



監査ログファイルおよびメッセージの形式

StorageGRID 11.5

NetApp
April 11, 2024

目次

監査ログファイルおよびメッセージの形式	1
監査ログファイルの形式	1
監査メッセージの形式	14

監査ログファイルおよびメッセージの形式

監査ログを使用して、システムに関する情報を収集し、問題のトラブルシューティングを行うことができます。監査ログファイルの形式と、監査メッセージに使用される一般的な形式を理解しておく必要があります。

監査ログファイルの形式

監査ログファイルはすべての管理ノードに存在し、一連の監査メッセージが格納されています。

各監査メッセージには次の情報が含まれます。

- 監査メッセージ（ATIM）をトリガーしたイベントの協定世界時（UTC）を ISO 8601 形式で表した値と、末尾のスペース。

`YYYY-MM-DDTHH:MM:SS.UUUUUU`、ここで `UUUUUU` はマイクロ秒です。

- 監査メッセージ。全体が角かっこで囲まれ、で始まる `AUDT`。

次の例は、監査ログファイル内の 3 つの監査メッセージを示しています（読みやすくするために改行しています）。これらのメッセージは、テナントが S3 バケットを作成し、オブジェクトを 2 つバケットに追加したときに生成されました。

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]]
```

デフォルトの形式のままでは、監査ログファイル内の監査メッセージを読んで解釈するのは簡単ではありません。を使用できます `audit-explain` 監査ログ内の監査メッセージの概要を取得するためのツール。を使用できます `audit-sum` ログに記録された書き込み、読み取り、削除の処理数と、それらの処理に要した時間を表示するツールです。

関連情報

["audit-explainツールの使用"](#)

["audit-sumツールを使用する"](#)

audit-explainツールの使用

を使用できます audit-explain 監査ログ内の監査メッセージをわかりやすい形式に変換するツール。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります Passwords.txt ファイル。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

。 audit-explain ツールはプライマリ管理ノードで使用でき、監査ログ内の監査メッセージの簡単な概要を取得できます。



。 audit-explain ツールは、主にトラブルシューティング処理の際にテクニカルサポートが使用することを目的としています。処理中です audit-explain クエリは大量のCPUパワーを消費する可能性があるため、StorageGRID の処理に影響を及ぼす場合があります。

次の例は、からの一般的な出力を示しています audit-explain ツール。4 つの SPUT 監査メッセージが、アカウント ID が 92484777680322627870 の S3 テナントが S3 PUT 要求を使用して「bucket1」という名前のバケットを作成し、バケットにオブジェクトを 3 つ追加したときに生成されました。

```
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 ツールは、プレーン形式または圧縮形式の監査ログを処理できます。例：

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

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

。 audit-explain ツールは、複数のファイルを一度に処理することもできます。例：

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

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

最後に、audit-explain ツールは、パイプからの入力を受け入れます。これにより、を使用して入力をフィルタ処理および前処理できます grep コマンドまたはその他の手段。例：

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

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

監査ログは非常に大きくなり、解析に時間がかかることがあるため、調べる部分や実行する部分をフィルタリングすることで時間を節約できます audit-explain ファイル全体ではなく、部分的に。



。audit-explain ツールは圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイル进行处理するには、ファイル名をコマンドライン引数として指定するか、を使用します zcat 最初にファイルを解凍するツール。例：

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

を使用します help (-h) 使用可能なオプションを表示するためのオプション。例：

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

手順

1. プライマリ管理ノードにログインします。
 - a. 次のコマンドを入力します。ssh admin@primary_Admin_Node_IP
 - b. に記載されているパスワードを入力します Passwords.txt ファイル。
2. 次のコマンドを入力します /var/local/audit/export/audit.log 分析するファイルの名前と場所を表します。

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

。audit-explain ツールは、指定されたファイル内のすべてのメッセージを、判読可能な形式に変換して出力します。



各行を短く読みやすくするために、デフォルトではタイムスタンプは表示されません。タイムスタンプを表示するには、タイムスタンプを使用します (-t) をクリックします。

関連情報

["SPUT : S3 PUT"](#)

audit-sum ツールを使用する

を使用できます audit-sum 書き込み、読み取り、HEAD、削除の各監査メッセージをカウントし、それぞれの処理タイプの最小、最大、平均時間（またはサイズ）を表示するツールです。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります Passwords.txt ファイル。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

。 audit-sum ツールはプライマリ管理ノードで使用でき、ログに記録された書き込み、読み取り、削除の処理数と、それらの処理に要した時間を取得できます。



。 audit-sum ツールは、主にトラブルシューティング処理の際にテクニカルサポートが使用することを目的としています。処理中です audit-sum クエリは大量のCPUパワーを消費する可能性があるため、StorageGRID の処理に影響を及ぼす場合があります。

次の例は、からの一般的な出力を示しています audit-sum ツール。この例は、プロトコル処理に要した時間を示しています。

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			

。 audit-sum ツールは、監査ログ内の次のS3、Swift、およびILM監査メッセージの数と時間を取得します。

コード	説明	を参照してください
ARCT	アーカイブをクラウド階層から取得します	"ARCT : クラウド階層からアーカイブを取得します"
▽ SCT。△	アーカイブストア - クラウド階層	"ASCT : アーカイブストアのクラウド階層"

コード	説明	を参照してください
IDEL	ILM Initiated Delete : ILM がオブジェクトを削除する処理を開始すると記録されます。	"IDEL : ILM Initiated Delete"
SDEL	S3 DELETE : オブジェクトまたはバケットを削除するトランザクションの成功をログに記録します。	"SDEL : S3 DELETE"
SGET	S3 GET : バケット内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。	"SGET : S3 GET"
Shea	S3 HEAD : オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。	"Shea : S3 ヘッド"
SPUT	S3 PUT : オブジェクトまたはバケットを新規に作成するトランザクションの成功をログに記録します。	"SPUT : S3 PUT"
WDEL	Swift DELETE : オブジェクトまたはコンテナを削除するトランザクションの成功をログに記録します。	"WDEL : Swift の削除"
wget	Swift GET : コンテナ内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。	"wget : Swift GET"
WHEA	Swift HEAD : オブジェクトまたはコンテナの存在を確認するトランザクションの成功をログに記録します。	"WHEA : Swift ヘッド"
WPUT	Swift PUT : オブジェクトまたはコンテナを新規に作成するトランザクションの成功をログに記録します。	"WPUT : Swift PUT"

。 `audit-sum` ツールは、プレーン形式または圧縮形式の監査ログを処理できます。例：

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

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

。 `audit-sum` ツールは、複数のファイルを一度に処理することもできます。例：


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

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

最後に、audit-sum ツールは、パイプからの入力を受け入れることもできます。これにより、を使用して、入力をフィルタ処理および前処理できます grep コマンドまたはその他の手段。例：

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

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

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



このツールは、圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイルを処理するには、ファイル名をコマンドライン引数として指定するか、を使用します zcat 最初にファイルを解凍するツール。例：

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

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

コマンドラインオプションを使用して、バケットに対する処理をオブジェクトに対する処理とは別にまとめたり、メッセージの概要をバケット名、期間、ターゲットタイプ別にグループ化したりできます。デフォルトでは、概要には最小、最大、平均の処理時間が表示されますが、を使用することもできます size (-s) オブジェクトサイズを表示するオプションです。

を使用します help (-h) 使用可能なオプションを表示するためのオプション。例：

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

手順

1. プライマリ管理ノードにログインします。
 - a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
 - b. に記載されているパスワードを入力します Passwords.txt ファイル。
2. 書き込み、読み取り、HEAD、削除の処理に関連するすべてのメッセージを分析するには、次の手順を実行します。

- a. 次のコマンドを入力します `/var/local/audit/export/audit.log` 分析するファイルの名前と場所を表します。

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

次の例は、からの一般的な出力を示しています `audit-sum` ツール。この例は、プロトコル処理に要した時間を示しています。

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			

この例では、平均処理時間では SGET (S3 GET) 処理が 1.13 秒と最も長い一方で、最大処理時間では SGET 処理と SPUT (S3 PUT) 処理がどちらも約 1、770 秒と一番長くなっています。

- b. 最も時間がかかった読み出し処理を10件表示するには、`grep`コマンドを使用してSGETメッセージのみを選択し、`long`出力オプションを追加します (`-l`) オブジェクトパスを含めるには：`grep SGET audit.log | audit-sum -l`

結果にはタイプ (オブジェクトまたはバケット) とパスが含まれます。この情報を使用して、監査ログを `grep` してこれらのオブジェクトに関連する他のメッセージを出力できます。

```

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

```

+ この出力例からは、最も時間がかかった 3 個の S3 GET 要求が、他のオブジェクトよりもはるかに大きい約 5GB のオブジェクトに対して実行されたことがわかります。サイズが大きいと、最悪の場合の読み出し時間が長くなります。

3. グリッドに取り込まれているオブジェクトとグリッドから読み出されているオブジェクトのサイズを特定するには、size オプションを使用します (-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

この例では、SPUT の平均オブジェクトサイズは 2.5MB 未満ですが、SGET の平均サイズははるかに大きいことがわかります。SPUT メッセージの数は SGET メッセージの数よりもはるかに多く、ほとんどのオブジェクトが読み出されていないことを示しています。

4. 昨日の読み出しに時間がかかっていないかどうかを確認するには、次の手順を実行
 - a. 該当する監査ログに対してコマンドを問題 処理し、group-by-time オプションを使用します (-gt) に続けて期間 (例: 15M、1H、10S) を指定します。

```
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

上記の結果は、06：00と07：00の間にS3 GETトラフィックが急増したことを示しています。この時間帯は最大時間と平均時間も大幅に長くなっており、データの増加に伴って徐々に長くなっているわけではありません。このことから、ネットワークまたはグリッドによる要求の処理能力のどこかでキャパシティを超えた可能性があります。

- b. どのサイズのオブジェクトが前日に読み出されていたかを1時間単位で確認するには、sizeオプションを追加します (-s) をコマンドに追加します。

```
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

この結果から、読み出しトラフィックの量が最大に達したときに、非常に大容量の読み出しが発生したことがわかります。

- c. 詳細を確認するには、を使用します `audit-explain` その時間にすべてのSGET処理を確認するためのツール：

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

`grep` コマンドの出力が多く行になると予想される場合は、を追加します `less` 監査ログファイルの内容を一度に1ページ（1画面）表示するコマンド。

- 5. バケットに対する SPUT 処理にオブジェクトに対する SPUT 処理よりも時間がかかっているかどうかを確認するには、次の手順を実行します。

- a. 最初にを使用します `-go` オプション。オブジェクト処理とバケット処理でメッセージをグループ化します。

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

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

上記の結果から、バケットに対する SPUT 処理とオブジェクトに対する SPUT 処理でパフォーマンス特性が異なることがわかります。

- b. SPUT処理に最も時間がかかっているバケットを特定するには、を使用します `-gb` オプション。バケットごとにメッセージをグループ化します。

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

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

- c. SPUTオブジェクトのサイズが最も大きいバケットを特定するには、両方を使用します `-gb` および `-s` オプション：

```
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

関連情報

["audit-explain"ツールの使用](#)

監査メッセージの形式

StorageGRID システム内でやり取りされる監査メッセージには、すべてのメッセージに共通の標準情報と、報告対象のイベントまたはアクティビティを説明する固有のコンテンツが含まれます。

によって提供された概要情報の場合 `audit-explain` および `audit-sum` ツールで十分ではありません。すべての監査メッセージの一般的な形式を把握するには、このセクションを参照してください。

以下は、監査ログファイルに記録されている監査メッセージの例です。

```
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]]
```

各監査メッセージには、一連の属性要素で構成されます。文字列全体が角かっこで囲まれます ([])、および文字列内の各属性要素には、次の特性があります。

- 角かっこで囲まれています []
- 文字列で導入されます `AUDT` を指定します
- 前後に区切り記号（カンマやスペース）がない
- 改行文字で終了します \n

各要素には、次の形式で報告される属性コード、データ型、および値が含まれます。


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

メッセージ内の属性要素の数は、メッセージのイベントタイプによって異なります。属性要素は特定の順序でリストされません。

次に、属性要素について説明します。

- ATTR は、報告される属性の4文字のコードです。すべての監査メッセージに共通する属性とイベント固有の属性があります。
- type は、UI64、FC32など、値のプログラミングデータ型の4文字の識別子です。タイプはかっこで囲まれます ()。
- value は属性の内容で、通常は数値またはテキスト値です。値の前には常にコロンが付きます (:)。データタイプCSTRの値は二重引用符で囲まれます " "。

関連情報

["audit-explain"ツールの使用](#)

["audit-sum"ツールを使用する](#)

["監査メッセージ"](#)

["監査メッセージの共通要素"](#)

["データ型"](#)

["監査メッセージの例"](#)

データ型

監査メッセージ内の情報の格納にはさまざまなデータタイプが使用されます。

を入力します	説明
UI32	符号なし長整数（32ビット）。0~4、294、967、295の数値を格納できます。
UI64	符号なし倍精度長整数（64ビット）。0~18、446、744、073、709、551、615の数値を格納できます。
FC32	4文字の定数。"ABCD"などの4つのASCII文字で表される32ビットの符号なし整数値です。
iPad	IPアドレスに使用されます。

を入力します	説明
CSTR	<p>UTF-8 文字の可変長アレイです。文字は次の方法でエスケープできます。</p> <ul style="list-style-type: none"> • バックスラッシュは \\。 • 復帰文字は \r です • 二重引用符は \" • 改行（新しい行）は \n です • 文字は、それぞれに相当する 16 進数に置き換えることができます（\xHH の形式、HH は該当する文字を表す 16 進値）。

イベント固有のデータ

監査ログ内の各監査メッセージはシステムイベントに固有のデータを記録します。

開口部に続いて [AUDT: メッセージ自体を識別するコンテナ。次の一連の属性は、監査メッセージによって記述されるイベントまたはアクションに関する情報を提供します。以下の例では、これらの属性を強調表示しています。

```
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_Nc8SO1H6w3w0nCOFCGgk_E6dYzKlumRsKJA==" ]*
`*[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]* ` []
[SBAI (CSTR) : "60025621595611246499"] [SBAC (CSTR) : "account"] [S3BK (CSTR) : "bucket"] []
`*[S3KY(CSTR):"object"] [CBID(UI64):0xCC128B9B9E428347]* ` [] [UUID (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 要素（この例では下線付き）は、メッセージを生成したイベントを識別します。この例のメッセージには、SHEA メッセージコード（[ATYP (FC32) : SHEA]）が含まれています。これは、成功した S3 HEAD 要求によってメッセージが生成されたことを示します。

関連情報

["監査メッセージの共通要素"](#)

["監査メッセージ"](#)

監査メッセージの共通要素

すべての監査メッセージには、共通の要素が含まれています。

コード	を入力します	説明
AMid	FC32	Module ID : メッセージを生成したモジュールの 4 文字の識別子。これは、監査メッセージが生成されたコードセグメントを示します。
ANID	UI32	Node ID : メッセージを生成したサービスに割り当てられたグリッドノード ID。各サービスには、StorageGRID システムの設定およびインストール時に一意の識別子が割り当てられます。この ID は変更できません。
ASES	UI64	Audit Session Identifier : 以前のリリースでは、この要素はサービスの開始後に監査システムが初期化された時間を示していました。この時間値は、オペレーティングシステムのエPOCH (1970 年 1 月 1 日 00 : 00 : 00 UTC) からのマイクロ秒数で計測されていました。 • 注 : * この要素は廃止され、監査メッセージには表示されなくなりました。
ASQN	UI64	Sequence Count : 以前のリリースでは、このカウンタはグリッドノード (ANID) 上で監査メッセージが生成されるたびに増分し、サービスの再起動時にゼロにリセットされていました。 • 注 : * この要素は廃止され、監査メッセージには表示されなくなりました。
ATID	UI64	Trace ID : 1 つのイベントによってトリガーされた一連のメッセージで共有される識別子。
ATIM	UI64	Timestamp : 監査メッセージをトリガーしたイベントが生成された時刻。オペレーティングシステムのエPOCH (1970 年 1 月 1 日 00 : 00 : 00 UTC) からのマイクロ秒数で計測されます。タイムスタンプをローカルの日時に変換するためのツールは、ほとんどがミリ秒に基づいています。 ログに記録されたタイムスタンプの丸めや切り捨てが必要な場合があります。の監査メッセージの先頭に表示される、人間が判読できる時間 <code>audit.log file</code> は、ISO 8601形式のATIM属性です。日付と時刻はの形式で表示されます <code>YYYY-MMDDTHH:MM:SS.UUUUUU`</code> を参照してください `T` は、日付の時間セグメントの先頭を示すリテラル文字です。 <code>UUUUUU</code> はマイクロ秒です。
ATYP	FC32	Event Type : ログに記録されるイベントの 4 文字の識別子。これは、メッセージの「ペイロード」コンテンツ、つまり含まれる属性を管理します。
バージョン	UI32	Version : 監査メッセージのバージョン。StorageGRID ソフトウェアのバージョンアップに伴い、新しいバージョンのサービスによって新しい機能が監査レポートに組み込まれる可能性があります。このフィールドは、旧バージョンのサービスのメッセージを処理できるよう、AMS サービスにおける下位互換性を可能にします。
RSLT	FC32	Result : イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、誤ってフィルタリングされないように SUCS ではなく NONE が使用されます。

監査メッセージの例

各監査メッセージには詳細な情報が含まれています。監査メッセージはすべて同じ形式です。

に表示される監査メッセージの例を次に示します audit.log ファイル：

```
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]]
```

監査メッセージには、記録されたイベントに関する情報と、監査メッセージ自体に関する情報が含まれていません。

監査メッセージによって記録されているイベントは、ATYP 属性（以下で強調表示されている部分）で識別します。

```
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 属性の値は SPUT です。SPUT は S3 PUT トランザクションを表し、バケットへのオブジェクトの取り込みをログに記録します。

次の監査メッセージは、オブジェクトが関連付けられているバケットも示しています。

```
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 イベントがいつ発生したかを調べるには、監査メッセージの先頭の世界標準時（UTC）のタイムスタンプを確認します。この値は、監査メッセージ自体の ATIM 属性を判読可能な形式で表したものです。

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 は、UNIX エポックの開始時点からの時間をマイクロ秒数で記録します。この例では、の値を指定します 1405631878959669 2014年7月17日（木）21：17：59 UTCに変換されます。

関連情報

["SPUT : S3 PUT"](#)

["監査メッセージの共通要素"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。