플랫폼 서비스 엔드포인트 관리

StorageGRID software

NetApp
July 23, 2026

목차

플랫폼 서비스 엔드포인트 관리

StorageGRID에서 플랫폼 서비스 엔드포인트 구성

버킷에 대한 플랫폼 서비스를 구성하기 전에 플랫폼 서비스의 대상으로 사용할 엔드포인트를 하나 이상 구성해야 합니다.

플랫폼 서비스에 대한 액세스는 StorageGRID 관리자가 테넌트별로 활성화합니다. 플랫폼 서비스 엔드포인트를 생성하거나 사용하려면, 스토리지 노드가 외부 엔드포인트 리소스에 액세스할 수 있도록 네트워킹이 구성된 그리드에서 엔드포인트 관리 또는 루트 액세스 권한이 있는 테넌트 사용자여야 합니다. 단일 테넌트에 대해 최대 500개의 플랫폼 서비스 엔드포인트를 구성할 수 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하십시오.

플랫폼 서비스 엔드포인트란 무엇인가요?

플랫폼 서비스 엔드포인트는 StorageGRID가 외부 대상에 액세스하는 데 필요한 정보를 지정합니다.

예를 들어 StorageGRID 버킷의 객체를 Amazon S3 버킷으로 복제하려면 StorageGRID가 Amazon의 대상 버킷에 액세스하는 데 필요한 정보와 자격 증명이 포함된 플랫폼 서비스 엔드포인트를 생성해야 합니다.

각 플랫폼 서비스 유형에는 고유한 엔드포인트가 필요하므로 사용하려는 각 플랫폼 서비스에 대해 최소 하나 이상의 엔드포인트를 구성해야 합니다. 플랫폼 서비스 엔드포인트를 정의한 후에는 해당 엔드포인트의 URN을 서비스 활성화에 사용되는 구성 XML의 대상으로 사용합니다.

여러 소스 버킷에 대해 동일한 엔드포인트를 대상으로 사용할 수 있습니다. 예를 들어, 여러 소스 버킷에서 객체 메타데이터를 동일한 검색 통합 엔드포인트로 전송하도록 구성하여 여러 버킷에서 검색을 수행할 수 있습니다. 또한 소스 버킷이 여러 엔드포인트를 대상으로 사용하도록 구성할 수 있으므로 객체 생성 알림은 하나의 Amazon Simple Notification Service(Amazon SNS) 주제로, 객체 삭제 알림은 다른 Amazon SNS 주제로 전송하는 등의 작업을 수행할 수 있습니다.

CloudMirror 복제용 엔드포인트

StorageGRID는 S3 버킷을 나타내는 복제 엔드포인트를 지원합니다. 이러한 버킷은 Amazon Web Services, 동일하거나 원격의 StorageGRID 배포 환경, 또는 다른 서비스에 호스팅될 수 있습니다.

알림 엔드포인트

StorageGRID는 Amazon SNS, Kafka 및 웹훅 엔드포인트를 지원합니다. Simple Queue Service(SQS) 및 AWS Lambda 엔드포인트는 지원하지 않습니다.

Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 따라서 Kafka 브로커 구성에서 `ssl.client.auth`을(를) `required`로 설정한 경우 Kafka 엔드포인트 구성 문제가 발생할 수 있습니다.

검색 통합 서비스의 엔드포인트

StorageGRID는 Elasticsearch 클러스터를 나타내는 검색 통합 엔드포인트를 지원합니다. 이러한 Elasticsearch 클러스터는 로컬 데이터 센터에 있거나 AWS 클라우드 또는 다른 곳에 호스팅될 수 있습니다.

검색 통합 엔드포인트는 특정 Elasticsearch 인덱스 및 유형을 참조합니다. StorageGRID에서 엔드포인트를 생성하기 전에 Elasticsearch에서 인덱스를 생성해야 합니다. 그렇지 않으면 엔드포인트 생성이 실패합니다. 유형은 엔드포인트를 생성하기 전에 생성할 필요가 없습니다. StorageGRID는 객체 메타데이터를 엔드포인트로 전송할 때

필요한 경우 유형을 생성합니다.

관련 정보

"StorageGRID 관리"

StorageGRID 플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오

플랫폼 서비스 엔드포인트를 생성할 때는 고유 리소스 이름(URN)을 지정해야 합니다. 이 URN은 플랫폼 서비스의 구성 XML을 생성할 때 엔드포인트를 참조하는 데 사용됩니다. 각 엔드포인트의 URN은 고유해야 합니다.

StorageGRID는 플랫폼 서비스 엔드포인트를 생성할 때 유효성을 검사합니다. 플랫폼 서비스 엔드포인트를 생성하기 전에 엔드포인트에 지정된 리소스가 존재하고 접근 가능한지 확인하십시오.

URN 요소

플랫폼 서비스 엔드포인트의 URN은 다음과 같이 `arn:aws` 또는 `urn:mysite`로 시작해야 합니다.

- 서비스가 Amazon Web Services(AWS)에서 호스팅되는 경우 다음을 사용하십시오 `arn:aws`
- 서비스가 Google Cloud Platform(GCP)에서 호스팅되는 경우 다음을 사용하세요. `arn:aws`
- 서비스가 로컬에서 호스팅되는 경우 다음을 사용하십시오 `urn:mysite`

예를 들어 StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 URN을 지정하는 경우 URN은 `urn:sgws`으로 시작할 수 있습니다.

URN의 다음 요소는 다음과 같이 플랫폼 서비스 유형을 지정합니다.

서비스	유형
CloudMirror 복제	`s3`
알림	`sns`, `kafka` 또는 `webhook`
검색 통합	`es`

예를 들어 StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 URN을 계속 지정하려면 `s3`을 추가하여 `urn:sgws:s3`을 얻습니다.

대부분의 엔드포인트에서 URN의 마지막 요소는 대상 URI의 특정 대상 리소스를 식별합니다(예: `sns-topic-name`).

웹훅 엔드포인트의 경우 대상 리소스는 대상 URI 자체입니다.

서비스	특정 리소스
CloudMirror 복제	`bucket-name`

서비스	특정 리소스
알림	`sns-topic-name` 또는 `kafka-topic-name` 참고: 웹훅 엔드포인트의 경우, URN의 마지막 요소는 엔드포인트의 URN이 고유하기만 하면 어떤 문자열이든 될 수 있습니다.
검색 통합	`domain-name/index-name/type-name` 참고: Elasticsearch 클러스터가 인덱스를 자동으로 생성하도록 구성되어 있지 않은 경우, 엔드포인트를 생성하기 전에 인덱스를 수동으로 생성해야 합니다.

AWS 및 GCP에서 호스팅되는 서비스에 대한 URN

AWS 및 GCP 엔티티의 경우 전체 URN은 유효한 AWS ARN입니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

```
arn:aws:s3:::bucket-name
```

- 알림:

```
arn:aws:sns:region:account-id:topic-name
```

- 검색 통합:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> AWS 검색 통합 엔드포인트의 경우, `domain-name`에는 여기에 표시된 것처럼 리터럴 문자열 `domain/`이 포함되어야 합니다.

로컬에서 호스팅되는 서비스에 대한 URN

클라우드 서비스 대신 로컬 호스팅 서비스를 사용하는 경우, 세 번째와 마지막 위치에 필수 요소가 포함되어 있는 한, 유효하고 고유한 URN을 생성하는 어떤 방식으로든 URN을 지정할 수 있습니다. 선택 사항으로 표시된 요소는 비워두거나, 리소스를 식별하고 URN을 고유하게 만드는 데 도움이 되는 방식으로 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

```
urn:mysite:s3:optional:optional:bucket-name
```

StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 경우, 다음으로 시작하는 유효한 URN을 지정할 수

있습니다 `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- 알림:

  Amazon Simple Notification Service 엔드포인트를 지정하십시오.

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Kafka 엔드포인트를 지정합니다:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

  웹훅 엔드포인트를 지정합니다.

  ```
  urn:mysite:webhook:optional:optional:webhook-name
  ```

- 검색 통합:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  로컬에서 호스팅되는 검색 통합 엔드포인트의 경우, 해당 `domain-name` 요소는 엔드포인트의 URN이 고유한 한 어떤 문자열이든 될 수 있습니다.

StorageGRID 플랫폼 서비스 엔드포인트를 생성합니다.

플랫폼 서비스를 활성화하려면 먼저 올바른 유형의 엔드포인트를 하나 이상 생성해야 합니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.
- ${post_edited_translations.segment}
  - CloudMirror 복제: S3 버킷
  - 이벤트 알림: Amazon Simple Notification Service(Amazon SNS) 토픽, Kafka 토픽 또는 웹훅 엔드포인트
  - 검색 알림: 타겟 클러스터가 인덱스를 자동으로 생성하도록 구성되어 있지 않은 경우 Elasticsearch 인덱스에 대한 알림이 표시됩니다.

- 대상 리소스에 대한 정보를 가지고 있습니다.
  - URI(Uniform Resource Identifier)의 호스트 및 포트

    StorageGRID 시스템에서 호스팅되는 버킷을 CloudMirror 복제의 엔드포인트로 사용하려는 경우, 입력해야 할 값을 확인하려면 그리드 관리자에게 문의하십시오.

  - 고유 리소스 이름(URN)

    "플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오."

  - 인증 자격 증명(필요한 경우):

    검색 통합 엔드포인트

    검색 통합 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

    - 액세스 키: 액세스 키 ID 및 비밀 액세스 키
    - 기본 HTTP: 사용자 이름과 비밀번호

    CloudMirror 복제 엔드포인트

    CloudMirror 복제 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

    - 액세스 키: 액세스 키 ID 및 비밀 액세스 키
    - ${post_edited_translations.segment}

    Amazon SNS 엔드포인트

    Amazon SNS 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

    - 액세스 키: 액세스 키 ID 및 비밀 액세스 키

    Kafka 엔드포인트

    ${post_edited_translations.segment}

    - SASL/PLAIN: 사용자 이름 및 비밀번호
    - SASL/SCRAM-SHA-256: 사용자 이름 및 비밀번호
    - ${post_edited_translations.segment}

  - 보안 인증서(인증서 확인이 필요한 경우)
- Elasticsearch 보안 기능이 활성화된 경우 연결 테스트를 위한 클러스터 모니터링 권한과 문서 업데이트를 위한 쓰기 인덱스 권한 또는 인덱스 및 인덱스 삭제 권한 모두가 필요합니다.

단계

1. **STORAGE (S3)** > *Platform services endpoints*를 선택합니다. Platform services endpoints 페이지가 나타납니다.
2. *엔드포인트 생성*을 선택합니다.
3. 엔드포인트와 그 용도를 간략하게 설명하는 표시 이름을 입력하십시오.

${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   ```
   https://host:port
   http://host:port
   ```

   포트를 지정하지 않으면 다음 기본 포트가 사용됩니다.

   - HTTPS URI의 경우 포트 443, HTTP URI의 경우 포트 80(대부분의 엔드포인트)
   - HTTPS 및 HTTP URI용 포트 9092 (Kafka 엔드포인트에만 해당)

   예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같을 수 있습니다.

   ```
   https://s3.example.com:10443
   ```

   이 예에서 `s3.example.com`은 StorageGRID 고가용성(HA) 그룹의 가상 IP(VIP)에 대한 DNS 엔트리를 나타내며, `10443`은 로드 밸런서 엔드포인트에 정의된 포트를 나타냅니다.

   가능한 경우 단일 장애 지점을 방지하기 위해 로드 밸런싱 노드의 HA 그룹에 연결해야 합니다.

   마찬가지로 AWS에서 호스팅되는 버킷의 URI는 다음과 같을 수 있습니다.

   ```
   https://s3-aws-region.amazonaws.com
   ```

   엔드포인트가 CloudMirror 복제 서비스에 사용되는 경우, URI에 버킷 이름을 포함하지 마십시오. 버킷 이름은 **URN** 필드에 포함합니다.

5. 엔드포인트의 고유 리소스 이름(URN)을 입력하십시오.

   엔드포인트가 생성된 후에는 해당 엔드포인트의 URN을 변경할 수 없습니다.

6. *Continue*를 선택합니다.
7. *인증 유형*에 대한 값을 선택하십시오.

   웹훅 엔드포인트에 대한 인증을 사용하려면 9단계에서 mTLS(상호 전송 계층 보안)를 구성하십시오.

검색 통합 엔드포인트

검색 통합 엔드포인트에 대한 자격 증명을 입력하거나 업로드하십시오.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.
액세스 키	대상과의 연결을 인증하기 위해 AWS 스타일 자격 증명을 사용합니다.	• 액세스 키 ID • ${post_edited_translations.segment}
기본 HTTP	${post_edited_translations.segment}	• 사용자 이름 • 비밀번호

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트에 대한 자격 증명을 입력하거나 업로드하세요.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.
액세스 키	대상과의 연결을 인증하기 위해 AWS 스타일 자격 증명을 사용합니다.	• 액세스 키 ID • ${post_edited_translations.segment}

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
${post_edited_translations.segment}	대상과의 연결을 인증하기 위해 인증서와 키를 사용합니다.	• 임시 자격 증명 URL • ${post_edited_translations.segment} • 클라이언트 인증서(PEM 파일 업로드) • 클라이언트 개인 키(PEM 파일 업로드, OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식) • 클라이언트 개인 키 암호(선택 사항)

Amazon SNS 엔드포인트

Amazon SNS 엔드포인트에 대한 자격 증명을 입력하거나 업로드하십시오.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.
액세스 키	대상과의 연결을 인증하기 위해 AWS 스타일 자격 증명을 사용합니다.	• 액세스 키 ID • ${post_edited_translations.segment}

Kafka 엔드포인트

Kafka 엔드포인트에 대한 자격 증명을 입력하거나 업로드합니다.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
SASL/PLAIN	${post_edited_translations.segment}	• 사용자 이름 • 비밀번호
SASL/SCRAM-SHA-256	${post_edited_translations.segment}	• 사용자 이름 • 비밀번호
SASL/SCRAM-SHA-512	챌린지-응답 프로토콜과 SHA-512 해싱을 사용하는 사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 비밀번호

사용자 이름과 비밀번호가 Kafka 클러스터에서 얻은 위임 토큰에서 파생된 경우 *위임된 토큰 인증 사용*을 선택하십시오.

8. *Continue*를 선택합니다.
9. 인증서 확인 라디오 버튼을 선택하여 엔드포인트에 대한 TLS 연결을 확인하는 방법을 선택하십시오.

대부분의 엔드포인트

검색 통합, CloudMirror 복제, Amazon SNS 또는 Kafka 엔드포인트에 대한 TLS 연결을 확인하십시오.

인증서 검증 유형	설명
TLS	엔드포인트 리소스에 대한 TLS 연결에 사용되는 서버 인증서를 검증합니다.
비활성화됨	인증서 확인 기능이 비활성화되었습니다. 이 옵션은 안전하지 않습니다.
사용자 지정 CA 인증서 사용	사용자 지정 CA 인증서는 엔드포인트에 연결할 때 서버의 신원을 확인하는 데 사용됩니다.
운영 체제 CA 인증서 사용	${post_edited_translations.segment}

웹훅 엔드포인트만 해당

웹훅 엔드포인트에 대한 TLS 연결을 확인하십시오.

인증서 검증 유형	설명
TLS	엔드포인트 리소스에 대한 TLS 연결에 사용되는 서버 인증서를 검증합니다.
mTLS	엔드포인트 리소스에 대한 상호 TLS 연결에 사용되는 클라이언트 및 서버 인증서를 검증합니다.
비활성화됨	인증서 확인 기능이 비활성화되었습니다. 이 옵션은 안전하지 않습니다.
사용자 지정 CA 인증서 사용	사용자 지정 CA 인증서는 엔드포인트에 연결할 때 서버의 신원을 확인하는 데 사용됩니다.

${post_edited_translations.segment}

인증서 검증 유형	설명
서버 인증서를 확인하지 않음	서버 인증서 검증을 비활성화합니다. 즉, 서버의 신원이 확인되지 않습니다. 이 옵션은 보안에 취약합니다.
클라이언트 인증서	클라이언트 인증서는 엔드포인트에 연결할 때 클라이언트의 신원을 확인하는 데 사용됩니다.
클라이언트 개인 키	클라이언트 인증서의 개인 키입니다. 암호화된 경우 기존 PKCS #1 형식을 사용해야 합니다(PKCS #8 형식은 지원되지 않습니다).

인증서 검증 유형	설명
클라이언트 개인 키 암호	클라이언트 개인 키를 복호화하는 데 사용할 암호입니다. 개인 키가 암호화되지 않은 경우 이 필드를 비워 두십시오.

10. *테스트 및 엔드포인트 생성*을 선택합니다.
    - 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
    - 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하기 위해 엔드포인트를 수정해야 하는 경우, *엔드포인트 세부 정보로 돌아가기*를 선택하고 정보를 업데이트합니다. 그런 다음 *엔드포인트 테스트 및 생성*을 선택합니다.

> ⓘ 테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다. StorageGRID 관리자에게 문의하십시오.

엔드포인트를 구성한 후에는 해당 URN을 사용하여 플랫폼 서비스를 구성할 수 있습니다.

관련 정보

- "플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오."
- "CloudMirror 복제 구성"
- "이벤트 알림 구성"
- "검색 통합 서비스 구성"

StorageGRID 플랫폼 서비스 엔드포인트의 연결을 테스트합니다

플랫폼 서비스에 대한 연결이 변경된 경우 엔드포인트에 대한 연결을 테스트하여 대상 리소스가 존재하고 지정한 자격 증명을 사용하여 접근할 수 있는지 확인할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.

이 작업 정보

StorageGRID는 자격 증명에 올바른 권한이 있는지 검증하지 않습니다.

단계

1. **STORAGE (S3)** > *플랫폼 서비스 엔드포인트*를 선택합니다.

   플랫폼 서비스 엔드포인트 페이지가 나타나고 이미 구성된 플랫폼 서비스 엔드포인트 목록이 표시됩니다.

2. 연결을 테스트할 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

3. *연결 테스트*를 선택합니다.
   - 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
   - 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하기 위해 엔드포인트를 수정해야 하는 경우, *구성*을 선택하고 정보를 업데이트합니다. 그런 다음 *테스트 및 변경 사항 저장*을 선택합니다.

StorageGRID에서 플랫폼 서비스 엔드포인트 편집

플랫폼 서비스 엔드포인트의 구성을 편집하여 이름, URI 또는 기타 세부 정보를 변경할 수 있습니다. 예를 들어 만료된 자격 증명을 업데이트하거나 장애 조치를 위해 백업 Elasticsearch 인덱스를 가리키도록 URI를 변경해야 할 수 있습니다. 플랫폼 서비스 엔드포인트의 URN은 변경할 수 없습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. **STORAGE (S3)** > *플랫폼 서비스 엔드포인트*를 선택합니다.

   플랫폼 서비스 엔드포인트 페이지가 나타나고 이미 구성된 플랫폼 서비스 엔드포인트 목록이 표시됩니다.

2. 편집할 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

3. *구성*을 선택합니다.
4. 필요에 따라 엔드포인트의 구성을 변경하십시오.

   엔드포인트가 생성된 후에는 해당 엔드포인트의 URN을 변경할 수 없습니다.

   a. 엔드포인트의 표시 이름을 변경하려면 편집 아이콘 을 선택합니다.
   b. 필요에 따라 URI를 변경하십시오.
   c. 필요에 따라 인증 유형을 변경하십시오.
      - 액세스 키 인증의 경우, *S3 키 편집*을 선택하고 새 액세스 키 ID와 비밀 액세스 키를 붙여넣어 필요에 따라 키를 변경하십시오. 변경 사항을 취소하려면 *S3 키 편집 되돌리기*를 선택하십시오.
      - CAP(C2S 액세스 포털) 인증의 경우, 필요에 따라 임시 자격 증명 URL 또는 선택적 클라이언트 개인 키 암호를 변경하고 새 인증서 및 키 파일을 업로드하십시오.

        클라이언트 개인 키는 OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식이어야 합니다.

   d. 필요에 따라 인증서 확인 방법을 변경하십시오.
5. *테스트 후 변경 사항 저장*을 선택합니다.

◦ 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

◦ 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하려면 엔드포인트를 수정하고 *테스트 및 변경 사항 저장*을 선택하십시오.

StorageGRID 플랫폼 서비스 엔드포인트를 삭제합니다

연결된 플랫폼 서비스를 더 이상 사용하지 않으려면 엔드포인트를 삭제할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. **STORAGE (S3)** > *플랫폼 서비스 엔드포인트*를 선택합니다.

   플랫폼 서비스 엔드포인트 페이지가 나타나고 이미 구성된 플랫폼 서비스 엔드포인트 목록이 표시됩니다.

2. 삭제하려는 각 엔드포인트의 확인란을 선택합니다.

   사용 중인 플랫폼 서비스 엔드포인트를 삭제하면 해당 엔드포인트를 사용하는 모든 버킷에 대해 연결된 플랫폼 서비스가 비활성화됩니다. 아직 완료되지 않은 요청은 모두 삭제됩니다. 삭제된 URN을 더 이상 참조하지 않도록 버킷 구성을 변경하기 전까지는 새로운 요청이 계속 생성됩니다. StorageGRID는 이러한 요청을 복구할 수 없는 오류로 보고합니다.

3. 작업 > *엔드포인트 삭제*를 선택합니다.

   확인 메시지가 나타납니다.

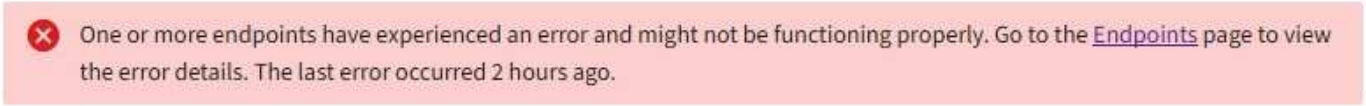
4. *엔드포인트 삭제*를 선택합니다.

StorageGRID 플랫폼 서비스 엔드포인트 오류 해결

StorageGRID가 플랫폼 서비스 엔드포인트와 통신하려고 할 때 오류가 발생하면 대시보드에 메시지가 표시됩니다. 플랫폼 서비스 엔드포인트 페이지의 마지막 오류 열에는 오류가 발생한 시간이 표시됩니다. 엔드포인트 자격 증명과 연결된 권한이 올바르지 않은 경우에는 오류가 표시되지 않습니다.

오류가 발생했는지 확인합니다.

지난 7일 동안 플랫폼 서비스 엔드포인트 오류가 발생한 경우 테넌트 관리자 대시보드에 알림 메시지가 표시됩니다. 플랫폼 서비스 엔드포인트 페이지에서 오류에 대한 자세한 내용을 확인할 수 있습니다.



대시보드에 표시되는 것과 동일한 오류가 플랫폼 서비스 엔드포인트 페이지 상단에도 나타납니다. 자세한 오류 메시지를 보려면 다음을 참조하십시오.

단계

1. 엔드포인트 목록에서 오류가 발생한 엔드포인트를 선택합니다.
2. 엔드포인트 세부 정보 페이지에서 *연결*을 선택합니다. 이 탭에는 엔드포인트에 대한 가장 최근 오류만 표시되며 오류 발생 시점이 표시됩니다. 빨간색 X 아이콘  이 포함된 오류는 지난 7일 이내에 발생한 오류입니다.

오류가 여전히 유효한지 확인하십시오.

일부 오류는 해결된 후에도 마지막 오류 열에 계속 표시될 수 있습니다. 오류가 현재 발생 중인지 확인하거나 해결된 오류를 표에서 강제로 제거하려면 다음 단계를 따르세요.

단계

1. 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

2. * 연결* > *연결 테스트*를 선택합니다.

*연결 테스트*를 선택하면 StorageGRID가 플랫폼 서비스 엔드포인트가 존재하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

엔드포인트 오류 해결

엔드포인트 세부 정보 페이지에서 마지막 오류 메시지를 확인하여 오류 원인을 파악할 수 있습니다. 일부 오류는 엔드포인트를 수정해야 해결할 수 있습니다. 예를 들어, StorageGRID가 올바른 액세스 권한이 없거나 액세스 키가 만료되어 대상 S3 버킷에 액세스할 수 없는 경우 CloudMirroring 오류가 발생할 수 있습니다. 이 경우 메시지는 "엔드포인트 자격 증명 또는 대상 액세스를 업데이트해야 합니다."이며, 세부 정보는 "AccessDenied" 또는 "InvalidAccessKeyId"로 표시됩니다.

오류를 해결하기 위해 엔드포인트를 수정해야 하는 경우, *테스트 및 변경 사항 저장*을 선택하면 StorageGRID가 업데이트된 엔드포인트를 검증하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트 연결은 각 사이트의 한 노드에서 검증됩니다.

단계

1. 엔드포인트를 선택합니다.
2. 엔드포인트 세부 정보 페이지에서 *구성*을 선택합니다.
3. 필요에 따라 엔드포인트 구성을 편집하십시오.
4. * 연결* > *연결 테스트*를 선택합니다.

${post_edited_translations.segment}

StorageGRID 플랫폼 서비스 엔드포인트를 검증할 때, 해당 엔드포인트의 자격 증명을 사용하여 대상 리소스에 연결할 수 있는지 확인하고 기본적인 권한 검사를 수행합니다. 그러나 StorageGRID는 특정 플랫폼 서비스 작업에 필요한 모든 권한을 검증하지는 않습니다. 따라서 플랫폼 서비스를 사용하려고 할 때 오류(예: "403 Forbidden")가 발생하는 경우, 엔드포인트 자격 증명과 연결된 권한을 확인하십시오.

관련 정보

- **StorageGRID** 관리 **›** 플랫폼 서비스 문제 해결
- "플랫폼 서비스 엔드포인트 생성"
- "플랫폼 서비스 엔드포인트에 대한 연결 테스트"
- "플랫폼 서비스 엔드포인트 편집"

저작권 정보

상표 정보