監査ログを確認します
StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-118/audit/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

目次

監査ログを確認します 1
監査ログの確認：概要 1
監査メッセージのフローと保持 1
監査メッセージのフロー 1
監査ログファイルにアクセスします 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：概要 5
audit-explain ツールを使用してください 7
audit-sum ツールを使用します 9
監査メッセージの形式 19
監査メッセージの形式：概要 19
データ型 20
イベント固有のデータ 20
監査メッセージの共通要素 21
監査メッセージの例 22
監査メッセージとオブジェクトライフサイクル 23
監査メッセージはいつ生成されますか？ 24
オブジェクトの取り込みトランザクション 24
オブジェクトの削除トランザクション 27
オブジェクトの読み出しトランザクション 28
メタデータの更新メッセージです 30
監査メッセージ 31
監査メッセージ：概要 31
監査メッセージのカテゴリ 32
監査メッセージリファレンス 37

監査ログを確認します

監査ログの確認：概要

ここでは、 StorageGRID 監査メッセージおよび監査ログの構造と内容について説明します。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判読し、分析できます。

ここに記載する手順は、システムのアクティビティおよび使用状況のレポート生成を担当する管理者を対象としています。このようなレポートの生成には、 StorageGRID システムの監査メッセージの分析が必要となります。

テキストログファイルを使用するには、管理ノード上に設定されている監査共有へのアクセスが必要です。

監査メッセージレベルの設定および外部syslogサーバの使用については、を参照してください "監査メッセージとログの送信先を設定します"。

監査メッセージのフローと保持

すべての StorageGRID サービスは通常のシステム運用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 システムからにどのように転送されるかを理解しておく必要があります `audit.log` ファイル。

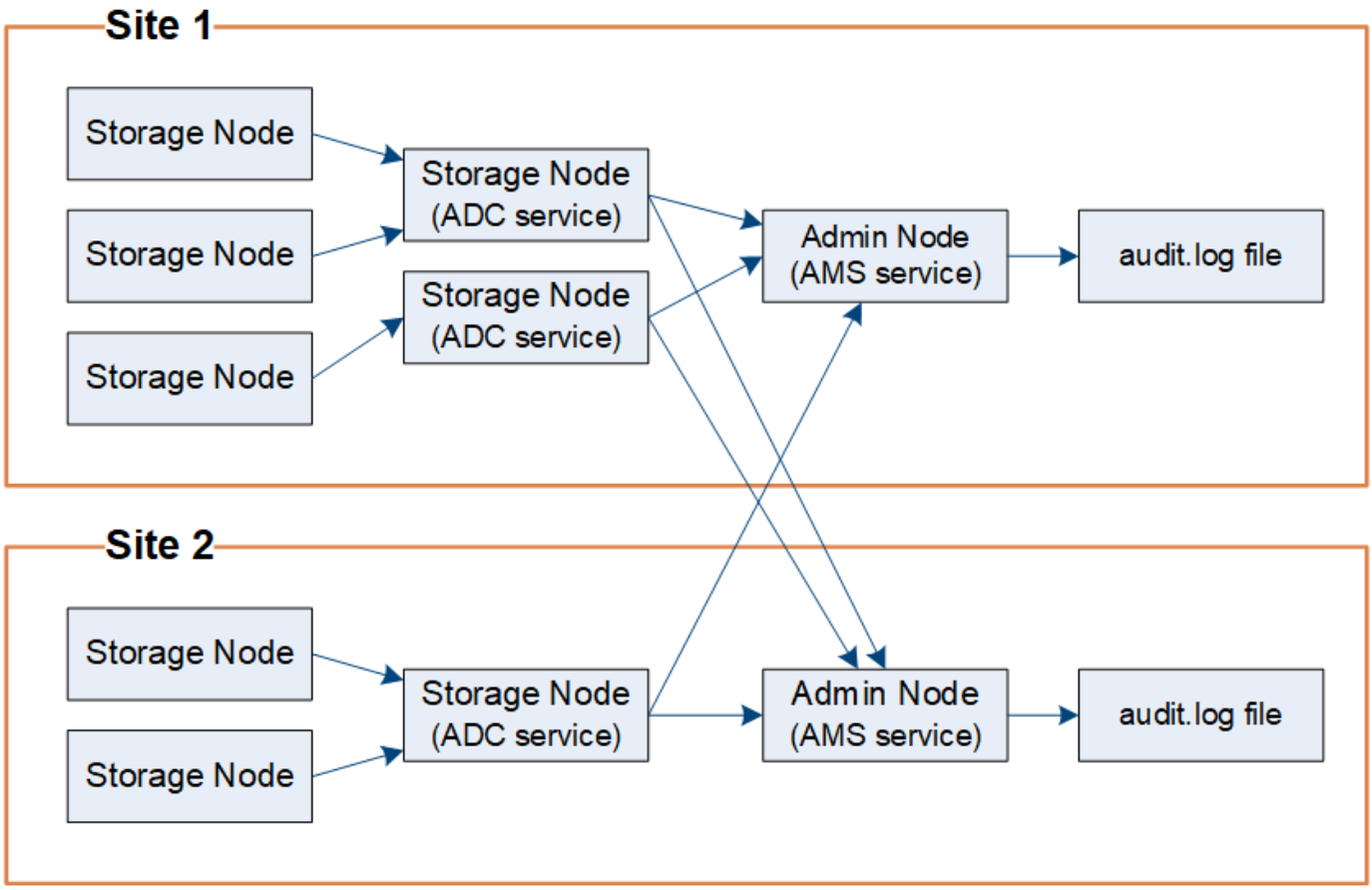
監査メッセージのフロー

監査メッセージは、管理ノードおよび Administrative Domain Controller （ ADC ）サービスが用意されているストレージノードによって処理されます。

監査メッセージのフロー図に示すように、各 StorageGRID ノードは監査メッセージをデータセンターサイトにあるいずれかの ADC サービスに送信します。ADC サービスは、各サイトに設置されている最初の 3 つのストレージノードで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、監査メッセージの集合を 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、システムアクティビティの完全な記録が各管理ノードに提供されます。

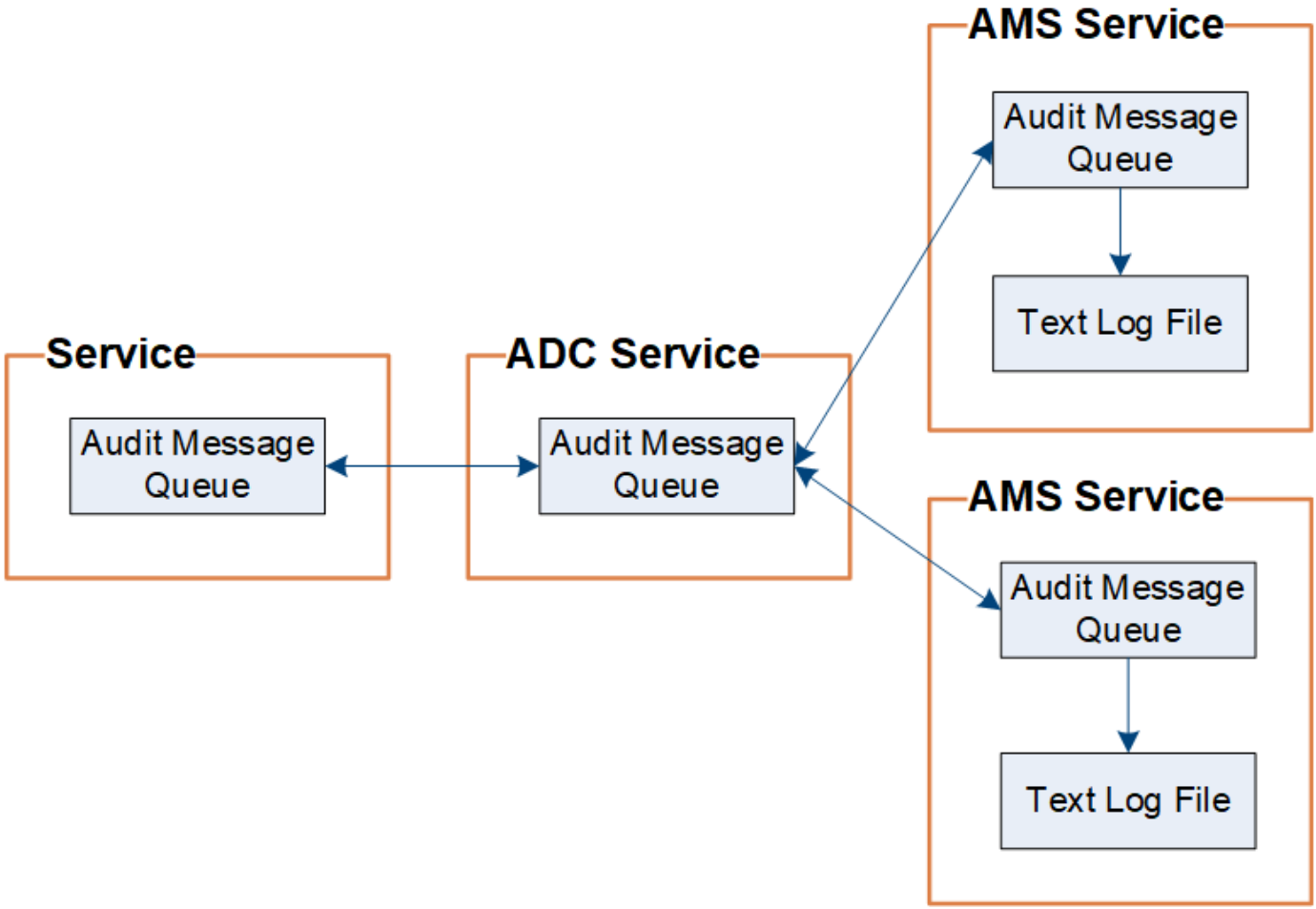
各管理ノードでは、監査メッセージがテキストログファイルに保存されます。アクティブなログファイルの名前はです `audit.log`。



監査メッセージの保持

StorageGRID では、コピー / 削除プロセスを使用して、監査ログに書き込まれる前に監査メッセージが失われないようにします。

ノードが生成またはリレーした監査メッセージは、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。メッセージが管理ノード内の監査ログファイルに書き込まれるまで、メッセージのコピーは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、監査メッセージが転送中に失われることはありません。



ネットワーク接続の問題または監査容量の不足が原因で、監査メッセージキューが一時的に増加する可能性があります。キューが増加すると、各ノードの使用可能スペースがキューによってさらに消費されます `/var/local/` ディレクトリ。問題 が解除されず、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、個々のノードがバックログの処理の優先順位を設定し、一時的に新しいメッセージに使用できなくなります。

具体的には、次のような動作が発生することがあります。

- 状況に応じて `/var/local/log` 管理ノードで使用されるディレクトリがいっぱいになると、ディレクトリに空きが出るまでその管理ノードを新しい監査メッセージに使用できないことを示すフラグが設定されます。S3およびSwiftクライアント要求には影響しません。監査リポジトリにアクセスできない場合に XAMS （ Unreachable Audit Repositories ）アラームがトリガーされます。
- 状況に応じて `/var/local/` ADCサービスを採用するストレージノードで使用されるディレクトリが92%フルになると、ディレクトリが87%フルになるまでそのノードを監査メッセージに使用できないことを示すフラグが設定されます。他のノードへのS3およびSwiftクライアント要求には影響しません。監査リレーにアクセスできない場合に NRLY （ Available Audit Relays ）アラームがトリガーされます。

  ADCサービスを使用する使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のに格納します `/var/local/log/localaudit.log` ファイル。

- 状況に応じて `/var/local/` ストレージノードで使用されるディレクトリが85%フルになると、ノードはS3およびSwiftクライアントの要求を拒否し始めます `503 Service Unavailable`。

原因 監査メッセージキューが大幅に増加すると、次のような問題が発生する可能性があります。

- 管理ノードまたは ADC サービスを採用するストレージノードの停止。システムのいずれかのノードが停止すると、残りのノードはバックログ状態になる可能性があります。
- システムの監査キャパシティを超えるアクティビティ率の継続。
- 。 `/var/local/` 監査メッセージには関連のない理由でADCストレージノード上ののスペースがいっぱいになる。この場合、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログの優先順位を設定します。これにより、他のノードで原因 バックログが発生する可能性があります。

Large audit queue アラートと **Audit Messages Queued** （ **AMQS** ）アラーム

時間の経過に伴う監査メッセージキューのサイズを監視できるように、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の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。

「 Large audit queue * 」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、最初にシステムの負荷を確認します。最近のトランザクションの数が膨大であった場合は、アラートとアラームは時間が経過すると解決するため、無視してかまいません。

アラートまたはアラームが解決せず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。クライアントの書き込みとクライアントの読み取りでエラーまたはオフの監査レベルを変更して、クライアントの処理速度を下げるか、ログに記録される監査メッセージの数を減らしてください。を参照してください "監査メッセージとログの送信先を設定します"。

重複メッセージです

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。そのため、監査ログでメッセージが重複する可能性があります。

監査ログファイルにアクセスします

監査共有にはアクティブなが含まれています `audit.log` ファイルおよび圧縮された監査ログファイル。監査ログファイルには、管理ノードのコマンドラインから直接アクセスできます。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 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。

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. 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。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. 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。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 監査ログファイルが保存さ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に保存されます `/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です `audit.log`。

必要に応じて、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。を参照してください "監査メッセージとログの送信先を設定します"。

1日に1回、アクティブです `audit.log` ファイルが保存され、新しいファイルが作成されます `audit.log` ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています *`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と番号が付加された日付が使用されます *`yyyy-mm-dd.txt.n`*。例： `2018-04-15.txt` および `2018-04-15.txt.1` 2018年4月15日に作成および保存された1つ目のログファイルおよび2つ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、という形式で名前が変更されます *`yyyy-mm-dd.txt.gz`*`元の日付を保持します。そのため、時間の経過とともに、管理ノード上の監査ログ用に割り当てられたストレージが消費されます。スクリプトによって監査ログのスペース消費が監視され、のスペースを解放するために、必要に応じてログファイルが削除されます `/var/local/log` ディレクトリ。監査ログは、作成日に基づいて、古い順に削除されます。スクリプトの処理は、次のファイルで監視できます。 `/var/local/log/manage-audit.log`。

この例は、アクティブを示しています `audit.log` ファイル。前日のファイルです (`2018-04-15.txt`）、および前日の圧縮ファイルです (`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：概要

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][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):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::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

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の読みやすさや解釈が容易ではありません。を使用できます "audit-explainツール" を使用して、監査ログ内の監査メッセージの簡単な概要を取得します。を使用できます "audit-sumツール" ログに記録された書き込み、読み取り、削除の各処理の所要時間をまとめます。

audit-explain ツールを使用してください

を使用できます `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。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- 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。この4人 "SPUT" 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、そのバケットに3つのオブジェクトを追加した場合に、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
```

。 `audit-explain` ツールでは次の操作を実行できます。

- プレーンまたは圧縮された監査ログを処理します。例：

  ```
  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：

  ```
  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ます。これにより、を使用して入力をフィルタリング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、解析に時間がかかることがあるため、確認して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：
>
> ```
> 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。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. 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。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
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
   ```

   。 `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。

   > 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。

audit-sum ツールを使用します

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。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- 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            count     min(sec)         max(sec)
average(sec)
  =============            =====     ========         ========
============
  IDEL                       274
  SDEL                    213371        0.004          20.934
0.352
  SGET                    201906        0.010        1740.290
1.132
  SHEA                     22716        0.005           2.349
0.272
  SPUT                   1771398        0.011        1770.563
0.487
```

。 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"
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"

コード	説明	を参照してください
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` ツールでは次の操作を実行できます。

- プレーンまたは圧縮された監査ログを処理します。例：

```
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：

```
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ます。これにより、を使用して入力をフィルタリング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。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. 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。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
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/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
      ```

      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           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

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

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

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

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ツール" その時間内のすべてのSGET処理を確認するには、次の手順を実行します。

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

grepコマンドの出力が多くの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)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

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

監査メッセージの形式

監査メッセージの形式：概要

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 "監査-説明する" および "audit-sumの略" 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(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

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。
CSTR	UTF-8文字の可変長配列。文字は次の方法でエスケープできます。 • 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：**\[RST\（FC32\）：SUCS\] \[time\(UI64\):11454\]\[SAIP\(iPad\):"10.224.0.100"\]\[S3AI\(CStr\):"60025621595611246499"\] \[SACC\(CStr\):"account"\]\[S3AK\(CStr\):"SGKH4_Nc8SO1H6w3w0nCOFCGK__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。このメッセージ例には、が含まれています "Shea" メッセージコード（[ATYP（FC32）：Shea]）。S3 HEAD要求が成功し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	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。
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ポック（ 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。

コード	を入力します	説明
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ポック（ 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判読可能な時刻 `audit.log` file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 *`YYYY-MMDDTHH:MM:SS.UUUUUU`* 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。 *`UUUUUU`* 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。
ビーバー	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。

以下は、に表示される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):"s3small1"][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す。

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):"s3small1"][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" 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\(CSTR\):"s3small1"][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属性を判読できる形式です。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][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。

監査メッセージとオブジェクトライフサイクル

監査メッセージはいつ生成されますか？

監査メッセージは、オブジェクトの取り込み、読み出し、または削除が行われるたびに生成されます。監査ログでこれらのトランザクションを特定するには、 API 固有の（ S3 または Swift ）監査メッセージを検索します。

監査メッセージは各プロトコルに固有な識別子によってリンクされます。

プロトコル	コード
S3 処理をリンクしています	S3BK（バケット）、S3KY（キー）、またはその両方
Swift 処理をリンクしています	WCON（コンテナ）、WOBJ（オブジェクト）、またはその両方
内部処理をリンクしています	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、オブジェクトサイズ、ネットワーク遅延などの要因により、各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に記載する例とは異なる場合があります。

アーカイブノード

アーカイブノードから外部アーカイブストレージシステムにオブジェクトデータを送信するときに生成される一連の監査メッセージは、 SCMT （ Store Object Commit ）メッセージがないことを除き、ストレージノードの場合と似ています。 さらに、オブジェクトデータのアーカイブコピーごとに ATCE （ Archive Object Store Begin ）メッセージと ASCE （ Archive Object Store End ）メッセージが生成されます。

アーカイブノードが外部のアーカイブストレージシステムからオブジェクトデータを読み出すときに生成される一連の監査メッセージは、ストレージノードの場合と似ていますが、オブジェクトデータのアーカイブコピーごとに ARCB （ Archive Object Retrieve Begin ）メッセージと ARCE （ Archive Object Retrieve End ）メッセージが生成される点が異なります。

アーカイブノードが外部のアーカイブストレージシステムからオブジェクトデータを削除するときに生成される一連の監査メッセージは、ストレージノードのメッセージと似ています。ただし、 SREM （ Object Store Remove ）メッセージがなく、削除要求ごとに AREM （ Archive Object Remove ）メッセージが生成される点が異なります。

オブジェクトの取り込みトランザクション

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特定するには、 API 固有の（ S3 または Swift ）監査メッセージを検索します。

以下の表には、取り込みトランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、取り込みトランザクションをトレースするために必要なメッセージのみが含まれています。

S3 の取り込み監査メッセージ

コード	名前	説明	トレース	を参照してください
SPUT	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	"SPUT ： S3 PUT"
ORLM の場合	オブジェクトルールを満たしました	このオブジェクトが ILM ポリシーを満たしました。	CBID	"ORLM ：オブジェクトルールが満たされています"

Swift の取り込み監査メッセージ

コード	名前	説明	トレース	を参照してください
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 、 WCON 、 WOBJ	"WPUT ： Swift PUT"
ORLM の場合	オブジェクトルールを満たしました	このオブジェクトが ILM ポリシーを満たしました。	CBID	"ORLM ：オブジェクトルールが満たされています"

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 クライアントがストレージノード（ LDR サービス）にオブジェクトを取り込んだときに生成され、監査ログに保存された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Make 2 Copies 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たすべての監査メッセージが含まれているわけではなく、S3 取り込みトランザクション（ SPUT ）に関連するメッセージだけが示されています。

この例では、 S3 バケットは以前に作成済みであることを前提としています。

SPUT ： S3 PUT

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 S3 PUT トランザクションが実行されたことを示します。

```
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(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(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ています

ORLM メッセージは、このオブジェクトが ILM ポリシーに準拠し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ています。

レプリケート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 が記録されます。

```
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]]
```

イレイジャーコーディングオブジェクトの場合は、LOCSフィールドにイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループIDが表示されます。

```
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、使用される 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記録されます。

```
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]]
```

オブジェクトの削除トランザクション

監査ログでオブジェクトの削除トランザクションを特定するには、 API 固有の（ S3 および Swift ）監査メッセージを検索します。

以下の表には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、削除トランザクションをトレースするために必要なメッセージのみが含まれています。

S3 の削除監査メッセージ

コード	名前	説明	トレース	を参照してください
SDEL	S3 削除	バケットからのオブジェクトの削除が要求されました。	CBID 、 S3KY	"SDEL ： S3 DELETE"

Swift の削除監査メッセージ

コード	名前	説明	トレース	を参照してください
WDEL	Swift の削除	コンテナまたはコンテナからのオブジェクトの削除が要求されました。	CBID 、 WOBJ	"WDEL ： Swift の削除"

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て監査ログに保存されます。

以下の例には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 の削除トランザクション（ SDEL ）に関連するメッセージだけが示されています。

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要求を送信した時点で開始されます。メッセージには、オブジェクトの削除元のバケットと、オブジェクトの識別に使用される 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):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(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]]
```

オブジェクトの読み出しトランザクション

監査ログでオブジェクトの読み出しトランザクションを特定するには、 API 固有の（ S3 および Swift ）監査メッセージを検索します。

以下の表には、読み出しトランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、読み出しトランザクションをトレースするために必要なメッセージのみが含まれています。

S3 の読み出し監査メッセージ

コード	名前	説明	トレース	を参照してください
SGET	S3 GET	バケットからのオブジェクトの読み出しが要求されました。	CBID 、 S3BK 、 S3KY	"SGET ： S3 GET"

Swift の読み出し監査メッセージ

コード	名前	説明	トレース	を参照してください
wget	Swift GET	コンテナからのオブジェクトの読み出しが要求されました。	CBID 、 WCON 、 WOBJ	"wget ： Swift GET"

例： **S3** オブジェクトの読み出し

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読み出すと、監査メッセージが生成されて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たすべての監査メッセージが含まれているわけではなく、S3 読み出しトランザクション（ SGET ）に関連するメッセージだけが示されています。

SGET ： S3 GET

オブジェクトの読み出しは、クライアントがLDRサービスにGetObject要求を送信したときに開始されます。メッセージには、オブジェクトの読み出し元のバケットと、オブジェクトの識別に使用される 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][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][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、クライアントはオブジェクトを匿名で読み出したり、別のテナントアカウントが所有しているバケットからオブジェクトを読み出すことができます。監査メッセージには、このような匿名要求およびクロスアカウント要求を追跡できるように、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ます。

次のメッセージ例では、クライアントが所有していないバケットに格納されているオブジェクトに対するGetObject要求を送信しています。SBAI と 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が、これは S3AI および SACC に記録されているクライアントのテナントアカウント ID および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_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][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：オブジェクトの **S3 Select**

S3 クライアントがオブジェクトに対して S3 Select クエリを実行すると、監査メッセージが生成されて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たすべての監査メッセージが含まれているわけではなく、S3 Select トランザクション（ SelectObjectContent ）に関連するトランザクションのみが表示されます。

各クエリには2つの監査メッセージが生成されます。1つはS3 Select要求の承認を実行するメッセージ（S3SRフィールドが「select」に設定されている）で、もう1つは処理中にストレージからデータを取得する標準のGET処理です。

```
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]]
```

メタデータの更新メッセージです

S3 クライアントがオブジェクトのメタデータを更新すると、監査メッセージが生成されます。

S3 メタデータの更新監査メッセージ

コード	名前	説明	トレース	を参照してください
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まれたオブジェクトのメタデータを更新すると生成されます。	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

次の例は、既存の S3 オブジェクトのメタデータを更新するトランザクションの成功を示しています。

SUPD ： **S3** メタデータの更新

S3クライアントが、指定されたメタデータを更新する要求（SUPD）を実行します (`x-amz-meta-\*`）をクリックします。この例では、要求ヘッダーは監査プロトコルヘッダー (**configuration> Monitoring> Audit** および **syslog server**) として設定されているため、 HTRH フィールドに含まれています。を参照してください "監査メッセージとログの送信先を設定します"。

```
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：概要

システムから返される監査メッセージの詳細について、次のセクションで説明します。各監査メッセージをメッセージが表すアクティビティのクラスでグループ化して、表に記載します。これらの分類は、監査対象のアクティビティのタイプを理解し、必要な監査メッセージフィルタリングのタイプを選択する場合に役立ちます。

監査メッセージは、 4 文字のコードでアルファベット順に一覧表示されます。このアルファベット順のリストでは、特定のメッセージに関する情報を検索できます。

この章で使用する4文字のコードは、次のメッセージ例に示すように、監査メッセージ内の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]]
```

監査メッセージレベルの設定、ログの送信先の変更、および監査情報への外部syslogサーバの使用については、を参照してください "監査メッセージとログの送信先を設定します"

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処理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概要	を参照してください
ECMC	Missing Erasure-Coded Data Fragment：イレイジャーコーディングされた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：イレイジャーコーディングされたデータフラグメントの欠落"
ECOC	Corrupt Erasure-Coded Data Fragment：イレイジャーコーディングデータフラグメントの破損が検出されたことを示します。	"ECOC：イレイジャーコーディングされたデータフラグメントの破損"
ETAF	Security Authentication Failed ： Transport Layer Security （ 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 Registration ：サービスが StorageGRID システムに自身に関する情報を更新または登録しました。	"GNRG ： GNDS 登録"
GNUR	GNDS Unregistration ：サービスが StorageGRID システムから自身の登録を解除しました。	"GNUR ： GNDS 登録解除"
GTED	Grid Task Ended ： CMN サービスがグリッドタスクの処理を完了しました。	"GTED ： Grid タスクが終了しました"
GTSt	Grid Task Started ： CMN サービスがグリッドタスクの処理を開始しました。	"GTSt ： Grid タスクが開始されました"
GTSU	Grid Task Submitted ：グリッドタスクが CMN サービスに送信されました。	"GTSU ： Grid タスクが送信されました"

コード	メッセージのタイトルと概要	を参照してください
LLST	Location Lost ：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 ：ロケーションが失われました"
OLST	Object Lost ：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: システムが損失オブジェクトを検出しました"
サッド	Security Audit Disable ：監査メッセージのロギングがオフになりました。	"SADD ：セキュリティ監査無効"
Sade 社	Security Audit Enable ：監査メッセージのロギングが再開されました。	"Sade ：セキュリティ監査を有効にします"
SVRF	Object Store Verify Fail ：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の検証に失敗しました"
SVRU の場合	Object Store Verify Unknown ：オブジェクトストアで想定外の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検証が不明です"
SYSD	Node Stop ：シャットダウンが要求されました。	"SYSD ：ノード停止"
SYST	Node Stopping ：サービスが正常な停止を開始しました。	"SYST ：ノードを停止しています"
SYSU	Node Start ：サービスが開始されました。前回のシャットダウンのタイプがメッセージに示されます。	"SYSU ：ノードが開始されました"

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格納と管理に関連するイベントに使用されます。オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、および検証が含まれます。

コード	説明	を参照してください
APCT	Archive Purge from Cloud-Tier ： S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが削除されました。	"APCT ：クラウド階層からのアーカイブの削除"
ARCB	Archive Object Retrieve Begin ： ARC サービスが、外部アーカイブストレージシステムからオブジェクトデータの読み出しを開始しました。	"ARCB ：アーカイブオブジェクトの読み出しが開始されました"

コード	説明	を参照してください
ARCE	Archive Object Retrieve End ：オブジェクトデータが外部アーカイブストレージシステムから読み出され、 ARC サービスが読み出し処理のステータスをレポートします。	"ARCE ：アーカイブオブジェクトの読み出しが終了しました"
ARCT	Archive Retrieve from Cloud-Tier ： S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが読み出されました。	"ARCT ：クラウド階層からアーカイブを取得します"
AREM	Archive Object Remove ：外部アーカイブストレージシステムからのコンテンツブロックの削除が成功または失敗しました。	"AREM ：アーカイブオブジェクトの削除"
ASCE	Archive Object Store End ：コンテンツブロックが外部アーカイブストレージシステムに書き込まれ、 ARC サービスが書き込み処理のステータスをレポートします。	"ASCE ：アーカイブオブジェクトストアの終了"
▽ SCT 。△	Archive Store Cloud-Tier ： S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムに、オブジェクトデータが格納されました。	"ASCT ：アーカイブストアのクラウド階層"
ATCE	Archive Object Store Begin ：外部アーカイブストレージへのコンテンツブロックの書き込みが開始されました。	"ATCE ：アーカイブオブジェクトストアが開始されました"
AVCC の場合	Archive Validate Cloud-Tier Configuration ：指定されたアカウントおよびバケットの設定の検証に成功または失敗しました。	"AVCC ：アーカイブによってクラウド階層の構成を検証"
ブロア	Bucket Read Only Request：バケットが読み取り専用モードになったか、または終了しました。	"BROR：バケット読み取り専用要求"
CBSE	Object Send End ：ソースエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。	"CBSE ：オブジェクト送信終了"
CBRE	Object Receive End ：デスティネーションエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。	"CBRE ：オブジェクト受信終了"

コード	説明	を参照してください
CGRR	Cross-Grid Replication Request：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レプリケートするために、グリッド間レプリケーション処理を試行しました。	"CGRR：クロスグリッドレプリケーション要求"
EBDL	Empty Bucket Delete：ILMスキャナが、すべてのオブジェクトを削除中のバケット内のオブジェクトを削除しました（空のバケット処理を実行中）。	"EBDL：空のバケット削除"
EBKR	Empty Bucket Request：ユーザが、空のバケットをオンまたはオフにする（バケットオブジェクトを削除する、またはオブジェクトの削除を停止する）要求を送信しました。	"EBKR：バケット要求が空です"
SCMT	Object Store Commit ：コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になりました。	"SCMT：オブジェクトストアコミット要求"
SREM	Object Store Remove ：コンテンツブロックがグリッドノードから削除され、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

クライアント読み取り監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトを読み出す要求を行うときに記録されます。

コード	説明	によって使用されます	を参照してください
S3SL	S3 Select要求：S3 Select要求がクライアントに返されたあとに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を含めることができます。要求は成功しなかった可能性があります。	S3 クライアント	"S3SL：S3 Select要求"
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。 • 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。	S3 クライアント	"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。	S3 クライアント	"Shea ： S3 ヘッド"

コード	説明	によって使用されます	を参照してください
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。	Swift クライアント	"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。	Swift クライアント	"WHEA ： Swift ヘッド"

クライアント書き込み監査メッセージ

クライアント書き込み監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトを作成または変更する要求を行うときに記録されます。

コード	説明	によって使用されます	を参照してください
OWR	Object Overwrite ：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ログに記録します。	S3およびSwiftクライアント	"OVWR ：オブジェクトを上書き"
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。 • 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。	S3 クライアント	"SDEL ： S3 DELETE"
SPO	S3 POST ：オブジェクトを AWS Glacier ストレージからクラウドストレージプールにリストアするトランザクションの成功をログに記録します。	S3 クライアント	"SPO ： S3 POST"
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。 • 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。	S3 クライアント	"SPUT ： S3 PUT"
SUPD	S3 Metadata Updated ：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トランザクションの成功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トランザクションの成功をログに記録します。	Swift クライアント	"WDEL ： Swift の削除"

コード	説明	によって使用されます	を参照してください
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。	Swift クライアント	"WPUT ： Swift PUT"

管理監査メッセージ

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。

コード	メッセージのタイトルと概要	を参照してください
MGAU	管理 API 監査メッセージ：ユーザ要求のログ。	"MGAU ：管理監査メッセージ"

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）処理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概要	を参照してください
IDEL	ILM Initiated Delete ：この監査メッセージは、 ILM がオブジェクトを削除する処理を開始すると生成されます。	"IDEL ： ILM Initiated Delete"
LCU	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、ストレージスペースを解放するために上書きされたオブジェクトが自動的に削除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"
ORLM の場合	Object Rules Met：この監査メッセージは、ILMルールの指定に従ってオブジェクトデータが格納された場合に生成されます。	"ORLM ：オブジェクトルールが満たされています"

監査メッセージリファレンス

APCT ：クラウド階層からのアーカイブの削除

このメッセージは、 S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが削除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 ID	削除され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
CSIZ	コンテンツサイズ（ Content Size ）	オブジェクトのサイズ（バイト単位）。常に 0 を返します。
RSLT	結果コード	成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	オブジェクトが削除されたクラウド階層の一意の識別子（ UUID ）。

ARCB ：アーカイブオブジェクトの読み出しが開始されました

このメッセージは、アーカイブされたオブジェクトデータの読み出し要求が送信されて読み出しプロセスが開始されたときに生成されます。読み出し要求はすぐに処理されますが、順序を変更してテープなどのリニアなメディアからの読み出し効率を高めることができます。

コード	フィールド	説明
CBID	コンテンツブロック ID	外部アーカイブストレージシステムから読み出すコンテンツブロックの一意の識別子。
RSLT	結果	アーカイブ読み出しプロセスを開始した結果を示します。現在定義されている値： SUCS ：コンテンツ要求が受信され、読み出しのためにキューに登録されました。

この監査メッセージにはアーカイブ読み出しの時間が記録されます。メッセージを対応する ARCE 終了メッセージと照合することで、アーカイブ読み出しの所要時間および処理が成功したかどうかを判断できます。

ARCE ：アーカイブオブジェクトの読み出しが終了しました

このメッセージは、アーカイブノードが外部アーカイブストレージシステムからオブジェクトデータを読み出す試行が完了したときに生成されます。成功した場合、メッセージには、要求されたオブジェクトデータがアーカイブ先から完全に読み取られ、検証に成功したことが示されます。読み出しと検証が完了すると、オブジェクトデータは要求元のサービスに配信されます。

コード	フィールド	説明
CBID	コンテンツブロック ID	外部アーカイブストレージシステムから読み出すコンテンツブロックの一意の識別子。
VLID	ボリューム識別子	データがアーカイブされたボリュームの識別子。コンテンツのアーカイブ先が見つからない場合は、ボリュームID 0が返されます。

コード	フィールド	説明
RSLT	取得結果	アーカイブ読み出しプロセスの完了ステータス： • SUCS ：成功しました • VRFL ：失敗（オブジェクトの検証に失敗） • ARUN ：失敗（外部アーカイブストレージシステムを使用できない） • CANC ：失敗（読み出し処理がキャンセルされた） • GERR ：失敗（一般的なエラー）

このメッセージと対応する ARCB メッセージを組み合わせることで、アーカイブ読み出しの所要時間を特定できます。このメッセージは読み出しが成功したかどうかを示し、失敗した場合には原因 がコンテンツブロックの読み出しに失敗したことを示します。

ARCT ：クラウド階層からアーカイブを取得します

このメッセージは、 S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが読み出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 ID	読み出されたコンテンツブロックの一意の識別子。
CSIZ	コンテンツサイズ（ Content Size ）	オブジェクトのサイズ（バイト単位）。読み出しが成功した場合にのみ正確な値が表示されます。
RSLT	結果コード	成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	外部アーカイブストレージシステムの一意の識別子（ UUID ）。
時間	時間	要求の合計処理時間（マイクロ秒）。

AREM ：アーカイブオブジェクトの削除

Archive Object Remove 監査メッセージは、アーカイブノードからのコンテンツブロックの削除が成功または失敗したことを示します。アーカイブノードが StorageGRID がオブジェクトの場所を解放したことを外部アーカイブストレージシステムに通知した場合、結果は成功です。オブジェクトが外部アーカイブストレージシステムから削除されるかどうかは、システムのタイプと構成によって異なります。

コード	フィールド	説明
CBID	コンテンツブロック ID	外部アーカイブメディアシステムから読み出すコンテンツブロックの一意の識別子。
VLID	ボリューム識別子	オブジェクトデータがアーカイブされていたボリュームの識別子。
RSLT	結果	アーカイブ削除プロセスの完了ステータス： • SUCS ：成功しました • ARUN ：失敗（外部アーカイブストレージシステムを使用できない） • GERR ：失敗（一般的なエラー）

ASCE ：アーカイブオブジェクトストアの終了

このメッセージは、外部アーカイブストレージシステムへのコンテンツブロックの書き込みが終了したことを示します。

コード	フィールド	説明
CBID	Content Block Identifier の略	外部アーカイブストレージシステムに格納されているコンテンツブロックの識別子。
VLID	ボリューム識別子	オブジェクトデータの書き込み先のアーカイブボリュームの一意の識別子。
VREN	検証が有効です	コンテンツブロックに対して検証が実行されるかどうかを示します。現在定義されている値は次のとおり • VENA ：検証が有効になっています • VDSA ：検証は無効です
MCLS	管理クラス	コンテンツブロックが割り当てられている TSM 管理クラスを識別する文字列（該当する場合）。

コード	フィールド	説明
RSLT	結果	アーカイブプロセスの結果を示します。現在定義されている値は次のとおり • SUCS ：成功（アーカイブプロセスが成功） • OFFL ：失敗（アーカイブがオフライン） • VRFL ：失敗（オブジェクトの検証に失敗） • ARUN ：失敗（外部アーカイブストレージシステムを使用できない） • GERR ：失敗（一般的なエラー）

この監査メッセージは、指定されたコンテンツブロックが外部アーカイブストレージシステムに書き込まれたことを意味します。書き込みが失敗した場合は、どこで失敗したかを示す基本的なトラブルシューティング情報が結果として記録されます。より詳細な失敗原因については、 StorageGRID システムでアーカイブノードの属性を調べてください。

ASCT ：アーカイブストアのクラウド階層

このメッセージは、 S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムに、アーカイブされたオブジェクトデータが格納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 ID	読み出されたコンテンツブロックの一意の識別子。
CSIZ	コンテンツサイズ（ Content Size ）	オブジェクトのサイズ（バイト単位）。
RSLT	結果コード	成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	コンテンツ格納先クラウド階層の一意の識別子（ UUID ）。
時間	時間	要求の合計処理時間（マイクロ秒）。

ATCE ：アーカイブオブジェクトストアが開始されました

このメッセージは、外部アーカイブストレージへのコンテンツブロックの書き込みが開始されたことを示します。

コード	フィールド	説明
CBID	コンテンツブロック ID	アーカイブされるコンテンツブロックの一意の識別子。
VLID	ボリューム識別子	コンテンツブロックの書き込み先のボリュームの一意の識別子。処理に失敗した場合は 0 が返されます。
RSLT	結果	コンテンツブロックの転送結果を示します。現在定義されている値は次のとおり • SUCS ：成功（コンテンツブロックは正常に格納されました） • EXIS ：無視（コンテンツブロックはすでに格納されています） • ISFD ：失敗（ディスクスペースが足りません） • STER ：失敗（ CBID の格納エラー） • OFFL ：失敗（アーカイブがオフライン） • GERR ：失敗（一般的なエラー）

AVCC ：アーカイブによってクラウド階層の構成を検証

このメッセージは、クラウド階層 - Simple Storage Service （ S3 ）ターゲットタイプの構成設定が検証されたときに生成されます。

コード	フィールド	説明
RSLT	結果コード	成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	検証対象の外部アーカイブストレージシステムに関連付けられている UUID 。

BROR：バケット読み取り専用要求

この監査メッセージは、バケットが読み取り専用モードになったときまたは終了したときにLDRサービスによって生成されます。たとえば、すべてのオブジェクトが削除されている間にバケットが読み取り専用モードになったとします。

コード	フィールド	説明
BKHD	バケットUUID	バケットID。
ブローブ	バケットの読み取り専用要求値	バケットが読み取り専用になっているか、または読み取り専用のままになっているか（1=読み取り専用、0=読み取り専用ではない）。

コード	フィールド	説明
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なっている理由、または読み取り専用状態のままになっている理由。たとえば、emptyBucketなどです。
S3AI	S3テナントアカウントID	要求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であることを示します。
S3BK	S3バケット	S3 バケット名。

CBRB ：オブジェクト受信が開始されました

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、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したときに転送先のエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理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（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。
CTSS	開始シーケンスカウント（ Start Sequence Count ）	最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。
CTES	想定される終了シーケンス数	最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。

コード	フィールド	説明
RSLT	転送開始ステータス	転送が開始された時点のステータス： SUCS ：転送が開始されました。

この監査メッセージは、 Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「 Start Sequence Count 」から「 Expected End Sequence Count 」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

CBRE ：オブジェクト受信終了

このメッセージは、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したときに転送先のエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理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（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。
CTSS	開始シーケンスカウント（ Start Sequence Count ）	転送が開始されたシーケンスカウントを示します。
CTA	実際の終了シーケンス数	転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、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。

コード	フィールド	説明
RSLT	転送結果	（送信側エンティティから見た）転送処理の結果： 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 ：接続の確立中または転送中に接続がタイムアウトしました UNRE ：デスティネーションノード ID に到達できません CRPT：破損したデータまたは無効なデータの受信が原因で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処理が完了したことを意味します。転送結果が成功した場合は、「 Start Sequence Count 」から「 Actual End Sequence Count 」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、レプリカ数の検証にも使用できます。

CBSB ：オブジェクト送信の開始

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、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したときにソースエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理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（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。

コード	フィールド	説明
CTSS	開始シーケンスカウント（ Start Sequence Count ）	最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。
CTES	想定される終了シーケンス数	最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。
RSLT	転送開始ステータス	転送が開始された時点のステータス： SUCS ：転送が開始されました。

この監査メッセージは、 Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「 Start Sequence Count 」から「 Expected End Sequence Count 」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

CBSE ：オブジェクト送信終了

このメッセージは、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したときに転送元のエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理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（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。

コード	フィールド	説明
CTSS	開始シーケンスカウント（ Start Sequence Count ）	転送が開始されたシーケンスカウントを示します。
CTA	実際の終了シーケンス数	転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、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	（送信側エンティティから見た）転送処理の結果： 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 ：接続の確立中または転送中に接続がタイムアウトしました UNRE ：デスティネーションノード ID に到達できません CRPT：破損したデータまたは無効なデータの受信が原因で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処理が完了したことを意味します。転送結果が成功した場合は、「 Start Sequence Count 」から「 Actual End Sequence Count 」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、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レプリケートするためにグリッド間レプリケーション処理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（バイト単位）。 CSIZ属性はStorageGRID 11.8で導入されました。そのため、StorageGRID 11.7から11.8へのアップグレードにまたがるグリッド間レプリケーション要求で、オブジェクトの合計サイズが不正確になることがあります。
S3AI	S3テナントアカウントID	オブジェクトのレプリケート元のバケットを所有するテナントアカウントのID。

コード	フィールド	説明
GFID	グリッドフェデレーション接続ID	グリッド間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。
オペー	CGR操作	クロスグリッドレプリケーション処理が試行されたタイプ。 • 0 =オブジェクトをレプリケートします • 1 =マルチパートオブジェクトをレプリケートします • 2 =削除マーカーを複製します
S3BK	S3バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。
VSID	バージョン ID	レプリケート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：空のバケット削除

すべてのオブジェクトを削除中のバケット内のオブジェクトがILMスキャナによって削除されました（空のバケット処理を実行中）。

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（バイト単位）。
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	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
RSLT	削除処理の結果	イベント、プロセス、またはトランザクションの結果。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。

EBKR：バケット要求が空です

このメッセージは、ユーザが、空のバケットをオンまたはオフにする（バケットオブジェクトを削除する、または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ています。

コード	フィールド	説明
bUID	バケットUUID	バケットID。
EBJS	空のバケットJSON設定	現在の空のバケットの設定を表すJSONが格納されます。
S3AI	S3テナントアカウントID	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。

ECMC：イレイジャーコーディングされたデータフラグメントの欠落

この監査メッセージは、イレイジャーコーディングされたデータフラグメントの欠落がシステムで検出されたことを示します。

コード	フィールド	説明
VCMC	VCS ID を入力します	欠落しているチャンクが含まれている VCS の名前。
MCID	チャンク ID	欠落しているイレイジャーコーディング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、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。

ECOC：イレイジャーコーディングされたデータフラグメントの破損

この監査メッセージは、イレイジャーコーディングされたデータフラグメントの破損がシステムで検出されたことを示します。

コード	フィールド	説明
Vcco	VCS ID を入力します	破損したチャンクが含まれている VCS の名前。

コード	フィールド	説明
VLID	ボリューム ID	破損したイレイジャーコーディングフラグメントが含まれている RangeDB ボリューム。
CCID	チャンク ID	破損したイレイジャーコーディング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、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」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、 Transport Layer Security （ TLS ）を使用した接続試行が失敗した場合に生成されます。

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 接続の一意のシステム識別子。
RUID	ユーザ ID	リモートユーザの ID を表すサービスに依存する識別子。
RSLT	理由コード	失敗の理由： SCNI ：セキュアな接続を確立できませんでした。 CERM ：証明書がありません。 CERT ：証明書が無効です。 CERE ：証明書が期限切れです。 CERR ：証明書が取り消されています。 CSGN ：証明書の署名が無効です。 CSGU ：証明書の署名者が不明です。 UCRM ：ユーザクレデンシャルがありません。 UCRI ：ユーザクレデンシャルが無効です。 UCRU ：ユーザのクレデンシャルが拒否されました。 TOUT ：認証がタイムアウトしました。

TLS を使用するセキュアなサービスへの接続が確立されると、サービスに組み込まれている TLS プロファイルおよびその他のロジックを使用してリモートエンティティのクレデンシャルが検証されます。無効、想定

外、許可されていない証明書またはクレデンシャルが原因でこの認証が失敗すると、監査メッセージがログに記録されます。これにより、不正アクセスやその他のセキュリティ関連の接続問題を照会できます。

このメッセージは、リモートエンティティの設定が正しくない場合や、無効または許可されていないクレデンシャルをシステムに提示しようとした場合に生成されることがあります。この監査メッセージを監視して、システムへの不正なアクセス試行を検出する必要があります。

GNRG ： **GNDS** 登録

CMN サービスは、 StorageGRID システムで CMN サービスに関する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	更新リクエストの結果： • SUCS ：成功しました • SUNV ：サービスを使用できません • GERR ：その他の失敗
GNID	ノードID	更新要求を開始したサービスのノード ID 。
GNTP	デバイスタイプ	グリッドノードのデバイスタイプ（ LDR サービスの場合は BLDR など）。
GNDV	デバイスモデルのバージョン	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 - クエリランキングのコンテキストで）。
GNIA	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自身のエントリを更新するたびに生成されます。

GNUR ： **GNDS** 登録解除

CMN サービスは、 StorageGRID システムから CMN サービスに関する情報の登録を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： • SUCS ：成功しました • SUNV ：サービスを使用できません • GERR ：その他の失敗
GNID	ノードID	更新要求を開始したサービスのノード ID 。

GTED ： **Grid** 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 Historical テーブルに移動したことを示します。結果が SUCS 、 ABRT 、 ROLF のいずれかである場合は、対応する Grid Task Started 監査メッセージも生成されます。それ以外の結果は、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ます。

コード	フィールド	説明
TSID	タスク ID	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ます。また、グリッドタスクをライフサイクル全体にわたって管理できます。 • 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。
RSLT	結果	グリッドタスクの最終ステータス： • SUCS ：グリッドタスクが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：グリッドタスクは終了し、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前にユーザ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前に期限切れとなりました。 • IVLD ：グリッドタスクは無効でした。 • AUTH ：グリッドタスクは許可されていませんでした。 • DUPL ：グリッドタスクは重複として拒否されました。

GTSt ： Grid 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。この監査メッセージは、内部の Grid Task Submission サービスによって開始されて自動アクティブ化用に選択されているグリッドタスクの Grid Task Submitted メッセージの直後に生成されます。Pending テーブルに送信されるグリッドタスクの場合、このメッセージはユーザがグリッドタスクを開始するときに生成されます。

コード	フィールド	説明
TSID	タスク ID	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ます。また、タスクをライフサイクル全体にわたって管理できます。 • 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。
RSLT	結果	結果。このフィールドの値は 1 つだけです。 • SUCS ：グリッドタスクが正常に開始されました。

GTSU ： Grid 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。 • 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。
ttyp	タスクタイプ（ Task Type ）	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 概要 の略	グリッドタスクの判読可能な概要 。

コード	フィールド	説明
付加価値を提供します	タイムスタンプ後の有効な値	グリッドタスクの有効期間の開始時間（ UNIX 時間 1970 年 1 月 1 日からの UINT64 マイクロ秒数）。
VBTS	タイムスタンプの前に有効です	グリッドタスクの有効期間の終了時間（ UNIX 時間 1970 年 1 月 1 日からの UINT64 マイクロ秒数）。
TsRC	ソース	タスクのソース： • TXTB ：グリッドタスクは、 StorageGRID システム経由で署名付きテキストブロックとして送信されました。 • GRID ：グリッドタスクは、内部の Grid Task Submission サービス経由で送信されました。
ACTV	アクティベーションタイプ	アクティブ化のタイプ： • Auto ：グリッドタスクは自動でアクティブ化されます。 • PEND ：グリッドタスクは Pending テーブルに追加されました。TXTB ソースの場合はこのタイプのみです。
RSLT	結果	送信結果： • SUCS ：グリッドタスクは正常に送信されました。 • FAIL ：タスクは Historical テーブルに直接移動されました。

IDEL ： ILM Initiated Delete

このメッセージは、 ILM によってオブジェクトを削除する処理が開始された場合に生成されます。

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 * ：このメッセージは、保持期間が経過したために ILM によってオブジェクトの自動削除処理が開始された場合に生成されます（自動削除設定が有効になっていて、リーガルホールドがオフの場合）。
- * 非準拠 S3 バケットまたは Swift コンテナ内のオブジェクト * 。このメッセージは、現在オブジェクトに適用されている配置手順がアクティブなILMポリシーにないためにオブジェクトを削除する処理がILMによって開始された場合に生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	オブジェクトの CBID 。

コード	フィールド	説明
CMPA	準拠：自動削除	準拠 S3 バケット内のオブジェクトのみが対象。0 （ false ）または 1 （ true ）。バケットがリーガルホールドの対象である場合を除き、保持期間の終了時に準拠オブジェクトを自動的に削除するかどうかを示します。
テンプレート	コンプライアンス：リーガルホールド	準拠 S3 バケット内のオブジェクトのみが対象。0 （ false ）または 1 （ true ）。バケットが現在リーガルホールドの対象であるかどうかを示します。
CMPR	準拠：保持期間	準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの保持期間の長さ（分）。
CTME	準拠：取り込み時間	準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの取り込み時間。この値に保持期間を分単位で追加することで、オブジェクトをバケットから削除できるタイミングを判断できます。
dmrk	マーカーバージョン ID を削除します	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た削除マーカーのバージョン ID 。バケットに対する処理では、このフィールドは指定されません。
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト単位）。
LOCS	ロケーション	StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、 LOCS の値は "" です。 CLEC：イレイジャーコーディングオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループID。 CLDI ：レプリケート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は、オブジェクトの場所の ARC ノード ID 。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
RSLT	結果	ILM 処理の結果。 SUCS ： ILM 処理が成功しました。

コード	フィールド	説明
ルール	ルールラベル（ Rules Label ）	• 保持期間が経過したために準拠 S3 バケット内のオブジェクトが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る配置手順がない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）	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、オブジェクトが取り込まれたサイトではありません。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、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、ストレージスペースを解放するためにクリーンアップが必要な上書きされたオブジェクトを StorageGRID が削除した場合に生成されます。オブジェクトがすでに含まれているパスに S3 または Swift クライアントがオブジェクトを書き込むと、オブジェクトが上書きされます。削除処理は自動的にバックグラウンドで実行されます。

コード	フィールド	説明
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト単位）。
LTYP	クリーンアップのタイプ	_ 内部使用のみ。 _
LUID （ LUID ）	オブジェクト UUID が削除されました	削除されたオブジェクトの識別子。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
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。

コード	フィールド	説明
UUID	Universally Unique Identifier の略	まだ存在するオブジェクトの ID 。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。

LLST ：ロケーションが失われました

このメッセージは、オブジェクトコピー（レプリケートまたはイレイジャーコーディング）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	イレイジャーコーディングプロファイル	イレイジャーコーディングされたオブジェクトデータ用。使用されているイレイジャーコーディングプロファイルのID。
LTYP	保管場所タイプ	CLDI （ Online ）：レプリケートされたオブジェクトデータ用 CLEC （ Online ）：イレイジャーコーディングされたオブジェクトデータ用 CLNL （ Nearline ）：アーカイブされたレプリケートオブジェクトデータ用
NOID	ソースノード ID	場所が失われたノード ID 。
PCLD	レプリケートオブジェクトへのパス	損失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 （つまりレプリケートオブジェクトの場合）の場合にのみ返されます。 フォームを使用します `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	結果	常に NONE 。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該当しません。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	トリガ元	USER ：ユーザがトリガーしました SYST ：システムがトリガーされました
UUID	Universally Unique ID の略	StorageGRID システムでの該当オブジェクトの識別子。

MGAU ：管理監査メッセージ

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。API に対する GET または HEAD 以外のすべての要求は、応答に加えて要求のユーザ名、 IP 、およびタイプをログに記録します。

コード	フィールド	説明
MDIP	宛先 IP アドレス	サーバ（デスティネーション）の IP アドレス。
MDNA	ドメイン名	ホストのドメイン名。
MPAT	要求のパス	要求のパス。
MPQP	要求クエリパラメータ	要求のクエリパラメータ。
MRBD の略	本文を要求します	要求の本文の内容。応答の本文はデフォルトでログに記録されますが、要求の本文は応答の本文が空の特定のケースでログに記録されます。応答の本文には次の情報が含まれていないため、それぞれの POST メソッドの要求本文から取り込まれます。 • ユーザ名とアカウント ID ： * POST authorize * • 新しいサブネット設定： * POST /grid/grid-networks/update * • 新しい NTP サーバ： * POST /grid/ntp-servers /update * に含まれています • 運用停止されたサーバ ID は、 * POST /grid/servers/decommission * に記載されています • 注： * 機密情報は、削除（ S3 アクセスキーなど）またはアスタリスクでマスク（パスワードなど）されます。
検査	要求メソッド	HTTP 要求メソッド： • 投稿（ Post ） • PUT • 削除 • パッチ
MRSC	応答コード	応答コード。
MRSP	応答の本文	デフォルトでは、応答の内容（応答の本文）がログに記録されます。 • 注： * 機密情報は、削除（ S3 アクセスキーなど）またはアスタリスクでマスク（パスワードなど）されます。

コード	フィールド	説明
MSIP	送信元 IP アドレス	クライアント（送信元）の IP アドレス。
MUUN	ユーザの URN	要求を送信したユーザの 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が返されます。

OLST: システムが損失オブジェクトを検出しました

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ることができない場合に生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	損失オブジェクトの CBID 。
NOID	ノードID	損失オブジェクトが最後に確認された直接またはニアラインの場所（該当する場合）。ボリューム情報がない場合は、ノード ID だけでボリューム ID がないケースもあります。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	該当する場合は、 S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
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、このメッセージには該当しません。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	Universally Unique ID の略	StorageGRID システム内の損失オブジェクトの識別子。
ヴォル	ボリューム ID	使用可能な場合は、損失オブジェクトが最後に確認された場所のストレージノードまたはアーカイブ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ています

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格納およびコピーされた場合に生成されます。

ORLM メッセージは、ポリシー内の別のルールで高度なフィルタ「オブジェクトサイズ」が使用されている場合に、オブジェクトがデフォルトの Make 2 Copies ルールによって格納されたときには生成されません。

コード	フィールド	説明
bUID	バケットヘッダー	バケット ID フィールド。内部処理に使用されます。STAT が PRGD の場合にのみ表示されます。
CBID	Content Block Identifier の略	オブジェクトの CBID 。
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト単位）。
LOCS	ロケーション	StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、 LOCS の値は "" です。 CLEC：イレイジャーコーディングオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループID。 CLDI ：レプリケート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は、オブジェクトの場所の ARC ノード ID 。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
RSLT	結果	ILM 処理の結果。 SUCS ： ILM 処理が成功しました。
ルール	ルールラベル（ Rules Label ）	このオブジェクトに適用されている ILM ルールの判読可能なラベル。
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	コンテナの 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。

コード	フィールド	説明
統計	ステータス	ILM 処理のステータス。 DONE ：オブジェクトに対する ILM 処理が完了しました。 DFER ： ILM によって再評価されるようオブジェクトがマークされました。 PRGD ：オブジェクトが StorageGRID システムから削除されました。 NLOC ：オブジェクトデータを StorageGRID システムで検出できなくなります。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または破損していることを示している可能性があります。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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で作成された新しいオブジェクトのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

ORLM監査メッセージは、1つ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。

- オブジェクトが対応する ILM ルールを無期限に満たしたとき。
- オブジェクトが対応する ILM ルールを一時的に満たしたとき。
- オブジェクトが ILM ルールによって削除されたとき。
- バックグラウンド検証プロセスにより、レプリケート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たとき。StorageGRID システムは、破損したオブジェクトを交換するために ILM 評価を実行します。

関連情報

- "オブジェクトの取り込みトランザクション"
- "オブジェクトの削除トランザクション"

OVWR ：オブジェクトを上書き

このメッセージは、外部（クライアントが要求した）処理によって、あるオブジェクトが別のオブジェクトで上書きされた場合に生成されます。

コード	フィールド	説明
CBID	Content Block Identifier （新規）	新しいオブジェクトの CBID 。

コード	フィールド	説明
CSIZ	前のオブジェクトサイズ	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（前のもの）	既存のオブジェクトの CBID 。
UUID	Universally Unique ID （新規）	StorageGRID システム内での新しいオブジェクトの識別子。
OUID	Universally Unique ID （旧）	StorageGRID システム内での以前のオブジェクトの識別子。
パス	S3 または Swift オブジェクトのパス	既存のオブジェクトと新しいオブジェクトの両方に使用する S3 または Swift オブジェクトのパス
RSLT	結果コード	Object Overwrite トランザクションの結果。常に次の結果になります。 SUCS ：成功しました
SgRP	サイト（グループ）	上書きされたオブジェクトがある場合は指定したサイトで削除されています。このサイトは、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 Select要求

このメッセージは、S3 Select要求がクライアントに返されたあとに完了を記録します。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を含めることができます。要求は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は圧縮されたバイト数を持ち、BYPRは解凍後のバイト数になります。
BYPR	処理されたバイト数	処理されたバイト数。S3 Selectジョブで実際に処理または処理された「スキャンされたバイト数」の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されたバイト数。

コード	フィールド	説明
レポート	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	レコードが返されました	S3 Selectジョブがクライアントに返されたレコードまたは行の数。
JOFI	ジョブは終了しました	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、ジョブは完了しませんでした。エラーフィールドにはデータが含まれている可能性があります。クライアントに結果が一部しか表示されていない場合や、結果がまったく表示されない場合があります。
リード	リクエスト ID	S3 Select要求の識別子。
EXTM	実行時間	S3 Selectジョブが完了するまでにかかった時間（秒）。
ERMG	エラーメッセージ	S3 Selectジョブが生成されたことを示すエラーメッセージ。
アーティ	エラータイプ	S3 Selectジョブが生成したエラータイプ。
エルスト	スタックトレースエラー	S3 Selectジョブが生成したエラーStacktrace。
S3BK	S3バケット	S3 バケット名。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのS3アクセスキーID。
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。
S3KY	S3 キー	バケット名を除く S3 キーの名前。

SADD ：セキュリティ監査無効

このメッセージは、元のサービス（ノード ID ）が監査メッセージのロギングをオフにしたことを示します。監査メッセージの収集や配信は停止しています。

コード	フィールド	説明
AETM	enable メソッド	監査を無効にするために使用されたメソッド。

コード	フィールド	説明
EUN	ユーザ名	監査ログを無効にするコマンドを実行したユーザ名。
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該当しません。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、以前は有効だったロギングが現在は無効になっていることを示します。一般には、システムの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実行される処理です。一括アクティビティ後に監査がリストアされ（ SADE ）、監査を無効にする機能は永続的にブロックされます。

Sade ：セキュリティ監査を有効にします

このメッセージは、元のサービス（ノード ID ）が監査メッセージのロギングをリストアしたことを示します。監査メッセージの収集や配信は再開されています。

コード	フィールド	説明
AETM	enable メソッド	監査を有効にするために使用されたメソッド。
EUN	ユーザ名	監査ログを有効にするコマンドを実行したユーザ名。
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該当しません。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、以前は無効（ SADD ）だったロギングが現在は有効になっていることを示します。一般には、システムの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実行される処理です。一括アクティビティ後に監査がリストアされ、監査を無効にする機能は永続的にブロックされます。

SCMT ：オブジェクトストアのコミット

グリッドコンテンツは、コミット（永続的に格納）されるまでは、使用可能にならず、格納済みとして認識されません。永続的に格納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たコンテンツです。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生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	永続的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格納された時点のステータス： SUCS ：オブジェクトが正常に格納されました。

このメッセージは、コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になったことを意味します。この機能を使用すると、システム内のデータフローを追跡できます。

SDEL ： S3 DELETE

S3クライアントがDELETEトランザクションを実行すると、指定したオブジェクトまたはバケットを削除する要求、またはバケット/オブジェクトサブリソースを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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（ Content Size ）	削除されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
dmrk	マーカーバージョン ID を削除します	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た削除マーカーのバージョン ID 。バケットに対する処理では、このフィールドは指定されません。
GFID	グリッドフェデレーション接続ID	グリッド間レプリケーションの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。デスティネーショングリッドの監査ログにのみ含まれます。
gfsaだ	Gridフェデレーションのソースアカウント ID	グリッド間レプリケーションの削除要求を行うソースグリッド上のテナントのアカウントID。デスティネーション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 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。 x-amz-bypass-governance-retention は、要求に含まれている場合は自動的に追加されます。
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。
RSLT	結果コード	DELETEトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理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（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	説明
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 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SgRP	サイト（グループ）	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、オブジェクトが取り込まれたサイトではありません。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	削除マーカーのUniversally Unique Identifier（汎用一意識別子）	削除マーカーの識別子。監査ログメッセージでは、UUDMまたはUUIDのいずれかを指定します。UUDMはオブジェクトの削除要求によって作成された削除マーカー、UUIDはオブジェクトを示します。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

SGET ： S3 GET

S3クライアントがGETトランザクションを実行すると、オブジェクトを読み出したりバケット内のオブジェクトをリストしたり、バケット/オブジェクトサブリソースを削除したりする要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。

コード	フィールド	説明
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。
能力	ListObjectsV2	_v2 format_responseが要求されました。詳細については、を参照してください "AWS ListObjectsV2"。GET Bucket処理の場合のみ。
NCHD	子の数	キーと共通のプレフィックスが含まれます。GET Bucket処理の場合のみ。
rang	範囲の読み取り	範囲読み取り処理の場合のみ。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。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

コード	フィールド	説明
S3SR	S3 サブリソース	必要に応じて、処理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（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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。
TRNC	切り捨てられる、または切り捨てられない	すべての結果が返された場合はfalseに設定されます。より多くの結果が返される場合はtrueに設定します。GET Bucket処理の場合のみ。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

Shea ： S3 ヘッド

S3 クライアントが HEAD トランザクションを実行すると、オブジェクトまたはバケットの存在をチェックし、オブジェクトに関するメタデータを読み出す要求が送信されま

す。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
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（ Content Size ）	チェックしたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。
RSLT	結果コード	GETトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。

コード	フィールド	説明
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

SPO ： S3 POST

S3 クライアントが POST Object 要求を実行すると、トランザクションが成功した場合にサーバによってこのメッセージが生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。

コード	フィールド	説明
CSIZ	コンテンツサイズ（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。 （SPOSでは想定されません）。
RSLT	結果コード	RestoreObject要求の結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。 S3 Select処理の場合は、を「select」に設定します。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。

コード	フィールド	説明
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SRCF	サブリソースの設定	リストア情報。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

SPUT ： S3 PUT

S3クライアントがPUTトランザクションを実行すると、新しいオブジェクトまたはバケットを作成する要求、またはバケット/オブジェクトサブリソースを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。

コード	フィールド	説明
CMP	コンプライアンス設定	バケットの作成時に使用された準拠設定（要求に存在する場合）（最初の1024文字に切り詰められます）。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
GFID	グリッドフェデレーション接続ID	グリッド間レプリケーション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。デスティネーショングリッドの監査ログにのみ含まれます。
gfsaだ	Gridフェデレーションのソースアカウント ID	グリッド間レプリケーションPUT要求を行うソースグリッド上のテナントのアカウントID。デスティネーショングリッドの監査ログにのみ含まれます。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。 x-amz-bypass-governance-retention は、要求に含まれている場合は自動的に追加されます。
LKEN	オブジェクトロックが有効になりました	要求ヘッダーの値 x-amz-bucket-object-lock-enabled（リクエストに存在する場合）。
LKLH	オブジェクトロックリーガルホールド	要求ヘッダーの値 x-amz-object-lock-legal-hold（PutObject要求に存在する場合）。
LKMD	オブジェクトロック保持モード	要求ヘッダーの値 x-amz-object-lock-mode（PutObject要求に存在する場合）。

コード	フィールド	説明
LKRU	オブジェクトロック終了日まで保持	要求ヘッダーの値 `x-amz-object-lock-retain-until-date`（PutObject要求に存在する場合）。
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。
RSLT	結果コード	PUT トランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理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（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SRCF	サブリソースの設定	新しいサブリソース設定（最初の 1024 文字に切り詰められます）。

コード	フィールド	説明
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	ID をアップロードします	CompleteMultipartUpload処理の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、アセンブルされたことを示します。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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で作成された新しいオブジェクトのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。
VSST	バージョン管理の状態	バケットの新しいバージョン管理状態。「enabled」または「suspended」の2つの状態が使用されます。 オブジェクトに対する処理には、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、コンテンツが永続的ストレージから削除され、通常の API でアクセスできなくなった場合に表示されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	永続的ストレージから削除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	コンテンツ削除処理の結果を示します。次の値のみが定義されています。 SUCS ：コンテンツが永続的ストレージから削除されました

この監査メッセージは、指定された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。このメッセージを使用して、システム内の削除されたコンテンツのフローを追跡できます。

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まれた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。このメッセージは、メタデータの更新が成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	バケットの準拠設定の更新時に要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。
RSLT	結果コード	GETトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

コード	フィールド	説明
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

SVRF ：オブジェクトストアの検証に失敗しました

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したときに生成されます。レプリケートされたオブジェクトデータがディスクに対して読み書きされるたびに、要求元ユーザに送信されるデータがシステムにもともと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複数の検証チェック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、破損したレプリケートオブジェクトデータは再び読み出されないように自動的に隔離されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	検証に失敗したコンテンツブロックの一意の識別子。
RSLT	結果コード	検証失敗のタイプ： CRCF ：巡回冗長検査（ CRC ）が失敗しました。 HMAC ：ハッシュベースのメッセージ認証コード（ HMAC ）チェックが失敗しました。 EHSH ：暗号化されたコンテンツハッシュが想定外です。 PHSH ：元のコンテンツハッシュが想定外です。 SEQC ：ディスク上のデータシーケンスが正しくありません。 PERR ：ディスクファイルの構造が無効です。 DERR ：ディスクエラーです。 FNAM ：ファイル名が無効です。

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、ハードウェア障害の兆候を示している可能性があります。

メッセージをトリガーした処理を確認するには、 AMID （ Module ID ）フィールドの値を参照してください。たとえば、 SVFY はバックグラウンド検証である Storage Verifier モジュールによってメッセージが生成されたことを示し、 STOR はコンテンツの読み出しによってメッセージがトリガーされたことを示します。

SVRU ：オブジェクトストア検証が不明です

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レプリケート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、レプリケートされたオブジェクトデータの不明または想定外のコピーがオブジェクトストアで検出されて隔離ディレクトリに移動されたときに生成されます。

コード	フィールド	説明
FPTH	ファイルパス	想定外の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該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。

SVRU：Object Store Verify Unknown監査メッセージは注意深く監視する必要があります。オブジェクトストアでオブジェクトデータの想定外のコピーが検出されたことを意味します。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、この状況をすぐに調査してこれらのコピーが作成された方法を特定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ためにこのメッセージが生成されます。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、通常、このメッセージは次回の再起動後にのみ送信されます。サービスが再起動していない場合は、シャットダウンシーケンスの最初に送信された SYST メッセージを確認します。

コード	フィールド	説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS ：システムはクリーンシャットダウンされました。

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。SYSDのRSLTは、「クリーン」シャットダウンによってのみ生成されるため、「ダーティー」シャットダウンを示すことはできません。

SYST ：ノードを停止しています

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て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ためにこのメッセージが生成されます。SYST を使用すると、シャットダウンが要求されたかどうかをサービスが再起動される前に特定できます（ SYSD は通常、サービスの再起動後に送信されます）。

コード	フィールド	説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS ：システムはクリーンシャットダウンされました。

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。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生成されるため、「ダーティー」シャットダウンを示すことはできません。

SYSU ：ノードが開始されました

サービスが再起動されると、前回のシャットダウンがクリーン（コマンドによるもの）か不規則（想定外）かを示すため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
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS ：システムはクリーンシャットダウンされました。 DSDN ：システムはクリーンシャットダウンされませんでした。 VRGN ：サーバインストール（または再インストール）後の初めての起動です。

このメッセージが示すのはレポート元のサービスの起動のみで、ホストサーバの起動については示されません。このメッセージは、次の場合に使用できます。

- 監査証跡における不連続を検出します。
- サービスが処理中に失敗していないかどうかを確認します（ StorageGRID システムの分散によってこれらのエラーが隠されることがあります）。失敗したサービスは、 Server Manager によって自動的に再開されます。

WDEL ： Swift の削除

Swift クライアントが DELETE トランザクションを実行すると、指定したオブジェクトまたはコンテナを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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（ Content Size ）	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 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。

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。常に次の結果になります。 SUCS ：成功しました
saip	要求元クライアントの IP アドレス	要求を送信し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）	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、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	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 オブジェクトの識別子。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	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名。

wget ： Swift GET

Swift クライアントが GET トランザクションを実行すると、オブジェクトを読み出す、コンテナ内のオブジェクトを一覧表示する、またはアカウント内のコンテナを一覧表示する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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関する操作には、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（ Content Size ）	読み出され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関する操作には、このフィールドは含まれません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。
RSLT	結果コード	GETトランザクションの結果。結果は常にです SUCS ：成功しました
saip	要求元クライアントの IP アドレス	要求を送信したクライアントアプリケーションの IP アドレス。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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。アカウントの操作には、このフィールドは含まれません。
WOBJ	Swift オブジェクト	Swift オブジェクトの識別子。アカウントおよびコンテナに関する操作には、このフィールドは含まれません。
WUSR	Swift アカウントユーザ	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名。

WHEA ： Swift ヘッド

Swift クライアントが HEAD トランザクションを実行すると、アカウント、コンテナ、またはオブジェクトの存在をチェックし、関連するメタデータを読み出す要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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関する操作には、このフィールドは含まれません。
CSIZ	コンテンツサイズ（ Content Size ）	読み出され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関する操作には、このフィールドは含まれません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。
RSLT	結果コード	HEADトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
saip	要求元クライアントの IP アドレス	要求を送信したクライアントアプリケーションの IP アドレス。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 。

コード	フィールド	説明
WCON	Swift コンテナ	Swift コンテナ名。アカウントの操作には、このフィールドは含まれません。
WOBJ	Swift オブジェクト	Swift オブジェクトの識別子。アカウントおよびコンテナに関する操作には、このフィールドは含まれません。
WUSR	Swift アカウントユーザ	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名。

WPUT ： Swift PUT

Swift クライアントが PUT トランザクションを実行すると、新しいオブジェクトまたはコンテナを作成する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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（ Content Size ）	読み出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 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。
RSLT	結果コード	PUT トランザクションの結果。常に次の結果になります。 SUCS ：成功しました
saip	要求元クライアントの IP アドレス	要求を送信したクライアントアプリケーションの IP アドレス。

コード	フィールド	説明
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 オブジェクトの識別子。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	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。