



監査ログを確認する StorageGRID software

NetApp
December 03, 2025

目次

監査ログを確認する	1
監査メッセージとログ	1
監査メッセージフローと保持	1
監査メッセージフロー	1
アクセス監査ログファイル	4
監査ログファイルのローテーション	5
監査ログファイルの形式	5
監査ログファイルの形式	5
監査説明ツールを使用する	7
監査合計ツールを使用する	8
監査メッセージの形式	18
監査メッセージの形式	18
データ型	19
イベント固有のデータ	19
監査メッセージの共通要素	20
監査メッセージの例	21
監査メッセージとオブジェクトのライフサイクル	23
監査メッセージはいつ生成されますか?	23
オブジェクト取り込みトランザクション	23
オブジェクト削除トランザクション	25
オブジェクト取得トランザクション	26
メタデータ更新メッセージ	29
監査メッセージ	30
監査メッセージの説明	30
監査メッセージのカテゴリ	31
監査メッセージの参照	35

監査ログを確認する

監査メッセージとログ

これらの手順には、StorageGRID監査メッセージと監査ログの構造と内容に関する情報が含まれています。この情報を使用して、システム アクティビティの監査証跡を読み取って分析できます。

これらの手順は、StorageGRIDシステムの監査メッセージの分析を必要とするシステム アクティビティと使用状況のレポートを作成する責任を持つ管理者を対象としています。

テキスト ログ ファイルを使用するには、管理ノードで構成された監査共有にアクセスできる必要があります。

監査メッセージレベルの設定と外部Syslogサーバの使用については、以下を参照してください。["監査メッセージとログの保存先を構成する"](#)。

監査メッセージフローと保持

すべてのStorageGRIDサービスは、通常のシステム操作中に監査メッセージを生成します。これらの監査メッセージがStorageGRIDシステムを経由してどのように移動するかを理解する必要があります。`audit.log`ファイル。

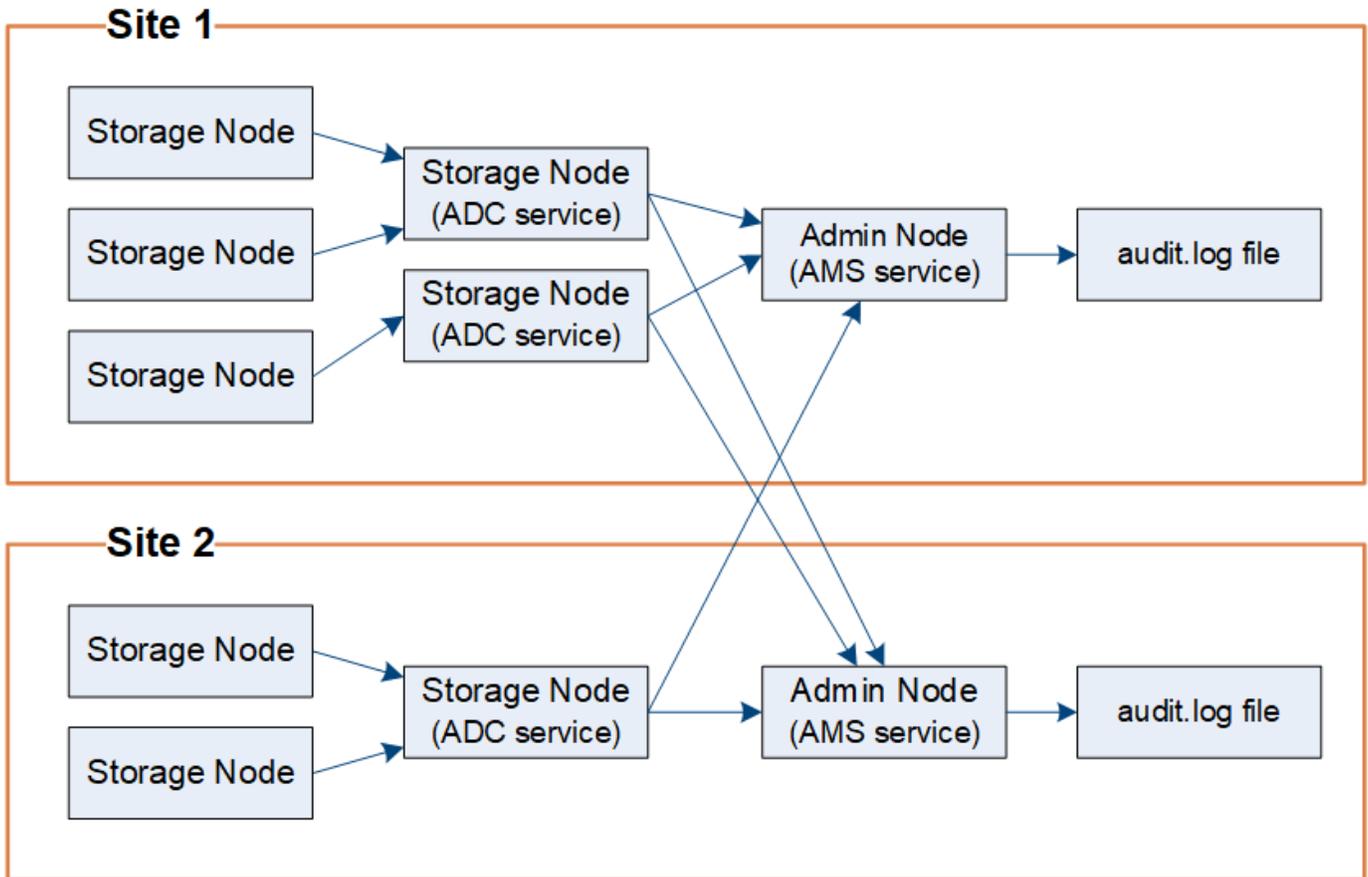
監査メッセージフロー

監査メッセージは、管理ノードと、管理ドメイン コントローラ (ADC) サービスを持つストレージ ノードによって処理されます。

監査メッセージ フロー図に示されているように、各StorageGRIDノードは、データ センター サイトのADCサービスの1つに監査メッセージを送信します。ADC サービスは、各サイトにインストールされた最初の3つのストレージ ノードに対して自動的に有効になります。

次に、各ADC サービスはリレーとして機能し、監査メッセージのコレクションをStorageGRIDシステム内のすべての管理ノードに送信します。これにより、各管理ノードにシステム アクティビティの完全な記録が提供されます。

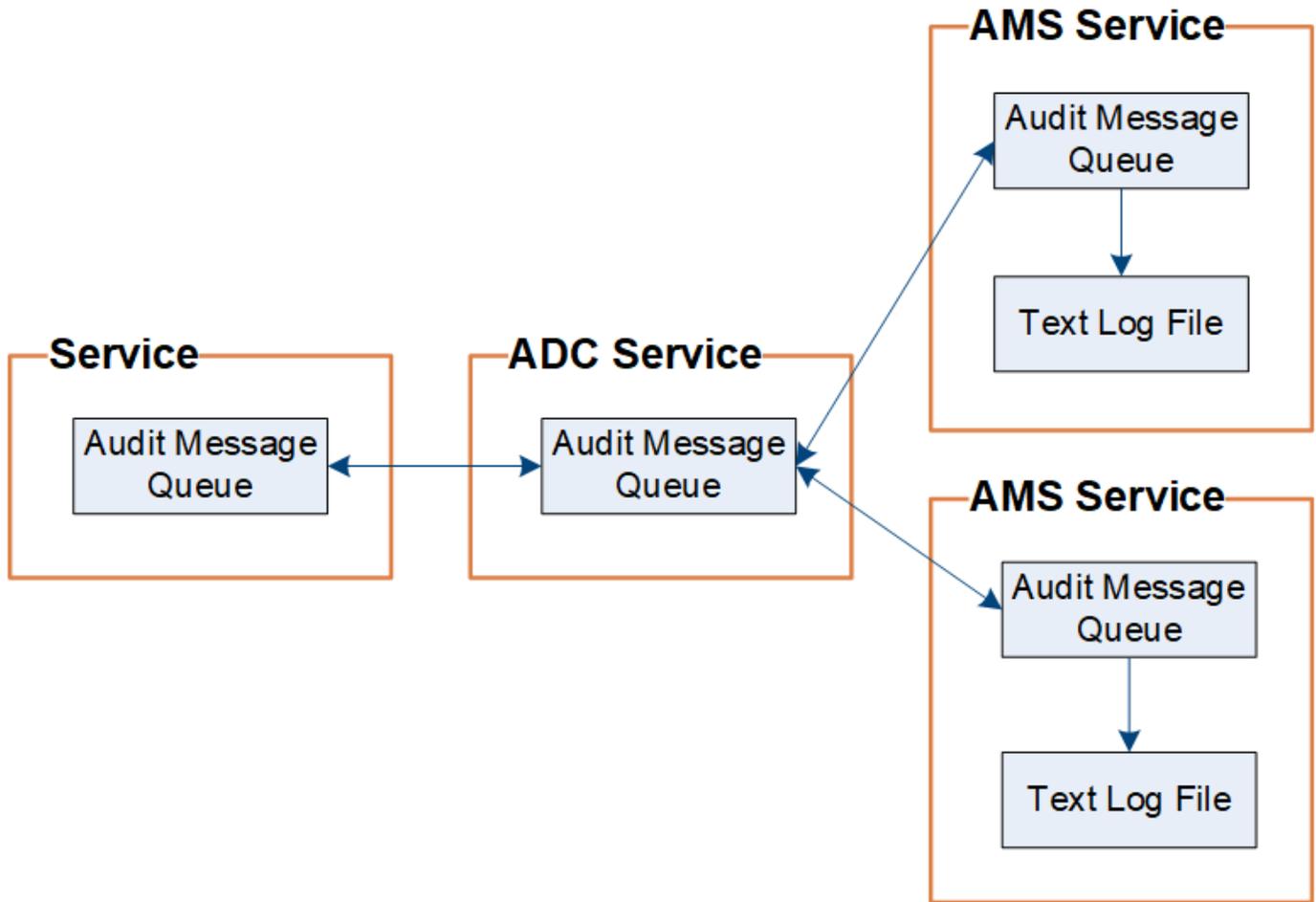
各管理ノードは監査メッセージをテキストログファイルに保存します。アクティブなログファイルの名前は `audit.log`。



監査メッセージの保持

StorageGRID はコピーおよび削除のプロセスを使用して、監査メッセージが監査ログに書き込まれる前に失われないようにします。

ノードが監査メッセージを生成または中継すると、そのメッセージはグリッド ノードのシステム ディスク上の監査メッセージ キューに格納されます。メッセージのコピーは、管理ノードの監査ログファイルにメッセージが書き込まれるまで、常に監査メッセージキューに保持されます。`/var/local/log`ディレクトリ。これにより、転送中に監査メッセージが失われるのを防ぐことができます。



ネットワーク接続の問題や監査容量の不足により、監査メッセージ キューが一時的に増加する場合があります。キューが増加すると、各ノードの利用可能なスペースをより多く消費するようになります。`/var/local/`ディレクトリ。問題が解決せず、ノードの監査メッセージ ディレクトリがいっぱいになると、個々のノードはバックログの処理を優先し、一時的に新しいメッセージを処理できなくなります。

具体的には、次のような動作が見られる場合があります。

- もし `/var/local/log` 管理ノードが使用するディレクトリがいっぱいになると、ディレクトリがいっぱいではなくなるまで、管理ノードは新しい監査メッセージに使用できないというフラグが付けられます。S3 クライアント要求は影響を受けません。監査リポジトリに到達できない場合、XAMS (到達不能監査リポジトリ) アラームがトリガーされます。
- もし `/var/local/` ADC サービスを使用するストレージ ノードによって使用されるディレクトリが 92% いっぱいになると、ディレクトリが 87% いっぱいになるまで、ノードは監査メッセージに使用できないというフラグが付けられます。他のノードへの S3 クライアント要求は影響を受けません。監査リレーに到達できない場合、NRLY (使用可能な監査リレー) アラームがトリガーされます。



ADCサービスに利用可能なストレージノードがない場合、ストレージノードは監査メッセージをローカルに保存します。`/var/local/log/localaudit.log`ファイル。

- もし `/var/local/` ストレージノードが使用するディレクトリが85%いっぱいになると、ノードはs3クライアントのリクエストを拒否し始めます。`503 Service Unavailable`。

次の種類の問題により、監査メッセージ キューが非常に大きくなる可能性があります。

- ADC サービスを備えた管理ノードまたはストレージ ノードの停止。システムのノードの 1 つがダウンすると、残りのノードがバックログになる可能性があります。
- システムの監査能力を超える持続的なアクティビティ レート。
- その `/var/local/` 監査メッセージとは関係のない理由で、ADC ストレージ ノードのスペースがいっぱいになります。このような状況が発生すると、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログを優先するため、他のノードでバックログが発生する可能性があります。

大規模な監査キューアラートと監査メッセージキュー (AMQS) アラーム

監査メッセージ キューのサイズを長期にわたって監視できるように、ストレージ ノード キューまたは管理ノード キュー内のメッセージ数が特定のしきい値に達すると、**Large audit queue** アラートと従来の AMQS アラームがトリガーされます。

大きな監査キュー アラートまたは従来の AMQS アラームがトリガーされた場合は、まずシステムの負荷を確認します。最近大量のトランザクションが発生している場合は、アラートとアラームは時間の経過とともに解決されるため、無視できます。

アラートまたはアラームが継続して発生し、重大度が増す場合は、キュー サイズのグラフを表示します。数時間または数日にわたってその数が着実に増加している場合は、監査負荷がシステムの監査能力を超えている可能性があります。クライアント書き込みとクライアント読み取りの監査レベルをエラーまたはオフに変更して、クライアント操作率を下げるか、ログに記録される監査メッセージの数を減らします。見る["監査メッセージとログの保存先を構成する"](#)。

重複メッセージ

StorageGRIDシステムは、ネットワークまたはノードの障害が発生した場合に保守的なアプローチを採用します。このため、監査ログに重複したメッセージが存在する可能性があります。

アクセス監査ログファイル

監査シェアにはアクティブな `audit.log` ファイルおよび圧縮された監査ログ ファイル。管理ノードのコマンド ラインから監査ログ ファイルに直接アクセスできます。

開始する前に

- あなたが持っている["特定のアクセス権限"](#)。
- あなたは `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを知っておく必要があります。

手順

1. 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. 記載されているパスワードを入力してください `Passwords.txt` ファイル。
 - c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
 - d. 記載されているパスワードを入力してください `Passwords.txt` ファイル。

ルートとしてログインすると、プロンプトは `$` に `#`。

2. 監査ログ ファイルが含まれているディレクトリに移動します。

```
cd /var/local/log
```

3. 必要に応じて、現在の監査ログ ファイルまたは保存された監査ログ ファイルを表示します。

監査ログファイルのローテーション

監査ログファイルは管理ノードの `/var/local/log`` ディレクトリ。アクティブな監査ログファイルの名前は ``audit.log`。



必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る["監査メッセージとログの保存先を構成する"](#)。

1日1回、アクティブ `audit.log`` ファイルが保存され、新しい ``audit.log`` ファイルが開始されます。保存されたファイルの名前は、保存された日時を示し、``yyyy-mm-dd.txt`。1日に複数の監査ログが作成される場合、ファイル名にはファイルが保存された日付に数字が付加され、次の形式になります。`yyyy-mm-dd.txt.n`。例えば、``2018-04-15.txt``そして ``2018-04-15.txt.1``これらは、2018年4月15日に作成され保存された最初のログ ファイルと2番目のログ ファイルです。

1日後、保存されたファイルは圧縮され、名前が変更され、形式は次のようになります。`yyyy-mm-dd.txt.gz`、元の日付が保持されます。時間が経つにつれて、管理ノード上の監査ログに割り当てられたストレージが消費されることとなります。スクリプトは監査ログのスペース消費を監視し、必要に応じてログ ファイルを削除して、`/var/local/log``ディレクトリ。監査ログは作成日に基づいて削除され、最も古いものから順に削除されます。次のファイルでスクリプトのアクションを監視できます。

```
`/var/local/log/manage-audit.log。
```

この例では、アクティブな `audit.log`` ファイル、前日のファイル (``2018-04-15.txt`)、および前日の圧縮ファイル (`2018-04-14.txt.gz`)。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

監査ログファイルの形式

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上に存在し、個々の監査メッセージのコレクションが含まれています。

各監査メッセージには次の内容が含まれます。

- 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 形式で示し、その後にスペースを1つ入力します。

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

- 監査メッセージ自体は角括弧で囲まれ、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が追加されています)。これらのメッセージは、テナントが S3 バケットを作成し、そのバケットに2つのオブジェクトを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] [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]]
```

デフォルトの形式では、監査ログ ファイル内の監査メッセージは読みやすく解釈しにくいものです。使用する

ることができます"[監査説明ツール](#)"監査ログ内の監査メッセージの簡略化された要約を取得します。使用することができます"[監査合計ツール](#)"記録された書き込み、読み取り、削除操作の数と、これらの操作にかかった時間を要約します。

監査説明ツールを使用する

使用することができます `audit-explain` 監査ログ内の監査メッセージを読みやすい形式に変換するツール。

開始する前に

- あなたが持っている"[特定のアクセス権限](#)"。
- あなたは `Passwords.txt` ファイル。
- プライマリ管理ノードの IP アドレスを知っておく必要があります。

タスク概要

その `audit-explain` プライマリ管理ノードで利用可能なツールは、監査ログ内の監査メッセージの簡略化された概要を提供します。



その `audit-explain` このツールは主に、トラブルシューティング操作中にテクニカル サポートが使用することを目的としています。処理 `audit-explain` クエリは大量の CPU パワーを消費する可能性があり、StorageGRID の操作に影響を与える可能性があります。

この例は、`audit-explain` 道具。これら4つ"[吐き出す](#)"アカウント ID 92484777680322627870 の S3 テナントが S3 PUT リクエストを使用して「bucket1」という名前のバケットを作成し、そのバケットに3つのオブジェクトを追加したときに、監査メッセージが生成されました。

```
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
```

その `audit-explain` このツールは次のことができます。

- プレーンまたは圧縮された監査ログを処理します。例えば：

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

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

- 複数のファイルを同時に処理します。例えば：

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

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

- パイプからの入力を受け入れ、入力をフィルタリングしたり前処理したりすることができます。`grep`命令またはその他の手段。例えば：

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

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

監査ログは非常に大きく、解析に時間がかかるため、確認したい部分をフィルタリングして実行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、部分ごとに行います。



その`audit-explain`ツールはパイプ入力として圧縮ファイルを受け入れません。圧縮ファイルを処理するには、コマンドライン引数としてファイル名を指定するか、`zcat`まずファイルを解凍するツールです。例えば：

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

使用`help (-h)`利用可能なオプションを表示するには、オプションを選択します。例えば：

```
$ 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. 記載されているパスワードを入力してください`Passwords.txt`ファイル。
 - c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
 - d. 記載されているパスワードを入力してください`Passwords.txt`ファイル。

ルートとしてログインすると、プロンプトは`\$`に`#`。

2. 次のコマンドを入力します。`/var/local/log/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/log/audit.log
```

その`audit-explain`このツールは、指定されたファイル内のすべてのメッセージの人間が読める形式の解釈を出力します。



行の長さを短くし、読みやすくするために、タイムスタンプはデフォルトでは表示されません。タイムスタンプを確認したい場合は、タイムスタンプを使用してください`(-t)`オプション。

監査合計ツールを使用する

使用することができます`audit-sum`書き込み、読み取り、ヘッド、削除の監査メッセージをカウントし、各操作タイプの最小時間、最大時間、平均時間(またはサイズ)を確認するツール。

開始する前に

- あなたが持っている"[特定のアクセス権限](#)".
- あなたは `Passwords.txt` ファイル。
- プライマリ管理ノードの IP アドレスを知っておく必要があります。

タスク概要

その `audit-sum` プライマリ管理ノードで利用可能なツールは、ログに記録された書き込み、読み取り、削除操作の数と、これらの操作にかかった時間を要約します。



その `audit-sum` このツールは主に、トラブルシューティング操作中にテクニカル サポートが使用することを目的としています。処理 `audit-sum` クエリは大量の CPU パワーを消費する可能性があります、StorageGRID の操作に影響を与える可能性があります。

この例は、`audit-sum` 道具。この例では、プロトコル操作にかかった時間を示します。

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			

その `audit-sum` このツールは、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提供します。



機能が廃止されると、監査コードは製品およびドキュメントから削除されます。ここに記載されていない監査コードが発生した場合は、このトピックの以前のバージョンで古い SG リリースを確認してください。例："[StorageGRID 11.8 監査合計ツールの使用に関するドキュメント](#)"。

コード	説明	参照
アイデル	ILM による削除の開始: ILM がオブジェクトの削除プロセスを開始したときにログに記録します。	" IDEL: ILM による削除開始 "
SDEL	S3 DELETE: オブジェクトまたはバケットを削除する成功したトランザクションをログに記録します。	" SDEL: S3 削除 "

コード	説明	参照
SGET	S3 GET: オブジェクトを取得したり、バケット内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。	"SGET: S3 ゲット"
シア	S3 HEAD: オブジェクトまたはバケットの存在を確認するために成功したトランザクションをログに記録します。	"シア: S3ヘッド"
吐き出す	S3 PUT: 新しいオブジェクトまたはバケットを作成するための成功したトランザクションをログに記録します。	"スプット: S3 プット"
WDEL	Swift DELETE: オブジェクトまたはコンテナを削除する成功したトランザクションをログに記録します。	"WDEL: 迅速な削除"
WGET	Swift GET: オブジェクトを取得したり、コンテナ内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。	"WGET: Swift GET"
ウィー	Swift HEAD: オブジェクトまたはコンテナの存在を確認するために成功したトランザクションをログに記録します。	"WHEA: Swift HEAD"
WPUT	Swift PUT: 新しいオブジェクトまたはコンテナを作成するための成功したトランザクションをログに記録します。	"WPUT: Swift PUT"

その `audit-sum` このツールは次のことができます。

- プレーンまたは圧縮された監査ログを処理します。例えば：

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

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

- 複数のファイルを同時に処理します。例えば：

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

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

- パイプからの入力を受け入れ、入力をフィルタリングしたり前処理したりすることができます。`grep` 命令またはその他の手段。例えば：

```
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、パイプ入力として圧縮ファイルを受け入れません。圧縮ファイルを処理するには、コマンドライン引数としてファイル名を指定するか、`zcat`まずファイルを解凍するツールです。例えば：

```
audit-sum audit.log.gz

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

コマンドライン オプションを使用すると、オブジェクトの操作とは別にバケットの操作を要約したり、バケット名、期間、またはターゲット タイプごとにメッセージの概要をグループ化したりできます。デフォルトでは、要約には最小、最大、平均操作時間が表示されますが、`size (-s)`代わりにオブジェクトのサイズを確認するオプション。

使用 `help (-h)` 利用可能なオプションを表示するには、オプションを選択します。例えば：

```
$ 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. 記載されているパスワードを入力してください `Passwords.txt` ファイル。
- c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
- d. 記載されているパスワードを入力してください `Passwords.txt` ファイル。

ルートとしてログインすると、プロンプトは `\$` に `#`。

2. 書き込み、読み取り、ヘッド、削除操作に関連するすべてのメッセージを分析する場合は、次の手順に従います。

- a. 次のコマンドを入力します。 `/var/local/log/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/log/audit.log
```

この例は、`audit-sum` 道具。この例では、プロトコル操作にかかった時間を示します。

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、SGET (S3 GET) 操作の平均時間が 1.13 秒で最も遅いですが、SGET 操作と SPUT (S3 PUT) 操作はどちらも最悪で約 1,770 秒という長い時間を示しています。

- b. 最も遅い10件の取得操作を表示するには、grepコマンドを使用してSGETメッセージのみを選択し、長い出力オプションを追加します。(-l)を使用してオブジェクトパスを含めます。

```
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) とパスが含まれるため、監査ログで grep を実行して、これらの特定のオブジェクトに関連する他のメッセージを検索できます。

```

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、最も遅い3つのS3 GETリクエストは、サイズが約5GBのオブジェクトに対するものであり、他のオブジェクトよりもはるかに大きいことがわかります。サイズが大きいと、最悪の場合、取得時間が遅くなります。

3. グリッドに取り込まれるオブジェクトのサイズとグリッドから取得されるオブジェクトのサイズを決定するには、サイズ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 2.5 MB 未満ですが、SGET の平均サイズははるかに大きくなります。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取得されないことを示しています。

- 4. 昨日の取得が遅かったかどうかを判断したい場合:
 - a. 適切な監査ログに対してコマンドを発行し、時間別グループオプションを使用します。(-gt) の後に期間 (例: 15M、1H、10S) を続けます。

```
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

これらの結果は、S3 GET トラフィックが 06:00 から 07:00 の間に急増したことを示しています。これらの時間では、最大時間と平均時間はどちらもかなり長くなっており、カウントが増加しても徐々に増加することはありません。これは、ネットワークまたはグリッドのリクエスト処理能力のどこかで容量が超過したことを示しています。

- b. 昨日1時間ごとに取得されたオブジェクトのサイズを確認するには、サイズ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

これらの結果は、全体的な検索トラフィックが最大になったときに、非常に大規模な検索がいくつか発生したことを示しています。

c. さらに詳しく見るには、["監査説明ツール"](#)その時間中のすべての SGET 操作を確認します。

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

grep コマンドの出力が複数行になることが予想される場合は、`less` 監査ログ ファイルの内容を一度に 1 ページ (1 画面) ずつ表示するコマンド。

5. バケットに対する SPUT 操作がオブジェクトに対する SPUT 操作よりも遅いかどうかを確認するには、次の手順を実行します。

a. まずは `go` オブジェクト操作とバケット操作のメッセージを個別にグループ化するオプション:

```
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			

結果は、バケットに対する SPUT 操作は、オブジェクトに対する SPUT 操作とは異なるパフォーマンス特性を持つことを示しています。

b. SPUT操作が最も遅いバケットを特定するには、`-gb`メッセージをバケットごとにグループ化するオプション:

```
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、`-gb`そして`-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

監査メッセージの形式

監査メッセージの形式

StorageGRIDシステム内で交換される監査メッセージには、すべてのメッセージに共通する標準情報と、報告されるイベントまたはアクティビティを説明する特定のコンテンツが含まれます。

提供された概要情報が"[監査説明](#)"そして"[監査合計](#)"ツールだけでは不十分な場合は、このセクションを参照して、すべての監査メッセージの一般的な形式を理解してください。

以下は、監査ログ ファイルに表示され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(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

各監査メッセージには、属性要素の文字列が含まれています。文字列全体が括弧で囲まれている([])であり、文字列内の各属性要素には次の特性があります。

- 括弧内 []
- 文字列によって導入 `AUDT` 監査メッセージを示す
- 前後に区切り文字（カンマやスペースなし）なし
- 改行文字で終了する \n

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

```
[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ていません。

次のリストは、属性要素について説明しています。

- `ATTR` 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` `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。型は括弧で囲まれます `()`。
- `value` 属性の内容であり、通常は数値またはテキスト値です。値は常にコロンの後に続きます (`:`)。データ型 `CSTR` の値は二重引用符 `"` で囲まれます。

データ型

監査メッセージに情報を格納するために、さまざまなデータ型が使用されます。

タイプ	説明
UI32	符号なし長整数 (32 ビット)。0 から 4,294,967,295 までの数値を格納できます。
UI64	符号なし倍精度整数 (64 ビット)。0 から 18,446,744,073,709,551,615 まで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 文字として表される 32 ビットの符号なし整数値。
iPad	IP アドレスに使用されます。
CSTR	UTF-8 文字の可変長配列。文字は次の規則に従ってエスケープできます。 <ul style="list-style-type: none">• バックスラッシュは `\\` です。• キャリッジリターンは `\\r` です。• 二重引用符は `\\"` です。• 改行(新しい行)は `\\n` です。• 文字は、それに相当する 16 進数値 (`\\xHH` 形式、HH は文字を表す 16 進数値) に置き換えることができます。

イベント固有のデータ

監査ログ内の各監査メッセージには、システム イベントに固有のデータが記録されません。

オープニングに続いて `AUDT:`メッセージ自体を識別するコンテナの次の属性セットは、監査メッセージによって記述されたイベントまたはアクションに関する情報を提供します。これらの属性は次の例で強調表示されています。

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT(FC32):SUCS]*
\[TIME(UI64):11454]\[SAIP(IPAD):"10.224.0.100"]\[S3AI(CSTR):"60025621595611246499"]
\[SACC(CSTR):"アカウント"
\[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="
\[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"
\[SBAI(CSTR):"60025621595611246499"]\[SBAC(CSTR):"アカウント"
\[S3BK(CSTR):"バケット"
\[S3KY(CSTR):"オブジェクト"
\[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]
```

その `ATYP` 要素 (例では下線部) は、メッセージを生成したイベントを識別します。このサンプルメッセージには、"シア"メッセージコード ([ATYP(FC32):SHEA])。これは、S3 HEAD 要求が成功したことによって生成されたことを示します。

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	タイプ	説明
真ん中	FC32	モジュール ID: メッセージを生成したモジュール ID 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。
アニド	UI32	ノード 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。StorageGRIDシステムが構成およびインストールされたときに、各サービスに一意的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	監査セッション識別子: 以前のリリースでは、この要素は、サービスの起動後に監査システムが初期化された時刻を示していました。この時間値は、オペレーティング システムのエポック (1970 年 1 月 1 日 00:00:00 UTC) からのマイクロ秒単位で測定されました。 注: この要素は廃止されており、監査メッセージには表示されなくなりました。
ASQN	UI64	シーケンス カウント: 以前のリリースでは、このカウンタはグリッド ノード (ANID) で生成された監査メッセージごとに増加し、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ており、監査メッセージには表示されなくなりました。

コード	タイプ	説明
ATID	UI64	トレース ID: 単一のイベントによってトリガーされたメッセージのセットによって共有される識別子。
アティム	UI64	<p>タイムスタンプ: 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 システムのエポック (1970 年 1 月 1 日 00:00:00 UTC) からのマイクロ秒単位で測定されます。タイムスタンプをローカルの日付と時刻に変換するための利用可能なツールのほとんどは、ミリ秒に基づいていることに注意してください。</p> <p>ログに記録されたタイムスタンプの丸めまたは切り捨てが必要になる場合があります。監査メッセージの冒頭に表示される、人間が読める形式の時刻。audit.log ファイルは ISO 8601 形式の ATIM 属性です。日付と時刻は次のように表されます `YYYY-MMDDTHH:MM:SS.UUUUUU`、ここで `T` 日付の時間セグメントの開始を示すリテラル文字列文字です。`UUUUUU` マイクロ秒です。</p>
ATYP	FC32	イベント タイプ: 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制御します。
アバー	UI32	バージョン: 監査メッセージのバージョン。StorageGRIDソフトウェアが進化するにつれて、新しいバージョンのサービスに監査レポートの新しい機能が組み込まれる可能性があります。このフィールドにより、AMS サービスでの下位互換性が有効になり、古いバージョンのサービスからのメッセージを処理できるようになります。
RSLT	FC32	結果: イベント、プロセス、またはトランザクションの結果。メッセージに関連しない場合は、メッセージが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詳細情報が記載されています。すべての監査メッセージは同じ形式を使用します。

以下は、監査メッセージの例です。`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、記録される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ます。

監査メッセージによって記録されるイベントを識別するには、ATYP 属性 (以下に強調表示) を探します。

```
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。"吐き出す"バケットへのオブジェクトの取り込みを記録する S3 PUT トランザクションを表します。

次の監査メッセージには、オブジェクトが関連付けられているバケットも表示されます。

```
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確認するには、監査メッセージの先頭にある協定世界時 (UTC) のタイムスタンプに注目してください。この値は、監査メッセージ自体の ATIM 属性の人間が読めるバージョンです。

```
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):15792241
44102530435]]
```

ATIM は、UNIX エポックの開始からの時間をマイクロ秒単位で記録します。この例では、値 `1405631878959669` 2014年7月17日木曜日 21:17:59 UTC に翻訳されます。

監査メッセージとオブジェクトのライフサイクル

監査メッセージはいつ生成されますか？

オブジェクトが取り込まれたり、取得されたり、削除されたりするたびに、監査メッセージが生成されます。S3 API 固有の監査メッセージを見つけることで、監査ログでこれらのトランザクションを識別できます。

監査メッセージは、各プロトコルに固有の識別子を通じてリンクされます。

プロトコル	コード
S3操作のリンク	S3BK (バケット)、S3KY (キー)、またはその両方
Swift操作のリンク	WCON (コンテナ)、WOBJ (オブジェクト)、またはその両方
内部業務の連携	CBID (オブジェクトの内部識別子)

監査メッセージのタイミング

グリッド ノード間のタイミングの違い、オブジェクトのサイズ、ネットワークの遅延などの要因により、さまざまなサービスによって生成される監査メッセージの順序は、このセクションの例に示されている順序と異なる場合があります。

オブジェクト取り込みトランザクション

S3 API 固有の監査メッセージを見つけることで、監査ログでクライアントの取り込みトランザクションを識別できます。

取り込みトランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。取り込みトランザクションのトレースに必要なメッセージのみが含まれます。

S3 取り込み監査メッセージ

コード	Name	説明	トレース	詳細については、
吐き出す	S3 PUT トランザクション	S3 PUT 取り込みトランザクションが正常に完了しました。	CBID、S3BK、S3KY	" スプット: S3 プット "
オーム	オブジェクトルールが満たされました	このオブジェクトに対して ILM ポリシーが満たされました。	CBID	" ORLM: オブジェクトルールが満たされました "

Swift の監査メッセージの取り込み

コード	Name	説明	トレース	詳細については、
WPUT	Swift PUT トランザクション	Swift PUT 取り込みトランザクションが正常に完了しました。	CBID、WCORN、WOBJ	"WPUT: Swift PUT"
オーム	オブジェクトルールが満たされました	このオブジェクトに対して ILM ポリシーが満たされました。	CBID	"ORLM: オブジェクトルールが満たされました"

例: S3 オブジェクトの取り込み

以下の一連の監査メッセージは、S3 クライアントがオブジェクトをストレージ ノード (LDR サービス) に取り込むときに生成され、監査ログに保存される監査メッセージの例です。

この例では、アクティブな ILM ポリシーに「2 つのコピーを作成」ILM ルールが含まれています。



以下の例には、トランザクション中に生成されるすべての監査メッセージがリストされているわけではありません。S3 取り込みトランザクション (SPUT) に関連するものだけがリストされます。

この例では、S3 バケットが以前に作成されていることを前提としています。

スプット: S3 プット

SPUT メッセージは、特定のバケットにオブジェクトを作成するために S3 PUT トランザクションが発行されたことを示すために生成されます。

```
2017-07-17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CSTR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:identity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBAC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32):S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: オブジェクトルールが満たされました

ORLM メッセージは、このオブジェクトに対して ILM ポリシーが満たされていることを示します。メッセージには、オブジェクトの CBID と適用された ILM ルールの名前が含まれます。

複製されたオブジェクトの場合、LOCS フィールドにはオブジェクトの場所の LDR ノード ID とボリューム ID が含まれます。

2019-07-

```
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

消失訂正符号化オブジェクトの場合、LOCSフィールドには消失訂正符号化プロファイルIDと消失訂正符号化グループIDが含まれます。

2019-02-23T01:52:54.647537

```
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

PATH フィールドには、使用された API に応じて、S3 バケットとキーの情報、または Swift コンテナとオブジェクトの情報が含まれます。

2019-09-15.txt:2018-01-24T13:52:54.131559

```
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

オブジェクト削除トランザクション

S3 API 固有の監査メッセージを見つけることで、監査ログ内のオブジェクト削除トランザクションを識別できます。

削除トランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。削除トランザクションのトレースに必要なメッセージのみが含まれます。

S3 監査メッセージ削除

コード	Name	説明	トレース	詳細については、
SDEL	S3 削除	バケットからオブジェクトを削除するリクエストが行われました。	CBID、S3KY	"SDEL: S3 削除"

監査メッセージを迅速に削除

コード	Name	説明	トレース	詳細については、
WDEL	迅速な削除	コンテナからオブジェクトまたはコンテナを削除する要求。	CBID、WOBJ	"WDEL: 迅速な削除"

例: S3 オブジェクトの削除

S3 クライアントがストレージ ノード (LDR サービス) からオブジェクトを削除すると、監査メッセージが生成され、監査ログに保存されます。



削除トランザクション中に生成されるすべての監査メッセージが以下の例にリストされているわけではありません。S3 削除トランザクション (SDEL) に関連するものだけがリストされません。

SDEL: S3 削除

オブジェクトの削除は、クライアントが LDR サービスに DeleteObject 要求を送信すると開始されます。メッセージには、オブジェクトを削除するバケットと、オブジェクトを識別するために使用されるオブジェクトの S3 キーが含まれています。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBA
C(CSTR):"test"]\[S3BK\CSTR\):"example"\]\[S3KY\CSTR\):"testobject-0-
7"\][CBID(UI64):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP(FC32):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

オブジェクト取得トランザクション

S3 API 固有の監査メッセージを見つけることで、監査ログ内のオブジェクト取得トランザクションを識別できます。

取得トランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。取得トランザクションのトレースに必要なメッセージのみが含まれます。

S3 取得監査メッセージ

コード	Name	説明	トレース	詳細については、
SGET	S3 GET	バケットからオブジェクトを取得する要求が行われました。	CBID、S3BK、S3KY	"SGET: S3 ゲット"

監査メッセージの迅速な取得

コード	Name	説明	トレース	詳細については、
WGET	Swift GET	コンテナからオブジェクトを取得する要求。	CBID、WCON、WOBJ	"WGET: Swift GET"

例: S3 オブジェクトの取得

S3 クライアントがストレージ ノード (LDR サービス) からオブジェクトを取得すると、監査メッセージが生成され、監査ログに保存されます。

以下の例には、トランザクション中に生成されるすべての監査メッセージがリストされているわけではないことに注意してください。S3 取得トランザクション (SGET) に関連するものだけがリストされます。

SGET: S3 ゲット

オブジェクトの取得は、クライアントが LDR サービスに `GetObject` 要求を送信すると開始されます。メッセージには、オブジェクトを取得するバケットと、オブジェクトを識別するために使用されるオブジェクトの S3 キーが含まれています。

```
2017-09-20T22:53:08.782605
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :47807] [SAIP (IPAD) : "10.96.112.26"] [S3AI (CSTR) : "43979298178977966408"] [SACC (CSTR) : "s3-account-a"] [S3AK (CSTR) : "SGKht7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-O_FEw=="] [SUSR (CSTR) : "urn:sgws:identity::43979298178977966408:root"] [SBAI (CSTR) : "43979298178977966408"] [SBAC (CSTR) : "s3-account-a"] \ [S3BK \ (CSTR \) : "bucket-anonymous" \] \ [S3KY \ (CSTR \) : "Hello.txt" \] [CBID (UI64) : 0x83D70C6F1F662B02] [CSIZ (UI64) : 12] [AVER (UI32) : 10] [ATIM (UI64) : 1505947988782605] \ [ATYP \ (FC32 \) : SGET \] [ANID (UI32) : 12272050] [AMID (FC32) : S3RQ] [ATID (UI64) : 17742374343649889669] ]
```

バケット ポリシーで許可されている場合、クライアントは匿名でオブジェクトを取得したり、別のテナントアカウントが所有するバケットからオブジェクトを取得したりできます。監査メッセージにはバケット所有者のテナント アカウントに関する情報が含まれているため、これらの匿名リクエストやアカウント間リクエストを追跡できます。

次のサンプル メッセージでは、クライアントは、自分が所有していないバケットに保存されているオブジェ

クトに対して GetObject リクエストを送信します。SBAI および SBAC の値には、バケット所有者のテナント アカウント ID と名前が記録されます。これは、S3AI および SACC に記録されるクライアントのテナント アカウント ID と名前とは異なります。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\CSTR\):"17915054115450519830"\]\[SACC\CSTR\):"s3-account-
b"\]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls81BUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\CSTR\):"4397929817
8977966408"\]\[SBAC\CSTR\):"s3-account-a"\]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

例: オブジェクトに対する S3 Select

S3 クライアントがオブジェクトに対して S3 Select クエリを発行すると、監査メッセージが生成され、監査ログに保存されます。

以下の例には、トランザクション中に生成されるすべての監査メッセージがリストされているわけではないことに注意してください。S3 Select トランザクション (SelectObjectContent) に関連するものだけがリストされます。

各クエリの結果、2 つの監査メッセージが生成されます。1 つは S3 Select リクエストの承認を実行するメッセージ (S3SR フィールドは「select」に設定されます)、もう 1 つは処理中にストレージからデータを取得する後続の標準 GET 操作です。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"]\[S3AI(CSTR):"63147909414576125820"]\[SACC(CSTR):"Ten
ant1636027116"]\[S3AK(CSTR):"AUFd1XNVZ905F3TW7KSU"]\[SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"]\[SBAI(CSTR):"63147909414576125820"]\[SBA
C(CSTR):"Tenant1636027116"]\[S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"]\[S3KY(CSTR):"SUB-
EST2020_ALL.csv"]\[CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"]\[CSIZ(UI64):0][S3SR(CSTR):"select"]\[AVER(UI32):10][ATIM(UI64)
:1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```

2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\": \"unix:\"}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant16
36027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CST
R):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"] [S3KY(CSTR):"SUB-
EST2020_ALL.csv"] [CBID(UI64):0x0496F0408A721171] [UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"] [CSIZ(UI64):10185581] [MTME(UI64):1636380348695262] [AVER(UI32
):10] [ATIM(UI64):1636385732604886] [ATYP(FC32):SGET] [ANID(UI32):12733063] [A
MID(FC32):S3RQ] [ATID(UI64):16562288121152341130]]

```

メタデータ更新メッセージ

監査メッセージは、S3 クライアントがオブジェクトのメタデータを更新したときに生成されます。

S3 メタデータ更新監査メッセージ

コード	Name	説明	トレース	詳細については、
SUPD	S3 メタデータが更新されました	S3 クライアントが取り込んだオブジェクトのメタデータを更新したときに生成されます。	CBID、S3KY、HTRH	"SUPD: S3 メタデータが更新されました"

例: S3 メタデータの更新

この例では、既存の S3 オブジェクトのメタデータを更新する成功したトランザクションを示します。

SUPD: S3 メタデータの更新

S3クライアントは指定されたメタデータを更新するリクエスト (SUPD) を発行します。(x-amz-meta-*) を S3 オブジェクト (S3KY) 用に作成します。この例では、監査プロトコルヘッダーとして構成されているため (構成 > 監視 > 監査および **syslog** サーバー)、要求ヘッダーは HTRH フィールドに含まれています。見る"[監査メッセージとログの保存先を構成する](#)"。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrDplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

監査メッセージ

監査メッセージの説明

システムによって返される監査メッセージの詳細な説明は、次のセクションに記載されています。各監査メッセージは、まず、メッセージが表すアクティビティのクラス別に関連するメッセージをグループ化したテーブルにリストされます。これらのグループ化は、監査されるアクティビティの種類を理解する場合と、必要な監査メッセージフィルタリングの種類を選択する場合の両方に役立ちます。

監査メッセージも4文字のコードごとにアルファベット順にリストされます。このアルファベット順のリストを使用すると、特定のメッセージに関する情報を見つけることができます。

この章全体で使用される4文字のコードは、次の例メッセージに示すように、監査メッセージで見つかったATYP値です。

```
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):94457363265
00603516]]
```

監査メッセージのレベルの設定、ログの保存先の変更、監査情報用の外部Syslogサーバーの使用については、以下を参照してください。["監査メッセージとログの保存先を構成する"](#)

監査メッセージのカテゴリ

システム監査メッセージ

システム監査カテゴリに属する監査メッセージは、監査システム自体、グリッド ノードの状態、システム全体のタスク アクティビティ (グリッド タスク)、およびサービス バックアップ操作に関連するイベントに使用されます。

コード	メッセージのタイトルと説明	詳細については、
ECMC	消失コード化データ フラグメントの欠落: 消失コード化データ フラグメントの欠落が検出されたことを示します。	"ECMC: 消失符号化データフラグメントの欠落"
ECOC	破損した消去符号化データ フラグメント: 破損した消去符号化データ フラグメントが検出されたことを示します。	"ECOC: 破損した消去符号化データフラグメント"
ETAF	セキュリティ認証に失敗しました: トランスポート層セキュリティ (TLS) を使用した接続試行が失敗しました。	"ETAF: セキュリティ認証に失敗しました"
GNRG	GNDS 登録: サービスがStorageGRIDシステム内で自身の情報を更新または登録しました。	"GNRG: GNDS登録"
グヌール	GNDS 登録解除: サービスがStorageGRIDシステムから登録解除されました。	"GNUR: GNDS 登録解除"
GTED	グリッド タスクが終了しました: CMN サービスはグリッド タスクの処理を終了しました。	"GTED: グリッドタスクが終了しました"
GTST	グリッド タスクが開始されました: CMN サービスがグリッド タスクの処理を開始しました。	"GTST: グリッドタスクが開始されました"
GTSU	グリッド タスクが送信されました: グリッド タスクが CMN サービスに送信されました。	"GTSU: グリッドタスクが送信されました"
LLST	場所の紛失: この監査メッセージは、場所が失われたときに生成されます。	"LLST: 位置情報が失われました"
オルスト	オブジェクトの損失: 要求されたオブジェクトがStorageGRIDシステム内に見つかりません。	"OLST: システムが紛失物体を検出しました"
サッド	セキュリティ監査の無効化: 監査メッセージのログ記録がオフになりました。	"SADD: セキュリティ監査の無効化"

コード	メッセージのタイトルと説明	詳細については、
サデ	セキュリティ監査の有効化: 監査メッセージのログ記録が復元されました。	"SADE: セキュリティ監査の有効化"
SVRF	オブジェクトストア検証失敗: コンテンツブロックが検証チェックに失敗しました。	"SVRF: オブジェクトストア検証失敗"
SVRU	オブジェクトストアの検証が不明です: オブジェクトストアで予期しないオブジェクトデータが検出されました。	"SVRU: オブジェクトストアの検証が不明です"
システム	ノード停止: シャットダウンが要求されました。	"SYSD: ノード停止"
システム	ノードの停止: サービスが正常な停止を開始しました。	"SYST: ノード停止"
シス	ノードの開始: サービスが開始されました。前回のシャットダウンの性質がメッセージに示されます。	"SYSU: ノード開始"

オブジェクトストレージ監査メッセージ

オブジェクトストレージ監査カテゴリに属する監査メッセージは、StorageGRIDシステム内のオブジェクトの保存と管理に関連するイベントに使用されます。これらには、オブジェクトの保存と取得、グリッドノード間の転送、検証が含まれます。



機能が廃止されると、監査コードは製品およびドキュメントから削除されます。ここに記載されていない監査コードが発生した場合は、このトピックの以前のバージョンで古いSGリリースを確認してください。例: "[StorageGRID 11.8 オブジェクトストレージ監査メッセージ](#)"。

コード	説明	詳細については、
ブロル	バケット読み取り専用要求: バケットが読み取り専用モードになったか、読み取り専用モードを終了しました。	"BROR: バケット読み取り専用リクエスト"
CBSE	オブジェクト送信終了: ソースエンティティがグリッドノード間のデータ転送操作を完了しました。	"CBSE: オブジェクト送信終了"
CBRE	オブジェクト受信終了: 宛先エンティティがグリッドノード間のデータ転送操作を完了しました。	"CBRE: オブジェクト受信終了"
CGRR	クロスグリッドレプリケーション要求: StorageGRIDは、グリッドフェデレーション接続内のバケット間でオブジェクトを複製するために、クロスグリッドレプリケーション操作を試行しました。	"CGRR: クロスグリッドレプリケーション要求"

コード	説明	詳細については、
EBDL	空のバケットの削除: ILM スキャナーは、すべてのオブジェクトを削除するバケット内のオブジェクトを削除しました (空のバケット操作を実行しています)。	"EBDL: 空のバケットの削除"
EBKR	空のバケットのリクエスト: ユーザーが空のバケットをオンまたはオフにするリクエスト (つまり、バケット オブジェクトを削除するか、オブジェクトの削除を停止するリクエスト) を送信しました。	"EBKR: 空のバケットリクエスト"
SCMT	オブジェクト ストア コミット: コンテンツ ブロックが完全に保存され、検証されたため、要求できるようになりました。	"SCMT: オブジェクトストアコミット要求"
SREM	オブジェクト ストアの削除: コンテンツ ブロックがグリッド ノードから削除されたため、直接要求できなくなりました。	"SREM: オブジェクトストアの削除"

クライアント読み取り監査メッセージ

S3 クライアント アプリケーションがオブジェクトの取得を要求すると、クライアント読み取り監査メッセージが記録されます。

コード	説明	使用者	詳細については、
S3SL	S3 Select リクエスト: S3 Select リクエストがクライアントに返された後の完了をログに記録します。S3SL メッセージには、エラー メッセージとエラーコードの詳細が含まれる場合があります。リクエストが成功しなかった可能性があります。	S3クライアント	"S3SL: S3 選択リクエスト"
SGET	S3 GET: オブジェクトを取得したり、バケット内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。 注: トランザクションがサブリソースに対して実行される場合、監査メッセージにはフィールド S3SR が含まれます。	S3クライアント	"SGET: S3 ゲット"
シア	S3 HEAD: オブジェクトまたはバケットの存在を確認するために成功したトランザクションをログに記録します。	S3クライアント	"シア: S3ヘッド"
WGET	Swift GET: オブジェクトを取得したり、コンテナ内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。	Swiftクライアント	"WGET: Swift GET"

コード	説明	使用者	詳細については、
ウィー	Swift HEAD: オブジェクトまたはコンテナの存在を確認するために成功したトランザクションをログに記録します。	Swiftクライアント	"WHEA: Swift HEAD"

クライアント書き込み監査メッセージ

S3 クライアント アプリケーションがオブジェクトの作成または変更を要求すると、クライアント書き込み監査メッセージが記録されます。

コード	説明	使用者	詳細については、
オーバーブレイカー	オブジェクトの上書き: あるオブジェクトを別のオブジェクトで上書きするトランザクションを記録します。	S3 および Swift クライアント	"OVWR: オブジェクトの上書き"
SDEL	S3 DELETE: オブジェクトまたはバケットを削除する成功したトランザクションをログに記録します。 注: トランザクションがサブリソースに対して実行される場合、監査メッセージにはフィールド S3SR が含まれます。	S3クライアント	"SDEL: S3 削除"
スpos	S3 POST: AWS Glacier ストレージからクラウド ストレージ プールにオブジェクトを復元する成功したトランザクションをログに記録します。	S3クライアント	"SPOS: S3 ポスト"
吐き出す	S3 PUT: 新しいオブジェクトまたはバケットを作成するための成功したトランザクションをログに記録します。 注: トランザクションがサブリソースに対して実行される場合、監査メッセージにはフィールド S3SR が含まれます。	S3クライアント	"スプット: S3 プット"
SUPD	S3 メタデータの更新: 既存のオブジェクトまたはバケットのメタデータを更新する成功したトランザクションをログに記録します。	S3クライアント	"SUPD: S3 メタデータが更新されました"
WDEL	Swift DELETE: オブジェクトまたはコンテナを削除する成功したトランザクションをログに記録します。	Swiftクライアント	"WDEL: 迅速な削除"
WPUT	Swift PUT: 新しいオブジェクトまたはコンテナを作成するための成功したトランザクションをログに記録します。	Swiftクライアント	"WPUT: Swift PUT"

経営監査メッセージ

管理カテゴリは、管理 API へのユーザー リクエストを記録します。

コード	メッセージのタイトルと説明	詳細については、
MGAU	管理 API 監査メッセージ: ユーザー リクエストのログ。	"MGAU: 経営監査メッセージ"

ILM監査メッセージ

ILM 監査カテゴリに属する監査メッセージは、情報ライフサイクル管理 (ILM) 操作に関連するイベントに使用されます。

コード	メッセージのタイトルと説明	詳細については、
アイデル	ILM による削除の開始: この監査メッセージは、ILM がオブジェクトの削除プロセスを開始したときに生成されます。	"IDEL: ILM による削除開始"
LKCU	上書きされたオブジェクトのクリーンアップ。この監査メッセージは、上書きされたオブジェクトが自動的に削除され、ストレージ領域が解放されたときに生成されます。	"LKCU: 上書きされたオブジェクトのクリーンアップ"
オーム	オブジェクト ルールが満たされました: この監査メッセージは、オブジェクト データが ILM ルールで指定されたとおりに保存されたときに生成されます。	"ORLM: オブジェクトルールが満たされました"

監査メッセージの参照

BROR: バケット読み取り専用リクエスト

LDR サービスは、バケットが読み取り専用モードになったとき、または読み取り専用モードを終了したときに、この監査メッセージを生成します。たとえば、すべてのオブジェクトが削除されている間、バケットは読み取り専用モードになります。

コード	フィールド	説明
BKHD	バケットUUID	バケット ID。
プロブ	バケット読み取り専用リクエスト値	バケットが読み取り専用になるか、読み取り専用状態から抜けるか (1 = 読み取り専用、0 = 読み取り専用ではない)。
ブラザーズ	バケット読み取り専用の理由	バケットが読み取り専用にされる理由、または読み取り専用状態が解除される理由。たとえば、emptyBucket。

コード	フィールド	説明
S3AI	S3テナントアカウントID	リクエストを送信したテナント アカウントの ID。空の値は匿名アクセスを示します。
S3BK	S3バケット	S3 バケット名。

CBRB: オブジェクト受信開始

通常のシステム操作中は、データがアクセスされ、複製され、保持されるにつれて、コンテンツ ブロックは異なるノード間で継続的に転送されます。あるノードから別のノードへのコンテンツ ブロックの転送が開始されると、このメッセージは宛先エンティティによって発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	要求された最初のシーケンス数を示します。成功した場合、転送はこのシーケンス カウントから開始されます。
CTES	予想される終了シーケンス数	要求された最後のシーケンス数を示します。成功した場合、このシーケンス カウントが受信された時点で転送が完了したとみなされます。
RSLT	転送開始ステータス	転送開始時のステータス: SUCS: 転送が正常に開始されました。

この監査メッセージは、コンテンツ ブロック識別子によって識別される単一のコンテンツに対してノード間データ転送操作が開始されたことを意味します。この操作では、「開始シーケンス カウント」から「予想される終了シーケンス カウント」までのデータが要求されます。送信ノードと受信ノードはノード ID によって識別されます。この情報は、システム データ フローを追跡するために使用でき、ストレージ監査メッセージ

と組み合わせてレプリカ数を確認するために使用できます。

CBRE: オブジェクト受信終了

あるノードから別のノードへのコンテンツ ブロックの転送が完了すると、宛先エンティティによってこのメッセージが発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	転送が開始されたシーケンス数を示します。
CTAS	実際の終了シーケンス数	正常に転送された最後のシーケンス数を示します。実際の終了シーケンス数が開始シーケンス数と同じで、転送結果が成功しなかった場合、データは交換されませんでした。
RSLT	転送結果	転送操作の結果 (送信エンティティの観点から) : SUCS: 転送が正常に完了しました。要求されたすべてのシーケンス カウントが送信されました。 CONL: 転送中に接続が失われました CTMO: 確立または転送中に接続がタイムアウトしました UNRE: 宛先ノードIDに到達できません CRPT: 破損または無効なデータを受信したため転送が終了しました

この監査メッセージは、ノード間のデータ転送操作が完了したことを意味します。転送結果が成功した場合、操作によって「開始シーケンス カウント」から「実際の終了シーケンス カウント」にデータが転送されました。送信ノードと受信ノードはノード ID によって識別されます。この情報を使用して、システムのデータフ

ローを追跡し、エラーを特定、表にまとめ、分析することができます。ストレージ監査メッセージと組み合わせると、レプリカ数の検証にも使用できます。

CBSB: オブジェクト送信開始

通常システム操作中は、データがアクセスされ、複製され、保持されるにつれて、コンテンツ ブロックは異なるノード間で継続的に転送されます。あるノードから別のノードへのコンテンツ ブロックの転送が開始されると、ソース エンティティによってこのメッセージが発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	要求された最初のシーケンス数を示します。成功した場合、転送はこのシーケンス カウントから開始されます。
CTES	予想される終了シーケンス数	要求された最後のシーケンス数を示します。成功した場合、このシーケンス カウントが受信された時点で転送が完了したとみなされます。
RSLT	転送開始ステータス	転送開始時のステータス: SUCS: 転送が正常に開始されました。

この監査メッセージは、コンテンツ ブロック識別子によって識別される単一のコンテンツに対してノード間データ転送操作が開始されたことを意味します。この操作では、「開始シーケンス カウント」から「予想される終了シーケンス カウント」までのデータが要求されます。送信ノードと受信ノードはノード ID によって識別されます。この情報は、システム データ フローを追跡するために使用でき、ストレージ監査メッセージと組み合わせてレプリカ数を確認するために使用できます。

CBSE: オブジェクト送信終了

あるノードから別のノードへのコンテンツ ブロックの転送が完了すると、ソース エンテ

ィティによってこのメッセージが発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意的識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意的識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	転送が開始されたシーケンス数を示します。
CTAS	実際の終了シーケンス数	正常に転送された最後のシーケンス数を示します。実際の終了シーケンス数が開始シーケンス数と同じで、転送結果が成功しなかった場合、データは交換されませんでした。
RSLT	転送結果	転送操作の結果 (送信エンティティの観点から) : SUCS: 転送が正常に完了しました。要求されたシーケンス カウントがすべて送信されました。 CONL: 転送中に接続が失われました CTMO: 確立または転送中に接続がタイムアウトしました UNRE: 宛先ノードIDに到達できません CRPT: 破損または無効なデータを受信したため転送が終了しました

この監査メッセージは、ノード間のデータ転送操作が完了したことを意味します。転送結果が成功した場合、操作によって「開始シーケンス カウント」から「実際の終了シーケンス カウント」にデータが転送されました。送信ノードと受信ノードはノード ID によって識別されます。この情報を使用して、システムのデータ フローを追跡し、エラーを特定、表にまとめ、分析することができます。ストレージ監査メッセージと組み合わせると、レプリカ数の検証にも使用できます。

CGRR: クロスグリッドレプリケーション要求

このメッセージは、StorageGRID がグリッド フェデレーション接続内のバケット間でオブジェクトを複製するクロス グリッド レプリケーション操作を試行したときに生成されます。

コード	フィールド	説明
CSIZ	オブジェクトサイズ	オブジェクトのサイズ (バイト)。 CSIZ 属性はStorageGRID 11.8 で導入されました。その結果、StorageGRID 11.7 から 11.8 へのアップグレードにまたがるクロスグリッド レプリケーション要求では、オブジェクトの合計サイズが不正確になる可能性があります。
S3AI	S3テナントアカウントID	オブジェクトの複製元となるバケットを所有するテナント アカウントの ID。
GFID	グリッドフェデレーション接続ID	クロスグリッドレプリケーションに使用されているグリッドフェデレーション接続の ID。
オペラ	CGR操作	試行されたクロスグリッド レプリケーション操作のタイプ: <ul style="list-style-type: none">• 0 = オブジェクトを複製する• 1 = マルチパートオブジェクトを複製する• 2 = 削除マーカを複製する
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。
VSID	バージョン ID	複製されていたオブジェクトの特定のバージョンのバージョン ID。
RSLT	結果コード	成功 (SUCS) または一般エラー (GERR) を返します。

EBDL: 空のバケットの削除

ILM スキャナーは、すべてのオブジェクトを削除するバケット内のオブジェクトを削除しました (空のバケット操作を実行しています)。

コード	フィールド	説明
CSIZ	オブジェクトサイズ	オブジェクトのサイズ (バイト)。

コード	フィールド	説明
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナの UUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
RSLT	削除操作の結果	イベント、プロセス、またはトランザクションの結果。メッセージに関連しない場合は、メッセージが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。

EBKR: 空のバケットリクエスト

このメッセージは、ユーザーが空のバケットをオンまたはオフにする（つまり、バケットオブジェクトを削除するか、オブジェクトの削除を停止する）要求を送信したことを示します。

コード	フィールド	説明
ビルド	バケットUUID	バケット ID。
EBJS	空のバケットのJSON構成	現在の空のバケット構成を表す JSON が含まれます。
S3AI	S3テナントアカウントID	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。

ECMC: 消失符号化データフラグメントの欠落

この監査メッセージは、システムが消失訂正符号化データ フラグメントの欠落を検出したことを示します。

コード	フィールド	説明
VCMC	VCS ID	不足しているチャンクを含む VCS の名前。
MCID	チャンクID	欠落した消去コード化フラグメントの識別子。

コード	フィールド	説明
RSLT	結果	このフィールドの値は「NONE」です。RSLT は必須のメッセージフィールドですが、この特定のメッセージには関係ありません。このメッセージは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。

ECOC: 破損した消去符号化データフラグメント

この監査メッセージは、システムが破損した消去符号化データフラグメントを検出したことを示します。

コード	フィールド	説明
VCCO	VCS ID	破損したチャンクを含む VCS の名前。
VLID	ボリューム ID	破損した消去コード化フラグメントを含む RangeDB ボリューム。
CCID	チャンクID	破損した消去コード化フラグメントの識別子。
RSLT	結果	このフィールドの値は「NONE」です。RSLT は必須のメッセージフィールドですが、この特定のメッセージには関係ありません。このメッセージは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。

ETAF: セキュリティ認証に失敗しました

このメッセージは、トランスポート層セキュリティ (TLS) を使用した接続試行が失敗したときに生成されます。

コード	フィールド	説明
CNID	接続識別子	認証が失敗した TCP/IP 接続の一意的システム識別子。
ルイド	ユーザーID	リモート ユーザーの ID を表すサービス依存の識別子。

コード	フィールド	説明
RSLT	理由コード	<p>失敗の理由：</p> <p>SCNI: 安全な接続の確立に失敗しました。</p> <p>CERM: 証明書が見つかりません。</p> <p>CERT: 証明書が無効でした。</p> <p>CERE: 証明書の有効期限が切れています。</p> <p>CERR: 証明書は取り消されました。</p> <p>CSGN: 証明書の署名が無効です。</p> <p>CSGU: 証明書の署名者が不明です。</p> <p>UCRM: ユーザー資格情報が見つかりません。</p> <p>UCRI: ユーザー資格情報が無効です。</p> <p>UCRU: ユーザー資格情報が許可されませんでした。</p> <p>TOUT: 認証がタイムアウトしました。</p>

TLS を使用する安全なサービスへの接続が確立されると、TLS プロファイルとサービスに組み込まれた追加ロジックを使用して、リモート エンティティの資格情報が検証されます。無効、予期しない、または許可されていない証明書または資格情報のためにこの認証が失敗した場合、監査メッセージが記録されます。これにより、不正なアクセスの試みやその他のセキュリティ関連の接続の問題を照会できるようになります。

このメッセージは、リモート エンティティの構成が誤っているか、無効または許可されていない資格情報をシステムに提示しようとしたことが原因で発生する可能性があります。システムへの不正アクセスの試みを検出するには、この監査メッセージを監視する必要があります。

GNRG: GNDS登録

CMN サービスは、サービスがStorageGRIDシステム内で自身の情報を更新または登録したときに、この監査メッセージを生成します。

コード	フィールド	説明
RSLT	結果	<p>更新リクエストの結果:</p> <ul style="list-style-type: none"> • SUCS: 成功 • SUNV: サービスは利用できません • GERR: その他の障害
GNID	ノードID	更新要求を開始したサービスのノード ID。

コード	フィールド	説明
GNTP	デバイスタイプ	グリッド ノードのデバイス タイプ (たとえば、LDR サービスの場合は BLDR)。
GNDV	デバイスモデルバージョン	DMDL バンドル内のグリッド ノードのデバイス モデル バージョンを識別する文字列。
GNGP	グループ	グリッド ノードが属するグループ (リンク コストとサービス クエリのランキングのコンテキスト)。
グニア	IP アドレス	グリッド ノードの IP アドレス。

このメッセージは、グリッド ノードがグリッド ノード バンドル内のエントリを更新するたびに生成されません。

GNUR: GNDS 登録解除

CMN サービスは、サービスがStorageGRIDシステムから自身に関する情報を登録解除したときに、この監査メッセージを生成します。

コード	フィールド	説明
RSLT	結果	更新リクエストの結果: <ul style="list-style-type: none"> • SUCS: 成功 • SUNV: サービスは利用できません • GERR: その他の障害
GNID	ノードID	更新要求を開始したサービスのノード ID。

GTED: グリッドタスクが終了しました

この監査メッセージは、CMN サービスが指定されたグリッド タスクの処理を完了し、タスクを履歴テーブルに移動したことを示します。結果が SUCS、ABRT、または ROLF の場合、対応するグリッド タスク開始監査メッセージが表示されます。その他の結果は、このグリッド タスクの処理が開始されなかったことを示しています。

コード	フィールド	説明
TSID	タスクID	<p>このフィールドは、生成されたグリッド タスクを一意に識別し、グリッド タスクをそのライフサイクルにわたって管理できるようにします。</p> <p>注: タスク ID は、グリッド タスクが送信されたときではなく、生成されたときに割り当てられます。特定のグリッド タスクが複数回送信される可能性があります。この場合、タスク ID フィールドでは、送信済み、開始済み、および終了済みの監査メッセージを一意にリンクするには不十分です。</p>
RSLT	結果	<p>グリッド タスクの最終ステータス結果:</p> <ul style="list-style-type: none"> • SUCS: グリッド タスクは正常に完了しました。 • ABRT: グリッド タスクはロールバック エラーなしで終了しました。 • ROLF: グリッド タスクが終了し、ロールバック プロセスを完了できませんでした。 • CANC: グリッド タスクは、開始される前にユーザーによってキャンセルされました。 • EXPR: グリッド タスクは開始される前に期限が切れました。 • IVLD: グリッド タスクが無効でした。 • AUTH: グリッド タスクは許可されていません。 • DUPL: グリッド タスクは重複として拒否されました。

GTST: グリッドタスクが開始されました

この監査メッセージは、CMN サービスが指定されたグリッド タスクの処理を開始したことを示します。監査メッセージは、内部グリッド タスク送信サービスによって開始され、自動アクティブ化が選択されたグリッド タスクのグリッド タスク送信メッセージの直後に表示されます。保留テーブルに送信されたグリッド タスクの場合、ユーザーがグリッド タスクを開始したときにこのメッセージが生成されます。

コード	フィールド	説明
TSID	タスクID	<p>このフィールドは、生成されたグリッド タスクを一意に識別し、タスクをそのライフサイクル全体にわたって管理できるようにします。</p> <p>注: タスク ID は、グリッド タスクが送信されたときではなく、生成されたときに割り当てられます。特定のグリッド タスクが複数回送信される可能性があります。この場合、タスク ID フィールドでは、送信済み、開始済み、および終了済みの監査メッセージを一意にリンクするには不十分です。</p>

コード	フィールド	説明
RSLT	結果	結果。このフィールドには1つの値のみが含まれます。 <ul style="list-style-type: none"> • SUCS: グリッド タスクが正常に開始されました。

GTSU: グリッドタスクが送信されました

この監査メッセージは、グリッド タスクが CMN サービスに送信されたことを示します。

コード	フィールド	説明
TSID	タスクID	生成されたグリッド タスクを一意に識別し、タスクをそのライフサイクルにわたって管理できるようにします。 注: タスク ID は、グリッド タスクが送信されたときではなく、生成されたときに割り当てられます。特定のグリッド タスクが複数回送信される可能性があります。この場合、タスク ID フィールドでは、送信済み、開始済み、および終了済みの監査メッセージを一意にリンクするには不十分です。
TTYF	タスクタイプ	グリッド タスクのタイプ。
TVER	タスクバージョン	グリッド タスクのバージョンを示す番号。
TDSC	Task Description	グリッド タスクの人間が読める形式の説明。
VATS	タイムスタンプの有効期限	グリッド タスクが有効になる最も早い時刻 (1970 年 1 月 1 日からの UIN64 マイクロ秒 - UNIX 時間)。
VBTS	有効期限前タイムスタンプ	グリッド タスクが有効な最終時刻 (1970 年 1 月 1 日からの UIN64 マイクロ秒 - UNIX 時間)。
TSRC	ソース	タスクのソース: <ul style="list-style-type: none"> • TXTB: グリッド タスクは、署名されたテキスト ブロックとして StorageGRID システムを通じて送信されました。 • GRID: グリッド タスクは、内部のグリッド タスク送信サービスを通じて送信されました。

コード	フィールド	説明
ACTV	アクティベーションタイプ	アクティベーションの種類: <ul style="list-style-type: none"> • AUTO: グリッド タスクは自動アクティブ化のために送信されました。 • PEND: グリッド タスクが保留中のテーブルに送信されました。これは、TXTB ソースの唯一の可能性です。
RSLT	結果	提出の結果: <ul style="list-style-type: none"> • SUCS: グリッド タスクが正常に送信されました。 • 失敗: タスクは履歴テーブルに直接移動されました。

IDEL: ILM による削除開始

このメッセージは、ILM がオブジェクトの削除プロセスを開始したときに生成されます。

IDEL メッセージは、次のいずれかの状況で生成されます。

- 準拠 **S3** バケット内のオブジェクトの場合: このメッセージは、オブジェクトの保持期間が終了したために ILM がオブジェクトの自動削除プロセスを開始したときに生成されます (自動削除設定が有効になっていて、法的保留がオフになっていると想定)。
- 非準拠の **S3** バケット内のオブジェクトの場合: このメッセージは、アクティブな ILM ポリシー内の配置指示が現在オブジェクトに適用されていないため、ILM がオブジェクトの削除プロセスを開始したときに生成されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	オブジェクトの CBID。
CMPA	コンプライアンス: 自動削除	準拠した S3 バケット内のオブジェクトのみ対象です。0 (false) または 1 (true)。バケットが法的保留中でない限り、準拠オブジェクトを保持期間の終了時に自動的に削除するかどうかを示します。
CMPL	コンプライアンス: 法的保留	準拠した S3 バケット内のオブジェクトのみ対象です。0 (false) または 1 (true)。バケットが現在法的保留中かどうかを示します。
CMPR	コンプライアンス: 保存期間	準拠した S3 バケット内のオブジェクトのみ対象です。オブジェクトの保持期間の長さ (分)。
CTME	コンプライアンス: 取り込み時間	準拠した S3 バケット内のオブジェクトのみ対象です。オブジェクトの取り込み時間。この値に保持期間 (分単位) を追加して、バケットからオブジェクトを削除できるタイミングを決定できます。

コード	フィールド	説明
DMRK	マーカーバージョンIDを削除	バージョン管理されたバケットからオブジェクトを削除するとき作成される削除マーカーのバージョン ID。バケットに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	オブジェクトのサイズ (バイト)。
LOCS	場所	StorageGRIDシステム内のオブジェクト データの保存場所。オブジェクトに場所がない場合 (たとえば、削除されている場合)、LOCS の値は "" になります。 CLEC: 消去コード化オブジェクトの場合、オブジェクトのデータに適用される消去コード化プロファイル ID と消去コード化グループ ID。 CLDI: 複製されたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID。 CLNL: オブジェクト データがアーカイブされている場合のオブジェクトの場所の ARC ノード ID。
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
RSLT	結果	ILM 操作の結果。 SUCS: ILM 操作は成功しました。
ルール	ルールラベル	<ul style="list-style-type: none"> • 準拠 S3 バケット内のオブジェクトが保持期間の期限切れにより自動的に削除されている場合、このフィールドは空白になります。 • 現在オブジェクトに適用されている配置指示がなくなったためにオブジェクトが削除されている場合、このフィールドには、オブジェクトに適用された最後の ILM ルールの判読可能なラベルが表示されます。
SGRP	サイト (グループ)	存在する場合、オブジェクトは指定されたサイトで削除されましたが、そのサイトはオブジェクトが取り込まれたサイトではありません。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	削除されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

LKCU: 上書きされたオブジェクトのクリーンアップ

このメッセージは、ストレージ領域を解放するために以前にクリーンアップが必要だった上書きされたオブジェクトをStorageGRID が削除したときに生成されます。S3 クライアントが、すでにオブジェクトが含まれているパスにオブジェクトを書き込むと、オブジェクトは上書きされます。削除プロセスは自動的にバックグラウンドで実行されません。

コード	フィールド	説明
CSIZ	コンテンツサイズ	オブジェクトのサイズ (バイト)。
LTYP	クリーンアップの種類	社内使用のみ。
ルイド	削除されたオブジェクトのUUID	削除されたオブジェクトの識別子。
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナの UUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
UUID	ユニバーサルユニーク識別子	まだ存在するオブジェクトの識別子。この値は、オブジェクトが削除されていない場合にのみ使用できます。

LKDM: リークされたオブジェクトのクリーンアップ

このメッセージは、リークされたチャンクがクリーンアップまたは削除されたときに生成されます。チャンクは、複製されたオブジェクトまたは消去エンコードされたオブジェクトの一部になることができます。

コード	フィールド	説明
クロック	チャンクの位置	削除されたリークされたチャンクのファイルパス。
CTYP	チャンクタイプ	チャンクの種類: ec: Erasure-coded object chunk repl: Replicated object chunk

コード	フィールド	説明
LTYP	リークタイプ	検出できる漏れの 5 つのタイプ: object_leaked: Object doesn't exist in the grid location_leaked: Object exists in the grid, but found location doesn't belong to object mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment no_parent: Container object is deleted, but object segment was left out and not deleted
CTIM	チャンク作成時間	リークされたチャンクが作成された時刻。
UUID	ユニバーサルユニーク識別子	チャンクが属するオブジェクトの識別子。
CBID	コンテンツブロック識別子	リークされたチャンクが属するオブジェクトの CBID。
CSIZ	コンテンツサイズ	チャンクのサイズ (バイト単位)。

LLST: 位置情報が失われました

このメッセージは、オブジェクト コピー (複製または消去コード化) の場所が見つからない場合に生成されます。

コード	フィールド	説明
CBIL	CBID	影響を受ける CBID。
ECPR	消失訂正符号化プロファイル	消失訂正符号化オブジェクトデータ用。使用される消去コーディングプロファイルの ID。
LTYP	場所の種類	CLDI (オンライン) : 複製されたオブジェクトデータ用 CLEC (オンライン) : 消失訂正符号化オブジェクトデータ用 CLNL (ニアライン) : アーカイブされた複製オブジェクトデータ用

コード	フィールド	説明
ノイド	ソースノードID	場所が失われたノード ID。
PCLD	複製されたオブジェクトへのパス	失われたオブジェクトデータのディスクの場所への完全なパス。LTypの値がCLDIの場合(つまり、複製されたオブジェクトの場合)のみ返されます。 形式は /var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@
RSLT	結果	常になし。RSLTは必須のメッセージフィールドですが、このメッセージには関係ありません。このメッセージが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。
TSRC	トリガーソース	ユーザー: ユーザーがトリガー SYST: システムが起動しました
UUID	ユニバーサルユニークID	StorageGRIDシステム内の影響を受けるオブジェクトの識別子。

MGAU: 経営監査メッセージ

管理カテゴリは、管理APIへのユーザーリクエストを記録します。有効なAPI URIへのGETまたはHEADリクエストではないすべてのHTTPリクエストでは、ユーザー名、IP、およびAPIへのリクエストの種類を含む応答がログに記録されます。無効なAPI URI (/api/v3-authorize など) および有効なAPI URIへの無効なリクエストはログに記録されません。

コード	フィールド	説明
MDIP	宛先IPアドレス	サーバー(宛先)のIPアドレス。
遺伝子組み換えDNA	ドメイン名	ホストドメイン名。
MPAT	Request PATH	リクエストパス。
MPQP	リクエストクエリパラメータ	リクエストのクエリパラメータ。

コード	フィールド	説明
MRBD	リクエスト本文	<p>リクエスト本体の内容。デフォルトではレスポンス本文がログに記録されますが、レスポンス本文が空の場合、特定のケースではリクエスト本文がログに記録されます。次の情報はレスポンス本文では取得できないため、次の POST メソッドのリクエスト本文から取得されます。</p> <ul style="list-style-type: none"> • POST authorize のユーザー名とアカウント ID • POST /grid/grid-networks/update での新しいサブネット構成 • POST /grid/ntp-servers/update の新しい NTP サーバー • POST /grid/servers/decommission 内の廃止されたサーバー ID <p>注: 機密情報は削除されるか (S3 アクセス キーなど)、アスタリスクでマスクされます (パスワードなど)。</p>
MRMD	リクエスト方法	<p>HTTP リクエストメソッド:</p> <ul style="list-style-type: none"> • POST • PUT • DELETE • PATCH
MRSC	応答コード	応答コード。
MRSP	応答の本文	<p>応答の内容 (応答本体) はデフォルトでログに記録されます。</p> <p>注: 機密情報は削除されるか (S3 アクセス キーなど)、アスタリスクでマスクされます (パスワードなど)。</p>
MSIP	送信元IPアドレス	クライアント (送信元) IP アドレス。
ムーン	ユーザーURN	リクエストを送信したユーザーの URN (Uniform Resource Name)。
RSLT	結果	成功 (SUCS) またはバックエンドによって報告されたエラーを返します。

OLST: システムが紛失物体を検出しました

このメッセージは、DDS サービスがStorageGRIDシステム内でオブジェクトのコピーを見つけられない場合に生成されます。

コード	フィールド	説明
CBID	コンテンツブロッック識別子	紛失したオブジェクトの CBID。
ノイド	ノードID	入手可能な場合、紛失した物体の最後の既知の直接位置または近距離位置。ボリューム情報が利用できない場合は、ボリューム ID なしでノード ID のみを持つことが可能です。
パス	S3 バケット/キー	可能な場合は、S3 バケット名と S3 キー名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには関係ありません。このメッセージが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。
UUID	ユニバーサルユークID	StorageGRIDシステム内で失われたオブジェクトの識別子。
ヴォリ	ボリューム ID	利用可能な場合、失われたオブジェクトの最後の既知の場所のストレージノードのボリューム ID。

ORLM: オブジェクトルールが満たされました

このメッセージは、ILM ルールで指定されたとおりにオブジェクトが正常に保存およびコピーされたときに生成されます。



ポリシー内の別のルールがオブジェクト サイズの詳細フィルターを使用している場合、デフォルトの 2 つのコピーを作成するルールによってオブジェクトが正常に保存されても、ORLM メッセージは生成されません。

コード	フィールド	説明
ビルド	バケットヘッダー	バケット ID フィールド。内部操作に使用されます。STAT が PRGD の場合にのみ表示されます。
CBID	コンテンツブロッック識別子	オブジェクトの CBID。
CSIZ	コンテンツサイズ	オブジェクトのサイズ (バイト)。

コード	フィールド	説明
LOCS	場所	StorageGRIDシステム内のオブジェクトデータの保存場所。オブジェクトに場所がない場合（たとえば、削除されている場合）、LOCSの値は "" になります。 CLEC: 消去コード化オブジェクトの場合、オブジェクトのデータに適用される消去コード化プロファイル ID と消去コード化グループ ID。 CLDI: 複製されたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID。 CLNL: オブジェクトデータがアーカイブされている場合のオブジェクトの場所の ARC ノード ID。
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
RSLT	結果	ILM 操作の結果。 SUCS: ILM 操作は成功しました。
ルール	ルールラベル	このオブジェクトに適用された ILM ルールに与えられた、人間が判読できるラベル。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナの UUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
SGCB	コンテナCBID	セグメント化されたオブジェクトのコンテナの CBID。この値は、セグメント化されたオブジェクトとマルチパート オブジェクトに対してのみ使用できます。
統計	ステータス	ILM 操作のステータス。 完了: オブジェクトに対する ILM 操作が完了しました。 DFER: オブジェクトは将来の ILM 再評価の対象としてマークされています。 PRGD: オブジェクトはStorageGRIDシステムから削除されました。 NLOC: オブジェクトデータがStorageGRIDシステム内に見つかりません。このステータスは、オブジェクトデータのすべてのコピーが欠落しているか破損していることを示している可能性があります。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。

コード	フィールド	説明
VSID	バージョン ID	バージョン管理されたバケットに作成された新しいオブジェクトのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

ORLM 監査メッセージは、単一のオブジェクトに対して複数回発行できます。たとえば、次のいずれかのイベントが発生するたびに発行されます。

- オブジェクトの ILM ルールは永久に満たされます。
- このエポックでは、オブジェクトの ILM ルールが満たされています。
- ILM ルールによってオブジェクトが削除されました。
- バックグラウンド検証プロセスにより、複製されたオブジェクト データのコピーが破損していることが検出されます。StorageGRIDシステムは ILM 評価を実行して、破損したオブジェクトを置き換えます。

関連情報

- ["オブジェクト取り込みトランザクション"](#)
- ["オブジェクト削除トランザクション"](#)

OVWR: オブジェクトの上書き

このメッセージは、外部 (クライアントが要求した) 操作によって 1 つのオブジェクトが別のオブジェクトによって上書きされたときに生成されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子 (新規)	新しいオブジェクトの CBID。
CSIZ	前のオブジェクトのサイズ	上書きされるオブジェクトのサイズ (バイト単位)。
OCBD	コンテンツブロック識別子 (前)	前のオブジェクトの CBID。
UUID	ユニバーサルユニークID (新規)	StorageGRIDシステム内の新しいオブジェクトの識別子。
OUID	ユニバーサルユニークID (前)	StorageGRIDシステム内の前のオブジェクトの識別子。
パス	S3 オブジェクトパス	以前のオブジェクトと新しいオブジェクトの両方に使用されるS3オブジェクトパス

コード	フィールド	説明
RSLT	結果コード	オブジェクト上書きトランザクションの結果。結果は常に次のようになります: SUCS: 成功
SGRP	サイト (グループ)	存在する場合、上書きされたオブジェクトは指定されたサイトで削除されましたが、そのサイトは上書きされたオブジェクトが取り込まれたサイトではありません。

S3SL: S3 選択リクエスト

このメッセージは、S3 Select リクエストがクライアントに返された後の完了を記録します。S3SL メッセージには、エラー メッセージとエラー コードの詳細が含まれる場合があります。リクエストが成功しなかった可能性があります。

コード	フィールド	説明
BYSC	スキャンされたバイト数	ストレージ ノードからスキャン (受信) されたバイト数。 オブジェクトが圧縮されている場合、BYSC と BYPR は異なる可能性があります。オブジェクトが圧縮されている場合、BYSC には圧縮されたバイト数が含まれ、BYPR には解凍後のバイト数が含まれます。
BYPR	処理されたバイト数	処理されたバイト数。S3 Select ジョブによって実際に処理または操作された「スキャンされたバイト数」を示します。
BYRT	返されたバイト数	S3 Select ジョブがクライアントに返したバイト数。
再広報	処理されたレコード	S3 Select ジョブがストレージノードから受信したレコードまたは行の数。
RERT	返されたレコード	S3 Select ジョブがクライアントに返したレコードまたは行の数。
ジョフィ	仕事完了	S3 Select ジョブの処理が完了したかどうかを示します。これが false の場合、ジョブは完了に失敗し、エラー フィールドにデータが含まれる可能性があります。クライアントは部分的な結果を受け取ったか、まったく結果を受け取った可能性があります。
リード	Request ID	S3 Select リクエストの識別子。
外務省	実行時間	S3 選択ジョブが完了するまでにかかった時間 (秒)。

コード	フィールド	説明
ERMG	エラー メッセージ	S3 Select ジョブによって生成されたエラー メッセージ。
エルティ	エラーの種類	S3 Select ジョブによって生成されたエラーの種類。
ERST	エラースタック トレース	S3 Select ジョブによって生成されたエラー スタック トレース。
S3BK	S3バケット	S3 バケット名。
S3AK	S3 アクセスキー ID (リクエスト送 信者)	リクエストを送信したユーザーの S3 アクセスキー ID。
S3AI	S3テナントアカ ウントID (リク エスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。
S3KY	S3キー	バケット名を含まない S3 キー名。

SADD: セキュリティ 監査の無効化

このメッセージは、発信元サービス (ノード ID) が監査メッセージのログ記録をオフにしたことを示します。監査メッセージは収集も配信もされなくなりました。

コード	フィールド	説明
AETM	有効化メソッド	監査を無効にするために使用される方法。
アウン	ユーザー名	監査ログを無効にするコマンドを実行したユーザー名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージが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。

このメッセージは、以前はログ記録が有効だったが、現在は無効になっていることを示しています。これは通常、システム パフォーマンスを向上させるために一括取り込み時にのみ使用されます。一括アクティビティの後、監査が復元され (SADE)、監査を無効にする機能が永続的にブロックされます。

SADE: セキュリティ 監査の有効化

このメッセージは、発信元サービス (ノード ID) が監査メッセージのログ記録を復元し、監査メッセージが再び収集および配信されていることを示します。

コード	フィールド	説明
AETM	有効化メソッド	監査を有効にするために使用される方法。
アウン	ユーザー名	監査ログを有効にするコマンドを実行したユーザー名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージが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。

このメッセージは、以前はログ記録が無効 (SADD) だったが、現在は復元されていることを示しています。これは通常、システム パフォーマンスを向上させるために一括取り込み時にのみ使用されます。一括アクティビティの後、監査が復元され、監査を無効にする機能が永続的にブロックされます。

SCMT: オブジェクトストアコミット

グリッド コンテンツは、コミットされるまで (つまり永続的に保存されるまで) 使用可能にならず、保存済みとして認識されません。永続的に保存されたコンテンツはディスクに完全に書き込まれ、関連する整合性チェックに合格しました。このメッセージは、コンテンツ ブロックがストレージにコミットされたときに発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	永続ストレージにコミットされたコンテンツ ブロックの一意の識別子。
RSLT	結果コード	オブジェクトがディスクに保存された時点のステータス: SUCS: オブジェクトは正常に保存されました。

このメッセージは、特定のコンテンツ ブロックが完全に保存され、検証され、要求できる状態になったことを意味します。システム内のデータフローを追跡するために使用できます。

SDEL: S3 削除

S3 クライアントが DELETE トランザクションを発行すると、指定されたオブジェクトまたはバケットを削除するか、バケット/オブジェクトのサブリソースを削除するように要求されます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	削除されたオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。
DMRK	マーカーバージョンIDを削除	バージョン管理されたバケットからオブジェクトを削除するときに作成される削除マーカーのバージョン ID。バケットに対する操作にはこのフィールドは含まれません。
GFID	グリッドフェデレーション接続ID	クロスグリッド レプリケーション削除要求に関連付けられたグリッドフェデレーション接続の接続 ID。宛先グリッドの監査ログにのみ含まれます。
GFSA	グリッドフェデレーションソースアカウントID	クロスグリッド レプリケーション削除リクエストのソース グリッド上のテナントのアカウント ID。宛先グリッドの監査ログにのみ含まれます。
HTRH	HTTPリクエストヘッダー	<p>構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p>`X-Forwarded-For` リクエストに存在し、`X-Forwarded-For` 値が要求送信者の IP アドレス（SAIP 監査フィールド）と異なります。</p> </div> <p>`x-amz-bypass-governance-retention` リクエスト内に存在する場合は自動的に含まれます。</p>
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。
RSLT	結果コード	<p>DELETE トランザクションの結果。結果は常に次のようになります:</p> <p>SUCS: 成功</p>
S3AI	S3テナントアカウントID (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキーID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。

コード	フィールド	説明
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。
SACC	S3テナントアカウント名 (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス (リクエスト送信者)	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名 (バケット所有者)	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SGRP	サイト (グループ)	存在する場合、オブジェクトは指定されたサイトで削除されましたが、そのサイトはオブジェクトが取り込まれたサイトではありません。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： urn:sgws:identity::03393893651506583485:root 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間 (マイクロ秒単位)。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUDM	削除マーカのユニバーサルユニーク識別子	削除マーカの識別子。監査ログ メッセージは UUDM または UUID のいずれかを指定します。UUDM はオブジェクト削除要求の結果として作成された削除マーカを示し、UUID はオブジェクトを示します。

コード	フィールド	説明
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	削除されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

SGET: S3 ゲット

S3 クライアントが GET トランザクションを発行すると、オブジェクトを取得するかバケット内のオブジェクトを一覧表示するか、バケット/オブジェクトのサブリソースを削除する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意的システム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ (バイト単位)。バケットに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>`X-Forwarded-For` リクエストに存在し、`X-Forwarded-For` 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。</p> </div>
リティ	リストオブジェクトV2	<code>_v2 形式_</code> の応答が要求されました。詳細については、" AWS ListObjectsV2 "。GET バケット操作のみ。
NCHD	子供の数	キーと一般的なプレフィックスが含まれます。GET バケット操作のみ。

コード	フィールド	説明
鳴った	範囲読み取り	範囲読み取り操作のみ。この要求によって読み取られたバイトの範囲を示します。スラッシュ (/) の後の値は、オブジェクト全体のサイズを示します。
RSLT	結果コード	GET トランザクションの結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキーID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキーID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。
SACC	S3テナントアカウント名 (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス (リクエスト送信者)	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名 (バケット所有者)	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウントID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SUSR	S3 ユーザーURN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例: <code>urn:sgws:identity::03393893651506583485:root</code> 匿名のリクエストの場合は空です。

コード	フィールド	説明
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサによってルーティングされた場合は、ロードバランサのIPアドレス。
北キプロス共和国	切り捨てまたは切り捨てなし	すべての結果が返された場合は false に設定します。返される結果がさらにある場合は true に設定します。GET バケット操作のみ。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

シア：S3ヘッド

S3 クライアントが HEAD トランザクションを発行すると、オブジェクトまたはバケットの存在を確認し、オブジェクトに関するメタデータを取得する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	チェックされたオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>`X-Forwarded-For` リクエストに存在し、`X-Forwarded-For` 値が要求送信者の IP アドレス（SAIP 監査フィールド）と異なります。</p> </div>
RSLT	結果コード	GET トランザクションの結果。結果は常に次のようになります： SUCS: 成功

コード	フィールド	説明
S3AI	S3テナントアカウントID (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキーID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキーID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
SACC	S3テナントアカウント名 (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス (リクエスト送信者)	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名 (バケット所有者)	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： urn:sgws:identity::03393893651506583485:root 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間 (マイクロ秒単位)。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。

コード	フィールド	説明
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

SPOS: S3 ポスト

S3 クライアントが POST オブジェクト リクエストを発行すると、トランザクションが成功するとサーバーによってこのメッセージが発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意的システム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ (バイト単位)。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>`X-Forwarded-For` リクエストに存在し、`X-Forwarded-For` 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。</p> </div> <p>(SPOS では予想されません)。</p>
RSLT	結果コード	RestoreObject 要求の結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。

コード	フィールド	説明
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。 S3 Select 操作の場合は「select」に設定します。
SACC	S3テナントアカウント名 (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス (リクエスト送信者)	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名 (バケット所有者)	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SRCF	サブリソース構成	情報を復元します。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： <code>urn:sgws:identity::03393893651506583485:root</code> 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間 (マイクロ秒単位)。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。

コード	フィールド	説明
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

スプット: S3 プット

S3 クライアントが PUT トランザクションを発行すると、新しいオブジェクトまたはバケットを作成するか、バケット/オブジェクトのサブリソースを削除するように要求されます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CMPS	コンプライアンス設定	リクエスト内に存在する場合、バケットの作成時に使用されたコンプライアンス設定 (最初の 1024 文字に切り捨てられます)。
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ (バイト単位)。バケットに対する操作にはこのフィールドは含まれません。
GFID	グリッドフェデレーション接続 ID	クロスグリッド レプリケーション PUT 要求に関連付けられたグリッドフェデレーション接続の接続 ID。宛先グリッドの監査ログにのみ含まれます。
GFSA	グリッドフェデレーションソースアカウント ID	クロスグリッド レプリケーション PUT リクエストのソース グリッド上のテナントのアカウント ID。宛先グリッドの監査ログにのみ含まれます。

コード	フィールド	説明
HTRH	HTTPリクエストヘッダー	<p>構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p>`X-Forwarded-For` リクエストに存在し、 `X-Forwarded-For` 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。</p> </div> <p>`x-amz-bypass-governance-retention` リクエスト内に存在する場合は自動的に含まれます。</p>
ルケン	オブジェクトロックが有効	リクエストヘッダーの値 <code>x-amz-bucket-object-lock-enabled</code> (リクエスト内に存在する場合)。
LKLH	オブジェクトロック法的保留	リクエストヘッダーの値 <code>`x-amz-object-lock-legal-hold`PutObject</code> リクエストに存在する場合。
LKMD	オブジェクトロック保持モード	リクエストヘッダーの値 <code>`x-amz-object-lock-mode`PutObject</code> リクエストに存在する場合。
LKRU	オブジェクトロックの保持期限	リクエストヘッダーの値 <code>`x-amz-object-lock-retain-until-date`PutObject</code> リクエストに存在する場合。値は、オブジェクトが取り込まれた日付から 100 年以内に制限されます。
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。
RSLT	結果コード	<p>PUT トランザクションの結果。結果は常に次のようになります:</p> <p>SUCS: 成功</p>
S3AI	S3テナントアカウントID (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキーID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキーID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。
SACC	S3テナントアカウント名 (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス (リクエスト送信者)	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名 (バケット所有者)	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SRCF	サブリソース構成	新しいサブリソース構成 (最初の 1024 文字に切り捨てられます)。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： <code>urn:sgws:identity::03393893651506583485:root</code> 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間 (マイクロ秒単位)。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
ULID	アップロードID	CompleteMultipartUpload 操作の SPUT メッセージにのみ含まれます。すべてのパーツがアップロードされ、組み立てられたことを示します。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	バージョン管理されたバケットに作成された新しいオブジェクトのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

コード	フィールド	説明
VSST	バージョン管理状態	バケットの新しいバージョン管理状態。使用される状態は、「有効」または「一時停止」の2つです。オブジェクトに対する操作にはこのフィールドは含まれません。

SREM: オブジェクトストアの削除

このメッセージは、コンテンツが永続ストレージから削除され、通常の API 経由でアクセスできなくなったときに発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	永続ストレージから削除されたコンテンツ ブロックの一意的識別子。
RSLT	結果コード	コンテンツ削除操作の結果を示します。次の値のみが定義されています。 SUCS: 永続ストレージからコンテンツが削除されました

この監査メッセージは、特定のコンテンツ ブロックがノードから削除され、直接要求できなくなったことを意味します。このメッセージは、システム内で削除されたコンテンツの流れを追跡するために使用できます。

SUPD: S3 メタデータが更新されました

このメッセージは、S3 クライアントが取り込んだオブジェクトのメタデータを更新したときに、S3 API によって生成されます。メタデータの更新が成功した場合、サーバーによってメッセージが発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CNCH	一貫性制御ヘッダー	バケットのコンプライアンス設定を更新するときの、Consistency-Control HTTP リクエスト ヘッダーの値 (リクエスト内に存在する場合)。
CNID	接続識別子	TCP/IP 接続の一意的システム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ (バイト単位)。バケットに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
HTRH	HTTPリクエストヘッダー	<p>構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>`X-Forwarded-For` リクエストに存在し、 `X-Forwarded-For` 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。</p> </div>
RSLT	結果コード	<p>GET トランザクションの結果。結果は常に次のようになります:</p> <p>SUCS: 成功</p>
S3AI	S3テナントアカウントID (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキーID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキーID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
SACC	S3テナントアカウント名 (リクエスト送信者)	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス (リクエスト送信者)	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名 (バケット所有者)	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウントID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。

コード	フィールド	説明
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： urn:sgws:identity::03393893651506583485:root 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	メタデータが更新されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

SVRF: オブジェクトストア検証失敗

このメッセージは、コンテンツ ブロックが検証プロセスに失敗するたびに発行されます。複製されたオブジェクト データがディスクから読み取られたり、ディスクに書き込まれたりするときは毎回、要求元のユーザーに送信されるデータがシステムに最初に取り込まれたデータと同一であることを確認するために、いくつかの検証と整合性チェックが実行されます。これらのチェックのいずれかが失敗した場合、システムは破損した複製オブジェクト データを自動的に隔離し、再度取得されないようにします。

コード	フィールド	説明
CBID	コンテンツブロック識別子	検証に失敗したコンテンツ ブロックの一意の識別子。

コード	フィールド	説明
RSLT	結果コード	<p>検証失敗の種類:</p> <p>CRCF: 巡回冗長検査 (CRC) に失敗しました。</p> <p>HMAC: ハッシュベースのメッセージ認証コード (HMAC) チェックに失敗しました。</p> <p>EHS: 予期しない暗号化されたコンテンツ ハッシュ。</p> <p>PHS: 予期しない元のコンテンツ ハッシュ。</p> <p>SEQC: ディスク上のデータ シーケンスが正しくありません。</p> <p>PERR: ディスク ファイルの構造が無効です。</p> <p>DERR: ディスク エラー。</p> <p>FNAM: ファイル名が間違っています。</p>



このメッセージは注意深く監視する必要があります。コンテンツ検証の失敗は、ハードウェア障害が差し迫っていることを示している可能性があります。

どの操作によってメッセージがトリガーされたかを確認するには、AMID (モジュール ID) フィールドの値を確認します。たとえば、SVFY 値は、メッセージが Storage Verifier モジュール (つまりバックグラウンド検証) によって生成されたことを示し、STOR は、メッセージがコンテンツの取得によってトリガーされたことを示します。

SVRU: オブジェクトストアの検証が不明です

LDR サービスのストレージ コンポーネントは、オブジェクト ストア内の複製されたオブジェクト データのすべてのコピーを継続的にスキャンします。このメッセージは、複製されたオブジェクト データの不明なまたは予期しないコピーがオブジェクト ストアで検出され、隔離ディレクトリに移動されたときに発行されます。

コード	フィールド	説明
FPTH	ファイルパス	予期しないオブジェクト コピーのファイルパス。
RSLT	結果	このフィールドの値は「NONE」です。RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージは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。



SVRU: オブジェクト ストアの検証不明監視メッセージを注意深く監視する必要があります。これは、オブジェクト ストアでオブジェクト データの予期しないコピーが検出されたことを意味します。この状況はハードウェア障害の兆候を示している可能性があるため、これらのコピーがどのように作成されたかを判断するためにすぐに調査する必要があります。

SYSD: ノード停止

サービスが正常に停止されると、シャットダウンが要求されたことを示すこのメッセージが生成されます。通常、監査メッセージ キューはシャットダウン前にクリアされないため、このメッセージはその後の再起動後にのみ送信されます。サービスが再起動されていない場合は、シャットダウン シーケンスの開始時に送信される SYST メッセージを探します。

コード	フィールド	説明
RSLT	クリーンシャットダウン	シャットダウンの性質: SUCS: システムは正常にシャットダウンされました。

メッセージには、ホスト サーバーが停止されているかどうかは示されず、レポート サービスのみが示されます。SYSD の RSLT は、「クリーン」シャットダウンによってのみメッセージが生成されるため、「ダーティ」シャットダウンを示すことはできません。

SYST: ノード停止

サービスが正常に停止されると、シャットダウンが要求され、サービスがシャットダウン シーケンスを開始したことを示すこのメッセージが生成されます。SYST は、サービスが再起動される前にシャットダウンが要求されたかどうかを判断するために使用できます (通常、サービスの再起動後に送信される SYSD とは異なります)。

コード	フィールド	説明
RSLT	クリーンシャットダウン	シャットダウンの性質: SUCS: システムは正常にシャットダウンされました。

メッセージには、ホスト サーバーが停止されているかどうかは示されず、レポート サービスのみが示されます。SYST メッセージの RSLT コードは、「クリーン」シャットダウンによってのみメッセージが生成されるため、「ダーティ」シャットダウンを示すことはできません。

SYSU: ノード開始

サービスが再起動されると、前回のシャットダウンが正常 (コマンドによる) であったか、異常 (予期しない) であったかを示すこのメッセージが生成されます。

コード	フィールド	説明
RSLT	クリーンシャットダウン	シャットダウンの性質: SUCS: システムは正常にシャットダウンされました。 DSDN: システムが正常にシャットダウンされませんでした。 VRGN: サーバーのインストール (または再インストール) 後にシステムが初めて起動されました。

メッセージには、ホスト サーバーが起動されたかどうかは示されず、レポート サービスのみが示されます。このメッセージは次の目的で使用できます。

- 監査証跡の不連続性を検出します。
- 操作中にサービスに障害が発生しているかどうかを判断します (StorageGRIDシステムの分散性により、これらの障害が隠される可能性があるため)。サーバー マネージャーは障害が発生したサービスを自動的に再起動します。

WDEL: 迅速な削除

Swift クライアントが DELETE トランザクションを発行すると、指定されたオブジェクトまたはコンテナを削除する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	削除されたオブジェクトのサイズ (バイト単位)。コンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For` リクエストに存在し、`X-Forwarded-For` 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。

コード	フィールド	説明
RSLT	結果コード	DELETE トランザクションの結果。結果は常に次のようになります: SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
SGRP	サイト (グループ)	存在する場合、オブジェクトは指定されたサイトで削除されましたが、そのサイトはオブジェクトが取り込まれたサイトではありません。
時間	Time	リクエストの合計処理時間 (マイクロ秒単位)。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。コンテナに対する操作にはこのフィールドは含まれません。
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

WGET: Swift GET

Swift クライアントが GET トランザクションを発行すると、オブジェクトの取得、コンテナ内のオブジェクトのリスト、またはアカウント内のコンテナのリストの取得の要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> `X-Forwarded-For` リクエストに存在し、 `X-Forwarded-For` 値が要求送信者の IP アドレス（SAIP 監査フィールド）と異なります。 </div>
RSLT	結果コード	GET トランザクションの結果。結果は常に SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。アカウントに対する操作にはこのフィールドは含まれません。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

WHEA: Swift HEAD

Swift クライアントが HEAD トランザクションを発行すると、アカウント、コンテナ、またはオブジェクトの存在を確認し、関連するメタデータを取得する要求が行われま

す。トランザクションが成功した場合、このメッセージはサーバーによって発行されま
す。

コード	フィールド	説明
CBID	コンテンツブ ロック識別子	要求されたコンテンツ ブロックの一意的識別子。CBID が不明な場 合、このフィールドは 0 に設定されます。アカウントおよびコンテナに 対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイ ズ	取得したオブジェクトのサイズ (バイト単位)。アカウントおよびコン テナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエスト ヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値の リスト。 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <code>`X-Forwarded-For`</code> リクエストに存在し、 <code>`X-Forwarded- For`</code> 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。 </div>
RSLT	結果コード	HEAD トランザクションの結果。結果は常に次のようになります: SUCS: 成功
SAIP	要求元クライア ントのIPアドレ ス	要求を行ったクライアント アプリケーションの IP アドレス。
時間	Time	リクエストの合計処理時間 (マイクロ秒単位)。
TLIP	信頼できるロード バランサのIP アドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティ ングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユ ニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	Swiftアカウン トID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。アカウントに対する操作にはこのフィールドは含ま れません。
WOBJ	Swiftオブジェク ト	Swift オブジェクト識別子。アカウントおよびコンテナに対する操作に はこのフィールドは含まれません。

コード	フィールド	説明
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

WPUT: Swift PUT

Swift クライアントが PUT トランザクションを発行すると、新しいオブジェクトまたはコンテナを作成する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。コンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>`X-Forwarded-For` リクエストに存在し、`X-Forwarded-For` 値が要求送信者の IP アドレス（SAIP 監査フィールド）と異なります。</p> </div>
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。
RSLT	結果コード	PUT トランザクションの結果。結果は常に次のようになります: SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。

コード	フィールド	説明
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。コンテナに対する操作にはこのフィールドは含まれません。
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

著作権に関する情報

Copyright © 2025 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権を有し、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権については、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。