로그 관리 및 외부 **syslog** 서버 구성

StorageGRID software

NetApp
July 23, 2026

목차

로그 관리 및 외부 **syslog** 서버 구성

StorageGRID의 외부 **syslog** 서버

외부 syslog 서버는 StorageGRID 외부에 있는 서버로, 시스템 감사 정보를 한 곳에 수집하는 데 사용할 수 있습니다. 외부 syslog 서버를 사용하면 관리 노드의 네트워크 트래픽을 줄이고 정보를 더욱 효율적으로 관리할 수 있습니다. StorageGRID의 경우 발신 syslog 메시지 패킷 형식은 RFC 3164를 준수합니다.

외부 syslog 서버로 전송할 수 있는 감사 정보 유형은 다음과 같습니다.

- 정상 시스템 작동 중에 생성된 감사 메시지가 포함된 감사 로그
- 로그인 및 루트 권한 획득과 같은 보안 관련 이벤트
- 발생한 문제를 해결하기 위해 지원 사례를 개설해야 하는 경우 요청될 수 있는 애플리케이션 로그입니다.

외부 **syslog** 서버를 사용해야 하는 시점

대규모 그리드 환경을 구축했거나, 여러 유형의 S3 애플리케이션을 사용했거나, 모든 감사 데이터를 보존하려는 경우 외부 syslog 서버가 특히 유용합니다. 감사 정보를 외부 syslog 서버로 전송하면 다음과 같은 이점을 얻을 수 있습니다.

- 감사 메시지, 애플리케이션 로그, 보안 이벤트 등의 감사 정보를 보다 효율적으로 수집하고 관리합니다.
- 감사 정보가 관리 노드를 거치지 않고 다양한 스토리지 노드에서 외부 syslog 서버로 직접 전송되므로 관리 노드의 네트워크 트래픽이 줄어듭니다.

> 로그를 외부 syslog 서버로 전송할 때, 8,192바이트를 초과하는 단일 로그는 외부 syslog 서버 구현의 일반적인 제한 사항을 준수하기 위해 메시지 끝부분이 잘립니다.

> 외부 syslog 서버 장애 발생 시 전체 데이터 복구 옵션을 극대화하기 위해 각 노드에 최대 20GB의 감사 기록 로컬 로그(`localaudit.log`)가 유지됩니다.

외부 **syslog** 서버를 구성하는 방법

외부 syslog 서버를 구성하는 방법을 알아보려면 "로그 관리 및 외부 syslog 서버 구성"을 참조하십시오.

TLS 또는 RELP/TLS 프로토콜을 사용하도록 구성하려면 다음 인증서가 필요합니다.

- 서버 **CA** 인증서: 외부 syslog 서버를 확인하기 위한 하나 이상의 신뢰할 수 있는 CA 인증서(PEM 인코딩). 생략하면 기본 Grid CA 인증서가 사용됩니다.
- 클라이언트 인증서: 외부 syslog 서버에 대한 인증에 사용되는 클라이언트 인증서(PEM 인코딩).
- 클라이언트 개인 키: PEM 인코딩 형식의 클라이언트 인증서용 개인 키입니다.

> 클라이언트 인증서를 사용하는 경우 클라이언트 개인 키도 함께 사용해야 합니다. 암호화된 개인 키를 제공하는 경우 암호도 함께 제공해야 합니다. 암호화된 개인 키를 사용한다고 해서 보안상 큰 이점이 있는 것은 아닙니다. 키와 암호를 저장해야 하기 때문입니다. 따라서 간편함을 위해 가능하다면 암호화되지 않은 개인 키를 사용하는 것이 좋습니다.

외부 **syslog** 서버의 크기를 추정하는 방법

일반적으로 그리드는 초당 S3 작업 수 또는 초당 바이트 수로 정의되는 필요한 처리량을 달성하도록 크기가 조정됩니다. 예를 들어, 그리드가 초당 1,000건의 S3 작업을 처리하거나 초당 2,000MB의 객체 수집 및 검색을 처리해야 하는 요구 사항이 있을 수 있습니다. 외부 syslog 서버는 그리드의 데이터 요구 사항에 따라 크기를 조정해야 합니다.

이 섹션에서는 외부 syslog 서버가 처리해야 하는 다양한 유형의 로그 메시지 속도와 평균 크기를 추정하는 데 도움이 되는 몇 가지 경험적 공식을 제공합니다. 이러한 공식은 그리드의 알려진 또는 원하는 성능 특성(초당 S3 작업 수)을 기준으로 표현됩니다.

추정 공식에 초당 **S3** 연산 횟수를 사용하십시오**.**

그리드 크기가 초당 바이트 단위로 표시된 처리량을 기준으로 설계된 경우, 추정 공식을 사용하려면 이 크기를 초당 S3 작업 수로 변환해야 합니다. 그리드 처리량을 변환하려면 먼저 평균 객체 크기를 확인해야 합니다. 이는 기존 감사 로그 및 메트릭(있는 경우)의 정보를 사용하거나 StorageGRID를 사용할 애플리케이션에 대한 지식을 활용하여 확인할 수 있습니다. 예를 들어, 그리드 크기가 초당 2,000MB의 처리량을 달성하도록 설계되었고 평균 객체 크기가 2MB인 경우, 그리드는 초당 1,000건의 S3 작업(2,000MB / 2MB)을 처리할 수 있도록 설계된 것입니다.

> ⓘ 다음 섹션에 제시된 외부 syslog 서버 크기 조정 공식은 최악의 경우가 아닌 일반적인 경우에 대한 추정치입니다. 구성 및 워크로드에 따라 syslog 메시지 발생 빈도 또는 syslog 데이터 양이 공식 예측치보다 높거나 낮을 수 있습니다. 따라서 이 공식은 지침으로만 사용해야 합니다.

감사 로그 추정 공식

그리드에서 지원할 것으로 예상되는 초당 S3 작업 수 외에 S3 워크로드에 대한 정보가 없는 경우, 감사 수준을 기본값(저장소 범주를 제외한 모든 범주를 보통으로 설정하고 저장소 범주만 오류로 설정)으로 유지한다는 가정 하에 다음 공식을 사용하여 외부 syslog 서버에서 처리해야 하는 감사 로그 볼륨을 추정할 수 있습니다.

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

예를 들어, 그리드가 초당 1,000건의 S3 작업을 처리하도록 설계된 경우, 외부 syslog 서버는 초당 2,000건의 syslog 메시지를 지원할 수 있도록 설계되어야 하며, 초당 1.6MB의 속도로 감사 로그 데이터를 수신(및 일반적으로 저장)할 수 있어야 합니다.

워크로드에 대해 더 자세히 알고 있다면 더 정확한 예측이 가능합니다. 감사 로그의 경우 가장 중요한 추가 변수는 S3 작업 중 PUT 작업의 비율(GET 작업 대비)과 다음 S3 필드의 평균 크기(바이트)입니다(표에 사용된 4자리 약어는 감사 로그 필드 이름입니다).

코드	필드	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청의 경우 비어 있습니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 계정 간 액세스 또는 익명 액세스를 식별하는 데 사용됩니다.

코드	필드	설명
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름입니다. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.

S3 작업 중 PUT 작업의 비율을 P로 나타내겠습니다. 여기서 P는 0 ≤ P ≤ 1입니다(즉, PUT 작업이 100%인 경우 P = 1이고, GET 작업이 100%인 경우 P = 0입니다).

S3 계정 이름, S3 버킷, S3 키의 합계 평균 크기를 K라고 하겠습니다. S3 계정 이름은 항상 my-s3-account(13바이트)이고, 버킷 이름은 /my/application/bucket-12345(28바이트)처럼 고정 길이이며, 객체 키는 5733a5d7-f069-41ef-8fbd-13247494c69c(36바이트)처럼 고정 길이라고 가정해 보겠습니다. 그러면 K의 값은 90(13+13+28+36)이 됩니다.

P와 K 값을 결정할 수 있다면, 감사 수준을 기본값(Storage 범주를 제외한 모든 범주를 Normal로 설정하고 Storage 범주만 Error로 설정)으로 유지한다는 가정 하에 다음 공식을 사용하여 외부 syslog 서버에서 처리해야 할 감사 로그의 양을 추정할 수 있습니다.

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

예를 들어, 그리드 크기가 초당 1,000건의 S3 작업 처리에 맞춰져 있고, 워크로드의 50%가 PUT 작업이며, S3 계정 이름, 버킷 이름, 객체 이름의 평균 크기가 90바이트인 경우, 외부 syslog 서버는 초당 1,500건의 syslog 메시지를 처리할 수 있도록 크기를 조정해야 하며, 초당 약 1MB의 속도로 감사 로그 데이터를 수신(및 일반적으로 저장)할 수 있어야 합니다.

비기본 감사 수준에 대한 추정 공식

제공된 감사 로그 계산 공식은 기본 감사 수준 설정(저장소 범주를 제외한 모든 범주가 '일반'으로 설정되고 저장소 범주는 '오류'로 설정됨)을 기준으로 합니다. 기본값이 아닌 감사 수준 설정에 대한 감사 메시지 발생률 및 평균 크기를 추정하는 자세한 공식은 제공되지 않습니다. 그러나 다음 표를 사용하여 대략적인 발생률을 추정할 수 있습니다. 감사 로그에 제공된 평균 크기 공식을 사용할 수도 있지만, '추가' 감사 메시지는 평균적으로 기본 감사 메시지보다 크기가 작기 때문에 실제보다 과대평가될 가능성이 높다는 점에 유의하시기 바랍니다.

상태	공식
복제: 감사 수준이 모두 디버그 또는 보통으로 설정되어 있습니다.	감사 로그 전송률 = 8 x S3 운영률
Erasure coding: 감사 수준이 모두 디버그 또는 일반으로 설정됨	기본 설정과 동일한 공식을 사용합니다

보안 이벤트 예측 공식

보안 이벤트는 S3 작업과 상관관계가 없으며 일반적으로 로그 및 데이터 양이 매우 적습니다. 따라서 추정 공식은 제공되지 않습니다.

애플리케이션 로그 추정 공식

그리드에서 지원할 것으로 예상되는 초당 S3 작업 수 외에 S3 워크로드에 대한 정보가 없는 경우 다음 공식을 사용하여 외부 syslog 서버에서 처리해야 하는 애플리케이션 로그 볼륨을 추정할 수 있습니다.

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

예를 들어, 그리드가 초당 1,000건의 S3 작업을 처리하도록 설계된 경우, 외부 syslog 서버는 초당 3,300건의 애플리케이션 로그를 지원하고 초당 약 1.2MB의 속도로 애플리케이션 로그 데이터를 수신(및 저장)할 수 있도록 설계되어야 합니다.

워크로드에 대해 더 자세히 알면 더 정확한 예측이 가능합니다. 애플리케이션 로그의 경우 가장 중요한 추가 변수는 데이터 보호 전략(복제 vs. 소거 코딩), S3 작업 중 PUT 작업 비율(GET/기타 작업 대비), 그리고 다음 S3 필드의 평균 크기(바이트)입니다(표에 사용된 4자리 약어는 감사 로그 필드 이름입니다).

코드	필드	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청의 경우 비어 있습니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 계정 간 액세스 또는 익명 액세스를 식별하는 데 사용됩니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름입니다. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.

예시 크기 추정

이 섹션에서는 다음과 같은 데이터 보호 방법을 사용하는 그리드에 대한 추정 공식 사용 사례를 설명합니다.

- 복제
- 소거 코딩

데이터 보호를 위해 복제를 사용하는 경우

P는 S3 작업 중 PUT 작업의 비율을 나타내며, 0 ≤ P ≤ 1입니다(즉, PUT 작업량이 100%인 경우 P = 1이고, GET 작업량이 100%인 경우 P = 0입니다).

K를 S3 계정 이름, S3 버킷, S3 키의 합의 평균 크기라고 합시다. S3 계정 이름은 항상 my-s3-account(13바이트)이고, 버킷 이름은 /my/application/bucket-12345(28바이트)와 같이 고정 길이이며, 객체 키는 5733a5d7-f069-41ef-8fbd-13247494c69c(36바이트)와 같이 고정 길이라고 가정합니다. 그러면 K의 값은 90(13+13+28+36)입니다.

P와 K 값을 결정할 수 있다면 다음 공식을 사용하여 외부 syslog 서버가 처리해야 하는 애플리케이션 로그의 양을 추정할 수 있습니다.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x K))) Bytes
```

예를 들어, 그리드 크기가 초당 1,000건의 S3 작업 처리에 맞춰져 있고, 워크로드의 50%가 PUT 작업이며, S3 계정 이름, 버킷 이름, 객체 이름의 평균 크기가 90바이트라면, 외부 syslog 서버는 초당 1,800건의 애플리케이션 로그를 처리할 수 있도록 크기를 조정해야 하며, 초당 0.5MB의 속도로 애플리케이션 데이터를 수신(및 저장)하게 됩니다.

데이터 보호를 위해 소거 코딩을 사용하는 경우

P는 S3 작업 중 PUT 작업의 비율을 나타내며, 0 ≤ P ≤ 1입니다(즉, PUT 작업량이 100%인 경우 P = 1이고, GET 작업량이 100%인 경우 P = 0입니다).

K를 S3 계정 이름, S3 버킷, S3 키의 합의 평균 크기라고 합시다. S3 계정 이름은 항상 my-s3-account(13바이트)이고, 버킷 이름은 /my/application/bucket-12345(28바이트)와 같이 고정 길이이며, 객체 키는 5733a5d7-f069-41ef-8fbd-13247494c69c(36바이트)와 같이 고정 길이라고 가정합니다. 그러면 K의 값은 90(13+13+28+36)입니다.

P와 K 값을 결정할 수 있다면 다음 공식을 사용하여 외부 syslog 서버가 처리해야 하는 애플리케이션 로그의 양을 추정할 수 있습니다.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 + (0.9 x K))) Bytes
```

예를 들어, 그리드 크기가 초당 1,000건의 S3 작업 처리에 맞춰져 있고, 워크로드의 50%가 PUT 작업이며, S3 계정 이름, 버킷 이름, 객체 이름의 평균 크기가 90바이트라면, 외부 syslog 서버는 초당 2,250개의 애플리케이션 로그를 처리할 수 있도록 크기를 조정해야 하며, 초당 0.6MB의 속도로 애플리케이션 데이터를 수신(및 저장)할 수 있어야 합니다.

StorageGRID에서 로그 관리 구성

필요에 따라 감사 수준, 프로토콜 헤더, 감사 메시지 및 로그의 위치를 구성하십시오.

모든 StorageGRID 노드는 시스템 활동 및 이벤트를 추적하기 위해 감사 메시지와 로그를 생성합니다. 감사 메시지와 로그는 모니터링 및 문제 해결에 필수적인 도구입니다.

선택적으로 "외부 syslog 서버 구성"감사 정보를 원격으로 저장할 수 있습니다. 외부 서버를 사용하면 감사 데이터의 완전성을 유지하면서 감사 메시지 로깅으로 인한 성능 영향을 최소화할 수 있습니다. 외부 syslog 서버는 대규모 그리드 환경을 구축했거나, 여러 유형의 S3 애플리케이션을 사용하거나, 모든 감사 데이터를 보존하려는 경우에 특히 유용합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "유지 관리 또는 루트 액세스 권한"

- 외부 syslog 서버를 구성할 계획이라면, "외부 syslog 서버 사용 시 고려 사항"을 검토하고 따라야 합니다.
- TLS 또는 RELP/TLS 프로토콜을 사용하여 외부 syslog 서버를 구성하려면 필요한 서버 CA 및 클라이언트 인증서와 클라이언트 개인 키가 있어야 합니다.

감사 메시지 수준 변경

감사 로그의 다음 각 메시지 범주에 대해 서로 다른 감사 수준을 설정할 수 있습니다.

감사 범주	기본 설정	추가 정보
시스템	정상	"시스템 감사 메시지"
스토리지	오류	"객체 저장소 감사 메시지"
관리	정상	"관리 감사 메시지"
클라이언트 읽기	정상	"클라이언트 읽기 감사 메시지"
클라이언트 쓰기	정상	"클라이언트 쓰기 감사 메시지"
ILM	정상	"ILM 감사 메시지"
교차 그리드 복제	오류	"CGRR: 그리드 간 복제 요청"

업그레이드 중에는 감사 수준 구성이 즉시 적용되지 않습니다.

단계

1. * 구성 * > * 모니터링 * > * 로그 관리 * 를 선택합니다.
2. 각 감사 메시지 범주에 대해 드롭다운 목록에서 감사 수준을 선택하십시오.

감사 수준	설명
끄기	해당 범주의 감사 메시지는 기록되지 않습니다.
오류	오류 메시지만 기록됩니다. 즉, 결과 코드가 "성공"(SUCS)이 아닌 감사 메시지만 기록됩니다.
정상	일반적인 거래 메시지는 로그에 기록됩니다. 이러한 메시지는 해당 범주에 대해 이 지침에 나열된 메시지입니다.
디버그	더 이상 사용되지 않습니다. 이 수준은 일반 감사 수준과 동일하게 작동합니다.

특정 레벨에 포함되는 메시지는 상위 레벨에 기록되는 메시지들을 모두 포함합니다. 예를 들어, 일반 레벨에는 모든 오류 메시지가 포함됩니다.

S3 애플리케이션의 클라이언트 읽기 작업에 대한 자세한 기록이 필요하지 않은 경우, 선택적으로 클라이언트 읽기 설정을 *오류*로 변경하여 감사 로그에 기록되는 감사 메시지 수를 줄일 수 있습니다.

3. *저장*을 선택하세요.

HTTP 요청 헤더 정의

클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 선택적으로 정의할 수 있습니다.

단계

1. 감사 프로토콜 헤더 섹션에서 클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 정의합니다.

   별표(*)를 와일드카드로 사용하여 0개 이상의 문자와 일치시킬 수 있습니다. 이스케이프 시퀀스(*)를 사용하여 문자 그대로의 별표와 일치시킬 수 있습니다.

2. 필요한 경우 *다른 헤더 추가*를 선택하여 추가 헤더를 생성합니다.

   요청에서 HTTP 헤더가 발견되면 해당 헤더는 감사 메시지의 HTRH 필드에 포함됩니다.

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

3. *저장*을 선택합니다

로그 위치 구성

기본적으로 감사 메시지와 로그는 생성된 노드에 저장됩니다. 과도한 디스크 공간을 사용하지 않도록 주기적으로 교체되고 결국 삭제됩니다. 감사 메시지와 로그의 일부를 외부에 저장하려면 외부 syslog 서버 사용.

로그 파일을 내부적으로 저장하려면 로그 저장소용 테넌트와 버킷을 선택하고 로그 아카이빙을 활성화하세요.

외부 syslog 서버 사용

선택적으로 외부 syslog 서버를 구성하여 감사 로그, 애플리케이션 로그 및 보안 이벤트 로그를 그리드 외부 위치에 저장할 수 있습니다.

외부 syslog 서버를 사용하지 않으려면 이 단계를 건너뛰고 로그 위치 선택으로 이동하세요.

이 절차에서 제공되는 구성 옵션이 요구 사항을 충족할 만큼 유연하지 않은 경우, `audit-destinations` 엔드포인트를 사용하여 추가 구성 옵션을 적용할 수 있습니다. 이 엔드포인트는 "그리드 관리 API"의 비공개 API 섹션에 있습니다. 예를 들어, 노드 그룹별로 다른 syslog 서버를 사용하려면 해당 API를 사용할 수 있습니다.

syslog 정보 입력

외부 syslog 서버 구성 마법사에 액세스하여 StorageGRID가 외부 syslog 서버에 액세스하는 데 필요한 정보를 제공하십시오.

단계

1. 로컬 노드 및 외부 서버 탭에서 *외부 syslog 서버 구성*을 선택합니다. 또는 이전에 외부 syslog 서버를 구성한 경우 *외부 syslog 서버 편집*을 선택합니다.

   외부 syslog 서버 구성 마법사가 나타납니다.

2. 마법사의 **syslog** 정보 입력 단계에서 호스트 필드에 외부 syslog 서버에 대한 유효한 정규화된 도메인 이름 또는 IPv4 또는 IPv6 주소를 입력하십시오.
3. 외부 syslog 서버의 대상 포트를 입력하십시오(1에서 65535 사이의 정수여야 함). 기본 포트는 514입니다.
4. 외부 syslog 서버로 감사 정보를 전송하는 데 사용되는 프로토콜을 선택하십시오.

   TLS 또는 **RELP/TLS** 사용을 권장합니다. 이러한 옵션을 사용하려면 서버 인증서를 업로드해야 합니다. 인증서를 사용하면 그리드와 외부 syslog 서버 간의 연결을 안전하게 보호할 수 있습니다. 자세한 내용은 "보안 인증서 관리"을 참조하십시오.

   모든 프로토콜 옵션은 외부 syslog 서버의 지원 및 구성이 필요합니다. 외부 syslog 서버와 호환되는 옵션을 선택해야 합니다.

   > ⓘ 신뢰할 수 있는 이벤트 로깅 프로토콜(RELP)은 syslog 프로토콜의 기능을 확장하여 이벤트 메시지를 안정적으로 전달합니다. RELP를 사용하면 외부 syslog 서버가 재시작될 경우 감사 정보 손실을 방지할 수 있습니다.

5. *Continue*를 선택합니다.
6. **TLS** 또는 *RELP/TLS*를 선택한 경우 서버 CA 인증서, 클라이언트 인증서 및 클라이언트 개인 키를 업로드하십시오.
   a. 사용할 인증서 또는 키에 대해 *찾아보기*를 선택합니다.
   b. 인증서 또는 키 파일을 선택하십시오.
   c. 파일을 업로드하려면 *열기*를 선택합니다.

      인증서 또는 키 파일 이름 옆에 녹색 체크 표시가 나타나면 업로드가 성공적으로 완료된 것입니다.

7. *Continue*를 선택합니다.

syslog 콘텐츠 관리

외부 syslog 서버로 전송할 정보를 선택할 수 있습니다.

단계

1. 마법사의 **syslog** 콘텐츠 관리 단계에서 외부 syslog 서버로 전송할 각 감사 정보 유형을 선택하십시오.
   - 감사 로그 전송: StorageGRID 이벤트 및 시스템 활동을 전송합니다.
   - 보안 이벤트 전송: 권한이 없는 사용자가 로그인을 시도하거나 사용자가 루트 권한으로 로그인하는 등의 보안 이벤트를 전송합니다.
   - 애플리케이션 로그 전송: 문제 해결에 유용한 "StorageGRID 소프트웨어 로그 파일"을 전송합니다. 여기에는 다음이 포함됩니다.
     - `bycast-err.log`
     - `bycast.log`

- `jaeger.log`
- `nms.log` (관리자 노드 전용)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

◦ 액세스 로그 전송: Grid Manager, Tenant Manager, 구성된 로드 밸런서 엔드포인트 및 원격 시스템의 그리드 페더레이션 요청에 대한 외부 요청의 HTTP 액세스 로그를 전송합니다.

2. 드롭다운 메뉴를 사용하여 전송하려는 각 감사 정보 범주에 대한 심각도와 기능(메시지 유형)을 선택하십시오.

   심각도 및 시설 값을 설정하면 로그를 사용자 지정 방식으로 집계하여 분석을 더 쉽게 할 수 있습니다.

   a. *심각도*의 경우 *통과*를 선택하거나 0에서 7 사이의 심각도 값을 선택하십시오.

      값을 선택하면 선택한 값이 해당 유형의 모든 메시지에 적용됩니다. 심각도 값을 고정된 값으로 재정의하면 심각도별 정보가 손실됩니다.

심각성	설명
패스스루	외부 시스템 로그로 전송되는 각 메시지는 해당 노드에 로컬로 기록될 때와 동일한 심각도 값을 갖습니다. • 감사 로그의 경우 심각도는 "info"입니다. • 보안 이벤트의 경우 심각도 값은 노드의 Linux 배포판에서 생성됩니다. • 애플리케이션 로그의 경우, 심각도 등급은 문제 유형에 따라 "info"에서 "notice"까지 다양합니다. 예를 들어, NTP 서버를 추가하고 HA 그룹을 구성하는 경우에는 "info" 등급이 부여되는 반면, SSM 또는 RSM 서비스를 의도적으로 중지하는 경우에는 "notice" 등급이 부여됩니다. • 액세스 로그의 경우 심각도는 "info"입니다.
0	긴급 상황: 시스템을 사용할 수 없습니다
1	경고: 즉시 조치를 취해야 합니다
2	위급: 위급한 상황
3	오류: 오류 조건
4	경고: 경고 상황
5	주의: 일반적이지만 중요한 상태입니다
6	정보성: 정보성 메시지

심각성	설명
7	디버그: 디버그 수준 메시지

b. *Facilty*의 경우 *Passthrough*를 선택하거나 0에서 23 사이의 시설 값을 선택하십시오.

값을 선택하면 해당 유형의 모든 메시지에 적용됩니다. 시설 정보를 고정 값으로 덮어쓰면 각 시설에 대한 정보가 손실됩니다.

시설	설명
패스스루	외부 syslog로 전송되는 각 메시지는 해당 메시지가 노드에 로컬로 기록될 때와 동일한 facility 값을 갖습니다. • 감사 로그의 경우 외부 syslog 서버로 전송되는 시설은 "local7"입니다. • 보안 이벤트의 경우, 시설 값은 노드의 Linux 배포판에서 생성됩니다. • 애플리케이션 로그의 경우, 외부 syslog 서버로 전송되는 애플리케이션 로그에는 다음과 같은 facility 값이 있습니다. ◦ `bycast.log`: 사용자 또는 데몬 ◦ `bycast-err.log`: 사용자, 데몬, local3 또는 local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • 액세스 로그의 경우 외부 syslog 서버로 전송되는 시설은 "local0."입니다.
0	kern(커널 메시지)
1	사용자(사용자 수준 메시지)
2	메일
3	데몬(시스템 데몬)
4	인증(보안/권한 부여 메시지)
5	syslog(syslogd에서 내부적으로 생성되는 메시지)
6	lpr (라인 프린터 서브시스템)
7	뉴스 (네트워크 뉴스 하위 시스템)

시설	설명
8	UUCP
9	cron(클록 데몬)
10	보안 (보안/인증 메시지)
11	FTP
12	NTP
13	logaudit(log audit)
14	logalert (로그 알림)
15	clock(클록 데몬)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. *Continue*를 선택합니다.

테스트 메시지 보내기

외부 syslog 서버를 사용하기 전에 그리드의 모든 노드가 외부 syslog 서버로 테스트 메시지를 전송하도록 요청해야 합니다. 이러한 테스트 메시지를 사용하여 외부 syslog 서버로 데이터를 전송하기 전에 전체 로그 수집 인프라를 검증해야 합니다.

그리드의 각 노드에서 외부 syslog 서버가 테스트 메시지를 수신하고 해당 메시지가 예상대로 처리되었는지 확인하기 전까지는 외부 syslog 서버 구성을 사용하지 마십시오.

단계

1. 외부 syslog 서버가 올바르게 구성되어 그리드의 모든 노드에서 감사 정보를 수신할 수 있다고 확신하여 테스트 메시지를 보내지 않으려면 *건너뛰고 완료*를 선택하십시오.

   녹색 배너는 구성이 저장되었음을 나타냅니다.

2. 그렇지 않으면 *테스트 메시지 보내기*를 선택합니다(권장).

   테스트 결과는 테스트를 중지할 때까지 페이지에 계속 표시됩니다. 테스트가 진행되는 동안 감사 메시지는 이전에 구성된 대상으로 계속 전송됩니다.

3. syslog 서버 구성 또는 실행 중에 오류가 발생하면 오류를 수정하고 *테스트 메시지 보내기*를 다시 선택하십시오.

   "외부 syslog 서버 문제 해결"을 참조하여 오류를 해결하십시오.

4. 모든 노드가 테스트를 통과했음을 나타내는 녹색 배너가 나타날 때까지 기다리십시오.
5. 테스트 메시지가 예상대로 수신 및 처리되는지 확인하려면 syslog 서버를 확인하십시오.

   UDP를 사용하고 있다면 전체 로그 수집 인프라를 점검하십시오. UDP 프로토콜은 다른 프로토콜만큼 엄격한 오류 감지 기능을 제공하지 않습니다.

6. *중지 후 완료*를 선택합니다.

   감사 및 **syslog** 서버 페이지로 돌아갑니다. 녹색 배너는 syslog 서버 구성이 저장되었음을 나타냅니다.

   StorageGRID 감사 정보는 외부 syslog 서버를 포함하는 대상을 선택하기 전까지는 외부 syslog 서버로 전송되지 않습니다.

로그 위치 선택

감사 로그, 보안 이벤트 로그, "StorageGRID 애플리케이션 로그" 및 액세스 로그가 전송될 위치를 지정할 수 있습니다.

StorageGRID 기본적으로 로컬 노드 감사 대상을 사용하며 감사 정보를 `/var/local/log/localaudit.log`에 저장합니다.

`/var/local/log/localaudit.log`를 사용할 때 Grid Manager 및 Tenant Manager 감사 로그 항목이 스토리지 노드로 전송될 수 있습니다. `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` 명령을 사용하여 가장 최근 항목이 있는 노드를 찾을 수 있습니다.

일부 대상은 외부 syslog 서버를 구성한 경우에만 사용할 수 있습니다.

단계

1. 로그 위치 > *로컬 노드 및 외부 서버*를 선택하십시오.
2. 로그 유형별 로그 위치를 변경하려면 다른 옵션을 선택하십시오.

일반적으로 *로컬 노드만 사용*하고 *외부 syslog 서버*를 사용하는 것이 더 나은 성능을 제공합니다.

옵션	설명
로컬 노드만(기본값)	감사 메시지, 보안 이벤트 로그 및 애플리케이션 로그는 관리 노드로 전송되지 않습니다. 대신, 이러한 로그는 해당 로그를 생성한 노드("로컬 노드")에만 저장됩니다. 각 로컬 노드에서 생성된 감사 정보는 `/var/local/log/localaudit.log`에 저장됩니다. 참고: StorageGRID는 공간 확보를 위해 주기적으로 로컬 로그를 순환 방식으로 삭제합니다. 노드의 로그 파일 크기가 1GB에 도달하면 기존 파일이 저장되고 새 로그 파일이 시작됩니다. 로그의 순환 제한은 21개 파일입니다. 22번째 버전의 로그 파일이 생성되면 가장 오래된 로그 파일이 삭제됩니다. 평균적으로 각 노드에는 약 20GB의 로그 데이터가 저장됩니다. 로그를 장기간 저장하려면 로그 스토리지에 테넌트 및 버킷 사용.
관리자 노드/로컬 노드	감사 메시지는 관리 노드의 감사 로그로 전송되며, 보안 이벤트 로그 및 애플리케이션 로그는 해당 메시지를 생성한 노드에 저장됩니다. 감사 정보는 다음 파일에 저장됩니다. • 관리자 노드(기본 및 보조 노드): `/var/local/audit/export/audit.log` • 모든 노드: 해당 `/var/local/log/localaudit.log` 파일은 일반적으로 비어 있거나 없습니다. 일부 메시지의 추가 복사본과 같은 보조 정보가 포함될 수 있습니다.
외부 syslog 서버	감사 정보는 외부 syslog 서버로 전송되어 로컬 노드에 저장됩니다 (`/var/local/log/localaudit.log`). 전송되는 정보의 유형은 외부 syslog 서버 구성 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성했습니다.을 완료한 후에만 활성화됩니다.
관리 노드 및 외부 syslog 서버	감사 메시지는 감사 로그 (`/var/local/audit/export/audit.log`)로 관리 노드에 전송되고, 감사 정보는 외부 syslog 서버로 전송되어 로컬 노드에 저장됩니다 (`/var/local/log/localaudit.log`). 전송되는 정보의 유형은 외부 syslog 서버 구성 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성했습니다.을 완료한 후에만 활성화됩니다.

3. *저장*을 선택하세요.

   경고 메시지가 나타납니다.

4. 감사 정보의 대상을 변경하려면 *확인*을 선택하십시오.

   새로운 로그는 사용자가 선택한 대상으로 전송됩니다. 기존 로그는 현재 위치에 그대로 유지됩니다.

버킷 사용

로그는 주기적으로 순환됩니다. 장기간 로그를 저장하려면 동일한 그리드 내의 S3 버킷을 사용하십시오.

1. 로그 위치 > *버킷 사용*을 선택합니다.
2. 보관 로그 활성화 확인란을 선택하십시오.
3. 표시된 테넌트와 버킷이 사용하려는 것이 아닌 경우 테넌트 및 버킷 변경*을 선택한 다음 *테넌트 및 버킷 생성 또는 *테넌트 및 버킷 선택*을 선택하십시오.

   테넌트 및 버킷 생성

   a. 새 테넌트 이름을 입력하세요.
   b. 새 테넌트의 암호를 입력하고 확인합니다.
   c. 새 버킷 이름을 입력합니다.
   d. *생성 및 활성화*를 선택합니다.

   테넌트 및 버킷 선택

   a. 드롭다운 메뉴에서 테넌트 이름을 선택합니다.
   b. 드롭다운 메뉴에서 버킷을 선택합니다.
   c. *선택 후 활성화*를 선택합니다.

4. *저장*을 선택하세요.

   로그는 사용자가 지정한 테넌트 및 버킷에 저장됩니다. 로그의 객체 키 이름은 다음 형식입니다.

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   예를 들면 다음과 같습니다.

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```