審計日誌檔案格式

StorageGRID software

NetApp
May 29, 2026

目錄

審計日誌檔案格式

審計日誌檔案格式

每個管理節點上都有審計日誌文件，其中包含一系列單獨的審計訊息。

每條審計訊息包含以下內容：

- 觸發審計訊息 (ATIM) 的事件的協調世界時 (UTC)，採用 ISO 8601 格式，後面跟著一個空格：

  YYYY-MM-DDTHH:MM:SS.UUUUUU， 在哪裡 `*UUUUUU*` 是微秒。

- 審計訊息本身，括在方括號內，以 `AUDT`。

以下範例顯示了審計日誌檔案中的三個審計訊息（為便於閱讀添加了換行符）。當租用戶建立 S3 儲存桶並在該儲存桶中新增兩個物件時，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::17530064241597054
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::17530064241597054
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):84396067221084560 22]]

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::17530064241597054
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]]
```

在預設格式下，審計日誌檔案中的審計訊息不易閱讀或解釋。您可以使用"審計解釋工具"取得審計日誌中審計訊息的簡化摘要。您可以使用"審計總和工具"總結記錄了多少寫入、讀取和刪除操作以及這些操作花費了多長時間。

使用審計解釋工具

您可以使用 `audit-explain`工具將稽核日誌中的稽核訊息轉換為易於閱讀的格式。

開始之前

- 你有"特定存取權限"。
- 你必須擁有 `Passwords.txt`文件。
- 您必須知道主管理節點的 IP 位址。

關於此任務

這 `audit-explain`主管理節點上提供的工具可在稽核日誌中提供稽核訊息的簡化摘要。

> 這 `audit-explain`該工具主要供技術支援人員在故障排除操作期間使用。加工 `audit-explain`查詢會消耗大量 CPU 能力，這可能會影響StorageGRID操作。

此範例顯示了 `audit-explain`工具。這四個"噴管"當帳戶 ID 為 92484777680322627870 的 S3 租用戶使用 S3 PUT 請求建立名為「bucket1」的儲存桶並向該儲存桶新增三個物件時，產生了稽核訊息。

```
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
```

這 `audit-explain`工具可以執行以下操作：

- 處理純文字或壓縮的稽核日誌。例如：

  ```
  audit-explain audit.log

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

- 同時處理多個文件。例如：

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

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

- 接受來自管道的輸入，這允許您使用以下方式過濾和預處理輸入 `grep`命令或其他方式。例如：

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

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

由於審計日誌可能非常大且解析速度很慢，因此您可以透過篩選要查看的部分並運行來節省時間 `audit-explain`對各個部分進行操作，而不是對整個文件進行操作。

這 `audit-explain`工具不接受壓縮檔案作為管道輸入。若要處理壓縮文件，請將其檔案名稱作為命令列參數提供，或使用 `zcat`工具先解壓縮檔案。例如：

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

使用 `help (-h)`選項來查看可用的選項。例如：

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

步驟

1. 登入主管理節點：
   a. 輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

      當您以 root 身分登入時，提示字元將從 `$`到 `#`。
2. 輸入以下命令，其中 `/var/local/log/audit.log`代表您要分析的檔案的名稱和位置：

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

   這 `audit-explain`工具列印指定檔案中所有訊息的人類可讀的解釋。

   為了減少行長度並提高可讀性，預設不顯示時間戳。如果你想查看時間戳，請使用時間戳(`-t`) 選項。

使用審計總和工具

您可以使用 `audit-sum`工具來統計寫入、讀取、頭部和刪除稽核訊息，並查看每種操作類型的最小、最大和平均時間（或大小）。

開始之前

- 你有"特定存取權限"。
- 你必須擁有 `Passwords.txt`文件。
- 您必須知道主管理節點的 IP 位址。

關於此任務

這 `audit-sum`主管理節點上提供的工具總結了記錄了多少寫入、讀取和刪除操作以及這些操作花費了多長時間。

這 `audit-sum`該工具主要供技術支援人員在故障排除操作期間使用。加工 `audit-sum`查詢會消耗大量 CPU 能力，這可能會影響StorageGRID操作。

此範例顯示了 `audit-sum`工具。此範例顯示了協定操作花費了多長時間。

```
  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
```

這 `audit-sum`此工具為稽核日誌中的以下 S3、Swift 和 ILM 稽核訊息提供計數和時間。

> 由於功能已被棄用，因此審計代碼已從產品和文件中刪除。如果您遇到此處未列出的審計代碼，請檢查此主題的先前版本以了解較舊的 SG 版本。例如， "StorageGRID 11.8 使用稽核總和工具文檔" 。

程式碼	描述	參考
伊德爾	ILM 啟動的刪除：記錄 ILM 啟動刪除物件的過程的時間。	"IDEL：ILM 發起的刪除"
斯德勒	S3 DELETE：記錄成功刪除物件或儲存桶的交易。	"SDEL：S3 刪除"
星載衛星	S3 GET：記錄檢索物件或列出儲存桶中物件的成功交易。	"SGET：S3 獲取"
乳木果	S3 HEAD：記錄成功的事務以檢查物件或儲存桶是否存在。	"乳木果：S3 頭"
噴管	S3 PUT：記錄建立新物件或儲存桶的成功交易。	"噴口：S3 放置"
WDEL	Swift DELETE：記錄成功刪除物件或容器的交易。	"WDEL：快速刪除"
無線獲取	Swift GET：記錄成功的交易以擷取物件或列出容器中的物件。	"WGET：快速獲取"
小麥小麥胚芽萃取物	Swift HEAD：記錄成功的事務以檢查物件或容器是否存在。	"WHEA：Swift HEAD"
西普特	Swift PUT：記錄成功的交易以建立新的物件或容器。	"WPUT：Swift PUT"

這 `audit-sum`工具可以執行以下操作：

- 處理純文字或壓縮的稽核日誌。例如：

```
audit-sum audit.log

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

- 同時處理多個文件。例如：

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

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

- 接受來自管道的輸入，這允許您使用以下方式過濾和預處理輸入 `grep`命令或其他方式。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作為管道輸入。若要處理壓縮文件，請將其檔案名稱作為命令列參數提供，或使用 `zcat`工具先解壓縮檔案。例如：
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

您可以使用命令列選項分別匯總儲存桶上的操作和物件上的操作，或按儲存桶名稱、時間段或目標類型對訊息摘要進行分組。預設情況下，摘要顯示最小、最大和平均操作時間，但您可以使用 `size (-s)`選項來查看物件大小。

使用 `help (-h)`選項來查看可用的選項。例如：

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

步驟

1. 登入主管理節點：
   a. 輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

      當您以 root 身分登入時，提示字元將從 `$`到 `#`。
2. 如果要分析與寫入、讀取、頭部和刪除操作相關的所有訊息，請按照以下步驟操作：
   a. 輸入以下命令，其中 `/var/local/log/audit.log`代表您要分析的檔案的名稱和位置：

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

      此範例顯示了 `audit-sum`工具。此範例顯示了協定操作花費了多長時間。

```
  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
```

在此範例中，SGET（S3 GET）操作平均最慢，為 1.13 秒，但 SGET 和 SPUT（S3 PUT）操作均顯示最壞時間較長，約 1,770 秒。

b. 若要顯示最慢的 10 個檢索操作，請使用 grep 指令僅選擇 SGET 訊息並新增長輸出選項(`-l`) 以包含物件路徑：

```
grep SGET audit.log | audit-sum -l
```

結果包括類型（物件或儲存桶）和路徑，這可讓您在稽核日誌中尋找與這些特定物件相關的其他訊息。

```
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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-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
```

+ 從此範例輸出中，您可以看到三個最慢的 S3 GET 請求針對的物件大小約為 5 GB，這比其他物件大得多。較大的尺寸導致最壞情況下的檢索時間較慢。

3. 如果要確定從網格中提取和檢索的物件的大小，請使用 size 選項(`-s`):

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

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

在此範例中，SPUT 的平均物件大小小於 2.5 MB，但 SGET 的平均大小要大得多。 SPUT 訊息的數量遠高於 SGET 訊息的數量，這表明大多數物件從未被檢索過。

4. 如果您想確定昨天的檢索是否很慢：

   a. 在適當的審計日誌上發出命令並使用按時間分組選項(`-gt`)，後跟時段（例如，15M、1H、10S）：

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

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

這些結果表明，S3 GET 流量在 06:00 至 07:00 之間出現峰值。此時最大時間和平均時間也都相當高，且不會隨著數量的增加而逐漸增加。這表示某個地方的容量已經超出，可能是網路或電網處理請求的能力。

b. 要確定昨天每小時檢索的物件大小，請新增 size 選項(`-s`) 命令：

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

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

這些結果表明，當整體檢索流量達到最大值時，會發生一些非常大的檢索。

c. 要查看更多詳細信息，請使用"審計解釋工具"查看該小時內的所有 SGET 操作：

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

如果預計 grep 命令的輸出會有很多行，請添加 `less`指令一次顯示一頁（一畫面）稽核日誌檔的內容。

5. 如果要確定儲存桶上的 SPUT 操作是否比物件的 SPUT 操作慢：

a. 首先使用 `-go`選項，它將物件和儲存桶操作的訊息分別分組：

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

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

結果表明，針對儲存桶的 SPUT 操作與針對物件的 SPUT 操作具有不同的效能特性。

b. 若要確定哪些 bucket 具有最慢的 SPUT 操作，請使用 `-gb`選項，按儲存桶將訊息分組：

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

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. 若要確定哪些 buckets 具有最大的 SPUT 物件大小，請使用 `-gb`以及 `-s`選項：

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

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

版權資訊

商標資訊