



감사 로그 파일 및 메시지 형식 StorageGRID

NetApp
April 10, 2024

목차

감사 로그 파일 및 메시지 형식	1
감사 로그 파일 형식	1
감사 메시지 형식	14

감사 로그 파일 및 메시지 형식

감사 로그를 사용하여 시스템에 대한 정보를 수집하고 문제를 해결할 수 있습니다. 감사 로그 파일의 형식과 감사 메시지에 사용되는 일반 형식을 이해해야 합니다.

감사 로그 파일 형식

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

각 감사 메시지에는 다음이 포함됩니다.

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

'YYYY-MM-DDTHH:MM:SS.UUUUUUU'는 마이크로초입니다.

- 대괄호로 묶인 감사 메시지 자체가 AUDT로 시작하는 메시지입니다.

다음 예제에서는 감사 로그 파일에 포함된 세 가지 감사 메시지를 보여 줍니다(가독성을 위해 줄 바꿈이 추가됨). 이러한 메시지는 테넌트가 S3 버킷을 생성하고 이 버킷에 두 개의 오브젝트를 추가할 때 생성되었습니다.

2019-08-07T18:43:30.247711

[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="] [SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"] [SBAC(CSTR):"s3tenant"] [S3BK(CSTR):"bucket1"] [AVER(UI32):10] [ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT] [ANID(UI32):12454421] [AMID(FC32):S3RQ] [ATID(UI64):7074142142472611085]]

2019-08-07T18:43:30.783597

[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"] [S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"] [S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="] [SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"] [SBAC(CSTR):"s3tenant"] [S3BK(CSTR):"bucket1"] [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(FC32):S3RQ] [ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558

[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"] [S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"] [S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="] [SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"] [SBAC(CSTR):"s3tenant"] [S3BK(CSTR):"bucket1"] [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(FC32):S3RQ] [ATID(UI64):13489590586043706682]]

감사 로그 파일의 감사 메시지는 기본적으로 읽기 또는 해석하기가 쉽지 않습니다. 감사-설명 도구를 사용하면 감사 로그의 감사 메시지 요약물 간단하게 확인할 수 있습니다. '감사 합계' 도구를 사용하여 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업에 소요된 시간을 요약할 수 있습니다.

관련 정보

[감사 설명 도구를 사용합니다](#)

[감사 합계 도구를 사용합니다](#)

감사 설명 도구를 사용합니다

감사-설명 도구를 사용하여 감사 로그의 감사 메시지를 읽기 쉬운 형식으로 변환할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

기본 관리 노드에서 사용할 수 있는 감사 설명 도구는 감사 로그에 감사 메시지를 간단히 요약해 줍니다.



감사-설명 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하기 위한 것입니다. '감사 설명' 쿼리를 처리하면 StorageGRID 작업에 영향을 줄 수 있는 많은 CPU 성능이 소모될 수 있습니다.

이 예는 감사 설명 도구의 일반적인 출력을 보여줍니다. 이러한 4개의 SPUT 감사 메시지는 계정 ID 92484777680322627870이 있는 S3 테넌트가 S3 PUT 요청을 사용하여 "bucket1"이라는 이름의 버킷을 생성하고 해당 버킷에 3개의 오브젝트를 추가할 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
```

감사-설명 도구는 일반 감사 로그 또는 압축 감사 로그를 처리할 수 있습니다. 예를 들면 다음과 같습니다.

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

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

감사-설명 도구는 동시에 여러 파일을 처리할 수도 있습니다. 예를 들면 다음과 같습니다.

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

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

마지막으로, 감사-설명 도구는 파이프에서 입력을 받아 "grep" 명령이나 다른 방법을 사용하여 입력을 필터링하고 미리 처리할 수 있습니다. 예를 들면 다음과 같습니다.

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

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

감사 로그는 매우 크고 구문 분석 속도가 느릴 수 있으므로 전체 파일 대신 파트에 대해 보고 실행할 부분을 필터링하여 시간을 절약할 수 있습니다.



감사 설명 도구는 압축된 파일을 파이프 입력 파일로 받아들이지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 "zcat" 도구를 사용하여 먼저 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

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

사용 가능한 옵션을 보려면 도움말(-h) 옵션을 사용하십시오. 예를 들면 다음과 같습니다.

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

단계

1. 기본 관리자 노드에 로그인합니다.
 - a. 'ssh admin@primary_Admin_Node_IP' 명령을 입력합니다
 - b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 다음 명령을 입력합니다. 여기서 '/var/local/audit/export/audit.log'는 분석할 파일의 이름과 위치를 나타냅니다.

```
'$audit-exit/var/local/audit/export/audit.log'
```

감사-설명 도구는 지정된 파일 또는 파일의 모든 메시지에 대해 사람이 읽을 수 있는 해석을 인쇄합니다.



선 길이를 줄이고 가독성을 높이기 위해 타임스탬프가 기본적으로 표시되지 않습니다. 타임스탬프를 보려면 timestamp("-t") 옵션을 사용합니다.

관련 정보

[SPUT: S3 PUT](#)

감사 합계 도구를 사용합니다

'Audit-sum' 툴을 사용하면 감사 메시지 쓰기, 읽기, 헤드 및 삭제 횟수를 세고 각 작업 유형에 대한 최소, 최대 및 평균 시간(또는 크기)을 확인할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.

- "passwords.txt" 파일이 있어야 합니다.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

기본 관리 노드에서 사용할 수 있는 감사 합계 도구는 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업이 소요된 시간을 요약합니다.



감사 합계 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하도록 설계되었습니다. '감사 합계' 쿼리를 처리하면 많은 CPU 성능이 소모되어 StorageGRID 작업에 영향을 줄 수 있습니다.

이 예에서는 '감사 합계' 도구의 일반적인 출력을 보여 줍니다. 이 예에서는 프로토콜 작업이 얼마나 오래 걸렸는지 보여 줍니다.

```

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

```

"감사 합계" 도구는 감사 로그에 다음 S3, Swift 및 ILM 감사 메시지의 수와 시간을 제공합니다.

코드	설명	을 참조하십시오
ARCT	클라우드 계층에서 아카이브 검색 - 계층	ARCT: 클라우드 계층에서 아카이브 검색
ASCT	Archive Store Cloud - Tier 를 선택합니다	ASCT: Archive Store Cloud - Tier(아카이브 저장소 클라우드 - 계층)
IDEL	ILM에서 삭제 시작: ILM이 개체 삭제 프로세스를 시작할 때 기록합니다.	IDEL: ILM 삭제 시작
SDEL	S3 삭제: 오브젝트 또는 버킷을 삭제하기 위해 트랜잭션을 성공적으로 기록합니다.	SDEL: S3 삭제
SGET	S3 GET: 성공적인 트랜잭션을 로그하여 객체를 검색하거나 버킷의 오브젝트를 나열합니다.	SGET: S3 GET

코드	설명	을 참조하십시오
세어	S3 HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 버킷의 존재 여부를 확인합니다.	Shea: S3 헤드
SPUT	S3 PUT: 새 오브젝트 또는 버킷을 생성하기 위한 성공적인 트랜잭션을 기록합니다.	SPUT: S3 PUT
WDEL	Swift DELETE(빠른 삭제): 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너를 삭제합니다.	WDEL: Swift 삭제
윅입니다	Swift GET: 성공한 트랜잭션을 로그하여 객체를 검색하거나 컨테이너의 객체를 나열합니다.	wget: Swift get
WHEA	Swift HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너의 존재를 확인합니다.	WHEA: 스윙프트 헤드
WPUT	Swift PUT: 새 개체 또는 컨테이너를 생성하기 위해 트랜잭션을 성공적으로 기록합니다.	WPUT: Swift Put

감사 합계 도구는 일반 감사 로그 또는 압축 감사 로그를 처리할 수 있습니다. 예를 들면 다음과 같습니다.

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

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

감사 합계 도구는 동시에 여러 파일을 처리할 수도 있습니다. 예를 들면 다음과 같습니다.

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

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

마지막으로, 감사 합계 도구는 파이프에서 입력을 받아 "grep" 명령이나 다른 방법을 사용하여 입력을 필터링하고 미리 처리할 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 압축된 파일을 파이프된 입력으로 허용하지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 "zcat" 도구를 사용하여 먼저 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

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

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

명령줄 옵션을 사용하여 객체에 대한 작업과 별도로 버킷 작업을 요약하거나 버킷 이름, 기간 또는 목표 유형별로 메시지 요약을 그룹화할 수 있습니다. 기본적으로 요약에는 최소, 최대 및 평균 작동 시간이 표시되지만 '크기(-s)' 옵션을 사용하여 개체 크기를 확인할 수 있습니다.

사용 가능한 옵션을 보려면 도움말(-h) 옵션을 사용하십시오. 예를 들면 다음과 같습니다.

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

단계

1. 기본 관리자 노드에 로그인합니다.
 - a. 'ssh admin@primary_Admin_Node_IP' 명령을 입력합니다
 - b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 쓰기, 읽기, 헤드 및 삭제 작업과 관련된 모든 메시지를 분석하려면 다음 단계를 수행하십시오.
 - a. 다음 명령을 입력합니다. 여기서 '/var/local/audit/export/audit.log'는 분석할 파일의 이름과 위치를 나타냅니다.

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

이 예에서는 '감사 합계' 도구의 일반적인 출력을 보여 줍니다. 이 예에서는 프로토콜 작업이 얼마나 오래 걸렸는지 보여 줍니다.

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			

이 예에서 SGET(S3 GET) 작업은 평균 1.13초 동안 가장 느리지만, SGET 및 SPUT(S3 PUT) 작업은 모두 1,770초 정도의 긴 최악의 경우를 나타냅니다.

- b. 가장 느린 10개의 검색 작업을 표시하려면 `grep` 명령을 사용하여 SGET 메시지만 선택하고 긴 출력 옵션('-l')을 추가하여 객체 경로('grep SGET audit.log | audit-sum-l')를 포함시킵니다

결과에 유형(오브젝트 또는 버킷) 및 경로가 포함되어 있어 이러한 특정 오브젝트와 관련된 다른 메시지에 대해 감사 로그를 작성할 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/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

```

+ 이 예제 출력에서 세 개의 가장 느린 S3 GET 요청은 크기가 약 5GB인 오브젝트에 대해 다른 오브젝트보다 훨씬 크다는 것을 알 수 있습니다. 크기가 크면 검색 시간이 느려질 수 있습니다.

3. 그리드에서 인제스트되고 검색되는 오브젝트 크기를 결정하려면 크기 옵션('-s')을 사용합니다.

```
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

이 예에서 SPUT의 평균 개체 크기는 2.5MB 미만이지만 SGET의 평균 크기는 훨씬 큼니다. SPUT 메시지 수가 SGET 메시지 수보다 훨씬 많음을 나타내며, 이는 대부분의 개체가 검색되지 않음을 나타냅니다.

4. 어제 검색 속도가 느리는지 확인하려면:

- 적절한 감사 로그에 명령을 입력하고 GROUP-By-TIME 옵션('-GT')을 사용한 다음 기간(예: 15M, 1H, 10S)을 사용합니다.

```
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

이러한 결과는 S3이 06:00에서 07:00 사이에 트래픽이 증가하는 것을 보여줍니다. 최대 시간과 평균 시간도 이 시기에 상당히 높으면서, 수가 증가할수록 점차 증가하지는 않았습니다. 이는 네트워크 또는 그리드의 요청 처리 능력 중 어느 곳보다 용량이 초과된 것을 의미합니다.

b. 어제 매시간 검색되는 개체의 크기를 확인하려면 명령에 size 옵션('-s')을 추가합니다.

```
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

이러한 결과는 전체 검색 트래픽이 최대값일 때 매우 큰 검색 결과가 발생했음을 나타냅니다.

c. 자세한 내용을 보려면 '감사 설명' 도구를 사용하여 해당 시간 동안 모든 SGET 작업을 검토하십시오.

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

grep 명령의 출력이 여러 줄로 예상되는 경우 "less" 명령을 추가하여 감사 로그 파일의 내용을 한 번에 한 페이지(한 화면)씩 표시합니다.

5. 버킷의 SPUT 작업이 개체에 대한 SPUT 작업보다 느리는지 확인하려면 다음을 수행합니다.

a. 먼저 오브젝트 및 버킷 작동을 위해 개별적으로 메시지를 그룹화하는 '-go' 옵션을 사용합니다.

```
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

결과는 버킷에 대한 SPUT 작업의 성능 특성이 객체에 대한 SPUT 작업과 다르다는 것을 보여줍니다.

- b. 어떤 버킷이 가장 느린 SPUT 작업을 가지는지 확인하려면 버킷별로 메시지를 그룹화하는 '-GB' 옵션을 사용합니다.

```
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.ldt002 0.361	1564563	0.011	51.569

- c. SPUT 객체 크기가 가장 큰 버킷을 결정하려면 '-GB'와 '-s' 옵션을 모두 사용합니다.

```
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.ltd002 0.352	1564563	0.000	999.972

관련 정보

[감사 설명 도구를 사용합니다](#)

감사 메시지 형식

StorageGRID 시스템 내에서 교환되는 감사 메시지에는 모든 메시지에 공통되는 표준 정보 및 보고되는 이벤트 또는 활동을 설명하는 특정 콘텐츠가 포함됩니다.

감사-설명 및 감사-합계 도구가 제공하는 요약 정보가 부족한 경우 이 섹션을 참조하여 모든 감사 메시지의 일반적인 형식을 파악하십시오.

다음은 감사 로그 파일에 표시될 수 있는 감사 메시지의 예입니다.

```
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]]
```

각 감사 메시지에는 특성 요소의 문자열이 포함됩니다. 전체 문자열은 대괄호("[]")로 묶이고 문자열의 각 특성 요소에는 다음과 같은 특성이 있습니다.

- 괄호 '['로 묶습니다
- 감사 메시지를 나타내는 AUDT 문자열에 의해 도입되었습니다
- 앞 또는 뒤에 구분 기호(침표 또는 공백 없음)를 사용하지 않습니다
- 줄 바꿈 문자 '\n'에 의해 종료되었습니다

각 요소에는 특성 코드, 데이터 형식 및 다음 형식으로 보고된 값이 포함됩니다.


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

메시지의 특성 요소 수는 메시지의 이벤트 유형에 따라 달라집니다. 특성 요소는 특정 순서로 나열되지 않습니다.

다음 목록에서는 특성 요소에 대해 설명합니다.

- ATTR은 보고되는 특성에 대한 4자리 코드입니다. 모든 감사 메시지에 공통적으로 적용되는 일부 특성 및 이벤트별 특성이 있습니다.
- type은 UI64, FC32 등 값의 프로그래밍 데이터 형식의 4자리 식별자입니다. 형식은 괄호 '(')로 묶습니다.
- 값 은 특성의 내용으로 일반적으로 숫자 또는 텍스트 값입니다. 값은 항상 콜론(':')을 따릅니다. CStr 데이터 형식의 값은 큰따옴표 " ""로 둘러싸입니다.

관련 정보

[감사 설명 도구를 사용합니다](#)

[감사 집계 도구를 사용합니다](#)

[감사 메시지](#)

[감사 메시지의 공통 요소](#)

[데이터 유형](#)

[감사 메시지 예](#)

데이터 유형

감사 메시지에 정보를 저장하는 데 사용되는 데이터 유형은 다양합니다.

유형	설명
UI32	부호 없는 긴 정수(32비트). 0에서 4,294,967,295 사이의 숫자를 저장할 수 있습니다.
UI64	부호 없는 이중 긴 정수(64비트). 0에서 18,446,744,073,709,551,615까지의 숫자를 저장할 수 있습니다.
FC32	4자 상수. 32비트 부호 없는 정수 값은 "ABCD"와 같은 4개의 ASCII 문자로 표시됩니다.
아이패드	IP 주소에 사용됩니다.

유형	설명
CStr(문자열)	<p>UTF - 8 문자의 가변 길이 배열입니다. 문자는 다음과 같은 규약을 사용하여 이스케이프할 수 있습니다.</p> <ul style="list-style-type: none"> 백슬래시는 \ 입니다. 캐리지 리턴은 \r 입니다 큰따옴표는 \" 지 않습니다. 라인 피드(새 라인)는 \n 입니다 문자는 해당 16진수 등가물(\xHH 형식으로, 여기서 HH는 문자를 나타내는 16진수 값)로 대체할 수 있습니다.

이벤트 관련 데이터

감사 로그의 각 감사 메시지는 시스템 이벤트와 관련된 데이터를 기록합니다.

메시지 자체를 식별하는 열기 '[AUDT:]' 컨테이너에 이어 다음 속성 집합은 감사 메시지에서 설명하는 이벤트 또는 작업에 대한 정보를 제공합니다. 이러한 특성은 다음 예제에서 강조됩니다.

```
2018-12-05T08:24:45.921845 [AUDT: * \[RSLT\(\FC32\):SUCS\] * \[TIME\(\UI64\):11454\]
\[SAIP\(\iPad\):"10.224.0.100"\)\[S3SStr\S31124562C642S562S564C6100C4S562S564CW5100C6100C6
100C4C4S564C4C4C4C4C4C4CW4S5100C4S562S564S564CW5100C4CW4S562S5100C4S5100C
4C4C4C4C4CW5100C4C4C4C4C6100C6100C6100CWs\S564C4C6100C4C4C4CWs\S564C4C4C4
CWs\S564CWs\S564C4C4S
```

이 예제에서 밑줄이 그어진 ATYP 요소는 메시지를 생성한 이벤트를 식별합니다. 이 예제 메시지에는 S3 헤드 요청에 의해 생성되었음을 나타내는 Shea 메시지 코드([ATYP(FC32):Shea])가 포함됩니다.

관련 정보

[감사 메시지의 공통 요소](#)

[감사 메시지](#)

감사 메시지의 공통 요소

모든 감사 메시지에는 공통 요소가 포함됩니다.

코드	유형	설명
있습니다	FC32	모듈 ID: 메시지를 생성한 모듈 ID의 4자리 식별자입니다. 이것은 감사 메시지가 생성된 코드 세그먼트를 나타냅니다.

코드	유형	설명
ANID	UI32	노드 ID: 메시지를 생성한 서비스에 할당된 그리드 노드 ID입니다. 각 서비스는 StorageGRID 시스템을 구성하고 설치할 때 고유 식별자를 할당합니다. 이 ID는 변경할 수 없습니다.
ASE	UI64	감사 세션 식별자: 이전 릴리즈에서는 이 요소는 서비스가 시작된 후 감사 시스템이 초기화된 시간을 나타냅니다. 이 시간 값은 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정되었습니다. • 참고: * 이 요소는 사용되지 않으며 감사 메시지에 더 이상 나타나지 않습니다.
ASQN	UI64	시퀀스 수: 이전 릴리즈에서는 그리드 노드(ANID)에서 생성된 각 감사 메시지에 대해 이 카운터가 증가했으며 서비스 재시작 시 0으로 재설정됩니다. • 참고: * 이 요소는 사용되지 않으며 감사 메시지에 더 이상 나타나지 않습니다.
ATID	UI64	추적 ID: 단일 이벤트에 의해 트리거된 메시지 집합에서 공유하는 식별자입니다.
ATIM	UI64	Timestamp: 감사 메시지를 트리거한 이벤트가 생성된 시간으로, 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정됩니다. 타임스탬프를 로컬 날짜 및 시간으로 변환하는 데 사용할 수 있는 대부분의 도구는 밀리초를 기반으로 합니다. 로깅된 타임스탬프의 반올림 또는 잘라내기가 필요할 수 있습니다. AUDIT.LOG 파일에서 감사 메시지 시작 부분에 나타나는 사람이 읽을 수 있는 시간은 ISO 8601 형식의 ATIM 속성입니다. 날짜 및 시간은 'YYYY-MMDDTHH:MM:SS.UUUUUUUU'로 표시되며 여기서 T는 날짜 시간 세그먼트의 시작을 나타내는 리터럴 문자열 문자입니다. 'UUUUUUU'는 마이크로초입니다.
ATYP	FC32	이벤트 유형: 기록되는 이벤트의 4자리 식별자입니다. 이는 메시지의 "페이로드" 콘텐츠, 즉 포함된 속성을 제어합니다.
비버	UI32	버전: 감사 메시지의 버전입니다. StorageGRID 소프트웨어가 발전함에 따라 새로운 버전의 서비스에는 감사 보고에 새로운 기능이 포함될 수 있습니다. 이 필드를 사용하면 AMS 서비스의 이전 버전과의 호환성을 통해 이전 버전의 서비스에서 보낸 메시지를 처리할 수 있습니다.
RSLT	FC32	결과: 이벤트, 프로세스 또는 트랜잭션의 결과. 이 메시지와 관련이 없으면 메시지가 실수로 필터링되지 않도록 SUCS 대신 사용되지 않습니다.

감사 메시지 예

각 감사 메시지에서 자세한 정보를 찾을 수 있습니다. 모든 감사 메시지는 동일한 형식을 사용합니다.

다음은 감사 로그 파일에 나타날 수 있는 샘플 감사 메시지입니다.

```
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]]
```

감사 메시지에는 기록되는 이벤트에 대한 정보와 감사 메시지 자체에 대한 정보가 포함되어 있습니다.

감사 메시지에 의해 기록되는 이벤트를 식별하려면 ATYP 속성(아래에 강조 표시됨)을 찾습니다.

```
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 특성의 값은 SPUT입니다. SPUT는 오브젝트 인제스트를 버킷에 기록하는 S3 PUT 트랜잭션을 나타냅니다.

다음 감사 메시지는 객체가 연결된 버킷도 표시합니다.

```
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]]
```

PUT 이벤트가 발생한 시기를 확인하려면 감사 메시지 시작 부분에 UTC(Universal Coordinated Time) 타임스탬프를 기록합니다. 이 값은 감사 메시지 자체의 ATIM 속성:

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]]
```

ATIM은 UNIX epoch 시작 이후 시간(단위: 마이크로초)을 기록합니다. 이 예에서 값 '1405631878959669'는 2014년 7월 17일 목요일 21:17:59 UTC로 변환됩니다.

관련 정보

[SPUT: S3 PUT](#)

[감사 메시지의 공통 요소](#)

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.