감사 로그 파일 형식

StorageGRID software

NetApp
July 23, 2026

목차

감사 로그 파일 형식

StorageGRID의 감사 로그 파일 형식에 대해 알아보십시오

감사 로그 파일은 모든 관리 노드에서 찾을 수 있으며 개별 감사 메시지 모음을 포함합니다.

각 감사 메시지에는 다음 내용이 포함되어 있습니다.

- ISO 8601 형식으로 감사 메시지(ATIM)를 트리거한 이벤트의 협정 세계시(UTC) 뒤에 공백이 옵니다.

  YYYY-MM-DDTHH:MM:SS.UUUUUU, 여기서 `*UUUUUU*`는 마이크로초입니다.

- 감사 메시지 자체는 대괄호로 묶여 있고 `AUDT`으로 시작합니다.

다음 예시는 감사 로그 파일에 기록된 세 개의 감사 메시지를 보여줍니다(가독성을 위해 줄 바꿈을 추가했습니다). 이 메시지들은 테넌트가 S3 버킷을 생성하고 해당 버킷에 두 개의 객체를 추가했을 때 생성되었습니다.

```
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]]
```

감사 로그 파일의 감사 메시지는 기본 형식으로는 읽거나 해석하기가 쉽지 않습니다. "audit-explain 도구"을 사용하면 감사 로그의 감사 메시지에 대한 간략한 요약을 얻을 수 있습니다. "audit-sum 도구"을 사용하면 기록된 쓰기, 읽기 및 삭제 작업의 수와 각 작업에 소요된 시간을 요약할 수 있습니다.

audit-explain 도구를 사용하여 StorageGRID 감사 메시지를 해석하십시오

이 audit-explain 도구를 사용하면 감사 로그의 감사 메시지를 읽기 쉬운 형식으로 변환할 수

있습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 해당 `Passwords.txt` 파일이 있어야 합니다.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업 정보

기본 관리 노드에서 사용할 수 있는 `audit-explain` 도구는 감사 로그의 감사 메시지에 대한 간략한 요약을 제공합니다.

> 이 `audit-explain` 도구는 주로 기술 지원 문제 해결 작업을 수행하는 동안 사용하도록 설계되었습니다. `audit-explain` 쿼리를 처리하는 동안 상당한 CPU 성능이 소모될 수 있으며, 이는 StorageGRID 운영에 영향을 미칠 수 있습니다.

이 예시는 해당 `audit-explain`도구의 일반적인 출력 결과를 보여줍니다. 이 네 개의 "SPUT"감사 메시지는 계정 ID가 92484777680322627870인 S3 테넌트가 S3 PUT 요청을 사용하여 "bucket1"이라는 버킷을 생성하고 해당 버킷에 세 개의 객체를 추가했을 때 생성되었습니다.

```
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
```

이 `audit-explain` 도구는 다음과 같은 기능을 수행할 수 있습니다.

- 일반 또는 압축된 감사 로그를 처리합니다. 예를 들면 다음과 같습니다.

  ```
  audit-explain audit.log

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

- 여러 파일을 동시에 처리합니다. 예를 들면 다음과 같습니다.

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

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

- 파이프를 통해 입력을 받아 `grep` 명령이나 다른 방법을 사용하여 입력을 필터링하고 전처리할 수 있습니다. 예를 들면 다음과 같습니다.

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

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

감사 로그는 크기가 매우 크고 분석하는 데 시간이 오래 걸릴 수 있으므로 전체 파일 대신 확인하려는 부분을 필터링하고 해당 부분에 대해 `audit-explain`를 실행하면 시간을 절약할 수 있습니다.

> 이 `audit-explain` 도구는 파이프를 통해 압축 파일을 입력받지 않습니다. 압축 파일을 처리하려면 명령줄 인수로 파일 이름을 제공하거나, `zcat` 도구를 사용하여 먼저 파일의 압축을 해제하십시오. 예를 들면 다음과 같습니다.
>
> ```
> zcat audit.log.gz | audit-explain
> ```

`help (-h)` 옵션을 사용하여 사용 가능한 옵션을 확인하십시오. 예를 들면 다음과 같습니다.

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

단계

1. 기본 관리 노드에 로그인합니다.
   a. 다음 명령줄을 입력합니다: `ssh admin@primary_Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.
2. 다음 명령어를 입력하십시오. 여기서 `/var/local/audit/export/audit.log`는 분석하려는 파일의 이름과 위치를 나타냅니다.

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

   이 `audit-explain` 도구는 지정된 파일 또는 파일들에 있는 모든 메시지에 대한 사람이 읽을 수 있는 해석을 출력합니다.

   > 줄 길이를 줄이고 가독성을 높이기 위해 기본적으로 타임스탬프는 표시되지 않습니다. 타임스탬프를 보려면 timestamp (`-t`) 옵션을 사용하십시오.

audit-sum 도구를 사용하여 StorageGRID 감사 메시지를 요약하십시오

이 `audit-sum` 도구를 사용하면 쓰기, 읽기, 헤더 및 삭제 감사 메시지 수를 계산하고 각 작업 유형별 최소, 최대 및 평균 시간(또는 크기)을 확인할 수 있습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- You have the `Passwords.txt` 파일을 가지고 계시네요.
- 기본 관리 노드의 IP 주소를 알고 있습니다.

이 작업 정보

기본 관리 노드에서 사용할 수 있는 `audit-sum` 도구는 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업에 소요된 시간을 요약하여 보여줍니다.

> 이 `audit-sum` 도구는 주로 문제 해결 작업 중 기술 지원에서 사용하도록 설계되었습니다. `audit-sum` 쿼리를 처리하면 많은 양의 CPU 성능이 소모될 수 있으며, 이는 StorageGRID 운영에 영향을 미칠 수 있습니다.

이 예시는 해당 `audit-sum` 도구의 일반적인 출력 결과를 보여줍니다. 이 예시는 프로토콜 작업에 소요된 시간을 보여줍니다.

```
  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
```

이 `audit-sum` 도구는 감사 로그에서 다음 S3 및 ILM 감사 메시지의 수와 시간을 제공합니다.

> 감사 코드는 기능이 더 이상 사용되지 않게 되면 제품 및 설명서에서 제거됩니다. 여기에 나열되지 않은 감사 코드를 발견하면 이전 StorageGRID 릴리스에 대한 이 항목의 이전 버전을 확인하십시오. 예를 들어, "StorageGRID 11.8 감사 합계 도구 사용".

코드	설명	참조하십시오
IDEL	ILM 시작 삭제: ILM이 객체 삭제 프로세스를 시작할 때 로그를 기록합니다.	"IDEL: ILM 시작 삭제"
SDEL	S3 DELETE: 객체 또는 버킷 삭제가 성공적으로 완료된 트랜잭션을 로그에 기록합니다.	"SDEL: S3 DELETE"
SGET	S3 GET: 버킷에서 객체를 검색하거나 객체 목록을 가져오는 성공적인 트랜잭션을 로그에 기록합니다.	"SGET: S3 GET"
SHEA	S3 HEAD: 성공적인 트랜잭션을 기록하여 객체 또는 버킷의 존재 여부를 확인합니다.	"SHEA: S3 HEAD"
SPUT	S3 PUT: 새 객체 또는 버킷을 생성하는 성공적인 트랜잭션을 로그에 기록합니다.	"SPUT: S3 PUT"

이 `audit-sum` 도구는 다음과 같은 기능을 수행할 수 있습니다.

- 일반 또는 압축된 감사 로그를 처리합니다. 예를 들면 다음과 같습니다.

```
audit-sum audit.log

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

- 여러 파일을 동시에 처리합니다. 예를 들면 다음과 같습니다.

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

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

- 파이프를 통해 입력을 받아 `grep` 명령이나 다른 방법을 사용하여 입력을 필터링하고 전처리할 수 있습니다. 예를 들면 다음과 같습니다.

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

grep bucket1 audit.log | audit-sum

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

> 이 도구는 파이프를 통해 압축 파일을 입력받지 않습니다. 압축 파일을 처리하려면 명령줄 인수로 파일 이름을 제공하거나, `zcat` 도구를 사용하여 먼저 파일의 압축을 해제하십시오. 예를 들면 다음과 같습니다.
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

명령줄 옵션을 사용하여 버킷 작업과 객체 작업을 별도로 요약하거나 버킷 이름, 기간 또는 대상 유형별로 메시지 요약을 그룹화할 수 있습니다. 기본적으로 요약에는 최소, 최대 및 평균 작업 시간이 표시되지만, `size (-s)`옵션을 사용하여 객체 크기를 대신 확인할 수도 있습니다.

`help (-h)` 옵션을 사용하여 사용 가능한 옵션을 확인하십시오. 예를 들면 다음과 같습니다.

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

단계

1. 기본 관리 노드에 로그인합니다.
   a. 다음 명령줄을 입력합니다: `ssh admin@primary_Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.
2. 쓰기, 읽기, 헤더 및 삭제 작업과 관련된 모든 메시지를 분석하려면 다음 단계를 따르십시오.

a. 다음 명령어를 입력하십시오. 여기서 `/var/local/audit/export/audit.log`는 분석하려는 파일의 이름과 위치를 나타냅니다.

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

이 예시는 해당 `audit-sum` 도구의 일반적인 출력 결과를 보여줍니다. 이 예시는 프로토콜 작업에 소요된 시간을 보여줍니다.

```
  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
```

이 예시에서 SGET(S3 GET) 작업은 평균 1.13초로 가장 느리지만, SGET 및 SPUT(S3 PUT) 작업 모두 최악의 경우 약 1,770초라는 긴 시간을 보입니다.

b. 가장 느린 10개의 검색 작업을 표시하려면 grep 명령을 사용하여 SGET 메시지만 선택하고 긴 출력 옵션((`-l`)을 추가하여 객체 경로를 포함하십시오.

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

결과에는 유형(객체 또는 버킷)과 경로가 포함되어 있으므로 이러한 특정 객체와 관련된 다른 메시지에 대해 감사 로그를 grep할 수 있습니다.

```
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
```

+ 이 예시 출력에서 볼 수 있듯이, 가장 느린 S3 GET 요청 세 개는 크기가 약 5GB인 객체에 대한 것이었으며, 이는 다른 객체들에 비해 훨씬 큽니다. 이처럼 객체 크기가 크기 때문에 최악의 경우 검색 시간이 느려지는 것입니다.

3. 그리드에 수집되거나 그리드에서 검색되는 객체의 크기를 확인하려면 크기 옵션을 사용하세요((`-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
```

이 예시에서 SPUT의 평균 객체 크기는 2.5MB 미만이지만, SGET의 평균 크기는 훨씬 더 큽니다. SPUT 메시지 수가 SGET 메시지 수보다 훨씬 많다는 것은 대부분의 객체가 검색되지 않는다는 것을 나타냅니다.

4. 어제 검색 속도가 느렸는지 확인하려면 다음 단계를 따르세요.

   a. 해당 감사 로그에 명령을 실행하고 시간별 그룹화 옵션 (`-gt`)을 사용한 후 시간 간격(예: 15M, 1H, 10S)을 지정하십시오.

      ```
      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
```

이 결과는 S3 GET 트래픽이 오전 6시에서 7시 사이에 급증했음을 보여줍니다. 최대 및 평균 처리 시간 모두 이 시간대에 상당히 높았으며, 요청 건수가 증가함에 따라 점진적으로 증가하지 않았습니다. 이러한 지표는 네트워크 용량 또는 그리드의 요청 처리 능력에 문제가 발생하여 용량 초과가 일어났음을 시사합니다.

b. 어제 매시간 어떤 크기의 객체가 검색되었는지 확인하려면 명령에 크기 옵션 (`-s`을 추가하세요.

```
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
```

이러한 결과는 전체 검색 트래픽이 최대치에 달했을 때 매우 큰 규모의 검색이 몇 차례 발생했음을 나타냅니다.

c. 더 자세한 내용을 보려면 "audit-explain 도구"을 사용하여 해당 시간 동안의 모든 SGET 작업을 검토하십시오.

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

grep 명령의 출력 결과가 여러 줄일 것으로 예상되는 경우, `less` 명령을 추가하여 감사 로그 파일의 내용을 한 페이지(한 화면)씩 표시하십시오.

5. 버킷에 대한 SPUT 작업이 객체에 대한 SPUT 작업보다 느린지 확인하려면:

a. 먼저 객체 및 버킷 작업에 대한 메시지를 별도로 그룹화하는 `-go` 옵션을 사용하십시오.

```
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
```

결과에 따르면 버킷에 대한 SPUT 작업은 객체에 대한 SPUT 작업과 성능 특성이 다릅니다.

b. SPUT 작업 속도가 가장 느린 버킷을 확인하려면 메시지를 버킷별로 그룹화하는 `-gb` 옵션을 사용하십시오.

```
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. SPUT 객체 크기가 가장 큰 버킷을 확인하려면 `-gb` 및 `-s` 옵션을 모두 사용하십시오.

```
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
```