감사 메시지 개요

StorageGRID 11.5

NetApp
April 11, 2024

목차

감사 메시지 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.

귀하는 StorageGRID 시스템 내에서 감사 대상 활동의 특성을 제대로 이해하고 있다고 가정합니다. 텍스트 로그 파일을 사용하려면 관리자 노드에서 구성된 감사 공유에 액세스할 수 있어야 합니다.

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 로 이동하는 방법을 이해해야 합니다 `audit.log` 파일.

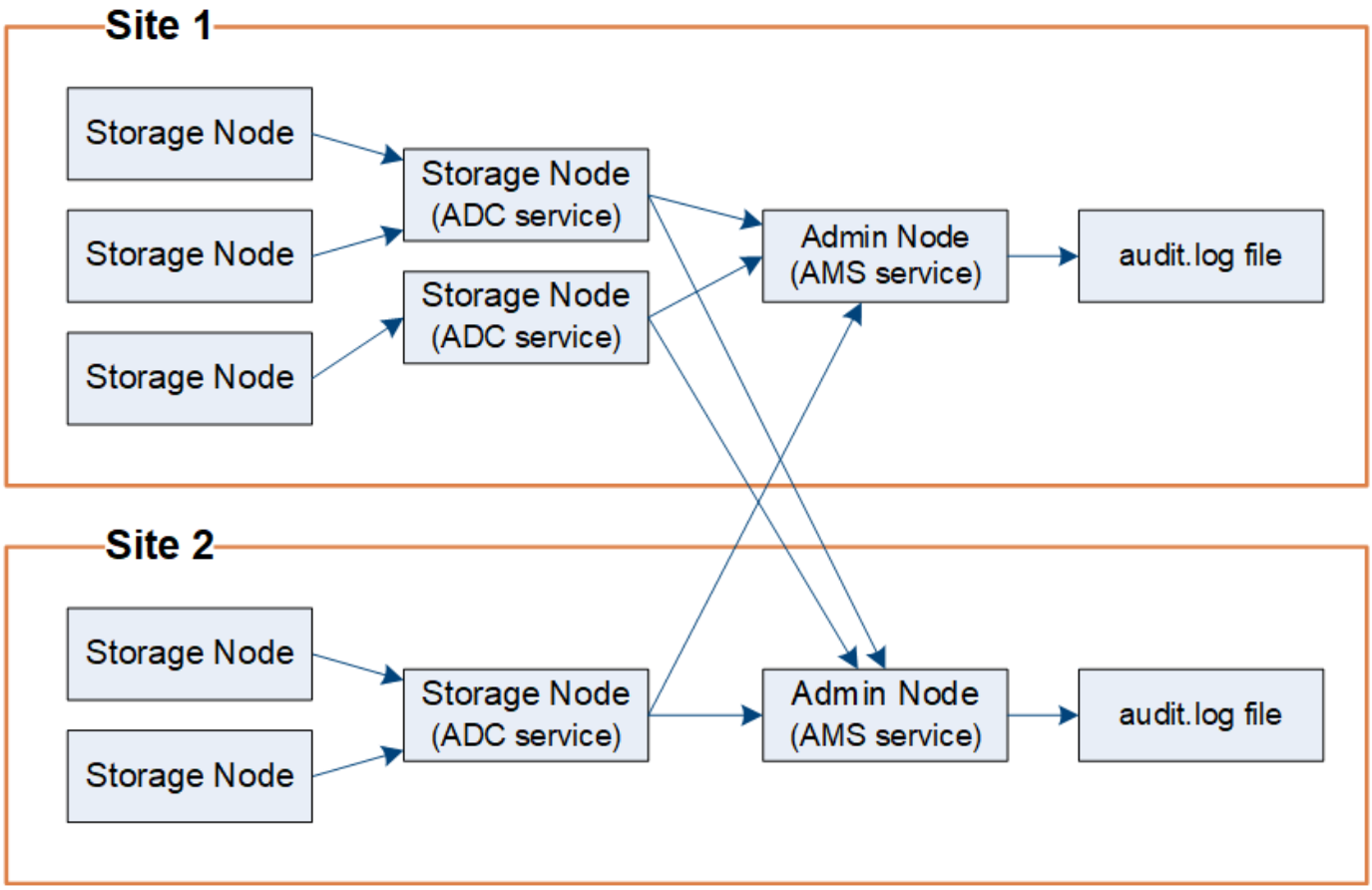
감사 메시지 흐름

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.

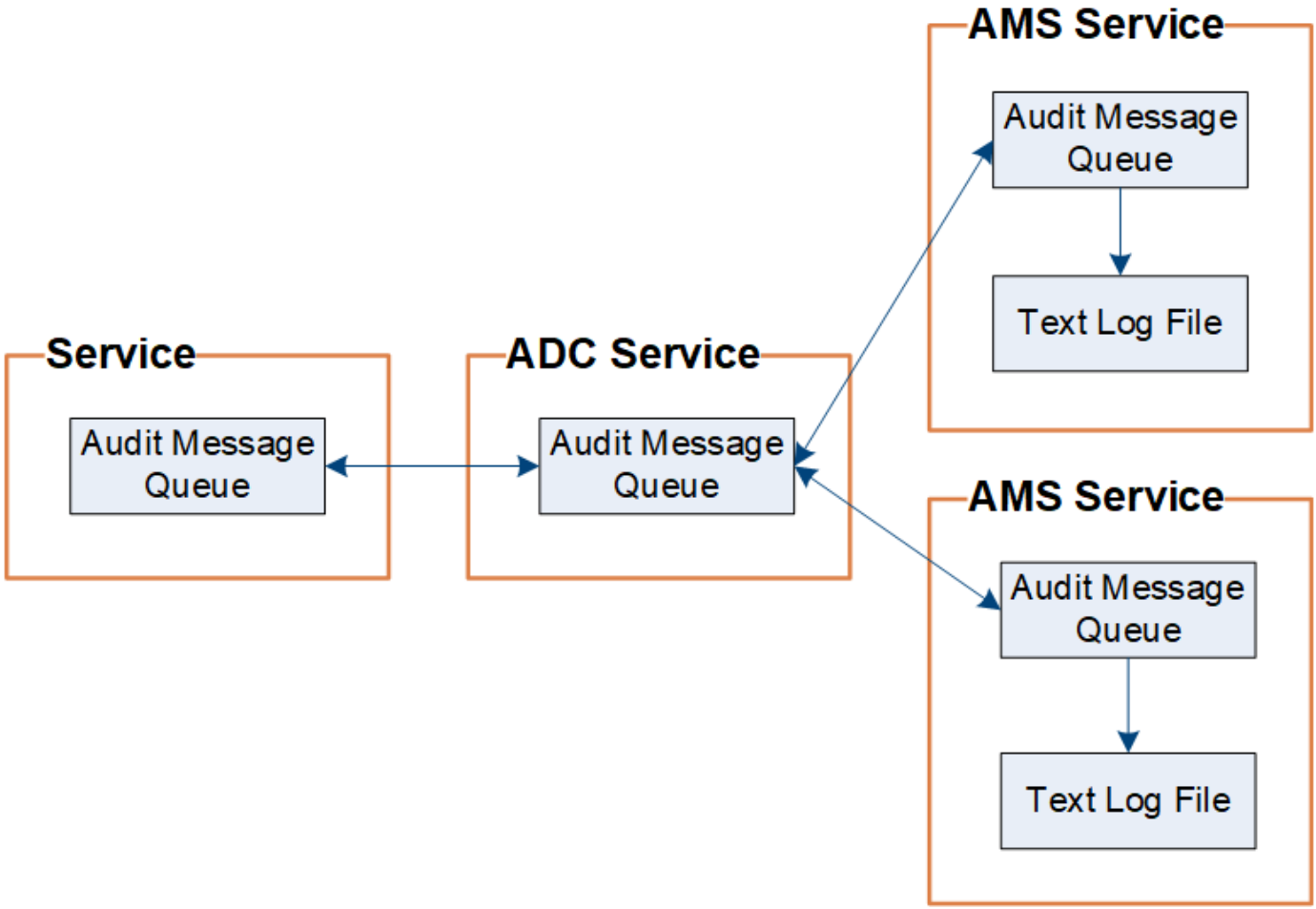
각 관리 노드는 감사 메시지를 텍스트 로그 파일에 저장합니다. 활성 로그 파일의 이름은 입니다 `audit.log`.



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. 메시지가 관리자 노드의 감사 로그 파일에 기록될 때까지 메시지 복사본은 항상 감사 메시지 큐에 유지됩니다 `/var/local/audit/export` 디렉토리. 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 증가하면 각 노드의 사용 가능한 공간을 더 많이 사용합니다 `/var/local/` 디렉토리. 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.

- 를 누릅니다 `/var/local/audit/export` 관리 노드에서 사용하는 디렉토리가 가득 차면 디렉토리가 더 이상 가득 차지 않을 때까지 관리 노드가 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.
- 를 누릅니다 `/var/local/` ADC 서비스가 있는 스토리지 노드에서 사용하는 디렉토리가 92% 가득 차면 디렉토리가 87%만 채워질 때까지 노드가 메시지를 감사할 수 없는 것으로 플래그 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 로컬에 저장합니다.

- 를 누릅니다 `/var/local/` 스토리지 노드에서 사용하는 디렉토리가 85% 차면 노드에서 로 S3 및 Swift 클라이언트 요청을 거절하기 시작합니다 `503 Service Unavailable`.

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.
- 를 클릭합니다 `/var/local/` 감사 메시지와 무관한 이유로 ADC 스토리지 노드의 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 수준 변경"있습니다."

중복된 메시지

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

감사 메시지 수준 변경

감사 수준을 조정하여 각 감사 메시지 범주에 대해 감사 로그에 기록된 감사 메시지 수를 늘리거나 줄일 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

감사 로그에 기록된 감사 메시지는 * 구성 * > * 모니터링 * > * 감사 * 페이지의 설정에 따라 필터링됩니다.

다음과 같은 각 메시지 범주에 대해 서로 다른 감사 수준을 설정할 수 있습니다.

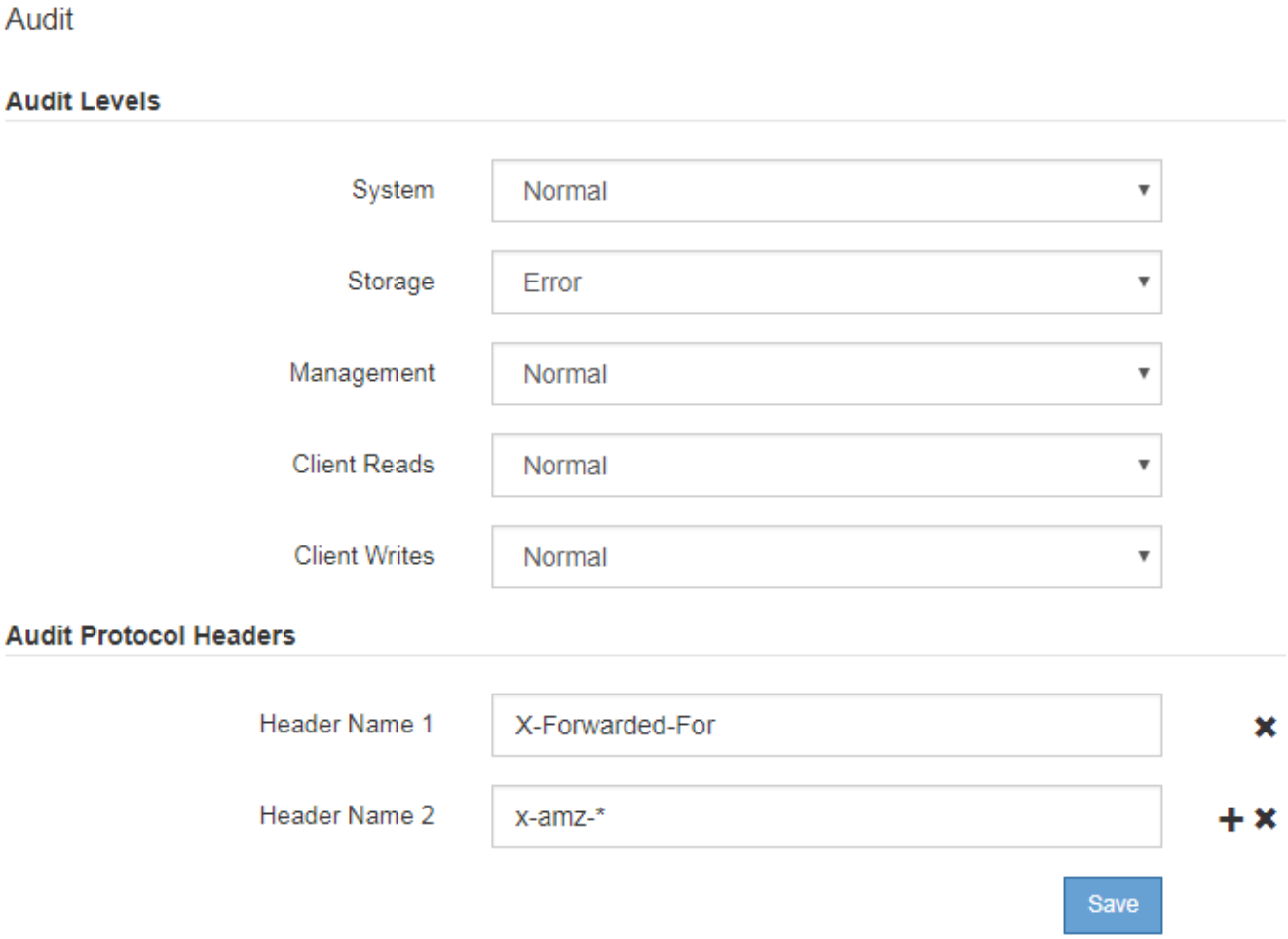
- * 시스템 *: 기본적으로 이 수준은 보통으로 설정됩니다.
- * 스토리지 *: 기본적으로 이 수준은 오류 로 설정됩니다.
- * 관리 *: 기본적으로 이 수준은 보통으로 설정됩니다.
- * 클라이언트 읽기 *: 기본적으로 이 수준은 보통으로 설정됩니다.
- * 클라이언트 쓰기 *: 기본적으로 이 수준은 보통으로 설정됩니다.

이 기본값은 버전 10.3 이상을 사용하여 StorageGRID를 처음 설치한 경우에 적용됩니다. 이전 버전의 StorageGRID에서 업그레이드한 경우 모든 범주의 기본값은 보통으로 설정됩니다.

업그레이드 중에는 감사 수준 구성이 즉시 적용되지 않습니다.

단계

1. 구성 * > * 모니터링 * > * 감사 * 를 선택합니다.



2. 각 감사 메시지 범주에 대해 드롭다운 목록에서 감사 수준을 선택합니다.

감사 수준	설명
꺼짐	범주의 감사 메시지가 기록되지 않습니다.
오류	오류 메시지만 기록됩니다. 결과 코드가 "성공"하지 않은 감사 메시지입니다(SUCS).
정상	표준 트랜잭션 메시지가 기록됩니다. — 범주에 대한 이 지침에 나열된 메시지입니다.
디버그	사용되지 않음. 이 수준은 일반 감사 수준과 동일하게 작동합니다.

특정 수준에 포함되는 메시지에는 더 높은 수준으로 기록되는 메시지가 포함됩니다. 예를 들어 일반 수준에는 모든

오류 메시지가 포함됩니다.

3. 감사 프로토콜 헤더 * 에서 클라이언트 읽기 및 클라이언트 쓰기 감사 메시지에 포함할 HTTP 요청 헤더의 이름을 입력합니다. 별표(\ *)를 와일드카드로 사용하거나 이스케이프 시퀀스(\ *)를 리터럴 별표로 사용합니다. 더하기 기호를 클릭하여 머리글 이름 필드 목록을 만듭니다.

   감사 프로토콜 헤더는 S3 및 Swift 요청에만 적용됩니다.

   이러한 HTTP 헤더가 요청에서 검색되면 HTRH 필드 아래의 감사 메시지에 포함됩니다.

   감사 프로토콜 요청 헤더는 * 클라이언트 읽기 * 또는 * 클라이언트 쓰기 * 에 대한 감사 수준이 * 꺼짐 * 이 아닌 경우에만 기록됩니다.

4. 저장 * 을 클릭합니다.

관련 정보

"시스템 감사 메시지"

"오브젝트 스토리지 감사 메시지"

"관리 감사 메시지입니다"

"클라이언트가 감사 메시지를 읽습니다"

"StorageGRID 관리"

감사 로그 파일에 액세스 중입니다

감사 공유에 활성 이 포함되어 있습니다 `audit.log` 파일 및 압축된 감사 로그 파일 감사 로그에 쉽게 액세스할 수 있도록 NFS 및 CIFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다(더 이상 사용 안 함). 관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수도 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 에 가 있어야 합니다 `Passwords.txt` 파일.
- 관리 노드의 IP 주소를 알아야 합니다.

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
2. 감사 로그 파일이 포함된 디렉토리로 이동합니다.

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

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

관련 정보

"StorageGRID 관리"

로그 파일 회전을 감사합니다

감사 로그 파일은 관리 노드의 에 저장됩니다 `/var/local/audit/export` 디렉토리. 활성 감사 로그 파일의 이름은 입니다 `audit.log`.

하루에 한 번, 활동입니다 `audit.log` 파일이 저장되고 새 파일이 저장됩니다 `audit.log` 파일이 시작되었습니다. 저장된 파일의 이름은 저장 시기를 형식으로 나타냅니다 *`yyyy-mm-dd.txt`*. 하루에 둘 이상의 감사 로그가 생성되는 경우 파일 이름에 숫자가 추가된 형식으로 파일이 저장된 날짜가 사용됩니다 *`yyyy-mm-dd.txt.n`*. 예를 들면, 다음과 같습니다. `2018-04-15.txt` 및 `2018-04-15.txt.1` 는 2018년 4월 15일에 생성 및 저장된 첫 번째 및 두 번째 로그 파일입니다.

하루 후에는 저장된 파일이 압축되고 이름이 파일 형식으로 변경됩니다 *`yyyy-mm-dd.txt.gz`*`원래 날짜를 유지합니다. 시간이 지남에 따라 이로 인해 관리 노드의 감사 로그에 할당된 스토리지가 소비됩니다. 스크립트는 감사 로그 공간 소비를 모니터링하고 에서 공간을 확보하기 위해 필요한 경우 로그 파일을 삭제합니다 `/var/local/audit/export` 디렉토리. 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 예제에서는 활성 을 보여 줍니다 `audit.log` 파일, 이전 날짜의 파일입니다 (`2018-04-15.txt`), 및 이전 날짜의 압축 파일 (`2018-04-14.txt.gz`)를 클릭합니다.

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