



외부 **syslog** 서버를 사용합니다

StorageGRID 11.7

NetApp
April 12, 2024

목차

외부 syslog 서버를 사용합니다	1
외부 syslog 서버에 대한 고려 사항	1
외부 syslog 서버를 구성합니다	5

외부 **syslog** 서버를 사용합니다

외부 **syslog** 서버에 대한 고려 사항

다음 지침에 따라 필요한 외부 **syslog** 서버의 크기를 추정합니다.

외부 **syslog** 서버란 무엇입니까?

외부 **syslog** 서버는 단일 위치에서 시스템 감사 정보를 수집하는 데 사용할 수 있는 StorageGRID 외부의 서버입니다. 외부 **syslog** 서버를 사용하면 감사 정보의 대상을 구성하여 관리 노드의 네트워크 트래픽을 줄이고 정보를 보다 효율적으로 관리할 수 있습니다. 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** 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.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.

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

K를 사용하여 S3 계정 이름, S3 버킷 및 S3 키의 평균 크기를 나타내보겠습니다. 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):

$$\text{Audit Log Rate} = ((2 \times P) + (1 - P)) \times \text{S3 Operations Rate}$$

$$\text{Audit Log Average Size} = (570 + K) \text{ bytes}$$

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 효율을 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 속도 = S3 작업 속도 8개
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.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	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 $0 \leq P \leq 1$ (100% put 워크로드의 경우 $P=1$, 100% get 워크로드의 경우 $P=0$)을 나타냅니다.

K는 S3 계정 이름, S3 버킷 및 S3 키의 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 $0 \leq P \leq 1$ (100% put 워크로드의 경우 $P=1$, 100% get 워크로드의 경우 $P=0$)을 나타냅니다.

K는 S3 계정 이름, S3 버킷 및 S3 키의 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 맞게 사이징된 경우, 작업 부하가 50%이고 S3 계정 이름, 버킷 이름, 객체 이름 평균 90바이트에서 외부 syslog 서버는 초당 2,250개의 애플리케이션 로그를 지원하도록 크기를 조정해야 하며, 초당 0.6MB의 속도로 애플리케이션 데이터를 수신(일반적으로 저장)할 수 있어야 합니다.

감사 메시지 수준 및 외부 syslog 서버 구성에 대한 자세한 내용은 다음을 참조하십시오.

- "외부 syslog 서버를 구성합니다"
- "감사 메시지 및 로그 대상을 구성합니다"

외부 **syslog** 서버를 구성합니다

감사 로그, 응용 프로그램 로그 및 보안 이벤트 로그를 그리드 외부의 위치에 저장하려면 다음 절차를 사용하여 외부 syslog 서버를 구성합니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 로그 파일을 수신하고 저장할 용량이 있는 syslog 서버가 있습니다. 자세한 내용은 을 참조하십시오 "[외부 syslog 서버에 대한 고려 사항](#)".
- TLS 또는 RELP/TLS를 사용하려는 경우 올바른 서버 및 클라이언트 인증을 보유하고 있습니다.

이 작업에 대해

외부 syslog 서버로 감사 정보를 보내려면 먼저 외부 서버를 구성해야 합니다.

감사 정보를 외부 syslog 서버로 전송하면 다음을 수행할 수 있습니다.

- 감사 메시지, 응용 프로그램 로그 및 보안 이벤트와 같은 감사 정보를 보다 효율적으로 수집 및 관리합니다
- 관리 노드를 거치지 않고도 감사 정보가 다양한 스토리지 노드에서 외부 syslog 서버로 직접 전송되므로 관리 노드의 네트워크 트래픽을 줄일 수 있습니다



외부 syslog 서버로 로그를 전송할 때 메시지 끝에서 8192바이트보다 큰 단일 로그가 잘려서 외부 syslog 서버 구현의 일반적인 제한 사항을 따릅니다.



외부 syslog 서버에 장애가 발생할 경우 전체 데이터 복구 옵션을 최대화하려면 각 노드에서 최대 20GB의 감사 레코드 로컬 로그(localaudit.log)가 유지됩니다.



이 절차에서 사용할 수 있는 구성 옵션이 요구 사항을 충족할 만큼 유연하지 않은 경우 전용 API를 사용하여 추가 구성 옵션을 적용할 수 있습니다 audit-destinations 엔드포인트, 예를 들어, 서로 다른 노드 그룹에 서로 다른 syslog 서버를 사용할 수 있습니다.

외부 서버를 구성합니다

마법사에 액세스합니다

시작하려면 외부 syslog 서버 구성 마법사에 액세스합니다.

단계

1. 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 를 선택합니다.

2. 감사 및 syslog 서버 페이지에서 * 외부 syslog 서버 구성 * 을 선택합니다. 이전에 외부 syslog 서버를 구성한 경우 * 외부 syslog 서버 편집 * 을 선택합니다.

외부 syslog 서버 구성 마법사가 나타납니다.

syslog 정보를 입력합니다

외부 syslog 서버에 액세스하는 데 필요한 정보를 StorageGRID에 제공해야 합니다.

단계

1. 마법사의 * syslog 정보 입력 * 단계에 대해 유효한 정규화된 도메인 이름 또는 외부 syslog 서버에 대한 IPv4 또는 IPv6 주소를 * Host * 필드에 입력합니다.
2. 외부 syslog 서버의 대상 포트를 입력합니다(1과 65535 사이의 정수여야 함). 기본 포트는 514입니다.
3. 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 [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.

4. Continue * 를 선택합니다.
5. * TLS * 또는 * RELP/TLS * 를 선택한 경우 다음 인증서를 업로드하십시오.
 - * 서버 CA 인증서 *: 외부 syslog 서버를 확인하기 위한 하나 이상의 트러스트된 CA 인증서(PEM 인코딩). 이 인수를 생략하면 기본 Grid CA 인증서가 사용됩니다. 여기에 업로드하는 파일은 CA 번들이 될 수 있습니다.
 - * 클라이언트 인증서 *: 외부 syslog 서버(PEM 인코딩)에 대한 인증을 위한 클라이언트 인증서입니다.
 - * 클라이언트 개인 키 *: 클라이언트 인증서에 대한 개인 키(PEM 인코딩).



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.

- i. 사용할 인증서 또는 키를 * 찾아보기 * 를 선택합니다.
- ii. 인증서 파일 또는 키 파일을 선택합니다.
- iii. 파일을 업로드하려면 * 열기 * 를 선택합니다.

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

6. 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
2. 드롭다운 메뉴를 사용하여 보내려는 감사 정보 범주에 대한 심각도 및 기능(메시지 유형)을 선택합니다.

심각도 및 설비에 대해 * 통과 * 를 선택하면 원격 syslog 서버로 전송되는 정보는 노드에 로컬로 로그인할 때와 동일한 심각도와 기능을 받습니다. 시설 및 심각도를 설정하면 더욱 쉽게 분석할 수 있도록 로그를 사용자 지정 가능한 방식으로 집계하는 데 도움이 됩니다.



StorageGRID 소프트웨어 로그에 대한 자세한 내용은 을 참조하십시오 "[StorageGRID 소프트웨어 로그](#)".

- a. 심각도 * 의 경우 * 통과 * 를 선택하여 외부 syslog에 전송되는 각 메시지의 심각도 값이 로컬 syslog와 동일하게 되도록 합니다.

감사 로그의 경우 * 통과 * 를 선택하면 '정보'가 심각합니다.

보안 이벤트의 경우 * 통과 * 를 선택하면 노드의 Linux 배포에서 심각도 값이 생성됩니다.

응용 프로그램 로그의 경우 * 통과 * 를 선택하면 문제의 내용에 따라 심각도가 '정보'와 '알림'에 따라 다릅니다. 예를 들어 NTP 서버를 추가하고 HA 그룹을 구성하면 '정보' 값이 제공되지만 SSM 또는 RSM 서비스를 의도적으로 중지하는 경우 '알림'이 표시됩니다.

- b. 통과 연결 값을 사용하지 않으려면 0에서 7 사이의 심각도 값을 선택합니다.

선택한 값은 이 유형의 모든 메시지에 적용됩니다. 심각도가 고정 값으로 재정의되면 서로 다른 심각도에 대한 정보가 손실됩니다.

심각도입니다	설명
0	비상: 시스템을 사용할 수 없습니다

심각도입니다	설명
1	경고: 즉시 조치를 취해야 합니다
2	심각: 심각 상태
3	오류: 오류 조건
4	경고: 경고 조건
5	주의사항: 정상이지만 중대한 조건
6	정보: 정보 메시지
7	디버그: 디버그 레벨 메시지

- c. Facility * 의 경우 * PassThrough * 를 선택하여 외부 syslog로 전송되는 각 메시지가 로컬 syslog와 동일한 설비 값을 가지도록 합니다.

감사 로그의 경우 * PassThrough * 를 선택하면 외부 syslog 서버로 전송되는 기능이 'local7'입니다.

보안 이벤트의 경우 * PassThrough * 를 선택하면 시설 값이 노드의 Linux 배포판에 의해 생성됩니다.

응용 프로그램 로그의 경우 * 통과 * 를 선택하면 외부 syslog 서버로 전송된 응용 프로그램 로그의 항목 값은 다음과 같습니다.

응용 프로그램 로그	통과 연결 값입니다
bycast.log	사용자 또는 데몬
bycast-err.log	사용자, 데몬, local3 또는 local4
jaeger.log	로컬2
nms.log	로컬3
prometheus.log	로컬4
raft.log	로컬5
hagroups.log	로컬6

- d. 통과 연결 값을 사용하지 않으려면 0에서 23 사이의 설비 값을 선택합니다.

선택한 값은 이 유형의 모든 메시지에 적용됩니다. 고정 값으로 시설을 재정의하면 다른 시설에 대한 정보가 손실됩니다.

있습니다	설명
0	Kern(커널 메시지)
1	사용자(사용자 수준 메시지)
2	메일
3	데몬(시스템 데몬)
4	인증(보안/인증 메시지)
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

있습니다	설명
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.

구성이 성공적으로 저장되었음을 나타내는 녹색 배너가 나타납니다.

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 서버 문제 해결](#)" 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 프로토콜처럼 엄격한 오류 감지를 허용하지 않습니다.

6. Stop and finish * 를 선택합니다.

감사 및 syslog 서버 * 페이지로 돌아갑니다. syslog 서버 구성이 성공적으로 저장되었음을 알리는 녹색 배너가 나타납니다.



외부 syslog 서버를 포함하는 대상을 선택할 때까지 StorageGRID 감사 정보가 외부 syslog 서버로 전송되지 않습니다.

감사 정보 대상을 선택합니다

보안 이벤트 로그, 응용 프로그램 로그 및 감사 메시지 로그를 보낼 위치를 지정할 수 있습니다.



StorageGRID 소프트웨어 로그에 대한 자세한 내용은 을 참조하십시오 "[StorageGRID 소프트웨어 로그](#)".

단계

1. 감사 및 syslog 서버 페이지의 나열된 옵션 중에서 감사 정보의 대상을 선택합니다.

옵션을 선택합니다	설명
기본값(관리자 노드/로컬 노드)	감사 메시지는 감사 로그에 전송됩니다 (audit.log) 및 보안 이벤트 로그 및 애플리케이션 로그는 관리 노드에 저장되며, 이를 생성된 노드("로컬 노드"라고도 함)에 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 (audit.log)를 선택하면 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.
로컬 노드만 해당	관리자 노드 또는 원격 syslog 서버로 감사 정보가 전송되지 않습니다. 감사 정보는 감사 정보를 생성한 노드에만 저장됩니다. • 참고 *: StorageGRID는 공간을 확보하기 위해 주기적으로 이러한 로컬 로그를 제거합니다. 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.



모든 로컬 노드에서 생성된 감사 정보는 에 저장됩니다 /var/local/log/localaudit.log

2. 저장 * 을 선택합니다. 그런 다음 * OK * 를 선택하여 로그 대상에 대한 변경 사항을 적용합니다.
3. 외부 syslog 서버 * 또는 * 관리 노드 및 외부 syslog 서버 * 를 감사 정보 대상으로 선택한 경우 추가 경고가 나타납니다. 경고 텍스트를 검토합니다.



외부 syslog 서버가 테스트 StorageGRID 메시지를 수신할 수 있는지 확인해야 합니다.

4. 감사 정보의 대상을 변경하려면 * OK * 를 선택합니다.

감사 구성이 성공적으로 저장되었음을 알리는 녹색 배너가 나타납니다.

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

관련 정보

"감사 메시지 개요"

"감사 메시지 및 로그 대상을 구성합니다"

"시스템 감사 메시지"

"오브젝트 스토리지 감사 메시지"

"관리 감사 메시지입니다"

"클라이언트가 감사 메시지를 읽습니다"

"StorageGRID 관리"

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.