



개요

StorageGRID

NetApp
October 03, 2025

목차

| | |
|------------------------|---|
| 감사 로그 검토: 개요 | 1 |
| 감사 메시지 흐름 및 보존 | 1 |
| 감사 메시지 흐름 | 1 |
| 감사 로그 파일에 액세스합니다 | 4 |
| 로그 파일 회전을 감사합니다 | 5 |

감사 로그 검토: 개요

이 지침에는 StorageGRID 감사 메시지 및 감사 로그의 구조 및 내용에 대한 정보가 포함되어 있습니다. 이 정보를 사용하여 시스템 활동의 감사 추적을 읽고 분석할 수 있습니다.

이 지침은 StorageGRID 시스템의 감사 메시지를 분석해야 하는 시스템 활동 및 사용 보고서를 작성하는 관리자를 위한 것입니다.

텍스트 로그 파일을 사용하려면 관리자 노드에서 구성된 감사 공유에 액세스할 수 있어야 합니다.

감사 메시지 수준 구성 및 외부 syslog 서버 사용에 대한 자세한 내용은 [을 참조하십시오](#) [감사 메시지 및 로그 대상을 구성합니다](#).

관련 정보

- [StorageGRID 관리](#)

감사 메시지 흐름 및 보존

모든 StorageGRID 서비스는 정상적인 시스템 작동 중에 감사 메시지를 생성합니다. 이러한 감사 메시지가 StorageGRID 시스템을 통해 어떻게 'audit.log' 파일로 이동하는지 이해해야 합니다.

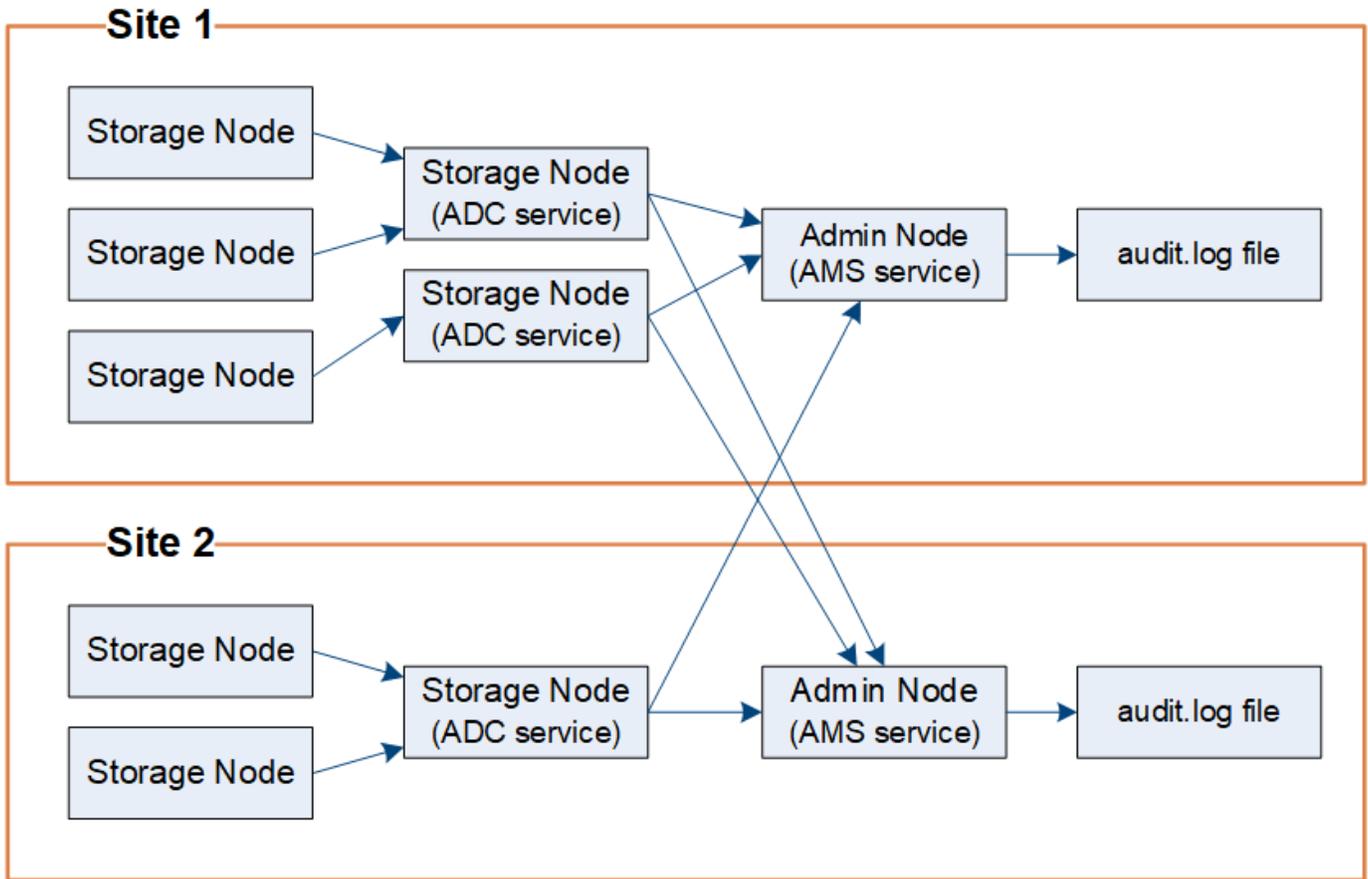
감사 메시지 흐름

감사 메시지는 관리 노드 및 ADC(관리 도메인 컨트롤러) 서비스가 있는 스토리지 노드에 의해 처리됩니다.

감사 메시지 흐름도에 표시된 대로 각 StorageGRID 노드는 데이터 센터 사이트의 ADC 서비스 중 하나에 감사 메시지를 보냅니다. ADC 서비스는 각 사이트에 설치된 처음 세 개의 스토리지 노드에 대해 자동으로 활성화됩니다.

그러면 각 ADC 서비스가 릴레이 역할을 하고 감사 메시지 모음을 StorageGRID 시스템의 모든 관리 노드로 전송하여 각 관리 노드에 시스템 활동의 전체 기록을 제공합니다.

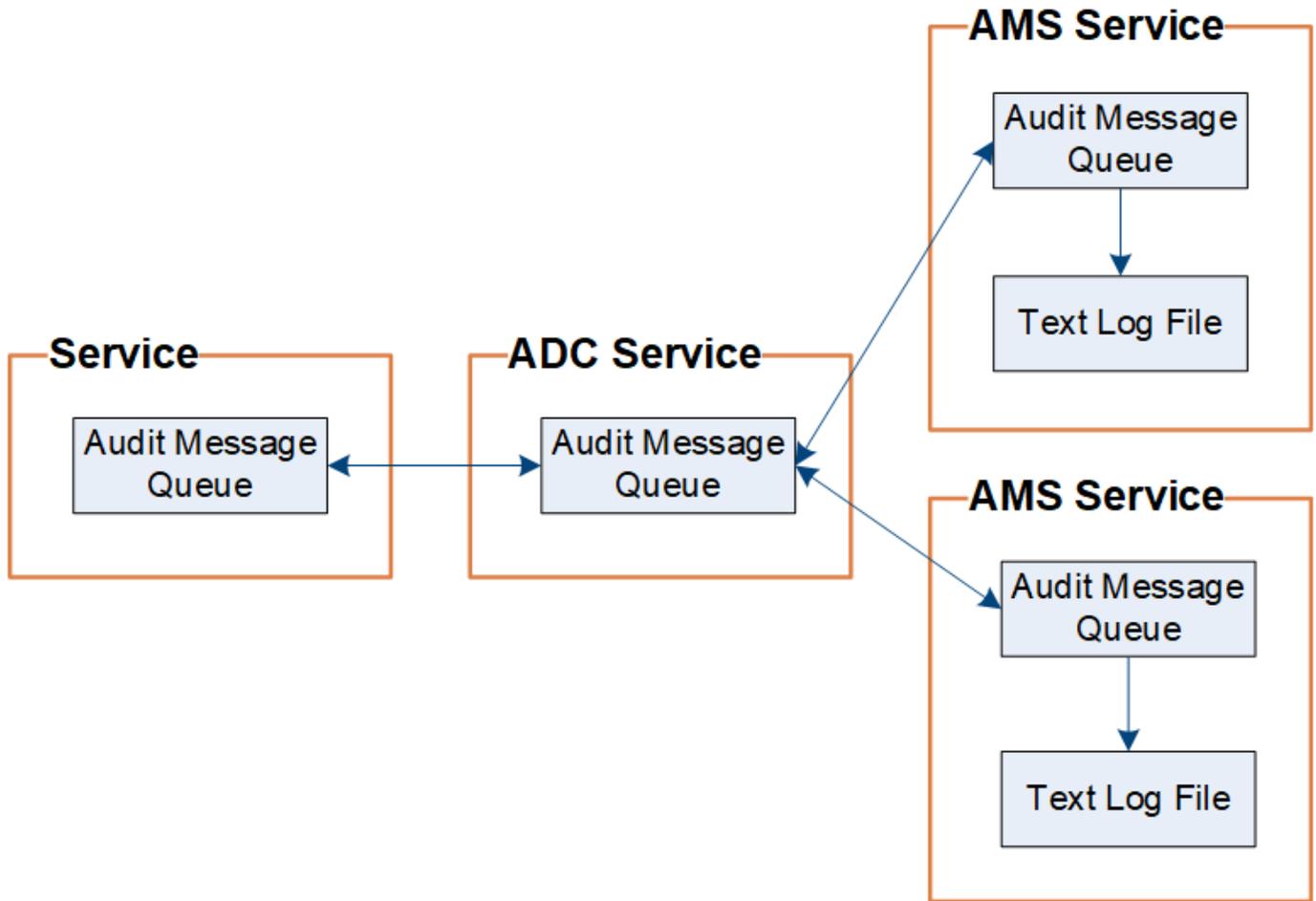
각 Admin Node는 텍스트 로그 파일에 감사 메시지를 저장하며, Active 로그 파일은 AUDIT.LOG로 명명된다.



감사 메시지 보존

StorageGRID는 복사 및 삭제 프로세스를 사용하여 감사 로그에 쓰기 전에 감사 메시지가 손실되지 않도록 합니다.

노드가 감사 메시지를 생성하거나 릴레이할 때 이 메시지는 그리드 노드의 시스템 디스크에 있는 감사 메시지 큐에 저장됩니다. 관리 노드의 '/var/local/audit/export' 디렉토리에 감사 로그 파일에 메시지가 기록될 때까지 메시지 복사본은 항상 감사 메시지 큐에 유지됩니다. 이렇게 하면 전송 중에 감사 메시지 손실을 방지할 수 있습니다.



네트워크 연결 문제 또는 감사 용량 부족으로 인해 감사 메시지 큐가 일시적으로 증가할 수 있습니다. 대기열이 늘어갈수록 각 노드의 '/var/local/' 디렉토리에서 사용 가능한 공간이 더 많이 사용됩니다. 문제가 지속되고 노드의 감사 메시지 디렉토리가 너무 가득 차면 개별 노드가 백로그 처리를 우선 순위에 따라 새 메시지에 일시적으로 사용할 수 없게 됩니다.

특히 다음과 같은 행동을 볼 수 있습니다.

- Admin Node에서 사용하는 '/var/local/audit/export' 디렉토리가 가득 차면 디렉토리가 더 이상 가득 차지 않을 때까지 Admin Node가 새 감사 메시지에 사용할 수 없는 것으로 플래그가 지정됩니다. S3 및 Swift 클라이언트 요청은 영향을 받지 않습니다. 감사 리포지토리에 연결할 수 없을 때 XAMS(Unreachable Audit Repositories) 경보가 트리거됩니다.
- ADC 서비스가 있는 스토리지 노드에서 사용하는 "/var/local/" 디렉토리가 92% 차면 디렉토리가 87%만 가득 찰 때까지 노드가 메시지를 감사할 수 없는 것으로 플래그가 지정됩니다. 다른 노드에 대한 S3 및 Swift 클라이언트 요청은 영향을 받지 않습니다. 감사 릴레이에 연결할 수 없는 경우 NRLY(사용 가능한 감사 릴레이) 경보가 트리거됩니다.



ADC 서비스에 사용 가능한 스토리지 노드가 없는 경우 스토리지 노드는 감사 메시지를 '/var/local/log/localaudit.log' 파일에 로컬로 저장합니다.

- 스토리지 노드에서 사용하는 "/var/local/" 디렉토리가 85%가 되면 노드에서 S3 및 Swift 클라이언트 요청을 거부하고 503 서비스 사용 불가 를 시작합니다.

다음과 같은 유형의 문제로 인해 감사 메시지 큐가 크게 증가할 수 있습니다.

- ADC 서비스가 있는 관리 노드 또는 스토리지 노드의 정전. 시스템의 노드 중 하나가 다운되면 나머지 노드가 백로그될 수 있습니다.
- 시스템의 감사 용량을 초과하는 지속적인 활동률입니다.
- 감사 메시지와 무관한 이유로 ADC 스토리지 노드의 '/var/local/' 공간이 가득 찼습니다. 이 경우 노드에서 새 감사 메시지 수신을 중지하고 현재 백로그의 우선 순위를 지정하며, 이로 인해 다른 노드에 백로그가 발생할 수 있습니다.

AMQS(Large audit queue alert and Audit messages Queued)(대형 감사 대기열 경고 및 감사 메시지 대기 중

시간에 따라 감사 메시지 대기열의 크기를 모니터링할 수 있도록 스토리지 노드 대기열 또는 관리 노드 대기열의 메시지 수가 특정 임계값에 도달하면 * 대규모 감사 대기열 * 경고와 레거시 AMQS 경보가 트리거됩니다.

대규모 감사 대기열 * 경고 또는 레거시 AMQS 경보가 트리거되면 시스템에서 로드를 확인하여 시작합니다. — 최근 트랜잭션이 많이 발생한 경우, 경고 및 알람은 시간이 지남에 따라 해결되어야 하며 무시할 수 있습니다.

경고 또는 경보가 지속되고 심각도가 증가하면 대기열 크기의 차트를 참조하십시오. 시간이 경과하거나 며칠 동안 꾸준히 증가하는 경우 감사 로드가 시스템의 감사 용량을 초과할 가능성이 높습니다. 클라이언트 쓰기 및 클라이언트 읽기의 감사 수준을 오류 또는 끄기로 변경하여 클라이언트 작업 속도를 줄이거나 기록된 감사 메시지 수를 줄입니다. 참조"감사 메시지 및 로그 대상을 구성합니다" 있습니다."

중복된 메시지

StorageGRID 시스템은 네트워크 또는 노드 장애가 발생할 경우 보수적인 접근 방식을 사용합니다. 따라서 감사 로그에 중복된 메시지가 있을 수 있습니다.

감사 로그 파일에 액세스합니다

감사 공유는 활성 'audit.log' 파일과 압축된 감사 로그 파일을 포함합니다. 감사 로그에 쉽게 액세스할 수 있도록 NFS 및 CIFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다(CIFS는 더 이상 사용되지 않음). 관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수도 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 관리 노드의 IP 주소를 알아야 합니다.

단계

1. 관리자 노드에 로그인:
 - a. 'ssh admin@primary_Admin_Node_IP' 명령을 입력합니다
 - b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 감사 로그 파일이 포함된 디렉토리로 이동합니다.

```
'cd /var/local/audit/export'
```

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

관련 정보

로그 파일 회전을 감사합니다

감사 로그 파일은 관리 노드의 '/var/local/audit/export' 디렉토리에 저장됩니다. 활성 감사 로그 파일은 audit.log로 명명됩니다.



선택적으로 감사 로그의 대상을 변경하고 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버가 구성되면 감사 레코드의 로컬 로그가 계속 생성되고 저장됩니다. 을 참조하십시오 [감사 메시지 및 로그 대상을 구성합니다](#).

하루 한 번, 활성화된 'audit.log' 파일이 저장되고, 새로운 'audit.log' 파일이 시작된다. 저장된 파일의 이름은 저장 시기를 나타냅니다('yyyy-mm-dd.txt' 형식). 하루에 둘 이상의 감사 로그가 생성되는 경우 파일 이름에 숫자가 추가된 파일 저장 날짜가 사용됩니다(yyyy-mm-dd.txt.n). 예를 들어 2018년 4월 15일 생성된 첫 번째 및 두 번째 로그 파일은 2018-04-15.txt와 2018-04-15.txt.1입니다.

하루 후에는 원래 날짜를 유지하는 형식(yyyy-mm-dd.txt.gz)으로 저장된 파일이 압축되고 이름이 변경됩니다. 시간이 지남에 따라 이로 인해 관리 노드의 감사 로그에 할당된 스토리지가 소비됩니다. 스크립트는 감사 로그 공간 소비를 모니터링하고 필요에 따라 로그 파일을 삭제하여 '/var/local/audit/export' 디렉토리의 공간을 확보합니다. 감사 로그는 작성된 날짜를 기준으로 삭제되며 가장 오래된 로그가 먼저 삭제됩니다. 다음 파일에서 스크립트의 작업을 모니터링할 수 있습니다: '/var/local/log/manage-audit.log'.

이 예에서는 액티브 'audit.log' 파일, 전날 파일('2018-04-15.txt') 및 전날 압축 파일('2018-04-14.txt.gz')을 보여 줍니다.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

저작권 정보

Copyright © 2025 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.