



監査メッセージの形式

StorageGRID software

NetApp
December 03, 2025

目次

監査メッセージの形式	1
監査メッセージの形式	1
データ型	2
イベント固有のデータ	2
監査メッセージの共通要素	3
監査メッセージの例	4

監査メッセージの形式

監査メッセージの形式

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

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

以下は、監査ログ ファイルに表示される監査メッセージの例です。

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

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

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

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

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

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

次のリストは、属性要素について説明しています。

- `ATTR` 報告される属性の 4 文字のコードです。すべての監査メッセージに共通する属性と、イベント固有の属性があります。
- type `UI64`、`FC32` など、値のプログラミング データ型の 4 文字の識別子です。型は括弧で囲まれません `()`。
- value `属性の内容であり、通常は数値またはテキスト値です。値は常にコロンの後に続きます (:)。データ型 CSTR の値は二重引用符 "" で囲まれます。

データ型

監査メッセージに情報を格納するために、さまざまなデータ型が使用されます。

タイプ	説明
UI32	符号なし長整数 (32 ビット)。0 から 4,294,967,295 までの数値を格納できます。
UI64	符号なし倍精度整数 (64 ビット)。0 から 18,446,744,073,709,551,615 までの数値を格納できます。
FC32	4 文字の定数。「ABCD」などの 4 つの ASCII 文字として表される 32 ビットの符号なし整数値。
iPad	IP アドレスに使用されます。
CSTR	UTF-8 文字の可変長配列。文字は次の規則に従ってエスケープできます。 <ul style="list-style-type: none">• バックスラッシュは \\ です。• キャリッジリターンは \r です。• 二重引用符は \" です。• 改行(新しい行)は \n です。• 文字は、それに相当する 16 進数値 (\xHH 形式、HH は文字を表す 16 進数値) に置き換えることができます。

イベント固有のデータ

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

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

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT(FC32):SUCS]*  
[TIME(UI64):11454][SAIP(IPAD):"10.224.0.100"][S3AI(CSTR):"60025621595611246499"]  
[SACC(CSTR):"アカウント"  
ト"][S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA==" ]  
[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]  
[SBAI(CSTR):"60025621595611246499"][SBAC(CSTR):"アカウント"][S3BK(CSTR):"バケッ  
ト"][S3KY(CSTR):"オブジェクト"][CBID(UI64):0xCC128B9B9E428347]  
[UUID(CSTR):"B975D2CE-E4DA-4D14-8A23-  
1CB4B83F2CD8"][CSIZ(UI64):30720][AVER(UI32):10]  
[ATIM(UI64):1543998285921845][ATYP(FC32):SHEA][ANID(UI32):12281045][AMID(FC32):S3RQ]  
[ATID(UI64):15552417629170647261]]
```

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

監査メッセージの共通要素

すべての監査メッセージには共通の要素が含まれています。

コード	タイプ	説明
真ん中	FC32	モジュール ID: メッセージを生成したモジュール ID の 4 文字の識別子。これは、監査メッセージが生成されたコード セグメントを示します。
アニド	UI32	ノード ID: メッセージを生成したサービスに割り当てられたグリッド ノード ID。 StorageGRIDシステムが構成およびインストールされたときに、各サービスに一意的識別子が割り当てられます。このIDは変更できません。
ASES	UI64	<p>監査セッション識別子: 以前のリリースでは、この要素は、サービスの起動後に監査システムが初期化された時刻を示していました。この時間値は、オペレーティング システムのエポック (1970 年 1 月 1 日 00:00:00 UTC) からのマイクロ秒単位で測定されました。</p> <p>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。</p>
ASQN	UI64	<p>シーケンス カウント: 以前のリリースでは、このカウンタはグリッド ノード (ANID) で生成された監査メッセージごとに増加し、サービスの再起動時にゼロにリセットされていました。</p> <p>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。</p>
ATID	UI64	トレース ID: 単一のイベントによってトリガーされたメッセージのセットによって共有される識別子。
アティム	UI64	<p>タイムスタンプ: 監査メッセージをトリガーしたイベントが生成された時刻。オペレーティング システムのエポック (1970 年 1 月 1 日 00:00:00 UTC) からのマイクロ秒単位で測定されます。タイムスタンプをローカルの日付と時刻に変換するための利用可能なツールのほとんどは、ミリ秒に基づいていることに注意してください。</p> <p>ログに記録されたタイムスタンプの丸めまたは切り捨てが必要になる場合があります。監査メッセージの冒頭に表示される、人間が読める形式の時刻。audit.log`ファイルは ISO 8601 形式の ATIM 属性です。日付と時刻は次のように表されます `YYYY-MMDDTHH:MM:SS.UUUUUU、ここで `T`日付の時間セグメントの開始を示すリテラル文字列文字です。`UUUUUU`マイクロ秒です。</p>

コード	タイプ	説明
ATYP	FC32	イベント タイプ: 記録されるイベントの 4 文字の識別子。これは、メッセージの「ペイロード」コンテンツ、つまり含まれる属性を制御します。
アバー	UI32	バージョン: 監査メッセージのバージョン。StorageGRIDソフトウェアが進化するにつれて、新しいバージョンのサービスに監査レポートの新しい機能が組み込まれる可能性があります。このフィールドにより、AMS サービスでの下位互換性が有効になり、古いバージョンのサービスからのメッセージを処理できるようになります。
RSLT	FC32	結果: イベント、プロセス、またはトランザクションの結果。メッセージに関連しない場合は、メッセージが誤ってフィルタリングされないように、SUCS ではなく NONE が使用されます。

監査メッセージの例

各監査メッセージに詳細情報が記載されています。すべての監査メッセージは同じ形式を使用します。

以下は、監査メッセージの例です。`audit.log` ファイル：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"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]]
```

監査メッセージには、記録されるイベントに関する情報と、監査メッセージ自体に関する情報が含まれます。

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"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]]
```

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

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\CSTR\):"s3small11"][S3K
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\ (UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

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

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。