監査ログを確認する
StorageGRID software

NetApp
July 23, 2026

目次

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およびコンテンツ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り、分析することができます。

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、システムの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負う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、管理ノード上で設定済みの監査共有フォルダへのアクセス権が必要です。

監査メッセージレベルの設定と外部 syslog サーバーの使用については、"ログ管理と外部 syslog サーバの設定"を参照してください。

監査メッセージが**StorageGRID**システムを通じて保存用の**audit.log**ファイルにどのように移動するか

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 `audit.log`ファイルへ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。

監査メッセージおよび監査メッセージの保持に関する以下のワークフローは、StorageGRID が 管理ノード/ローカルノード または 管理ノードと外部 **syslog** サーバー 用に構成されている場合にのみ適用されます。StorageGRID が「ローカルノードのみ」（デフォルト）または「外部 syslog サーバー」に設定されている場合、監査メッセージは各ノードの `/var/local/log/localaudit.log`ファイルにローカルに保存され、管理ノードまたはストレージノードで処理することはできません。

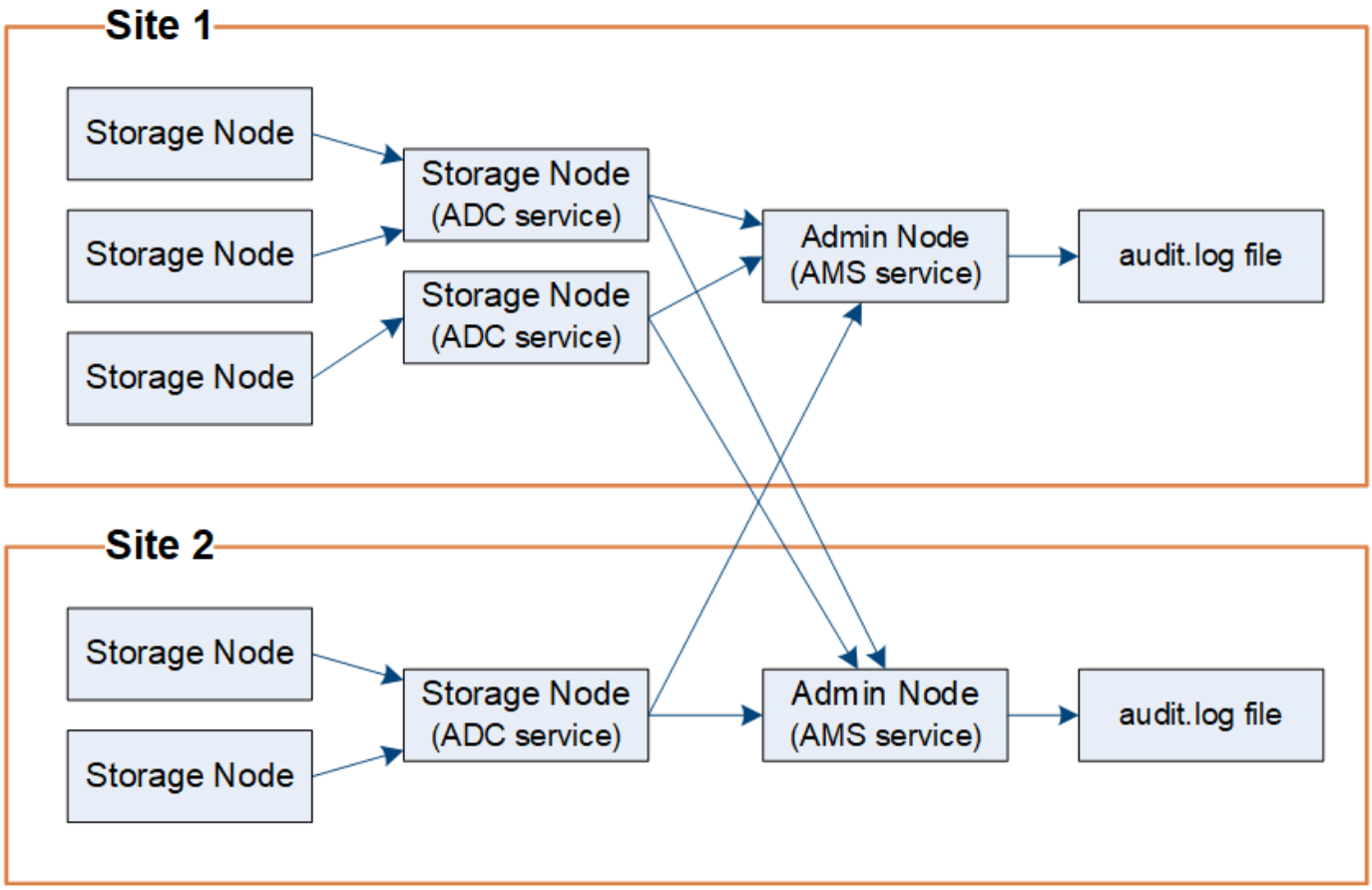
監査メッセージフロー

監査メッセージは、StorageGRID が 管理ノード/ローカルノード または 管理ノードと外部 **syslog** サーバーに設定されている場合は管理ノードによって、また管理ドメインコントローラー（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ADCサービスのいずれかに送信します。ADCサービスは、各サイトに設置された最初の3台のストレージノードに対して自動的に有効化されます。

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、各管理ノードはシステムアクティビティの完全な記録を保持します。

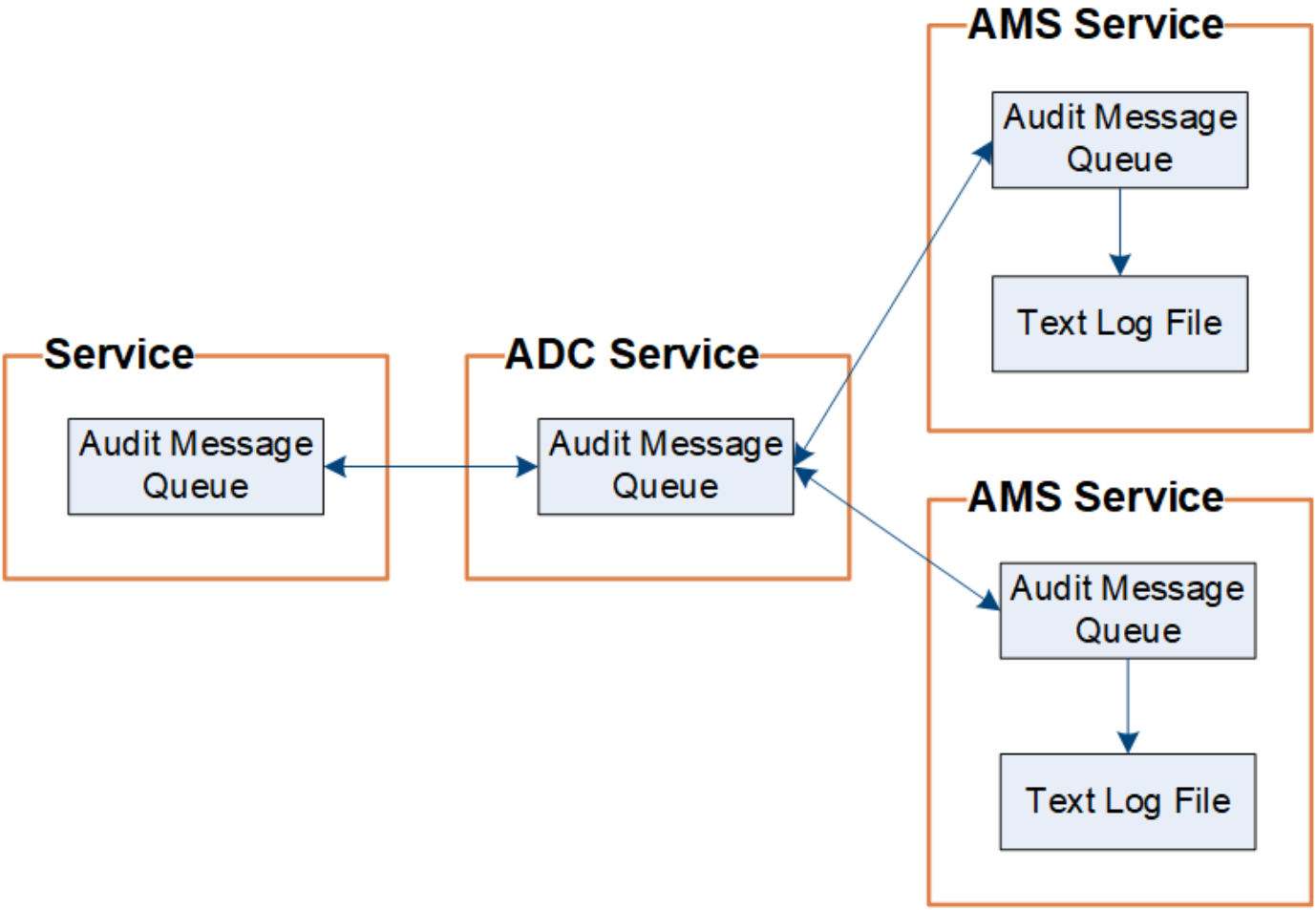
各管理ノードは監査メッセージをテキストログファイルに保存します。アクティブなログファイルの名前は `audit.log`です。



監査メッセージの保持

StorageGRID は、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、コピーと削除のプロセスを使用します。

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、メッセージが管理ノードの `/var/local/audit/export`ディレクトリの監査ログファイルに書き込まれるまで、常に監査メッセージキューに保持されます。これは、監査メッセージが転送中に失われるのを防ぐのに役立ちます。



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。キューが増えると、各ノードの `/var/local/`ディレクトリの利用可能なスペースをより多く消費します。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った場合、各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の受信ができなくなります。

具体的には、以下のような動作が見られる可能性があります。

- `/var/local/audit/export`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なくなるまで、管理ノードは新しい監査メッセージに対して利用不可としてフラグが立てられます。S3クライアントからのリクエストには影響はありません。XAMS（到達不能監査リポジトリ）アラームは、監査リポジトリにアクセスできなくなった場合にトリガーされます。
- ADCサービスを使用しているストレージノードが使用する `/var/local/`ディレクトリが92%まで使用されると、ディレクトリの使用率が87%になるまで、そのノードは監査メッセージに対して利用不可としてフラグが設定されます。他のノードへのS3クライアントリクエストは影響を受けません。NRLY（利用可能な監査リレー）アラームは、監査リレーに到達できない場合にトリガーされます。

> ADC サービスで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 `/var/local/log/localaudit.log`ファイルにローカルに保存します。

- `/var/local/`ディレクトリの使用量がStorage Nodeで85%に達すると、ノードは `503 Service Unavailable`でS3クライアントリクエストの受け付けを拒否し始めます。

以下のような問題が発生すると、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サービスを使用している管理ノードまたはストレージノードの障害。システムのノードのいずれかがダウンした場合、残りのノードに処理が滞留す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。
- ADC Storage Nodeの `/var/local/`スペースが、監査メッセージとは無関係の理由でいっぱいになることがあります。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、現在のバックログを優先するため、他のノードにもバックログが発生する可能性があります。

大規模監査キューアラートおよび監査メッセージキューイング（**AMQS**）アラーム

監査メッセージキューのサイズを長期的に監視できるように、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。

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、まずシステムの負荷を確認してください。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とともに解消されるため、無視しても問題ありません。

アラートまたはアラームが継続し、深刻度が増す場合は、キューのサイズを示すグラフを確認してください。その数値が数時間または数日かけて着実に増加している場合、監査負荷がシステムの監査処理能力を超えている可能性が高いです。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」に変更することで、クライアントの操作頻度を下げたり、ログに記録される監査メッセージの数を減らしたりできます。参照："ログ管理と外部 syslog サーバの設定"

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。そのため、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。

StorageGRID 管理ノードのコマンドラインから監査ログファイルにアクセスする

監査共有には、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が含まれています。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。

StorageGRID を 管理ノード/ローカルノード または 管理ノードと外部 **syslog** サーバ 用に設定しない限り、`audit.log` ファイルは空のままです。詳細については、"ログの保存場所を選択" を参照してください。

開始する前に

- "特定のアクセス権限"があります。
- `Passwords.txt`ファイルが必要です。
- 管理ノードのIPアドレスを知っている必要があります。

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. `Passwords.txt`ファイルに記載されているパスワードを入力してください。

c. 以下のコマンドを入力して root に切り替えます： `su -`

d. `Passwords.txt`ファイルに記載されているパスワードを入力してください。

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

2. 監査ログファイルが格納されているディレクトリに移動します。

```
cd /var/local/audit/export/
```

3. 必要に応じて、現在または保存済みの監査ログファイルを表示します。

StorageGRIDにおける監査ログファイルのローテーションについて学ぶ

StorageGRID が 管理ノード/ローカルノード または 管理ノードと外部 **syslog** サーバー用に設定されている場合、監査ログファイルは管理ノードの `/var/local/audit/export/`ディレクトリに保存されます。アクティブな監査ログファイルの名前は `audit.log`です。

> オプションで、監査ログの送信先を変更し、監査情報を外部 syslog サーバーに送信できます。外部 syslog サーバーが設定されている場合も、監査レコードのローカルログは引き続き生成および保存されます。"監査メッセージと外部 syslog サーバの設定"を参照してください。

1日に1回、アクティブな `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、保存日時を次の形式で示します： `*yyyy-mm-dd.txt*`1日に複数の監査ログが作成された場合、ファイル名にはファイルが保存された日付に番号を付加した形式が使用されます： `*yyyy-mm-dd.txt.n*`たとえば、 `2018-04-15.txt`と `2018-04-15.txt.1`は、2018年4月15日に作成および保存された1番目と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、元の日付を保持する次の形式で名前が変更されます： `*yyyy-mm-dd.txt.gz*`時間の経過とともに、監査ログ用に割り当てられた管理ノードのストレージ容量が消費されます。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/audit/export/`ディレクトリのスペースを解放します。監査ログは作成日を基準に削除されます。古いログから順に削除されます。スクリプトの動作は、以下のファイルで監視できます： `/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`）を示しています。

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

監査ログファイル形式

StorageGRIDの監査ログファイルの形式について学ぶ

監査ログファイルはすべての管理ノードに存在し、個々の監査メッセージの集合が含まれています。

各監査メッセージには、以下の内容が含まれています。

- 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形式で記述し、その後にスペースを挿入します：

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

- 監査メッセージ自体は角括弧で囲まれ、 `AUDT`で始まります。

以下の例は、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を追加しています）。これらのメッセージは、テナントがS3バケットを作成し、そのバケットに2つのオブジェクトを追加した際に生成されました。

```
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):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

監査ログファイル内の監査メッセージは、デフォルトの形式では読みにくく、解釈も容易ではありません。"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略化されたサマリーを取得できます。"audit-sumツール"を使用して、ログに記録された書き込み、読み取り、および削除操作の回数と、これらの操作にかかった時間をまとめることができます。

audit-explainツールを使用してStorageGRID監査メッセージを翻訳する

`audit-explain`ツールを使用して、監査ログ内の監査メッセージを読みやすい形式に変換できます。

開始する前に

- "特定のアクセス権限"があります。
- `Passwords.txt`ファイルが必要です。
- プライマリ管理ノードのIPアドレスを知っている必要があります。

タスク概要

`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略化された要約を提供します。

> この `audit-explain`ツールは、主にテクニカルサポート担当者がトラブルシューティング作業を行う際に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の運用に影響を与える場合があります。

この例は、 `audit-explain`ツールの一般的な出力を示しています。これら4つの"SPUT"監査メッセージは、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/audit/export/*
```

- パイプからの入力を受け付け、`grep`コマンドやその他の手段を使用して入力をフィルタリングおよび前処理することができます。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場合があります。ファイル全体ではなく、確認したい部分をフィルタリングして`audit-explain`を実行することで、時間を節約できます。

> `audit-explain`ツールは、圧縮ファイルをパイプ入力として受け付けません。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、`zcat`ツールを使用してファイルを最初に解凍してください。例：

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

`help (-h)`オプションを使用して、利用可能なオプションを確認します。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. `Passwords.txt`ファイルに記載されているパスワードを入力してください。
   c. 以下のコマンドを入力して root に切り替えます： `su -`
   d. `Passwords.txt`ファイルに記載されているパスワードを入力してください。

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

2. 次のコマンドを入力してください。ここで、`/var/local/audit/export/audit.log`は分析するファイルの名前と場所を表します：

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

   `audit-explain`ツールは、指定されたファイル内のすべてのメッセージを人間が読みやすい形式で出力します。

   行の長さを短縮し、読みやすさを向上させるため、デフォルトではタイムスタンプは表示されません。タイムスタンプを表示したい場合は、タイムスタンプ (`-t`) オプションを使用してください。

audit-sumツールを使用してStorageGRID監査メッセージを要約する

`audit-sum`ツールを使用して、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、最大、平均時間（またはサイズ）を確認できます。

開始する前に

- "特定のアクセス権限"があります。
- あなたは `Passwords.txt`ファイルを持っています。
- プライマリ管理ノードのIPアドレスを把握している必要があります。

タスク概要

`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、および削除操作の回数と、これらの操作にかかった時間を要約します。

The `audit-sum`ツールは、主にテクニカルサポート担当者がトラブルシューティング作業を行う際に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、StorageGRIDの運用に影響を与える場合があります。

この例は、 `audit-sum`ツールの一般的な出力を示しています。この例は、プロトコル操作にかかっ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、監査ログ内の以下のS3およびILM監査メッセージの件数と時刻を提供します。

監査コードは、機能が廃止されると、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見つかった場合は、古い StorageGRID リリースについて、このトピックの以前のバージョンを確認してください。例えば、 "StorageGRID 11.8 監査合計ツールの使用"。

Code	説明	参照先
IDEL	ILMによる削除開始：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を記録します。	"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トランザクションが成功したことをログに記録します。	"SDEL：S3 DELETE"
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トランザクションが成功したことをログに記録します。	"SGET：S3 GET"
SHEA	S3 HEAD: オブジェクトまたはバケットの存在を確認するために、トランザクションが成功したことをログに記録します。	"SHEA：S3 HEAD"
SPUT	S3 PUT：新しいオブジェクトまたはバケットを作成するトランザクションが成功したことをログに記録します。	"SPUT：S3 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/audit/export/*
```

- パイプからの入力を受け付け、`grep`コマンドやその他の手段を使用して入力をフィルタリングおよび前処理することができます。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入力として受け付けません。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、 `zcat`ツールを使用してファイルを最初に解凍してください。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すると、バケットに対する操作をオブジェクトに対する操作とは別に集計したり、メッセージの概要をバケット名、期間、またはターゲットタイプごと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、平均操作時間が表示されますが、 `size (-s)`オプションを使用して代わりにオブジェクトのサイズを確認することもできます。

`help (-h)`オプションを使用して、利用可能なオプションを確認します。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. `Passwords.txt`ファイルに記載されているパスワードを入力してください。
   c. 以下のコマンドを入力して root に切り替えます： `su -`
   d. `Passwords.txt`ファイルに記載されているパスワードを入力してください。

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

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、次の手順に従ってください。
   a. 次のコマンドを入力してください。ここで、 `/var/local/audit/export/audit.log`は分析するファイルの名前と場所を表します：

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

      この例は、 `audit-sum`ツールの一般的な出力を示しています。この例は、プロトコル操作にかかっ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、SGET（S3 GET）操作が平均1.13秒と最も遅いですが、SGETとSPUT（S3 PUT）操作はどちらも最悪ケースで約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(`-l`）を追加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、監査ログから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grepで検索できます。

```
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/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
```

+ この出力例からわかるように、最も処理速度の遅い3つのS3 GETリクエストは、約5GBのサイズのオブジェクトに対するものであり、これは他のオブジェクトよりもはるかに大きいサイズです。データのサイズが大きいことが、最悪の場合のデータ取得時間の遅延の原因となっています。

3. グリッドに取り込まれるオブジェクトとグリッドから取り出されるオブジェクトのサイズを判定したい場合は、サイズオプション (`-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2.5 MB未満ですが、SGETの平均サイズははるかに大きくなっています。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、これはほとんどのオブジェクトが取得されていないことを示しています。

4. 昨日のデータ取得が遅かったかどうかを確認する場合は、次の手順に従ってください。

   a. 適切な監査ログでコマンドを実行し、時間によるグループ化オプション（(`-gt`）に続いて、時間区分（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
```

これらの結果は、S3 GETトラフィックが午前6時から午前7時の間に急増したことを示しています。この期間中、最大時間と平均時間はどちらもかなり長くなっており、カウント数の増加に伴って徐々に増加したわけではありません。これらの指標は、ネットワークまたはグリッドのリクエスト処理能力において、容量が超過したことを示唆しています。

b. 昨日、毎時間どのサイズのオブジェクトが取得されていたかを確認するには、サイズオプション (`-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
```

これらの結果は、全体のデータ取得トラフィックが最大になったときに、非常に大規模なデータ取得がいくつか発生したことを示しています。

c. 詳細を表示するには、"audit-explain ツール"を使用して、その時間帯のすべての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`コマンドを追加して、監査ログファイルの内容を1ページ（1画面）ずつ表示します。

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場合は、次の手順を実行します。

a. まず、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 `-go`オプションを使用します：

```
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
```

結果から、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が明らかになりました。

b. どのバケットのSPUT操作が最も遅いかを判断するには、メッセージをバケットごとにグループ化する `-gb`オプションを使用します。

```
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. バケットの中でSPUTオブジェクトサイズが最大となるものを特定するには、 `-gb`と `-s`の両方のオプションを使用します：

```
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
```

監査メッセージ形式

StorageGRID監査メッセージの構造について学ぶ

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、報告されているイベントまたはアクティビティを説明する具体的な内容が含まれています。

"audit-explain"および"audit-sum"ツールが提供する要約情報が不十分な場合は、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可能性のあ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。文字列全体は括弧（`[ ]`）で囲まれており、文字列内の各属性要素には以下の特性があります：

- 括弧で囲まれています `[ ]`
- 文字列 `AUDT`によって導入され、監査メッセージを示します
- 前後に区切り文字（カンマやスペース）を入れずに
- 改行文字で終了 `\n`

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

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

メッセージに含まれる属性要素の数は、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るわけではありません。

以下に属性要素について説明します。

- `ATTR` は、報告対象の属性を表す4文字のコードです。監査メッセージには、すべての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を示す4文字の識別子です。型は括弧で囲まれています `( )`。
- `value`は属性の内容であり、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。

StorageGRID監査メッセージのデータ型

監査メッセージ内の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。

Type	説明
UI32を使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	符号なし倍長整数（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を使用したチャンク アップロード署名要求がサポートされるようになりました。	4文字の定数。32ビットの符号なし整数値で、「ABCD」などの4つのASCII文字で表されます。
IPAD	IPアドレスに使用されます。

Type	説明
CSTR	UTF-8文字の可変長配列。文字は、以下の規則に従ってエスケープできます。 • 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。 • 改行は \n です。 • 文字は、その16進数の等価値（形式は\xHH、HHは文字を表す16進数値）に置き換えることができます。

StorageGRID監査メッセージ内の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す。

メッセージ自体を識別する開始 `[AUDT:`コンテナに続き、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。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\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"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][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

`ATYP`要素（例では下線が引かれている部分）は、どのイベントがメッセージを生成したかを識別します。この例のメッセージにはlink:shea-s3-head.html["SHEA"]
メッセージコード（[ATYP(FC32):SHEA]）が含まれており、S3
HEADリクエストが成功したことによって生成されたことを示します。

StorageGRID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。

Code	Type	説明
AMID	FC32を使用したチャンク アップロード署名要求がサポートされるようになりました。	モジュール ID：メッセージを生成したモジュール ID を示す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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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。各サービスには、StorageGRIDシステムの設定と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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	シーケンスカウント：以前のリリースでは、このカウンターはグリッドノード（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。
ATID	UI64を使用したチャンク アップロード署名要求がサポートされるようになりました。	トレースID：単一のイベントによって発生した一連のメッセージ間で共有される識別子。
ATIM	UI64を使用したチャンク アップロード署名要求がサポートされるようになりました。	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発生した時刻。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に利用可能なツールのほとんどは、ミリ秒単位に基づいていることに注意してください。 記録されたタイムスタンプの丸め処理または切り捨て処理が必要になる場合があります。監査メッセージの先頭に表示される人間が読める時刻は、 `audit.log`ファイルのISO 8601形式のATIM属性です。日付と時刻は `*YYYY-MMDDTHH:MM:SS.UUUUUU*` のように表されます。 `T`は、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*` はマイクロ秒です。

Code	Type	説明
ATYP	FC32を使用したチャンク アップロード署名要求がサポートされるようになりました。	イベントタイプ：ログに記録されるイベントを識別する4文字の識別子。これはメッセージの「ペイロード」の内容（含まれる属性）を制御します。
AVER	UI32を使用したチャンク アップロード署名要求がサポートされるようになりました。	バージョン：監査メッセージのバージョン。StorageGRID ソフトウェアの進化に伴い、サービスの新しいバージョンには監査レポートに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 サービスにおける下位互換性が確保され、旧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を使用したチャンク アップロード署名要求がサポートされるようになりました。	結果：イベント、プロセス、またはトランザクションの結果。メッセージに関係がない場合は、SUCS の代わりに NONE が使用され、メッセージが誤ってフィルタリングされることを防ぎます。

StorageGRID監査メッセージの形式と例

各監査メッセージには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、 `audit.log`ファイルに表示される可能性のある監査メッセージの例です：

```
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):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

監査メッセージには、記録対象の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。

監査メッセージに記録されているイベントを特定するには、ATYP属性（以下で強調表示）を探してください：

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

以下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\(CSTR\):"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イベントが発生した日時を知るには、監査メッセージの冒頭にある協定世界時（UTC）のタイムスタンプを確認してください。この値は、監査メッセージ自体のATIM属性を人間が読みやすい形式にしたものです：

```
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エポックの開始からの経過時間をマイクロ秒単位で記録します。この例では、値`1405631878959669`は、2014年7月17日木曜日 21:17:59 UTC に相当します。

監査メッセージとオブジェクトのライフサイクル

StorageGRIDで監査メッセージが生成される場合

監査メッセージは、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

たびに生成されます。これらのトランザクションは、監査ログ内でS3 API固有の監査メッセージを探すことで特定できます。

監査メッセージは、各プロトコル固有の識別子によってリンクされています。

Protocol	Code
S3オペレーションの連携	S3BK（バケット）、S3KY（キー）、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ずれ、オブジェクトのサイズ、ネットワーク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ものと異なる場合があります。

StorageGRID でのオブジェクト取り込みトランザクションの監査メッセージ

監査ログ内でS3 API固有の監査メッセージを探すことで、クライアントのデータ取り込みトランザクションを特定できます。

以下の表には、取り込みトランザクション中に生成されるすべての監査メッセージが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を追跡するため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

Code	Name	説明	トレース	詳細については、
SPUT	S3 PUTトランザクション	S3へのPUTによるデータ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	対象ルールを満たしました	このオブジェクトについては、ILMポリシーの要件が満たされています。	CBID	"ORLM: オブジェクトルールを満たしました"

例：**S3**オブジェクトの取り込み

以下に示す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際に生成され、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、有効なILMポリシーには「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るすべての監査メッセージが記載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）に関連するもののみが表示されます。

この例では、S3バケットが既に作成されてい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ための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(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を満たしました

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たことを示しています。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。

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を示す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]]
```

イレイジャー コーディングオブジェクトの場合、LOCSフィールドにはイレイジャー 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、S3バケットとキー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]]
```

StorageGRIDにおけるオブジェクト削除トランザクションの監査メッセージ

S3 API固有の監査メッセージを探すことで、監査ログ内のオブジェクト削除トランザクションを特定できます。

以下の表には、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を追跡するために必要なメッセージのみが含まれます。

S3 削除監査メッセージ

Code	Name	説明	トレース	詳細については、
SDEL	S3 Delete	バケットからオブジェクトを削除するよう要求されました。	CBID、S3KY	"SDEL：S3 DELETE"

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。

以下の例には、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記載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）に関連するもののみが表示されます。

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 リクエスト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):"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]]
```

StorageGRID のオブジェクト取得トランザクションの監査メッセージ

S3 API固有の監査メッセージを探すことで、監査ログ内のオブジェクト取得トランザクションを特定できます。

以下の表には、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を追跡するため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

Code	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リクエストが送信されました。	CBID、S3BK、S3KY	"SGET：S3 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。

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、以下の例に記載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）に関連するもののみが表示されます。

SGET：**S3 GET**

オブジェクトの取得は、クライアントが LDR サービスに GetObject リクエスト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][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。

次の例のメッセージでは、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。これは、S3AIと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_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。

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、以下の例に記載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）に関連するもののみがリストされています。

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リクエストの認可を実行するメッセージ（S3SRフィールドが「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標準の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]]
```

StorageGRIDにおけるS3オブジェクトのメタデータ更新に関する監査メッセージ

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

Code	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が正常に完了したことを示して

います。

SUPD: S3メタデータ更新

S3クライアントは、S3オブジェクト（S3KY）の指定されたメタデータ（(`x-amz-meta-*`）を更新するリクエスト（SUPD）を行います。この例では、監査プロトコルヘッダーとして設定されているため、リクエストヘッダーがフィールド HTRH に含まれています（*設定* > 監視 > 監査と **syslog** サーバ）。"ログ管理と外部 syslog サーバの設定"を参照してください。

```
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

StorageGRIDの監査メッセージの種類とコードについて学ぶ

システムから返される監査メッセージの詳細な説明は、以下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ごとに関連するメッセージをグループ化した表に一覧表示されます。これらのグループ分けは、監査対象となるアクティビティの種類を理解する上でも、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上でも役立ちます。

監査メッセージは、4文字のコードに基づいて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リストを使えば、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。

この章全体を通して使用される4文字のコードは、次のメッセージ例に示すように、監査メッセージに含まれる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、ログ出力先の変更、および監査情報用の外部 syslog サーバーの使用については、"ログ管理と外部 syslog サーバの設定"を参照してください。

監査メッセージカテゴリ

StorageGRID のシステムイベントの監査メッセージ

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。

Code	メッセージのタイトルと説明	詳細については、
ECMC	欠落した消去符号化データ断片：欠落した消去符号化データ断片が検出されたことを示します。	"ECMC: 欠落した消去符号化データ断片"
ECOC	破損した消去符号化データ断片：破損した消去符号化データ断片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断片"
ETAF	セキュリティ認証に失敗しました：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登録：サービスが StorageGRID システムに自身の情報を更新または登録しました。	"GNRG: GNDS登録"
GNUR	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完了しました。	"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	Location Lost：この監査メッセージは、位置情報が失われたときに生成されます。	"LLST：位置情報不明"

Code	メッセージのタイトルと説明	詳細については、
OLST	オブジェクトが見つかりません：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：システムが失われたオブジェクトを検出しました"
SADD	セキュリティ監査無効化：監査メッセージのログ記録が無効になりました。	"SADD: セキュリティ監査無効化"
SADE	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：セキュリティ監査有効化"
SVRF	オブジェクトストアの検証に失敗しました：コンテンツブロックの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	Object Store Verify Unknown：オブジェクトストア内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検証不明"
SYSD	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"
SYST	ノード停止：サービスによってグレースフルストップが開始されました。	"SYST: ノード停止中"
SYSU	ノード起動：サービスが開始されました。前回のシャットダウンの内容はメッセージに示されています。	"SYSU: ノード起動"

StorageGRID のオブジェクトストレージイベントの監査メッセージ

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ストレージ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、および検証が含まれます。

監査コードは、機能が廃止されると、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見つかった場合は、以前の SG リリースに対応するこのトピックの旧バージョンを確認してください。例えば、 "StorageGRID 11.8 オブジェクトストレージ監査メッセージ"。

Code	説明	詳細については、
BROR	バケット読み取り専用リクエスト：バケットが読み取り専用モードに入ったか、読み取り専用モードから解除されました。	"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は、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"

Code	説明	詳細については、
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 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ために、クロスグリッドレプリケーション操作を試みました。	"CGRR：クロスグリッドレプリケーション要求"
EBDL	バケットの空削除：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（バケットを空にする操作を実行中）。	"EBDL：空のバケットの削除"
EBKR	バケット空化リクエスト：ユーザーがバケット空化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）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および検証され、リクエスト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、直接リクエストすることはできなくなりました。	"SREM: オブジェクトストア削除"

StorageGRID におけるクライアントの読み取り操作の監査メッセージ

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した際に、クライアント読み取り監査メッセージがログに記録されます。

Code	説明	使用者	詳細については、
S3SLを使用したチャンク アップロード署名要求がサポートされるようになりました。	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、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 Select リクエスト"

Code	説明	使用者	詳細については、
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トランザクションが成功したこと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 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ために、トランザクションが成功したことをログに記録します。	S3クライアント	"SHEA：S3 HEAD"

StorageGRID におけるクライアント書き込み操作の監査メッセージ

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ログに記録されます。

Code	説明	使用者	詳細については、
OVWR	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ログに記録します。	S3クライアント	"OVWR：オブジェクト上書き"
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が成功したこと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 DELETE"
SPOS	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トランザクションが成功したことをログに記録します。	S3クライアント	"SPOS：S3 POST"
SPUT	S3 PUT：新しいオブジェクトまたはバケットを作成するトランザクションが成功したこと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	"SPUT：S3 PUT"

Code	説明	使用者	詳細については、
SUPD	S3メタデータ更新：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トランザクションが成功したこと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"

StorageGRID管理監査メッセージ

管理カテゴリは、Management APIへのユーザーリクエストをログに記録します。

Code	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：管理監査メッセージ"

StorageGRID 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。

Code	メッセージのタイトルと説明	詳細については、
IDEL	ILM Initiated Delete：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ストレージ容量を解放するために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	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場合に生成されます。	"ORLM: オブジェクトルールを満たしました"

監査メッセージ参照

StorageGRIDのバケット読み取り専用リクエストのBROR監査メッセージ

LDRサービスは、バケットが読み取り専用モードに入ったり、読み取り専用モードから解除されたりしたときに、この監査メッセージを生成します。例えば、バケット内の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。

Code	フィールド	説明
BKHD	バケットUUID	バケットIDです。

Code	フィールド	説明
BROV	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解除されるかを示します（1 = 読み取り専用、0 = 読み取り専用ではない）。
BROS	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る、または読み取り専用状態から解除される理由。例えば、emptyBucket。
S3AIを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	S3バケット	S3バケット名。

StorageGRIDにおけるオブジェクト受信開始の**CBRB**監査メッセージ

通常のシステム運用中、データのアクセス、複製、保持が行われるにつれて、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。コンテンツブロックの転送が一方のノードから他方のノードへ開始されると、このメッセージは転送先のエンティティによって発行されます。

Code	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型かプル開始型かを示します。 PUSH：転送操作は送信元エンティティによって要求されました。 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転送の送信元（ソース）のノードID。

Code	フィールド	説明
CTDS	宛先エンティティ	CBID転送の宛先（受信者）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カウントを示します。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	予想される末端シーケンス数	最後に要求されたシーケンスカウントを示します。転送が成功した場合、このシーケンスカウントが受信された時点で転送は完了とみなされます。
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、「Start Sequence Count」から「Expected End Sequence Count」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、それぞれのノード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の追跡に使用でき、ストレージ監査メッセージと組み合わせることで、レプリカ数の検証にも使用できます。

StorageGRIDにおけるオブジェクト受信終了の**CBRE**監査メッセージ

コンテンツブロックが1つのノードから別のノードへ転送されると、転送先のエンティティからこのメッセージが発行されます。

Code	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型かプル開始型かを示します。 PUSH：転送操作は送信元エンティティによって要求されました。 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転送の送信元（ソース）のノードID。
CTDS	宛先エンティティ	CBID転送の宛先（受信者）のノードID。

Code	フィールド	説明
CTSS	開始シーケンス数	転送が開始されたシーケンス番号を示します。
CTAS	実際の終了シーケンス数	最後に正常に転送されたシーケンス数を示します。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	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: 転送中に接続が切断されました 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「Start Sequence Count」から「Actual End Sequence Count」にデータが転送されます。送信ノードと受信ノードは、それぞれのノードIDによって識別されます。この情報は、システムデータの流れを追跡したり、エラーを特定、集計、分析したりするために使用できます。ストレージ監査メッセージと組み合わせることで、レプリカ数の検証にも使用できます。

StorageGRIDでのオブジェクト送信開始の**CBSB**監査メッセージ

通常のシステム運用中、データのアクセス、複製、保持が行われるにつれて、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。コンテンツブロックが1つのノードから別のノードへの転送が開始されると、このメッセージは送信元エンティティによって発行されます。

Code	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型かプル開始型かを示します。 PUSH：転送操作は送信元エンティティによって要求されました。 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。

Code	フィールド	説明
CTSR	ソースエンティティ	CBID転送の送信元（ソース）のノードID。
CTDS	宛先エンティティ	CBID転送の宛先（受信者）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カウントを示します。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	予想される末端シーケンス数	最後に要求されたシーケンスカウントを示します。転送が成功した場合、このシーケンスカウントが受信された時点で転送は完了とみなされます。
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、「Start Sequence Count」から「Expected End Sequence Count」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、それぞれのノード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の追跡に使用でき、ストレージ監査メッセージと組み合わせることで、レプリカ数の検証にも使用できます。

StorageGRIDにおけるオブジェクト送信終了の**CBSE**監査メッセージ

コンテンツブロックが1つのノードから別のノードへの転送が完了すると、送信元エンティティからこのメッセージが発行されます。

Code	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型かプル開始型かを示します。 PUSH：転送操作は送信元エンティティによって要求されました。 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転送の送信元（ソース）のノードID。

Code	フィールド	説明
CTDS	宛先エンティティ	CBID転送の宛先（受信者）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番号を示します。
CTAS	実際の終了シーケンス数	最後に正常に転送されたシーケンス数を示します。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	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: 転送中に接続が切断されました 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「Start Sequence Count」から「Actual End Sequence Count」にデータが転送されます。送信ノードと受信ノードは、それぞれのノードIDによって識別されます。この情報は、システムデータの流れを追跡したり、エラーを特定、集計、分析したりするために使用できます。ストレージ監査メッセージと組み合わせることで、レプリカ数の検証にも使用できます。

StorageGRIDのクロスグリッドレプリケーション要求の**CGRR**監査メッセージ

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みたときに生成されます。

Code	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。

Code	フィールド	説明
S3AIを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3テナントアカウントID	オブジェクトが複製される元の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	グリッド間レプリケーションに使用されるグリッドフェデレーション接続のID。
OPER	CGRの運用	試みられたクロスグリッド複製操作の種類： • 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 = 複製削除マーカー
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3バケット	S3バケット名。
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3キー	バケット名を含まない S3 キー名。
VSID	バージョン ID	複製対象となったオブジェクトの特定バージョンのバージョンID。
RSLT	結果コード	成功（SUCS）または一般的なエラー（GERR）を返します。

StorageGRIDにおける空のバケットオブジェクトの削除に関する**EBDL**監査メッセージ

ILMスキャナは、すべてのオブジェクトを削除中のバケット（空のバケット操作を実行中のバケット）内のオブジェクトを削除しました。

Code	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）。

Code	フィールド	説明
PATH	S3バケット/キー	S3バケット名とS3キー名。
SEGC	コンテナUUID	分割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利用できます。
UUID	汎用一意識別子	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。メッセージに関係がない場合は、SUCS の代わりに NONE が使用され、メッセージが誤ってフィルタリングされることを防ぎます。

StorageGRIDにおける空のバケットリクエストに対する**EBKR**監査メッセージ

このメッセージは、ユーザーが空のバケットを有効または無効にする（つまり、バケット内の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）よう要求したことを示しています。

Code	フィールド	説明
BUID	バケットUUID	バケットIDです。
EBJS	空のバケットのJSON設定	現在の空のバケット構成を表す JSON が含まれています。
S3AIを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。

StorageGRIDにおける消失訂正符号化データの欠落に関する**ECMC**監査メッセージ

この監査メッセージは、システムが欠落している消去符号化データフラグメントを検出したことを示しています。

Code	フィールド	説明
VCMC	VCS ID	欠落しているチャンクを含むVCSの名前。
MCID	チャンクID	欠落している消去符号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項目ですが、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。

StorageGRIDの破損した消去符号化データに関する**ECOC**監査メッセージ

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断片を検出したことを示しています。

Code	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	破損したイレイジャーコーディング断片を含むRangeDBボリューム。
CCID	チャンクID	破損した消去符号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項目ですが、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。

StorageGRIDにおけるセキュリティ認証失敗に関する**ETAF**監査メッセージ

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場合に表示されます。

Code	フィールド	説明
CNID	接続識別子	認証に失敗したTCP/IP接続の一意のシステム識別子。
RUID	ユーザーID	リモートユーザーの識別情報を表す、サービス依存の識別子。

Code	フィールド	説明
RSLT	理由コード	失敗の理由： SCNI: セキュア接続の確立に失敗しました。 CERM: 証明書が見つかりませんでした。 CERT：証明書が無効です。 CERE：証明書の有効期限が切れています。 CERR: 証明書が失効しました。 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：ユーザー認証情報が不足しています。 UCRI：ユーザー認証情報が無効です。 UCRU: ユーザー認証情報が許可されませんでした。 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、TLSプロファイルとサービスに組み込まれた追加のロジックを使用して、リモートエンティティの認証情報が検証されます。無効な証明書、予期しない証明書、または許可されていない証明書や資格情報が原因で認証が失敗した場合、監査メッセージがログに記録されます。これにより、不正アクセス試行やその他のセキュリティ関連の接続問題に関する照会が可能になります。

このメッセージは、リモートエンティティの設定が誤っているか、システムに無効または許可されていない認証情報を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。この監査メッセージは、システムへの不正アクセスを試みる行為を検出するために監視する必要があります。

StorageGRIDにおける**GNDS**登録の**GNRG**監査メッセージ

CMN サービスは、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たときに、この監査メッセージを生成します。

Code	フィールド	説明
RSLT	結果	更新リクエストの結果： • SUCS：成功 • SUNV：サービス利用不可 • GERR: その他の失敗

Code	フィールド	説明
GNID	ノードID	更新要求を開始したサービスのノードID。
GNTP	Device Type	グリッドノードのデバイスタイプ（例：LDR サービスの場合は BLDR ）。
GNDV	デバイスモデルバージョン	DMDLバンドル内で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において）。
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エントリを更新するたびに生成されます。

StorageGRIDにおける**GNDS**登録解除に関する**GNUR**監査メッセージ

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。

Code	フィールド	説明
RSLT	結果	更新リクエストの結果： • SUCS：成功 • SUNV：サービス利用不可 • 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。

StorageGRIDで終了したグリッドタスクの**GTED**監査メッセージ

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ています。結果がSUCS、ABRT、またはROLFの場合は、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。

Code	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、グリッドタスク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。 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が複数回送信される可能性があり、この場合、タスクIDフィールドだけでは、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。
RSLT	結果	グリッドタスクの最終ステータス結果： • 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: グリッドタスクが終了し、ロールバック処理を完了できませんでした。 • CANC: グリッドタスクが開始される前に、ユーザーによってキャンセルされました。 • EXPR: グリッドタスクが開始される前に期限切れになりました。 • IVLD: グリッドタスクが無効でした。 • AUTH：グリッドタスクは認証されていませんでした。 • DUPL: グリッドタスクは重複として却下されました。

StorageGRIDで開始されたグリッドタスクの**GTST**監査メッセージ

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、自動アクティブ化のために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続きます。保留テーブルに送信されたグリッドタスクの場合、このメッセージはユーザーがグリッドタスクを開始したときに生成されます。

Code	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、タスク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。 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が複数回送信される可能性があり、この場合、タスクIDフィールドだけでは、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。

Code	フィールド	説明
RSLT	結果	結果。このフィールドには値が1つだけあります。 • SUCS: グリッドタスクが正常に開始されました。

StorageGRIDで送信されたグリッドタスクの**GTSU**監査メッセージ

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ています。

Code	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。 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が複数回送信される可能性があり、この場合、タスクIDフィールドだけでは、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。
TTYP	タスクタイプ	グリッドタスクの種類。
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	グリッドタスクを人間が理解しやすい形で記述したもの。
VATS	有効開始タイムスタンプ	グリッドタスクが有効となる最も早い時刻（1970年1月1日からのUINT64マイクロ秒 - UNIX時間）。
VBTS	有効期限前のタイムスタンプ	グリッドタスクが有効となる最終時刻（1970年1月1日からのUINT64マイクロ秒、UNIX時間）。
TSRC	ソース	タスクの発生源： • TXTB: グリッドタスクは、署名付き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 Grid Task Submission Service を通じて送信されました。
アクティブ	アクティベーションの種類	アクティベーションの種類： • AUTO：グリッドタスクが自動起動のために送信されました。 • PEND：グリッドタスクが保留テーブルに送信されました。これは TXTB ソースにとって唯一の可能性です。

Code	フィールド	説明
RSLT	結果	提出結果： • 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。

StorageGRIDにおける**ILM**開始削除の**IDEL**監査メッセージ

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

IDELメッセージは、以下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、保持期間が経過したため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で、法的保留が無効になっている場合）。
- 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、現在有効な ILM ポリシーにオブジェクトに適用できる配置指示がないため、ILM がオブジェクトの削除処理を開始したときに生成されます。

Code	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が対象です。0（false）または 1（true）。バケットがリーガルホールド下にない限り、準拠オブジェクトの保持期間終了時に自動的に削除され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が対象です。バケットが現在法的保留状態にあるかどうかを示す、0（false）または 1（true）。
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が対象です。オブジェクトの保持期間（分単位）。
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が対象です。オブジェクトの取り込み時間。この値に保持期間（分単位）を加算することで、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。
DMRK	削除マーカーバージョン ID	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した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。
CSIZ	コンテンツサイズ	オブジェクトのサイズ（バイト）。

Code	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割り当てられていない場合（例えば、削除された場合）、LOCS の値は「」になります。 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：複製されたオブジェクトの場合、LDR ノード ID とオブジェクトの場所のボリューム ID。 CLNL: オブジェクトデータがアーカイブされている場合、オブジェクトの場所を示すARCノードID。
PATH	S3バケット/キー	S3バケット名とS3キー名。
RSLT	結果	ILM処理の結果。 SUCS：ILM操作は成功しました。
ルール	ルールラベル	• 準拠した S3 バケット内のオブジェクトが、保持期間の満了により自動的に削除される場合、このフィールドは空白になります。 • オブジェクトに適用され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 ルールの人間が読める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、そのオブジェクトは指定されたサイトで削除されました。そのサイトは、オブジェクトが取り込まれたサイトとは異なります。
UUID	汎用一意識別子	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バージョンのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。

StorageGRIDで上書きされたオブジェクトのクリーンアップに関する**LKCU**監査メッセージ

このメッセージは、StorageGRID がストレージ容量を解放するため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を含む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。削除処理は自動的にバックグラウンドで実行されます。

Code	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	社内利用のみ。
LUID	削除されたオブジェクトUUID	削除されたオブジェクトの識別子。
PATH	S3バケット/キー	S3バケット名とS3キー名。
SEGC	コンテナUUID	分割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利用できます。
UUID	汎用一意識別子	現存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利用可能です。

StorageGRIDでリークされたオブジェクトのクリーンアップに関する**LKDM**監査メッセージ

このメッセージは、リークしたデータ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イレイジャー コーディングされたオブジェクトの一部になり得ます。

Code	フィールド	説明
CLOC	チャンクの位置	削除されたリーク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`

Code	フィールド	説明

LTYP	漏洩タイプ	検出可能な漏洩の種類は以下の5つです：
		
		`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	リークされたデータチャンクが作成された時刻。
UUID	汎用一意識別子	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）。

StorageGRIDで失われたオブジェクトのコピー場所に関する**LLST**監査メッセージ

このメッセージは、オブジェクトのコピー（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。

Code	フィールド	説明
CBIL	CBID	影響を受けた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の場合。使用されたイレイジャー コーディングプロファイルのID。

Code	フィールド	説明
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）：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（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
NOID	ソースノードID	位置情報が失われたノードの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上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）にのみ返されます。 形式は `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	結果	常に NONE。RSLT は必須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	トリガーとなるソース	ユーザー: ユーザーがトリガーしました SYST: システムトリガー
UUID	ユニバーサル一意ID	影響を受けるオブジェクトの識別子（StorageGRID システム内）。

StorageGRIDの管理**API**リクエストの**MGAU**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ログに記録します。有効なAPI URIへのGETまたはHEADリクエスト以外のすべてのHTTPリクエストは、ユーザー名、IP、およびAPIへの要求タイプを含むレスポンスをログに記録します。無効なAPI URI（例：/api/v3-authorize）や、有効なAPI URIに対する無効なリクエストはログに記録されません。

Code	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。
MDNA	ドメイン名	ホストドメイン名。
MPAT	Request PATH	リクエストパス。

Code	フィールド	説明
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。
MRBD	要求の本文	リクエスト本文の内容。デフォルトではレスポンスボディがログに記録されますが、レスポンスボディが空の場合にはリクエストボディがログに記録されることもあります。以下の情報はレスポンスボディに含まれていないため、以下のPOSTメソッドについてはリクエストボディから取得します。 • *POST authorize*における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** の廃止済みサーバー ID 注: 機密情報は削除されるか（例：S3アクセスキー）、またはアスタリスクでマスクされます（例：パスワード）。
MRMD	リクエストメソッド	HTTPリクエストメソッド： • POST • PUT • DELETE • PATCH
MRSC	応答コード	レスポンスコード。
MRSP	応答の本文	レスポンスの内容（レスポンスボディ）は、デフォルトでログに記録されます。 注: 機密情報は削除されるか（例：S3アクセスキー）、またはアスタリスクでマスクされます（例：パスワード）。
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から報告されたエラーを返します。

StorageGRIDでシステムが検出した紛失オブジェクトに関する**OLST**監査メッセージ

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どこにも見つけられない場合に生成されます。

Code	フィールド	説明
CBID	コンテンツブロック識別子	紛失オブジェクトのCBID。
NOID	ノードID	入手可能な場合は、紛失したオブジェクトの最後に確認された直接位置またはニアライン位置。ボリューム情報が利用できない場合は、Volume ID なしで Node ID のみを保持することも可能です。
PATH	S3バケット/キー	利用可能な場合は、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	ユニバーサル一意ID	StorageGRID システム内の紛失オブジェクトの識別子。
VOLI	ボリューム ID	利用可能な場合は、紛失したオブジェクトの最後に確認された場所に対応するストレージノードのボリュームID。

StorageGRIDでILMルールが満たされた場合のORLM監査メッセージ

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

ポリシー内の別のルールでオブジェクトサイズの詳細フィルターが使用されている場合、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たときに、ORLMメッセージは生成されません。

Code	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）。

Code	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割り当てられていない場合（例えば、削除された場合）、LOCS の値は「」になります。 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：複製されたオブジェクトの場合、LDR ノード ID とオブジェクトの場所のボリューム ID。 CLNL: オブジェクトデータがアーカイブされている場合、オブジェクトの場所を示すARCノードID。
PATH	S3バケット/キー	S3バケット名とS3キー名。
RSLT	結果	ILM処理の結果。 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ルールに付けられた、人間が読みやすいラベル。
SEGC	コンテナUUID	分割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利用できます。
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でのみ利用可能です。
STAT	ステータス	ILMの運用状況。 完了：オブジェクトに対するILM操作が完了しました。 DFER：このオブジェクトは、将来のILM再評価のためにマークされました。 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は StorageGRID システムで見つかりません。この状態は、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	汎用一意識別子	StorageGRID システム内のオブジェクトの識別子。

Code	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内に作成された新しいオブジェクトのバージョンID。バージョン管理され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される可能性があります。例えば、以下のいずれかの事象が発生した場合に発行されます。

- そのオブジェクトのILMルールは永久に満たされます。
- このエポックにおいては、オブジェクトのILMルールが満たされています。
- ILMルールにより、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した。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"

StorageGRIDにおけるオブジェクトの上書きに関する**OVWR**監査メッセージ

このメッセージは、外部（クライアントからの要求）操作によってある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場合に生成されます。

Code	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）	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（前述）	StorageGRID システム内の前のオブジェクトの識別子。
PATH	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

Code	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。これは、上書きされたオブジェクトが取り込まれたサイトとは異なります。

StorageGRIDにおける**S3 Select**リクエストの**S3SL**監査メッセージ

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に完了したこと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。リクエストは成功しなかった可能性があります。

Code	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 は異なる値になる可能性が高いです。オブジェクトが圧縮されている場合、BYSC には圧縮後のバイト数が格納され、BYPR には解凍後のバイト数が格納されます。
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アクションされた「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。
REPR	処理済みレコード	S3 Selectジョブがストレージノードから受信したレコード数または行数。
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数または行数。
JOFI	作業完了	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、ジョブは完了せず、エラーフィールドにデータが含まれてい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場合もあれば、まったく結果を受け取れなかった場合もあります。
REID	Request ID	S3 Selectリクエストの識別子。
EXTM	実行時間	S3 Selectジョブの完了にかかった時間（秒）。

Code	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。
ERTY	エラーの種類	S3 Selectジョブが生成したエラーの種類。
ERST	エラースタックトレース	S3 Selectジョブが生成したエラースタックトレース。
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3バケット	S3バケット名。
S3AKを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	S3キー	バケット名を含まない S3 キー名。

StorageGRIDにおけるセキュリティ監査の無効化に関する**SADD**監査メッセージ

このメッセージは、発信元のサービス（ノードID）が監査メッセージのログ記録を無効にしたことを示しています。StorageGRID は監査メッセージの収集および配信を停止しました。

Code	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た方法。

Code	フィールド	説明
AEUN	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ー名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須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になっていたが、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、大量データ取り込み時にのみ使用されます。大量処理が完了すると、監査機能が復元され（SADE）、監査機能を無効にする機能は永久的にブロックされます。

StorageGRIDにおけるセキュリティ監査有効化のための**SADE**監査メッセージ

このメッセージは、発信元のサービス（ノードID）が監査メッセージのログ記録を復元したことを示しています。StorageGRID は監査メッセージの収集と配信を再開しました。

Code	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。
AEUN	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ー名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須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）されていたが、現在は復元された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、大量データ取り込み時にのみ使用されます。一括処理が完了すると、監査機能が復元され、監査機能を無効にする機能は永久的にブロックされます。

StorageGRIDのオブジェクトストアコミットの**SCMT**監査メッセージ

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）、利用可能になったり、保存されたものとして認識されたりしません。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ています。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表示されます。

Code	フィールド	説明
CBID	コンテンツブロック識別子	永続ストレージに保存されるコンテンツブロックの一意の識別子。

Code	フィールド	説明
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状態： SUCS: オブジェクトが正常に保存されました。

このメッセージは、指定されたコンテンツブロックが完全に保存および検証され、リクエストが可能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。

StorageGRIDにおける**S3 DELETE**トランザクションの**SDEL**監査メッセージ

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要求されます。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ーから送信されます。

Code	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が不明な場合は、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	リクエストにConsistency-Control HTTPリクエストヘッダーが存在する場合、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	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	削除マーカーバージョン ID	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した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対象となる、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。

Code	フィールド	説明
HTRH	HTTPリクエストヘッダー	設定時に選択された、ログに記録された HTTP リクエストヘッダー名と値のリスト。 `X-Forwarded-For`はリクエストに存在し、かつ `X-Forwarded-For`の値がリクエスト送信者のIP アドレス（SAIP監査フィールド）と異なる場合、自動的に含まれます。 `x-amz-bypass-governance-retention`はリクエストに含まれている場合、自動的に含まれます。
MTME	最終更新日時	オブジェクトが最後に変更された日時を示す、マイクロ秒単位のUnixタイムスタンプ。
RSLT	結果コード	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
S3AIを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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をハッシュ化したもの。空の値は、匿名アクセスを示します。
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	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。

Code	フィールド	説明
S3SRを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 サブリソース	操作対象のバケットまたはオブジェクトのサブリソース（該当する場合）。
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名。匿名リクエストの場合は空欄です。
SAIP	IPアドレス（リクエスト送信元）	リクエスト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）	対象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します。
SGRP	サイト（グループ）	オブジェクトが存在する場合、そのオブジェクトは指定されたサイトで削除されました。そのサイトは、オブジェクトが取り込まれたサイトとは異なります。
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、リクエストを行った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です。例：`urn:sgws:identity::03393893651506583485:root` 匿名リクエストの場合は空欄です。
時間	Time	リクエストの処理にかかった合計時間（マイクロ秒）。
TLIP	信頼できるロードバランサーのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサーによってルーティングされた場合、ロードバランサーのIPアドレス。
UUDM	削除マーカーのUniversally Unique Identifier	削除マーカーの識別子。監査ログメッセージには、UUDM または UUID のいずれかが指定されます。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ーを示し、UUID はオブジェクトを示します。
UUID	汎用一意識別子	StorageGRID システム内のオブジェクトの識別子。

Code	フィールド	説明
VSID	バージョン ID	削除されたオブジェクトの特定バージョンのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。

StorageGRIDにおける**S3 GET**トランザクションの**SGET**監査メッセージ

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リクエストが行われます。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ーから送信されます。

Code	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が不明な場合は、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	リクエストにConsistency-Control HTTPリクエストヘッダーが存在する場合、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	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	設定時に選択された、ログに記録された HTTP リクエストヘッダー名と値のリスト。 `X-Forwarded-For`はリクエストに存在し、かつ `X-Forwarded-For`の値がリクエスト送信者のIP アドレス（SAIP監査フィールド）と異なる場合、自動的に含まれます。
LITY	ListObjectsV2を使用したチャンク アップロード署名要求がサポートされるようになりました。	_v2形式_の応答が要求されました。詳細については、 "AWS ListObjectsV2"を参照してください。GETバケット操作のみに適用されます。
NCHD	子供の数	キーと共通プレフィックスが含まれます。GET バケット操作のみに適用されます。

Code	フィールド	説明
RANG	範囲読み取り	範囲読み取り操作専用です。このリクエストによって読み取られたバイト範囲を示します。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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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をハッシュ化したもの。空の値は、匿名アクセスを示します。
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 サブリソース	操作対象のバケットまたはオブジェクトのサブリソース（該当する場合）。
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名。匿名リクエストの場合は空欄です。

Code	フィールド	説明
SAIP	IPアドレス（リクエスト送信元）	リクエスト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）	対象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、リクエストを行った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です。例：`urn:sgws:identity::03393893651506583485:root` 匿名リクエストの場合は空欄です。
時間	Time	リクエストの処理にかかった合計時間（マイクロ秒）。
TLIP	信頼できるロードバランサーのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサーによってルーティングされた場合、ロードバランサーのIPアドレス。
TRNC	切り捨てられたか、切り捨てられていないか	すべての結果が返された場合は、false に設定します。返せる結果がさらにある場合は、true に設定します。GET バケット操作のみに適用されます。
UUID	汎用一意識別子	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バージョンのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。

StorageGRIDにおける**S3 HEAD**操作の**SHEA**監査メッセージ

S3クライアントがHEAD操作を発行すると、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リクエストが送信されます。このメッセージは、操作が成功した場合にサーバーから発行されます。

Code	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が不明な場合は、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。

Code	フィールド	説明
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	チェック対象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	設定時に選択された、ログに記録された HTTP リクエストヘッダー名と値のリスト。 `X-Forwarded-For`はリクエストに存在し、かつ `X-Forwarded-For`の値がリクエスト送信者のIP アドレス（SAIP監査フィールド）と異なる場合、自動的に含まれます。
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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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をハッシュ化したもの。空の値は、匿名アクセスを示します。
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	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。

Code	フィールド	説明
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名。匿名リクエストの場合は空欄です。
SAIP	IPアドレス（リクエスト送信元）	リクエスト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）	対象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、リクエストを行った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です。例：`urn:sgws:identity::03393893651506583485:root` 匿名リクエストの場合は空欄です。
時間	Time	リクエストの処理にかかった合計時間（マイクロ秒）。
TLIP	信頼できるロードバランサーのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサーによってルーティングされた場合、ロードバランサーのIPアドレス。
UUID	汎用一意識別子	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バージョンのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。

StorageGRIDにおける**S3 POST**トランザクションの**SPOS**監査メッセージ

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した場合にサーバーからこのメッセージが発行されます。

Code	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が不明な場合は、このフィールドは0に設定されます。

Code	フィールド	説明
CNCH	一貫性制御ヘッダー	リクエストにConsistency-Control HTTPリクエストヘッダーが存在する場合、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	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	設定時に選択された、ログに記録された HTTP リクエストヘッダー名と値のリスト。 `X-Forwarded-For`はリクエストに存在し、かつ `X-Forwarded-For`の値がリクエスト送信者のIP アドレス（SAIP監査フィールド）と異なる場合、自動的に含まれます。 （SPOSでは想定外）。
RSLT	結果コード	RestoreObject リクエストの結果。結果は常に次のとおりです： SUCS：成功
S3AIを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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をハッシュ化したもの。空の値は、匿名アクセスを示します。
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。

Code	フィールド	説明
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 サブリソース	操作対象のバケットまたはオブジェクトのサブリソース（該当する場合）。 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名。匿名リクエストの場合は空欄です。
SAIP	IPアドレス（リクエスト送信元）	リクエスト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）	対象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します。
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、リクエストを行った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です。例：`urn:sgws:identity::03393893651506583485:root` 匿名リクエストの場合は空欄です。
時間	Time	リクエストの処理にかかった合計時間（マイクロ秒）。
TLIP	信頼できるロードバランサーのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサーによってルーティングされた場合、ロードバランサーのIPアドレス。
UUID	汎用一意識別子	StorageGRID システム内のオブジェクトの識別子。

Code	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バージョンのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。

StorageGRIDにおける**S3 PUT**トランザクションの**SPUT**監査メッセージ

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リクエストが行われます。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ーから送信されます。

Code	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が不明な場合は、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	バケット作成時に使用されたコンプライアンス設定（リクエストに含まれている場合、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	リクエストにConsistency-Control HTTPリクエストヘッダーが存在する場合、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	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リクエスト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リクエストにおける、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。

Code	フィールド	説明
HTRH	HTTPリクエストヘッダー	設定時に選択された、ログに記録された HTTP リクエストヘッダー名と値のリスト。 `X-Forwarded-For`はリクエストに存在し、かつ `X-Forwarded-For`の値がリクエスト送信者のIP アドレス（SAIP監査フィールド）と異なる場合、自動的に含まれます。 `x-amz-bypass-governance-retention`はリクエストに含まれている場合、自動的に含まれます。
LKEN	オブジェクトロックが有効	リクエストヘッダーの値 x-amz-bucket-object-lock-enabled（リクエストに含まれている場合）。
LKLH	オブジェクトロック法務保留	リクエストヘッダーの値 `x-amz-object-lock-legal-hold`が PutObject 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 x-amz-object-lock-mode（PutObjectリクエストに存在する場合）。
LKRU	オブジェクトロック保持期限日	リクエストヘッダー `x-amz-object-lock-retain-until-date`の値。PutObjectリクエストに存在する場合に適用されます。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日時を示す、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
S3AIを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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をハッシュ化したもの。空の値は、匿名アクセスを示します。

Code	フィールド	説明
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 サブリソース	操作対象のバケットまたはオブジェクトのサブリソース（該当する場合）。
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名。匿名リクエストの場合は空欄です。
SAIP	IPアドレス（リクエスト送信元）	リクエスト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）	対象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します。
SRCF	サブリソース構成	新しいサブリソース構成（最初の1024文字に切り詰められています）。
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、リクエストを行った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です。例：`urn:sgws:identity::03393893651506583485:root` 匿名リクエストの場合は空欄です。
時間	Time	リクエストの処理にかかった合計時間（マイクロ秒）。

Code	フィールド	説明
TLIP	信頼できるロードバランサーのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサーによってルーティングされた場合、ロードバランサーのIPアドレス。
ULID	アップロードID	SPUT メッセージにのみ含まれます（CompleteMultipartUpload 操作の場合）。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	汎用一意識別子	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内に作成された新しいオブジェクトのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。
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「enabled」または「suspended」の2種類です。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。

StorageGRIDにおけるオブジェクトストア削除の**SREM**監査メッセージ

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 を通じてアクセスできなくなった場合に表示されます。

Code	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の識別子。
RSLT	結果コード	コンテンツ削除操作の結果を示します。唯一定義されている値は次のとおりです。 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、直接リクエストできなくなったことを意味します。このメッセージは、システム内における削除済みコンテンツの流れを追跡するために使用できます。

StorageGRIDの**S3**メタデータ更新の**SUPD**監査メッセージ

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際に、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、サーバーからこのメッセージが送信されます。

Code	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が不明な場合は、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際に、リクエストにConsistency-Control HTTPリクエストヘッダーが存在する場合、そのヘッダーの値。
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。
HTRH	HTTPリクエストヘッダー	設定時に選択された、ログに記録された HTTP リクエストヘッダー名と値のリスト。 `X-Forwarded-For`はリクエストに存在し、かつ `X-Forwarded-For`の値がリクエスト送信者のIPアドレス（SAIP監査フィールド）と異なる場合、自動的に含まれます。
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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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を使用したチャンク アップロード署名要求がサポートされるようになりました。	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をハッシュ化したもの。空の値は、匿名アクセスを示します。
S3BKを使用したチャンク アップロード署名要求がサポートされるようになりました。	S3 バケット	S3バケット名。

Code	フィールド	説明
S3KYを使用したチャンク アップロード署名要求がサポートされるようになりました。	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名。匿名リクエストの場合は空欄です。
SAIP	IPアドレス（リクエスト送信元）	リクエスト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）	対象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、リクエストを行った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です。例：`urn:sgws:identity::03393893651506583485:root` 匿名リクエストの場合は空欄です。
時間	Time	リクエストの処理にかかった合計時間（マイクロ秒）。
TLIP	信頼できるロードバランサーのIPアドレス	リクエストが信頼できるレイヤー7ロードバランサーによってルーティングされた場合、ロードバランサーのIPアドレス。
UUID	汎用一意識別子	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バージョンのバージョンID。バージョン管理され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操作には、このフィールドは含まれません。

StorageGRIDにおけるオブジェクトストア検証失敗の**SVRF**監査メッセージ

このメッセージは、コンテンツブロックの検証プロセスが失敗した場合に発行されます。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たびに、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、いくつかの検証および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。

Code	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。
RSLT	結果コード	検証失敗の種類： CRCF: 巡回冗長検査（CRC）が失敗しました。 HMAC：ハッシュベースメッセージ認証コード（HMAC）のチェックに失敗しました。 EHSH: 予期しない暗号化コンテンツハッシュ。 PHSH: 予期しないオリジナルコンテンツのハッシュです。 SEQC：ディスク上のデータ順序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。 FNAM: ファイル名が不正です。

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、ハードウェアの故障が差し迫っていることを示している可能性があります。

メッセージが表示された原因となった操作を特定するには、AMID（モジュールID）フィールドの値を確認してください。例えば、SVFY の値は、メッセージがストレージ検証モジュール（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 の値は、メッセージがコンテンツ取得によってトリガーされたことを示します。

StorageGRID の不明なオブジェクトストアコンテンツに関する **SVRU** 監査メッセージ

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、オブジェクトストア内で複製されたオブジェクトデータの未知のコピーまたは予期しないコピーが検出され、隔離ディレクトリに移動された場合に表示されます。

Code	フィールド	説明
FPTH	File Path	予期しないオブジェクトのコピー先のファイルパス。

Code	フィールド	説明
RSLT	結果	このフィールドの値は「NONE」です。RSLTは必須メッセージ項目ですが、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。

SVRU: Object Store Verify Unknown の監査メッセージは、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内で予期しないオブジェクトデータのコピーが検出されたことを意味します。これらのコピーがどのように作成されたかを特定するため、この状況は直ちに調査してください。ハードウェア障害が差し迫っている兆候である可能性があります。

StorageGRIDにおける正常なノード停止の**SYSD**監査メッセージ

サービスが正常に停止された場合、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。通常、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。これは、シャットダウン前に監査メッセージキューがクリアされないためです。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開始時に送信されるSYST メッセージを探してください。

Code	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。

このメッセージは、ホストサーバーが停止しているかどうかは示しておらず、レポートサービスが停止しているかどうかのみを示しています。SYSDのRSLTは「ダーティ」シャットダウンを示すことはできません。このメッセージは「クリーン」シャットダウンによってのみ生成されるためです。

StorageGRIDでノードが停止する際の**SYST**監査メッセージ

サービスが正常に停止された場合、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ために、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、サービスが再起動された後に送信されるSYSDとは異なります）。

Code	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。

このメッセージは、ホストサーバーが停止しているかどうかは示しておらず、レポートサービスが停止しているかどうかのみを示しています。SYSTメッセージのRSLTコードは、「ダーティ」シャットダウンを示すことはできません。このメッセージは「クリーン」シャットダウンによってのみ生成されるためです。

StorageGRIDでノードの**SYSU**監査メッセージが開始されます

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（指示によるもの）であったか、異常（予期しないもの）であったかを示すメッセージが生成されます。

Code	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、システムが初めて起動されました。

このメッセージは、ホストサーバーが起動したかどうかは示しておらず、レポートサービスが起動したかどうかのみを示しています。このメッセージは以下の目的で使用できます：

- 監査証跡における不連続性を検出します。
- サービスが運用中に障害を起こしているかどうかを判断します（StorageGRIDシステムの分散型の性質上、これらの障害が隠蔽される場合があります）。Server Managerは、障害が発生したサービスを自動的に再起動します。

著作権に関する情報

商標に関する情報