감사 메시지 및 로그 대상을 구성합니다

StorageGRID 11.8

NetApp
March 19, 2024

목차

감사 메시지 및 로그 대상을 구성합니다

외부 **syslog** 서버 사용 시 고려 사항

외부 syslog 서버는 단일 위치에서 시스템 감사 정보를 수집하는 데 사용할 수 있는 StorageGRID 외부의 서버입니다. 외부 syslog 서버를 사용하면 관리 노드의 네트워크 트래픽을 줄이고 정보를 보다 효율적으로 관리할 수 있습니다. StorageGRID의 경우 아웃바운드 syslog 메시지 패킷 형식은 RFC 3164와 호환됩니다.

외부 syslog 서버로 보낼 수 있는 감사 정보의 유형은 다음과 같습니다.

- 정상적인 시스템 작동 중에 생성된 감사 메시지를 포함하는 감사 로그
- 로그인 및 루트 에스컬레이션과 같은 보안 관련 이벤트입니다
- 발생한 문제를 해결하기 위해 지원 케이스를 열어야 하는 경우 요청될 수 있는 응용 프로그램 로그

외부 **syslog** 서버를 사용해야 하는 경우

외부 syslog 서버는 큰 그리드가 있거나 여러 유형의 S3 애플리케이션을 사용하거나 모든 감사 데이터를 보존하려는 경우에 특히 유용합니다. 감사 정보를 외부 syslog 서버로 전송하면 다음을 수행할 수 있습니다.

- 감사 메시지, 응용 프로그램 로그 및 보안 이벤트와 같은 감사 정보를 보다 효율적으로 수집하고 관리합니다.
- 관리자 노드를 거치지 않고도 감사 정보가 다양한 스토리지 노드에서 외부 syslog 서버로 직접 전송되므로 관리자 노드의 네트워크 트래픽이 감소합니다.

로그가 외부 syslog 서버로 전송되면 메시지가 끝날 때 8,192바이트보다 큰 단일 로그가 잘려서 외부 syslog 서버 구현의 일반적인 제한 사항을 준수합니다.

외부 syslog 서버에 장애가 발생할 경우 전체 데이터 복구에 대한 옵션을 최대화하기 위해 최대 20GB의 감사 레코드 로컬 로그 (`localaudit.log`각 노드에서 유지 관리됩니다.

외부 **syslog** 서버를 구성하는 방법

외부 syslog 서버를 구성하는 방법은 을 참조하십시오 "감사 메시지 및 외부 syslog 서버를 구성합니다".

TLS 또는 RELP/TLS 프로토콜 사용을 구성하려면 다음 인증서가 있어야 합니다.

- * 서버 CA 인증서 *: PEM 인코딩에서 외부 syslog 서버를 확인하기 위한 하나 이상의 신뢰할 수 있는 CA 인증서. 이 인수를 생략하면 기본 Grid CA 인증서가 사용됩니다.
- * 클라이언트 인증서 * : PEM 인코딩에서 외부 syslog 서버에 인증하기 위한 클라이언트 인증서입니다.
- * 클라이언트 개인 키 *: PEM 인코딩의 클라이언트 인증서에 대한 개인 키입니다.

클라이언트 인증서를 사용하는 경우 클라이언트 개인 키도 사용해야 합니다. 암호화된 개인 키를 제공하는 경우 암호문도 제공해야 합니다. 키와 암호를 저장해야 하므로 암호화된 개인 키를 사용하면 보안 상의 큰 이점이 없습니다. 사용 가능한 경우 암호화되지 않은 개인 키를 사용하는 것이 좋습니다.

외부 **syslog** 서버의 크기를 예측하는 방법

일반적으로, 그리드는 초당 S3 작업 또는 초당 바이트 수로 정의되는 필요한 처리량을 달성하도록 크기가 조정됩니다. 예를 들어, 그리드에서 1,000개의 초당 S3 작업, 즉 2,000개의 오브젝트 검색 및 검색을 처리해야 하는 요구사항이 있을 수 있습니다. 그리드의 데이터 요구 사항에 따라 외부 syslog 서버의 크기를 지정해야 합니다.

이 섹션에서는 외부 syslog 서버가 처리할 수 있어야 하는 다양한 유형의 로그 메시지 속도 및 평균 크기를 예측하는 데 도움이 되는 몇 가지 발견적 공식을 제공합니다. 이는 그리드의 알려진 성능 특성 또는 원하는 성능 특성(초당 S3 작업 수)을 기준으로 합니다.

계산 공식에서 초당 **S3** 작업을 사용합니다

그리드의 크기가 초당 바이트 수로 표시된 처리량인 경우 이 사이징을 초당 S3 작업으로 변환하여 추정 공식을 사용해야 합니다. 그리드 처리량을 변환하려면 먼저 평균 개체 크기를 확인해야 합니다. 이 크기는 기존 감사 로그 및 메트릭의 정보(있는 경우)를 사용하거나 StorageGRID를 사용할 애플리케이션에 대한 지식을 사용하여 확인할 수 있습니다. 예를 들어, 그리드의 크기가 2,000 MB/s의 처리량을 달성할 수 있도록 조정되었고 평균 오브젝트 크기가 2MB인 경우, 그리드는 초당 1,000 S3 작업(2,000MB/2MB)을 처리할 수 있도록 크기가 조정되었습니다.

> 다음 섹션의 외부 syslog 서버 크기 조정 공식은 최악의 경우를 추정하는 대신 일반적인 대/소문자 추정치를 제공합니다. 구성 및 워크로드에 따라 syslog 메시지 또는 syslog 데이터 볼륨이 수식에 따라 예측되는 것보다 높거나 낮을 수 있습니다. 수식은 지침으로만 사용됩니다.

감사 로그의 계산 공식

그리드에서 지원해야 하는 초당 S3 작업 수 이외의 S3 작업 부하에 대한 정보가 없는 경우 외부 syslog 서버가 다음 공식을 사용하여 처리해야 하는 감사 로그 볼륨을 예측할 수 있습니다. 감사 수준을 기본값으로 설정했다고 가정합니다 (오류 로 설정된 스토리지를 제외한 모든 범주는 보통 으로 설정됨).

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

예를 들어, 그리드가 초당 1,000개의 S3 작업용으로 사이징된 경우 외부 syslog 서버는 초당 2,000개의 syslog 메시지를 지원하도록 크기를 조정해야 하며 초당 1.6MB의 속도로 감사 로그 데이터를 수신(일반적으로 저장)할 수 있어야 합니다.

당신이 당신의 업무량에 대해 더 알고 있다면, 더 정확한 예측들이 가능합니다. 감사 로그의 경우 가장 중요한 추가 변수는 S3 작업이 놓이는 비율(대)입니다 다음 S3 필드의 평균 크기(바이트)와 평균 크기(표에 사용된 4자 약어는 감사 로그 필드 이름입니다).

코드	필드에 입력합니다	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.

코드	필드에 입력합니다	설명
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.

P를 사용하여 S3 작업 중 위치, 0 ≤ P ≤ 1(100% put 워크로드, P=1 및 100% get 워크로드, P=0)의 비율을 표시하겠습니다.

K를 사용하여 S3 계정 이름, S3 버킷 및 S3 키의 합계에 대한 평균 크기를 나타내겠습니다. S3 계정 이름이 항상 -s3-계정(13바이트)이고, 버킷에는 /my/application/bucket-12345(28바이트)와 같은 고정 길이 이름이 있고, 오브젝트에는 5733a5d7-f069-411f-8fbd-13247494c69c(36바이트)와 같은 고정 길이 키가 있다고 가정해 보겠습니다. 그런 다음 K 값은 90(13+13+28+36)입니다.

P와 K의 값을 결정할 수 있는 경우 감사 수준을 기본값으로 설정했다는 가정 하에 외부 syslog 서버가 처리해야 하는 감사 로그 볼륨을 다음 공식을 사용하여 추정할 수 있습니다(스토리지를 제외한 모든 범주는 Normal로 설정됨). 오류 로 설정된 경우):

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

예를 들어, 그리드가 초당 1,000개의 S3 작업용으로 사이징된 경우, 작업 부하의 크기는 50%이고 S3 계정 이름, 버킷 이름은 개체 이름의 평균 90바이트는 외부 syslog 서버가 초당 1,500개의 syslog 메시지를 지원하도록 사이징되어야 하며, 일반적으로 초당 약 1MB의 속도로 감사 로그 데이터를 수신(및 저장)할 수 있어야 합니다.

기본 감사 수준이 아닌 감사 수준에 대한 계산 공식

감사 로그에 제공된 수식에서는 기본 감사 수준 설정(오류 로 설정된 스토리지를 제외한 모든 범주가 보통으로 설정됨)을 사용한다고 가정합니다. 기본값이 아닌 감사 수준 설정에 대한 감사 메시지의 비율 및 평균 크기를 추정하는 자세한 공식은 사용할 수 없습니다. 그러나 다음 표를 사용하여 요율을 대략적으로 추정할 수 있습니다. 감사 로그에 제공된 평균 크기 수식을 사용할 수 있지만 "추가" 감사 메시지는 평균적으로 기본 감사 메시지보다 작기 때문에 과대 평가로 이어질 수 있습니다.

조건	수식
복제: 감사 수준 모두 디버그 또는 정상 으로 설정됩니다	감사 로그 비율 = 8 x S3 작업 비율
삭제 코딩: 모두 디버그 또는 정상 으로 설정된 감사 수준	기본 설정과 동일한 수식을 사용합니다

보안 이벤트의 계산 공식

보안 이벤트는 S3 운영과 관련이 없으며 일반적으로 최소한의 로그 및 데이터 볼륨을 생성합니다. 이러한 이유로 추정 공식은 제공되지 않습니다.

응용 프로그램 로그의 계산 공식

그리드에서 지원해야 하는 초당 S3 작업 수 이외의 S3 작업 부하에 대한 정보가 없는 경우 외부 syslog 서버에서 다음 공식을 사용하여 처리해야 하는 애플리케이션 로그 볼륨을 예측할 수 있습니다.

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

예를 들어, 그리드가 초당 1,000개의 S3 작업용으로 사이징된 경우 외부 syslog 서버는 초당 3,300개의 애플리케이션 로그를 지원할 수 있도록 사이징되어야 하고 초당 약 1.2MB의 속도로 애플리케이션 로그 데이터를 수신 및 저장할 수 있어야 합니다.

당신이 당신의 업무량에 대해 더 알고 있다면, 더 정확한 예측들이 가능합니다. 애플리케이션 로그의 경우 가장 중요한 추가 변수는 데이터 보호 전략(복제 및 삭제 코딩), 위치(vs 다음 S3 필드의 평균 크기(바이트)와 평균 크기(표에 사용되는 4자 약어는 감사 로그 필드 이름입니다).

코드	필드에 입력합니다	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.

크기 예측의 예

이 섹션에서는 다음과 같은 데이터 보호 방법을 사용하여 그리드에 대한 예측 공식을 사용하는 방법의 예를 설명합니다.

- 복제
- 삭제 코딩

데이터 보호를 위해 복제를 사용하는 경우

P는 S3 작업의 비율을, 여기서 0 ≤ P ≤ 1(100% put 워크로드의 경우 P=1, 100% get 워크로드의 경우 P=0)을 나타냅니다.

K는 S3 계정 이름, S3 버킷 및 S3 키의 합계에 대한 평균 크기를 나타냅니다. S3 계정 이름이 항상 -s3-계정(13바이트)이고, 버킷에는 /my/application/bucket-12345(28바이트)와 같은 고정 길이 이름이 있고, 오브젝트에는 5733a5d7-f069-411f-8fbd-13247494c69c(36바이트)와 같은 고정 길이 키가 있다고 가정해 보겠습니다. 그런 다음 K의 값은 90(13+13+28+36)입니다.

P와 K의 값을 확인할 수 있는 경우, 외부 syslog 서버가 다음 공식을 사용하여 처리할 수 있어야 하는 애플리케이션 로그 볼륨을 예측할 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, 그리드가 초당 1,000개의 S3 작업에 맞게 사이징된 경우 작업 부하가 50%이고 S3 계정 이름, 버킷 이름 및 오브젝트 이름이 평균 90바이트인 경우, 외부 syslog 서버는 초당 1800개의 애플리케이션 로그를 지원하도록 크기여야 합니다. 그리고 애플리케이션 데이터를 초당 0.5MB의 속도로 수신(일반적으로 저장)할 것입니다.

데이터 보호를 위해 삭제 코딩을 사용하는 경우

P는 S3 작업의 비율을, 여기서 0 ≤ P ≤ 1(100% put 워크로드의 경우 P=1, 100% get 워크로드의 경우 P=0)을 나타냅니다.

K는 S3 계정 이름, S3 버킷 및 S3 키의 합계에 대한 평균 크기를 나타냅니다. S3 계정 이름이 항상 -s3-계정(13바이트)이고, 버킷에는 /my/application/bucket-12345(28바이트)와 같은 고정 길이 이름이 있고, 오브젝트에는 5733a5d7-f069-411f-8fbd-13247494c69c(36바이트)와 같은 고정 길이 키가 있다고 가정해 보겠습니다. 그런 다음 K의 값은 90(13+13+28+36)입니다.

P와 K의 값을 확인할 수 있는 경우, 외부 syslog 서버가 다음 공식을 사용하여 처리할 수 있어야 하는 애플리케이션 로그 볼륨을 예측할 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, 그리드가 초당 1,000개의 S3 작업에 대해 사이징된 경우 워크로드는 50%가 되고 S3 계정 이름, 버킷 이름 객체 이름은 평균 90바이트로, 외부 syslog 서버는 초당 2,250개의 애플리케이션 로그를 지원하도록 크기를 조정하고 초당 0.6MB의 속도로 애플리케이션 데이터를 수신(일반적으로 저장)할 수 있어야 합니다.

감사 메시지 및 외부 **syslog** 서버를 구성합니다

감사 메시지와 관련된 여러 설정을 구성할 수 있습니다. 기록된 감사 메시지 수를 조정하고, 클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 정의하며, 외부 syslog 서버를 구성하고, 감사 로그, 보안 이벤트 로그 및 StorageGRID 소프트웨어 로그를 보낼 위치를 지정할 수 있습니다.

감사 메시지와 로그는 시스템 활동 및 보안 이벤트를 기록하고, 모니터링 및 문제 해결에 필수적인 도구입니다. 모든 StorageGRID 노드는 감사 메시지와 로그를 생성하여 시스템 활동 및 이벤트를 추적합니다.

필요에 따라 감사 정보를 원격으로 저장하도록 외부 syslog 서버를 구성할 수 있습니다. 외부 서버를 사용하면 감사 데이터의 완성도를 낮추지 않고도 감사 메시지 로깅의 성능에 미치는 영향을 최소화할 수 있습니다. 외부 syslog 서버는 큰 그리드가 있거나 여러 유형의 S3 애플리케이션을 사용하거나 모든 감사 데이터를 보존하려는 경우에 특히 유용합니다. 을 참조하십시오 "외부 syslog 서버에 대한 고려 사항" 를 참조하십시오.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "유지 관리 또는 루트 액세스 권한".
- 외부 syslog 서버를 구성하려는 경우 를 검토한 것입니다 "외부 syslog 서버 사용 시 고려 사항" 그리고 서버에 로그 파일을 수신하고 저장할 수 있는 충분한 용량이 있는지 확인했습니다.
- TLS 또는 RELP/TLS 프로토콜을 사용하여 외부 syslog 서버를 구성하려는 경우 필요한 서버 CA 및 클라이언트 인증서, 클라이언트 개인 키가 있습니다.

감사 메시지 수준을 변경합니다

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

감사 범주	기본 설정	추가 정보
시스템	정상	"시스템 감사 메시지"
스토리지	오류	"오브젝트 스토리지 감사 메시지"
관리	정상	"관리 감사 메시지입니다"
클라이언트 읽기	정상	"클라이언트가 감사 메시지를 읽습니다"
클라이언트 쓰기	정상	"클라이언트가 감사 메시지를 기록합니다"
ILM을 참조하십시오	정상	"ILM 감사 메시지"
교차 그리드 복제	오류	"CGRR: 교차 그리드 복제 요청"

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

업그레이드 중에는 감사 수준 구성이 즉시 적용되지 않습니다.

단계

1. 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 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).

감사 수준	설명
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.

S3 응용 프로그램에 대한 클라이언트 읽기 작업에 대한 자세한 레코드가 필요하지 않은 경우 * 클라이언트 읽기 * 설정을 * 오류 * 로 변경하여 감사 로그에 기록되는 감사 메시지 수를 줄입니다.

3. 저장 * 을 선택합니다.

   녹색 배너는 구성이 저장되었음을 나타냅니다.

HTTP 요청 헤더를 정의합니다

클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 선택적으로 정의할 수 있습니다. 이러한 프로토콜 헤더는 S3 및 Swift 요청에만 적용됩니다.

단계

1. Audit protocol headers * 섹션에서 클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 정의합니다.

   0개 이상의 문자를 일치시키려면 별표(\ *)를 와일드카드로 사용하십시오. 이스케이프 시퀀스(\ *)를 사용하여 리터럴 별표를 일치시킵니다.

2. 필요한 경우 추가 헤더를 만들려면 * 다른 헤더 추가 * 를 선택합니다.

   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.

3. 저장 * 을 선택합니다

   녹색 배너는 구성이 저장되었음을 나타냅니다.

외부 syslog 서버를 사용합니다

필요에 따라 감사 로그, 응용 프로그램 로그 및 보안 이벤트 로그를 그리드 외부의 위치에 저장하도록 외부 syslog 서버를 구성할 수 있습니다.

외부 syslog 서버를 사용하지 않으려면 이 단계를 건너뛰고 로 이동합니다 감사 정보 대상을 선택합니다.

이 절차에서 사용할 수 있는 구성 옵션이 요구 사항을 충족하기에 충분히 유연하지 않은 경우 를 사용하여 추가 구성 옵션을 적용할 수 있습니다 `audit-destinations` 의 전용 API 섹션에 있는 끝점입니다 "Grid Management API를 참조하십시오". 예를 들어, 노드 그룹마다 서로 다른 syslog 서버를 사용하려는 경우 API를 사용할 수 있습니다.

syslog 정보를 입력합니다

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

단계

1. 감사 및 syslog 서버 페이지에서 * 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 * 단계에 대해 유효한 정규화된 도메인 이름 또는 외부 syslog 서버에 대한 IPv4 또는 IPv6 주소를 * Host * 필드에 입력합니다.
3. 외부 syslog 서버의 대상 포트를 입력합니다(1과 65535 사이의 정수여야 함). 기본 포트는 514입니다.
4. 외부 syslog 서버로 감사 정보를 보내는 데 사용되는 프로토콜을 선택합니다.

   TLS * 또는 * RELP/TLS * 를 사용하는 것이 좋습니다. 이러한 옵션 중 하나를 사용하려면 서버 인증서를 업로드해야 합니다. 인증서를 사용하면 그리드와 외부 syslog 서버 간의 연결을 보호할 수 있습니다. 자세한 내용은 을 참조하십시오 "보안 인증서를 관리합니다".

   모든 프로토콜 옵션에는 외부 syslog 서버에 대한 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 제공합니다. RELP를 사용하면 외부 syslog 서버를 다시 시작해야 하는 경우 감사 정보의 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 업로드합니다.
   a. 사용할 인증서 또는 키를 * 찾아보기 * 를 선택합니다.
   b. 인증서 또는 키 파일을 선택합니다.
   c. 파일을 업로드하려면 * 열기 * 를 선택합니다.

      인증서 또는 키 파일 이름 옆에 녹색 확인 표시가 나타나 성공적으로 업로드되었음을 알려줍니다.

7. Continue * 를 선택합니다.

syslog 콘텐츠를 관리합니다

외부 syslog 서버로 보낼 정보를 선택할 수 있습니다.

단계

1. 마법사의 * syslog 콘텐츠 관리 * 단계에서 외부 syslog 서버로 보낼 감사 정보의 각 유형을 선택합니다.
   - * 감사 로그 전송 *: StorageGRID 이벤트 및 시스템 활동을 전송합니다
   - * 보안 이벤트 전송 *: 권한이 없는 사용자가 로그인을 시도하거나 사용자가 루트로 로그인하는 등의 보안 이벤트를 전송합니다
   - * 응용 프로그램 로그 전송 *: 다음과 같은 문제 해결에 유용한 로그 파일을 전송합니다.
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (관리 노드만)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   StorageGRID 소프트웨어 로그에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 소프트웨어 로그".

2. 드롭다운 메뉴를 사용하여 보내려는 감사 정보의 각 범주에 대한 심각도 및 시설(메시지 유형)을 선택합니다.

   심각도 및 항목 값을 설정하면 보다 쉽게 분석할 수 있도록 로그를 사용자 지정 가능한 방식으로 집계할 수 있습니다.

   a. 심각도 * 에 대해 * 통과 * 를 선택하거나 0에서 7 사이의 심각도 값을 선택합니다.

      값을 선택하면 선택한 값이 이 유형의 모든 메시지에 적용됩니다. 심각도를 고정 값으로 재정의하면 다른 심각도에 대한 정보가 손실됩니다.

심각도입니다	설명
패스스루	외부 syslog로 전송되는 각 메시지는 노드에 로컬로 로그온한 경우와 동일한 심각도 값을 갖습니다. • 감사 로그의 심각도는 "info"입니다. • 보안 이벤트의 경우 심각도 값은 노드의 Linux 배포판에 의해 생성됩니다. • 응용 프로그램 로그의 심각도는 문제의 심각도에 따라 "정보"와 "알림" 사이에 차이가 있습니다. 예를 들어 NTP 서버를 추가하고 HA 그룹을 구성하면 "info"라는 값이 제공되지만 SSM 또는 RSM 서비스를 의도적으로 중지하면 "notice"라는 값이 제공됩니다.
0	비상: 시스템을 사용할 수 없습니다
1	경고: 즉시 조치를 취해야 합니다
2	심각: 심각 상태
3	오류: 오류 조건

심각도입니다	설명
4	경고: 경고 조건
5	주의사항: 정상이지만 중대한 조건
6	정보: 정보 메시지
7	디버그: 디버그 레벨 메시지

b. Facilty * 의 경우 * PassThrough * 를 선택하거나 0에서 23 사이의 시설 값을 선택합니다.

   값을 선택하면 이 유형의 모든 메시지에 적용됩니다. 시설을 고정 값으로 재정의하면 다른 시설에 대한 정보가 손실됩니다.

있습니다	설명
패스스루	외부 syslog로 전송되는 각 메시지는 노드에 로컬로 로그온한 경우와 동일한 시설 값을 갖습니다. • 감사 로그의 경우 외부 syslog 서버로 전송되는 기능은 "local7"입니다. • 보안 이벤트의 경우 노드의 Linux 배포에 의해 항목 값이 생성됩니다. • 응용 프로그램 로그의 경우 외부 syslog 서버로 전송된 응용 프로그램 로그에는 다음 항목 값이 있습니다. ◦ `bycast.log`: 사용자 또는 데몬 ◦ `bycast-err.log`사용자, 데몬, local3 또는 local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: 로컬3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6
0	Kern(커널 메시지)
1	사용자(사용자 수준 메시지)
2	메일
3	데몬(시스템 데몬)
4	인증(보안/인증 메시지)

있습니다	설명
5	syslog(syslogd에 의해 내부적으로 생성된 메시지)
6	LPR(라인 프린터 하위 시스템)
7	뉴스(네트워크 뉴스 서브시스템)
8	UUCP
9	cron(클록 데몬)
10	보안(보안/인증 메시지)
11	FTP
12	NTP
13	Logaudit(로그 감사)
14	Logalert(로그 경고)
15	클록(클록 데몬)
16	로컬0
17	로컬1
18	로컬2
19	로컬3
20	로컬4
21	로컬5
22	로컬6
23	로컬7

3. Continue * 를 선택합니다.

테스트 메시지를 보냅니다

외부 syslog 서버를 사용하기 전에 그리드의 모든 노드가 외부 syslog 서버로 테스트 메시지를 보내도록 요청해야 합니다. 외부 syslog 서버로 데이터를 전송하기 전에 이러한 테스트 메시지를 사용하여 전체 로그 수집 인프라의 유효성을 확인해야 합니다.

> 외부 syslog 서버가 그리드의 각 노드로부터 테스트 메시지를 수신하고 메시지가 예상대로 처리되었음을 확인하기 전까지는 외부 syslog 서버 구성을 사용하지 마십시오.

단계

1. 외부 syslog 서버가 제대로 구성되어 있고 그리드의 모든 노드에서 감사 정보를 수신할 수 있으므로 테스트 메시지를 전송하지 않으려면 * Skip and finish * 를 선택합니다.

   녹색 배너는 구성이 저장되었음을 나타냅니다.

2. 그렇지 않으면 * 테스트 메시지 전송 * (권장)을 선택합니다.

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

3. 오류가 발생하면 오류를 수정하고 * 테스트 메시지 보내기 * 를 다시 선택합니다.

   을 참조하십시오 "외부 syslog 서버의 문제를 해결합니다" 오류를 해결하는 데 도움이 됩니다.

4. 모든 노드가 테스트를 통과했음을 나타내는 녹색 배너가 나타날 때까지 기다립니다.
5. syslog 서버를 확인하여 테스트 메시지가 예상대로 수신 및 처리되는지 확인합니다.

   > UDP를 사용하는 경우 전체 로그 수집 인프라를 확인합니다. UDP 프로토콜은 다른 프로토콜만큼 엄격한 오류 감지를 허용하지 않습니다 프로토콜

6. Stop and finish * 를 선택합니다.

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

   > StorageGRID 감사 정보는 외부 syslog 서버가 포함된 대상을 선택할 때까지 외부 syslog 서버로 전송되지 않습니다.

감사 정보 대상을 선택합니다

감사 로그, 보안 이벤트 로그 및 를 지정할 수 있습니다 "StorageGRID 소프트웨어 로그" 전송됩니다.

> 일부 대상은 외부 syslog 서버를 구성한 경우에만 사용할 수 있습니다.

단계

1. 감사 및 syslog 서버 페이지에서 감사 정보의 대상을 선택합니다.

   > * 로컬 노드만 * 및 * 외부 syslog 서버 * 는 일반적으로 더 나은 성능을 제공합니다.

옵션을 선택합니다	설명
로컬 노드만 해당	감사 메시지, 보안 이벤트 로그 및 응용 프로그램 로그는 관리 노드로 전송되지 않습니다. 대신, 이 파일은 해당 노드를 생성한 노드에만 저장됩니다("로컬 노드"). 모든 로컬 노드에서 생성된 감사 정보는 에 저장됩니다 `/var/local/log/localaudit.log` • 참고 *: StorageGRID는 주기적으로 로테이션에서 로컬 로그를 제거하여 공간을 확보합니다. 노드의 로그 파일이 1GB에 도달하면 기존 파일이 저장되고 새 로그 파일이 시작됩니다. 로그의 회전 제한은 21개 파일입니다. 22버전의 로그 파일이 만들어지면 가장 오래된 로그 파일이 삭제됩니다. 평균적으로 약 20GB의 로그 데이터가 각 노드에 저장됩니다.
관리 노드/로컬 노드	감사 메시지는 감사 로그에 전송됩니다 (`/var/local/log/audit.log`) 관리자 노드에 보안 이벤트 로그와 애플리케이션 로그는 해당 로그를 생성한 노드에 저장됩니다.
외부 syslog 서버	감사 정보는 외부 syslog 서버로 전송되고 로컬 노드에 저장됩니다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.
관리 노드 및 외부 syslog 서버	감사 메시지는 감사 로그에 전송됩니다 (`/var/local/log/audit.log`), 그리고 감사 정보가 외부 syslog 서버로 전송되고 로컬 노드에 저장됩니다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.

2. 저장 * 을 선택합니다.

   경고 메시지가 나타납니다.

3. 감사 정보의 대상을 변경하려면 * OK * 를 선택합니다.

   녹색 배너는 감사 구성이 저장되었음을 나타냅니다.

   새 로그가 선택한 대상으로 전송됩니다. 기존 로그는 현재 위치에 남아 있습니다.