테넌트 계정을 사용합니다

StorageGRID

NetApp
April 10, 2024

목차

테넌트 계정을 사용합니다

테넌트 계정 사용: 개요

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API 또는 Swift REST API를 사용하여 StorageGRID 시스템에 오브젝트를 저장하고 검색할 수 있습니다.

테넌트 계정이란 무엇입니까?

각 테넌트 계정에는 자체 통합 또는 로컬 그룹, 사용자, S3 버킷 또는 Swift 컨테이너 및 객체가 있습니다.

필요한 경우 테넌트 계정을 사용하여 저장된 객체를 다른 엔터티로 분리할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 사용할 수 있습니다.

- * 기업 활용 사례: * 기업 내에서 StorageGRID 시스템을 사용하는 경우 그리드의 객체 스토리지를 조직의 여러 부서에서 분리할 수 있습니다. 예를 들어 마케팅 부서, 고객 지원 부서, 인사 부서 등의 테넌트 계정이 있을 수 있습니다.

> S3 클라이언트 프로토콜을 사용하는 경우 S3 버킷 및 버킷 정책을 사용하여 엔터프라이즈의 부서 간에 오브젝트를 분리할 수도 있습니다. 별도의 테넌트 계정을 생성할 필요가 없습니다. 를 참조하십시오 S3 클라이언트 애플리케이션 구현 지침.

- * 서비스 공급자 사용 사례: * 서비스 공급자가 StorageGRID 시스템을 사용 중인 경우, 스토리지를 임대하는 다른 엔터티로 그리드의 개체 스토리지를 분리할 수 있습니다. 예를 들어 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정이 있을 수 있습니다.

테넌트 계정을 생성하는 방법

테넌트 계정은 에 의해 생성됩니다 그리드 관리자를 사용하는 StorageGRID 그리드 관리자. 테넌트 계정을 생성할 때 그리드 관리자는 다음 정보를 지정합니다.

- 테넌트의 표시 이름(테넌트의 계정 ID가 자동으로 할당되며 변경할 수 없음)
- 테넌트 계정에서 S3 또는 Swift를 사용할지 여부를 나타냅니다.
- S3 테넌트 계정의 경우: 테넌트 계정이 플랫폼 서비스를 사용하도록 허용되는지 여부 플랫폼 서비스를 사용할 수 있는 경우 그리드 사용을 지원하도록 구성해야 합니다.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.
- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

또한, S3 테넌트 계정이 규정 요구 사항을 준수해야 하는 경우 그리드 관리자는 StorageGRID 시스템에 대해 S3 오브젝트 잠금 설정을 활성화할 수 있습니다. S3 오브젝트 잠금이 활성화된 경우 모든 S3 테넌트 계정에서 호환 버킷을 생성하고 관리할 수 있습니다.

S3 테넌트를 구성합니다

을(를) 마친 후 S3 테넌트 계정이 생성됩니다테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하거나(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 생성합니다
- S3 액세스 키 관리
- 규정 준수 버킷을 포함하여 S3 버킷 생성 및 관리
- 플랫폼 서비스 사용(활성화된 경우)
- 스토리지 사용량 모니터링

> 테넌트 관리자를 사용하여 S3 버킷을 생성 및 관리할 수 있지만 에는 가 있어야 합니다 S3 액세스 키를 사용하고 S3 REST API를 사용하여 오브젝트를 수집 및 관리합니다.

Swift 테넌트를 구성합니다

A 뒤에 Swift 테넌트 계정이 생성됩니다테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 만듭니다
- 스토리지 사용량 모니터링

> Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한에서는 사용자가 에 인증할 수 없습니다 Swift REST API 컨테이너 및 수집 개체 생성 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

테넌트 관리자를 사용합니다

테넌트 관리자를 사용하면 StorageGRID 테넌트 계정의 모든 측면을 관리할 수 있습니다.

테넌트 관리자를 사용하여 테넌트 계정의 스토리지 사용량을 모니터링하고 ID 페더레이션을 통해 사용자를 관리하거나 로컬 그룹 및 사용자를 생성할 수 있습니다. S3 테넌트 계정의 경우 S3 키를 관리하고 S3 버킷을 관리하고 플랫폼 서비스를 구성할 수도 있습니다.

로그인 및 로그아웃 방법

테넌트 관리자에 로그인합니다

의 주소 표시줄에 테넌트에 대한 URL을 입력하여 테넌트 관리자에 액세스합니다 지원되는 웹 브라우저.

필요한 것

- 로그인 자격 증명이 있어야 합니다.
- 그리드 관리자가 제공한 대로 테넌트 관리자에 액세스하기 위한 URL이 있어야 합니다. URL은 다음 예 중 하나로 표시됩니다.

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

URL은 항상 FQDN(정규화된 도메인 이름) 또는 관리 노드에 액세스하는 데 사용되는 IP 주소를 포함하며, 포트 번호, 20자리 테넌트 계정 ID 또는 둘 다를 선택적으로 포함할 수도 있습니다.

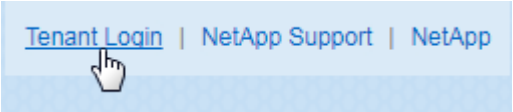
- URL에 테넌트의 20자리 계정 ID가 포함되지 않은 경우 이 계정 ID가 있어야 합니다.
- 을(를) 사용해야 합니다 지원되는 웹 브라우저.
- 웹 브라우저에서 쿠키를 활성화해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

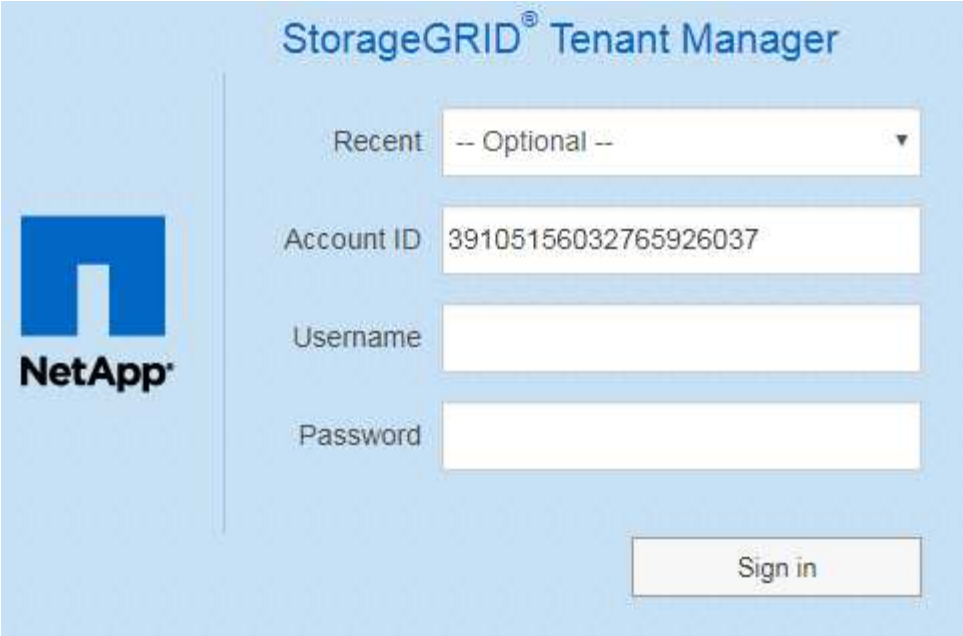
1. A를 시작합니다 지원되는 웹 브라우저.
2. 브라우저의 주소 표시줄에 Tenant Manager에 액세스하기 위한 URL을 입력합니다.
3. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다.
4. 테넌트 관리자에 로그인합니다.

   표시되는 로그인 화면은 입력한 URL과 조직에서 SSO(Single Sign-On)를 사용하고 있는지 여부에 따라 달라집니다. 다음 화면 중 하나가 표시됩니다.

   - Grid Manager 로그인 페이지 오른쪽 상단에서 * Tenant Login * 링크를 클릭합니다.

   - Tenant Manager 로그인 페이지. 아래와 같이 * Account ID * 필드가 이미 입력되어 있을 수 있습니다.



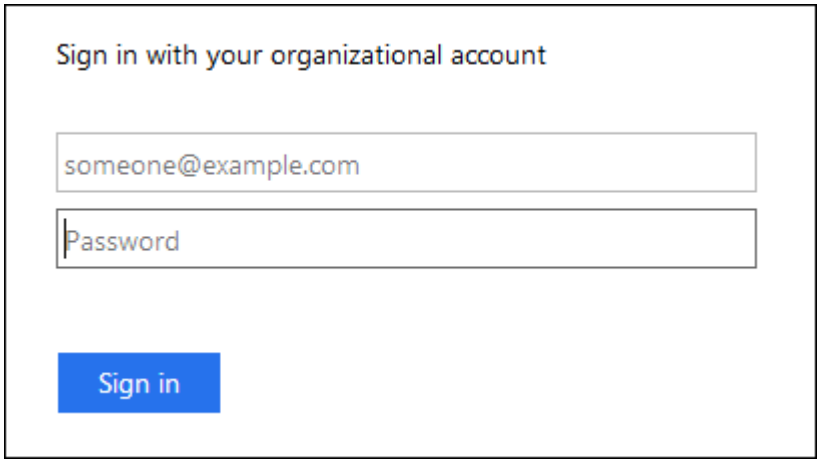
i. 테넌트의 20자리 계정 ID가 표시되지 않으면 최근 계정 목록에 테넌트 계정 이름이 나타날 경우 해당 계정 이름을 선택하거나 계정 ID를 입력합니다.

ii. 사용자 이름과 암호를 입력합니다.

iii. 로그인 * 을 클릭합니다.

Tenant Manager 대시보드가 나타납니다.

- SSO가 그리드에 활성화되어 있는 경우 조직의 SSO 페이지. 예를 들면 다음과 같습니다.



표준 SSO 자격 증명을 입력하고 * 로그인 * 을 클릭합니다.

- Tenant Manager SSO 로그인 페이지.

i. 테넌트의 20자리 계정 ID가 표시되지 않으면 최근 계정 목록에 테넌트 계정 이름이 나타날 경우 해당 계정 이름을 선택하거나 계정 ID를 입력합니다.

ii. 로그인 * 을 클릭합니다.

iii. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인합니다.

Tenant Manager 대시보드가 나타납니다.

5. 다른 사람으로부터 초기 암호를 받은 경우 암호를 변경하여 계정을 보호하십시오. 사용자 이름 _ * > * 암호 변경 * 을 선택합니다.

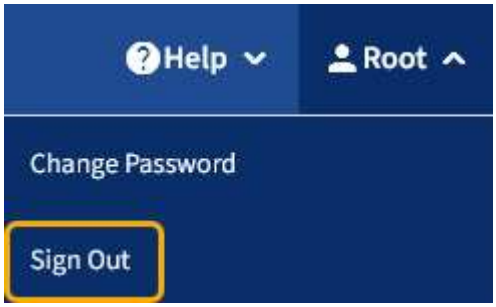
> StorageGRID 시스템에 SSO가 설정되어 있으면 테넌트 관리자에서 암호를 변경할 수 없습니다.

테넌트 관리자에서 로그아웃합니다

테넌트 관리자 작업을 마치면 로그아웃하여 권한이 없는 사용자가 StorageGRID 시스템에 액세스할 수 없도록 해야 합니다. 브라우저를 닫아도 브라우저 쿠키 설정에 따라 시스템에서 로그아웃되지 않을 수 있습니다.

단계

1. 사용자 인터페이스의 오른쪽 위 모서리에서 사용자 이름 드롭다운을 찾습니다.



2. 사용자 이름을 선택한 다음 * 로그아웃 * 을 선택합니다.

   - SSO가 사용되지 않는 경우:

관리자 노드에서 로그아웃되었습니다. Tenant Manager 로그인 페이지가 표시됩니다.

> 두 개 이상의 관리 노드에 로그인한 경우 각 노드에서 로그아웃해야 합니다.

- SSO가 활성화된 경우:

  액세스 중인 모든 관리 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. 방금 액세스한 테넌트 계정의 이름이 * 최근 계정 * 드롭다운에 기본값으로 나열되고 테넌트의 * 계정 ID * 가 표시됩니다.

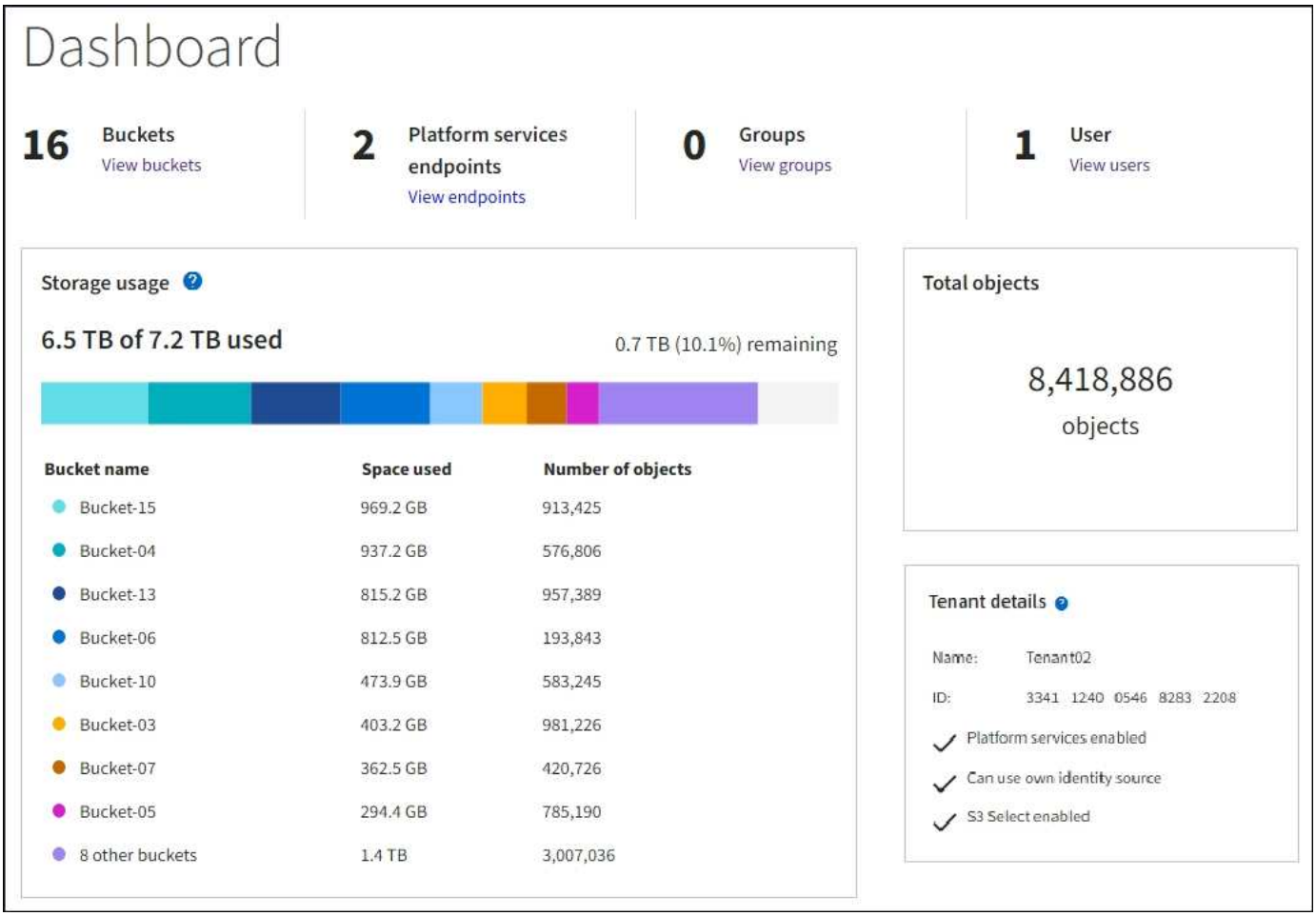
> SSO가 활성화되어 있고 Grid Manager에도 로그인한 경우, Grid Manager에서 로그아웃하여 SSO를 로그아웃해야 합니다.

테넌트 관리자 대시보드 이해

테넌트 관리자 대시보드에서는 테넌트 계정의 구성과 테넌트의 버킷(S3) 또는 컨테이너(Swift)에 있는 객체가 사용하는 공간의 양을 개괄적으로 보여 줍니다. 테넌트에 할당량이 있는 경우 대시보드에는 사용된 할당량의 양과 남아 있는 양이 표시됩니다. 테넌트 계정과 관련된 오류가 있는 경우 대시보드 에 오류가 표시됩니다.

> 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다.

객체가 업로드되면 대시보드는 다음 예제와 같습니다.



테넌트 계정 요약

대시보드 상단에는 다음 정보가 포함되어 있습니다.

- 구성된 버킷 또는 컨테이너, 그룹 및 사용자 수
- 구성된 플랫폼 서비스 엔드포인트의 수입니다

링크를 선택하여 세부 정보를 볼 수 있습니다.

대시보드의 오른쪽에는 다음과 같은 정보가 포함되어 있습니다.

- 테넌트의 총 객체 수입니다.

  S3 계정의 경우 오브젝트가 수집되지 않고 루트 액세스 권한이 있는 경우 총 오브젝트 수 대신 시작 지침이 나타납니다.

- 테넌트 계정 이름 및 ID와 테넌트가 사용할 수 있는지 여부를 포함한 테넌트 세부 정보입니다 플랫폼 서비스, 고유한 ID 소스입니다, 또는 S3 를 선택합니다 (설정된 권한만 나열됩니다).

스토리지 및 할당량 사용

Storage usage(저장소 사용) 패널에는 다음과 같은 정보가 포함되어 있습니다.

- 테넌트에 대한 객체 데이터의 양입니다.

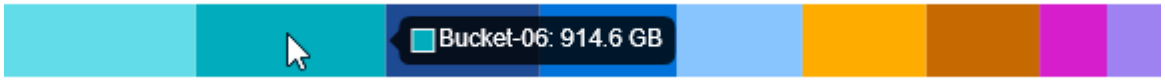
> 이 값은 업로드된 총 오브젝트 데이터 양을 나타내며 해당 오브젝트 및 해당 메타데이터의 복사본을 저장하는 데 사용되는 공간을 나타내지 않습니다.

- 할당량이 설정된 경우 개체 데이터에 사용할 수 있는 총 공간과 남은 공간의 양과 백분율이 표시됩니다. 할당량은 섭취 가능한 오브젝트 데이터의 양을 제한합니다.

> 할당량 활용도는 내부 추정치에 기반하며 경우에 따라 초과될 수 있습니다. 예를 들어, 테넌트가 객체를 업로드하기 시작할 때 StorageGRID는 할당량을 확인하고 테넌트가 할당량을 초과할 경우 새 베스트(ingest)를 거부합니다. 그러나 StorageGRID에서는 할당량이 초과되었는지 확인할 때 현재 업로드 크기를 고려하지 않습니다. 개체를 삭제하면 할당량 활용률이 다시 계산될 때까지 테넌트가 일시적으로 새 개체를 업로드하지 못할 수 있습니다. 할당량 사용률 계산에는 10분 이상이 소요될 수 있습니다.

- 가장 큰 버킷 또는 컨테이너의 상대적 크기를 나타내는 막대 차트.

  차트 세그먼트 위에 커서를 놓으면 해당 버킷이나 컨테이너에서 소비한 전체 공간을 볼 수 있습니다.



- 막대 도표에 대응하려면 총 오브젝트 데이터 양과 각 버킷 또는 컨테이너의 오브젝트 수를 포함하여 가장 큰 버킷 또는 컨테이너의 목록입니다.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  테넌트에 9개 이상의 버킷이나 컨테이너가 있는 경우 다른 모든 버킷이나 컨테이너는 목록 하단의 단일 항목으로 결합됩니다.

할당량 사용 알림을 표시합니다

그리드 관리자에서 할당량 사용 알림이 활성화된 경우 할당량이 낮거나 초과되면 다음과 같이 테넌트 관리자에

표시됩니다.

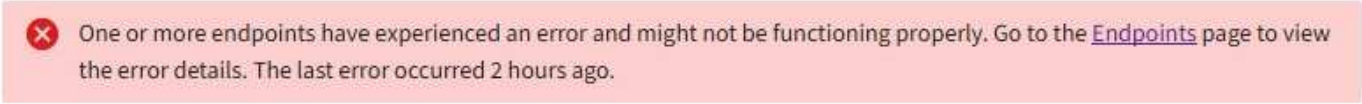
테넌트 할당량의 90% 이상이 사용된 경우 * Tenant quota usage high * 경고가 트리거됩니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 설명서의 경고 참조를 참조하십시오.

할당량을 초과하면 새 객체를 업로드할 수 없습니다.

추가 세부 정보를 보고 알림에 대한 규칙 및 알림을 관리하려면 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

끝점 오류

Grid Manager를 사용하여 플랫폼 서비스에 사용할 하나 이상의 엔드포인트를 구성한 경우 지난 7일 이내에 엔드포인트 오류가 발생한 경우 Tenant Manager 대시보드에 경고가 표시됩니다.



끝점 오류에 대한 세부 정보를 보려면 끝점 을 선택하여 끝점 페이지를 표시합니다.

관련 정보

플랫폼 서비스 끝점 오류 문제 해결

모니터링하고 문제를 해결합니다

테넌트 관리 API

테넌트 관리 API 이해

테넌트 관리자 사용자 인터페이스 대신 테넌트 관리 REST API를 사용하여 시스템 관리 작업을 수행할 수 있습니다. 예를 들어, API를 사용하여 작업을 자동화하거나 사용자와 같은 여러 엔터티를 더 빠르게 생성할 수 있습니다.

테넌트 관리 API:

- Swagger 오픈 소스 API 플랫폼을 사용합니다. Swagger는 개발자와 개발자가 아닌 사용자가 API와 상호 작용할 수 있는 직관적인 사용자 인터페이스를 제공합니다. Swagger 사용자 인터페이스는 각 API 작동에 대한 전체 세부 정보와 문서를 제공합니다.
- 사용 무중단 업그레이드를 지원하는 버전 관리.

테넌트 관리 API에 대한 Swagger 문서에 액세스하려면 다음을 수행합니다.

단계

1. 테넌트 관리자에 로그인합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택하고 * API Documentation * 을 선택합니다.

API 작업

테넌트 관리 API는 사용 가능한 API 작업을 다음 섹션으로 구성합니다.

- * 계정 * — 스토리지 사용 정보를 가져오는 것을 포함하여 현재 테넌트 계정의 작업입니다.
- * auth * — 사용자 세션 인증을 수행하기 위한 작업.

  Tenant Management API는 Bearer Token Authentication Scheme을 지원합니다. 테넌트 로그인의 경우 인증 요청의 JSON 본문에 사용자 이름, 암호 및 accountId를 입력합니다(즉, 'POST/API/v3/authorize'). 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization: Bearer token")에 제공되어야 합니다.

  인증 보안 개선에 대한 자세한 내용은 을 참조하십시오 사이트 간 요청 위조 방지.

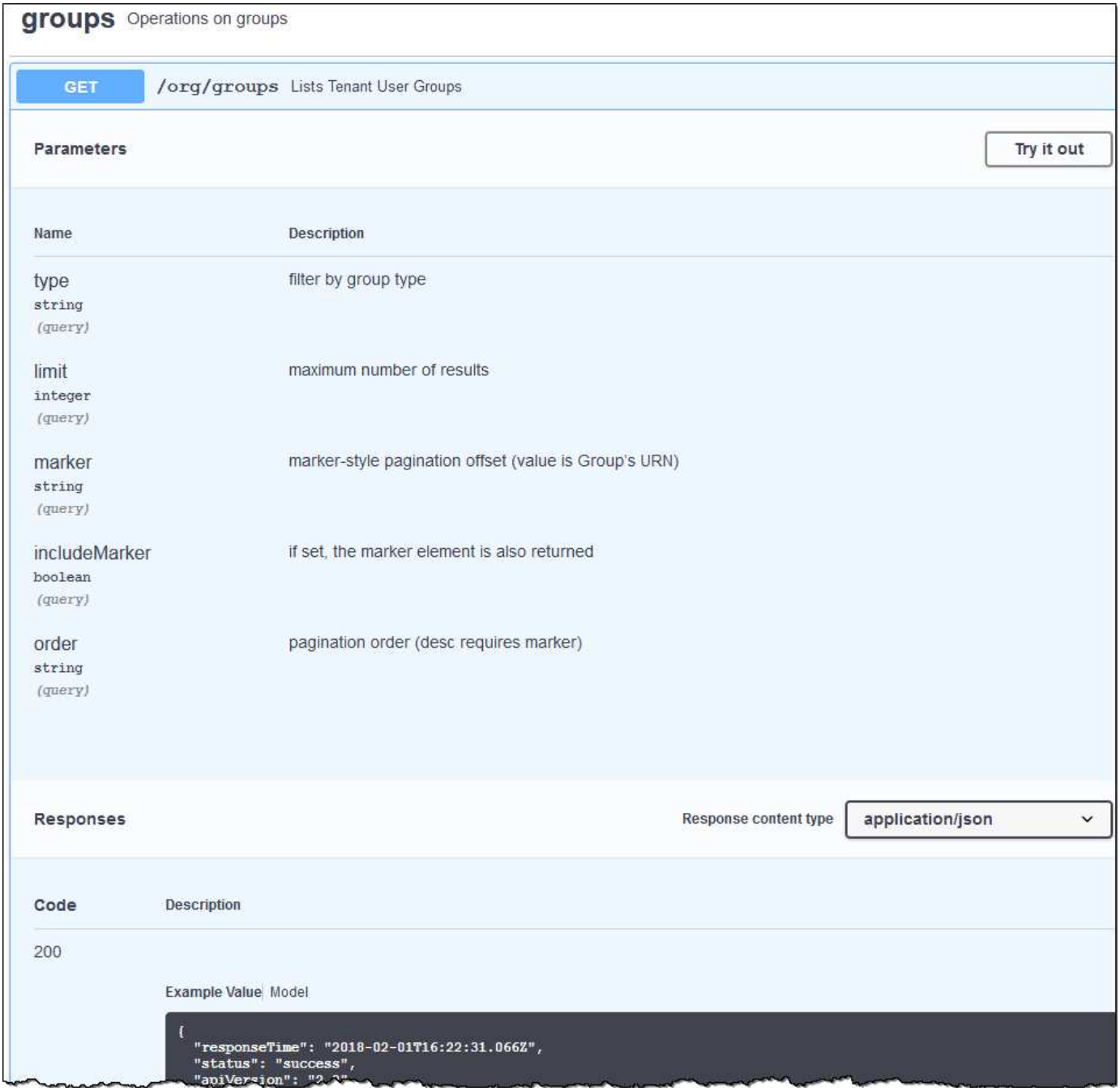
  > StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. 를 참조하십시오 Grid Management API 사용 지침.

- * config * — 제품 릴리스 및 테넌트 관리 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 컨테이너 * — S3 버킷 또는 Swift 컨테이너에서 다음과 같은 작업을 수행합니다.
- S3 *
  - 버킷 생성(S3 오브젝트 잠금이 활성화된 상태 및 활성화되지 않은 상태)
  - 버킷 기본 보존 수정(S3 오브젝트 잠금이 활성화된 버킷의 경우)
  - 객체에 대해 수행되는 작업에 대한 정합성 제어를 설정합니다
  - 버킷의 CORS 구성을 생성, 업데이트 및 삭제합니다
  - 객체에 대한 마지막 액세스 시간 업데이트를 설정 및 해제합니다
  - CloudMirror 복제, 알림 및 검색 통합(메타데이터 알림)을 비롯한 플랫폼 서비스에 대한 구성 설정 관리
  - 빈 버킷을 삭제합니다
- Swift *: 컨테이너에 사용되는 정합성 수준을 설정합니다
- * deactivated - features * — 비활성화된 기능을 보기 위한 작업.
- * 끝점 * — 끝점을 관리하는 작업. 엔드포인트는 S3 버킷이 StorageGRID CloudMirror 복제, 알림 또는 검색 통합에 외부 서비스를 사용할 수 있도록 합니다.
- * 그룹 * — 로컬 테넌트 그룹을 관리하고 외부 ID 소스에서 통합 테넌트 그룹을 검색하는 작업입니다.
- * identity-source * — 외부 ID 소스를 구성하고 통합 그룹 및 사용자 정보를 수동으로 동기화하는 작업.
- * 지역 * — StorageGRID 시스템에 대해 구성된 지역을 결정하는 작업.
- * S3 * — 테넌트 사용자를 위한 S3 액세스 키를 관리하는 운영
- * S3-오브젝트 잠금 * — 글로벌 S3 오브젝트 잠금 설정에서 운영, 규정 준수 지원에 사용됩니다.

- * 사용자 * — 테넌트 사용자를 보고 관리하는 작업.

작업 세부 정보

각 API 작업을 확장하면 HTTP 동작, 끝점 URL, 필수 또는 선택적 매개 변수 목록, 요청 본문(필요한 경우) 예제 및 가능한 응답을 볼 수 있습니다.



API 요청을 발행합니다

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. 요청 세부 정보를 보려면 HTTP 작업을 선택합니다.
2. 요청에 그룹 또는 사용자 ID와 같은 추가 매개 변수가 필요한지 확인합니다. 그런 다음 이 값을 구합니다. 필요한 정보를 얻기 위해 먼저 다른 API 요청을 발급해야 할 수도 있습니다.
3. 예제 요청 본문을 수정해야 하는지 확인합니다. 이 경우 * Model * 을 선택하여 각 필드의 요구 사항을 확인할 수 있습니다.
4. 체험하기 * 를 선택합니다.
5. 필요한 매개 변수를 제공하거나 요청 본문을 필요에 따라 수정합니다.
6. Execute * 를 선택합니다.
7. 응답 코드를 검토하여 요청이 성공했는지 확인합니다.

테넌트 관리 **API** 버전 관리

테넌트 관리 API는 버전 관리를 사용하여 무중단 업그레이드를 지원합니다.

예를 들어 이 요청 URL은 API의 버전 3을 지정합니다.

```
https://hostname_or_ip_address/api/v3/authorize
```

테넌트 관리 API의 주요 버전은 이전 버전과 * _호환되지 않는 _ * 변경 사항이 있을 때 충돌합니다. 테넌트 관리 API의 부 버전은 * _ 이(가) 이전 버전과 호환된다는 변경 사항이 있을 때 충돌합니다. 호환 가능한 변경 사항에는 새 끝점 또는 새 속성 추가가 포함됩니다. 다음 예제에서는 변경 유형에 따라 API 버전을 충돌하는 방법을 보여 줍니다.

API 변경 유형입니다	이전 버전	새 버전
이전 버전과 호환 가능합니다	2.1	2.2
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치하면 가장 최신 버전의 테넌트 관리 API만 활성화됩니다. 그러나 StorageGRID를 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.

오래된 요청은 다음과 같은 방법으로 더 이상 사용되지 않는 것으로 표시됩니다.

- 응답 헤더가 "DEPRECATED:TRUE"입니다.
- JSON 응답 본문에는 "DEPRECATED"가 포함됩니다. TRUE

현재 릴리즈에서 지원되는 **API** 버전을 확인합니다

다음 API 요청을 사용하여 지원되는 API 주요 버전 목록을 반환합니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

요청에 대한 **API** 버전을 지정합니다

PATH 파라미터('/api/v3')나 header('api-Version:3')를 이용하여 API 버전을 지정할 수 있다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

사이트 간 요청 위조(**CSRF**)로부터 보호

CSRF 토큰을 사용하여 쿠키를 사용하는 인증을 강화하면 StorageGRID에 대한 CSRF(사이트 간 요청 위조) 공격으로부터 보호할 수 있습니다. Grid Manager 및 Tenant Manager는 이 보안 기능을 자동으로 활성화합니다. 다른 API 클라이언트는 로그인할 때 활성화 여부를 선택할 수 있습니다.

HTTP 양식 POST와 같이 다른 사이트에 대한 요청을 트리거할 수 있는 공격자는 로그인한 사용자의 쿠키를 사용하여 특정 요청을 만들 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 활성화된 경우 특정 쿠키의 내용은 특정 헤더 또는 특정 POST 본문 매개 변수의 내용과 일치해야 합니다.

이 기능을 활성화하려면 인증 중에 csrfToken 매개 변수를 true로 설정하십시오. 기본값은 false 입니다.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

true이면 Grid Manager에 로그인할 때 임의의 값으로 GridCsrfToken 쿠키가 설정되고 테넌트 관리자에 로그인할 때

임의의 값으로 AccountCsrfToken 쿠키가 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- CSRF 토큰 쿠키의 값으로 설정된 헤더의 X-CSRF-Token 헤더입니다.
- 폼 인코딩된 본문을 허용하는 끝점의 경우 "csrfToken" 형식 인코딩된 요청 본문 매개 변수입니다.

CSRF 보호를 구성하려면 를 사용합니다 Grid Management API를 참조하십시오 또는 테넌트 관리 API.

> CSRF 토큰 쿠키 세트를 가진 요청은 또한 JSON 요청 본문을 CSRF 공격에 대한 추가 보호로서 기대하는 모든 요청에 대해 ""Content-Type:application/json"" 헤더를 적용합니다.

시스템 액세스를 관리합니다

ID 페더레이션을 사용합니다

ID 페더레이션을 사용하면 테넌트 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 테넌트 사용자는 익숙한 자격 증명을 사용하여 테넌트 계정에 로그인할 수 있습니다.

테넌트 관리자에 대한 ID 페더레이션을 구성합니다

테넌트 그룹 및 사용자를 Active Directory, Azure Active Directory(Azure AD), OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하도록 하려면 테넌트 관리자에 대한 ID 페더레이션을 구성할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

  > 목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

- OpenLDAP를 사용하려면 OpenLDAP 서버를 구성해야 합니다. 을 참조하십시오 OpenLDAP 서버 구성 지침.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다. 을 참조하십시오 발신 TLS 연결에 지원되는 암호.

이 작업에 대해

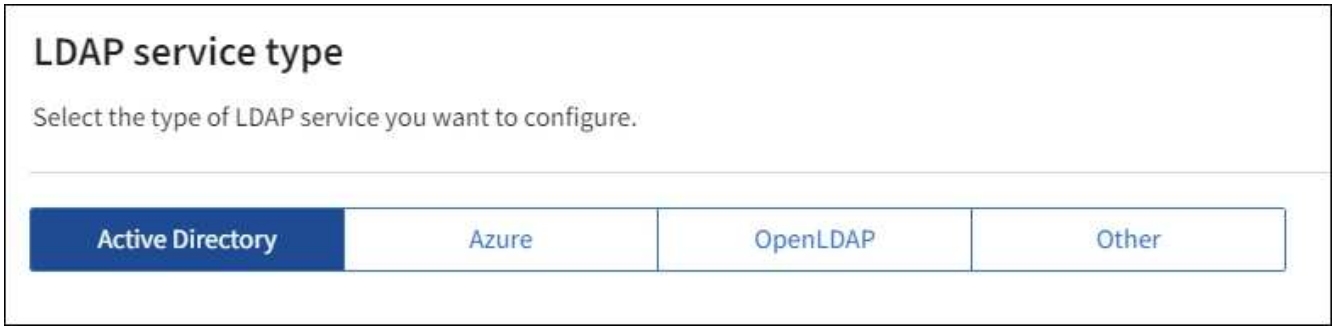
테넌트의 ID 페더레이션 서비스를 구성할 수 있는지 여부는 테넌트 계정 설정 방법에 따라 달라집니다. 테넌트가 Grid Manager용으로 구성된 ID 페더레이션 서비스를 공유할 수 있습니다. ID 페더레이션 페이지에 액세스할 때 이 메시지가 표시되면 이 테넌트에 대해 별도의 통합 ID 소스를 구성할 수 없습니다.

> This tenant account uses the LDAP server that is configured for the Grid Manager.
> Contact the grid administrator for information or to change this setting.

구성을 입력합니다

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.



Oracle Directory Server를 사용하는 LDAP 서버의 값을 구성하려면 * 기타 * 를 선택합니다.

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다. 그렇지 않으면 다음 단계로 이동합니다.
   - * 사용자 고유 이름 *: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 Active Directory의 경우 'AMAccountName', OpenLDAP의 경우 'uid'와 같습니다. Oracle Directory Server를 구성하는 경우 "uid"를 입력합니다.
   - * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory의 경우 objectGUID, OpenLDAP의 경우 entryUUID와 같습니다. Oracle Directory Server를 구성하는 경우 "n스uniqueid"를 입력합니다. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
   - * 그룹 고유 이름 *: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 Active Directory의 경우 'AMAccountName', OpenLDAP의 경우 'cn'과 같습니다. Oracle Directory Server를 구성하는 경우 cn을 입력합니다.
   - * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory의 경우 objectGUID, OpenLDAP의 경우 entryUUID와 같습니다. Oracle Directory Server를 구성하는 경우 "n스uniqueid"를 입력합니다. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.
   - * 호스트 이름 *: LDAP 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
   - * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다.

     STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.

   - * 사용자 이름 *: LDAP 서버에 연결할 사용자의 DN(고유 이름)의 전체 경로입니다.

     Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

        - '사계정 이름' 또는 'uid'
        - objectGUID, entryUUID, n스uniqueid
        - 'cn'입니다
        - 'emberOf' 또는 'isMemberOf'
        - Active Directory *: objectSid, primaryGroupID, userAccountControl, userPrincipalName
        - * Azure *:'accountEnabled' 및 'userPrincipalName'
    - * 암호 *: 사용자 이름과 연결된 암호입니다.
    - * Group Base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.

      > 그룹 고유 이름 * 값은 * 그룹 기본 DN * 내에서 고유해야 합니다.

    - * 사용자 기본 DN *: 사용자를 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

      > 사용자 고유 이름 * 값은 * 사용자 기본 DN * 내에서 고유해야 합니다.

    - * 사용자 이름 형식 바인딩 * (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 기본 사용자 이름 패턴을 사용해야 합니다.

      StorageGRID가 서비스 계정에 바인딩할 수 없는 경우 사용자가 로그인할 수 있으므로 * 사용자 이름 형식 바인딩 * 을 제공하는 것이 좋습니다.

      다음 패턴 중 하나를 입력합니다.

        - * UserPrincipalName 패턴(Active Directory 및 Azure) *: '[UserName]@*example*.com'
        - * 하위 수준 로그온 이름 패턴(Active Directory 및 Azure) *: `*example*\[사용자 이름]'
        - * 고유 이름 패턴 *:'CN=[UserName],CN=Users,DC=*Example*,DC=com'

          [UserName] * 을 서면 그대로 포함합니다.

6. TLS(전송 계층 보안) 섹션에서 보안 설정을 선택합니다.
    - * STARTTLS 사용 *: STARTTLS를 사용하여 LDAP 서버와의 통신 보안을 설정합니다. 이 옵션은 Active Directory, OpenLDAP 또는 기타 에 대해 권장되지만 Azure에서는 지원되지 않습니다.
    - * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. Azure의 경우 이 옵션을 선택해야 합니다.
    - * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Azure에서 지원되지 않습니다.

      > Active Directory 서버가 LDAP 서명을 적용하는 경우 * TLS 사용 안 함 * 옵션을 사용할 수 없습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.
    - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.

- * 사용자 지정 CA 인증서 사용 *: 사용자 지정 보안 인증서를 사용합니다.

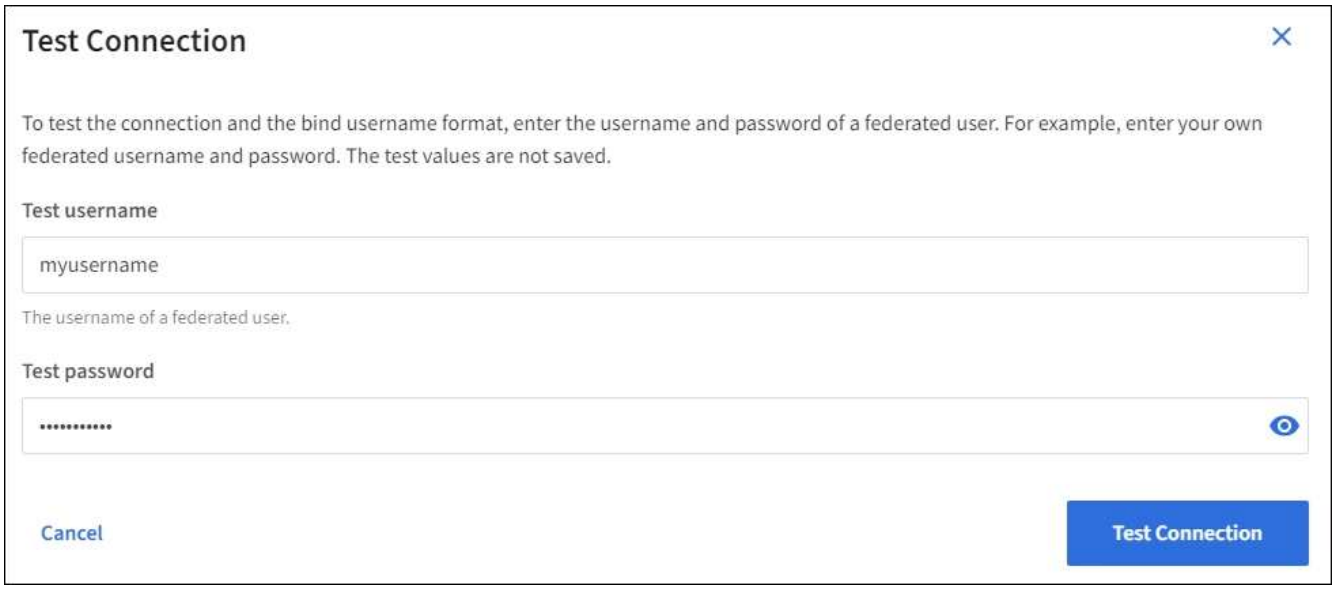
  이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 CA 인증서 텍스트 상자에 붙여 넣습니다.

연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버에 대한 연결 설정과 바인딩 사용자 이름 형식(제공한 경우)을 확인합니다.

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정이 잘못된 경우 ""테스트 연결을 설정할 수 없습니다"" 메시지가 나타납니다. 닫기 * 를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트합니다.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 통합 사용자의 사용자 이름과 암호를 입력합니다.

   예를 들어 사용자 이름과 암호를 입력합니다. @ 또는 / 같은 특수 문자를 사용자 이름에 포함하지 마십시오.



   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름과 암호가 올바르지 않으면 오류 메시지가 나타납니다. 모든 문제를 해결하고 연결을 다시 테스트합니다.

ID 소스와 강제로 동기화합니다

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹과 사용자를 정기적으로 동기화합니다. 사용자 권한을 최대한 빨리 설정하거나 제한하려는 경우 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 페더레이션 페이지로 이동합니다.

2. 페이지 맨 위에서 * 서버 동기화 * 를 선택합니다.

   동기화 프로세스는 환경에 따라 다소 시간이 걸릴 수 있습니다.

   ID 소스에서 페더레이션 그룹과 사용자를 동기화하는 데 문제가 있는 경우 * ID 페더레이션 동기화 실패 * 경고가 트리거됩니다.

ID 페더레이션을 비활성화합니다

그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 사용하지 않도록 설정하면 StorageGRID와 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않으며 동기화되지 않은 계정에 대해 알림 또는 경보가 발생하지 않습니다.
- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable identity federation *(ID 페더레이션 사용 *) 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 참조하십시오 SSO(Single Sign-On)를 비활성화합니다.

단계

1. ID 페더레이션 페이지로 이동합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.

OpenLDAP 서버 구성 지침

OpenLDAP 서버를 ID 페더레이션에 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

ActiveDirectory 또는 Azure가 아닌 ID 소스의 경우 StorageGRID는 외부에서 비활성화된 사용자에 대한 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 사용자의 S3 키를 삭제하고 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 의 역방향 그룹 구성원 유지 관리 지침을 참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- olcDbIndex:objectClass eq
- "olcDbIndex:uid eq,pres,sub'

- 올크DbIndex=cn eq,pres,sub
- olcDbIndex: entryUUID eq

또한 최적의 성능을 위해 사용자 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

에서 역방향 그룹 구성원 유지 관리에 대한 정보를 참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

그룹을 관리합니다

S3 테넌트에 대한 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹에 대한 권한을 관리할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

S3에 대한 자세한 내용은 을 참조하십시오 S3을 사용합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. Create group * 을 선택합니다.
3. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

4. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 'AMAccountName' 속성과 관련된 이름입니다. OpenLDAP의 경우 고유 이름은 "uid" 특성과 관련된 이름입니다.
5. Continue * 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
   - * 읽기-쓰기 * (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.
7. 이 그룹에 대한 그룹 권한을 선택합니다.

   테넌트 관리 권한에 대한 정보를 참조하십시오.
8. Continue * 를 선택합니다.
9. 그룹 정책을 선택하여 이 그룹의 구성원이 가질 S3 액세스 권한을 결정합니다.
   - * S3 액세스 없음 *: 기본값. 이 그룹의 사용자는 버킷 정책을 통해 액세스가 부여되지 않는 한 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
   - * 읽기 전용 액세스 *: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
   - * 전체 액세스 *: 이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
   - * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다. 언어 구문 및 예제를 비롯한 그룹 정책에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.
10. 사용자 정의 * 를 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책은 크기 제한이 5,120바이트입니다. 올바른 JSON 형식 문자열을 입력해야 합니다.

    이 예제에서 그룹 구성원은 지정된 버킷의 사용자 이름(키 접두사)과 일치하는 폴더만 나열하고 액세스할 수 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.

11. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.

    - 통합 그룹: * 그룹 생성 *
    - 로컬 그룹: * 계속 *

    로컬 그룹을 만드는 경우 * Continue * 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

12. 그룹에 추가할 각 사용자에 대한 확인란을 선택한 다음 * 그룹 생성 * 을 선택합니다.

    필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 추가할 때 그룹을 선택할 수 있습니다.

13. 마침 * 을 선택합니다.

    생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

Swift 테넌트의 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 Swift 테넌트 계정에 대한 액세스 권한을 관리할 수 있습니다. 하나 이상의 그룹에 Swift 관리자 권한이 있어야 합니다. 이 권한은 Swift 테넌트 계정의 컨테이너 및 개체를 관리하는 데 필요합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. Create group * 을 선택합니다.
3. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

4. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 'AMAccountName' 속성과 관련된 이름입니다. OpenLDAP의 경우 고유 이름은 "uid" 특성과 관련된 이름입니다.
5. Continue * 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
   - * 읽기-쓰기 * (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.
7. 그룹 권한을 설정합니다.
   - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 로그인해야 하는 경우 * Root Access * 확인란을 선택합니다. (기본값)
   - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 액세스할 필요가 없는 경우 * Root Access * (루트 액세스 *) 확인란의 선택을 취소합니다. 예를 들어, 테넌트에 액세스할 필요가 없는 응용 프로그램의 확인란을 선택

취소합니다. 그런 다음 이러한 사용자가 컨테이너 및 개체를 관리할 수 있도록 * Swift 관리자 * 권한을 할당합니다.

8. Continue * 를 선택합니다.
9. 사용자가 Swift REST API를 사용할 수 있어야 하는 경우 * Swift administrator * 확인란을 선택합니다.

   Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한은 사용자가 Swift REST API에 인증하여 컨테이너를 생성하고 객체를 수집하는 것을 허용하지 않습니다. 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

10. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.
    - 통합 그룹: * 그룹 생성 *
    - 로컬 그룹: * 계속 *

      로컬 그룹을 만드는 경우 * Continue * 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

11. 그룹에 추가할 각 사용자에 대한 확인란을 선택한 다음 * 그룹 생성 * 을 선택합니다.

    필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 만들 때 그룹을 선택할 수 있습니다.

12. 마침 * 을 선택합니다.

    생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

테넌트 관리 권한

Swift를 사용합니다

테넌트 관리 권한

테넌트 그룹을 생성하기 전에 해당 그룹에 할당할 권한을 고려하십시오. 테넌트 관리 권한은 사용자가 테넌트 관리자 또는 테넌트 관리 API를 사용하여 수행할 수 있는 작업을 결정합니다. 사용자는 하나 이상의 그룹에 속할 수 있습니다. 사용자가 여러 그룹에 속한 경우 권한은 누적됩니다.

테넌트 관리자에 로그인하거나 테넌트 관리 API를 사용하려면 사용자가 하나 이상의 권한이 있는 그룹에 속해야 합니다. 로그인할 수 있는 모든 사용자는 다음 작업을 수행할 수 있습니다.

- 대시보드 보기
- 자신의 암호 변경(로컬 사용자의 경우)

모든 권한에 대해 그룹의 액세스 모드 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정과 기능만 볼 수 있는지 여부를 결정합니다.

> 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

그룹에 다음 권한을 할당할 수 있습니다. S3 테넌트와 Swift 테넌트는 다른 그룹 권한을 가집니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

권한	설명
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다. • 참고: * Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.
관리자	Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다 • 참고: * Swift 사용자는 Swift REST API를 사용하여 모든 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.
자신의 S3 자격 증명을 관리합니다	S3 테넌트만 해당. 사용자가 자신의 S3 액세스 키를 생성하고 제거할 수 있습니다. 이 권한이 없는 사용자는 * storage(S3) * > * My S3 access keys * 메뉴 옵션을 볼 수 없습니다.
모든 버킷 관리	• S3 테넌트: 사용자가 테넌트 관리자 및 테넌트 관리 API를 사용하여 S3 버킷을 생성 및 삭제하고 S3 버킷 또는 그룹 정책에 관계없이 테넌트 계정의 모든 S3 버킷을 관리할 수 있습니다. 이 권한이 없는 사용자는 * Bucket * 메뉴 옵션을 볼 수 없습니다. • Swift 테넌트: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 정합성 수준을 제어할 수 있습니다. • 참고: * 테넌트 관리 API에서 Swift 그룹에만 모든 버킷 관리 권한을 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.
엔드포인트 관리	S3 테넌트만 해당. 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID 플랫폼 서비스의 대상으로 사용되는 엔드포인트를 생성하거나 편집할 수 있습니다. 이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션을 볼 수 없습니다.

관련 정보

S3을 사용합니다

Swift를 사용합니다

그룹 세부 정보를 보고 편집합니다

그룹의 세부 정보를 볼 때 그룹의 표시 이름, 사용 권한, 정책 및 그룹에 속한 사용자를 변경할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 세부 정보를 보거나 편집할 그룹의 이름을 선택합니다.

   또는 * Actions * > * View group details * 를 선택할 수 있습니다.

   그룹 세부 정보 페이지가 나타납니다. 다음 예에서는 S3 그룹 세부 정보 페이지를 보여 줍니다.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. 필요에 따라 그룹 설정을 변경합니다.

> 변경 내용을 저장하려면 각 섹션을 변경한 후 * 변경 사항 저장 * 을 선택합니다. 변경 내용이 저장되면 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

   a. 선택적으로 표시 이름 또는 편집 아이콘을 선택합니다 표시 이름을 업데이트합니다.

      그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

   b. 필요에 따라 사용 권한을 업데이트합니다.

   c. 그룹 정책의 경우 S3 또는 Swift 테넌트를 적절하게 변경합니다.

      - S3 테넌트의 그룹을 편집하는 경우 선택적으로 다른 S3 그룹 정책을 선택합니다. 사용자 지정 S3 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
      - Swift 테넌트의 그룹을 편집하는 경우, 필요에 따라 * Swift 관리자 * 확인란을 선택하거나 선택 취소합니다.

        Swift 관리자 권한에 대한 자세한 내용은 Swift 테넌트에 대한 그룹 생성 지침을 참조하십시오.

   d. 필요에 따라 사용자를 추가 또는 제거합니다.

4. 변경한 각 섹션에 대해 * 변경 사항 저장 * 을 선택했는지 확인합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

S3 테넌트용 그룹을 생성합니다

Swift 테넌트용 그룹을 생성합니다

로컬 그룹에 사용자를 추가합니다

필요에 따라 로컬 그룹에 사용자를 추가할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 사용자를 추가할 로컬 그룹의 이름을 선택합니다.

   또는 * Actions * > * View group details * 를 선택할 수 있습니다.

   그룹 세부 정보 페이지가 나타납니다.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

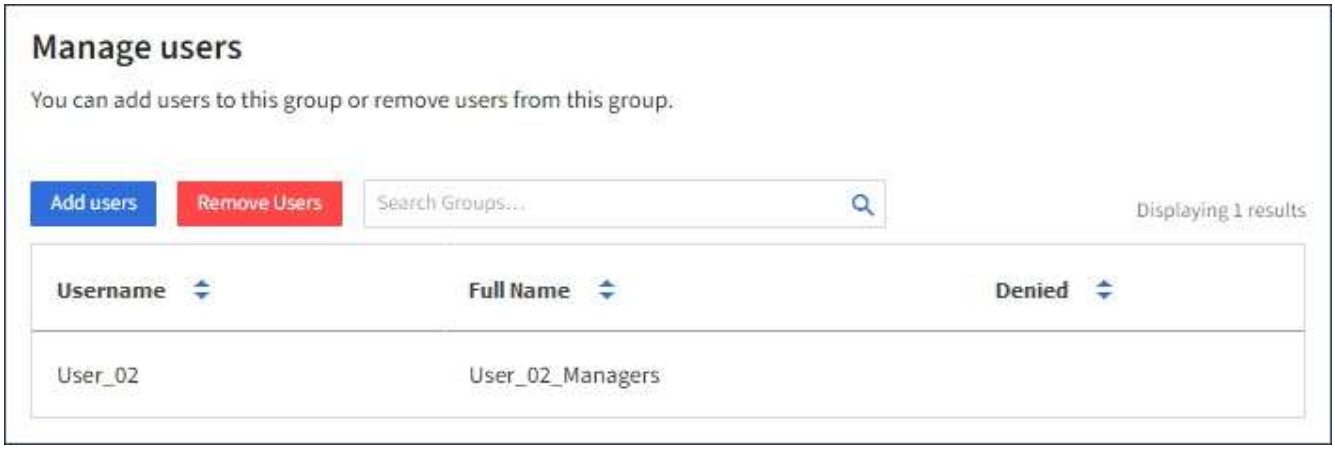
Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

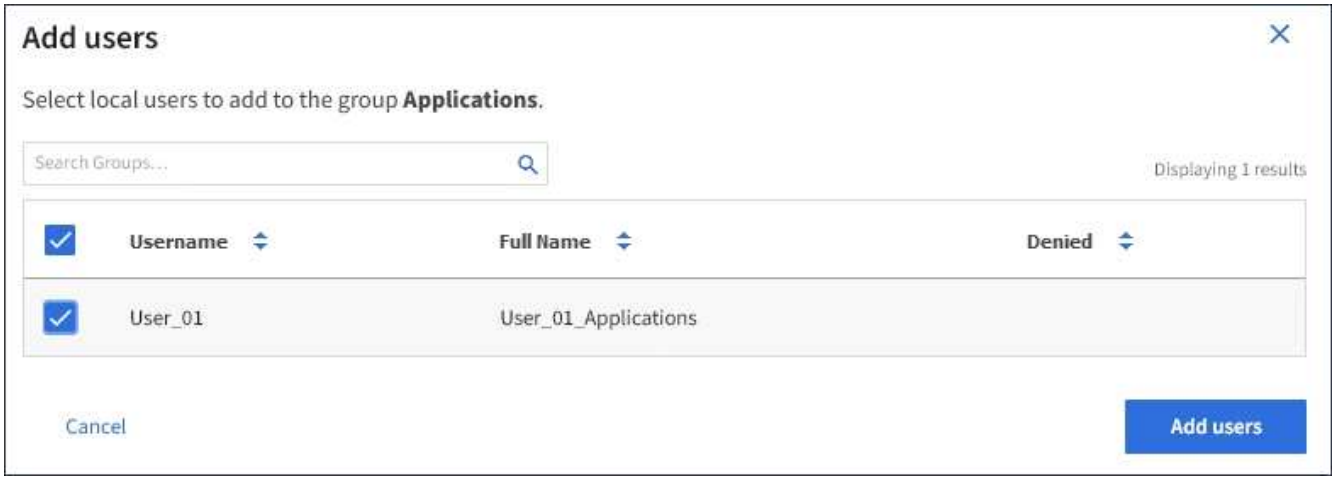
Allows users to create and delete their own S3 access keys.

Save changes

3. 사용자 * 를 선택한 다음 * 사용자 추가 * 를 선택합니다.



4. 그룹에 추가할 사용자를 선택한 다음 * 사용자 추가 * 를 선택합니다.



페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

그룹 이름을 편집합니다

그룹의 표시 이름을 편집할 수 있습니다. 그룹의 고유한 이름은 편집할 수 없습니다.

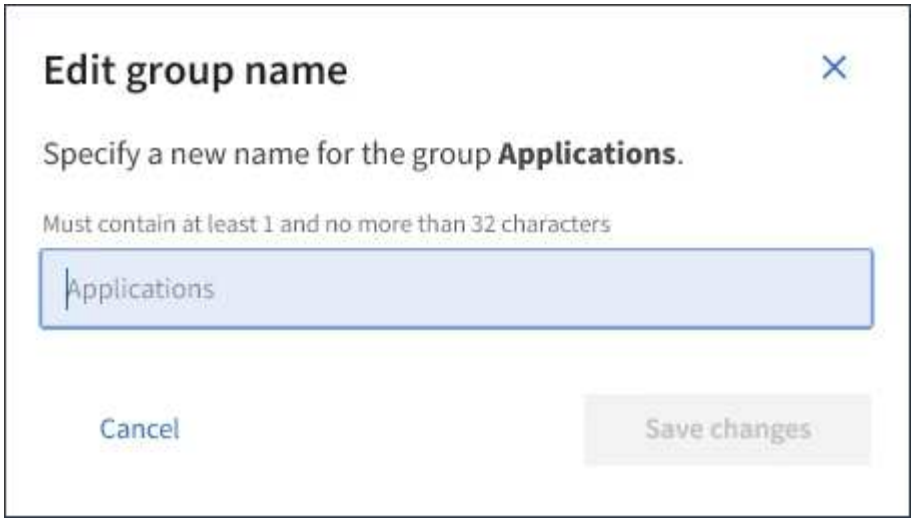
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 표시 이름을 편집할 그룹의 확인란을 선택합니다.
3. Actions * > * Edit group name * 을 선택합니다.

   Edit group name(그룹 이름 편집) 대화 상자가 나타납니다.



4. 로컬 그룹을 편집하는 경우 필요에 따라 표시 이름을 업데이트합니다.

   그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

5. 변경 내용 저장 * 을 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

그룹이 중복되었습니다

기존 그룹을 복제하면 새 그룹을 더 빠르게 만들 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 복제할 그룹의 확인란을 선택합니다.
3. Duplicate group * 을 선택합니다. 그룹 만들기에 대한 자세한 내용은 에 대한 그룹 만들기 지침을 참조하십시오 S3 테넌트 또는 을(를) 선택합니다 Swift 테넌트입니다.
4. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 그룹에 속하는 사용자는 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다. 그룹 권한에 따라 다릅니다.

5. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 'AMAccountName' 속성과 관련된 이름입니다. OpenLDAP의 경우 고유 이름은 "uid" 특성과 관련된 이름입니다.

6. Continue * 를 선택합니다.
7. 필요에 따라 이 그룹에 대한 권한을 수정합니다.
8. Continue * 를 선택합니다.
9. 필요에 따라 S3 테넌트에 대한 그룹을 복제할 경우 * S3 정책 추가 * 라디오 버튼에서 다른 정책을 선택할 수도 있습니다. 사용자 지정 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
10. Create group * 을 선택합니다.

그룹을 삭제합니다

시스템에서 그룹을 삭제할 수 있습니다. 해당 그룹에만 속하는 사용자는 더 이상 테넌트 관리자에 로그인하거나 테넌트 계정을 사용할 수 없습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. 삭제할 그룹의 확인란을 선택합니다.
3. Actions * > * Delete group * 을 선택합니다.

   확인 메시지가 나타납니다.

4. 확인 메시지에 표시된 그룹을 삭제하려면 * Delete group * 을 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자를 관리합니다

로컬 사용자를 만들고 로컬 그룹에 할당하여 사용자가 액세스할 수 있는 기능을 결정할 수 있습니다. Tenant Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 한 명 있습니다. 로컬 사용자를 추가 및 제거할 수는 있지만 루트 사용자는 제거할 수 없습니다.

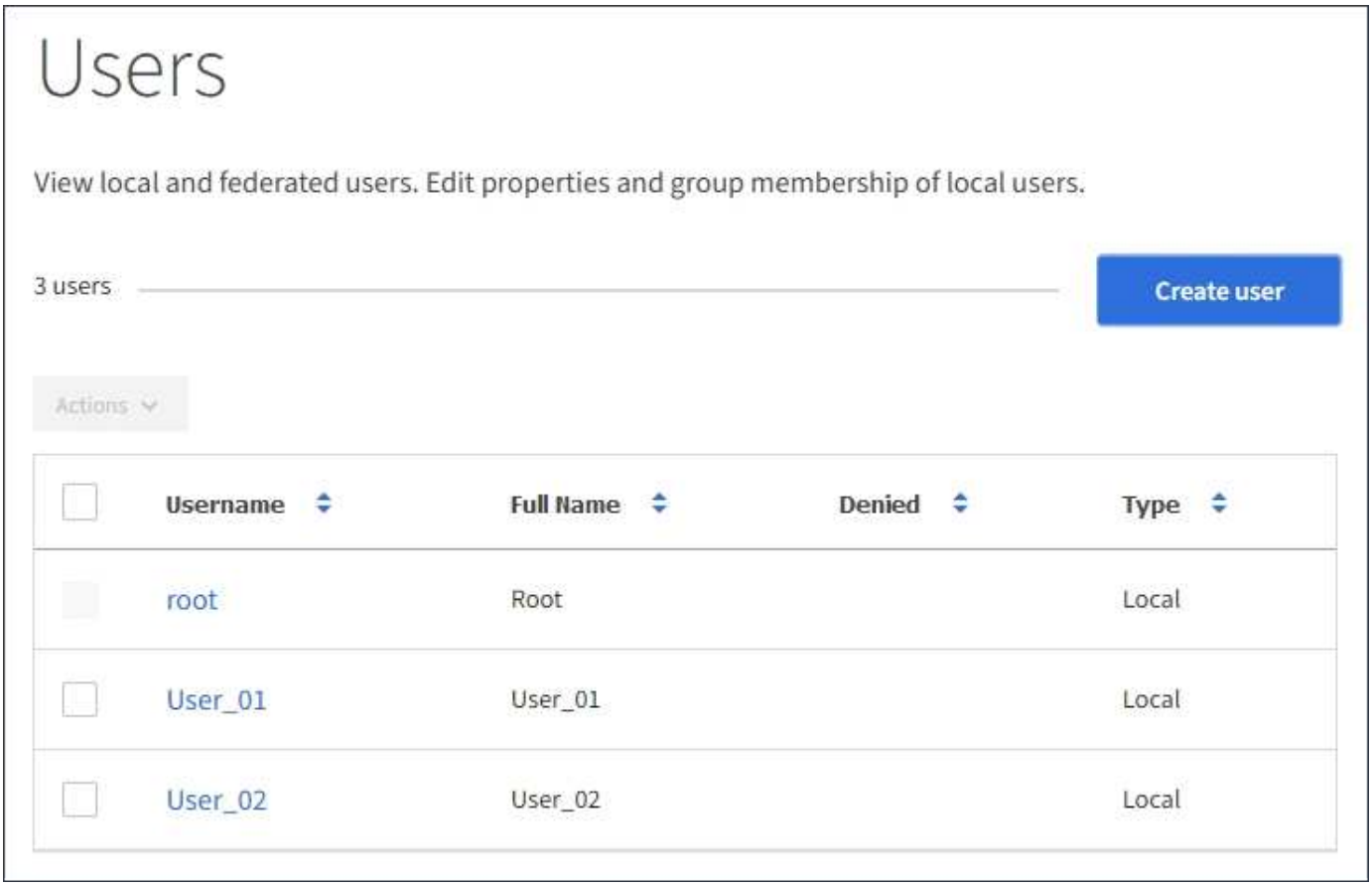
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 읽기-쓰기 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

> StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 그룹 사용 권한에 따라 S3 또는 Swift 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 수 있지만 로컬 사용자는 테넌트 관리자 또는 테넌트 관리 API에 로그인할 수 없습니다.

사용자 페이지에 액세스합니다

액세스 관리 * > * 사용자 * 를 선택합니다.



로컬 사용자를 생성합니다

로컬 사용자를 만들고 하나 이상의 로컬 그룹에 할당하여 액세스 권한을 제어할 수 있습니다.

그룹에 속하지 않은 S3 사용자는 관리 권한이나 S3 그룹 정책이 적용되지 않습니다. 이러한 사용자는 버킷 정책을 통해 S3 버킷 액세스가 부여될 수 있습니다.

그룹에 속하지 않는 Swift 사용자는 관리 권한이나 Swift 컨테이너 액세스 권한이 없습니다.

단계

1. 사용자 생성 * 을 선택합니다.
2. 다음 필드를 작성합니다.
   - * 전체 이름 *: 이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램 이름)입니다.
   - * 사용자 이름 *: 이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다.
   - * 암호 * : 사용자가 로그인할 때 사용하는 암호입니다.
   - * 암호 확인 *: 암호 필드에 입력한 것과 동일한 암호를 입력합니다.
   - * 액세스 거부 *: * 예 * 를 선택하면 사용자가 하나 이상의 그룹에 속해 있더라도 이 사용자는 테넌트 계정에 로그인할 수 없습니다.

     예를 들어 이 기능을 사용하여 사용자의 로그인 기능을 일시적으로 중단할 수 있습니다.
3. Continue * 를 선택합니다.
4. 사용자를 하나 이상의 로컬 그룹에 할당합니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다.
5. 사용자 생성 * 을 선택합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

사용자 세부 정보를 편집합니다

사용자의 세부 정보를 편집할 때 사용자의 전체 이름과 암호를 변경하고, 사용자를 다른 그룹에 추가하고, 사용자가 테넌트에 액세스하지 못하도록 할 수 있습니다.

단계

1. 사용자 목록에서 세부 정보를 보거나 편집할 사용자의 이름을 선택합니다.

   또는 사용자의 확인란을 선택한 다음 * Actions * > * View user details * 를 선택합니다.
2. 필요에 따라 사용자 설정을 변경합니다.
   a. 필요에 따라 전체 이름 또는 편집 아이콘을 선택하여 사용자의 전체 이름을 변경합니다 개요 섹션.

      사용자 이름은 변경할 수 없습니다.
   b. 암호 * 탭에서 필요에 따라 사용자 암호를 변경합니다.
   c. Access * 탭에서 사용자가 로그인(* 아니요 * 선택)하거나 사용자가 필요에 따라 로그인하지 못하도록 합니다(* 예 * 선택).
   d. 그룹 * 탭에서 사용자를 그룹에 추가하거나 필요에 따라 그룹에서 사용자를 제거합니다.
   e. 각 섹션에 필요한 경우 * 변경 사항 저장 * 을 선택합니다.

캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자가 중복되었습니다

로컬 사용자를 복제하면 새 사용자를 보다 빠르게 만들 수 있습니다.

단계

1. 사용자 목록에서 복제할 사용자를 선택합니다.
2. 사용자 복제 * 를 선택합니다.
3. 새 사용자에 대해 다음 필드를 수정합니다.
   - * 전체 이름 *: 이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램 이름)입니다.
   - * 사용자 이름 *: 이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다.
   - * 암호 * : 사용자가 로그인할 때 사용하는 암호입니다.
   - * 암호 확인 *: 암호 필드에 입력한 것과 동일한 암호를 입력합니다.
   - * 액세스 거부 *: * 예 * 를 선택하면 사용자가 하나 이상의 그룹에 속해 있더라도 이 사용자는 테넌트 계정에 로그인할 수 없습니다.

     예를 들어 이 기능을 사용하여 사용자의 로그인 기능을 일시적으로 중단할 수 있습니다.
4. Continue * 를 선택합니다.
5. 하나 이상의 로컬 그룹을 선택합니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다.
6. 사용자 생성 * 을 선택합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자를 삭제합니다

StorageGRID 테넌트 계정에 더 이상 액세스할 필요가 없는 로컬 사용자를 영구적으로 삭제할 수 있습니다.

테넌트 관리자를 사용하여 로컬 사용자는 삭제할 수 있지만 페더레이션 사용자는 삭제할 수 없습니다. 통합 사용자를 삭제하려면 통합 ID 소스를 사용해야 합니다.

단계

1. 사용자 목록에서 삭제할 로컬 사용자의 확인란을 선택합니다.
2. Actions * > * Delete user * 를 선택합니다.
3. 확인 대화 상자에서 * 사용자 삭제 * 를 선택하여 시스템에서 사용자를 삭제할 것인지 확인합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

S3 테넌트 계정 관리

S3 액세스 키를 관리합니다

S3 테넌트 계정의 각 사용자는 StorageGRID 시스템에 오브젝트를 저장하고 검색하기 위한 액세스 키가 있어야 합니다. 액세스 키는 액세스 키 ID와 비밀 액세스 키로 구성됩니다.

이 작업에 대해

S3 액세스 키는 다음과 같이 관리할 수 있습니다.

- 자신의 S3 자격 증명 관리 * 권한이 있는 사용자는 자신의 S3 액세스 키를 생성하거나 제거할 수 있습니다.
- 루트 액세스* 권한이 있는 사용자는 S3 루트 계정 및 다른 모든 사용자의 액세스 키를 관리할 수 있습니다. 루트 액세스 키는 버킷 정책에 의해 명시적으로 비활성화되지 않는 한 테넌트의 모든 버킷과 객체에 대한 전체 액세스를 제공합니다.

StorageGRID는 서명 버전 2 및 서명 버전 4 인증을 지원합니다. 버킷 정책에 의해 명시적으로 활성화되지 않은 경우 교차 계정 액세스가 허용되지 않습니다.

자체 S3 액세스 키를 생성합니다

S3 테넌트를 사용 중이며 적절한 권한이 있는 경우 자체 S3 액세스 키를 생성할 수 있습니다. S3 테넌트 계정의 버킷 및 오브젝트에 액세스하려면 액세스 키가 있어야 합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있어야 합니다. 을 참조하십시오 테넌트 관리 권한.

이 작업에 대해

하나 이상의 S3 액세스 키를 생성하여 테넌트 계정의 버킷을 생성하고 관리할 수 있습니다. 새 액세스 키를 생성한 후 새 액세스 키 ID와 비밀 액세스 키로 응용 프로그램을 업데이트합니다. 보안을 위해 필요한 것보다 더 많은 키를 생성하지 말고 사용하지 않는 키를 삭제하십시오. 하나의 키만 있고 만료되려고 하는 경우 이전 키가 만료되기 전에 새 키를 만든 다음 이전 키를 삭제합니다.

각 키에는 특정 만료 시간 또는 만료 기간이 있을 수 있습니다. 만료 시간에 대한 다음 지침을 따르십시오.

- 키의 만료 시간을 설정하여 특정 기간에 대한 액세스를 제한합니다. 만료 시간을 짧게 설정하면 액세스 키 ID 및 비밀 액세스 키가 실수로 노출되었을 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 제거됩니다.
- 환경의 보안 위험이 낮으며 정기적으로 새 키를 만들 필요가 없는 경우 키에 대한 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 만들려면 이전 키를 수동으로 삭제합니다.

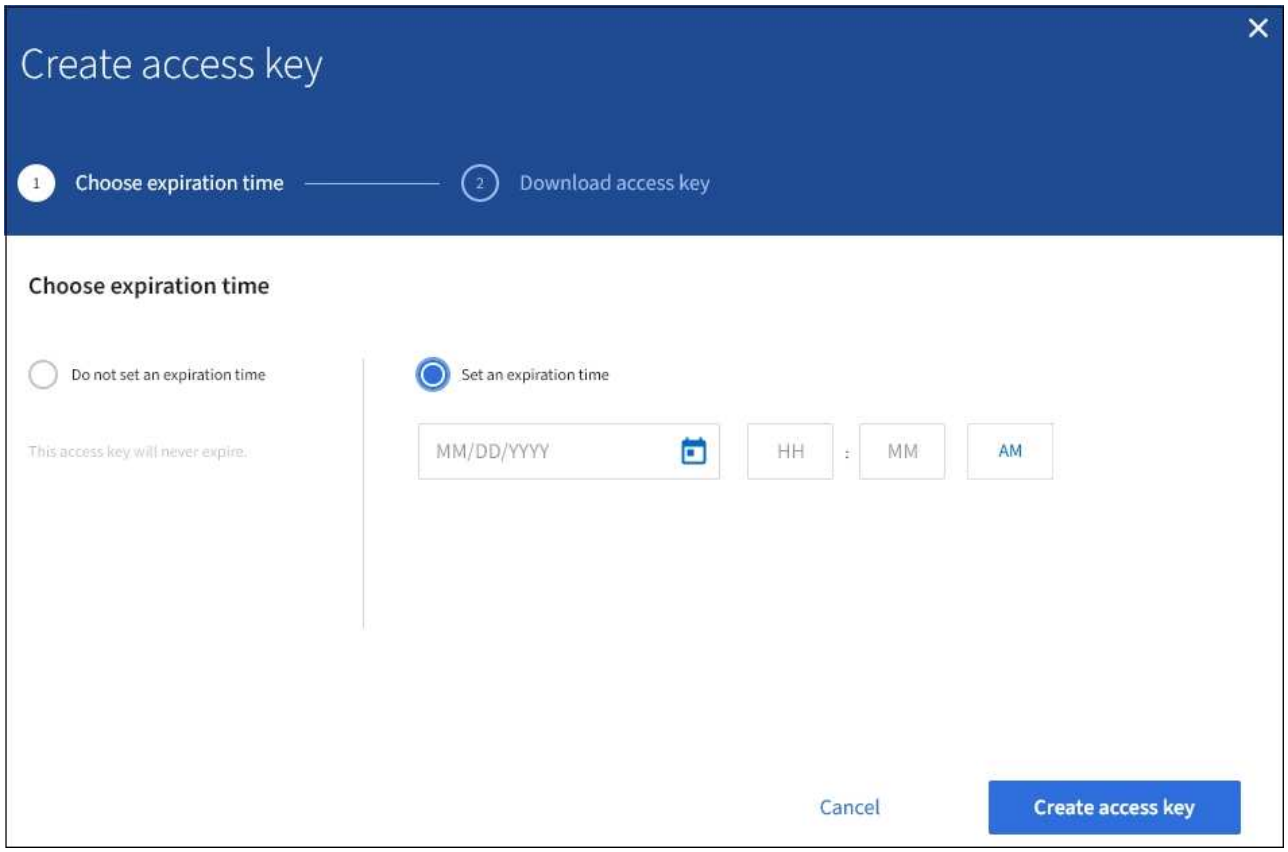
> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

2. Create key * 를 선택합니다.
3. 다음 중 하나를 수행합니다.
   - 만료 시간을 설정하지 않음 * 을 선택하여 만료되지 않는 키를 생성합니다. (기본값)
   - 만료 시간 설정 * 을 선택하고 만료 날짜 및 시간을 설정합니다.

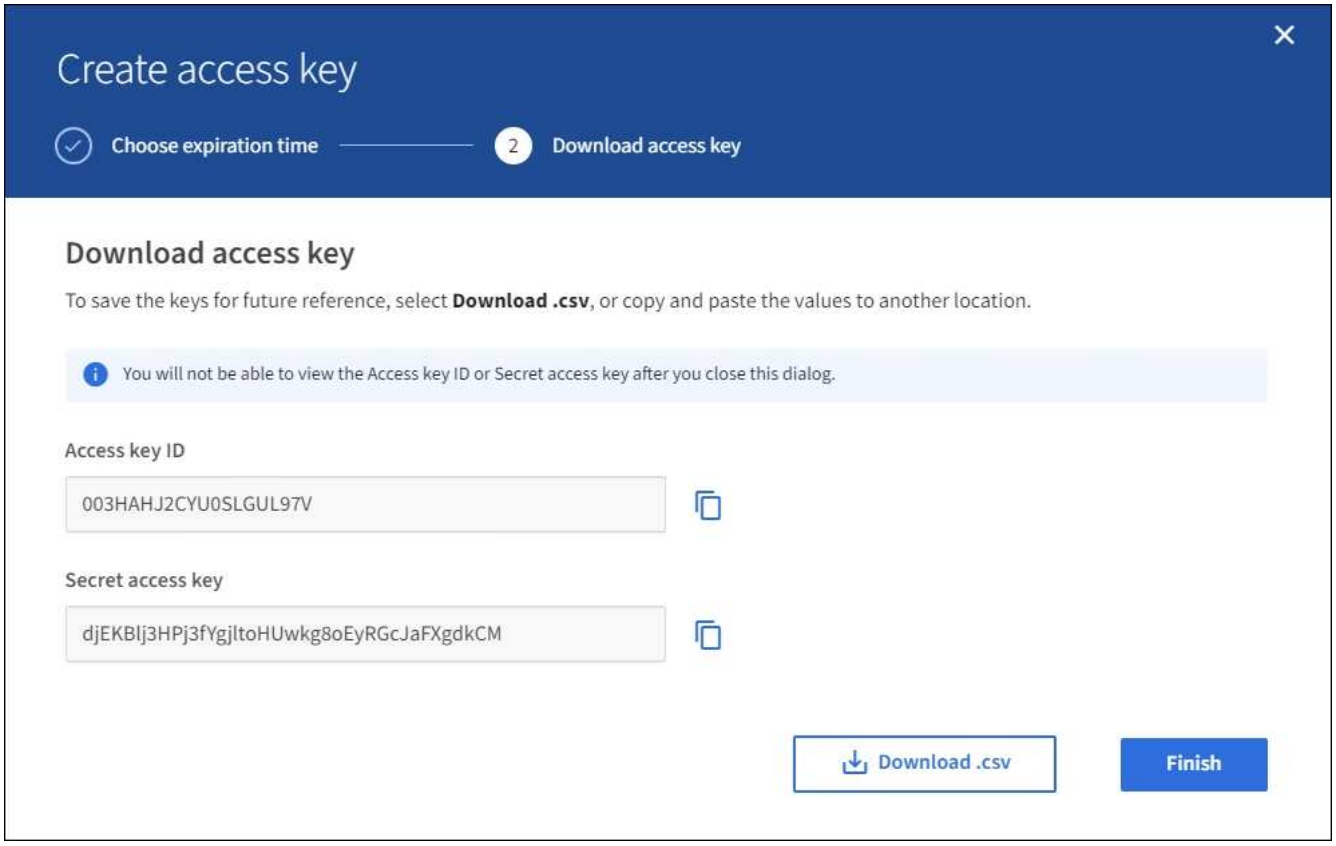


4. Create access key * 를 선택합니다.

   액세스 키 ID 및 비밀 액세스 키가 나열된 다운로드 액세스 키 대화 상자가 나타납니다.

5. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

   ⓘ 이 정보를 복사하거나 다운로드할 때까지 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.



6. 마침 * 을 선택합니다.

   새 키가 내 액세스 키 페이지에 나열됩니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

S3 액세스 키를 봅니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 S3 액세스 키 목록을 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬할 수 있으므로 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 새 키를 만들거나 더 이상 사용하지 않는 키를 삭제할 수 있습니다.

필요한 것

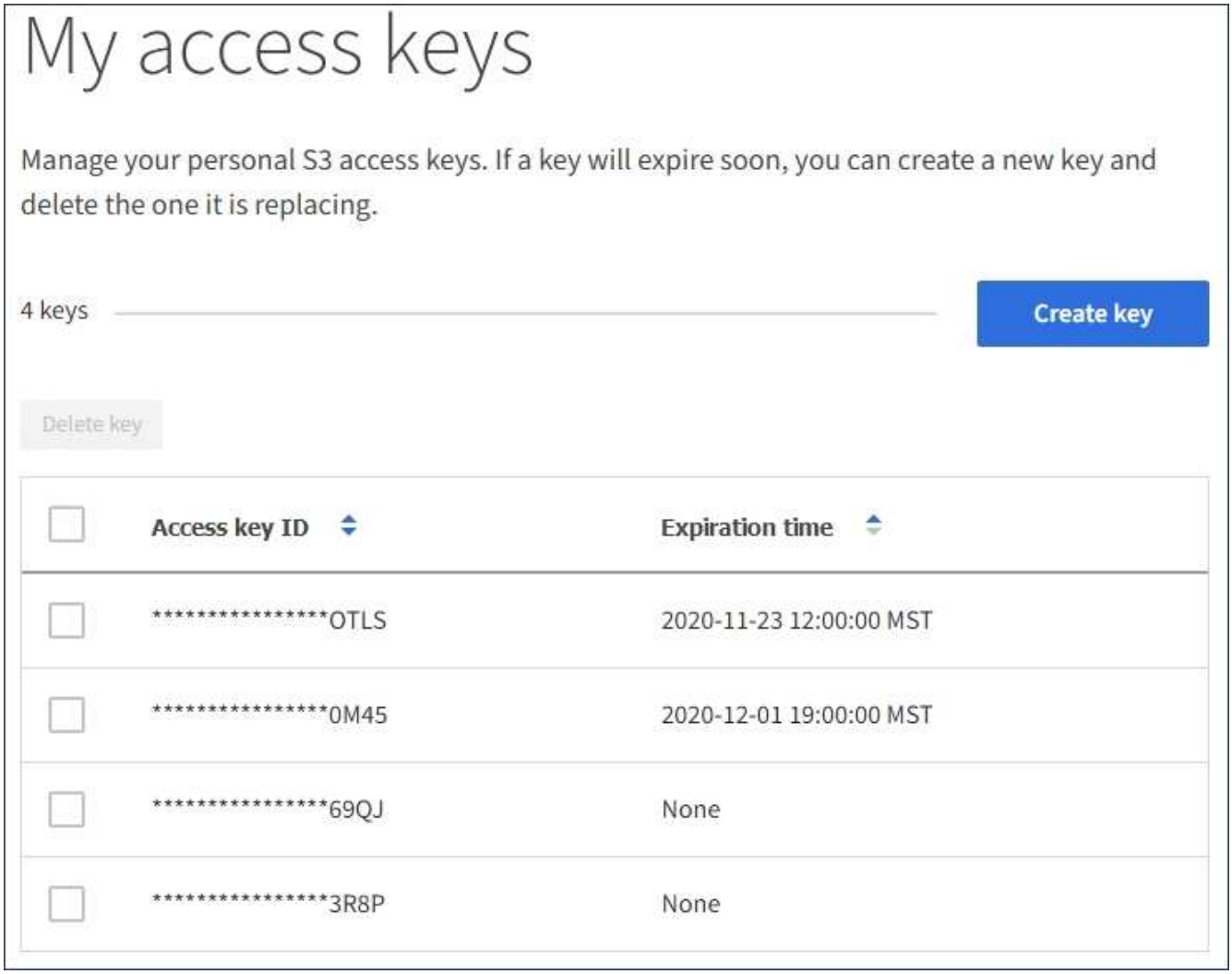
- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있어야 합니다.

> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.



2. 키를 * Expiration Time * 또는 * Access key ID * 로 정렬합니다.
3. 필요에 따라 새 키를 만들고 더 이상 사용하지 않는 키를 수동으로 삭제합니다.

   기존 키가 만료되기 전에 새 키를 만들면 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용할 수 있습니다.

   만료된 키는 자동으로 제거됩니다.

관련 정보

자체 S3 액세스 키를 생성합니다

자체 S3 액세스 키를 삭제합니다

자체 **S3** 액세스 키를 삭제합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 자신의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제된 후에는 더 이상 테넌트 계정의 객체와 버킷에 액세스할 수 없습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 자신의 S3 자격 증명 관리 권한이 있어야 합니다. 을 참조하십시오 테넌트 관리 권한.

> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

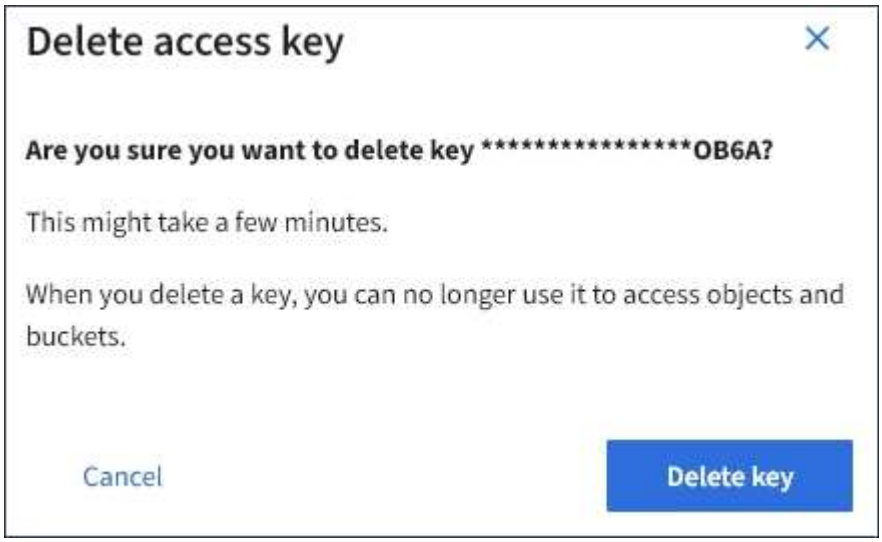
단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

2. 제거할 각 액세스 키에 대한 확인란을 선택합니다.
3. Delete key * 를 선택합니다.

   확인 대화 상자가 나타납니다.



4. Delete key * 를 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

다른 사용자의 **S3** 액세스 키를 생성합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 버킷 및 오브젝트에 액세스해야 하는 애플리케이션 같은 다른 사용자를 위한 S3 액세스 키를 생성할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

하나 이상의 다른 사용자를 위한 S3 액세스 키를 생성하여 해당 테넌트 계정에 대한 버킷을 생성하고 관리할 수 있습니다. 새 액세스 키를 생성한 후 새 액세스 키 ID와 비밀 액세스 키로 응용 프로그램을 업데이트합니다. 보안을 위해

사용자 요구 사항보다 많은 키를 생성하지 말고 사용하지 않는 키를 삭제하십시오. 하나의 키만 있고 만료되려고 하는 경우 이전 키가 만료되기 전에 새 키를 만든 다음 이전 키를 삭제합니다.

각 키에는 특정 만료 시간 또는 만료 기간이 있을 수 있습니다. 만료 시간에 대한 다음 지침을 따르십시오.

- 키의 만료 시간을 설정하여 사용자의 액세스를 특정 기간으로 제한합니다. 만료 시간을 짧게 설정하면 액세스 키 ID 및 비밀 액세스 키가 실수로 노출될 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 제거됩니다.
- 환경의 보안 위험이 낮으며 주기적으로 새 키를 만들 필요가 없는 경우 키의 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 만들려면 이전 키를 수동으로 삭제합니다.

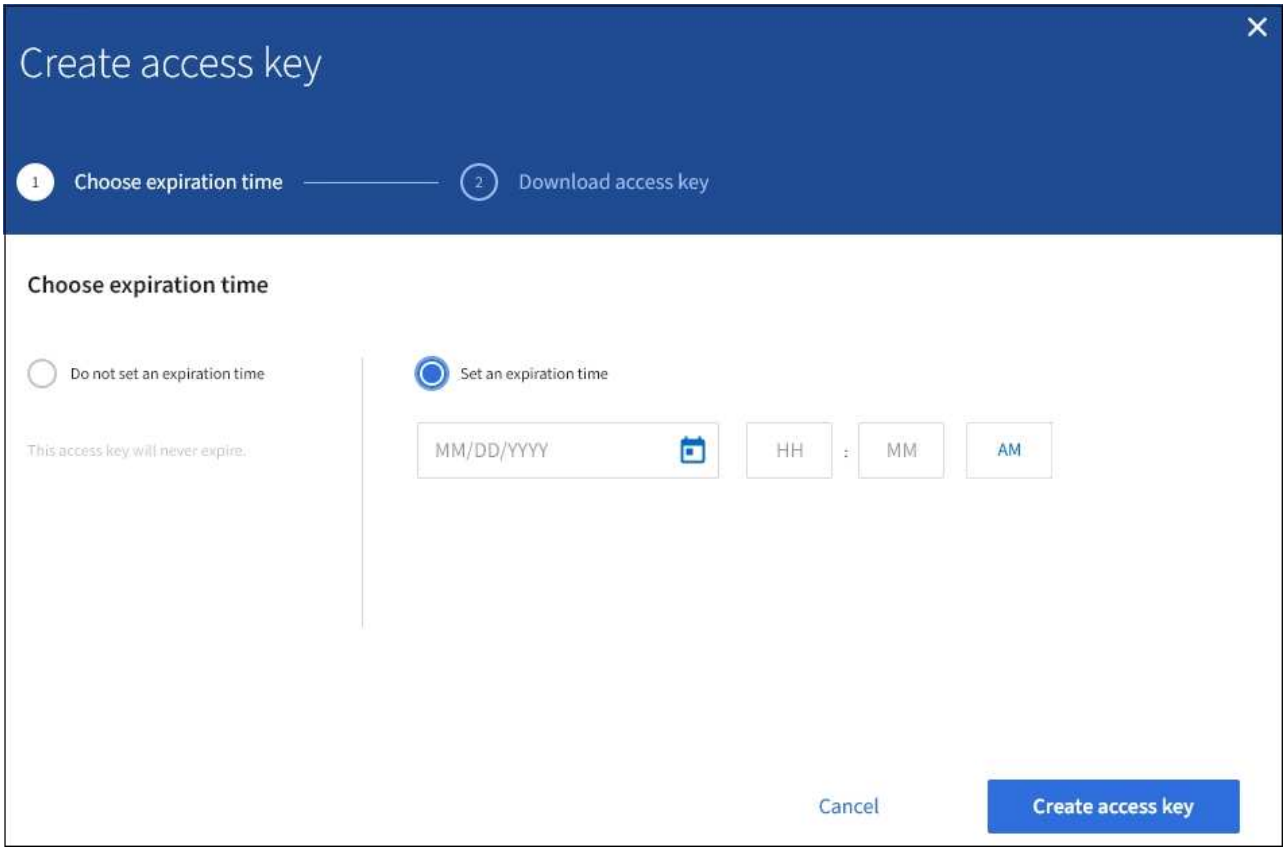
> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. S3 액세스 키를 관리할 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택한 다음 * 키 만들기 * 를 선택합니다.
4. 다음 중 하나를 수행합니다.
   - 만료 시간을 설정하지 않음 * 을 선택하여 만료되지 않는 키를 생성합니다. (기본값)
   - 만료 시간 설정 * 을 선택하고 만료 날짜 및 시간을 설정합니다.

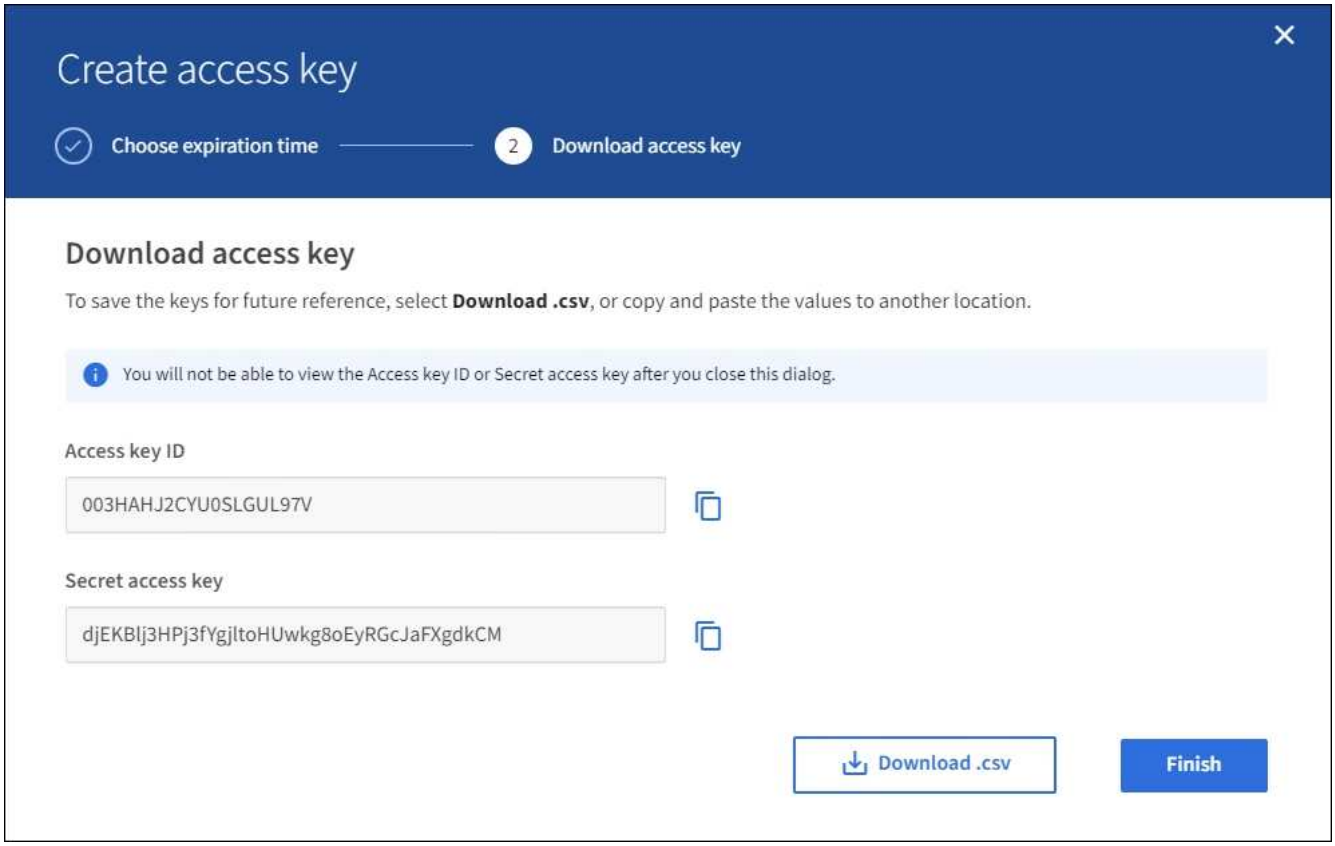


5. Create access key * 를 선택합니다.

   액세스 키 ID 및 비밀 액세스 키가 나열된 다운로드 액세스 키 대화 상자가 나타납니다.

6. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

   > 이 정보를 복사하거나 다운로드할 때까지 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.



7. 마침 * 을 선택합니다.

   새 키가 사용자 세부 정보 페이지의 액세스 키 탭에 나열됩니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

테넌트 관리 권한

다른 사용자의 **S3** 액세스 키를 봅니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 다른 사용자의 S3 액세스 키를 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬하면 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 새 키를 생성하고 더 이상 사용하지 않는 키를 삭제할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 루트 액세스 권한이 있어야 합니다.

> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

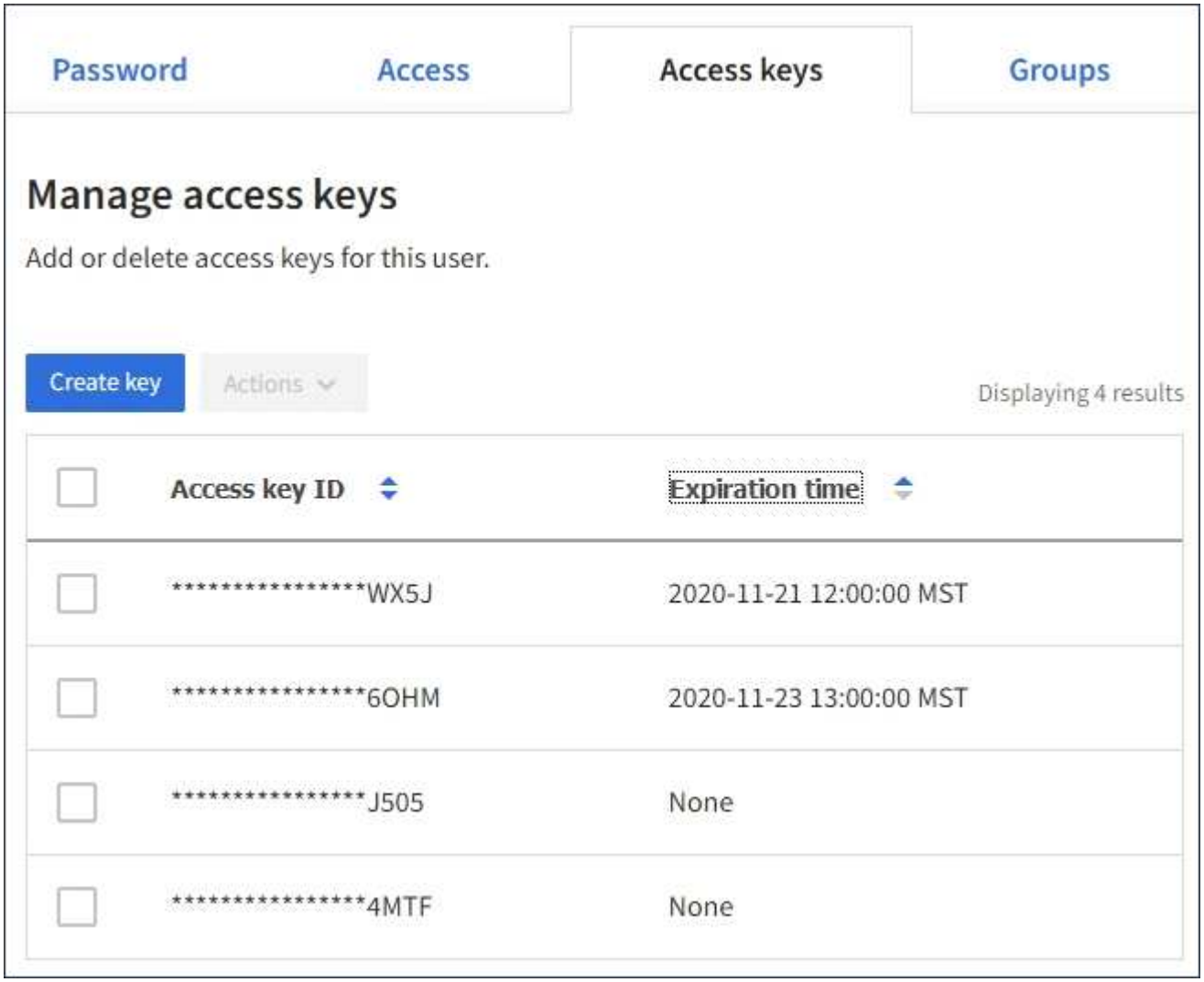
1. 액세스 관리 * > * 사용자 * 를 선택합니다.

   사용자 페이지가 나타나고 기존 사용자가 나열됩니다.

2. S3 액세스 키를 보려는 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택합니다.



4. 키를 * Expiration Time * 또는 * Access key ID * 로 정렬합니다.
5. 필요에 따라 새 키를 생성하고 에서 더 이상 사용하지 않는 키를 수동으로 삭제합니다.

기존 키가 만료되기 전에 새 키를 만들면 사용자는 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용할 수 있습니다.

만료된 키는 자동으로 제거됩니다.

관련 정보

다른 사용자의 S3 액세스 키를 생성합니다

다른 사용자의 S3 액세스 키를 삭제합니다

다른 사용자의 **S3** 액세스 키를 삭제합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 다른 사용자의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제된 후에는 더 이상 테넌트 계정의 객체와 버킷에 액세스할 수 없습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있어야 합니다. 을 참조하십시오 테넌트 관리 권한.

> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.

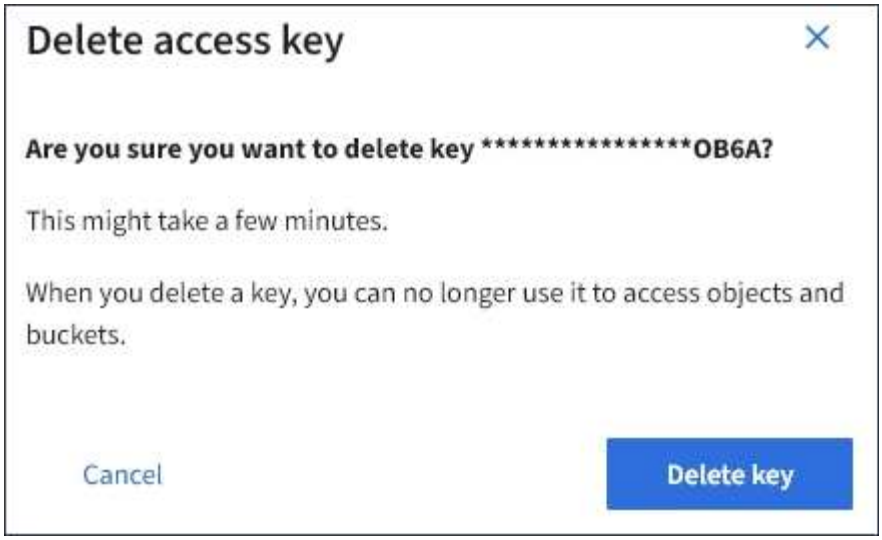
   사용자 페이지가 나타나고 기존 사용자가 나열됩니다.

2. S3 액세스 키를 관리할 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택한 다음 삭제할 각 액세스 키에 대한 확인란을 선택합니다.
4. Actions * > * Delete Selected key * 를 선택합니다.

   확인 대화 상자가 나타납니다.



5. Delete key * 를 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

S3 버킷을 관리합니다

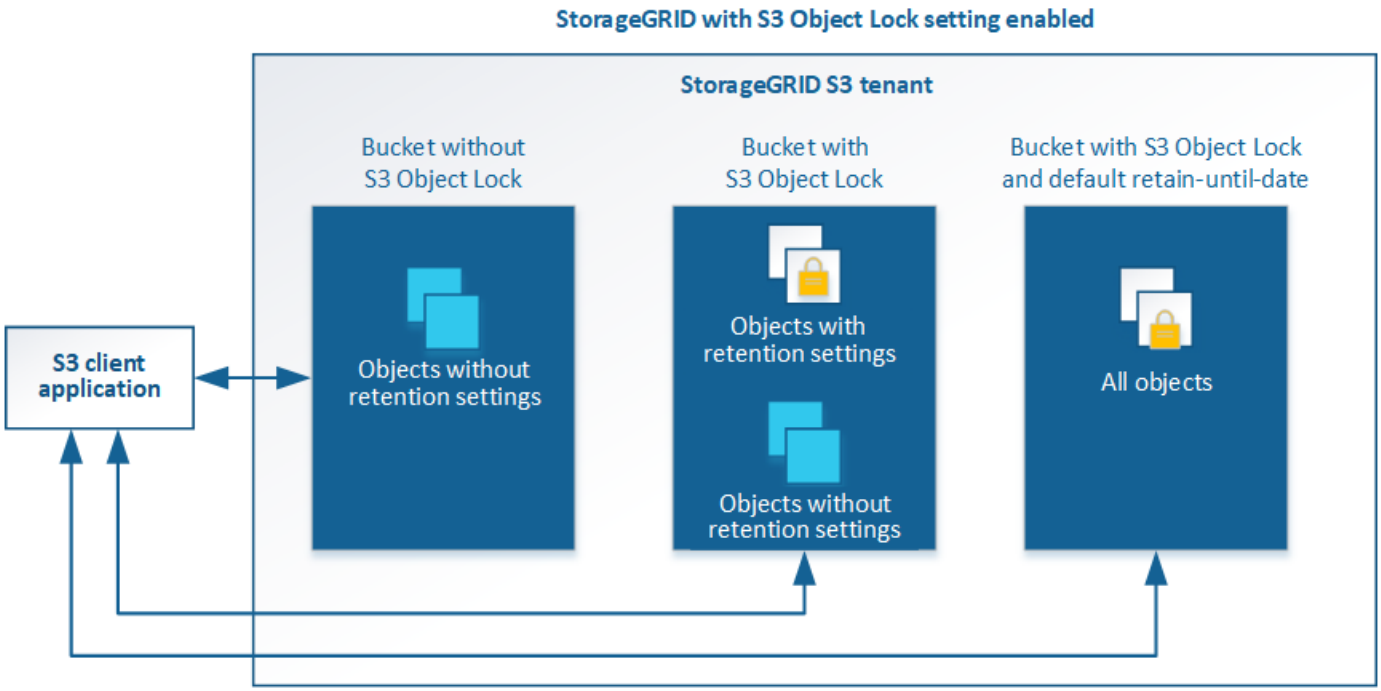
테넌트에 **S3** 오브젝트 잠금을 사용합니다

오브젝트가 보존 규정 요구사항을 충족해야 하는 경우 StorageGRID의 S3 오브젝트 잠금 기능을 사용할 수 있습니다.

S3 오브젝트 잠금이란 무엇입니까?

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3(Amazon Simple Storage Service)의 S3 오브젝트 잠금과 동등한 오브젝트 보호 솔루션입니다.

그림에서 볼 수 있듯이 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 사용하면 S3 테넌트 계정이 S3 오브젝트 잠금을 사용하거나 사용하지 않고 버킷을 생성할 수 있습니다. 버킷에 S3 오브젝트 잠금이 설정된 경우 S3 클라이언트 애플리케이션이 해당 버킷의 모든 오브젝트 버전에 대한 보존 설정을 선택적으로 지정할 수 있습니다. 오브젝트 버전에 S3 오브젝트 잠금으로 보호할 보존 설정이 지정되어 있어야 합니다.



StorageGRID S3 오브젝트 잠금 기능은 Amazon S3 규정 준수 모드에 상응하는 단일 보존 모드를 제공합니다. 기본적으로 보호된 개체 버전은 사용자가 덮어쓰거나 삭제할 수 없습니다. StorageGRID S3 오브젝트 잠금 기능은 거버넌스 모드를 지원하지 않으며, 특별한 권한이 있는 사용자가 보존 설정을 무시하거나 보호된 오브젝트를 삭제할 수 없습니다.

버킷에 S3 오브젝트 잠금이 활성화된 경우 오브젝트를 생성하거나 업데이트할 때 S3 클라이언트 애플리케이션에서 다음 오브젝트 레벨 보존 설정 중 하나 또는 모두를 선택적으로 지정할 수 있습니다.

- * Retain-until-date *: 개체 버전의 Retain-until-date가 미래인 경우 개체를 검색할 수 있지만 수정하거나 삭제할 수 없습니다. 필요에 따라 오브젝트의 보존 기간(Retain-until-date)을 늘릴 수 있지만 이 날짜는 줄일 수 없습니다.
- * 법적 증거 자료 보관 *: 개체 버전에 법적 증거 자료 보관 기능을 적용하면 해당 개체가 즉시 잠깁니다. 예를 들어 조사 또는 법적 분쟁과 관련된 객체에 법적 보류를 지정해야 할 수 있습니다. 법적 보류는 만료 날짜가 없지만 명시적으로 제거될 때까지 유지됩니다. 법적 보류는 보존 기한 과 무관합니다.

또한 가능합니다 버킷의 기본 보존 모드 및 기본 보존 기간을 지정합니다. 고유한 보존 설정을 지정하지 않는 버킷에 추가된 각 오브젝트에 적용됩니다.

이러한 설정에 대한 자세한 내용은 을 참조하십시오 S3 오브젝트 잠금을 사용합니다.

레거시 준수 버킷을 관리합니다

S3 오브젝트 잠금 기능은 이전 StorageGRID 버전에서 사용할 수 있었던 규정 준수 기능을 대체합니다. 이전 버전의 StorageGRID를 사용하여 준수 버킷을 생성한 경우 이러한 버켓의 설정을 계속 관리할 수 있지만, 더 이상 새로운 준수 버킷을 생성할 수 없습니다. 자세한 내용은 NetApp 기술 자료 문서를 참조하십시오.

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

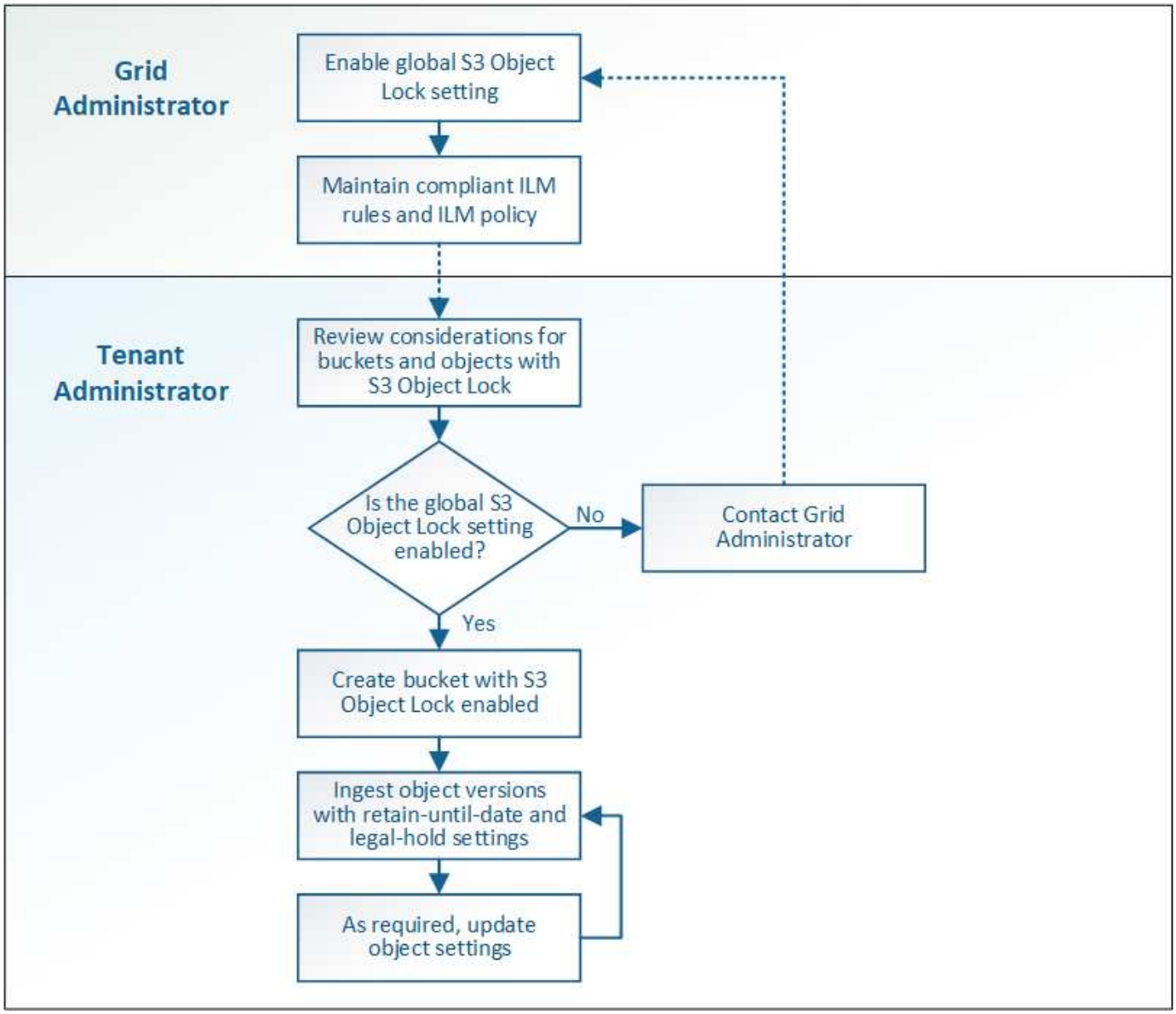
S3 오브젝트 잠금 워크플로

워크플로우 다이어그램은 StorageGRID에서 S3 오브젝트 잠금 기능을 사용하기 위한 상위 단계를 보여줍니다.

S3 오브젝트 잠금이 설정된 버킷을 생성하려면 그리드 관리자가 전체 StorageGRID 시스템에 대해 글로벌 S3

오브젝트 잠금 설정을 활성화해야 합니다. 또한 그리드 관리자는 을 확인해야 합니다 ILM(정보 수명 주기 관리) 정책 은(는) ""준수""입니다. S3 오브젝트 잠금이 활성화된 버킷의 요구 사항을 충족해야 합니다. 자세한 내용은 그리드 관리자에게 문의하거나 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

글로벌 S3 오브젝트 잠금 설정을 활성화한 후 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 있습니다. 그런 다음 S3 클라이언트 애플리케이션을 사용하여 필요에 따라 각 오브젝트 버전에 대한 보존 설정을 지정할 수 있습니다.



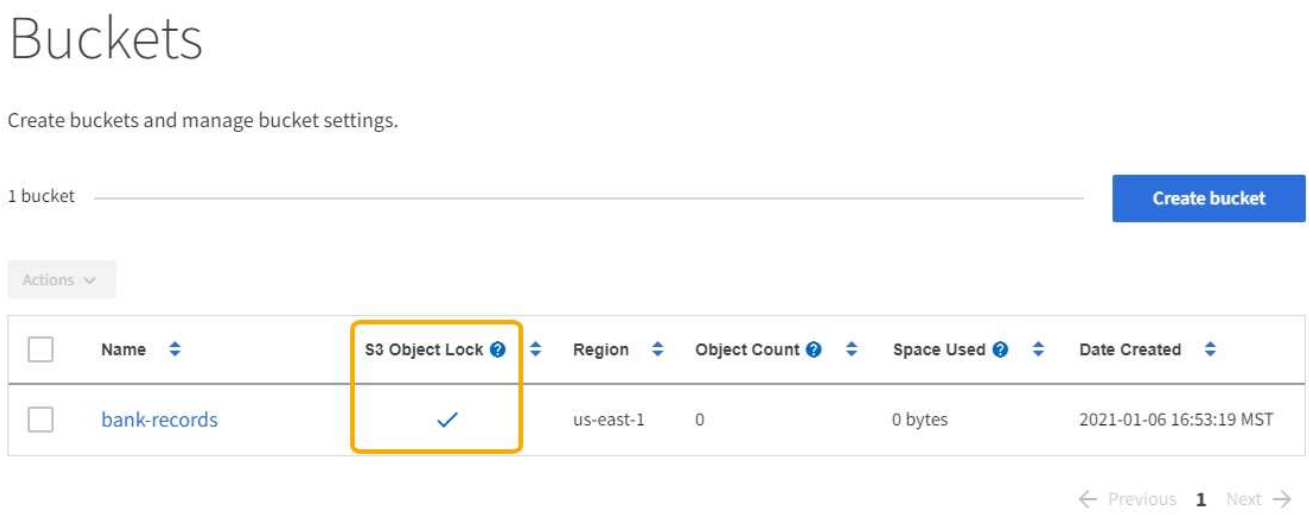
S3 오브젝트 잠금에 대한 요구사항

버킷에 대해 S3 오브젝트 잠금을 설정하기 전에 S3 오브젝트 잠금 버킷 및 오브젝트에 대한 요구사항과 S3 오브젝트 잠금이 활성화된 버킷에 포함된 오브젝트의 수명 주기를 검토하십시오.

S3 오브젝트 잠금이 설정된 버킷의 요구 사항

- StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 S3 오브젝트 잠금이 활성화된 버킷을 생성할 수 있습니다.

  테넌트 관리자의 이 예에서는 S3 오브젝트 잠금이 설정된 버킷을 보여 줍니다.



- S3 오브젝트 잠금을 사용하려는 경우 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에 대해 S3 오브젝트 잠금을 활성화할 수 없습니다.
- S3 오브젝트 잠금에서 버킷 버전 관리가 필요합니다. 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 StorageGRID는 해당 버킷의 버전 관리를 자동으로 활성화합니다.
- S3 오브젝트 잠금이 설정된 버킷을 생성한 후에는 해당 버켓에 대한 S3 오브젝트 잠금을 비활성화하거나 버전 관리를 일시 중단할 수 없습니다.
- 필요에 따라 버킷의 기본 보존을 구성할 수 있습니다. 개체 버전이 업로드되면 기본 보존 기간이 개체 버전에 적용됩니다. 객체 버전 업로드 요청에 보존 모드와 보존 기간을 지정하여 버킷 기본값을 재정의할 수 있습니다.
- S3 오브젝트 라이프사이클 버킷에 대해 버킷 라이프사이클 구성이 지원됩니다.
- S3 오브젝트 잠금이 설정된 버킷에는 CloudMirror 복제가 지원되지 않습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

- 오브젝트 버전을 보호하려면 S3 클라이언트 애플리케이션이 버킷 기본 보존을 구성하거나 각 업로드 요청에서 보존 설정을 지정해야 합니다.
- 개체 버전에 대한 보존 기간을 늘릴 수 있지만 이 값을 줄일 수는 없습니다.
- 법적 조치 또는 규제 조사가 보류 중인 경우 개체 버전에 법적 증거 자료를 두어 관련 정보를 보존할 수 있습니다. 개체 버전이 법적 증거 자료 보관 중인 경우, 해당 개체가 보존 기한 에 도달한 경우에도 StorageGRID에서 해당 개체를 삭제할 수 없습니다. 법적 증거 자료 보관 기간이 해제됨과 동시에, 보존 기한이 만료된 경우 개체 버전을 삭제할 수 있습니다.
- S3 오브젝트 잠금에는 버전 관리되는 버킷을 사용해야 합니다. 보존 설정은 개별 개체 버전에 적용됩니다. 개체 버전에는 보존 기한 및 법적 보류 설정이 둘 다 있을 수 있으며, 둘 중 하나만 설정할 수도 있고 둘 다 가질 수도 없습니다. 개체에 대한 보존 기한 또는 법적 보류 설정을 지정하면 요청에 지정된 버전만 보호됩니다. 이전 버전의 개체는 잠겨 있는 상태에서 새 버전의 개체를 만들 수 있습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 라이프사이클

S3 오브젝트 잠금이 설정된 버킷에 저장된 각 오브젝트는 다음 3단계를 거칩니다.

1. * 오브젝트 수집 *
    - S3 오브젝트 잠금이 설정된 버킷에 오브젝트 버전을 추가할 경우 S3 클라이언트 애플리케이션이 오브젝트에 대한 보존 설정을 선택적으로 지정할 수 있습니다(보존 기한, 법적 보류 또는 둘 다). 그런 다음

StorageGRID에서는 해당 개체의 메타데이터를 생성하며 고유한 UUID(Object Identifier)와 수집 날짜 및 시간이 포함됩니다.

- 보존 설정이 포함된 오브젝트 버전을 수집하면 해당 데이터와 S3 사용자 정의 메타데이터를 수정할 수 없습니다.
- StorageGRID는 오브젝트 메타데이터를 오브젝트 데이터와 독립적으로 저장합니다. 이 기능은 각 사이트에서 모든 오브젝트 메타데이터의 복사본을 3개 유지 관리합니다.

2. * 개체 보존 *
   - 개체의 여러 복사본이 StorageGRID에 저장됩니다. 정확한 복제본 수와 유형 및 스토리지 위치는 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다.
3. * 개체 삭제 *
   - 보존 기한 에 도달하면 개체를 삭제할 수 있습니다.
   - 법적 증거 자료 보관 중인 개체는 삭제할 수 없습니다.

S3 버킷을 생성합니다

테넌트 관리자를 사용하여 오브젝트 데이터용 S3 버킷을 생성할 수 있습니다. 버킷을 생성할 때 버킷의 이름과 영역을 지정해야 합니다. StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 버킷에 대해 S3 오브젝트 잠금을 선택적으로 활성화할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

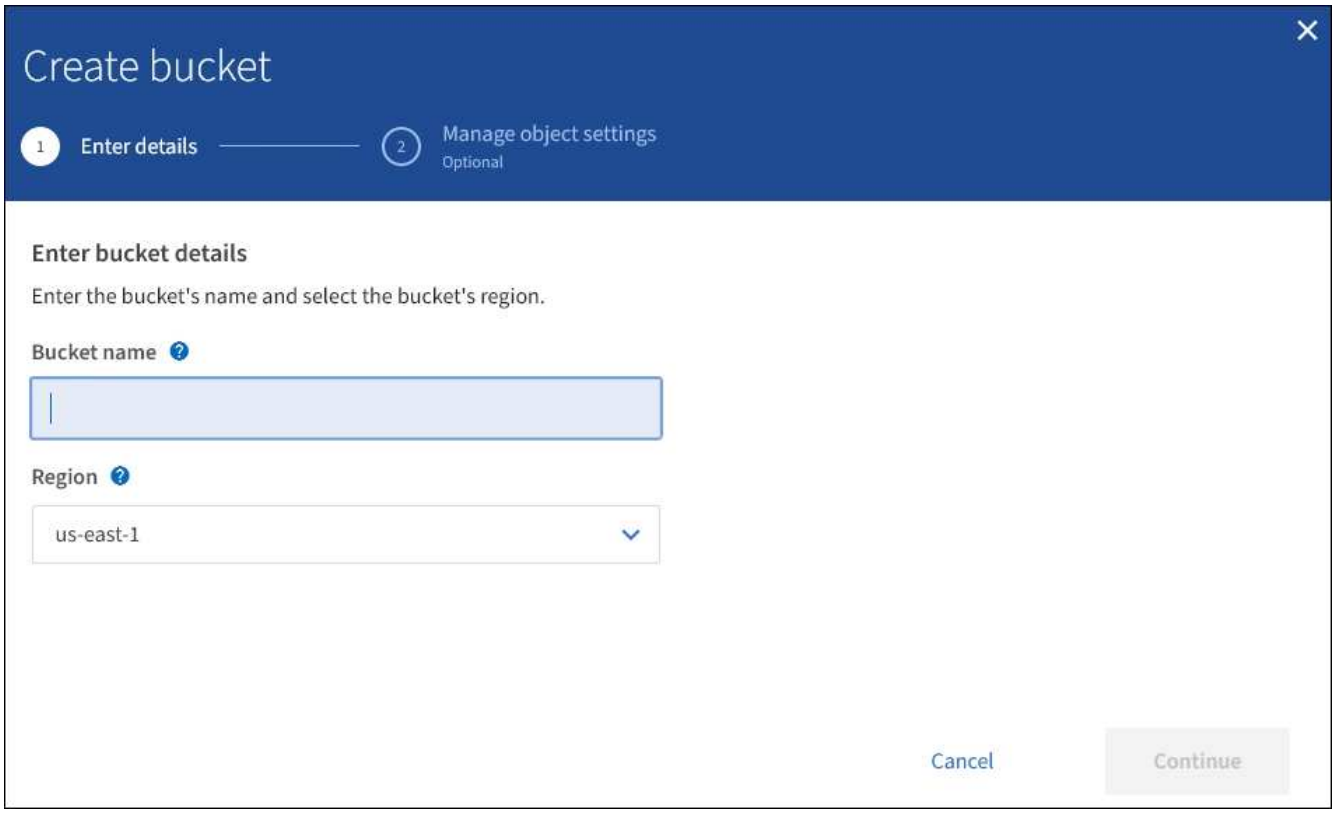
> 에서 버킷 또는 오브젝트의 S3 오브젝트 잠금 속성을 설정하거나 수정하는 권한을 부여할 수 있습니다 버킷 정책 또는 그룹 정책.

- S3 오브젝트 잠금을 사용하여 버킷을 생성하려는 경우 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 활성화하고 S3 오브젝트 잠금 버킷 및 오브젝트에 대한 요구사항을 검토했습니다.

  S3 오브젝트 잠금을 사용합니다

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. Create bucket * 을 선택합니다.



3. 버킷의 고유한 이름을 입력하십시오.

> 버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

버킷 이름은 다음 규칙을 준수해야 합니다.

- 각 StorageGRID 시스템에서 고유해야 합니다(테넌트 계정에서만 고유한 것은 아님).
- DNS를 준수해야 합니다.
- 3자 이상 63자 이하여야 합니다.
- 각 레이블은 소문자 또는 숫자로 시작하고 끝나야 하며 소문자, 숫자 및 하이픈만 사용할 수 있습니다.
- 가상 호스팅 스타일 요청에서 기간을 사용하지 않아야 합니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다.

> 자세한 내용은 를 참조하십시오 "버킷 명명 규칙에 대한 AWS(Amazon Web Services) 문서입니다".

4. 이 버킷의 영역을 선택합니다.

StorageGRID 관리자가 사용 가능한 영역을 관리합니다. 버킷 영역은 오브젝트에 적용되는 데이터 보호 정책에 영향을 미칠 수 있습니다. 기본적으로 모든 버킷은 us-east-1 영역에 생성됩니다.

> 버킷을 생성한 후에는 지역을 변경할 수 없습니다.

5. Continue * 를 선택합니다.
6. 필요한 경우 버킷에 대한 오브젝트 버전 관리를 활성화합니다.

이 버킷에 각 오브젝트의 모든 버전을 저장하려면 오브젝트 버전 관리를 활성화하십시오. 그런 다음 필요에 따라 개체의 이전 버전을 검색할 수 있습니다.

7. S3 오브젝트 잠금 섹션이 나타나면 버킷에 대해 S3 오브젝트 잠금을 선택적으로 활성화합니다.

   > 버킷을 생성한 후에는 S3 오브젝트 잠금을 설정하거나 해제할 수 없습니다.

   S3 오브젝트 잠금 섹션은 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우에만 나타납니다.

   S3 클라이언트 애플리케이션이 버킷에 추가된 오브젝트에 대한 보관 종료 날짜 및 법적 보류 설정을 지정하려면 먼저 버킷에 대해 S3 오브젝트 잠금을 활성화해야 합니다.

   버킷에 대해 S3 오브젝트 잠금을 설정하면 버킷 버전 관리가 자동으로 활성화됩니다. 또한 가능합니다 버킷의 기본 보존 모드 및 기본 보존 기간을 지정합니다 고유한 보존 설정을 지정하지 않는 버킷에 수집된 각 개체에 적용됩니다.

8. Create bucket * 을 선택합니다.

   버킷이 생성되어 버킷 페이지의 테이블에 추가됩니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

테넌트 관리 API 이해

S3을 사용합니다

S3 버킷 세부 정보를 봅니다

테넌트 계정에서 버킷 및 버킷 설정 목록을 볼 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 테넌트 계정에 대한 모든 버킷이 나열됩니다.

2. 각 버킷에 대한 정보를 검토합니다.

   필요에 따라 모든 열을 기준으로 정보를 정렬하거나 목록 앞뒤에 페이지를 표시할 수 있습니다.

   - 이름: 변경할 수 없는 버킷의 고유 이름입니다.
   - S3 오브젝트 잠금: 이 버킷에 대해 S3 오브젝트 잠금이 설정되었는지 여부.

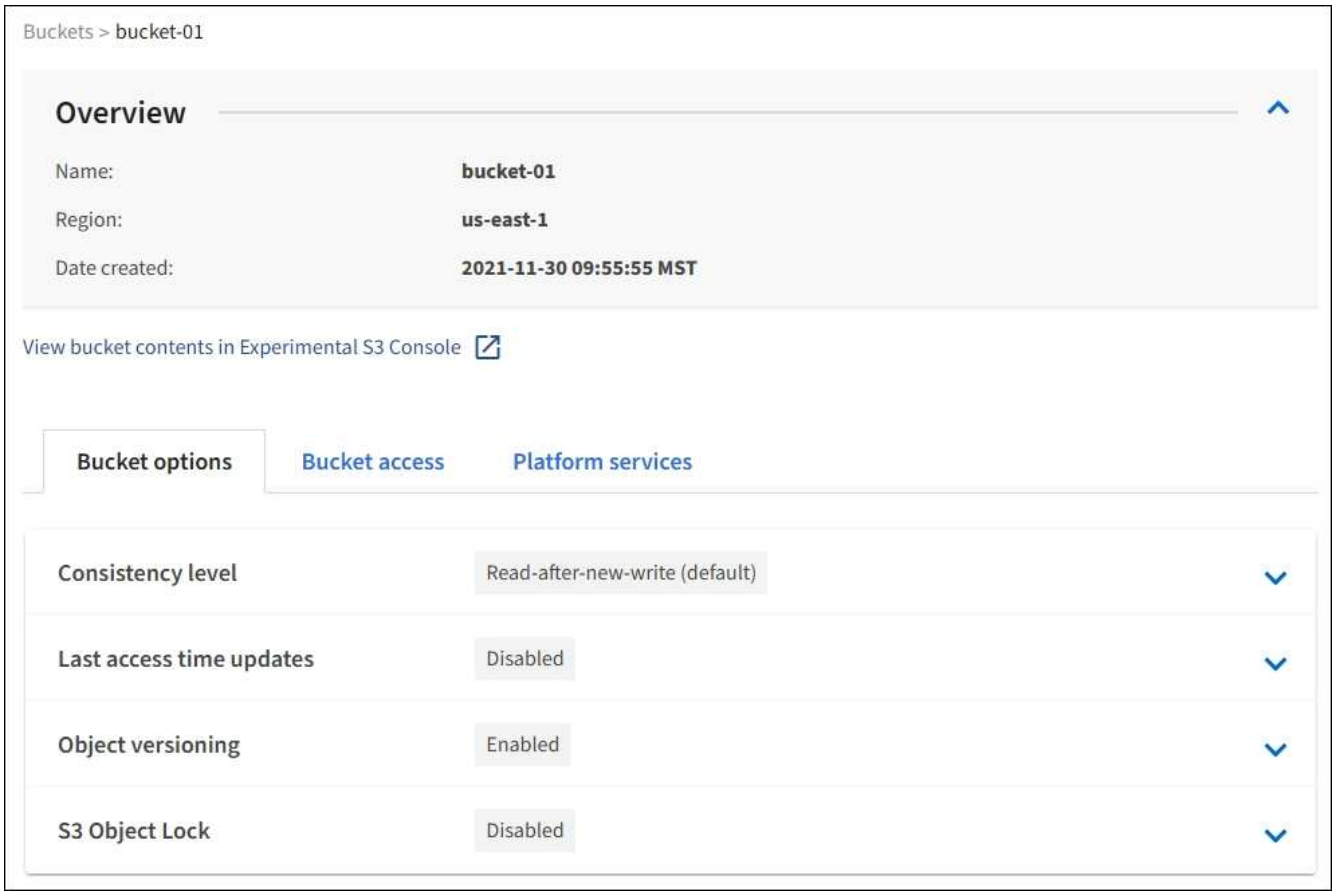
     전역 S3 오브젝트 잠금 설정이 비활성화된 경우 이 열은 표시되지 않습니다. 또한 이 열에는 레거시 준수 버킷에 대한 정보도 표시됩니다.

   - 지역: 변경할 수 없는 버킷의 영역입니다.
   - 개체 수: 이 버킷의 오브젝트 수입니다.
   - 사용된 공간: 이 버킷에 있는 모든 오브젝트의 논리적 크기입니다. 논리적 크기에는 복제 또는 삭제 코딩 복사본 또는 오브젝트 메타데이터에 필요한 실제 공간이 포함되지 않습니다.
   - 만든 날짜: 버킷을 만든 날짜 및 시간입니다.

   > 표시된 개체 수와 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다. 버킷에 버전 관리가 활성화된 경우 삭제된 개체 버전은 오브젝트 수에 포함됩니다.

3. 버킷의 설정을 보고 관리하려면 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지에서는 버킷 옵션, 버킷 액세스 및 에 대한 설정을 보고 편집할 수 있습니다 플랫폼 서비스.



정합성 보장 수준을 변경합니다

S3 테넌트를 사용하는 경우 테넌트 관리자 또는 테넌트 관리 API를 사용하여 S3 버킷의 오브젝트에 대해 수행된 작업의 정합성 제어를 변경할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다. 을 참조하십시오 테넌트 관리 권한.

이 작업에 대해

정합성 보장 레벨은 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트에서 이러한 오브젝트의 일관성 간의 균형을 제공합니다. 일반적으로 버킷에 대해 * Read-After-new-write * 정합성 수준을 사용해야 합니다.

새 쓰기 후 읽기 * 정합성 보장 레벨이 클라이언트 애플리케이션의 요구 사항을 충족하지 않는 경우 버킷 정합성 수준을 설정하거나 을 사용하여 정합성 보장 레벨을 변경할 수 있습니다 `Consistency-Control` 머리글. 를 클릭합니다 `Consistency-Control` 헤더는 버킷 정합성 레벨을 오버라이드합니다.

> 버킷의 정합성 수준을 변경하면 변경 후 수집된 객체만 수정된 레벨에 맞게 보장됩니다.

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.

버킷 세부 정보 페이지가 나타납니다.

3. 버킷 옵션 * > * 정합성 보장 레벨 * 을 선택합니다.
4. 이 버킷의 오브젝트에 대해 수행된 작업의 정합성 수준을 선택합니다.
   - * 모두 *: 최고 수준의 일관성을 제공합니다. 모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
   - * 강력한 글로벌 *: 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
   - * 강력한 사이트 *: 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
   - * Read-After-new-write * (기본값): 새 객체에 대해 읽기-쓰기 후 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 대부분의 경우에 권장됩니다.
   - * 사용 가능 *: 새 객체 및 객체 업데이트 모두에 대한 최종 일관성을 제공합니다. S3 버킷의 경우 필요에 따라 만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.
5. 변경 내용 저장 * 을 선택합니다.

마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다

그리드 관리자가 StorageGRID 시스템에 대한 ILM(정보 수명 주기 관리) 규칙을 만들 때 오브젝트의 마지막 액세스 시간을 사용하여 해당 오브젝트를 다른 스토리지 위치로 이동할지 여부를 결정하도록 선택적으로 지정할 수 있습니다. S3 테넌트를 사용하는 경우 S3 버킷의 오브젝트에 대한 마지막 액세스 시간 업데이트를 활성화하여 이러한 규칙을 활용할 수 있습니다.

이 지침은 배치 지침에서 * Last Access Time * 옵션을 사용하는 ILM 규칙을 하나 이상 포함하는 StorageGRID 시스템에만 적용됩니다. StorageGRID 시스템에 이러한 규칙이 포함되어 있지 않으면 이 지침을 무시할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다. 을 참조하십시오 테넌트 관리 권한.
- 마지막 액세스 시간 * 은 ILM 규칙에 대한 * 참조 시간 * 배치 명령에 사용할 수 있는 옵션 중 하나입니다. 규칙의 참조 시간을 마지막 액세스 시간으로 설정하면 그리드 관리자는 해당 개체를 마지막으로 검색한 시기(읽기 또는 보기)에 따라 특정 저장소 위치에 개체가 배치되도록 지정할 수 있습니다.

예를 들어, 최근에 본 오브젝트를 더 빠른 스토리지에 유지하기 위해 그리드 관리자는 다음을 지정하는 ILM 규칙을 생성할 수 있습니다.

- 지난 달 동안 검색된 객체는 로컬 스토리지 노드에 남아 있어야 합니다.
- 지난 달에 검색되지 않은 객체는 오프 사이트 위치로 이동해야 합니다.

> 정보 수명 주기 관리를 사용하여 개체를 관리하는 방법에 대한 지침을 참조하십시오.

기본적으로 마지막 액세스 시간에 대한 업데이트는 사용되지 않습니다. StorageGRID 시스템에 * Last Access Time * 옵션을 사용하는 ILM 규칙이 포함되어 있고 이 옵션이 이 버킷의 오브젝트에 적용되도록 하려면 해당 규칙에 지정된 S3 버킷에 대한 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다.

> 개체가 검색될 때 마지막 액세스 시간을 업데이트하면 특히 작은 개체의 StorageGRID 성능이 저하될 수 있습니다.

StorageGRID는 객체가 검색될 때마다 다음 추가 단계를 수행해야 하므로 마지막 액세스 시간 업데이트 시 성능 영향이 발생합니다.

- 객체를 새 타임스탬프로 업데이트합니다
- ILM 대기열에 개체를 추가하여 현재 ILM 규칙 및 정책에 대해 다시 평가할 수 있습니다

이 표에는 마지막 액세스 시간이 비활성화되거나 활성화될 때 버킷의 모든 오브젝트에 적용되는 동작이 요약되어 있습니다.

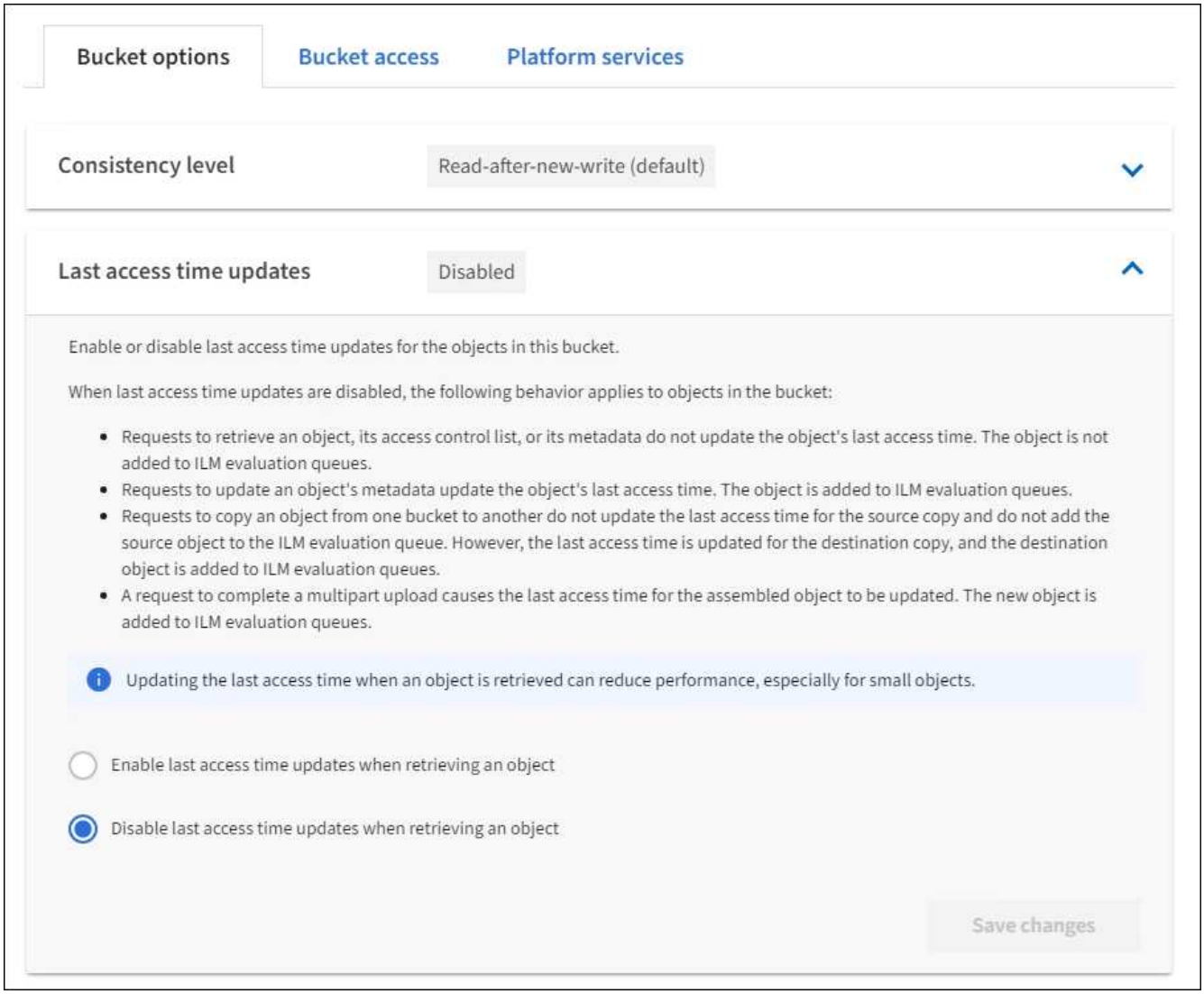
요청 유형입니다	마지막 액세스 시간이 비활성화된 경우의 동작(기본값)		마지막 액세스 시간이 설정된 경우의 동작	
	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?
개체, 해당 액세스 제어 목록 또는 해당 메타데이터를 검색하는 요청입니다	아니요	아니요	예	예
개체의 메타데이터를 업데이트하도록 요청합니다	예	예	예	예
한 버킷에서 다른 버킷으로 오브젝트 복사 요청	• 아니요, 소스 복제본입니다 • 예, 대상 복사본에 대해 입니다	• 아니요, 소스 복제본입니다 • 예, 대상 복사본에 대해 입니다	• 예. 소스 복제본에 대해 가능합니다 • 예, 대상 복사본에 대해 입니다	• 예. 소스 복제본에 대해 가능합니다 • 예, 대상 복사본에 대해 입니다
여러 부분 업로드를 완료하도록 요청합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

3. Bucket options * > * Last access time updates * 를 선택합니다.
4. 마지막 액세스 시간 업데이트를 활성화하거나 비활성화하려면 해당 라디오 버튼을 선택합니다.



5. 변경 내용 저장 * 을 선택합니다.

관련 정보

테넌트 관리 권한

ILM을 사용하여 개체를 관리합니다

버킷의 오브젝트 버전 관리를 변경합니다

S3 테넌트를 사용하는 경우 테넌트 관리자 또는 테넌트 관리 API를 사용하여 S3 버킷의 버전 관리 상태를 변경할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

  테넌트 관리 권한

이 작업에 대해

버킷에 대한 오브젝트 버전 관리를 설정하거나 일시 중지할 수 있습니다. 버켓에 대한 버전 관리를 활성화한 후에는 버전이 지정되지 않은 상태로 돌아갈 수 없습니다. 그러나 버킷의 버전 관리를 일시 중단할 수 있습니다.

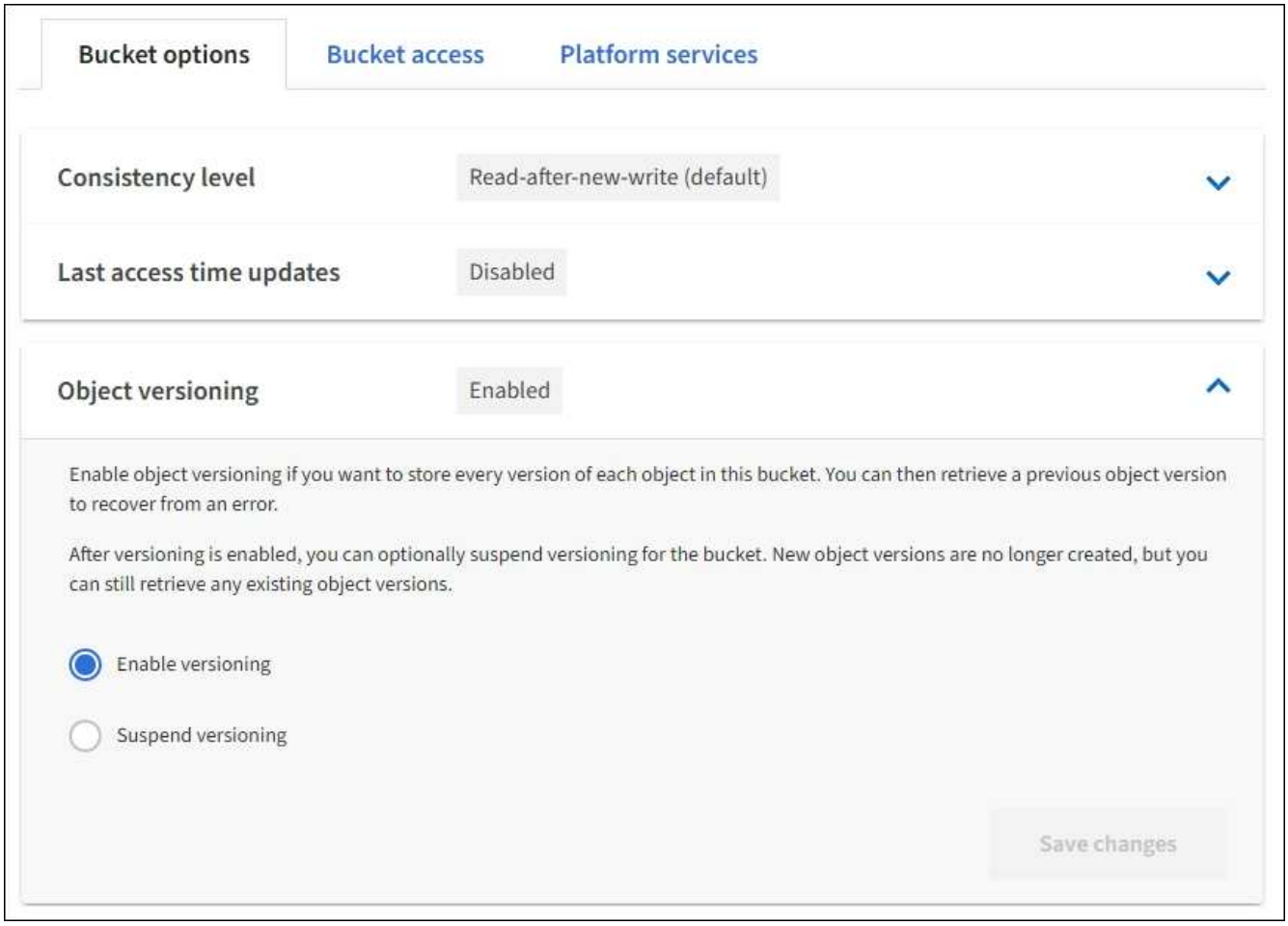
- 사용 안 함: 버전 관리가 활성화되지 않았습니다
- 사용: 버전 관리가 활성화됩니다
- 일시 중단됨: 버전 관리가 이전에 활성화되었으며 일시 중단되었습니다

S3 오브젝트 버전 관리

S3 버전 오브젝트 ILM 규칙 및 정책(예 4)

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.
3. 버킷 옵션 * > * 오브젝트 버전 관리 * 를 선택합니다.



4. 이 버킷의 오브젝트에 대한 버전 관리 상태를 선택합니다.

> S3 오브젝트 잠금 또는 레거시 규정 준수를 활성화하면 * 오브젝트 버전 관리 * 옵션이 비활성화됩니다.

옵션을 선택합니다	설명
버전 관리를 활성화합니다	이 버킷에 각 오브젝트의 모든 버전을 저장하려면 오브젝트 버전 관리를 활성화하십시오. 그런 다음 필요에 따라 개체의 이전 버전을 검색할 수 있습니다. 버킷에 이미 있던 객체는 사용자가 수정할 때 버전이 적용됩니다.
버전 관리를 일시 중단합니다	새 개체 버전을 더 이상 만들지 않으려면 개체 버전 관리를 일시 중단합니다. 기존 개체 버전을 검색할 수 있습니다.

5. 변경 내용 저장 * 을 선택합니다.

CORS(Cross-Origin Resource Sharing) 구성

다른 도메인의 웹 애플리케이션에서 해당 버킷의 버킷 및 오브젝트에 액세스할 수 있도록 하려면 S3 버킷에 대해 CORS(Cross-Origin Resource Sharing)를 구성할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

이 작업에 대해

CORS(Cross-Origin Resource Sharing)는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, 그래픽을 저장하기 위해 "이미지"라는 S3 버킷을 사용한다고 가정합니다. 영상물통용 CORS를 구성하여 해당 버켓의 영상을 웹사이트 http://www.example.com` 에 표시할 수 있습니다.

단계

1. 텍스트 편집기를 사용하여 CORS를 활성화하는 데 필요한 XML을 만듭니다.

   이 예에서는 S3 버킷에 대해 CORS를 활성화하는 데 사용되는 XML을 보여 줍니다. 이 XML을 사용하면 모든 도메인이 버킷에 GET 요청을 보낼 수 있지만 "http://www.example.com` 도메인에서만 POST 및 삭제 요청을 보낼 수 있습니다. 모든 요청 헤더가 허용됩니다.

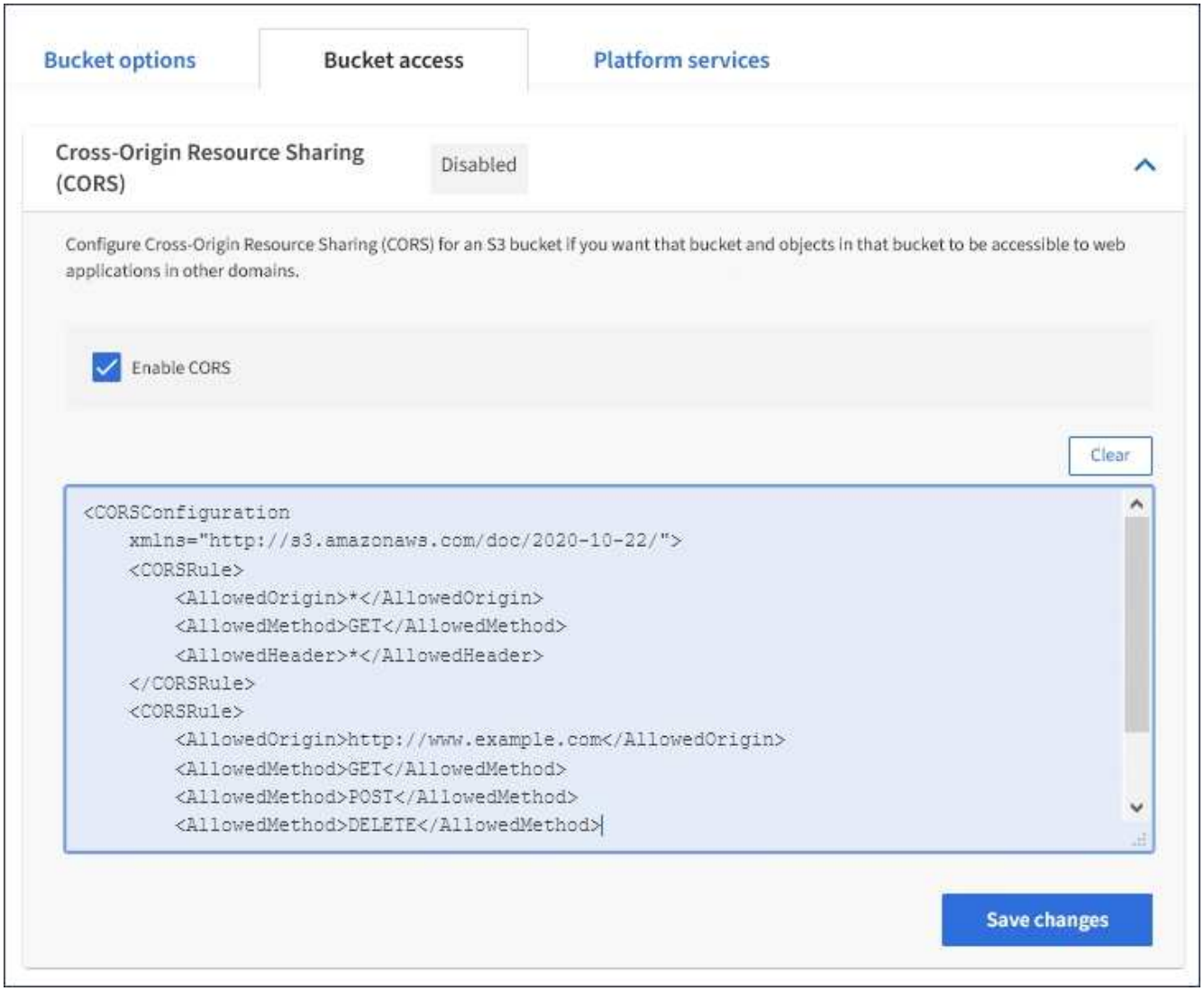
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

CORS 구성 XML에 대한 자세한 내용은 을 참조하십시오 "AWS(Amazon Web Services) 문서: Amazon Simple Storage Service 개발자 가이드 를 참조하십시오".

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 목록에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. Bucket access * > * Cross-Origin Resource Sharing (CORS) * 를 선택합니다.
5. CORS * 활성화 확인란을 선택합니다.
6. 텍스트 상자에 CORS 구성 XML을 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



7. 버킷의 CORS 설정을 수정하려면 텍스트 상자에서 CORS 구성 XML을 업데이트하거나 다시 시작하려면 * Clear * 를 선택하십시오. 그런 다음 * 변경 사항 저장 * 을 선택합니다.
8. 버킷에 대한 CORS를 비활성화하려면 * CORS * 활성화 확인란의 선택을 취소한 다음 * 변경 사항 저장 * 을 선택합니다.

S3 버킷을 삭제합니다

테넌트 관리자를 사용하여 비어 있는 하나 이상의 S3 버킷을 삭제할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다. 을 참조하십시오 테넌트 관리 권한.
- 삭제할 버킷이 비어 있습니다.

이 작업에 대해

다음 지침은 Tenant Manager를 사용하여 S3 버킷을 삭제하는 방법을 설명합니다. 를 사용하여 S3 버킷을 삭제할 수도 있습니다 테넌트 관리 API 또는 을 누릅니다 S3 REST API.

오브젝트 또는 비최신 오브젝트 버전이 포함된 S3 버킷을 삭제할 수 없습니다. S3 버전 오브젝트를 삭제하는 방법에 대한 자세한 내용은 를 참조하십시오 정보 수명 주기 관리를 사용하여 개체를 관리하기 위한 지침.

단계

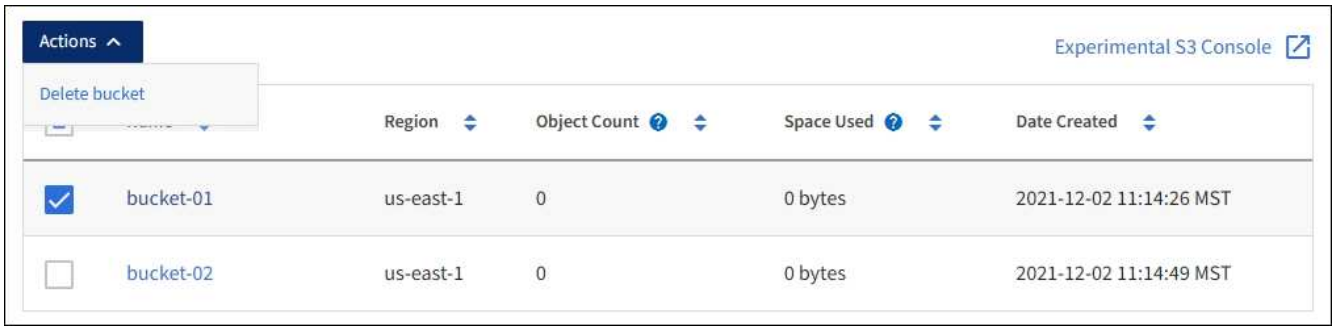
1. 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 기존의 모든 S3 버킷을 표시합니다.

2. 삭제할 빈 버킷의 확인란을 선택합니다. 한 번에 둘 이상의 버킷을 선택할 수 있습니다.

   작업 메뉴가 활성화됩니다.

3. 작업 메뉴에서 * 버킷 삭제 * (또는 둘 이상을 선택한 경우 * 버킷 삭제 *)를 선택합니다.



4. 확인 대화 상자가 나타나면 * 예 * 를 선택하여 선택한 모든 버킷을 삭제합니다.

   StorageGRID는 각 버킷이 비어 있음을 확인한 다음 각 버킷을 삭제합니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

   버킷이 비어 있지 않으면 오류 메시지가 나타납니다. 버킷을 삭제하려면 먼저 모든 오브젝트를 삭제해야 합니다.

Experimental S3 Console을 사용합니다

S3 콘솔을 사용하여 S3 버킷의 오브젝트를 볼 수 있습니다.

S3 콘솔을 사용하여 다음을 수행할 수도 있습니다.

- 개체, 개체 버전 및 폴더를 추가하고 삭제합니다
- 개체 이름을 바꿉니다
- 버킷 및 폴더 간에 오브젝트를 이동 및 복사합니다
- 오브젝트 태그 관리
- 개체 메타데이터를 봅니다
- 객체를 다운로드합니다

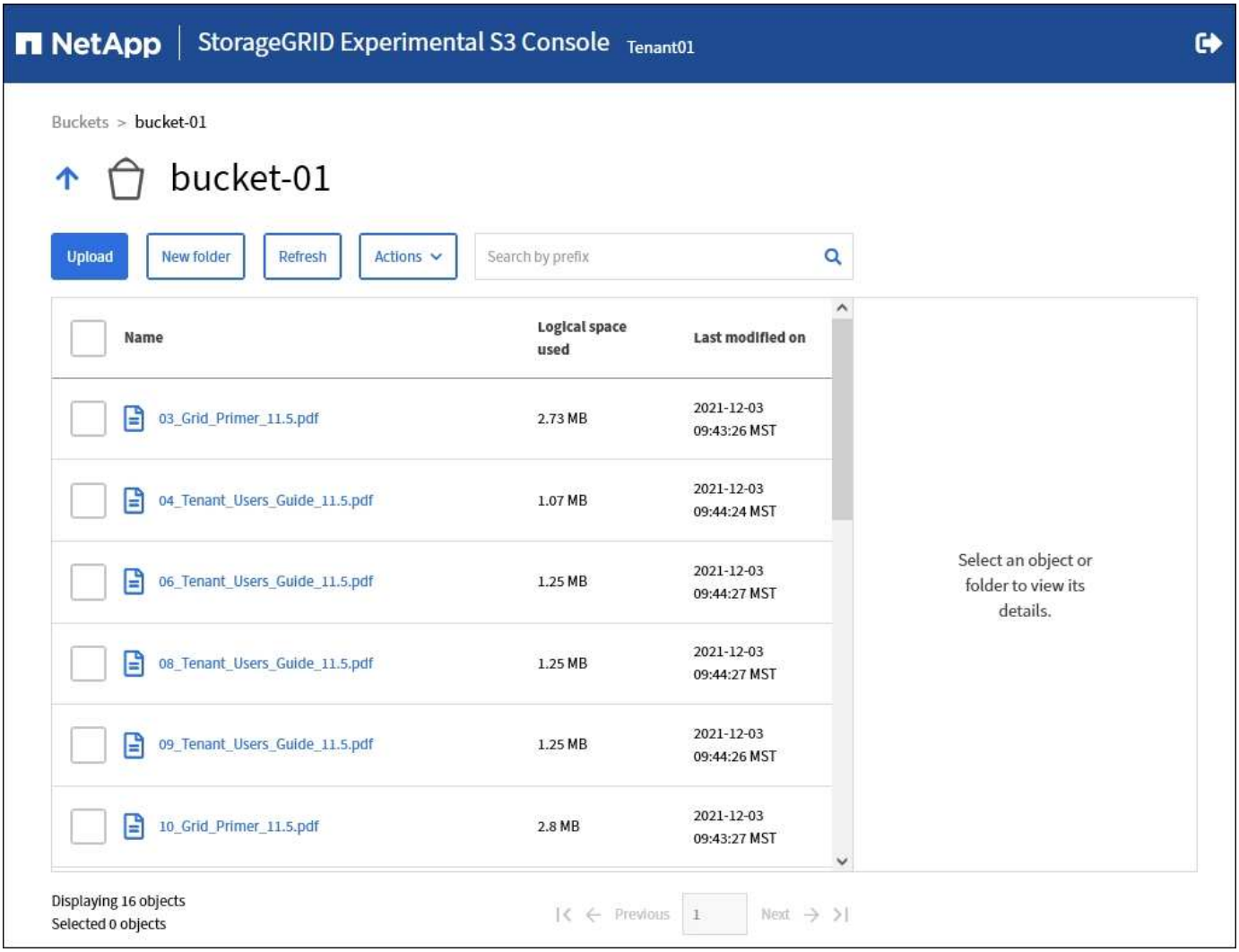
> S3 콘솔이 완전히 테스트되지 않았으며 "Experimental(실험)"으로 표시됩니다. 대량의 오브젝트 관리 또는 운영 환경에서 사용하기 위한 것이 아닙니다. 테넌트는 새로운 ILM 정책을 시뮬레이션하기 위해 개체를 업로드할 때, 수집 문제 해결 또는 개념 증명 또는 비운영 그리드를 사용하는 경우와 같이 소수의 개체에 대한 기능을 수행할 때만 S3 콘솔을 사용해야 합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있습니다.
- 버킷을 만들었습니다.
- 사용자의 액세스 키 ID와 비밀 액세스 키를 알고 있습니다. 필요한 경우 이 정보가 포함된 '.csv' 파일을 사용할 수 있습니다. 를 참조하십시오 액세스 키 생성에 대한 지침.

단계

1. Bucket * 을 선택합니다.
2. 를 선택합니다 Experimental S3 Console . 버킷 세부 정보 페이지에서 이 링크에 액세스할 수도 있습니다.
3. Experimental S3 Console 로그인 페이지에서 액세스 키 ID 및 비밀 액세스 키를 필드에 붙여 넣습니다. 그렇지 않으면 * 업로드 액세스 키 * 를 선택하고 '.csv' 파일을 선택합니다.
4. 로그인 * 을 선택합니다.
5. 필요에 따라 오브젝트 관리



S3 플랫폼 서비스 관리

플랫폼 서비스란 무엇입니까?

StorageGRID 플랫폼 서비스는 하이브리드 클라우드 전략을 구현하는 데 도움이 될 수 있습니다.

테넌트 계정에 플랫폼 서비스를 사용할 수 있는 경우 모든 S3 버킷에 대해 다음 서비스를 구성할 수 있습니다.

- * CloudMirror 복제 * StorageGRID CloudMirror 복제 서비스입니다 StorageGRID 버킷에서 지정된 외부 대상으로 특정 오브젝트를 미러링하는 데 사용됩니다.

  예를 들어, CloudMirror 복제를 사용하여 특정 고객 레코드를 Amazon S3에 미러링한 다음 AWS 서비스를 활용하여 데이터에 대한 분석을 수행할 수 있습니다.

  > 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.

- * 알림 *: 버킷당 이벤트 알림 지정된 외부 SNS(Amazon Simple Notification Service ™)에 객체에 대해 수행된 특정 작업에 대한 알림을 보내는 데 사용됩니다.

예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.

> S3 오브젝트 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(마지막 보존 날짜 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

- * 통합 서비스 검색 * 검색 통합 서비스 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있는 지정된 Elasticsearch 인덱스에 S3 개체 메타데이터를 전송하는 데 사용됩니다.

  예를 들어, S3 오브젝트 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷에 대한 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.

  > S3 오브젝트 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 구축과 외부적이기 때문에 플랫폼 서비스는 데이터에 대한 외부 스토리지 리소스, 알림 서비스 및 검색 또는 분석 서비스를 사용하여 얻을 수 있는 성능과 유연성을 제공합니다.

단일 S3 버킷에 대해 모든 플랫폼 서비스 조합을 구성할 수 있습니다. 예를 들어, StorageGRID S3 버킷에서 CloudMirror 서비스 및 알림을 모두 구성하여 특정 오브젝트를 Amazon Simple Storage Service에 미러링하고 이러한 각 오브젝트에 대한 알림을 타사 모니터링 애플리케이션에 전송하여 AWS 비용을 추적할 수 있도록 할 수 있습니다.

> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스 사용을 활성화해야 합니다.

플랫폼 서비스 구성 방법

플랫폼 서비스는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성한 외부 엔드포인트와 통신합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon 웹 서비스 버킷, SNS(Simple Notification Service) 주제 또는 로컬, AWS 또는 기타 위치에서 호스팅되는 Elasticsearch 클러스터와 같은 외부 대상을 나타냅니다.

끝점을 만든 후 버킷에 XML 구성을 추가하여 버킷에 대한 플랫폼 서비스를 활성화할 수 있습니다. XML 구성은 버킷이 작업해야 하는 오브젝트, 버킷이 취해야 하는 조치 및 버킷이 서비스에 사용해야 하는 엔드포인트를 식별합니다.

구성할 각 플랫폼 서비스에 대해 별도의 XML 구성을 추가해야 합니다. 예를 들면 다음과 같습니다.

1. 키가 '/images'로 시작하는 모든 오브젝트를 Amazon S3 버킷에 복제하려면 소스 버킷에 복제 구성을 추가해야 합니다.
2. 이러한 객체가 버킷에 저장될 때 알림을 보내려면 알림 구성을 추가해야 합니다.
3. 마지막으로 이러한 개체의 메타데이터를 인덱싱하려면 검색 통합을 구현하는 데 사용되는 메타데이터 알림 구성을 추가해야 합니다.

구성 XML의 형식은 StorageGRID 플랫폼 서비스를 구현하는 데 사용되는 S3 REST API를 통해 제어됩니다.

플랫폼 서비스	**S3 REST API**
CloudMirror 복제	• 버킷 복제를 가져옵니다 • 버킷 복제를 배치합니다
알림	• 버킷 알림을 받습니다 • 버킷 통지를 보냅니다
검색 통합	• Bucket 메타데이터 알림 구성 가져오기 • Put Bucket 메타데이터 알림 구성 이러한 작업은 StorageGRID에 맞게 맞춤형으로 제공됩니다.

StorageGRID에서 이러한 API를 구축하는 방법에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

관련 정보

플랫폼 서비스 사용에 대한 고려 사항

S3을 사용합니다

CloudMirror 복제 서비스

StorageGRID가 버킷에 추가된 지정된 오브젝트를 하나 이상의 대상 버킷에 복제하도록 하려면 S3 버킷에 대해 CloudMirror 복제를 활성화할 수 있습니다.

CloudMirror 복제는 그리드의 활성 ILM 정책과 독립적으로 작동합니다. CloudMirror 서비스는 소스 버킷에 저장된 객체를 복제하여 가능한 한 빨리 대상 버킷에 제공합니다. 오브젝트 수집의 성공 시 복제된 오브젝트 제공이 트리거됩니다.

기존 버킷에 대해 CloudMirror 복제를 설정하면 해당 버킷에 추가된 새 객체만 복제됩니다. 버킷의 기존 객체는 복제되지 않습니다. 기존 오브젝트의 복제를 강제로 수행하려면 오브젝트 복사를 수행하여 기존 오브젝트의 메타데이터를 업데이트할 수 있습니다.

> CloudMirror 복제를 사용하여 오브젝트를 AWS S3 대상으로 복사하는 경우 Amazon S3는 각 PUT 요청 헤더 내의 사용자 정의 메타데이터 크기를 2KB로 제한합니다. 객체에 2KB보다 큰 사용자 정의 메타데이터가 있는 경우 해당 객체가 복제되지 않습니다.

StorageGRID에서는 단일 버킷의 오브젝트를 여러 개의 대상 버킷으로 복제할 수 있습니다. 이렇게 하려면 복제 구성 XML에서 각 규칙의 대상을 지정합니다. 객체를 둘 이상의 버킷에 동시에 복제할 수 없습니다.

또한 버전 관리되거나 버전이 지정되지 않은 버킷에서 CloudMirror 복제를 구성하고 버전 관리되거나 버전이 지정되지 않은 버킷을 대상으로 지정할 수 있습니다. 버전 및 비버전 버킷의 모든 조합을 사용할 수 있습니다. 예를 들어 버전이 지정되지 않은 소스 버킷의 대상으로 버전 관리가 지정된 버킷을 지정하거나 그 반대로 지정할 수 있습니다. 버전이 지정되지 않은 버킷 간에 복제할 수도 있습니다.

CloudMirror 복제 서비스의 삭제 동작은 Amazon S3에서 제공하는 CRR(Cross Region Replication) 서비스의 삭제 동작과 같습니다. 소스 버킷에서 객체를 삭제해도 대상에서 복제된 객체는 삭제되지 않습니다. 소스 및 대상 버킷의

버전이 모두 지정된 경우 삭제 마커가 복제됩니다. 대상 버킷의 버전이 지정되지 않은 경우 소스 버킷에서 오브젝트를 삭제해도 삭제 마커가 대상 버킷에 복제되거나 대상 오브젝트가 삭제되지 않습니다.

객체가 대상 버킷에 복제되면 StorageGRID는 객체를 "replicas"로 표시합니다. 대상 StorageGRID 버킷은 복제본으로 표시된 객체를 다시 복제하지 않으므로 실수로 인한 복제 루프로부터 보호됩니다. 이 복제 마크는 StorageGRID 내부에 있으며 Amazon S3 버킷을 대상으로 사용할 때 AWS CRR을 활용하는 것을 방지하지 않습니다.

> 복제본을 표시하는 데 사용되는 사용자 지정 헤더는 X-NTAP-sg-replica입니다. 이 표시는 계단식 미러를 방지합니다. StorageGRID는 두 그리드 간의 양방향 CloudMirror를 지원합니다.

대상 버킷의 이벤트의 고유성과 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행된 작업의 결과로 소스 객체의 동일한 복제본이 두 개 이상 대상에 제공될 수 있습니다. 드물지만 둘 이상의 서로 다른 StorageGRID 사이트에서 동일한 객체가 동시에 업데이트되는 경우 대상 버킷의 작업 순서가 소스 버킷의 이벤트 순서와 일치하지 않을 수 있습니다.

CloudMirror 복제는 일반적으로 외부 S3 버킷을 대상으로 사용하도록 구성됩니다. 그러나 다른 StorageGRID 배포나 S3 호환 서비스를 사용하도록 복제를 구성할 수도 있습니다.

버킷에 대한 알림을 이해합니다

StorageGRID에서 지정된 이벤트에 대한 알림을 대상 SNS(Amazon Simple Notification Service)로 보내도록 하려면 S3 버킷에 대한 이벤트 알림을 활성화할 수 있습니다.

가능합니다 이벤트 알림을 구성합니다 알림 구성 XML을 소스 버킷과 연결합니다. 알림 구성 XML은 버킷 알림을 구성하기 위한 S3 규칙을 따르고, 엔드포인트의 URN으로 지정된 대상 SNS 항목을 따릅니다.

이벤트 알림은 알림 구성에 지정된 대로 소스 버킷에서 생성되며 대상으로 전달됩니다. 개체와 관련된 이벤트가 성공하면 해당 이벤트에 대한 알림이 생성되고 배달 대기 상태가 됩니다.

알림의 고유성과 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행된 작업의 결과로 하나 이상의 이벤트 알림이 대상에 전달될 수 있습니다. 그리고 납품이 비동기식이기 때문에, 특히 서로 다른 StorageGRID 사이트에서 발생하는 작업의 경우, 대상에서 알림의 시간 순서가 소스 버킷의 이벤트 순서와 일치한다고 보장할 수 없습니다. 이벤트 메시지에서 '시퀀스' 키를 사용하여 Amazon S3 문서에 설명된 대로 특정 객체에 대한 이벤트 순서를 결정할 수 있습니다.

지원되는 알림 및 메시지

StorageGRID 이벤트 알림은 Amazon S3 API를 따르며 다음과 같은 제한 사항이 적용됩니다.

- 다음 이벤트 유형에 대한 알림을 구성할 수 없습니다. 이러한 이벤트 유형은 * 지원되지 않습니다 *.
  - '3: RedundancyLostObject'를 선택합니다
  - '3:ObjectRestore:완료됨'
- StorageGRID에서 보낸 이벤트 알림은 표에 나와 있는 것처럼 일부 키를 포함하지 않고 다른 키에 대해 특정 값을 사용한다는 점을 제외하고 표준 JSON 형식을 사용합니다.

키 이름	**StorageGRID** 값
이벤트 소스	전쟁포로 S3

키 이름	**StorageGRID** 값
awsRegion	포함되지 않음
X-amz-id-2	포함되지 않음
ARN	"urn:SGWs:S3::bucket_name'

검색 통합 서비스를 이해합니다

오브젝트 메타데이터에 외부 검색 및 데이터 분석 서비스를 사용하려는 경우 S3 버킷에 대한 검색 통합을 활성화할 수 있습니다.

검색 통합 서비스는 오브젝트 또는 해당 메타데이터가 업데이트될 때마다 자동으로 그리고 비동기적으로 S3 오브젝트 메타데이터를 대상 끝점에 보내는 사용자 지정 StorageGRID 서비스입니다. 그런 다음 대상 서비스에서 제공하는 정교한 검색, 데이터 분석, 시각화 또는 머신 러닝 도구를 사용하여 오브젝트 데이터를 검색, 분석 및 분석할 수 있습니다.

버전 관리되거나 버전이 지정되지 않은 모든 버킷에 대해 검색 통합 서비스를 활성화할 수 있습니다. 검색 통합은 메타데이터 알림 구성 XML을 작업할 개체 및 개체 메타데이터에 대한 대상을 지정하는 버킷과 연결하여 구성됩니다.

알림은 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)로 명명된 JSON 문서의 형식으로 생성됩니다. 각 메타데이터 알림에는 개체의 모든 태그 및 사용자 메타데이터 외에도 개체에 대한 표준 시스템 메타데이터 세트가 포함되어 있습니다.

> 태그 및 사용자 메타데이터의 경우 StorageGRID는 날짜 및 숫자를 Elasticsearch에 문자열 또는 S3 이벤트 알림으로 전달합니다. 이러한 문자열을 날짜 또는 숫자로 해석하도록 Elasticsearch를 구성하려면 동적 필드 매핑 및 날짜 형식 매핑에 대한 Elasticsearch 지침을 따르십시오. 검색 통합 서비스를 구성하기 전에 인덱스에서 동적 필드 매핑을 활성화해야 합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 형식을 편집할 수 없습니다.

알림은 다음과 같은 경우에 생성되고 전송 대기 상태가 됩니다.

- 객체가 생성됩니다.
- 그리드의 ILM 정책 작업으로 인해 오브젝트가 삭제된 경우를 포함하여 오브젝트가 삭제됩니다.
- 오브젝트 메타데이터 또는 태그가 추가, 업데이트 또는 삭제됩니다. 메타데이터 및 태그의 전체 집합은 항상 변경된 값뿐만 아니라 업데이트 시 전송됩니다.

메타데이터 알림 구성 XML을 버킷에 추가하면 생성한 새 개체 및 데이터, 사용자 메타데이터 또는 태그를 업데이트하여 수정하는 모든 개체에 대한 알림이 전송됩니다. 그러나 버킷에 이미 있는 객체에 대해서는 알림이 전송되지 않습니다. 버킷의 모든 오브젝트에 대한 오브젝트 메타데이터가 대상으로 전송되도록 하려면 다음 중 하나를 수행해야 합니다.

- 버킷을 생성한 후 개체를 추가하기 전에 즉시 검색 통합 서비스를 구성합니다.
- 메타데이터 알림 메시지가 대상으로 전송되도록 버킷에 이미 있는 모든 객체에 대해 작업을 수행합니다.

StorageGRID 검색 통합 서비스는 Elasticsearch 클러스터를 대상으로 지원합니다. 다른 플랫폼 서비스와 마찬가지로 대상은 서비스의 구성 XML에서 URN이 사용되는 끝점에서 지정됩니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 지원되는 Elasticsearch 버전을 확인합니다.

관련 정보

검색 통합을 위한 구성 XML

메타데이터 알림에 포함된 개체 메타데이터입니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

검색 통합 서비스를 구성합니다

플랫폼 서비스 사용에 대한 고려 사항

플랫폼 서비스를 구현하기 전에 이러한 서비스를 사용하기 위한 권장 사항 및 고려 사항을 검토하십시오.

S3에 대한 자세한 내용은 을 참조하십시오 S3을 사용합니다.

플랫폼 서비스 사용에 대한 고려 사항

고려 사항	세부 정보
대상 엔드포인트 모니터링	각 대상 끝점의 가용성을 모니터링해야 합니다. 대상 끝점에 대한 연결이 오랜 시간 동안 손실되고 요청의 백로그가 많은 경우 StorageGRID에 대한 추가 클라이언트 요청(예: PUT 요청)이 실패합니다. 엔드포인트에 연결할 수 있게 되면 실패한 요청을 다시 시도해야 합니다.
대상 끝점 임계치 조절	요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다. 단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다. CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 영향을 받을 가능성이 더 높습니다.
주문 보증	StorageGRID은 사이트 내의 개체에 대한 작업을 주문할 수 있도록 보장합니다. 객체에 대한 모든 작업이 동일한 사이트 내에 있는 한 최종 객체 상태(복제의 경우)는 항상 StorageGRID의 상태와 동일합니다. StorageGRID는 StorageGRID 사이트 전체에서 작업이 수행되는 경우 요청을 주문하기 위해 최선의 노력을 다하고 있습니다. 예를 들어 처음에 사이트 A에 오브젝트를 작성한 다음 나중에 사이트 B에서 동일한 오브젝트를 덮어쓰는 경우 CloudMirror에서 대상 버킷에 복제한 최종 오브젝트는 새로운 오브젝트일 수 없습니다.

고려 사항	세부 정보
ILM 기반 오브젝트 삭제	AWS CRR 및 SNS 서비스의 삭제 동작과 일치하도록 StorageGRID ILM 규칙 때문에 소스 버킷의 객체가 삭제될 때 CloudMirror 및 이벤트 알림 요청이 전송되지 않습니다. 예를 들어 ILM 규칙이 14일 후에 개체를 삭제하는 경우 CloudMirror 또는 이벤트 알림 요청이 전송되지 않습니다. 반면, 검색 통합 요청은 ILM로 인해 객체가 삭제될 때 전송됩니다.

CloudMirror 복제 서비스 사용에 대한 고려 사항

고려 사항	세부 정보
복제 상태입니다	StorageGRID는 X-amz-replication-status 헤더를 지원하지 않습니다.
개체 크기	CloudMirror 복제 서비스를 통해 대상 버킷에 복제할 수 있는 개체의 최대 크기는 5TiB이며, 이는 maximum_supported_object 크기와 같습니다. • 참고 *: 단일 PUT 오브젝트 작업에 대한 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다.
버킷 버전 관리 및 버전 ID	StorageGRID의 소스 S3 버킷에서 버전 관리가 활성화된 경우 대상 버킷의 버전 관리도 활성화해야 합니다. 버전 관리를 사용할 때는 S3 프로토콜의 제한으로 인해 대상 버킷에서 오브젝트 버전 순서가 CloudMirror 서비스에 의해 보장되지 않는 것이 가장 좋습니다. • 참고 *: StorageGRID의 소스 버킷에 대한 버전 ID는 대상 버킷의 버전 ID와 관련이 없습니다.
개체 버전에 태그 달기	CloudMirror 서비스는 S3 프로토콜의 제한으로 인해 버전 ID를 제공하는 Put Object 태그 지정 또는 Delete Object 태그 지정 요청을 복제하지 않습니다. 소스 및 대상의 버전 ID는 관련이 없으므로 특정 버전 ID에 대한 태그 업데이트를 복제할 수 없습니다. 반면 CloudMirror 서비스는 Put Object 태그 지정 요청을 복제하거나 버전 ID를 지정하지 않는 Object 태그 지정 요청을 삭제합니다. 이러한 요청은 최신 키의 태그(또는 버킷의 버전이 지정된 경우 최신 버전)를 업데이트합니다. 태그가 있는 일반 베스트(업데이트 태그 지정 안 함)도 복제됩니다.
멀티파트 업로드 및 'ETag' 값	여러 부분 업로드를 사용하여 업로드한 개체를 미러링할 때 CloudMirror 서비스는 해당 파트를 보존하지 않습니다. 따라서 대칭 복사된 오브젝트의 ETag 값은 원래 오브젝트의 ETag 값과 다릅니다.
SSE-C로 암호화된 오브젝트(고객이 제공한 키를 사용한 서버측 암호화)	CloudMirror 서비스는 SSE-C로 암호화된 객체를 지원하지 않습니다 CloudMirror 복제를 위해 소스 버킷으로 객체를 수집하려고 하고 요청에 SSE-C 요청 헤더가 포함된 경우 작업이 실패합니다.

고려 사항	세부 정보
S3 오브젝트 잠금이 활성화된 버킷	CloudMirror 복제에 대한 대상 S3 버킷에서 S3 Object Lock이 활성화된 경우 버킷 복제(Put Bucket 복제)를 구성하려고 하면 AccessDenied 오류가 발생하고 실패합니다.

플랫폼 서비스 끝점을 구성합니다

버킷에 대한 플랫폼 서비스를 구성하려면 먼저 플랫폼 서비스의 대상으로 하나 이상의 엔드포인트를 구성해야 합니다.

플랫폼 서비스에 대한 액세스는 StorageGRID 관리자가 테넌트 단위로 사용하도록 설정합니다. 플랫폼 서비스 끝점을 만들거나 사용하려면 스토리지 노드가 외부 끝점 리소스에 액세스할 수 있도록 네트워킹이 구성된 그리드에서 끝점 관리 또는 루트 액세스 권한이 있는 테넌트 사용자여야 합니다. 자세한 내용은 StorageGRID 관리자에게 문의하십시오.

플랫폼 서비스 엔드포인트란 무엇입니까?

플랫폼 서비스 끝점을 만들 때 StorageGRID가 외부 대상에 액세스하는 데 필요한 정보를 지정합니다.

예를 들어, StorageGRID 버킷에서 AWS S3 버킷으로 오브젝트를 복제하려는 경우 StorageGRID에서 AWS의 대상 버킷에 액세스하는 데 필요한 정보와 자격 증명이 포함된 플랫폼 서비스 엔드포인트를 생성할 수 있습니다.

각 플랫폼 서비스 유형에는 고유한 엔드포인트가 필요하므로 사용하려는 각 플랫폼 서비스에 대해 하나 이상의 엔드포인트를 구성해야 합니다. 플랫폼 서비스 끝점을 정의한 후 서비스를 활성화하는 데 사용되는 구성 XML에서 끝점의 URN을 대상으로 사용합니다.

둘 이상의 소스 버킷에 대해 목적지와 동일한 끝점을 사용할 수 있습니다. 예를 들어, 여러 버킷에서 검색을 수행할 수 있도록 여러 소스 버킷을 구성하여 동일한 검색 통합 엔드포인트로 오브젝트 메타데이터를 보낼 수 있습니다. 또한 소스 버킷을 구성하여 둘 이상의 엔드포인트를 대상으로 사용할 수 있습니다. 이를 통해 하나의 SNS 항목에 개체 생성 알림을 보내고 개체 삭제에 대한 알림을 두 번째 SNS 항목으로 보내는 등의 작업을 수행할 수 있습니다.

CloudMirror 복제용 엔드포인트

StorageGRID는 S3 버킷을 나타내는 복제 엔드포인트를 지원합니다. 이러한 버킷은 Amazon Web Services, 동일한 또는 원격 StorageGRID 구축 또는 다른 서비스에서 호스팅될 수 있습니다.

알림의 끝점입니다

StorageGRID는 SNS(Simple Notification Service) 엔드포인트를 지원합니다. SQS(Simple Queue Service) 또는 AWS Lambda 엔드포인트는 지원되지 않습니다.

검색 통합 서비스의 끝점입니다

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

검색 통합 끝점은 특정 Elasticsearch 인덱스 및 유형을 참조합니다. StorageGRID에서 끝점을 만들기 전에 Elasticsearch에서 인덱스를 만들어야 합니다. 그렇지 않으면 끝점 생성이 실패합니다. 끝점을 만들기 전에 형식을 만들 필요가 없습니다. StorageGRID는 개체 메타데이터를 끝점으로 보낼 때 필요한 경우 형식을 만듭니다.

관련 정보

플랫폼 서비스 끝점에 **URN**을 지정합니다

플랫폼 서비스 끝점을 만들 때는 고유한 URN(리소스 이름)을 지정해야 합니다. 플랫폼 서비스에 대한 구성 XML을 만들 때 URN을 사용하여 끝점을 참조합니다. 각 끝점의 URN은 고유해야 합니다.

StorageGRID에서는 플랫폼 서비스 엔드포인트를 만들 때 이를 검증합니다. 플랫폼 서비스 끝점을 만들기 전에 끝점에 지정된 리소스가 있고 해당 리소스에 도달할 수 있는지 확인합니다.

urn 요소

플랫폼 서비스 끝점의 URN은 다음과 같이 "arn:AWS" 또는 "urn:mysite"로 시작해야 합니다.

- AWS(Amazon Web Services)에서 호스팅되는 서비스의 경우 'arn:AWS'를 사용합니다.
- 서비스가 GCP(Google Cloud Platform)에서 호스팅되는 경우 "arn:AWS"를 사용하십시오.
- 서비스가 로컬로 호스트되는 경우 urn:mysite를 사용합니다

예를 들어, StorageGRID에서 호스팅되는 CloudMirror 엔드포인트에 대해 URN을 지정하는 경우 URN은 "urn:SGWs"로 시작할 수 있습니다.

URN의 다음 요소는 다음과 같이 플랫폼 서비스의 유형을 지정합니다.

서비스	유형
CloudMirror 복제	S3
알림	SNS
검색 통합	ES

예를 들어, StorageGRID에서 호스팅되는 CloudMirror 엔드포인트에 대해 URN을 계속 지정하려면 's3'을 추가하여 urn:SGWs:s3'을 가져옵니다.

URN의 마지막 요소는 대상 URI에서 특정 대상 리소스를 식별합니다.

서비스	특정 리소스
CloudMirror 복제	버킷 이름
알림	SNS-주제-이름
검색 통합	domain-name/index-name/type-name'입니다 • 참고: * Elasticsearch 클러스터가 자동으로 인덱스를 만들도록 * 구성되지 * 인 경우 끝점을 만들기 전에 수동으로 인덱스를 만들어야 합니다.

AWS 및 GCP에서 호스팅되는 서비스의 여관

AWS 및 GCP 엔터티의 경우 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-name에는 여기에 나와 있는 리터럴 문자열 domain/"이 포함되어야 합니다.

현지 호스팅 서비스를 위한 여관

클라우드 서비스 대신 로컬로 호스팅된 서비스를 사용하는 경우 URN에 필요한 요소가 세 번째 및 최종 위치에 포함되어 있는 한 유효하고 고유한 URN을 만드는 방식으로 URN을 지정할 수 있습니다. 선택 사항으로 표시된 요소를 비워 두거나 자원을 식별하고 URN을 고유하게 만드는 데 도움이 되도록 원하는 방식으로 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

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

  StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 경우 "urn:SGW"로 시작하는 유효한 URN을 지정할 수 있습니다.

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

- 알림:

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

- 검색 통합:

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

> 로컬에서 호스팅되는 검색 통합 끝점의 경우 끝점의 URN이 고유하면 domain-name 요소는 모든 문자열이 될 수 있습니다.

플랫폼 서비스 끝점을 만듭니다

플랫폼 서비스를 사용하려면 먼저 올바른 유형의 끝점을 하나 이상 만들어야 합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 끝점 관리 권한이 있는 사용자 그룹에 속해야 합니다.
- 플랫폼 서비스 끝점에서 참조하는 리소스가 생성되어야 합니다.
  - CloudMirror 복제: S3 버킷
  - 이벤트 알림: SNS 항목
  - 검색 알림: 대상 클러스터가 인덱스를 자동으로 생성하도록 구성되지 않은 경우 Elasticsearch index입니다.
- 대상 리소스에 대한 정보가 있어야 합니다.
  - URI(Uniform Resource Identifier)의 호스트 및 포트

    > StorageGRID 시스템에서 호스팅되는 버킷을 CloudMirror 복제의 엔드포인트로 사용하려면 그리드 관리자에게 문의하여 입력해야 하는 값을 확인하십시오.

  - 고유 리소스 이름(URN)

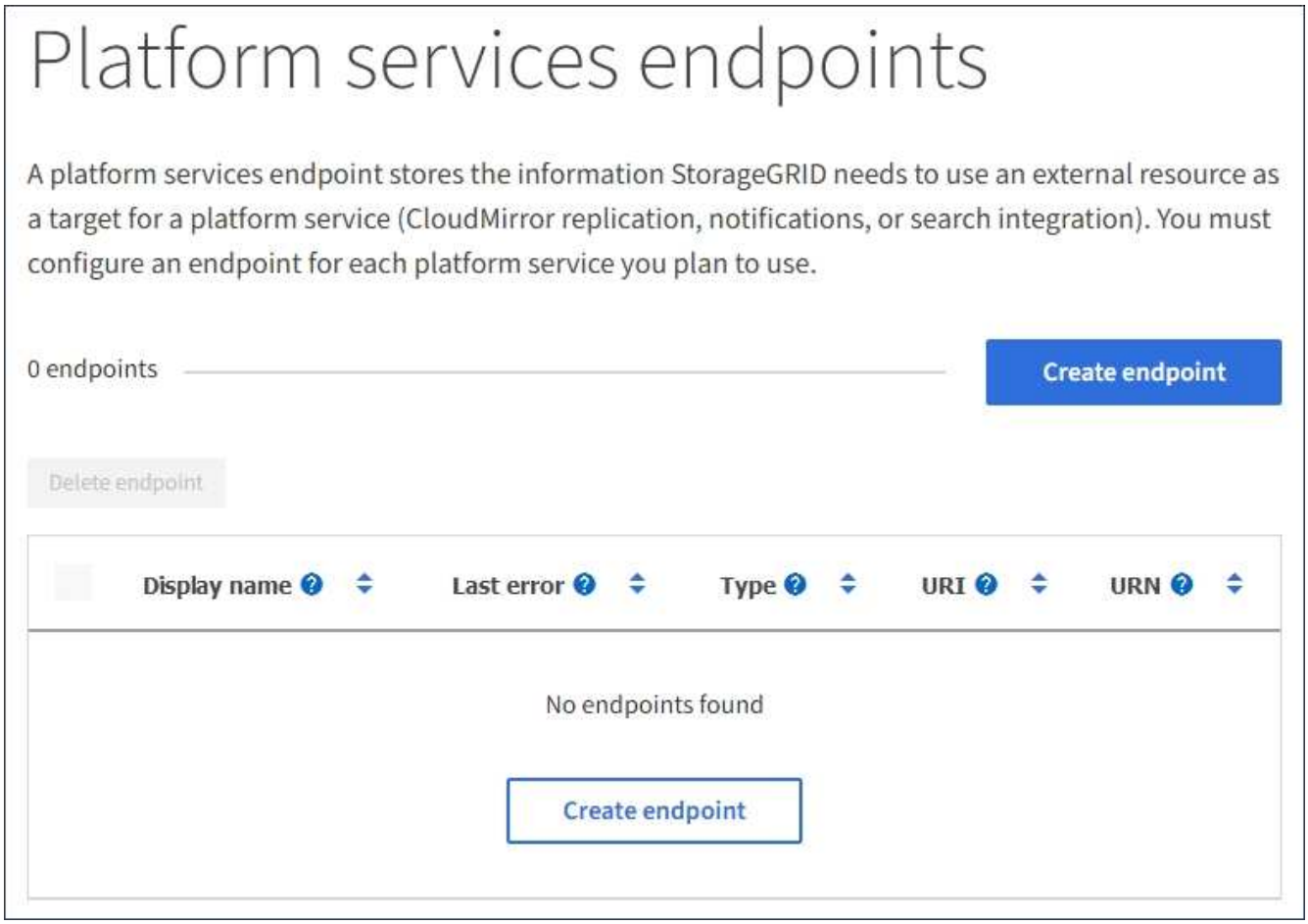
    플랫폼 서비스 끝점에 URN을 지정합니다

  - 인증 자격 증명(필요한 경우):
    - 액세스 키: 액세스 키 ID 및 비밀 액세스 키
    - 기본 HTTP: 사용자 이름 및 암호
    - CAP(C2S Access Portal): 임시 자격 증명 URL, 서버 및 클라이언트 인증서, 클라이언트 키 및 선택적 클라이언트 개인 키 암호.
  - 보안 인증서(사용자 지정 CA 인증서를 사용하는 경우)

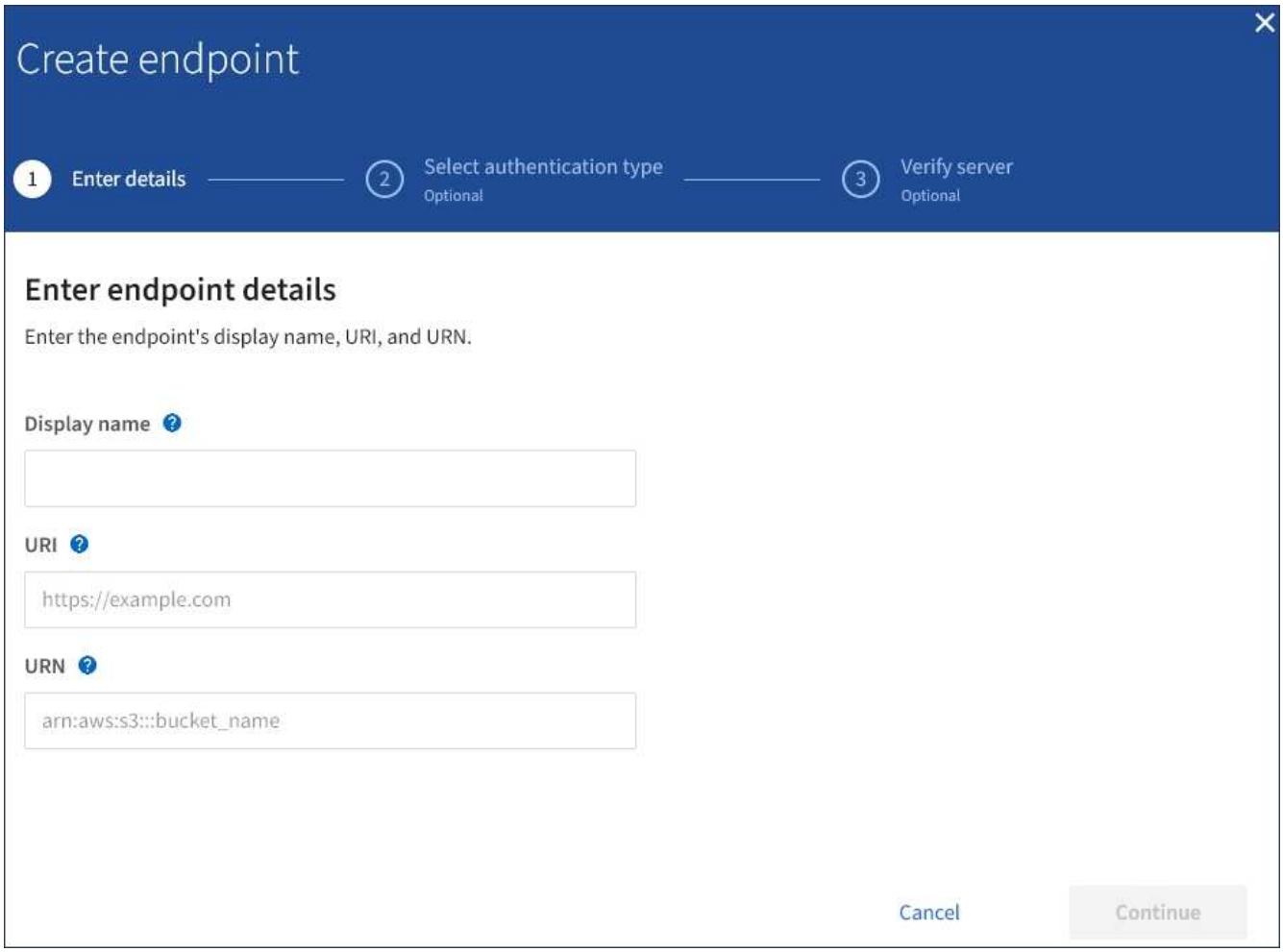
단계

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

   플랫폼 서비스 끝점 페이지가 나타납니다.



2. 끝점 만들기 * 를 선택합니다.



3. 표시 이름을 입력하여 끝점과 그 용도를 간략하게 설명합니다.

   끝점이 지원하는 플랫폼 서비스 유형은 끝점 페이지에 나열될 때 끝점 이름 옆에 표시됩니다. 따라서 이름에 해당 정보를 포함할 필요가 없습니다.

4. URI * 필드에서 끝점의 고유 URI(Resource Identifier)를 지정합니다.

   다음 형식 중 하나를 사용합니다.

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

   포트를 지정하지 않으면 포트 443이 HTTPS URI에 사용되고 포트 80은 HTTP URI에 사용됩니다.

   예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같습니다.

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

   이 예에서 '3.example.com'는 StorageGRID HA(High Availability) 그룹의 가상 IP(VIP)에 대한 DNS 항목을 나타내고, '10443'은 로드 밸런서 끝점에 정의된 포트를 나타냅니다.

가능하면 단일 장애 지점을 피하기 위해 로드 밸런싱 노드의 HA 그룹에 연결해야 합니다.

마찬가지로 AWS에서 호스팅되는 버킷의 URI는 다음과 같습니다.

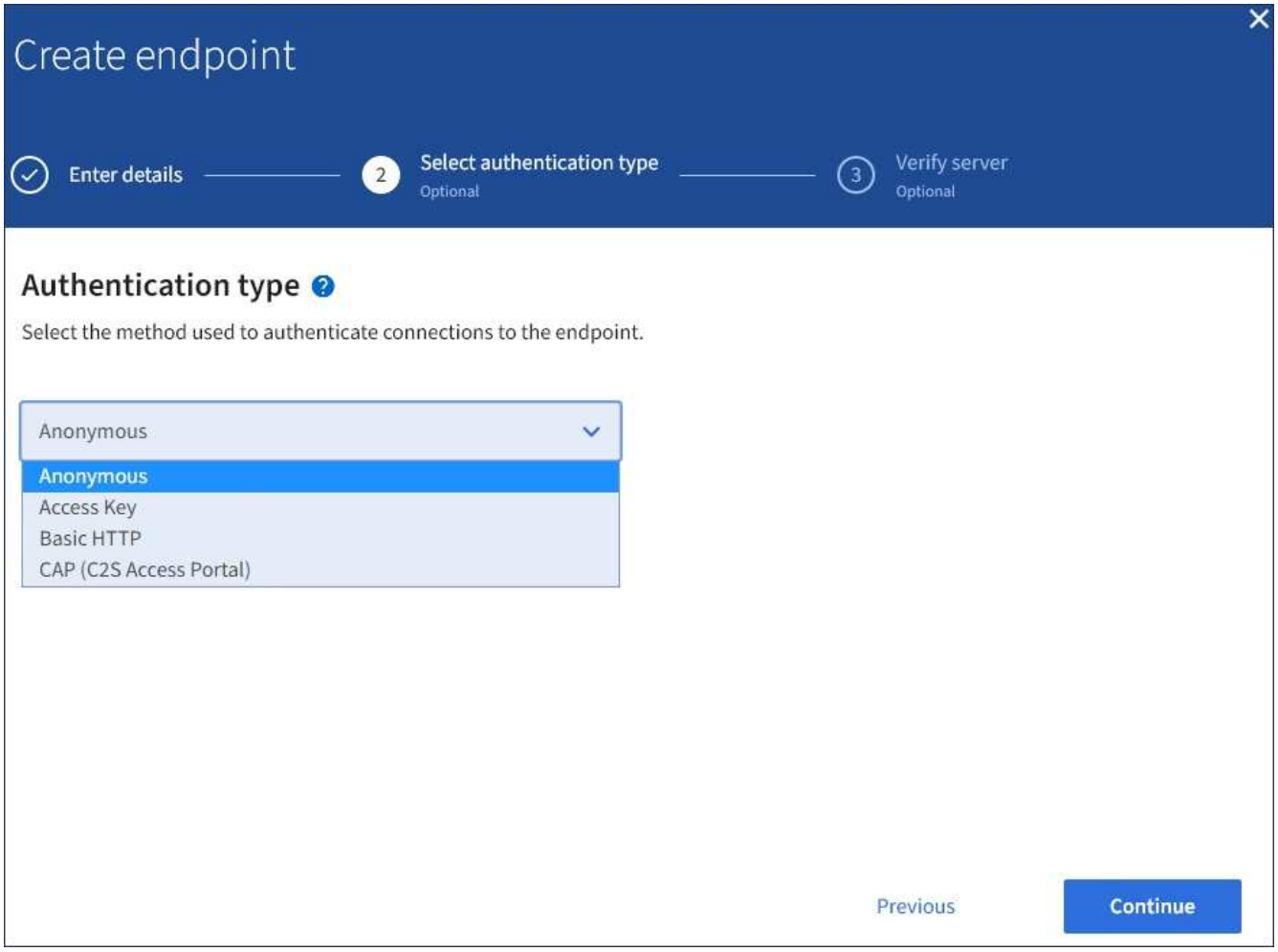
```
https://s3-aws-region.amazonaws.com
```

엔드포인트가 CloudMirror 복제 서비스에 사용되는 경우 버킷 이름을 URI에 포함하지 마십시오. 버킷 이름을 * URN * 필드에 포함시킵니다.

5. 끝점에 대한 고유 URN(리소스 이름)을 입력합니다.

   끝점이 생성된 후에는 끝점의 URN을 변경할 수 없습니다.

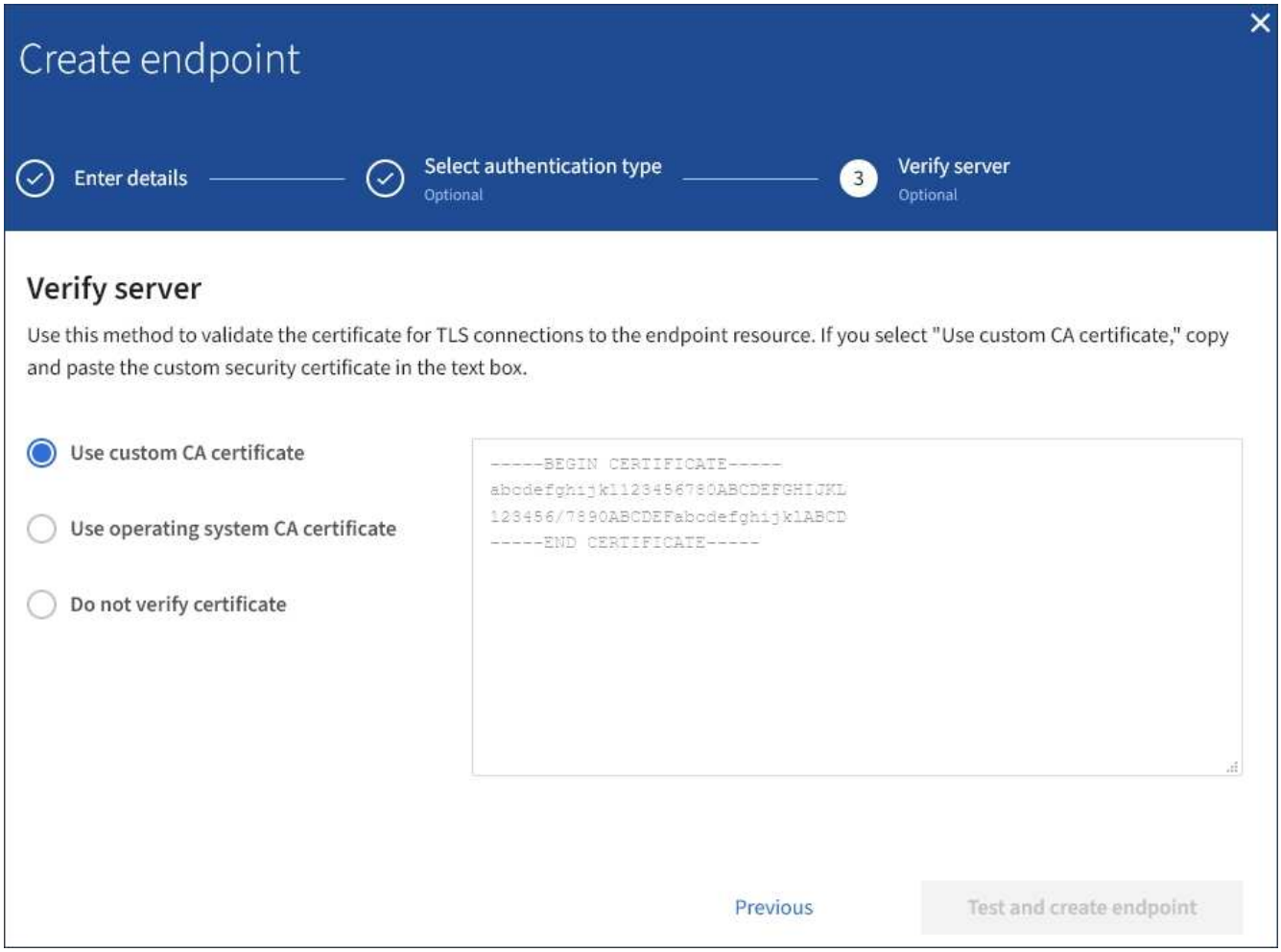
6. Continue * 를 선택합니다.
7. 인증 유형 * 의 값을 선택한 다음 필요한 자격 증명을 입력하거나 업로드합니다.



제공하는 자격 증명에 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

인증 유형입니다	설명	자격 증명
익명	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 끝점에서만 작동합니다.	인증이 없습니다.
액세스 키	AWS 스타일 자격 증명을 사용하여 대상과의 연결을 인증합니다.	• 액세스 키 ID입니다 • 비밀 액세스 키
기본 HTTP	사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
CAP(C2S 액세스 포털)	인증서 및 키를 사용하여 대상에 대한 연결을 인증합니다.	• 임시 자격 증명 URL입니다 • 서버 CA 인증서(PEM 파일 업로드) • 클라이언트 인증서(PEM 파일 업로드) • 클라이언트 개인 키(PEM 파일 업로드, OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식) • 클라이언트 개인 키 암호 구문(선택 사항)

8. Continue * 를 선택합니다.
9. 끝점에 대한 TLS 연결을 확인하는 방법을 선택하려면 * 서버 확인 * 에 대한 라디오 버튼을 선택합니다.



인증서 확인 유형입니다	설명
사용자 지정 CA 인증서를 사용합니다	사용자 지정 보안 인증서를 사용합니다. 이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다. 이 옵션은 안전하지 않습니다.

10. 테스트를 선택하고 끝점 * 을 작성합니다.
    - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
    - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 오류를 수정하기 위해 끝점을 수정해야 하는 경우 * 끝점 세부 정보로 돌아가기 * 를 선택하고 정보를 업데이트합니다. 그런 다음 * 테스트 를 선택하고 끝점 * 을 만듭니다.

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

끝점을 구성한 후 URN을 사용하여 플랫폼 서비스를 구성할 수 있습니다.

관련 정보

플랫폼 서비스 끝점에 URN을 지정합니다

CloudMirror 복제를 구성합니다

이벤트 알림을 구성합니다

검색 통합 서비스를 구성합니다

플랫폼 서비스 끝점에 대한 연결을 테스트합니다

플랫폼 서비스에 대한 연결이 변경된 경우 끝점에 대한 연결을 테스트하여 대상 리소스가 있는지 그리고 지정한 자격 증명을 사용하여 해당 리소스에 연결할 수 있는지 확인할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 끝점 관리 권한이 있는 사용자 그룹에 속해야 합니다.

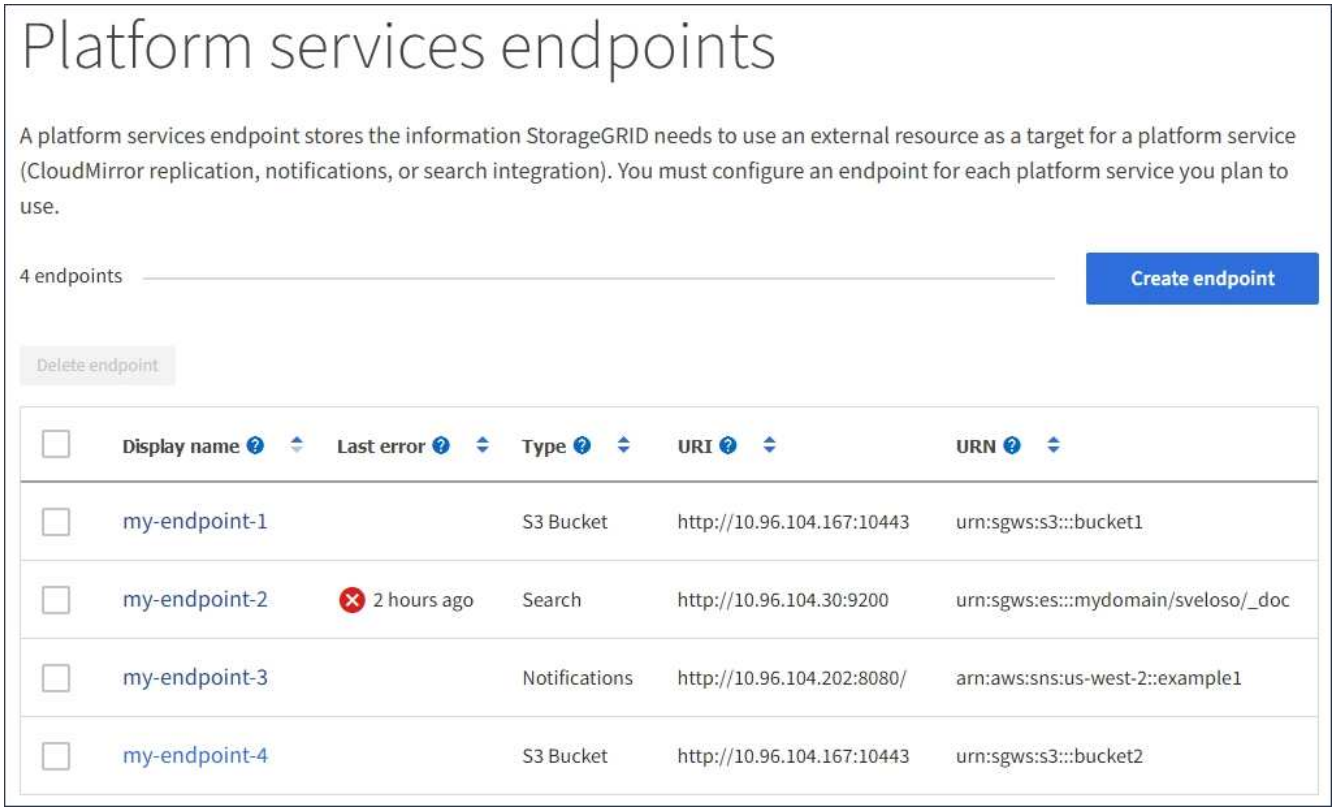
이 작업에 대해

StorageGRID는 자격 증명에 올바른 권한이 있는지 확인하지 않습니다.

단계

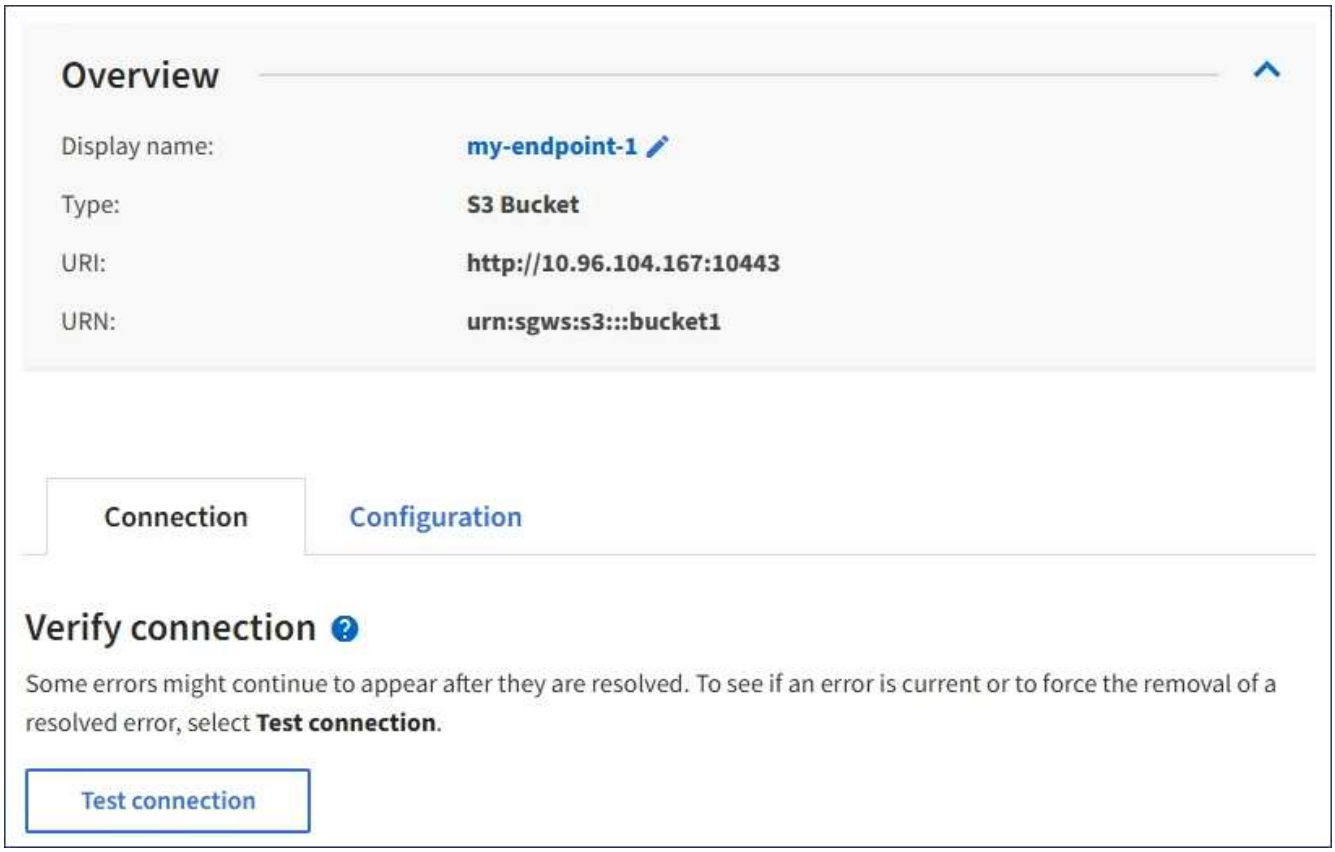
1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다.

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



2. 연결을 테스트할 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.



3. Test connection * 을 선택합니다.
   - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
   - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 오류를 정정하기 위해 끝점을 수정해야 하는 경우 * 구성 * 을 선택하고 정보를 업데이트합니다. 그런 다음 * 테스트 및 변경 내용 저장 * 을 선택합니다.

플랫폼 서비스 끝점을 편집합니다

플랫폼 서비스 끝점의 구성을 편집하여 이름, URI 또는 기타 세부 정보를 변경할 수 있습니다. 예를 들어 만료된 자격 증명을 업데이트하거나 대체 작동을 위한 백업 Elasticsearch 인덱스를 가리키도록 URI를 변경해야 할 수 있습니다. 플랫폼 서비스 끝점의 URN은 변경할 수 없습니다.

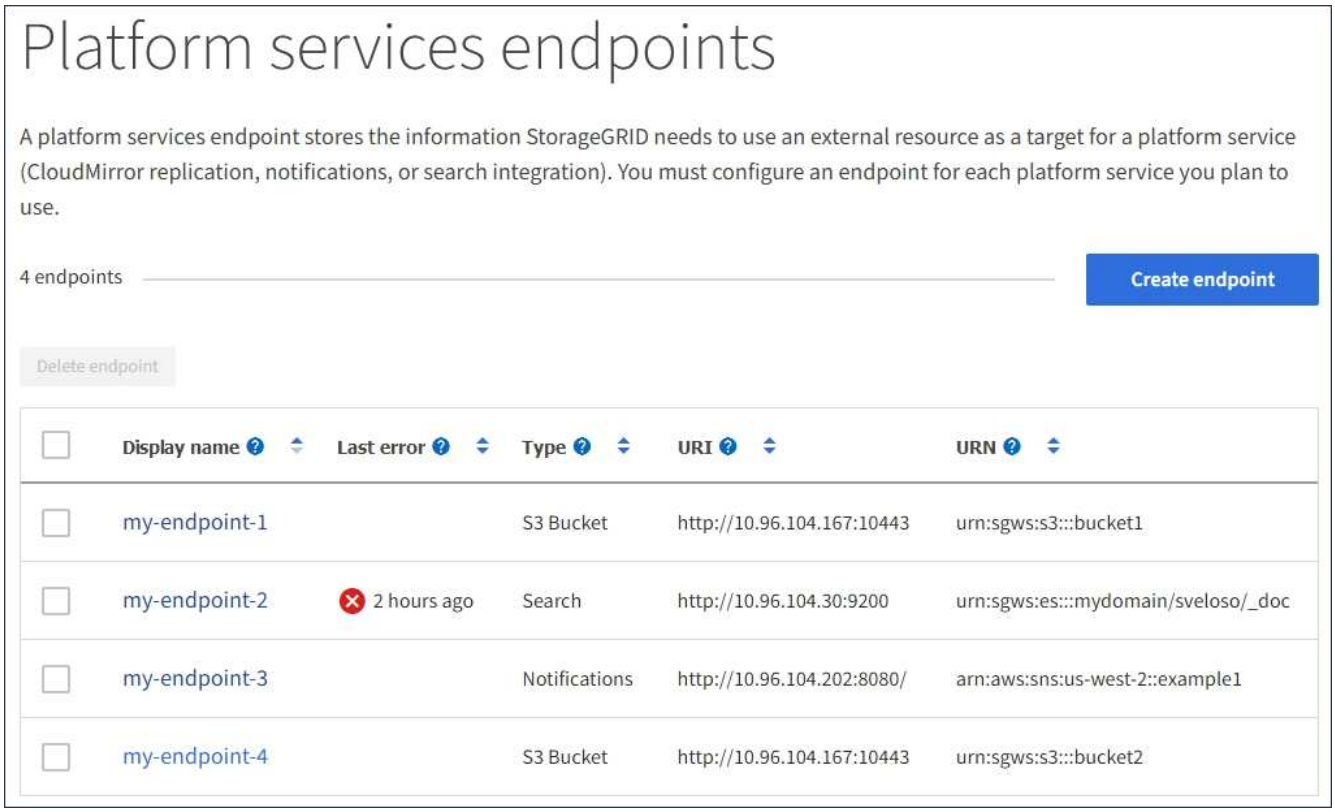
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 끝점 관리 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

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

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



2. 편집할 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.

3. Configuration * 을 선택합니다.

Overview

Display name:	my-endpoint-3
Type:	Notifications
URI:	http://10.96.104.202:8080/
URN:	arn:aws:sns:us-west-2::example1

Connection | Configuration

Edit configuration

Endpoint details

URI

http://10.96.104.202:8080/

URN

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP

Username

testme

Password

••••••••

Edit password

Verify server

- Use custom CA certificate
- Use operating system CA certificate
- Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
```

Test and save changes

4. 필요에 따라 끝점의 구성을 변경합니다.

> 끝점이 생성된 후에는 끝점의 URN을 변경할 수 없습니다.

   a. 끝점의 표시 이름을 변경하려면 편집 아이콘을 선택합니다 .
   b. 필요에 따라 URI를 변경합니다.
   c. 필요에 따라 인증 유형을 변경합니다.
      - 액세스 키 인증의 경우 * S3 키 편집 * 을 선택하고 새 액세스 키 ID 및 비밀 액세스 키를 붙여 넣어 필요에 따라 키를 변경합니다. 변경 사항을 취소하려면 * S3 키 편집 되돌리기 * 를 선택합니다.
      - 기본 HTTP 인증의 경우 필요에 따라 사용자 이름을 변경합니다. 필요에 따라 * 암호 편집 * 을 선택하고 새 암호를 입력하여 암호를 변경합니다. 변경 사항을 취소해야 하는 경우 * 암호 편집 되돌리기 * 를 선택합니다.
      - CAP(C2S Access Portal) 인증의 경우 임시 자격 증명 URL 또는 선택적 클라이언트 개인 키 암호를 변경하고 필요에 따라 새 인증서 및 키 파일을 업로드합니다.

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

   d. 필요에 따라 서버 확인 방법을 변경합니다.
5. Test(테스트)를 선택하고 변경 내용을 저장합니다 *.
   - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 확인합니다.
   - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 끝점을 수정하여 오류를 수정한 다음 * 테스트 및 변경 내용 저장 * 을 선택합니다.

플랫폼 서비스 끝점을 삭제합니다

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

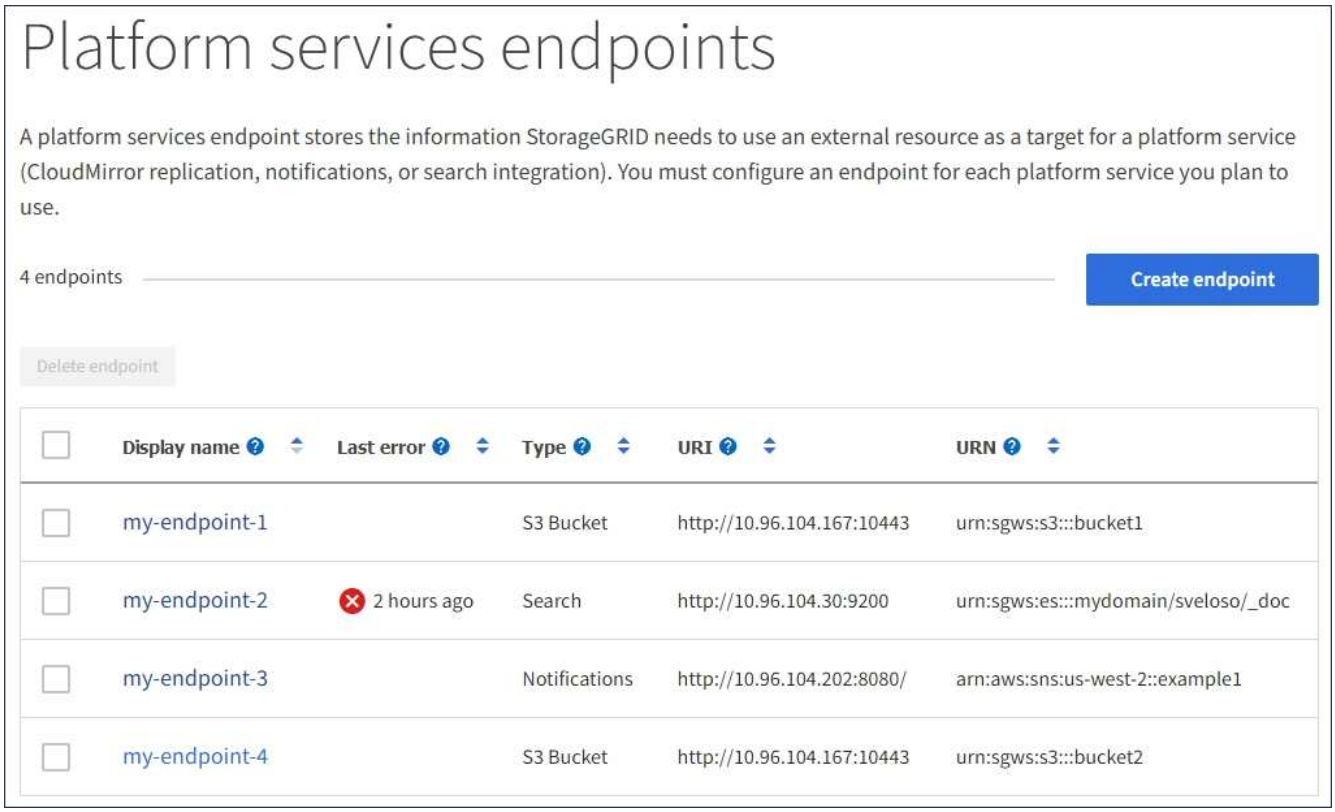
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 끝점 관리 * 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

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

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

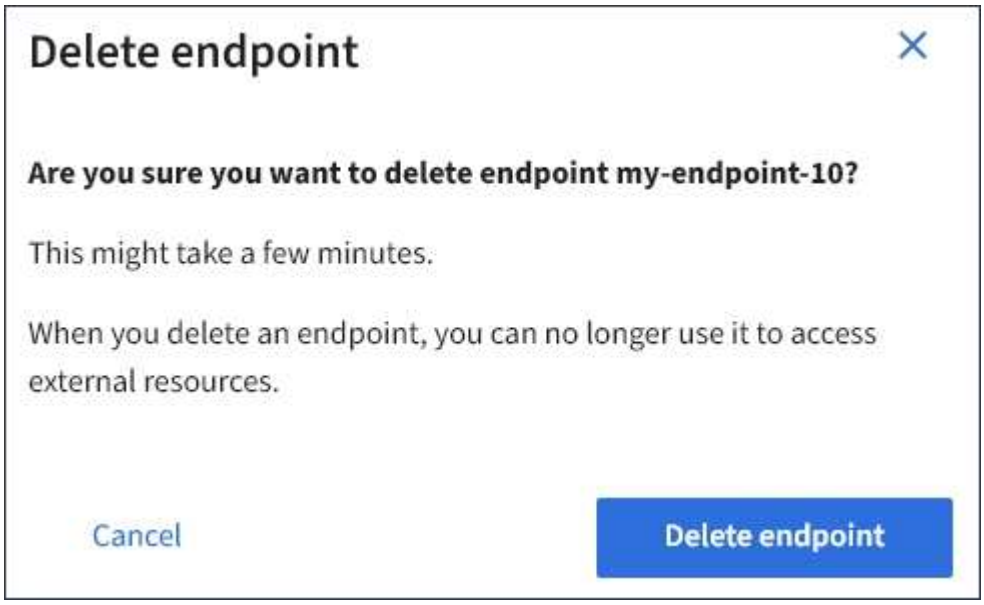


2. 삭제할 각 끝점의 확인란을 선택합니다.

> 사용 중인 플랫폼 서비스 끝점을 삭제하면 해당 끝점을 사용하는 모든 버킷에 대해 연결된 플랫폼 서비스가 비활성화됩니다. 아직 완료되지 않은 요청은 삭제됩니다. 삭제된 URN을 더 이상 참조하지 않도록 버킷 구성을 변경할 때까지 새 요청은 계속 생성됩니다. StorageGRID는 이러한 요청을 복구할 수 없는 오류로 보고합니다.

3. 작업 * > * 끝점 삭제 * 를 선택합니다.

   확인 메시지가 나타납니다.



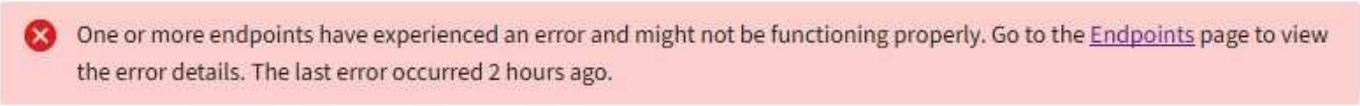
4. 끝점 삭제 * 를 선택합니다.

플랫폼 서비스 끝점 오류 문제 해결

StorageGRID가 플랫폼 서비스 끝점과 통신하려고 할 때 오류가 발생하면 대시보드에 메시지가 표시됩니다. 플랫폼 서비스 끝점 페이지에서 마지막 오류 열은 오류가 발생한 시간을 나타냅니다. 끝점의 자격 증명과 연결된 권한이 올바르지 않으면 오류가 표시되지 않습니다.

오류가 발생했는지 확인합니다

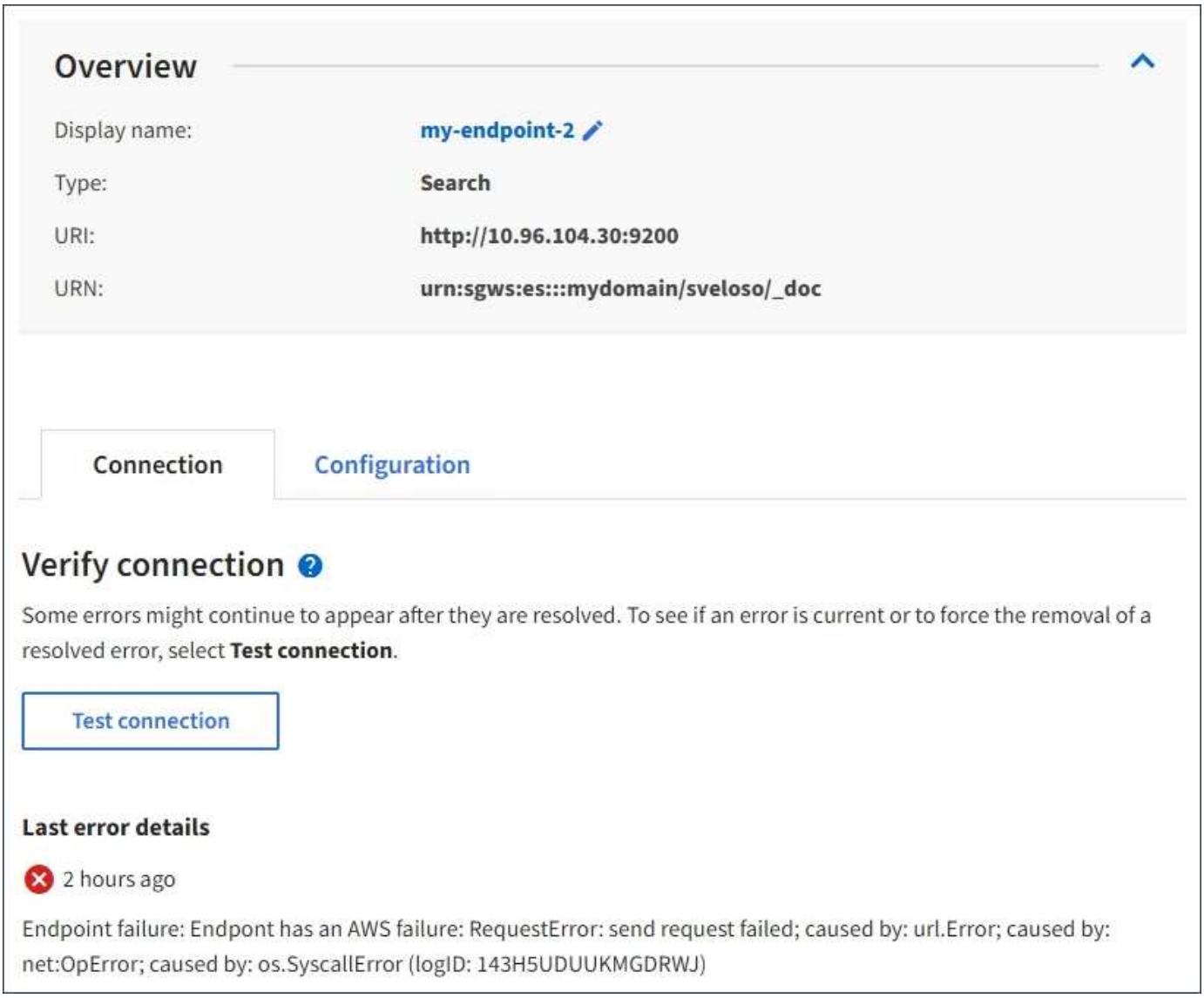
지난 7일 이내에 플랫폼 서비스 끝점 오류가 발생한 경우 테넌트 관리자 대시보드에 경고 메시지가 표시됩니다. 플랫폼 서비스 끝점 페이지로 이동하여 오류에 대한 자세한 정보를 볼 수 있습니다.



대시보드에 나타나는 동일한 오류가 플랫폼 서비스 끝점 페이지 맨 위에도 나타납니다. 자세한 오류 메시지를 보려면:

단계

1. 끝점 목록에서 오류가 있는 끝점을 선택합니다.
2. 끝점 세부 정보 페이지에서 * 연결 * 을 선택합니다. 이 탭은 끝점에 대한 가장 최근 오류만 표시하고 오류가 발생한 시간을 표시합니다. 빨간색 X 아이콘이 포함된 오류 지난 7일 이내에 발생했습니다.



오류가 여전히 최신 상태인지 확인합니다

일부 오류는 해결된 후에도 * 마지막 오류 * 열에 계속 표시될 수 있습니다. 오류가 현재 오류인지 확인하거나 테이블에서 해결된 오류를 강제로 제거하려면 다음과 같이 하십시오.

단계

1. 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.

2. 연결 * > * 연결 테스트 * 를 선택합니다.

연결 테스트 * 를 선택하면 StorageGRID가 플랫폼 서비스 끝점이 있는지, 그리고 현재 자격 증명으로 연결할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 오류를 해결합니다

끝점 세부 정보 페이지의 * 마지막 오류 * 메시지를 사용하여 오류의 원인을 확인할 수 있습니다. 일부 오류에서는 문제를 해결하기 위해 끝점을 편집해야 할 수 있습니다. 예를 들어, 올바른 액세스 권한이 없거나 액세스 키가 만료되어 StorageGRID가 대상 S3 버킷을 액세스할 수 없는 경우 클라우드미러링 오류가 발생할 수 있습니다. 이 메시지는

""끝점 자격 증명이나 대상 액세스 업데이트 필요""이며 세부 정보는 ""AccessDenied"" 또는 ""InvalidAccessKeyId""입니다.

오류를 해결하기 위해 끝점을 편집해야 하는 경우 * 테스트 및 변경 내용 저장 * 을 선택하면 StorageGRID가 업데이트된 끝점을 검증하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

단계

1. 끝점을 선택합니다.
2. 끝점 세부 정보 페이지에서 * 구성 * 을 선택합니다.
3. 필요에 따라 끝점 설정을 편집합니다.
4. 연결 * > * 연결 테스트 * 를 선택합니다.

권한이 부족한 끝점 자격 증명

StorageGRID에서 플랫폼 서비스 끝점의 유효성을 검사할 때 끝점의 자격 증명을 사용하여 대상 리소스에 연결할 수 있는지 확인하고 기본적인 사용 권한 검사를 수행합니다. 그러나 StorageGRID는 특정 플랫폼 서비스 작업에 필요한 모든 사용 권한의 유효성을 검사하지 않습니다. 따라서 플랫폼 서비스("403 사용 금지" 등)를 사용할 때 오류가 발생하면 끝점의 자격 증명과 관련된 권한을 확인하십시오.

추가 플랫폼 서비스 문제 해결

플랫폼 서비스 문제 해결에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

StorageGRID 관리

관련 정보

플랫폼 서비스 끝점을 만듭니다

플랫폼 서비스 끝점에 대한 연결을 테스트합니다

플랫폼 서비스 끝점을 편집합니다

CloudMirror 복제를 구성합니다

를 클릭합니다 CloudMirror 복제 서비스 는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. CloudMirror 복제를 사용하여 오브젝트를 외부 S3 버킷에 자동으로 복제할 수 있습니다.

필요한 것

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 복제 소스로 사용할 버킷을 이미 생성해야 합니다.
- CloudMirror 복제의 대상으로 사용하려는 엔드포인트가 이미 있어야 하며 URN이 있어야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이 권한을 사용하여 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

CloudMirror 복제는 소스 버킷에서 엔드포인트에 지정된 대상 버킷으로 객체를 복제합니다. 버킷에 대해 CloudMirror 복제를 설정하려면 유효한 버킷 복제 구성 XML을 생성하고 적용해야 합니다. 복제 구성 XML은 각 대상에 대해 S3 버킷 엔드포인트의 URN을 사용해야 합니다.

> S3 오브젝트 잠금이 활성화된 소스 또는 대상 버킷에는 복제가 지원되지 않습니다.

버킷 복제 및 구성 방법에 대한 일반적인 정보는 교차 지역 복제(CRR)에 대한 Amazon Simple Storage Service(S3) 설명서를 참조하십시오. StorageGRID에서 S3 버킷 복제 구성 API를 구현하는 방법에 대한 자세한 내용은 를 참조하십시오 S3 클라이언트 애플리케이션 구현 지침.

객체가 포함된 버킷에서 CloudMirror 복제를 활성화하면 버킷에 추가된 새 객체가 복제되지만 버킷의 기존 객체는 복제되지 않습니다. 복제를 트리거하려면 기존 객체를 업데이트해야 합니다.

복제 구성 XML에서 스토리지 클래스를 지정하는 경우 StorageGRID는 대상 S3 끝점에 대해 작업을 수행할 때 해당 클래스를 사용합니다. 대상 끝점은 지정된 저장소 클래스도 지원해야 합니다. 대상 시스템 공급업체에서 제공하는 권장 사항을 따르십시오.

단계

1. 소스 버킷에 대한 복제 지원:

   텍스트 편집기를 사용하여 S3 복제 API에 지정된 대로 복제를 활성화하는 데 필요한 복제 구성 XML을 생성합니다. XML을 구성할 때:

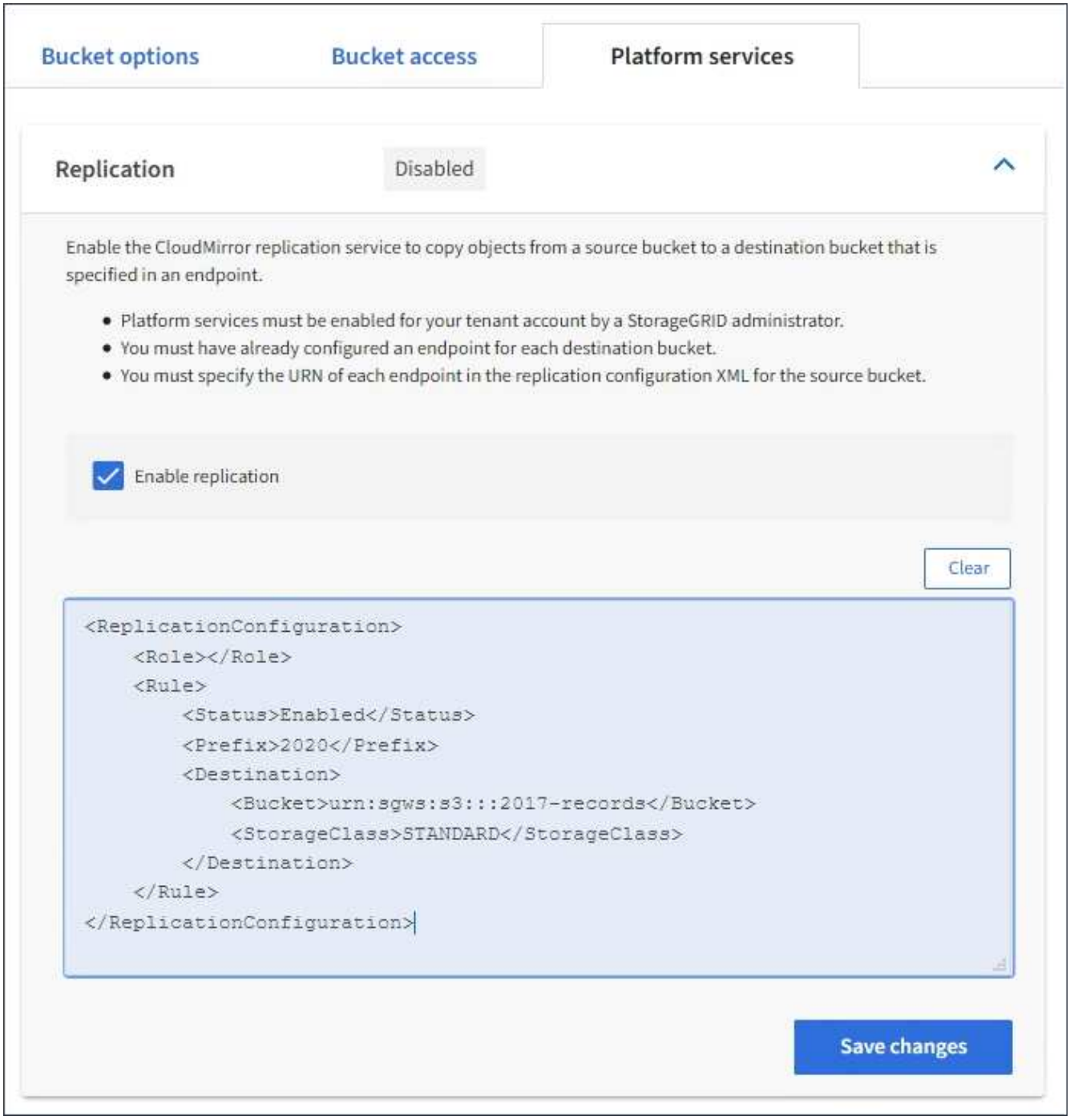
   - StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 대해 'Filter' 요소의 사용을 지원하지 않으며 개체 버전 삭제에 대해서는 V1 규약을 따릅니다. 자세한 내용은 복제 구성에 대한 Amazon 설명서를 참조하십시오.
   - S3 버킷 엔드포인트의 URN을 대상으로 사용합니다.
   - 필요한 경우 "<StorageClass>" 요소를 추가하고 다음 중 하나를 지정합니다.
     - 'Standard': 기본 스토리지 클래스. 객체를 업로드할 때 스토리지 클래스를 지정하지 않으면 '표준' 스토리지 클래스가 사용됩니다.
     - S tandard_IA: (Standard - Infrequent Access) 액세스 빈도가 낮지만 필요한 경우 빠른 액세스가 필요한 데이터에 이 스토리지 클래스를 사용합니다.
     - Reduced_redundancy: standard 스토리지 클래스보다 중복성이 적은 비위험, 재현 가능한 데이터에 이 스토리지 클래스를 사용합니다.
   - 구성 XML에서 Role을 지정하면 무시됩니다. 이 값은 StorageGRID에서 사용되지 않습니다.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 복제 * 를 선택합니다.
5. 복제 사용 * 확인란을 선택합니다.
6. 복제 구성 XML을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 복제가 올바르게 구성되었는지 확인합니다.
   a. 복제 구성에 지정된 대로 복제 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞서 설명한 예에서는 접두사 "2020"과 일치하는 객체가 복제됩니다.

   b. 객체가 대상 버킷에 복제되었는지 확인합니다.

      오브젝트 크기가 작은 경우 복제가 빠르게 수행됩니다.

관련 정보

S3을 사용합니다

플랫폼 서비스 끝점을 만듭니다

이벤트 알림을 구성합니다

알림 서비스는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. 버킷에 대한 알림을 활성화하여 지정된 이벤트에 대한 정보를 AWS SNS(Simple Notification Service ™)를 지원하는 대상 서비스로 전송할 수 있습니다.

필요한 것

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 알림 소스로 사용하려면 이미 버킷을 만들어야 합니다.
- 이벤트 알림 대상으로 사용하려는 엔드포인트가 이미 있어야 하며 URN이 있어야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이 권한을 사용하여 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

이벤트 알림을 구성한 후 소스 버킷의 개체에 대해 지정된 이벤트가 발생할 때마다 알림이 생성되어 대상 끝점으로 사용되는 SNS(Simple Notification Service) 항목으로 전송됩니다. 버킷에 대한 알림을 활성화하려면 유효한 알림 구성 XML을 생성하고 적용해야 합니다. 알림 구성 XML은 각 대상에 대해 이벤트 알림 끝점의 URN을 사용해야 합니다.

이벤트 알림 및 구성 방법에 대한 일반 정보는 아마존 문서를 참조하십시오. StorageGRID에서 S3 버킷 알림 구성 API를 구현하는 방법에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

객체가 포함된 버킷에 대해 이벤트 알림을 활성화하면 알림 구성이 저장된 후 수행되는 작업에 대해서만 알림이 전송됩니다.

단계

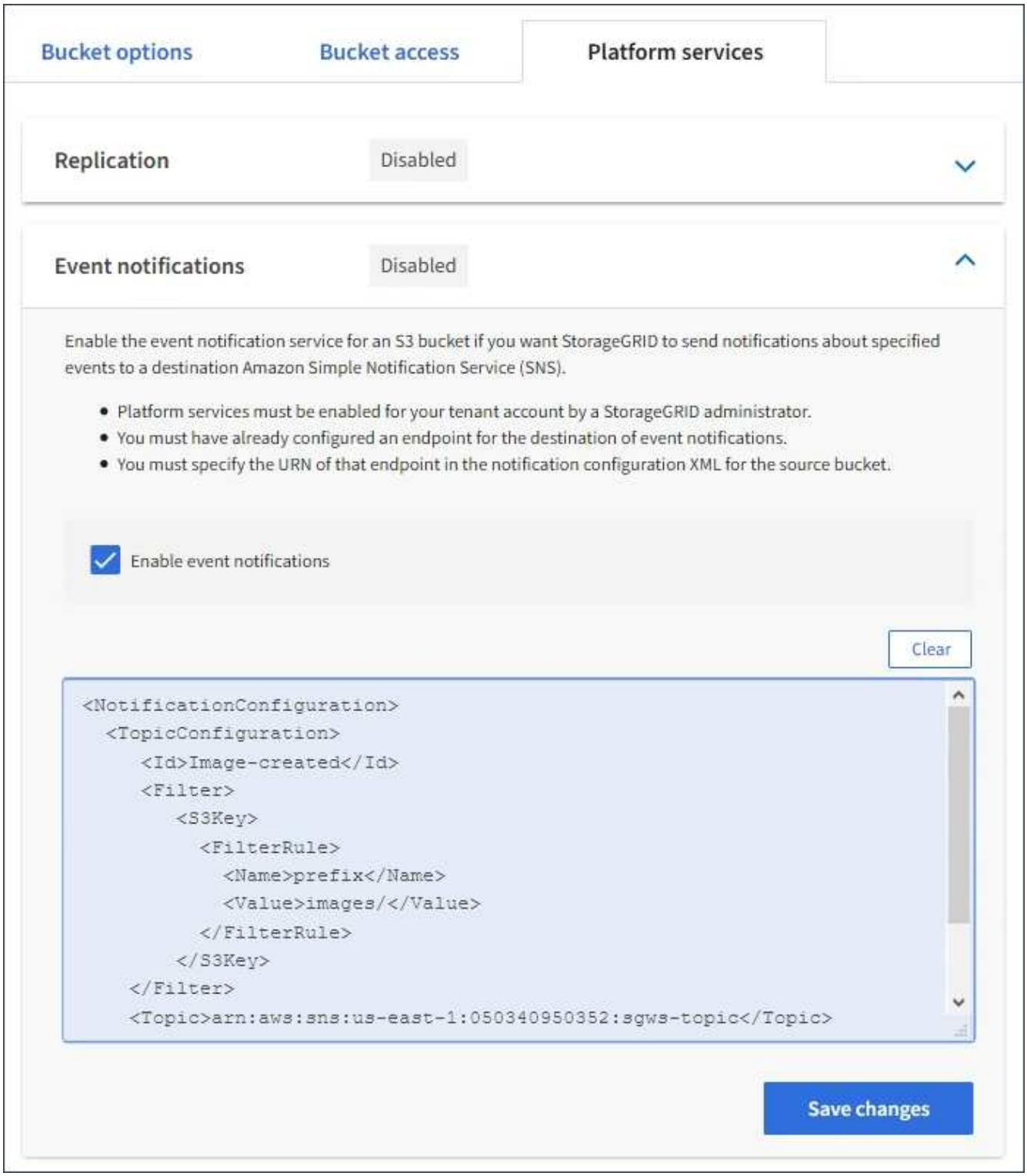
1. 소스 버킷에 대한 알림 활성화:
    - 텍스트 편집기를 사용하여 S3 알림 API에 지정된 대로 이벤트 알림을 활성화하는 데 필요한 알림 구성 XML을 생성합니다.
    - XML을 구성할 때는 이벤트 알림 끝점의 URN을 대상 항목으로 사용합니다.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 이벤트 알림 * 을 선택합니다.
5. 이벤트 알림 사용 * 확인란을 선택합니다.
6. 알림 구성 XML을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 이벤트 알림이 올바르게 구성되었는지 확인합니다.

   a. 구성 XML에 구성된 알림을 트리거하기 위한 요구 사항을 충족하는 소스 버킷의 객체에 대한 작업을 수행합니다.

이 예제에서는 "images/" 접두사로 객체를 만들 때마다 이벤트 알림이 전송됩니다.

b. 알림이 대상 SNS 항목으로 전달되었는지 확인합니다.

예를 들어 대상 주제가 AWS SNS(Simple Notification Service)에 호스팅된 경우, 알림 전송 시 이메일을 보내도록 서비스를 구성할 수 있습니다.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"1111111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"1111111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


대상 항목에서 알림이 수신되면 StorageGRID 알림에 대한 소스 버킷을 성공적으로 구성한 것입니다.

관련 정보

버킷에 대한 알림을 이해합니다

S3을 사용합니다

플랫폼 서비스 끝점을 만듭니다

검색 통합 서비스를 사용합니다

검색 통합 서비스는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. 오브젝트 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 오브젝트 메타데이터를 전송하도록 이 서비스를 활성화할 수 있습니다.

테넌트 관리자를 사용하여 버킷에 사용자 지정 StorageGRID 구성 XML을 적용하여 검색 통합을 구성할 수 있습니다.

> 검색 통합 서비스로 인해 개체 메타데이터가 대상으로 전송되기 때문에 해당 구성 XML을 _ 메타데이터 알림 구성 xml _ 이라고 합니다. 이 구성 XML은 이벤트 알림을 설정하는 데 사용되는 _notification 구성 xml_과 다릅니다.

를 참조하십시오 S3 클라이언트 애플리케이션 구현 지침 다음 사용자 지정 StorageGRID S3 REST API 작업에 대한 자세한 내용은 다음을 참조하십시오.

- 버킷 메타데이터 알림 구성 요청을 삭제합니다
- 버킷 메타데이터 알림 구성 요청을 가져옵니다
- PUT 버킷 메타데이터 알림 구성 요청

관련 정보

검색 통합을 위한 구성 XML

메타데이터 알림에 포함된 개체 메타데이터입니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

검색 통합 서비스를 구성합니다

S3을 사용합니다

검색 통합을 위한 구성 **XML**

검색 통합 서비스는 "<MetadataNotificationConfiguration>" 및 "</MetadataNotificationConfiguration>" 태그에 포함된 규칙 집합을 사용하여 구성됩니다. 각 규칙은 규칙이 적용되는 오브젝트와 StorageGRID가 해당 오브젝트의 메타데이터를 보내야 하는 대상을 지정합니다.

개체 이름의 접두어를 기준으로 개체를 필터링할 수 있습니다. 예를 들어, 접두어 '이미지'가 있는 객체에 대한 메타데이터를 한 대상으로, 접두어 '비디오'가 있는 객체에 대한 메타데이터를 다른 대상으로 전송할 수 있습니다. 중복되는 접두사가 있는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어 접두사 test를 가진 개체에 대해 하나의 규칙과 접두사 test2 를 가진 개체에 대한 두 번째 규칙을 포함하는 구성은 허용되지 않습니다.

검색 통합 서비스를 위해 생성된 StorageGRID 엔드포인트의 URN을 사용하여 대상을 지정해야 합니다. 이러한 엔드포인트는 Elasticsearch 클러스터에 정의된 인덱스 및 유형을 나타냅니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

이 표에서는 메타데이터 알림 구성 XML의 요소에 대해 설명합니다.

이름	설명	필수 요소입니다
MetadataNotificationConfiguration을 참조하십시오	메타데이터 알림의 개체 및 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 규칙 요소가 포함되어 있습니다.	예
규칙	메타데이터를 지정된 인덱스에 추가해야 하는 개체를 식별하는 규칙의 컨테이너 태그입니다. 접두사가 겹치는 규칙은 거부됩니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID입니다	규칙의 고유 식별자입니다. Rule 요소에 포함되어 있습니다.	아니요
상태	상태는 '활성화' 또는 '비활성화'가 될 수 있습니다. 비활성화된 규칙에 대해 어떠한 작업도 수행되지 않습니다. Rule 요소에 포함되어 있습니다.	예

이름	설명	필수 요소입니다
접두어	접두사와 일치하는 개체는 규칙의 영향을 받으며 해당 메타데이터는 지정된 대상으로 전송됩니다. 모든 오브젝트를 일치시키려면 빈 접두사를 지정합니다. Rule 요소에 포함되어 있습니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. Rule 요소에 포함되어 있습니다.	예
urn	객체 메타데이터가 전송되는 대상의 urn입니다. 다음 속성을 가진 StorageGRID 끝점의 URN이어야 합니다. • 세 번째 요소는 'es'여야 합니다. • URN은 메타데이터가 저장된 인덱스 및 형식으로 domain-name/myindex/MyType 형식으로 끝나야 합니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 취합니다. • "arn:aws:region:account-ID:domain/mydomain/myindex/MyType" • 'urn:mysite:es:::mydomain/myindex/MyType' 구성 XML을 제출하기 전에 끝점을 구성해야 합니다. 그렇지 않으면 404 오류로 인해 구성이 실패합니다. urn은 Destination 요소에 포함됩니다.	예

샘플 메타데이터 알림 구성 XML을 사용하여 고유한 XML을 구성하는 방법을 배웁니다.

모든 개체에 적용되는 메타데이터 알림 구성입니다

이 예제에서 모든 오브젝트의 오브젝트 메타데이터는 동일한 대상으로 전송됩니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

두 가지 규칙을 사용하여 메타데이터 알림 구성

이 예에서는 접두사 /images와 일치하는 객체의 객체 메타데이터가 한 대상으로 전송되고 접두사 /videos와 일치하는 객체의 객체 메타데이터는 두 번째 대상으로 전송됩니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

관련 정보

S3을 사용합니다

메타데이터 알림에 포함된 개체 메타데이터입니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

검색 통합 서비스를 구성합니다

검색 통합 서비스를 구성합니다

검색 통합 서비스는 개체가 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 개체 메타데이터를 보냅니다.

필요한 것

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 인덱싱할 콘텐츠가 있는 S3 버킷을 이미 생성해야 합니다.
- 검색 통합 서비스의 대상으로 사용하려는 끝점이 이미 있어야 하며 URN이 있어야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이 권한을 사용하여 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

소스 버킷에 대한 검색 통합 서비스를 구성한 후 객체를 만들거나 객체의 메타데이터 또는 태그를 업데이트하면 대상 엔드포인트로 객체 메타데이터가 전송됩니다. 이미 객체가 포함된 버킷에 대해 검색 통합 서비스를 활성화하면 기존 객체에 대한 메타데이터 알림이 자동으로 전송되지 않습니다. 이러한 기존 개체를 업데이트하여 대상 검색 인덱스에 해당 메타데이터가 추가되도록 해야 합니다.

단계

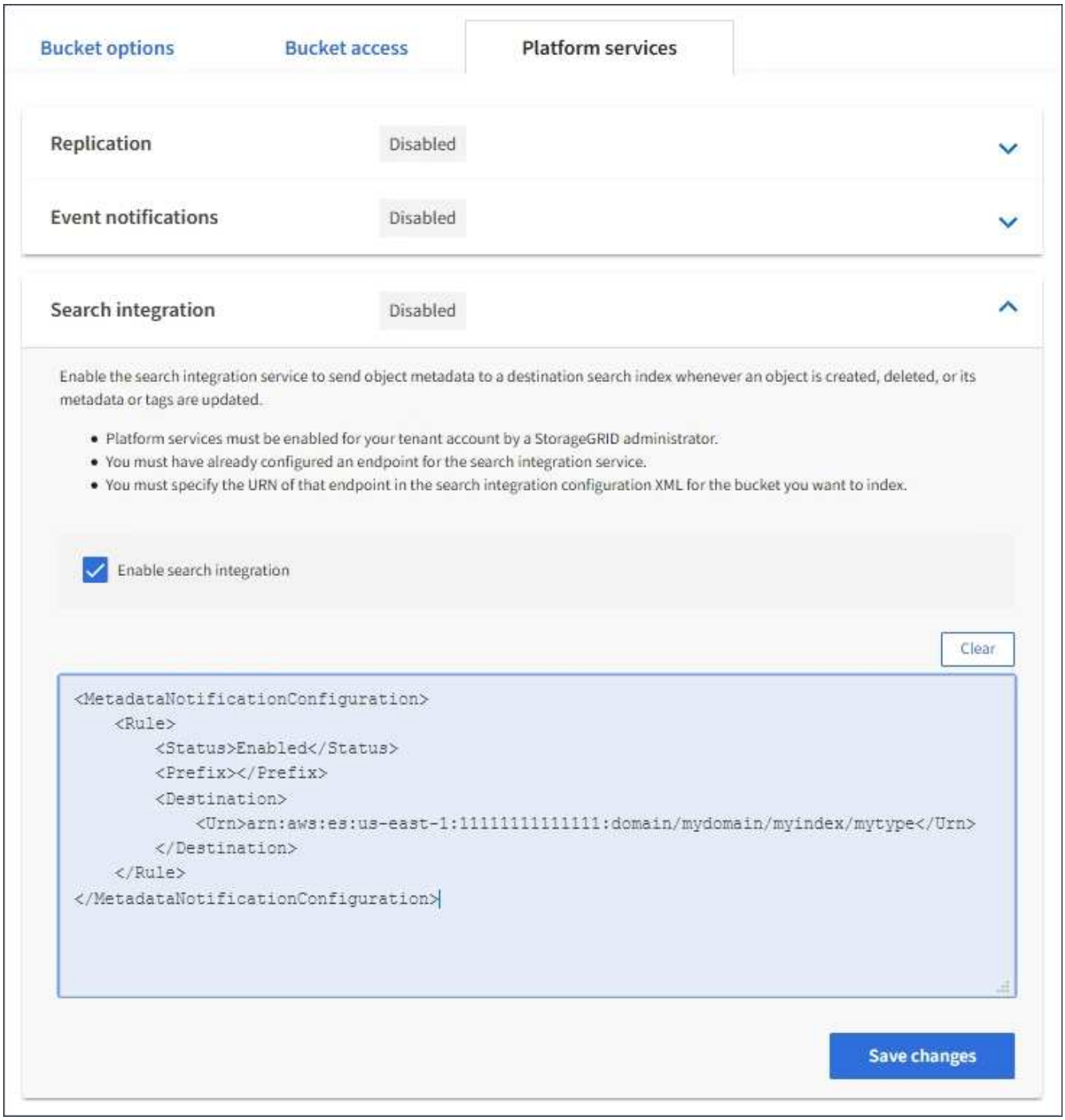
1. 텍스트 편집기를 사용하여 검색 통합을 활성화하는 데 필요한 메타데이터 알림 XML을 만듭니다.
   - 검색 통합을 위한 구성 XML에 대한 정보를 참조하십시오.
   - XML을 구성할 때는 검색 통합 끝점의 URN을 대상으로 사용합니다.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 통합 검색 * 을 선택합니다
5. 검색 통합 사용 * 확인란을 선택합니다.
6. 메타데이터 알림 구성을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



> 그리드 관리자 또는 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 검색 통합 서비스가 올바르게 구성되었는지 확인합니다.
   a. 구성 XML에 지정된 대로 메타데이터 알림을 트리거하기 위한 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞의 예제에서 버킷에 추가된 모든 오브젝트는 메타데이터 알림을 트리거합니다.

   b. 개체의 메타데이터와 태그가 포함된 JSON 문서가 끝점에 지정된 검색 인덱스에 추가되었는지 확인합니다.

작업을 마친 후

필요에 따라 다음 방법 중 하나를 사용하여 버킷에 대한 검색 통합을 비활성화할 수 있습니다.

- 스토리지(S3) * > * 버킷 * 을 선택하고 * 검색 통합 활성화 * 확인란의 선택을 취소합니다.
- S3 API를 직접 사용하는 경우 Delete Bucket 메타데이터 알림 요청을 사용합니다. S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

관련 정보

검색 통합 서비스를 이해합니다

검색 통합을 위한 구성 XML

S3을 사용합니다

플랫폼 서비스 끝점을 만듭니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

버킷에 대한 검색 통합 서비스를 활성화하면 개체 메타데이터 또는 태그를 추가, 업데이트 또는 삭제할 때마다 JSON 문서가 생성되어 대상 끝점으로 전송됩니다.

이 예에서는 'test'라는 버킷에 'gws/tagging.txt' 키가 있는 객체가 생성될 때 생성될 수 있는 JSON의 예를 보여 줍니다. 시험용 버킷은 버전 관리가 되지 않아 rionId 태그가 비어 있습니다.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

메타데이터 알림에 포함된 개체 메타데이터입니다

이 표에는 검색 통합이 활성화된 경우 대상 끝점으로 전송되는 JSON 문서에 포함된 모든 필드가 나열됩니다.

문서 이름에는 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)가 포함됩니다.

유형	항목 이름 및 설명입니다
버킷 및 오브젝트 정보	버켓 이름
키 : 개체 키 이름	거장된 버킷을 가진 개체의 개체 버전
'리기온': '우동-1'과 같은 버켓 지역	시스템 메타데이터
'크기': HTTP 클라이언트에 표시되는 개체 크기(바이트)입니다	'mD5': 객체 해시
사용자 메타데이터	metadata: 객체에 대한 모든 사용자 메타데이터를 키 값 쌍으로 사용합니다 키: 값
태그	"태그": 오브젝트에 대해 정의된 모든 오브젝트 태그는 키 값 쌍으로 제공됩니다 키: 값

태그 및 사용자 메타데이터의 경우 StorageGRID는 날짜 및 숫자를 Elasticsearch에 문자열 또는 S3 이벤트 알림으로 전달합니다. 이러한 문자열을 날짜 또는 숫자로 해석하도록 Elasticsearch를 구성하려면 동적 필드 매핑 및 날짜 형식 매핑에 대한 Elasticsearch 지침을 따르십시오. 검색 통합 서비스를 구성하기 전에 인덱스에서 동적 필드 매핑을 활성화해야 합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 형식을 편집할 수 없습니다.