



監査メッセージの形式

StorageGRID

NetApp
October 03, 2025

目次

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

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。

- 角かっこ [] 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。
CSTR	UTF-8 文字の可変長アレイです。文字は次の方法でエスケープできます。 <ul style="list-style-type: none">• バックスラッシュは \。• 復帰文字は r です• 二重引用符は "。• 改行（新しい行）は n です• 文字は、それぞれに相当する 16 進数に置き換えることができます（\xHH の形式、HH は該当する文字を表す 16 進値）。

イベント固有のデータ

監査ログ内の各監査メッセージはシステムイベントに固有のデータを記録します。

メッセージ自体を識別する先頭の「[AUDT:]」コンテナに続く一連の属性は、監査メッセージによって説明されているイベントやアクションに関する情報を提供します。以下の例では、これらの属性を強調表示しています。

コード	を入力し ます	説明
ATIM	UI64	<p>Timestamp : 監査メッセージをトリガーしたイベントが生成された時刻。オペレーティングシステムのエポック (1970 年 1 月 1 日 00 : 00 : 00 UTC) からマイクロ秒で計測されます。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。</p> <p>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。</p>
ATYP	FC32	<p>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。</p>
ビーバー	UI32	<p>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に、AMS サービスにおける下位互換性を可能にします。</p>
RSLT	FC32	<p>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。</p>

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):1579224144
102530435]]
```

監査メッセージには、記録されたイベントに関する情報と、監査メッセージ自体に関する情報が含まれていません。

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):"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、17-201421:17:59 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](#)

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。