



## 監査ログを確認します StorageGRID

NetApp  
October 03, 2025

# 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
監査ログファイルおよびメッセージの形式 .....	5
監査ログファイルの形式 .....	5
監査メッセージの形式 .....	19
監査メッセージとオブジェクトライフサイクル .....	24
監査メッセージのタイミング .....	24
情報ライフサイクル管理ポリシーの設定 .....	24
アーカイブノード .....	25
オブジェクトの取り込みトランザクション .....	25
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 .....	31
監査メッセージ .....	32
監査メッセージのカテゴリ .....	33
監査メッセージリファレンス .....	39

# 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](#)。

### 関連情報

- [StorageGRID の管理](#)

## 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 システムを介して「audit.log」ファイルにどのように移動するかを理解しておく必要があります。

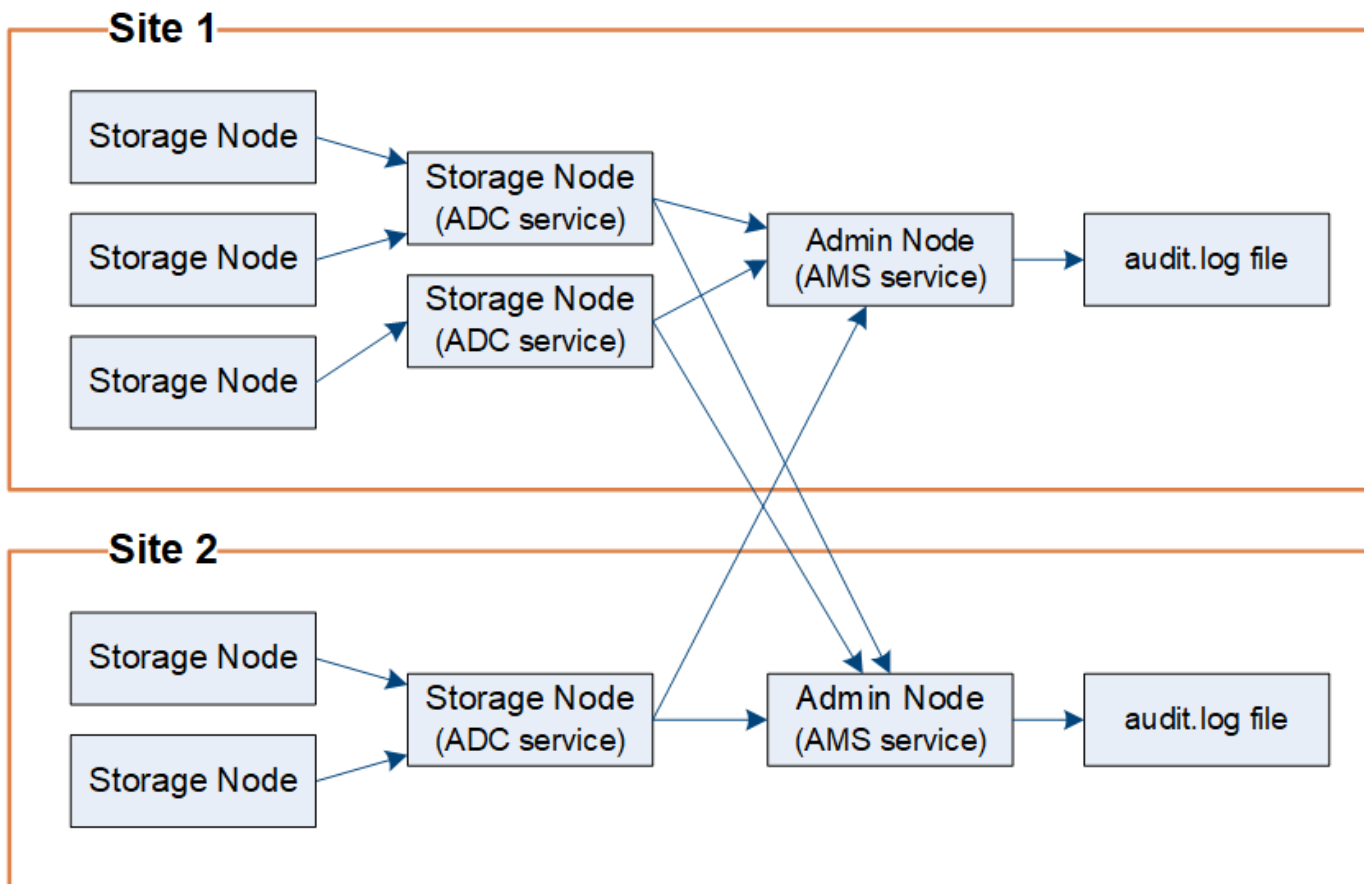
### 監査メッセージのフロー

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。

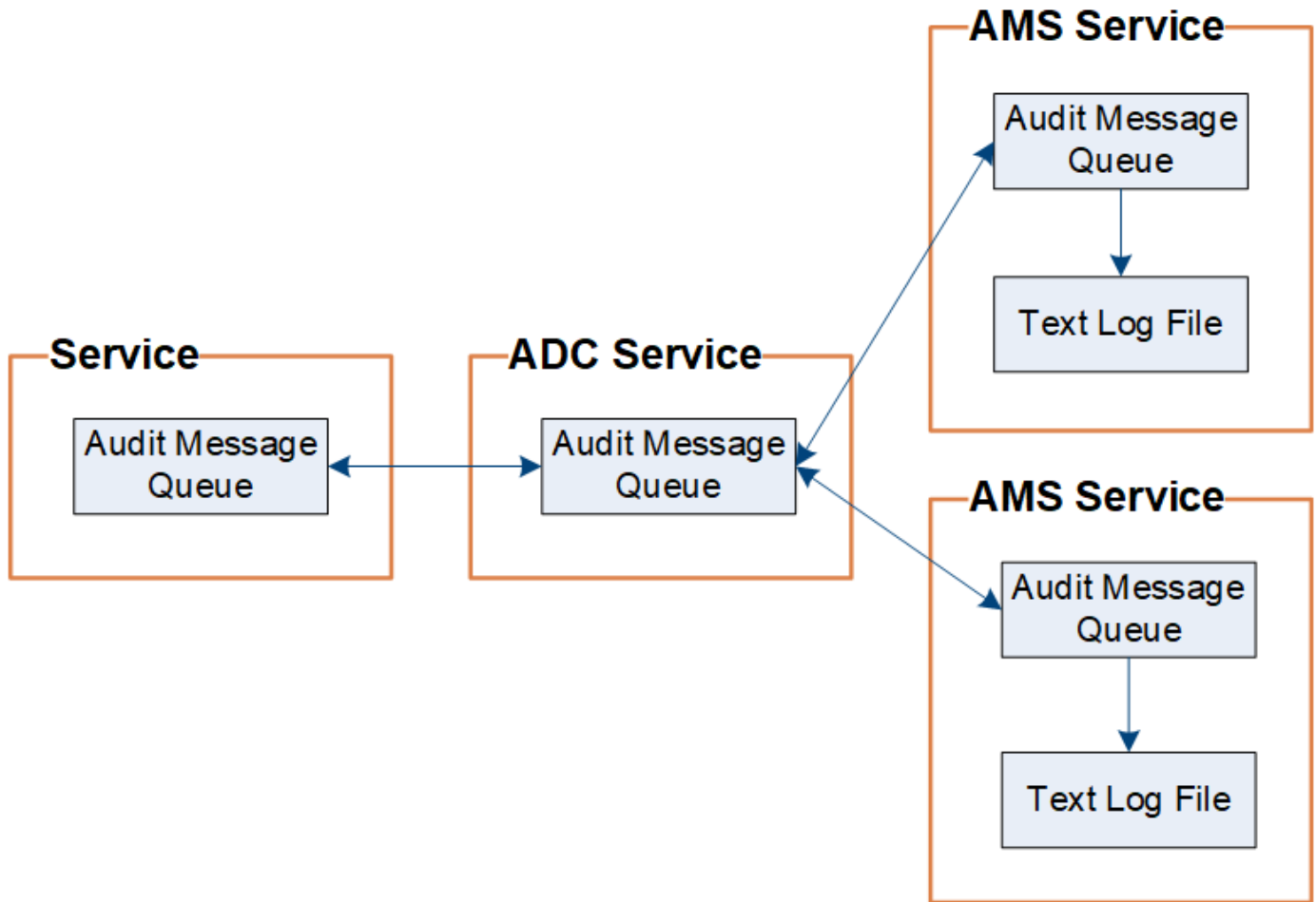
各管理ノードは、監査メッセージをテキスト・ログ・ファイルに保存します。アクティブ・ログ・ファイルの名前は 'audit.log' です。



#### 監査メッセージの保持

StorageGRID 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の `/var/local/audit/export` ディレクトリ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る。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 `/var/local/` ディレクトリ内の使用可能なスペースの消費量が増加します。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。

- 管理ノードで使用される `/var/local/audit/export` 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になるまで管理ノードに新しい監査メッセージを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。
- ADC サービスを持つストレージ・ノードで使用される `/var/local/` 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、そのノードは監査メッセージを使用できないことを示すフラグが設定されます。他のノードに対する 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 サービスを採用するストレージ・ノードが存在しない場合、ストレージ・ノードは監査メッセージをローカルの `/var/local/log/localaudit.log` ファイルに格納します。

- ストレージ・ノードで使用される `/var/local/` ディレクトリが 85% フルになると、ノードは `503 Service Unavailable` を使用して S3 および Swift クライアント要求の拒否を開始します。

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。
- 監査メッセージとは関係のない理由で ADC ストレージ・ノード上の /var/local/ の領域がいっぱいになる  
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[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「audit.log」ファイルと圧縮された監査ログファイルが含まれています。監査ログへのアクセスを簡単にするためには、NFS と CIFS の両方についてクライアントから監査共有へのアクセスを設定します（CIFS は廃止）。管理ノードのコマンドラインから直接監査ログファイルにアクセスすることもできます。

#### 必要なもの

- 特定のアクセス権限が必要です。
- 「passwords.txt」ファイルが必要です。
- 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. 「passwords.txt」ファイルに記載されたパスワードを入力します。
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/audit/export
```

- 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。

## 関連情報

### StorageGRID の管理

## 監査ログファイルのローテーション

監査ログファイルは管理ノードの `/var/local/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・ファイルには `'audit.log'` という名前が付けられています



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「保存された日時を `'yyyy-mm-dd.txt'` の形式で示します。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が使用されます。ファイル名には「番号が付加されます。フォーマットは `'yyyy-mm-dd.txt.n'`」です。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「`yyyy-mm-dd.txt.gz`」の形式で名前が変更されます。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'` ディレクトリ内のスペースを解放します。監査ログは、作成日に基づいて、古い順に削除されます。スクリプトのアクションは `'/var/local/log/manage-audit.log'` ファイルで監視できます。

この例は「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
```

## 監査ログファイルおよびメッセージの形式

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

### 監査ログファイルの形式

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

各監査メッセージには次の情報が含まれます。

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

`YYYY-MM-DDTHHH.MM:SS.UUUUUUUU`。ここで、`UUUUUUU` はマイクロ秒です。

- 監査メッセージ。監査メッセージは角かっこで囲まれ、先頭は「AUDT」です。

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::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

デフォルトの形式のままでは、監査ログファイル内の監査メッセージを読んで解釈するのは簡単ではありません。「audit-explain」ツールを使用すると、監査ログ内の監査メッセージの簡易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、および削除操作の数と、それらの操作に要した時間を要約できます。

#### 関連情報

[audit-explain ツールを使用してください](#)

[audit-sum ツールを使用します](#)

**audit-explain** ツールを使用してください

「audit-explain」ツールを使用すると、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。

必要なもの

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

このタスクについて

プライマリ管理ノードで使用可能な「audit-explain」ツールは、監査ログ内の監査メッセージの簡単な概要を提供します。



「audit-explain」ツールは、主にトラブルシューティング作業中にテクニカルサポートが使用することを目的としています。「audit-explain」クエリを処理すると、StorageGRID の動作に影響を与える可能性がある大量の CPU 消費電力が発生する可能性があります。

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

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

「audit-explain」ツールは、プレーン形式または圧縮された監査ログを処理できます。例：

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

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

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

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

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

最後に 'audit-explain' ツールは 'grep コマンドまたはその他の方法を使用して入力をフィルタリングおよび前処理できるパイプからの入力を受け入れます例：

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

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

監査ログは非常に大きくなり、解析に時間がかかる可能性があるため、ファイル全体ではなく、参照したい部分をフィルタリングして、その部分に対して「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、「zcat」ツールを使用して最初にファイルを解凍します。例：

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

利用可能なオプションを表示するには 'help (-h) オプションを使用します例：

```
$ 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たパスワードを入力します。
2. 次のコマンドを入力しますここで '/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 - /var/local/audit/export/audit.log` を説明します

「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、人間が判読できる形式で出力します。



各行を短く読みやすくするために、デフォルトではタイムスタンプは表示されません。タイムスタンプを表示するには 'timestamp(-t) オプションを使用します

## 関連情報

[SPUT : S3 PUT](#)

**audit-sum** ツールを使用します

「audit-sum」ツールを使用すると、書き込み、読み取り、HEAD、および削除の監査

メッセージをカウントしたり、各処理タイプの最小、最大、平均時間（またはサイズ）を表示したりできます。

必要なもの

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

このタスクについて

プライマリ管理ノードで使用可能な「audit-sum」ツールには、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が表示されます。



「audit-sum」ツールは、主にトラブルシューティング作業時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。「audit-sum」クエリを処理すると、大量の CPU 消費電力が発生し、StorageGRID の動作に影響を与える可能性があります。

次の例は 'audit-sum' ツールからの一般的な出力を示していますこの例は、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 監査メッセージのカウントと時間を提供します。

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	<a href="#">ARCT</a> : 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	<a href="#">ASCT</a> : 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。	<a href="#">IDEL</a> : ILM Initiated Delete

コード	説明	を参照してください
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。	<a href="#">SDEL : S3 DELETE</a>
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。	<a href="#">SGET : S3 GET</a>
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。	<a href="#">Shea : S3 ヘッド</a>
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。	<a href="#">SPUT : S3 PUT</a>
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。	<a href="#">WDEL : Swift の削除</a>
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。	<a href="#">wget : Swift GET</a>
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。	<a href="#">WHEA : Swift ヘッド</a>
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。	<a href="#">WPUT : Swift PUT</a>

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

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

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

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

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

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

最後に 'audit-sum ツールでは' パイプからの入力も受け入れられますこれにより 'grep コマンドまたはその他の方法を使用して' 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。圧縮ファイル进行处理するには、ファイル名をコマンドライン引数として指定するか、「zcat」ツールを使用して最初にファイルを解凍します。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 'サマリーには最小' 最大' 平均のオペレーション時間が表示されますが 'size (-s)' オプションを使用してオブジェクト・サイズを表示することもできます

利用可能なオプションを表示するには 'help (-h)' オプションを使用します例：

```
$ 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たパスワードを入力します。
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
```

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

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

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 回表示するには、grep コマンドを使用して SGET メッセージだけを選択し、long 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/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r90l0aQ8JB-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 'グリッドから取得されるオブジェクトのサイズを決定するには 'size オプション ('s') を使用します

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



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

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

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

```
grep SGET audit.log | audit-sum -gt 1H
```

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

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

- b. どのサイズのオブジェクトが昨日取得されたかを調べるには ' コマンドに size オプション ('-s') を追加します

```
grep SGET audit.log | audit-sum -gt 1H -s
```

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

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

- c. より詳細な情報を表示するには 'audit-explain' ツールを使用して 'その時間中のすべての SGET 操作を確認します

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

grep コマンドの出力が多くなると予想される場合は、「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 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. まず、'-go' オプションを使用します。このオプションは、オブジェクトおよびバケット操作のメッセージを個別にグループ化します。

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

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

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、バケットごとにメッセージをグループ化する `-gb` オプションを使用します。

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

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ltd002 0.361	1564563	0.011	51.569

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

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

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

## 関連情報

[audit-explain ツールを使用してください](#)

## 監査メッセージの形式

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

「audit-explain」および「audit-sum」ツールで提供されるサマリー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記録されている監査メッセージの例です。

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

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

- 角カッコ [] で囲まれています
- 監査メッセージを示す文字列「AUDT」で始まる
- 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した \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・タイプの 4 文字の識別子です。型は括弧で囲まれます
- 「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。

関連情報

[audit-explain ツールを使用してください](#)

[audit-sum ツールを使用します](#)

[監査メッセージ](#)

[監査メッセージの共通要素](#)

[データ型](#)

[監査メッセージの例](#)

データ型

監査メッセージ内の情報の格納にはさまざまなデータタイプが使用されます。

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



コード	を入力します	説明
ANID	UI32	Node ID : メッセージを生成したサービスに割り当てられたグリッドノード ID 。各サービスには、StorageGRID システムの設定およびインストール時に一意の識別子が割り当てられます。この ID は変更できません。
ASES	UI64	Audit Session Identifier : 以前のリリースでは、この要素はサービスの開始後に監査システムが初期化された時間を示していました。この時間値は、オペレーティングシステムのエPOCH（1970 年 1 月 1 日 00 : 00 : 00 UTC）からのマイクロ秒数で計測されていました。  ・注：* この要素は廃止され、監査メッセージには表示されなくなりました。
ASQN	UI64	Sequence Count : 以前のリリースでは、このカウンタはグリッドノード（ANID）上で監査メッセージが生成されるたびに増分し、サービスの再起動時にゼロにリセットされていました。  ・注：* この要素は廃止され、監査メッセージには表示されなくなりました。
ATID	UI64	Trace ID : 1 つのイベントによってトリガーされた一連のメッセージで共有される識別子。
ATIM	UI64	Timestamp : 監査メッセージをトリガーしたイベントが生成された時刻。オペレーティングシステムのエPOCH（1970 年 1 月 1 日 00 : 00 : 00 UTC）からのマイクロ秒数で計測されます。タイムスタンプをローカルの日時に変換するためのツールは、ほとんどがミリ秒に基づいています。  ログに記録されたタイムスタンプの丸めや切り捨てが必要な場合があります。「audit.log」ファイルの監査メッセージの先頭に表示される人間が判読できる時間は、ISO 8601 形式の ATIM 属性です。日付と時刻は「YYYY-MMDDTHH : MM : SS.UUUUUUUU」の形式で表されます。「T」は、時刻セグメントの先頭を示すリテラル文字です。_UUUUUUUU はマイクロ秒である。
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。

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPUT
] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):157922414
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):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP\ (FC32)\ : SP
UT] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):1579224
144102530435]]
```

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

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR)\ : "s3small11"] [S3
KY(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):
0] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPU
T] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):157922414
4102530435]]
```

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

**2014-07-17T21:17:58.959669**

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0][AVER(UI32):10][ATIM\ (UI64\):1405631878959669][ATYP(FC32):SPUT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144102530435]]
```

ATIM は、UNIX エポックの開始時点からの時間をマイクロ秒数で記録します。この例では、値「1405631878959669」は、Thursday、17-2014 21:17:59 UTC に変換されます。

関連情報

[SPUT : S3 PUT](#)

[監査メッセージの共通要素](#)

## 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、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 （S3 バケット）および / または S3KY （S3 キー）
Swift 処理をリンクしています	WCON （Swift コンテナ）および / または WOBJ （Swift オブジェクト）
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。

### 情報ライフサイクル管理ポリシーの設定

デフォルトの ILM ポリシー（Baseline 2 Copy）では、オブジェクトデータは 1 回コピーされ、コピーは合

計 2 つになります。3 つ以上のコピーが必要な ILM ポリシーの場合は、追加コピーごとに CBRE、CBSE、SCMT メッセージのセットが生成されます。ILM ポリシーの詳細については、情報ライフサイクル管理によるオブジェクトの管理に関する情報を参照してください。

## 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。

### 関連情報

[ILM を使用してオブジェクトを管理する](#)

## 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	<a href="#">SPUT：S3 PUT</a>
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	<a href="#">ORLM：オブジェクトルールが満たされています</a>

### 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	<a href="#">WPUT : Swift PUT</a>
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	<a href="#">ORLM : オブジェクトルールが満たされています</a>

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、組み込みの ILM ルール「Make 2 Copies」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、LOCS フィールドには、イレイジャーコーディングのプロファイル ID とグループ ID が記録されます

```
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	<a href="#">SDEL : S3 DELETE</a>

### 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	<a href="#">WDEL : Swift の削除</a>

### 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 DELETE Object 要求を送信した時点で始まります。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	<a href="#">SGET : S3 GET</a>

### 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	<a href="#">wget : Swift GET</a>

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 GET Object 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][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\):SGET\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
```

バケットポリシーで許可されている場合、クライアントは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、クライアントは、自身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 GET Object 要求を送信します。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。

各クエリの結果には、S3 Select 要求の承認を実行する監査メッセージ（S3SR フィールドが「SELECT」に設定されている）と、処理中にストレージからデータを読み出す後続の標準の GET 処理の 2 つが表示されます。

```
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	<a href="#">SUPD：S3 メタデータが更新されました</a>

### 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、S3 オブジェクト（S3KY）の指定されたメタデータ（x-amz-meta-*\**）を更新する要求（SUPD）を実行します。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せん。

```

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]]

```

## 関連情報

[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

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。アルファベット順に記載されているため、特定のメッセージに関する情報を簡単に見つけることができます。

この章で使用されている4文字のコードは、次のサンプルメッセージに示すように、監査メッセージ内にある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、ログの送信先の変更、および監査情報に外部 syslog サーバを使用する方法については、[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

監査メッセージの各カテゴリについて理解しておく必要があります。これらのグループは、メッセージが表すアクティビティのクラスに基づいて分類されます。

### 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について十分に理解しておく必要があります。潜在的な問題に対処できるよう、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ついて生成されます。

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。	<a href="#">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がありません</a>
ECOC	Corrupt 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破損が検出されたことを示します。	<a href="#">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が破損しています</a>
ETAF	Security Authentication Failed : Transport Layer Security ( TLS ) を使用した接続試行が失敗しました。	<a href="#">ETAF : セキュリティ認証に失敗しました</a>
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。	<a href="#">GNRG : GNDS 登録</a>
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。	<a href="#">GNUR : GNDS 登録解除</a>
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。	<a href="#">GTED : Grid タスクが終了しました</a>
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。	<a href="#">GTSt : Grid タスクが開始されました</a>

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
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
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
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
ORLM の場合	Object Rules Met : オブジェクトデータが ILM ルールに沿って格納されました。	ORLM : オブジェクトルールが満たされています
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

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
SYSD	Node Stop : シャットダウンが要求されました。	<a href="#">SYSD : ノード停止</a>
SYST	Node Stopping : サービスが正常な停止を開始しました。	<a href="#">SYST : ノードを停止しています</a>
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。	<a href="#">SYSU : ノードが開始されました</a>
VLST	ユーザーが開始したボリュームが失われました : /proc/CMSI/Volume_lost コマンドが実行されました	<a href="#">VLST : ユーザーが開始したボリュームが失われました</a>

#### 関連情報

[LKCU: 上書きされたオブジェクトのクリーンアップ](#)

#### 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について十分に理解しておく必要があります。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を示します。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。	<a href="#">APCT : クラウド階層からのアーカイブの削除</a>
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。	<a href="#">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</a>

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。	<a href="#">ARCE</a> : 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。	<a href="#">ARCT</a> : 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。	<a href="#">AREM</a> : 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。	<a href="#">ASCE</a> : 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。	<a href="#">ASCT</a> : 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。	<a href="#">ATCE</a> : 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。	<a href="#">AVCC</a> : アーカイブによってクラウド階層の構成を検証
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。	<a href="#">CBSE</a> : オブジェクト送信終了

コード	説明	を参照してください
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。	<a href="#">CBRE : オブジェクト受信終了</a>
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。	<a href="#">SCMT : オブジェクトストアのコミット</a>
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。	<a href="#">SREM : オブジェクトストアの削除</a>

#### 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
SGET	<p>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。</p> <p>• 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。</p>	S3 クライアント	<a href="#">SGET : S3 GET</a>
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	<a href="#">Shea : S3 ヘッド</a>
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	<a href="#">wget : Swift GET</a>

コード	説明	によって使用されます	を参照してください
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	<a href="#">WHEA : Swift ヘッド</a>

#### 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 クライアント Swift クライアント	<a href="#">OVWR : オブジェクトを上書き</a>
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。  <ul style="list-style-type: none"> <li>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。</li> </ul>	S3 クライアント	<a href="#">SDEL : S3 DELETE</a>
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	<a href="#">SPO : S3 POST</a>



コード	説明	によって使用されます	を参照してください
SPUT	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>	S3 クライアント	<a href="#">SPUT : S3 PUT</a>
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	<a href="#">SUPD : S3 メタデータが更新されました</a>
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	<a href="#">WDEL : Swift の削除</a>
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	<a href="#">WPUT : Swift PUT</a>

## 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。	<a href="#">MGAU : 管理監査メッセージ</a>

## 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。
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の場所が見つからない場合は、ボリューム ID 0 が返されます。
RSLT	取得結果	<p>アーカイブ読み出しプロセスの完了ステータス：</p> <ul style="list-style-type: none"> <li>• SUCS : 成功しました</li> <li>• VRFL : 失敗（オブジェクトの検証に失敗）</li> <li>• 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）</li> <li>• CANC : 失敗（読み出し処理がキャンセルされた）</li> <li>• GERR : 失敗（一般的なエラー）</li> </ul>

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。

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	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： <ul style="list-style-type: none"> <li>• SUCS：成功しました</li> <li>• 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）</li> <li>• GERR：失敗（一般的なエラー）</li> </ul>

#### 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的識別子。
VREN	検証が有効です	<p>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</p> <ul style="list-style-type: none"> <li>• VENA : 検証が有効になっています</li> <li>• VDSA : 検証は無効です</li> </ul>
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）。
RSLT	結果	<p>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</p> <ul style="list-style-type: none"> <li>• SUCS : 成功（アーカイブプロセスが成功）</li> <li>• OFFL : 失敗（アーカイブがオフライン）</li> <li>• VRFL : 失敗（オブジェクトの検証に失敗）</li> <li>• 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）</li> <li>• GERR : 失敗（一般的なエラー）</li> </ul>

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的識別子。
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的識別子（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的識別子。
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的識別子。処理に失敗した場合は 0 が返されます。

コード	フィールド	説明
RSLT	結果	<p>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</p> <ul style="list-style-type: none"> <li>• SUCS : 成功 (コンテンツブロックは正常に格納されました)</li> <li>• EXIS : 無視 (コンテンツブロックはすでに格納されています)</li> <li>• ISFD : 失敗 (ディスクスペースが足りません)</li> <li>• STER : 失敗 (CBID の格納エラー)</li> <li>• OFFL : 失敗 (アーカイブがオフライン)</li> <li>• GERR : 失敗 (一般的なエラー)</li> </ul>

**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。

**CBRB** : オブジェクト受信が開始されました

通常 of 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。

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

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 )	<p>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。</p> <p>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。</p> <p>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。</p>
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	<p>(送信側エンティティから見た) 転送処理の結果：</p> <p>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。</p> <p>CONL : 転送中に接続が失われました</p> <p>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</p> <p>UNRE : デスティネーションノード ID に到達できません</p> <p>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 (改ざんの可能性があります)。</p>

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 / 接続の一意的識別子。
CBID	Content Block Identifier の略	転送されるコンテンツブロックの一意的識別子。

コード	フィールド	説明
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。
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。

コード	フィールド	説明
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 ）	<p>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。</p> <p>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。</p> <p>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。</p>
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	<p>(送信側エンティティから見た) 転送処理の結果：</p> <p>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。</p> <p>CONL : 転送中に接続が失われました</p> <p>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</p> <p>UNRE : デスティネーションノード ID に到達できません</p> <p>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 (改ざんの可能性があります)。</p>

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。

**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がありません

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が破損しています

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。
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。

コード	フィールド	説明
RSLT	理由コード	<p>失敗の理由：</p> <p>SCNI：セキュアな接続を確立できませんでした。</p> <p>CERM：証明書がありません。</p> <p>CERT：証明書が無効です。</p> <p>CERE：証明書が期限切れです。</p> <p>CERR：証明書が取り消されています。</p> <p>CSGN：証明書の署名が無効です。</p> <p>CSGU：証明書の署名者が不明です。</p> <p>UCRM：ユーザクレデンシャルがありません。</p> <p>UCRI：ユーザクレデンシャルが無効です。</p> <p>UCRU：ユーザのクレデンシャルが拒否されました。</p> <p>TOUT：認証がタイムアウトしました。</p>

TLS を使用する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： <ul style="list-style-type: none"> <li>• SUCS : 成功しました</li> <li>• SUNV : サービスを使用できません</li> <li>• GERR : その他の失敗</li> </ul>
GNID	ノード ID	更新要求を開始したサービスのノード ID。
GNTTP	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： <ul style="list-style-type: none"> <li>• SUCS : 成功しました</li> <li>• SUNV : サービスを使用できません</li> <li>• GERR : その他の失敗</li> </ul>
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	<p>このフィールドは、生成されたグリッドタスクを一意に識別します。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。</p> <p>• 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。</p>

コード	フィールド	説明
RSLT	結果	<p>グリッドタスクの最終ステータス：</p> <ul style="list-style-type: none"> <li>• SUCS : グリッドタスクが正常に完了しました。</li> <li>• ABRT : グリッドタスクがロールバックエラーなしで中止されました。</li> <li>• ROLF : グリッドタスクが中止され、ロールバックプロセスを完了できませんでした。</li> <li>• 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。</li> <li>• EXPR : グリッドタスクは開始前に期限切れとなりました。</li> <li>• IVLD : グリッドタスクは無効でした。</li> <li>• AUTH : グリッドタスクは許可されていませんでした。</li> <li>• DUPL : グリッドタスクは重複として拒否されました。</li> </ul>

#### **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を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	<p>このフィールドは、生成されたグリッドタスクを一意に識別します。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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
RSLT	結果	<p>結果。このフィールドの値は 1 つだけです。</p> <ul style="list-style-type: none"> <li>SUCS：グリッドタスクが正常に開始されました。</li> </ul>

**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	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ttyp	タスクタイプ (Task Type)	グリッドタスクのタイプ。

コード	フィールド	説明
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。
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	<p>タスクのソース：</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
ACTV	アクティベーションタイプ	<p>アクティブ化のタイプ：</p> <ul style="list-style-type: none"> <li>• Auto：グリッドタスクは自動でアクティブ化されます。</li> <li>• 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。</li> </ul>
RSLT	結果	<p>送信結果：</p> <ul style="list-style-type: none"> <li>• SUCS：グリッドタスクは正常に送信されました。</li> <li>• FAIL：タスクは Historical テーブルに直接移動されました。</li> </ul>

#### 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 。
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	マーカージョ 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記録されません。
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）。

コード	フィールド	説明
LOCS	ロケーション	<p>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。</p> <p>CLEC : イレイジャーコーディングされた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。</p> <p>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。</p> <p>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。</p>
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	<p>ILM 処理の結果。</p> <p>SUCS : ILM 処理が成功しました。</p>
ルール	ルールラベル ( Rules Label )	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
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。バージョン管理されていないバケット内のバケットや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。
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、オブジェクトをコピー（レプリケートまたはイレイジャーコーディング）する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。
NOID	ソースノード ID	場所が失われたノード ID。
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。
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 です。

コード	フィールド	説明
LTyp	保管場所タイプ	<p>CLDI（Online）：レプリケートされたオブジェクトデータ用</p> <p>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</p> <p>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</p>
PCLD	レプリケートオブジェクトへのパス	<p>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。</p> <p>/var/local/rangedb/2/p/13/13/00oJs6X% {h {u} SeUFxE@ の形式をとります</p>
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	<p>USER：ユーザがトリガーしました</p> <p>SYST：システムがトリガーされました</p>

#### MG AU：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。



コード	フィールド	説明
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	<p>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。</p> <ul style="list-style-type: none"> <li>• ユーザ名とアカウント ID : * POST authorize *</li> <li>• 新しいサブネット設定 : * POST /grid/grid-networks/update *</li> <li>• 新しい NTP サーバ : * POST /grid/ntp-servers /update * に含まれています</li> <li>• 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</li> <li>• 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。</li> </ul>
検査	要求メソッド	<p>HTTP 要求メソッド :</p> <ul style="list-style-type: none"> <li>• 投稿 ( Post )</li> <li>• PUT</li> <li>• 削除</li> <li>• パッチ</li> </ul>
MRSC	応答コード	応答コード。

コード	フィールド	説明
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。
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 システム内にオブジェクトのコピーを 1 つも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ダイレクトまたはニアラインの場所がある場合。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。

コード	フィールド	説明
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された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。

コード	フィールド	説明
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。
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。

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生成でき、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。
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。

#### 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。
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是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記録されません。
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記録されません。
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記録されません。

コード	フィールド	説明
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>• 注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
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	<p>DELETE トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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記録されません。
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。



コード	フィールド	説明
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。
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。バージョン管理されていないバケット内のバケットや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またはバケット内のオブジェクト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。バケットに対する処理ではこのフィールドは記録されません。
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。

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)。バケットに対する処理ではこのフィールドは記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>• 注意 : *X-Forwarded-For は、要求に存在し、 'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド ) と異なる場合に自動的に含められます。</li> </ul>
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	<p>GET トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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記録されません。
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。

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）	<p>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`</p> <p>匿名の要求の場合は空です。</p>
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。バージョン管理されていないバケット内のバケットや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的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。
CNID	接続識別子	TCP / IP 接続の一意的システム識別子。
CSIZ	コンテンツサイズ ( 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記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>• 注意 : *X-Forwarded-For は、要求に存在し、 'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
RSLT	結果コード	<p>GET トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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。

コード	フィールド	説明
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記録されません。
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。
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）	<p>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`</p> <p>匿名の要求の場合は空です。</p>
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。バージョン管理されていないバケット内のバケットや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。
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	<p>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。</p> <ul style="list-style-type: none"> <li>注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
RSLT	結果コード	<p>POST Object restore 要求の結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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。

コード	フィールド	説明
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記録されません。
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「select」に設定されます。
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。
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。

コード	フィールド	説明
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。バージョン管理されていないバケット内のバケットや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的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。
CMP	コンプライアンス設定	バケットを作成する際に使用された準拠設定（PUT Bucket 要求にこの設定がある場合、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 接続の一意的システム識別子。
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記録されません。



コード	フィールド	説明
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
LKEN	オブジェクトロックが有効になりました	PUT Bucket 要求に要求ヘッダー「x-amz-bucketobject-lock-enabled」が存在する場合、その値
LKLH	オブジェクトロックリーガルホールド	PUT Object 要求に要求ヘッダーの「x-amz-object-lock-legal hold」の値が存在する場合
LKMD	オブジェクトロック保持モード	PUT Object 要求に要求ヘッダーの「x-amz-object-lock-mode」が存在する場合は、その値。
LKRU	オブジェクトロック終了日まで保持	PUT Object 要求に要求ヘッダーの「x-amz-object-lock-retain-date」の値が存在する場合
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	<p>PUT トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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。

コード	フィールド	説明
S3KY	S3KY	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記録されません。
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）。
サスペンション	S3 ユーザの URN（要求の送信者）	<p>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`</p> <p>匿名の要求の場合は空です。</p>
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。

コード	フィールド	説明
ULID	ID をアップロードします	Complete Multipart Upload 処理の SPUT メッセージのみに含まれます。すべてのパーツがアップロードされ、アSEMB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。バージョン管理されていないバケット内のバケットや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」のどちらかです。オブジェクトに関する処理ではこのフィールドは記録されません。

#### **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	<p>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。</p> <p>SUCS : コンテンツが永続的ストレージから削除されました</p>

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記録されません。
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記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド ) と異なる場合に自動的に含められます。</li> </ul>
RSLT	結果コード	<p>GET トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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。

コード	フィールド	説明
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く 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記録されません。
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。
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）	<p>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`</p> <p>匿名の要求の場合は空です。</p>
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。

コード	フィールド	説明
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。バージョン管理されていないバケット内のバケットや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的識別子。
RSLT	結果コード	<p>検証失敗のタイプ：</p> <p>CRCF : 巡回冗長検査（CRC）が失敗しました。</p> <p>HMAC : ハッシュベースのメッセージ認証コード（HMAC）チェックが失敗しました。</p> <p>EHSB : 暗号化されたコンテンツハッシュが想定外です。</p> <p>PHSH : 元のコンテンツハッシュが想定外です。</p> <p>SEQC : ディスク上のデータシーケンスが正しくありません。</p> <p>PERR : ディスクファイルの構造が無効です。</p> <p>DERR : ディスクエラーです。</p> <p>FNAM : ファイル名が無効です。</p>

- ・注：\* このメッセージは注意深く監視する必要があります。コンテンツ検証が失敗する場合、コンテンツが改ざんされようとしている可能性や、ハードウェア障害が近いうちに発生す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。

- ・注：\* 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。コンテンツが改ざんされようとしている可能性や、ハードウェア障害が近いうちに発生する可能性があるため、ただちに状況を調査してこれらのコピーが作成された経緯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その後の再起動後に送信されます。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 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、RSLT がダーティーシャットダウンを示すことはありません。

**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、メッセージの RSLT がダーティシャットダウンを示すことはありません。

**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。

**VLST** : ユーザーが開始したボリュームが失われました

このメッセージは '/proc/CMSI/Volume\_lost' コマンドが実行されるたびに発行されます



コード	フィールド	説明
VOLL	Volume Identifier（ボリューム識別子）下限	影響を受けるボリューム範囲の下端、または単一ボリューム。
volu	ボリューム識別子上限	影響を受けるボリューム範囲の終了 ID。単一ボリュームの場合は VOLL と同じです。
NOID	ソースノード ID	場所が失われたノード ID。
LTYP	保管場所タイプ	「CLDI」（オンライン）または「CLNL」（ニアライン）。指定しない場合、デフォルトは「CLDI」です。
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、「UCS」ではなく「none」が使用されます。

#### 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。コンテナに関する処理ではこのフィールドは記録されません。
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）。コンテナに関する処理ではこのフィールドは記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>注意：*X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
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。コンテナに関する処理ではこのフィールドは記録されません。
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的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。
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処理ではこのフィールドは記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
RSLT	結果コード	<p>GET トランザクションの結果。結果は常にです</p> <p>SUCS : 成功しました</p>
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。アカウントに関する処理ではこのフィールドは記録されません。
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処理ではこのフィールドは記録されません。
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処理ではこのフィールドは記録されません。
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処理ではこのフィールドは記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>

コード	フィールド	説明
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 。
WCON	Swift コンテナ	Swift コンテナ名。アカウントに関する処理ではこのフィールドは記録されません。
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処理ではこのフィールドは記録されません。
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的識別子。CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに関する処理ではこのフィールドは記録されません。
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)。コンテナに関する処理ではこのフィールドは記録されません。
HTRH	HTTP 要求ヘッダー	<p>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。</p> <ul style="list-style-type: none"> <li>• 注意 : *X-Forwarded-For は、要求に存在し、'X-Forwarded-For' 値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なる場合に自動的に含められます。</li> </ul>
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	<p>PUT トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
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。

コード	フィールド	説明
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。コンテナに関する処理ではこのフィールドは記録されません。
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权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

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