



## 감사 메시지 형식 StorageGRID 11.7

NetApp  
April 12, 2024

# 목차

감사 메시지 형식 .....	1
감사 메시지 형식: 개요 .....	1
데이터 유형 .....	2
이벤트 관련 데이터 .....	2
감사 메시지의 공통 요소 .....	2
감사 메시지 예 .....	4

# 감사 메시지 형식

## 감사 메시지 형식: 개요

StorageGRID 시스템 내에서 교환되는 감사 메시지에는 모든 메시지에 공통되는 표준 정보 및 보고되는 이벤트 또는 활동을 설명하는 특정 콘텐츠가 포함됩니다.

에서 제공한 요약 정보인 경우 "감사 - 설명" 및 "감사 집계" 도구가 충분하지 않습니다. 모든 감사 메시지의 일반 형식을 이해하려면 이 섹션을 참조하십시오.

다음은 감사 로그 파일에 표시될 수 있는 감사 메시지의 예입니다.

```
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]]
```

각 감사 메시지에는 특성 요소의 문자열이 포함됩니다. 전체 문자열은 대괄호로 묶여 있습니다 ([ ]) 및 문자열의 각 특성 요소에는 다음과 같은 특성이 있습니다.

- 대괄호로 묶입니다 [ ]
- 문자열에 의해 도입되었습니다 AUDT, 감사 메시지를 나타냅니다
- 앞 또는 뒤에 구분 기호(쉼표 또는 공백 없음)를 사용하지 않습니다
- 줄 바꿈 문자로 종료되었습니다 \n

각 요소에는 특성 코드, 데이터 형식 및 다음 형식으로 보고된 값이 포함됩니다.

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

메시지의 특성 요소 수는 메시지의 이벤트 유형에 따라 달라집니다. 특성 요소가 특정 순서로 나열되지 않습니다.

다음 목록에서는 특성 요소에 대해 설명합니다.

- ATTR 는 보고되는 특성에 대한 4자리 코드입니다. 모든 감사 메시지에 공통적으로 적용되는 일부 특성 및 이벤트별 특성이 있습니다.
- type 는 UI64, FC32 등과 같이 값의 프로그래밍 데이터 형식의 4자리 식별자입니다. 형식은 괄호로 묶입니다 ( ).
- value 특성의 내용이며 일반적으로 숫자 또는 텍스트 값입니다. 값은 항상 콜론을 따릅니다 (:)를 클릭합니다. 데이터 형식 CStr 의 값은 큰따옴표로 묶입니다 " ".

## 데이터 유형

감사 메시지에 정보를 저장하는 데 사용되는 데이터 유형은 다양합니다.

유형	설명
UI32	부호 없는 긴 정수(32비트). 0에서 4,294,967,295 사이의 숫자를 저장할 수 있습니다.
UI64	부호 없는 이중 긴 정수(64비트). 0에서 18,446,744,073,709,551,615까지의 숫자를 저장할 수 있습니다.
FC32	4자 상수. 32비트 부호 없는 정수 값은 "ABCD"와 같은 4개의 ASCII 문자로 표시됩니다.
아이패드	IP 주소에 사용됩니다.
CStr(문자열)	UTF-8 문자의 가변 길이 배열입니다. 문자는 다음과 같은 규약을 사용하여 이스케이프할 수 있습니다. <ul style="list-style-type: none"><li>백슬래시는 \\ 입니다.</li><li>캐리지 리턴은\r입니다</li><li>큰따옴표는 \"지 않습니다.</li><li>라인 피드(새 라인)는\n입니다</li><li>문자는 해당 16진수 등가물(\xHH 형식으로, 여기서 HH는 문자를 나타내는 16진수 값)로 대체할 수 있습니다.</li></ul>

## 이벤트 관련 데이터

감사 로그의 각 감사 메시지는 시스템 이벤트와 관련된 데이터를 기록합니다.

구멍을 따라오는 중입니다 [AUDT: 메시지 자체를 식별하는 컨테이너이며, 다음 특성 집합은 감사 메시지에서 설명하는 이벤트 또는 작업에 대한 정보를 제공합니다. 이러한 특성은 다음 예제에서 강조됩니다.

```
2018-12-05T08:24:45.921845 [AUDT: * \[RSLT\(\FC32\):SUCS\] * \[TIME\(\UI64\):11454\]
\[SAIP\(\iPad\):"10.224.0.100"\]\[S3SStr\S31124562C642S562S564C6100C4S562S564CW5100C6100C6
100C4C4S564C4C4C4C4C4C4CW4S5100C4S562S564S564CW5100C4CW4S562S5100C4S5100C
4C4C4C4C4CW5100C4C4C4C4C6100C6100C6100CWs\S564C4C6100C4C4C4C4CWs\S564C4C4C4
CWs\S564CWs\S564C4C4S
```

를 클릭합니다 ATYP 요소(예제에서 밑줄 표시) 메시지를 생성한 이벤트를 식별합니다. 이 예제 메시지에는 가 포함되어 있습니다 "세어" 메시지 코드([ATYP(FC32):Shea])로, S3 헤드 요청에 의해 생성되었음을 나타냅니다.

## 감사 메시지의 공통 요소

모든 감사 메시지에 공통 요소가 포함됩니다.

코드	유형	설명
있습니다	FC32	모듈 ID: 메시지를 생성한 모듈 ID의 4자리 식별자입니다. 이것은 감사 메시지가 생성된 코드 세그먼트를 나타냅니다.
ANID	UI32	노드 ID: 메시지를 생성한 서비스에 할당된 그리드 노드 ID입니다. 각 서비스는 StorageGRID 시스템을 구성하고 설치할 때 고유 식별자를 할당합니다. 이 ID는 변경할 수 없습니다.
ASE	UI64	감사 세션 식별자: 이전 릴리즈에서는 이 요소는 서비스가 시작된 후 감사 시스템이 초기화된 시간을 나타냅니다. 이 시간 값은 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정되었습니다.  <ul style="list-style-type: none"> <li>참고: * 이 요소는 사용되지 않으며 감사 메시지에 더 이상 나타나지 않습니다.</li> </ul>
ASQN	UI64	시퀀스 수: 이전 릴리즈에서는 그리드 노드(ANID)에서 생성된 각 감사 메시지에 대해 이 카운터가 증가했으며 서비스 재시작 시 0으로 재설정됩니다.  <ul style="list-style-type: none"> <li>참고: * 이 요소는 사용되지 않으며 감사 메시지에 더 이상 나타나지 않습니다.</li> </ul>
ATID	UI64	추적 ID: 단일 이벤트에 의해 트리거된 메시지 집합에서 공유하는 식별자입니다.
ATIM	UI64	Timestamp: 감사 메시지를 트리거한 이벤트가 생성된 시간으로, 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정됩니다. 타임 스탬프를 로컬 날짜 및 시간으로 변환하는 데 사용할 수 있는 대부분의 도구는 밀리초를 기반으로 합니다.  로그된 타임스탬프의 반올림 또는 잘라내기가 필요할 수 있습니다. 에서 감사 메시지의 시작 부분에 나타나는 사람이 읽을 수 있는 시간입니다 audit.log file 은 ISO 8601 형식의 ATIM 속성입니다. 날짜 및 시간은 로 표시됩니다 YYYY-MMDDTHH:MM:SS.UUUUUU, 위치 T 날짜 시간 세그먼트의 시작 부분을 나타내는 리터럴 문자열 문자입니다. UUUUUU 마이크로초
ATYP	FC32	이벤트 유형: 기록되는 이벤트의 4자리 식별자입니다. 이는 메시지의 "페이로드" 콘텐츠, 즉 포함된 속성을 제어합니다.
비버	UI32	버전: 감사 메시지의 버전입니다. StorageGRID 소프트웨어가 발전함에 따라 새로운 버전의 서비스에는 감사 보고에 새로운 기능이 포함될 수 있습니다. 이 필드를 사용하면 AMS 서비스의 이전 버전과의 호환성을 통해 이전 버전의 서비스에서 보낸 메시지를 처리할 수 있습니다.
RSLT	FC32	결과: 이벤트, 프로세스 또는 트랜잭션의 결과. 이 메시지와 관련이 없으면 메시지가 실수로 필터링되지 않도록 SUCS 대신 사용되지 않습니다.

## 감사 메시지 예

각 감사 메시지에서 자세한 정보를 찾을 수 있습니다. 모든 감사 메시지는 동일한 형식을 사용합니다.

다음은 예 표시될 수 있는 샘플 감사 메시지입니다 audit.log 파일:

```
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]]
```

감사 메시지에는 기록되는 이벤트에 대한 정보와 감사 메시지 자체에 대한 정보가 포함되어 있습니다.

감사 메시지에 의해 기록되는 이벤트를 식별하려면 ATYP 속성(아래에 강조 표시됨)을 찾습니다.

```
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 특성의 값은 SPUT입니다. "SPUT" 오브젝트 인제스트를 버킷에 기록하는 S3 PUT 트랜잭션을 나타냅니다.

다음 감사 메시지는 객체가 연결된 버킷도 표시합니다.

```
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 이벤트가 발생한 시기를 확인하려면 감사 메시지 시작 부분에 UTC(Universal Coordinated Time) 타임스탬프를 기록합니다. 이 값은 감사 메시지 자체의 ATIM 특성의 사람이 읽을 수 있는 버전입니다.

**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]]
```

ATIM은 UNIX epoch 시작 이후 시간(단위: 마이크로초)을 기록합니다. 이 예에서 값은 입니다 1405631878959669 2014년 7월 17일 목요일 21:17:59 UTC로 번역.

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.