9E428347]
[UID (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]]
```

◦ ATYP 元素（在範例中加上底線）可識別產生訊息的事件。此範例訊息包含Shea訊息代碼（[ATYP (FC32) :Shea]）、表示該訊息是由成功的S3標頭要求所產生。

相關資訊

["稽核訊息中的一般元素"](#)

["稽核訊息"](#)

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。中稽核訊息開頭顯示的人工可讀時間 <code>audit.log</code> 檔案是ISO 8601格式的ATIM屬性。日期和時間表示為 <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> 、其中 T 為文字字串字元、表示日期時間區段的開頭。 <code>UUUUUU</code> 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):"s3small11"]][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):"s3small11"]][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、會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):"s3small11"][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ATIM屬性的人工可讀版本：

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3KY(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):1579224144102530435]]
```

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。

相關資訊

["SPUT : S3"](#)

["稽核訊息中的一般元素"](#)

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。