



監査メッセージの形式

StorageGRID 11.8

NetApp
March 19, 2024

目次

監査メッセージの形式	1
監査メッセージの形式：概要	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：概要

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

によって提供された概要情報の場合 "監査-説明する" および "audit-sumの略" ツールで十分ではありません。すべての監査メッセージの一般的な形式を把握するには、このセクションを参照してください。

以下は、監査ログファイルに記録されている監査メッセージの例です。

```
2014-07-17T03:50:47.484627
[AUDT: [RSLT (FC32) :VRGN] [AVER (UI32) :10] [ATIM (UI64) :1405569047484627] [ATYP (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。文字列全体が角かっこで囲まれます ([])、および文字列内の各属性要素には、次の特性があります。

- 角かっこで囲まれています []
- 文字列で導入されます `AUDT` を指定します
- 前後に区切り記号（カンマやスペース）がない
- 改行文字で終了します \n

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

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

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

次に、属性要素について説明します。

- ATTR は、報告される属性の4文字のコードです。すべての監査メッセージに共通する属性とイベント固有の属性があります。
- type は、UI64、FC32など、値のプログラミングデータ型の4文字の識別子です。タイプはかっこで囲まれます ()。
- value は属性の内容で、通常は数値またはテキスト値です。値の前には常にコロンが付きます (:)。データ型CStrの値は二重引用符で囲まれます。

データ型

監査メッセージ内の情報の格納にはさまざまなデータタイプが使用されます。

を入力します	説明
UI32	符号なし長整数（32ビット）。0~4、294、967、295の数値を格納できます。
UI64	符号なし倍精度長整数（64ビット）。0~18、446、744、073、709、551、615の数値を格納できます。
FC32	4文字の定数。"ABCD"などの4つのASCII文字で表される32ビットの符号なし整数値です。
iPad	IPアドレスに使用されます。
CSTR	UTF-8文字の可変長配列。文字は次の方法でエスケープできます。 <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。

開口部に続いて [AUDT: メッセージ自体を識別するコンテナ。次の一連の属性は、監査メッセージによって記述されるイベントまたはアクションに関する情報を提供します。以下の例では、これらの属性を強調表示しています。

```
2018-12-05T08:24:45.921845 [AUDT: \RST\ (FC32\): SUCS\]
\time\ (UI64): 11454\ \SAIP\ (iPad): "10.224.0.100"\ \S3AI\ (CStr): "60025621595611246499"\
\SACC\ (CStr): "account"\ \S3AK\ (CStr): "SGKH4_Nc8SO1H6w3w0nCOFCGK__E6dYzKlumRsKJA
=="\ \SUSR\ (CStr): "urn:sgws:identity::60025621595611246499:root"\ \SBAL\ (CStr):
"60025621595611246499"\ \SBAC\ (CStr): "account"\ \S3BK\ (CStr): "bucket"\ \S3KY\
(CStr): "object"\ \CBID\ (UI64): 0xCC128B9B9E428347\ \UUID\ (CStr): "B975D2CE-
E4DA-4D14-8A23-1CB4B83F2CD8"\ \CSIZ\ (UI64): 30720\ [aver (UI32): 10] \ATIM (UI64)
: 1543998285921845\ \ATYP\ (FC32): Shea\ \ANID (UI32): 12281045\ \AMID (FC32): S3RQ\
\ATID (UI64): 15552417629170647261\]
```

。ATYP 要素（この例では下線付き）は、メッセージを生成したイベントを識別します。このメッセージ例には、が含まれています "Shea" メッセージコード（[ATYP (FC32) : Shea]）。S3 HEAD要求が成功して生成

されたことを示します。

監査メッセージの共通要素

すべての監査メッセージには、共通の要素が含まれています。

コード	を入力します	説明
AMid	FC32	Module ID：メッセージを生成したモジュールIDの4文字の識別子。これは、監査メッセージが生成されたコードセグメントを示します。
ANID	UI32	Node ID：メッセージを生成したサービスに割り当てられたグリッドノード ID。各サービスには、StorageGRID システムの設定およびインストール時に一意の識別子が割り当てられます。このIDは変更できません。
ASES	UI64	Audit Session Identifier：以前のリリースでは、この要素はサービスの開始後に監査システムが初期化された時間を示していました。この時間値は、オペレーティングシステムのエポック（1970年1月1日00：00：00 UTC）からのマイクロ秒数で計測されていました。 ・注：* この要素は廃止され、監査メッセージには表示されなくなりました。
ASQN	UI64	Sequence Count：以前のリリースでは、このカウンタはグリッドノード（ANID）上で監査メッセージが生成されるたびに増分し、サービスの再起動時にゼロにリセットされていました。 ・注：* この要素は廃止され、監査メッセージには表示されなくなりました。
ATID	UI64	Trace ID：1つのイベントによってトリガーされた一連のメッセージで共有される識別子。
ATIM	UI64	Timestamp：監査メッセージをトリガーしたイベントが生成された時刻。オペレーティングシステムのエポック（1970年1月1日00：00：00 UTC）からのマイクロ秒数で計測されます。タイムスタンプをローカルの日時に変換するためのツールは、ほとんどがミリ秒に基づいています。 ログに記録されたタイムスタンプの丸めや切り捨てが必要な場合があります。の監査メッセージの先頭に表示される判読可能な時刻 <code>audit.log</code> fileは、ISO 8601形式のATIM属性です。日付と時刻はの形式で表示されます <code>YYYY-MMDDTHH:MM:SS.UUUUUU`</code> を参照してください。`T`は、日付の時間セグメントの先頭を示すリテラル文字です。 <code>UUUUUU</code> はマイクロ秒です。

コード	を入力します	説明
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に、AMS サービスにおける下位互換性を可能にします。
RSLT	FC32	Result：イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、誤ってフィルタリングされないように SUCS ではなく NONE が使用されます。

監査メッセージの例

各監査メッセージには詳細な情報が含まれています。監査メッセージはすべて同じ形式です。

以下は、に表示される監査メッセージの例です。audit.log ファイル：

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK (CSTR) : "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" 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 属性を判読できる形式です。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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、の値を指定し ます 1405631878959669 2014年7月17日 (木) 21:17:59 UTC に変換されます。

著作権に関する情報

Copyright © 2024 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。