테넌트 계정 사용

StorageGRID software

NetApp
July 23, 2026

목차

테넌트 계정 사용

StorageGRID 테넌트 계정 사용

테넌트 계정을 사용하면 Simple Storage Service(S3) REST API를 이용하여 StorageGRID 시스템에 객체를 저장하고 검색할 수 있습니다.

테넌트 계정이란 무엇인가요?

각 테넌트 계정은 자체적인 연합 또는 로컬 그룹, 사용자, S3 버킷 및 객체를 보유합니다.

테넌트 계정을 사용하면 저장된 객체를 서로 다른 엔티티별로 구분할 수 있습니다. 예를 들어, 다음과 같은 두 가지 사용 사례에 여러 테넌트 계정을 사용할 수 있습니다.

- 엔터프라이즈 사용 사례**:** StorageGRID 시스템을 기업 환경에서 사용하는 경우, 그리드의 객체 스토리지는 조직 내 여러 부서별로 분리될 수 있습니다. 예를 들어 마케팅 부서, 고객 지원 부서, 인사 부서 등을 위한 테넌트 계정이 있을 수 있습니다.

> S3 클라이언트 프로토콜을 사용하는 경우 S3 버킷 및 버킷 정책을 사용하여 기업 내 부서 간에 객체를 분리할 수 있습니다. 별도의 테넌트 계정을 생성할 필요가 없습니다. 자세한 내용은 "S3 버킷 및 버킷 정책" 구현 지침을 참조하십시오.

- 서비스 제공업체 사용 사례**:** StorageGRID 시스템을 서비스 제공업체가 사용하는 경우, 그리드의 객체 스토리지는 스토리지를 임대하는 여러 주체별로 분리될 수 있습니다. 예를 들어, Company A, Company B, Company C 등의 테넌트 계정이 있을 수 있습니다.

테넌트 계정을 만드는 방법

테넌트 계정은 "StorageGRID 그리드 관리자가 Grid Manager를 사용합니다."이(가) 생성합니다. 테넌트 계정을 생성할 때 그리드 관리자는 다음 사항을 지정합니다.

- 테넌트 이름, 클라이언트 유형(S3) 및 선택적 스토리지 할당량을 포함한 기본 정보.
- 테넌트 계정에 대한 권한에는 테넌트 계정이 S3 플랫폼 서비스를 사용할 수 있는지, 자체 ID 소스를 구성할 수 있는지, S3 Select를 사용할 수 있는지, 또는 그리드 페더레이션 연결을 사용할 수 있는지 여부가 포함됩니다.
- 테넌트의 초기 루트 액세스는 StorageGRID 시스템이 로컬 그룹 및 사용자, ID 페더레이션 또는 단일 로그인(SSO)을 사용하는지에 따라 결정됩니다.

또한, 그리드 관리자는 S3 테넌트 계정이 규제 요건을 준수해야 하는 경우 StorageGRID 시스템에 대해 S3 객체 잠금 설정을 활성화할 수 있습니다. S3 객체 잠금이 활성화되면 모든 S3 테넌트 계정은 규정을 준수하는 버킷을 생성하고 관리할 수 있습니다.

S3 테넌트 구성

"S3 테넌트 계정이 생성되었습니다." 후에 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 페더레이션을 설정합니다(ID 소스가 그리드와 공유되는 경우는 제외).
- 그룹 및 사용자 관리

- 계정 복제 및 그리드 간 복제를 위해 그리드 페더레이션을 사용합니다.
- S3 액세스 키 관리
- S3 버킷 생성 및 관리
- S3 플랫폼 서비스 사용
- S3 Select 사용
- 스토리지 사용량 모니터링

테넌트 관리자를 사용하여 S3 버킷을 생성하고 관리할 수 있지만, 객체를 수집하고 관리하려면 "S3 클라이언트" 또는 "S3 콘솔"를 사용해야 합니다.

로그인 및 로그아웃 방법

StorageGRID 테넌트 관리자에 로그인

테넌트 관리자에 접속하려면 "지원되는 웹 브라우저"의 주소창에 해당 테넌트의 URL을 입력하십시오.

시작하기 전에

- 로그인 정보를 가지고 계십니다.
- 그리드 관리자가 제공한 Tenant Manager 액세스 URL이 있습니다. 해당 URL은 다음 예시 중 하나와 유사합니다.

  ```
  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
  ```

  URL에는 항상 정규화된 도메인 이름(FQDN), 관리 노드의 IP 주소 또는 관리 노드 HA 그룹의 가상 IP 주소가 포함됩니다. 또한 포트 번호, 20자리 테넌트 계정 ID 또는 둘 다 포함될 수 있습니다.

- URL에 테넌트의 20자리 계정 ID가 포함되어 있지 않으면 해당 계정 ID를 가지고 있습니다.
- 귀하는 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 웹 브라우저에서 쿠키가 활성화되어 있습니다.
- 귀하는 "특정 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. "지원되는 웹 브라우저"을(를) 시작합니다.
2. 브라우저 주소 표시줄에 테넌트 관리자에 액세스하기 위한 URL을 입력합니다.
3. 보안 경고 메시지가 표시되면 브라우저의 설치 마법사를 사용하여 인증서를 설치하십시오.
4. 테넌트 관리자에 로그인합니다.

표시되는 로그인 화면은 입력한 URL과 StorageGRID에 대해 SSO(Single Sign-On)가 구성되었는지 여부에 따라 다릅니다.

SSO를 사용하지 않음

StorageGRID가 SSO를 사용하지 않는 경우 다음 화면 중 하나가 나타납니다.

- 그리드 관리자 로그인 페이지입니다. 테넌트 로그인 링크를 선택합니다.
- 테넌트 관리자 로그인 페이지입니다. 계정 필드가 이미 입력되어 있을 수 있습니다.
  i. 테넌트의 20자리 계정 ID가 표시되지 않으면 최근 계정 목록에 테넌트 계정 이름이 있으면 해당 이름을 선택하거나 계정 ID를 입력하십시오.
  ii. 사용자 이름과 비밀번호를 입력하십시오.
  iii. *로그인*을 선택합니다.

  테넌트 관리자 대시보드가 나타납니다.

  iv. 다른 사람으로부터 초기 비밀번호를 받은 경우, 계정 보안을 위해 ***username*** > *Change password*를 선택하십시오.

SSO 사용

StorageGRID가 SSO를 사용하는 경우 다음 화면 중 하나가 나타납니다.

- 귀사 조직의 SSO 페이지.

  표준 SSO 자격 증명을 입력하고 *로그인*을 선택합니다.

- 테넌트 관리자 SSO 로그인 페이지입니다.
  i. 테넌트의 20자리 계정 ID가 표시되지 않으면 최근 계정 목록에 테넌트 계정 이름이 있으면 해당 이름을 선택하거나 계정 ID를 입력하십시오.
  ii. *로그인*을 선택합니다.
  iii. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인하십시오.

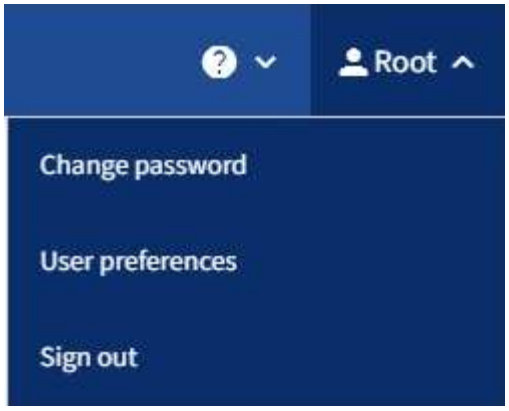
  테넌트 관리자 대시보드가 나타납니다.

StorageGRID 테넌트 관리자에서 로그아웃합니다**.**

테넌트 관리자 사용을 마친 후에는 무단 사용자가 StorageGRID 시스템에 접근하지 못하도록 반드시 로그아웃해야 합니다. 브라우저의 쿠키 설정에 따라 브라우저를 닫는 것만으로는 시스템에서 로그아웃되지 않을 수 있습니다.

단계

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



2. 사용자 이름을 선택한 다음 *로그아웃*을 선택하세요.

   ◦ SSO를 사용하지 않는 경우:

   관리자 노드에서 로그아웃되었습니다. 테넌트 관리자 로그인 페이지가 표시됩니다.

   둘 이상의 관리자 노드에 로그인한 경우, 각 노드에서 로그아웃해야 합니다.

   ◦ SSO가 활성화된 경우:

   현재 접속 중인 모든 관리자 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. 방금 접속한 테넌트 계정 이름이 최근 계정 드롭다운 메뉴에 기본값으로 표시되고, 테넌트의 *계정 ID*가 나타납니다.

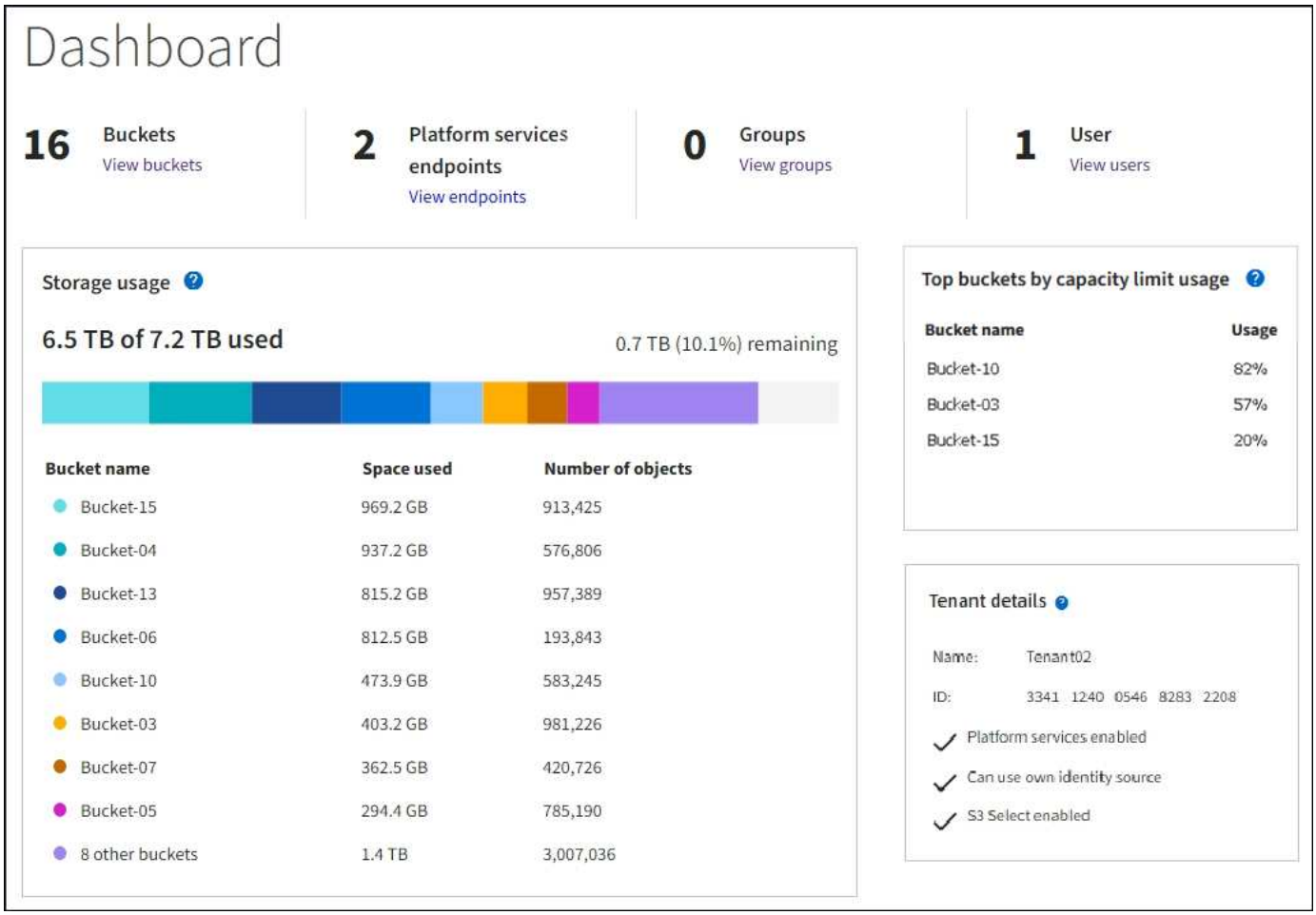
SSO가 활성화되어 있고 Grid Manager에도 로그인되어 있는 경우, SSO에서 로그아웃하려면 Grid Manager에서도 로그아웃해야 합니다.

StorageGRID의 테넌트 관리자 대시보드

테넌트 관리자 대시보드는 테넌트 계정의 구성과 테넌트의 S3 버킷에서 객체가 사용하는 공간 용량에 대한 개요를 제공합니다. 테넌트에 할당량이 있는 경우 대시보드에 할당량 사용량과 남은 용량이 표시됩니다. 테넌트 계정과 관련된 오류가 있는 경우 해당 오류가 대시보드에 표시됩니다.

이 테넌트에 속하는 모든 객체의 논리적 크기에는 미완료 및 진행 중인 멀티파트 업로드가 포함됩니다. 이 크기에는 ILM 정책에 사용되는 추가 물리적 공간은 포함되지 않습니다. 사용된 공간 값은 추정치입니다. 이러한 추정치는 데이터 수집 시간, 네트워크 연결 상태 및 노드 상태의 영향을 받습니다.

객체 업로드가 완료되면 대시보드는 다음 예시와 같이 표시됩니다.



테넌트 계정 정보

대시보드 상단에는 구성된 버킷 또는 컨테이너, 그룹 및 사용자 수가 표시됩니다. 또한 구성된 플랫폼 서비스 엔드포인트가 있는 경우 해당 엔드포인트 수도 표시됩니다. 링크를 선택하여 세부 정보를 확인하십시오.

보유한 "테넌트 관리 권한" 및 구성한 옵션에 따라 대시보드의 나머지 부분에는 다양한 지침, 스토리지 사용량, 객체 정보 및 테넌트 세부 정보의 조합이 표시됩니다.

저장 공간 및 할당량 사용량

저장 공간 사용량 패널에는 다음 정보가 포함되어 있습니다.

- 테넌트의 오브젝트 데이터 양입니다.

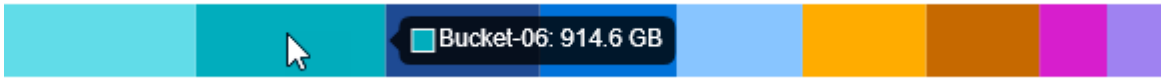
  이 값은 업로드된 객체 데이터의 총량을 나타내며, 해당 객체의 복사본과 메타데이터를 저장하는 데 사용된 공간을 나타내지 않습니다.

- 할당량이 설정된 경우, 객체 데이터에 사용할 수 있는 총 공간과 남은 공간의 양 및 비율이 표시됩니다. 할당량은 수집할 수 있는 객체 데이터의 양을 제한합니다.

할당량 사용량은 내부 추정치를 기반으로 하며 경우에 따라 초과될 수 있습니다. 예를 들어, StorageGRID는 테넌트가 객체 업로드를 시작할 때 할당량을 확인하고, 테넌트가 할당량을 초과한 경우 새로운 수집을 거부합니다. 그러나 StorageGRID는 할당량 초과 여부를 판단할 때 현재 업로드 중인 데이터의 크기를 고려하지 않습니다. 객체가 삭제되면 할당량 사용량이 재계산될 때까지 테넌트가 새 객체를 업로드하지 못할 수 있습니다. 할당량 사용량 계산에는 10분 이상 소요될 수 있습니다.

- 가장 큰 버킷 또는 컨테이너의 상대적인 크기를 나타내는 막대 그래프.

  차트의 각 부분 위에 커서를 올려놓으면 해당 버킷 또는 컨테이너에서 사용된 총 공간을 확인할 수 있습니다.



- 막대 그래프와 함께 가장 큰 버킷 또는 컨테이너 목록을 제공하며, 각 버킷 또는 컨테이너의 총 오브젝트 데이터 양과 오브젝트 수를 포함합니다.

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 버킷 또는 컨테이너가 있는 경우, 나머지 모든 버킷 또는 컨테이너는 목록 맨 아래에 하나의 항목으로 통합됩니다.

테넌트 관리자에 표시되는 저장 용량 값의 단위를 변경하려면 테넌트 관리자 오른쪽 상단에 있는 사용자 드롭다운 메뉴를 선택한 다음 *User preferences*를 선택하십시오.

할당량 사용량 알림

Grid Manager에서 할당량 사용량 알림을 활성화한 경우, 할당량이 부족하거나 초과되면 다음과 같이 Tenant Manager에 알림이 표시됩니다.

- 테넌트 할당량의 90% 이상이 사용된 경우, 테넌트 할당량 사용량 높음 알림이 트리거됩니다.

  그리드 관리자에게 할당량을 늘려달라고 요청하는 것을 고려하십시오.

- 할당량을 초과하면 새 개체를 업로드할 수 없다는 알림이 표시됩니다.

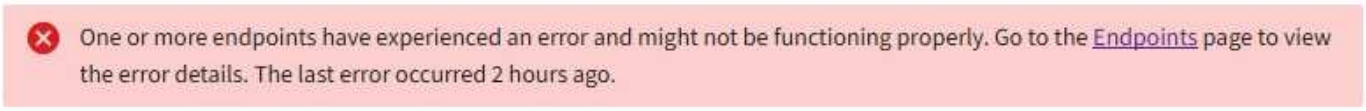
용량 제한 사용량

버킷에 용량 제한을 설정한 경우, 테넌트 관리자 대시보드에 용량 제한 사용량 기준으로 상위 버킷 목록이 표시됩니다.

버킷에 용량 제한이 설정되어 있지 않으면 용량은 무제한입니다. 하지만 테넌트 계정에 총 스토리지 할당량이 있고 해당 할당량에 도달하면 버킷의 남은 용량 제한과 관계없이 더 이상 객체를 수집할 수 없습니다.

엔드포인트 오류

그리드 관리자를 사용하여 플랫폼 서비스와 함께 사용할 하나 이상의 엔드포인트를 구성한 경우, 지난 7일 동안 엔드포인트 오류가 발생하면 테넌트 관리자 대시보드에 알림이 표시됩니다.



"플랫폼 서비스 엔드포인트 오류"에 대한 자세한 내용을 보려면 *Endpoints*를 선택하여 Endpoints 페이지를 표시하십시오.

테넌트 관리 API

StorageGRID 테넌트 관리 API에 대해 알아보십시오

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

테넌트 관리 API:

- Swagger 오픈 소스 API 플랫폼을 사용합니다. Swagger는 개발자와 비개발자 모두 API와 상호 작용할 수 있는 직관적인 사용자 인터페이스를 제공합니다. Swagger 사용자 인터페이스는 각 API 작업에 대한 자세한 정보와 문서를 제공합니다.
- "중단 없는 업그레이드를 지원하는 버전 관리"을(를) 사용합니다.

테넌트 관리 API에 대한 Swagger 문서에 액세스하려면 다음을 수행합니다.

1. 테넌트 관리자에 로그인합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택한 다음 *API 문서*를 선택합니다.

API 작업

테넌트 관리 API는 사용 가능한 API 작업을 다음과 같은 섹션으로 구성합니다.

- 계정: 현재 테넌트 계정에 대한 작업(저장 공간 사용량 정보 가져오기 포함).
- **auth**: 사용자 세션 인증을 수행하는 작업입니다.

  테넌트 관리 API는 베어러 토큰 인증 방식을 지원합니다. 테넌트 로그인을 위해 인증 요청의 JSON 본문에 사용자 이름, 비밀번호 및 accountId를 제공해야 합니다(즉, `POST /api/v3/authorize`). 사용자가 인증에 성공하면 보안 토큰이 반환됩니다. 이 토큰은 이후 API 요청의 헤더에 포함해야 합니다("Authorization: Bearer token").

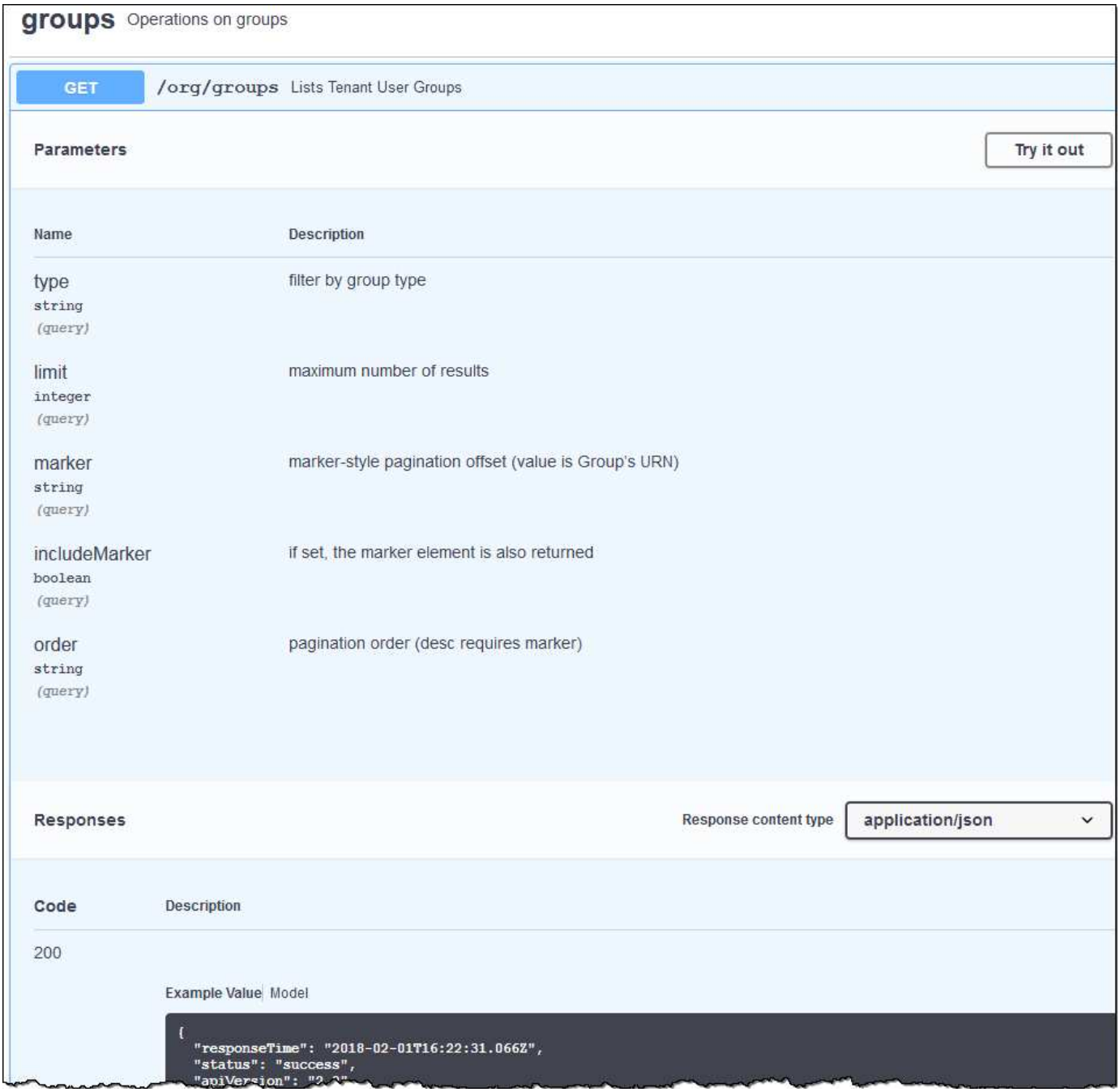
  인증 보안 개선에 대한 자세한 내용은 "사이트 간 요청 위조(CSRF) 공격으로부터 보호"을 참조하십시오.

  > StorageGRID 시스템에 단일 로그인(SSO)이 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. "그리드 관리 API 사용 지침"을 참조하십시오.

- **config**: 테넌트 관리 API의 제품 릴리스 및 버전과 관련된 작업입니다. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- 컨테이너: S3 버킷에 대한 작업.
- **deactivated-features**: 비활성화되었을 수 있는 기능을 확인하기 위한 작업입니다.
- 엔드포인트: 엔드포인트를 관리하는 작업입니다. 엔드포인트를 통해 S3 버킷은 StorageGRID CloudMirror 복제, 알림 또는 검색 통합을 위해 외부 서비스를 사용할 수 있습니다.
- **grid-federation-connections**: 그리드 페더레이션 연결 및 그리드 간 복제에 대한 작업입니다.
- **groups**: 로컬 테넌트 그룹을 관리하고 외부 ID 소스에서 페더레이션된 테넌트 그룹을 검색하는 작업입니다.
- **identity-source**: 외부 ID 소스를 구성하고 페더레이션된 그룹 및 사용자 정보를 수동으로 동기화하는 작업입니다.
- **ilm**: 정보 라이프사이클 관리(ILM) 설정에 대한 작업.
- **regions**: StorageGRID 시스템에 대해 구성된 지역을 확인하는 작업입니다.
- **s3**: 테넌트 사용자를 위한 S3 액세스 키 관리 작업입니다.
- **s3-object-lock**: 규정 준수를 지원하기 위해 사용되는 전역 S3 Object Lock 설정에 대한 작업입니다.
- 사용자: 테넌트 사용자를 보고 관리하는 작업입니다.

작업 세부 정보

각 API 작업을 펼쳐보면 HTTP 작업, 엔드포인트 URL, 필수 또는 선택적 매개변수 목록, 요청 본문 예시(필요한 경우) 및 가능한 응답을 확인할 수 있습니다.



API 요청 발행

> API 문서 웹페이지를 사용하여 수행하는 모든 API 작업은 실시간 작업입니다. 실수로 구성 데이터 또는 기타 데이터를 생성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. 요청 세부 정보를 보려면 HTTP 작업을 선택하십시오.
2. 요청에 그룹 또는 사용자 ID와 같은 추가 매개변수가 필요한지 확인합니다. 그런 다음 이러한 값을 가져옵니다. 필요한 정보를 얻기 위해 다른 API 요청을 먼저 수행해야 할 수도 있습니다.
3. 예제 요청 본문을 수정해야 하는지 판단하세요. 수정해야 하는 경우, *모델*을 선택하여 각 필드에 대한 요구 사항을 확인할 수 있습니다.

4. *직접 사용해보기*를 선택합니다.
5. 필요한 매개변수를 제공하거나 필요에 따라 요청 본문을 수정하십시오.
6. *실행*을 선택합니다.
7. 요청이 성공했는지 여부를 확인하려면 응답 코드를 검토하십시오.

StorageGRID Tenant Management API 버전 관리

테넌트 관리 API는 버전 관리를 사용하여 서비스 중단 없는 업그레이드를 지원합니다.

예를 들어, 이 요청 URL은 API 버전 4를 지정합니다.

`https://hostname_or_ip_address/api/v4/authorize`

API의 주 버전은 이전 버전과 호환되지 않는 변경 사항이 있을 때 업데이트됩니다. 반대로 API의 부 버전은 이전 버전과 호환되는 변경 사항이 있을 때 업데이트됩니다. 호환되는 변경 사항에는 새로운 엔드포인트 또는 새로운 속성 추가가 포함됩니다.

다음 예시는 변경 유형에 따라 API 버전이 어떻게 증가하는지 보여줍니다.

API 변경 유형	이전 버전	새 버전
이전 버전과 호환됩니다	2.1	2.2
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치할 때는 최신 버전의 API만 활성화됩니다. 하지만 StorageGRID의 새 기능 릴리스로 업그레이드할 때는 적어도 하나의 StorageGRID 기능 릴리스 동안 이전 버전의 API를 계속 사용할 수 있습니다.

> 지원되는 버전을 구성할 수 있습니다. "그리드 관리 API"에 대한 Swagger API 문서의 **config** 섹션을 참조하십시오. 모든 API 클라이언트를 최신 버전으로 업데이트한 후에는 이전 버전에 대한 지원을 비활성화해야 합니다.

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

- 응답 헤더는 "Deprecated: true"입니다.
- JSON 응답 본문에 "deprecated": true가 포함되어 있습니다.
- nms.log 파일에 더 이상 사용되지 않음을 알리는 경고 메시지가 추가됩니다. 예를 들면 다음과 같습니다.

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

현재 릴리스에서 지원되는 **API** 버전 확인

지원되는 API 주요 버전 목록을 반환하려면 `GET /versions` API 요청을 사용하십시오. 이 요청은 Swagger API 문서의 **config** 섹션에 있습니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

요청에 사용할 **API** 버전 지정

API 버전은 경로 매개변수 (`/api/v4`) 또는 헤더 (`Api-Version: 4`)를 사용하여 지정할 수 있습니다. 두 값을 모두 제공하는 경우 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

StorageGRID에서 교차 사이트 요청 위조 방지

쿠키를 사용하는 인증 방식을 강화하기 위해 CSRF 토큰을 사용하면 StorageGRID에 대한 교차 사이트 요청 위조(CSRF) 공격을 방지하는 데 도움이 됩니다. Grid Manager와 Tenant Manager는 이 보안 기능을 자동으로 활성화하며, 다른 API 클라이언트는 로그인 시 활성화 여부를 선택할 수 있습니다.

공격자는 HTTP 폼 POST와 같은 방식으로 다른 사이트에 요청을 보내 로그인한 사용자의 쿠키를 이용해 특정 요청을 발생시킬 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 이 기능이 활성화되면 특정 쿠키의 내용이 특정 헤더 또는 특정 POST 본문 매개변수의 내용과 일치해야 합니다.

이 기능을 활성화하려면 인증 중에 `csrfToken` 매개변수를 `true`으로 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"
```

이 값이 true이면 `GridCsrfToken` 쿠키는 Grid Manager 로그인 시 임의의 값으로 설정되고, `AccountCsrfToken` 쿠키는 Tenant Manager 로그인 시 임의의 값으로 설정됩니다.

쿠키가 존재하는 경우, 시스템 상태를 변경할 수 있는 모든 요청(POST, PUT, PATCH, DELETE)에는 다음 중 하나가 반드시 포함되어야 합니다.

- The `X-Csrf-Token` 헤더이며, 헤더의 값은 CSRF 토큰 쿠키의 값으로 설정됩니다.
- 폼 인코딩된 본문을 허용하는 엔드포인트의 경우: A `csrfToken` 폼 인코딩된 요청 본문 매개변수입니다.

CSRF 보호를 구성하려면 "그리드 관리 API" 또는 "테넌트 관리 API"을(를) 사용하십시오.

> CSRF 토큰 쿠키가 설정된 요청은 CSRF 공격에 대한 추가적인 보호 조치로 JSON 요청 본문을 예상하는 모든 요청에 대해 "Content-Type: application/json" 헤더를 강제 적용합니다.

그리드 페더레이션 연결 사용

StorageGRID에서 테넌트 그룹 및 사용자 복제

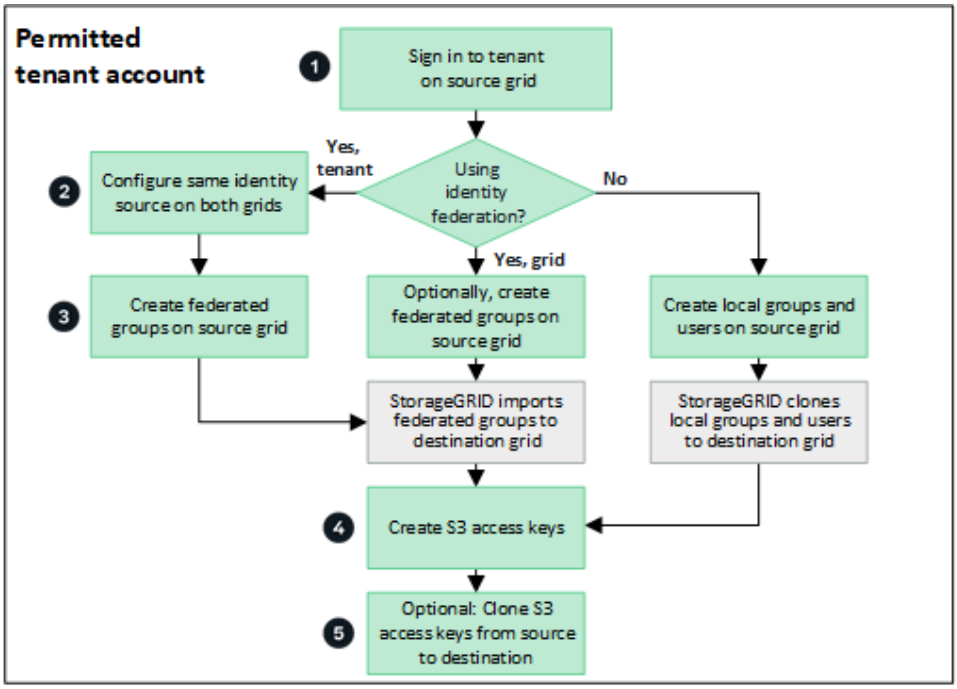
테넌트가 그리드 페더레이션 연결을 사용하도록 생성되거나 편집된 경우, 해당 테넌트는 하나의 StorageGRID 시스템(원본 테넌트)에서 다른 StorageGRID 시스템(복제본 테넌트)으로 복제됩니다. 테넌트가 복제된 후 원본 테넌트에 추가된 모든 그룹 및 사용자는 복제본 테넌트에 복제됩니다.

테넌트가 처음 생성된 StorageGRID 시스템을 테넌트의 _소스 그리드_라고 합니다. 테넌트가 복제되는 StorageGRID 시스템을 테넌트의 _대상 그리드_라고 합니다. 두 테넌트 계정은 동일한 계정 ID, 이름, 설명, 스토리지 할당량 및 할당된 권한을 가지지만, 대상 테넌트에는 초기에 루트 사용자 암호가 없습니다. 자세한 내용은 "계정 복제란 무엇인가요?" 및 "허용된 테넌트 관리"을 참조하십시오.

버킷 객체의 "교차 그리드 복제"을 위해 테넌트 계정 정보 복제가 필요합니다. 두 그리드 모두에 동일한 테넌트 그룹과 사용자가 있어야 각 그리드에서 해당 버킷과 객체에 액세스할 수 있습니다.

계정 복제를 위한 테넌트 워크플로

테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 워크플로 다이어그램을 검토하여 그룹, 사용자 및 S3 액세스 키를 복제하는 단계를 확인하십시오.



워크플로의 주요 단계는 다음과 같습니다.

1 테넌트에 로그인

소스 그리드(테넌트가 처음 생성된 그리드)의 테넌트 계정에 로그인합니다.

2 선택적으로 **ID** 페더레이션을 구성합니다**.**

테넌트 계정에 페더레이션 그룹 및 사용자를 사용하기 위한 자체 **ID** 소스 사용 권한이 있는 경우, 소스 및 대상 테넌트 계정 모두에 동일한 ID 소스(동일한 설정 포함)를 구성하십시오. 두 그리드가 동일한 ID 소스를 사용하지 않으면 페더레이션 그룹 및 사용자를 복제할 수 없습니다. 자세한 내용은 "ID 페더레이션 사용"을 참조하십시오.

3 그룹 및 사용자 생성

그룹 및 사용자를 생성할 때는 테넌트의 소스 그리드에서 시작하십시오. 새 그룹을 추가하면 StorageGRID가 해당 그룹을 대상 그리드에 자동으로 복제합니다.

- 전체 StorageGRID 시스템 또는 테넌트 계정에 대해 ID 페더레이션이 구성된 경우 "새로운 테넌트 그룹 생성" ID 소스에서 페더레이션된 그룹을 가져옵니다.
- ID 페더레이션을 사용하지 않는 경우, "새 로컬 그룹 만들기" 그런 다음 "로컬 사용자 생성".

4 **S3** 액세스 키 생성

소스 그리드 또는 대상 그리드에서 "액세스 키 생성" 하거나 "다른 사용자의 액세스 키 생성" 하여 해당 그리드의 버킷에 액세스할 수 있습니다.

5 선택적으로 **S3** 액세스 키 복제

두 그리드에서 동일한 액세스 키로 버킷에 액세스해야 하는 경우 소스 그리드에서 액세스 키를 생성한 다음 테넌트 관리자 API를 사용하여 대상 그리드로 수동으로 복제하세요. 자세한 내용은 "API를 사용하여 S3 액세스 키 복제"을 참조하세요.

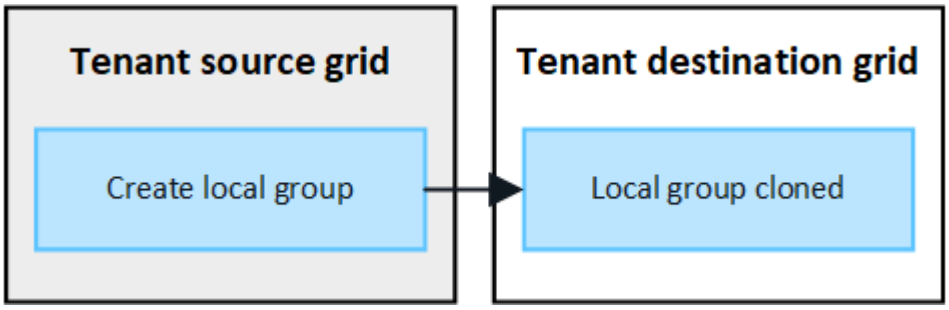
그룹, 사용자 및 S3 액세스 키는 어떻게 복제됩니까?

이 섹션을 검토하여 그룹, 사용자 및 S3 액세스 키가 테넌트 소스 그리드와 테넌트 대상 그리드 간에 어떻게 복제되는지 이해하십시오.

원본 그리드에 생성된 로컬 그룹은 복제됩니다.

테넌트 계정이 생성되고 대상 그리드로 복제되면 StorageGRID는 테넌트의 소스 그리드에 추가한 모든 로컬 그룹을 테넌트의 대상 그리드로 자동으로 복제합니다.

원본 그룹과 복제본 모두 동일한 액세스 모드, 그룹 권한 및 S3 그룹 정책을 가집니다. 자세한 내용은 "S3 테넌트에 대한 그룹 생성"을 참조하십시오.

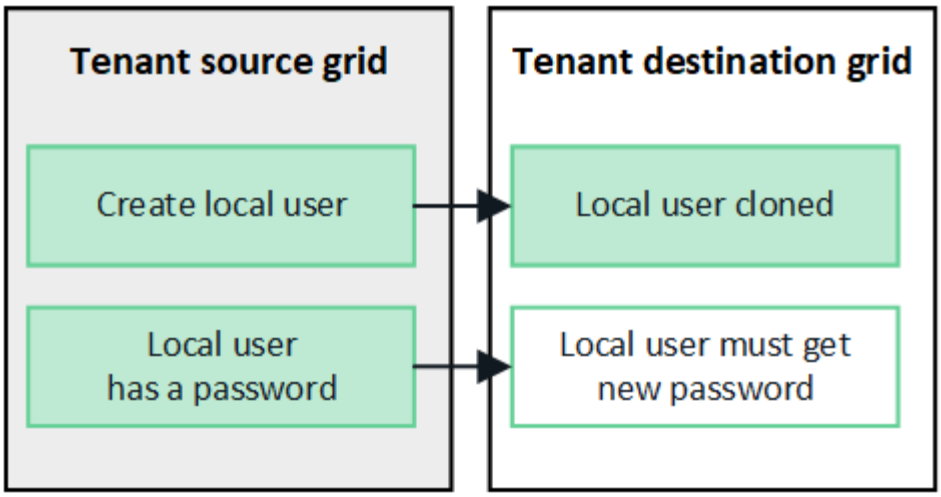


원본 그리드에서 로컬 그룹을 만들 때 선택한 사용자는 해당 그룹이 대상 그리드로 복제될 때 포함되지 않습니다. 따라서 그룹을 만들 때 사용자를 선택하지 마십시오. 대신 사용자를 만들 때 그룹을 선택하십시오.

원본 그리드에 생성된 로컬 사용자가 복제됩니다.

원본 그리드에서 새 로컬 사용자를 생성하면 StorageGRID가 해당 사용자를 대상 그리드로 자동으로 복제합니다. 원본 사용자와 복제된 사용자는 동일한 전체 이름, 사용자 이름 및 액세스 거부 설정을 갖습니다. 또한 두 사용자는 동일한 그룹에 속합니다. 자세한 내용은 "사용자 관리"을 참조하십시오.

보안상의 이유로 로컬 사용자 암호는 대상 그리드로 복제되지 않습니다. 로컬 사용자가 대상 그리드의 테넌트 관리자에 액세스해야 하는 경우, 해당 테넌트 계정의 루트 사용자가 대상 그리드에 해당 사용자의 암호를 추가해야 합니다. 자세한 내용은 "사용자 관리"을 참조하십시오.

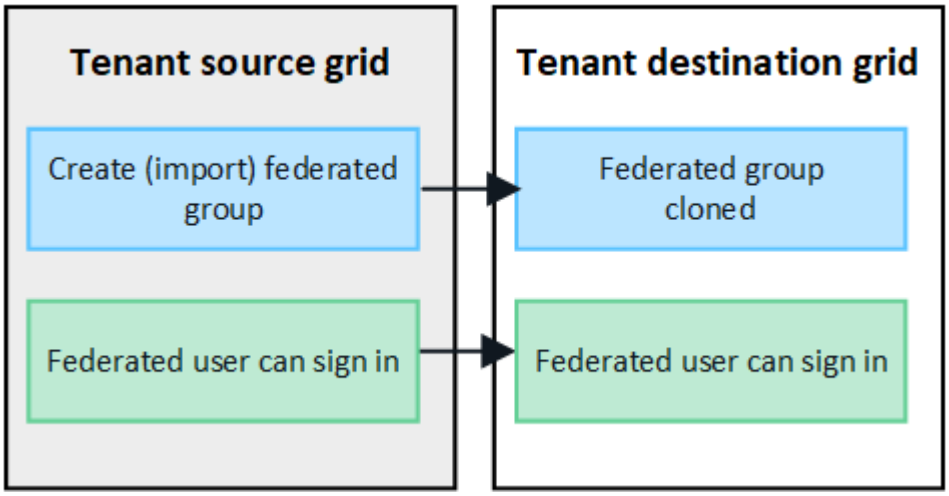


소스 그리드에서 생성된 페더레이션 그룹은 복제됩니다.

계정 복제 기능을 사용하기 위한 요구 사항이 "싱글 사인온" 및 "ID 페더레이션"에 대해 충족되었다고 가정하면, 소스 그리드의 테넌트에 대해 생성(가져오기)한 페더레이션 그룹은 대상 그리드의 테넌트로 자동으로 복제됩니다.

두 그룹 모두 동일한 액세스 모드, 그룹 권한 및 S3 그룹 정책을 가집니다.

원본 테넌트에 대해 페더레이션 그룹이 생성되고 대상 테넌트에 복제된 후, 페더레이션 사용자는 두 그리드 중 하나에서 테넌트에 로그인할 수 있습니다.

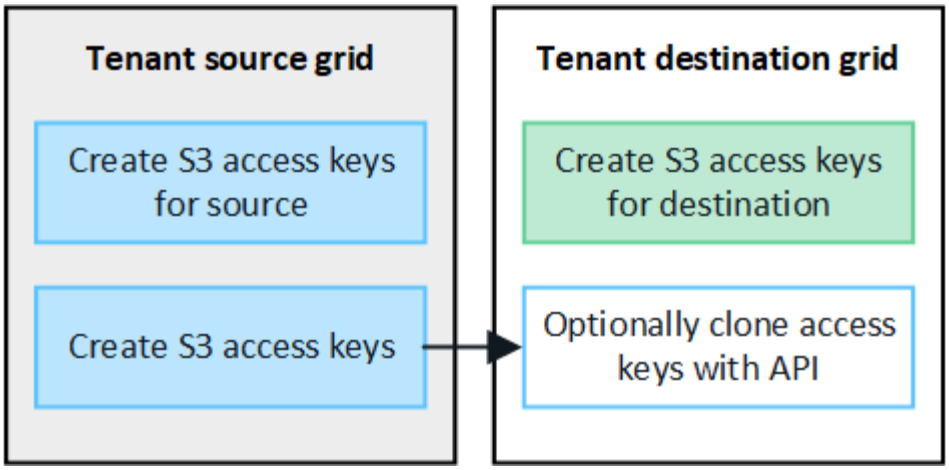


S3 액세스 키는 수동으로 복제할 수 있습니다.

StorageGRID는 각 그리드마다 서로 다른 키를 사용하면 보안이 강화되므로 S3 액세스 키를 자동으로 복제하지 않습니다.

두 그리드의 액세스 키를 관리하려면 다음 방법 중 하나를 사용할 수 있습니다.

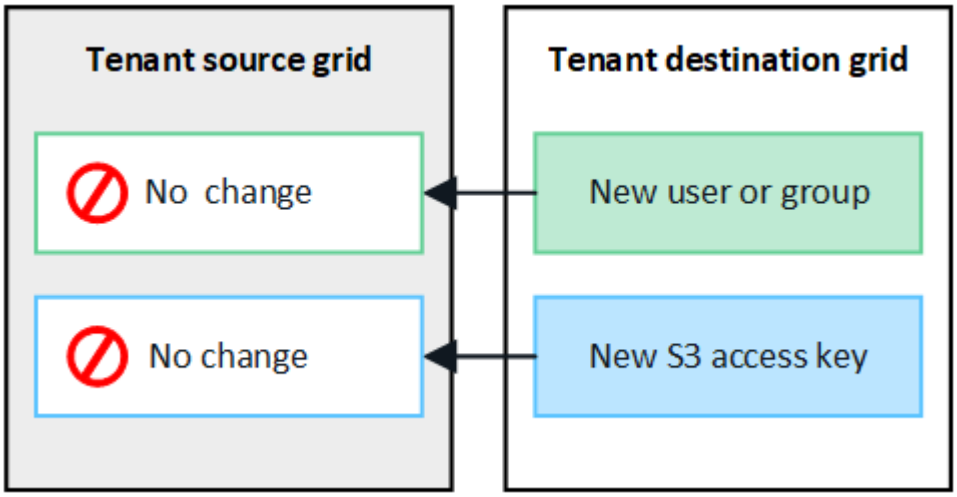
- 각 그리드에 동일한 키를 사용할 필요가 없다면 "액세스 키 생성" 또는 "다른 사용자의 액세스 키 생성" 각 그리드에서 설정할 수 있습니다.
- 두 그리드에서 동일한 키를 사용해야 하는 경우 소스 그리드에서 키를 생성한 다음 테넌트 관리자 API를 사용하여 수동으로 "키를 복제합니다" 대상 그리드에 키를 추가할 수 있습니다.



페더레이션 사용자의 S3 액세스 키를 복제하면 사용자와 S3 액세스 키 모두 대상 테넌트에 복제됩니다.

대상 그리드에 추가된 그룹과 사용자는 복제되지 않습니다.

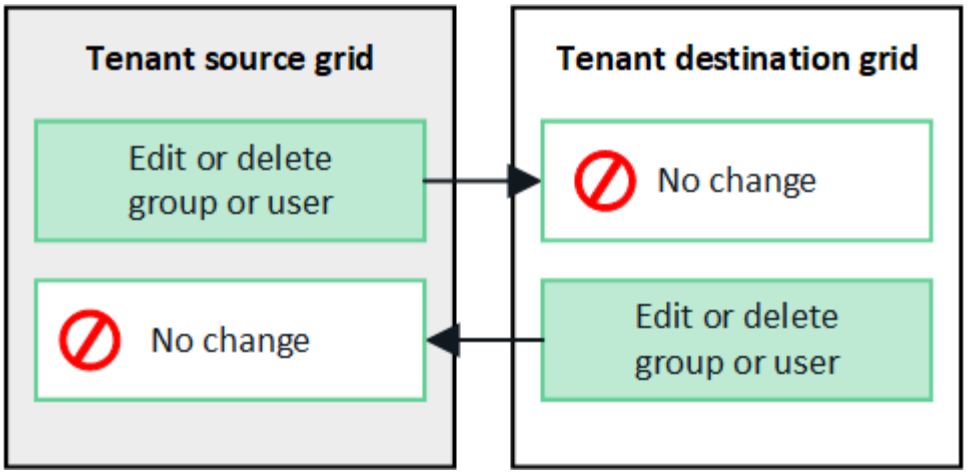
복제는 테넌트의 소스 그리드에서 테넌트의 대상 그리드로만 수행됩니다. 테넌트의 대상 그리드에서 그룹 및 사용자를 생성하거나 가져오는 경우 StorageGRID는 이러한 항목을 테넌트의 소스 그리드로 다시 복제하지 않습니다.



수정 또는 삭제된 그룹, 사용자 및 액세스 키는 복제되지 않습니다

복제는 새 그룹 및 사용자를 생성할 때만 발생합니다.

어느 한쪽 그리드에서 그룹, 사용자 또는 액세스 키를 편집하거나 삭제하면 해당 변경 사항이 다른 그리드에 복제되지 않습니다.



테넌트 관리 **API**를 사용하여 **StorageGRID** 그리드 간 **S3** 액세스 키 복제

StorageGRID 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제할 수 있습니다.

시작하기 전에

- 테넌트 계정에는 그리드 페더레이션 연결 사용 권한이 있습니다.
- 그리드 연합 연결의 *연결 상태*가 *연결됨*입니다.
- 테넌트의 소스 그리드에서 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인되어 있습니다.
- 귀하는 "S3 자격 증명 또는 루트 액세스 권한을 직접 관리합니다."이(가) 있는 사용자 그룹에 속해 있습니다.
- 로컬 사용자의 액세스 키를 복제하는 경우 해당 사용자는 이미 두 그리드 모두에 존재합니다.

> ⓘ 페더레이션 사용자의 S3 액세스 키를 복제하면 사용자와 S3 액세스 키가 모두 대상 테넌트에 추가됩니다.

자신의 액세스 키 복제

두 그리드에서 동일한 버킷에 액세스해야 하는 경우 자체 액세스 키를 복제할 수 있습니다.

단계

1. 소스 그리드의 테넌트 관리자를 사용하여 "액세스 키 생성" 및 `.csv` 파일을 다운로드합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택한 다음 *API 문서*를 선택합니다.
3. **s3** 섹션에서 다음 엔드포인트를 선택하십시오.

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. *직접 사용해보기*를 선택합니다.
5. 본문 텍스트 상자에서 **accessKey** 및 **secretAccessKey***의 예시 항목을 다운로드한 ***.csv** 파일의 값으로

바꾸세요.

각 문자열을 둘러싼 큰따옴표를 반드시 유지하십시오.

6. 키가 만료될 예정이라면, 예시 항목인 **expires***를 **ISO 8601** 날짜-시간 형식의 문자열로 된 만료 날짜 및 시간으로 바꾸십시오(예: `2024-02-28T22:46:33-08:00`). 키가 만료되지 않을 예정이라면, ***expires** 항목의 값으로 **null***을 입력하거나 ***Expires** 줄과 그 앞의 쉼표를 삭제하십시오.
7. *실행*을 선택합니다.
8. 서버 응답 코드가 *204*인지 확인하십시오. *204*는 키가 대상 그리드에 성공적으로 복제되었음을 나타냅니다.

다른 사용자의 액세스 키 복제

두 그리드 모두에서 동일한 버킷에 액세스해야 하는 경우 다른 사용자의 액세스 키를 복제할 수 있습니다.

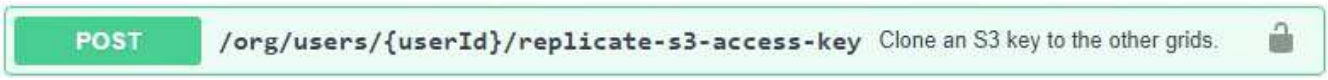
단계

1. 소스 그리드의 테넌트 관리자를 사용하여 "다른 사용자의 S3 액세스 키 생성" 및 `.csv` 파일을 다운로드합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택한 다음 *API 문서*를 선택합니다.
3. 사용자 ID를 확인하세요. 다른 사용자의 액세스 키를 복제하려면 이 값이 필요합니다.
   a. 사용자 섹션에서 다음 엔드포인트를 선택하십시오.

      ```
      GET /org/users
      ```

   b. *직접 사용해보기*를 선택합니다.
   c. 사용자 조회 시 사용할 매개변수를 지정하십시오.
   d. *실행*을 선택합니다.
   e. 키를 복제하려는 사용자를 찾고 **id** 필드의 번호를 복사합니다.
4. **s3** 섹션에서 다음 엔드포인트를 선택하십시오.

   ```
   POST /org/users/{userId}/replicate-s3-access-key
   ```

5. *직접 사용해보기*를 선택합니다.
6. * userId* 텍스트 상자에 복사한 사용자 ID를 붙여넣으세요.
7. 본문 텍스트 상자에서 예시 액세스 키 및 비밀 액세스 키*의 예시 항목을 해당 사용자의 ***.csv** 파일에 있는 값으로

바꾸십시오.

문자열을 둘러싼 큰따옴표를 반드시 유지하십시오.

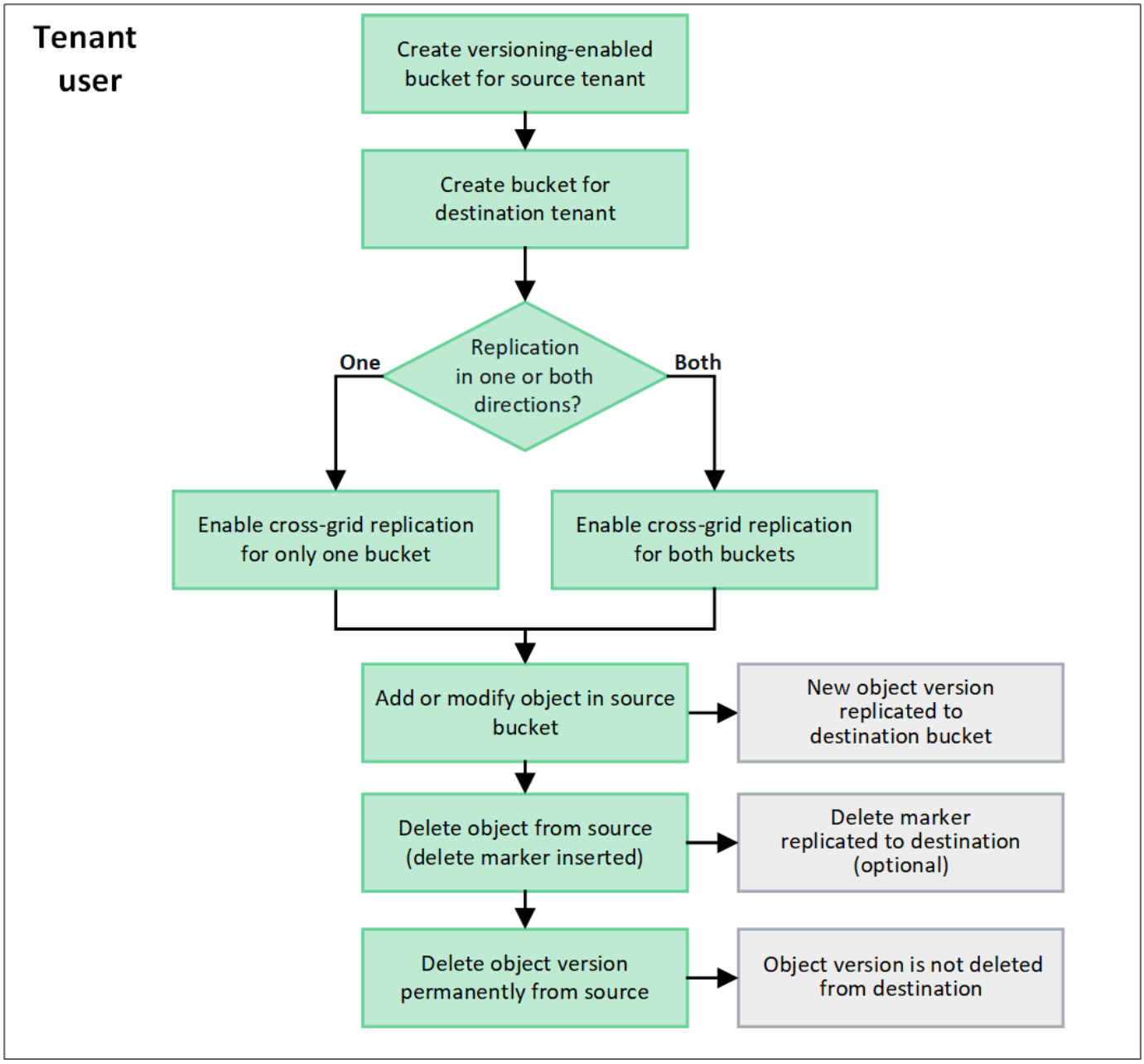
8. 키가 만료될 예정이라면, 예시 항목인 **expires***를 **ISO 8601** 날짜**-**시간 형식의 문자열로 된 만료 날짜 및 시간으로 바꾸십시오**(**예**: `2023-02-28T22:46:33-08:00`).** 키가 만료되지 않을 예정이라면**, *expires** 항목의 값으로 **null***을 입력하거나 ***Expires** 줄과 그 앞의 쉼표를 삭제하십시오.
9. *실행*을 선택합니다.
10. 서버 응답 코드가 *204*인지 확인하십시오. *204*는 키가 대상 그리드에 성공적으로 복제되었음을 나타냅니다.

StorageGRID에서 교차 그리드 복제 관리

테넌트 계정 생성 시 그리드 페더레이션 연결 사용 권한이 부여된 경우, 크로스 그리드 복제를 사용하여 테넌트의 소스 그리드 버킷과 테넌트의 대상 그리드 버킷 간에 객체를 자동으로 복제할 수 있습니다. 크로스 그리드 복제는 단방향 또는 양방향으로 수행될 수 있습니다.

그리드 간 복제 워크플로

워크플로 다이어그램은 두 그리드의 버킷 간 교차 그리드 복제를 구성하기 위해 수행하는 단계를 요약합니다. 이러한 단계는 다이어그램 아래에서 더 자세히 설명합니다.



그리드 간 복제 구성

교차 그리드 복제를 사용하려면 먼저 각 그리드에서 해당 테넌트 계정으로 로그인하고 버킷 두 개를 생성해야 합니다. 그런 다음 하나 또는 두 버킷 모두에서 교차 그리드 복제를 활성화할 수 있습니다.

시작하기 전에

- 그리드 간 복제에 필요한 사항을 검토하셨습니다. "크로스 그리드 복제란 무엇인가요?"을 참조하십시오.
- 현재 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 테넌트 계정에는 그리드 페더레이션 연결 사용 권한이 있으며, 동일한 테넌트 계정이 두 그리드에 모두 존재합니다. 자세한 내용은 "그리드 페더레이션 연결에 허용된 테넌트 관리"을 참조하십시오.
- 로그인하려는 테넌트 사용자는 이미 두 그리드 모두에 존재하며, "루트 액세스 권한"을(를) 가진 사용자 그룹에 속해 있습니다.
- 테넌트의 대상 그리드에 로컬 사용자로 로그인하는 경우, 테넌트 계정의 루트 사용자가 해당 그리드에서 사용자

계정에 대한 암호를 설정해 놓았습니다.

버킷 두 개 만들기

첫 번째 단계로 각 그리드에서 해당 테넌트 계정에 로그인하고 각 그리드에 버킷을 생성합니다.

단계

1. 그리드 연합 연결의 어느 그리드에서든 시작하여 새 버킷을 생성합니다.
   a. 두 그리드 모두에 존재하는 테넌트 사용자의 자격 증명을 사용하여 테넌트 계정에 로그인하십시오.

      로컬 사용자로 테넌트의 대상 그리드에 로그인할 수 없는 경우, 테넌트 계정의 루트 사용자가 사용자 계정에 암호를 설정했는지 확인하십시오.

   b. "S3 버킷을 생성합니다"의 지침을 따르세요.

      각 그리드마다 버킷 이름과 지역이 다를 수 있습니다.

   c. 객체 설정 관리 탭에서 *객체 버전 관리 활성화*를 선택합니다.
   d. StorageGRID 시스템에서 S3 Object Lock이 활성화된 경우 "S3 객체 잠금을 사용한 크로스 그리드 복제"을 참조하십시오.
   e. *버킷 생성*을 선택합니다.
   f. *완료*를 선택합니다.
2. 그리드 페더레이션 연결의 다른 그리드에서 동일한 테넌트 계정에 대한 버킷을 생성하려면 이 단계를 반복하십시오.

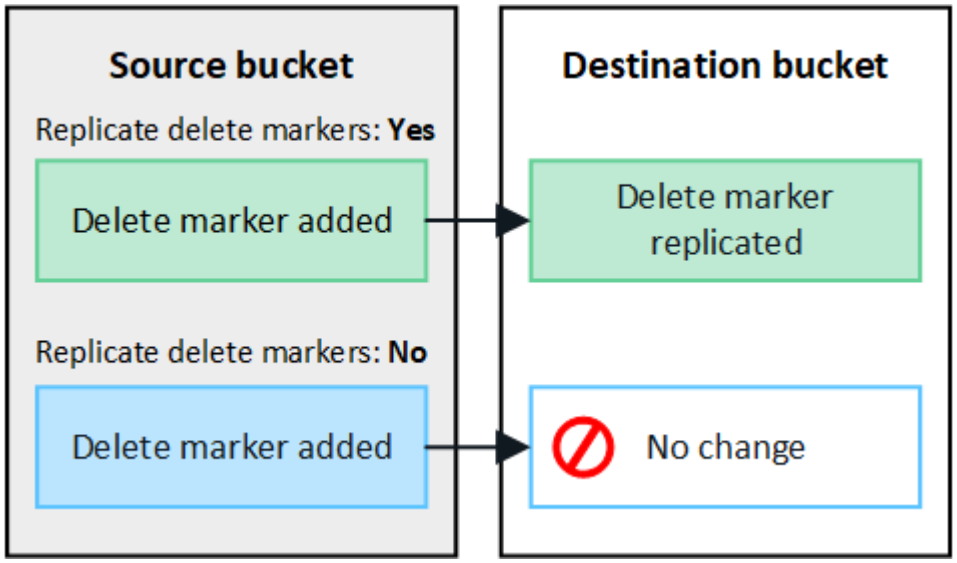
   필요에 따라 각 버킷은 서로 다른 지역을 사용할 수 있습니다.

그리드 간 복제 활성화

버킷에 객체를 추가하기 전에 반드시 다음 단계를 수행해야 합니다.

단계

1. 복제하려는 객체가 있는 그리드에서 시작하여 "한 방향으로의 교차 그리드 복제"을(를) 활성화합니다.
   a. 버킷의 테넌트 계정에 로그인합니다.
   b. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
   c. 표에서 버킷 이름을 선택하여 버킷 세부 정보 페이지에 액세스하십시오.
   d. 교차 그리드 복제 탭을 선택합니다.
   e. *활성화*를 선택하고 요구 사항 목록을 검토하십시오.
   f. 모든 요구 사항이 충족되면 사용할 그리드 페더레이션 연결을 선택하십시오.
   g. 선택적으로, 삭제 마커 복제 설정을 변경하여 S3 클라이언트가 버전 ID가 포함되지 않은 삭제 요청을 소스 그리드에 보낼 경우 대상 그리드에서 발생하는 상황을 결정할 수 있습니다.
      - 예(기본값): 삭제 마커가 소스 버킷에 추가되고 대상 버킷으로 복제됩니다.
      - 아니요: 삭제 표시가 소스 버킷에 추가되지만 대상 버킷으로 복제되지 않습니다.



삭제 요청에 버전 ID가 포함된 경우 해당 객체 버전은 소스 버킷에서 영구적으로 제거됩니다. StorageGRID는 버전 ID가 포함된 삭제 요청을 복제하지 않으므로 대상 버킷에서는 동일한 객체 버전이 삭제되지 않습니다.

자세한 내용은 "크로스 그리드 복제란 무엇인가요?"을 참조하십시오.

a. 선택적으로, 감사 메시지 볼륨을 관리하기 위해 **Cross-grid replication** 감사 범주 설정을 변경할 수 있습니다.
   - **Error** (기본값): 감사 출력에는 실패한 그리드 간 복제 요청만 포함됩니다.
   - **Normal**: 모든 그리드 간 복제 요청이 포함되므로 감사 출력량이 크게 증가합니다.

b. 선택 사항을 검토하세요. 두 버킷이 모두 비어 있어야만 이 설정을 변경할 수 있습니다.

c. *활성화 및 테스트*를 선택합니다.

   잠시 후 성공 메시지가 나타납니다. 이제 이 버킷에 추가된 객체가 다른 그리드로 자동으로 복제됩니다. 버킷 세부 정보 페이지에서 *그리드 간 복제*가 활성화된 기능으로 표시됩니다.

2. 선택적으로 다른 그리드의 해당 버킷으로 이동하여 "양방향으로 그리드 간 복제를 활성화합니다.".

그리드 간 복제 테스트

버킷에 대해 그리드 간 복제가 활성화된 경우 연결 및 그리드 간 복제가 올바르게 작동하는지, 그리고 소스 및 대상 버킷이 모든 요구 사항(예: 버전 관리가 여전히 활성화됨)을 충족하는지 확인해야 할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. 버킷의 테넌트 계정에 로그인합니다.
2. 대시보드에서 버킷 보기*를 선택하거나 *스토리지(S3) > *버킷*을 선택합니다.
3. 표에서 버킷 이름을 선택하여 버킷 세부 정보 페이지에 액세스하십시오.

4. 교차 그리드 복제 탭을 선택합니다.
5. *연결 테스트*를 선택합니다.

   연결이 정상적이면 성공 배너가 표시됩니다. 그렇지 않으면 오류 메시지가 표시되며, 이 메시지를 사용하여 사용자와 그리드 관리자가 문제를 해결할 수 있습니다. 자세한 내용은 "그리드 페더레이션 오류 해결"을 참조하십시오.

6. 그리드 간 복제가 양방향으로 구성된 경우, 다른 그리드의 해당 버킷으로 이동하여 *연결 테스트*를 선택하여 그리드 간 복제가 반대 방향으로 제대로 작동하는지 확인하십시오.

그리드 간 복제 비활성화

다른 그리드로 개체를 복사하지 않으려면 그리드 간 복제를 영구적으로 중지할 수 있습니다.

그리드 간 복제를 비활성화하기 전에 다음 사항에 유의하십시오.

- 그리드 간 복제를 비활성화해도 이미 그리드 간에 복사된 객체는 삭제되지 않습니다. 예를 들어, `my-bucket`그리드 1에 있는 객체가 `my-bucket`그리드 2로 복사된 경우, 해당 버킷에 대해 그리드 간 복제를 비활성화해도 객체는 삭제되지 않습니다. 이러한 객체를 삭제하려면 수동으로 삭제해야 합니다.
- 각 버킷에 대해 그리드 간 복제가 활성화된 경우(즉, 양방향 복제가 발생하는 경우), 하나 또는 두 버킷 모두에 대해 그리드 간 복제를 비활성화할 수 있습니다. 예를 들어, `my-bucket`그리드 1에서 `my-bucket`그리드 2로의 객체 복제는 비활성화하고 `my-bucket`그리드 2에서 `my-bucket`그리드 1로의 객체 복제는 계속 유지하도록 설정할 수 있습니다.
- 테넌트 그리드 페더레이션 연결을 사용할 수 있는 테넌트의 권한을 제거하기 전에 먼저 그리드 간 복제를 비활성화해야 합니다. 을(를) 참조하십시오. "허용된 테넌트 관리"
- 객체가 포함된 버킷에 대해 크로스 그리드 복제를 비활성화하면 소스 버킷과 대상 버킷에서 모든 객체를 삭제하지 않는 한 크로스 그리드 복제를 다시 활성화할 수 없습니다.

  버킷 두 개가 모두 비어 있어야 복제를 다시 활성화할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. 더 이상 복제하지 않으려는 객체가 있는 그리드부터 시작하여 해당 버킷에 대한 그리드 간 복제를 중지합니다.
   a. 버킷의 테넌트 계정에 로그인합니다.
   b. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
   c. 표에서 버킷 이름을 선택하여 버킷 세부 정보 페이지에 액세스하십시오.
   d. 교차 그리드 복제 탭을 선택합니다.
   e. *복제 사용 안 함*을 선택합니다.
   f. 이 버킷에 대한 크로스 그리드 복제를 비활성화하려면 텍스트 상자에 *Yes*를 입력하고 *Disable*을 선택하십시오.

      잠시 후 성공 메시지가 나타납니다. 이 버킷에 새로 추가된 객체는 더 이상 다른 그리드로 자동 복제되지

않습니다. 버킷 페이지에서 **Cross-grid replication** 기능이 더 이상 활성화된 기능으로 표시되지 않습니다.

2. 그리드 간 복제가 양방향으로 구성되었다면, 다른 그리드의 해당 버킷으로 이동하여 반대 방향의 그리드 간 복제를 중지하십시오.

StorageGRID에서 그리드 페더레이션 연결 보기

테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 허용된 연결을 확인할 수 있습니다.

시작하기 전에

- 테넌트 계정에는 그리드 페더레이션 연결 사용 권한이 있습니다.
- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. 스토리지**(S3)** > *그리드 페더레이션 연결*을 선택합니다.

   그리드 페더레이션 연결 페이지가 나타나고 다음 정보를 요약한 표가 포함됩니다.

열	설명
연결 이름	이 테넌트가 사용할 수 있는 그리드 페더레이션 연결입니다.
크로스 그리드 복제를 지원하는 버킷	각 그리드 페더레이션 연결에 대해, 그리드 간 복제가 활성화된 테넌트 버킷입니다. 이러한 버킷에 추가된 객체는 연결된 다른 그리드로 복제됩니다.
마지막 오류	각 그리드 연합 연결에 대해, 다른 그리드로 데이터가 복제되는 동안 발생한 가장 최근의 오류(있는 경우)를 표시합니다. 마지막 오류 지우기을 참조하십시오.

2. 선택적으로 버킷 이름을 "버킷 세부 정보 보기".

마지막 오류 지우기

마지막 오류 열에 오류가 나타날 수 있는 이유는 다음과 같습니다.

- 소스 객체 버전을 찾을 수 없습니다.
- 소스 버킷을 찾을 수 없습니다.
- 대상 버킷이 삭제되었습니다.
- 대상 버킷이 다른 계정에서 다시 생성되었습니다.
- 대상 버킷의 버전 관리가 일시 중단되었습니다.
- 대상 버킷은 동일한 계정으로 다시 생성되었지만 이제 버전 관리가 되지 않습니다.

이 열에는 가장 최근에 발생한 그리드 간 복제 오류만 표시됩니다. 이전에 발생했을 수 있는 오류는 표시되지 않습니다.

단계

1. 마지막 오류 열에 메시지가 표시되면 메시지 내용을 확인하십시오.

   예를 들어, 이 오류는 버전 관리가 일시 중단되었거나 S3 Object Lock이 활성화되었기 때문에 그리드 간 복제 대상 버킷이 유효하지 않은 상태였음을 나타냅니다.

2. 권장되는 조치를 수행하십시오. 예를 들어, 크로스 그리드 복제를 위해 대상 버킷에서 버전 관리가 일시 중단된 경우 해당 버킷에 대해 버전 관리를 다시 활성화하십시오.
3. 표에서 연결을 선택합니다.
4. *오류 지우기*를 선택합니다.
5. 메시지를 지우고 시스템 상태를 업데이트하려면 *예*를 선택하십시오.
6. 5~6분 정도 기다린 후 새 객체를 버킷에 수집합니다. 오류 메시지가 다시 나타나지 않는지 확인하십시오.

   오류 메시지가 완전히 사라지도록 하려면 메시지에 표시된 타임스탬프 이후 최소 5분이 지난 후에 새 객체를 수집하십시오.

7. 버킷 오류로 인해 복제에 실패한 객체가 있는지 확인하려면 "실패한 복제 작업 식별 및 재시도"을 참조하십시오.

그룹 및 사용자 관리

StorageGRID에서 ID 페더레이션 사용

ID 페더레이션을 사용하면 테넌트 그룹 및 사용자 설정이 더 빨라지고, 테넌트 사용자는 익숙한 자격 증명을 사용하여 테넌트 계정에 로그인할 수 있습니다.

테넌트 관리자에 대한 ID 페더레이션 구성

테넌트 그룹 및 사용자를 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하려면 테넌트 관리자에 대한 ID 페더레이션을 구성할 수 있습니다.

시작하기 전에

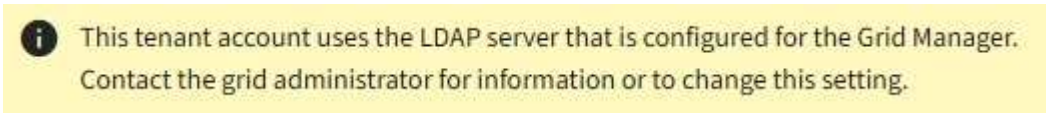
- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.
- 현재 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

  목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

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

이 작업 정보

테넌트에 대한 ID 페더레이션 서비스 구성 가능 여부는 테넌트 계정 설정 방식에 따라 다릅니다. 테넌트는 Grid Manager에 구성된 ID 페더레이션 서비스를 공유할 수도 있습니다. ID 페더레이션 페이지에 액세스할 때 이 메시지가 표시되면 해당 테넌트에 대해 별도의 페더레이션 ID 소스를 구성할 수 없습니다.

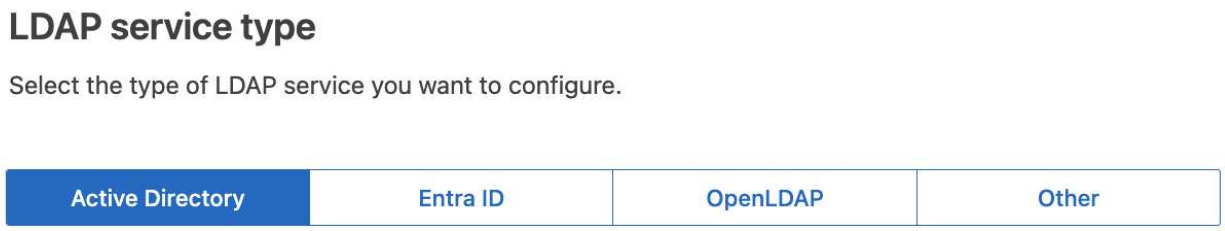


구성 입력

ID 페더레이션을 구성할 때 StorageGRID가 LDAP 서비스에 연결하는 데 필요한 값을 제공합니다.

단계

1. 액세스 관리 > *ID 페더레이션*을 선택합니다.
2. *ID 페더레이션 활성화*를 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성하려는 LDAP 서비스 유형을 선택합니다.



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

4. *기타*를 선택한 경우 LDAP 속성 섹션의 필드를 작성하십시오. 그렇지 않으면 다음 단계로 진행하십시오.
   - 사용자 고유 이름: LDAP 사용자의 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `sAMAccountName`, OpenLDAP의 경우 `uid`와 동일합니다. Oracle Directory Server를 구성하는 경우 `uid`를 입력합니다.
   - 사용자 **UUID**: LDAP 사용자의 영구 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `objectGUID`와, OpenLDAP의 경우 `entryUUID`와 동일합니다. Oracle Directory Server를 구성하는

경우 `nsuniqueid`를 입력하십시오. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.

- 그룹 고유 이름: LDAP 그룹의 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `sAMAccountName`, OpenLDAP의 경우 `cn`와 동일합니다. Oracle Directory Server를 구성하는 경우 `cn`를 입력합니다.
- 그룹 **UUID**: LDAP 그룹의 영구 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `objectGUID`, OpenLDAP의 경우 `entryUUID`와 동일합니다. Oracle Directory Server를 구성하는 경우 `nsuniqueid`를 입력합니다. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.

5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에서 필요한 LDAP 서버 및 네트워크 연결 정보를 입력하십시오.
   - 호스트 이름: LDAP 서버의 정규화된 도메인 이름(FQDN) 또는 IP 주소.
   - 포트: LDAP 서버에 연결하는 데 사용되는 포트입니다.

     STARTTLS의 기본 포트는 389이고, LDAPS의 기본 포트는 636입니다. 하지만 방화벽이 올바르게 구성되어 있다면 어떤 포트든 사용할 수 있습니다.

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

     Active Directory의 경우 하위 레벨 로그온 이름 또는 사용자 주체 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자 목록을 볼 수 있는 권한과 다음 속성에 접근할 수 있는 권한이 있어야 합니다.

     - `sAMAccountName` 또는 `uid`
     - `objectGUID`, `entryUUID` 또는 `nsuniqueid`
     - `cn`
     - `memberOf` 또는 `isMemberOf`
     - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, 및 `userPrincipalName`
     - **Entra ID**: `accountEnabled` 및 `userPrincipalName`

   - **Password**: 사용자 이름과 연결된 비밀번호입니다.

     향후 비밀번호를 변경하는 경우, 반드시 이 페이지에서 업데이트해야 합니다.

   - 그룹 기본 **DN**: 그룹을 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다. 아래 Active Directory 예시에서 고유 이름이 기본 DN(DC=storagegrid,DC=example,DC=com)을 기준으로 하는 모든 그룹은 페더레이션 그룹으로 사용할 수 있습니다.

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

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

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

◦ 바인드 사용자 이름 형식 (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 사용할 기본 사용자 이름 패턴입니다.

*바인딩 사용자 이름 형식*을 제공하는 것이 좋습니다. 이렇게 하면 StorageGRID 서비스 계정과 바인딩할 수 없는 경우에도 사용자가 로그인할 수 있습니다.

다음 패턴 중 하나를 입력하세요:

- **UserPrincipalName** 패턴**(AD** 및 **Entra ID)**: `[USERNAME]@example.com`
- 하위 레벨 로그온 이름 패턴**(AD** 및 **Entra ID)**: `example\[USERNAME]`
- 고유 이름 패턴: `CN=[USERNAME],CN=Users,DC=example,DC=com`

*[USERNAME]*을 정확히 입력하세요.

6. 전송 계층 보안(TLS) 섹션에서 보안 설정을 선택합니다.
   - **STARTTLS** 사용: STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. Active Directory, OpenLDAP 또는 기타 시스템에는 이 옵션을 권장하지만, Microsoft Entra ID에서는 이 옵션이 지원되지 않습니다.
   - **LDAPS** 사용: LDAPS(SSL을 통한 LDAP) 옵션은 TLS를 사용하여 LDAP 서버에 연결을 설정합니다. Microsoft Entra ID를 사용하려면 이 옵션을 선택해야 합니다.
   - **TLS**를 사용하지 마십시오: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Microsoft Entra ID에서 지원되지 않습니다.

> Active Directory 서버에서 LDAP 서명을 강제하는 경우 **TLS**를 사용하지 않음 옵션은 지원되지 않습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결을 보호하는 데 사용되는 인증서를 선택하십시오.
   - 운영체제 **CA** 인증서 사용: 연결을 보호하기 위해 운영체제에 설치된 기본 Grid CA 인증서를 사용합니다.
   - 사용자 지정 **CA** 인증서 사용: 사용자 지정 보안 인증서를 사용합니다.

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

연결을 테스트하고 구성을 저장합니다

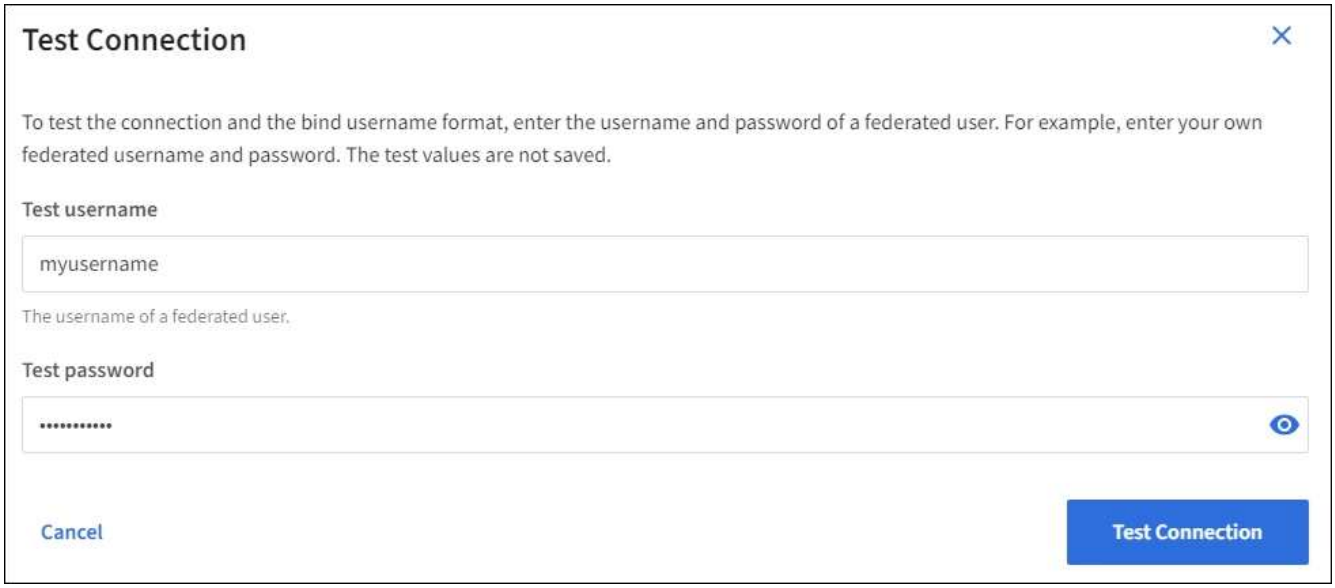
모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버의 연결 설정과 바인드 사용자 이름 형식(제공한 경우)을 확인합니다.

단계

1. *연결 테스트*를 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "연결 테스트 성공" 메시지가 나타납니다. *저장*을 선택하여 구성을 저장합니다.
   - 연결 설정이 올바르지 않으면 "테스트 연결을 설정할 수 없습니다"라는 메시지가 나타납니다. *닫기*를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트하십시오.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 페더레이션 사용자의 사용자 이름과 암호를 입력하십시오.

   예를 들어, 본인의 사용자 이름과 비밀번호를 입력하십시오. 사용자 이름에 @ 또는 /와 같은 특수 문자를 포함하지

마십시오.



- 연결 설정이 유효하면 "연결 테스트 성공" 메시지가 나타납니다. *저장*을 선택하여 구성을 저장합니다.
- 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름 및 암호가 유효하지 않으면 오류 메시지가 나타납니다. 문제를 해결한 후 연결을 다시 테스트하십시오.

ID 소스와의 강제 동기화

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹 및 사용자를 주기적으로 동기화합니다. 사용자 권한을 최대한 빨리 활성화하거나 제한하려면 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 연동 페이지로 이동합니다.
2. 페이지 상단에서 *동기화 서버*를 선택합니다.

   동기화 과정은 사용 환경에 따라 다소 시간이 걸릴 수 있습니다.

   ID 페더레이션 동기화 실패 경고는 ID 소스에서 페더레이션된 그룹 및 사용자를 동기화하는 데 문제가 발생할 경우 발생합니다.

ID 연동 비활성화

그룹 및 사용자에 대한 ID 페더레이션을 일시적 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션이 비활성화되면 StorageGRID 와 ID 소스 간의 통신이 중단됩니다. 하지만 구성한 설정은 모두 유지되므로 나중에 ID 페더레이션을 쉽게 다시 활성화할 수 있습니다.

이 작업 정보

ID 페더레이션을 비활성화하기 전에 다음 사항을 숙지해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인 중인 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 계속 액세스할 수 있지만, 세션이 만료된 후에는 로그인할 수 없습니다.

- StorageGRID 시스템과 ID 소스 간의 동기화는 발생하지 않으며, 동기화되지 않은 계정에 대한 알림도 표시되지 않습니다.
- 싱글 사인온(SSO) 상태가 '사용' 또는 '샌드박스 모드'인 경우 'ID 페더레이션 사용' 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 싱글 사인온 페이지의 SSO 상태가 '사용 안 함'이어야 합니다. "싱글 사인온 비활성화"을 참조하십시오.

단계

1. ID 연동 페이지로 이동합니다.
2. **ID** 페더레이션 활성화 확인란의 선택을 해제합니다.

OpenLDAP 서버 구성 지침

ID 페더레이션을 위해 OpenLDAP 서버를 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

> Active Directory 또는 Microsoft Entra ID가 아닌 ID 소스의 경우, StorageGRID는 외부에서 사용이 중지된 사용자의 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 해당 사용자의 S3 키를 삭제하거나 모든 그룹에서 해당 사용자를 제거하십시오.

Memberof 및 **refint** 오버레이

memberof 및 refint 오버레이를 활성화해야 합니다. 자세한 내용은 "OpenLDAP 문서: 버전 2.4 관리자 가이드"의 역방향 그룹 멤버십 유지 관리 지침을 참조하십시오.

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

또한, 최적의 성능을 위해 사용자 이름에 대한 도움말에 언급된 필드가 색인화되었는지 확인하십시오.

역방향 그룹 멤버십 유지 관리에 대한 정보는 "OpenLDAP 문서: 버전 2.4 관리자 가이드"을 참조하십시오.

테넌트 그룹 관리

StorageGRID에서 **S3** 테넌트에 대한 그룹 생성

페더레이션 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹의 권한을 관리할 수 있습니다.

시작하기 전에

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

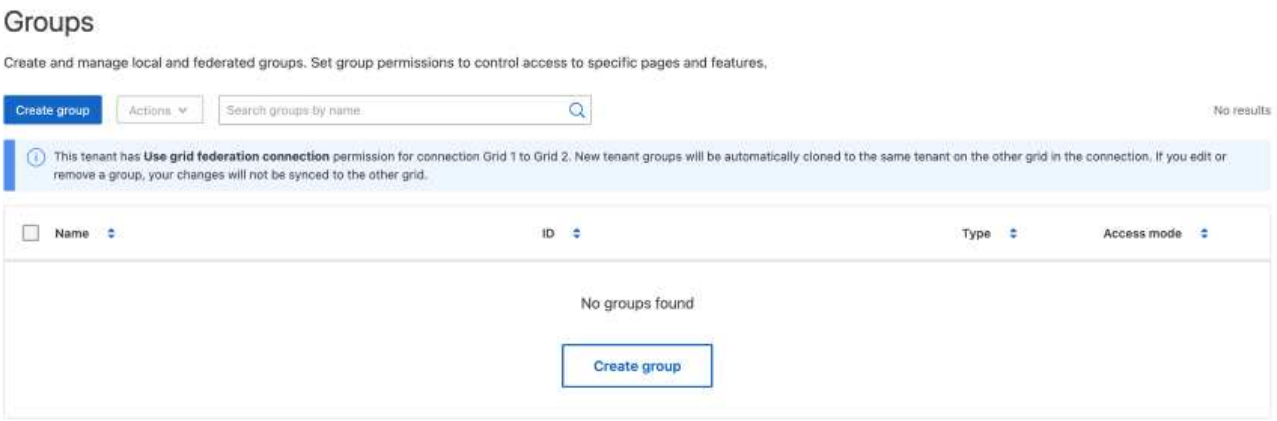
- 연합 그룹을 가져오려는 경우, "구성된 ID 페더레이션", 해당 연합 그룹이 구성된 ID 소스에 이미 존재합니다.
- 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 워크플로 및 고려 사항을 검토했으며 "테넌트 그룹 및 사용자 복제", 테넌트의 소스 그리드에 로그인되어 있어야 합니다.

그룹 생성 마법사에 액세스합니다.

첫 번째 단계로 그룹 생성 마법사에 액세스합니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 이 그리드에서 생성된 새 그룹이 연결된 다른 그리드의 동일한 테넌트에도 복제된다는 것을 나타내는 파란색 배너가 표시되는지 확인하십시오. 이 배너가 표시되지 않으면 테넌트의 대상 그리드에 로그인되어 있을 수 있습니다.



3. *그룹 생성*을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 연합 그룹을 가져올 수 있습니다.

단계

1. 로컬 그룹을 생성하려면 로컬 그룹 탭을 선택하고, 이전에 구성한 ID 소스에서 그룹을 가져오려면 연합 그룹 탭을 선택하십시오.

   StorageGRID 시스템에 단일 로그인(SSO)이 활성화된 경우 로컬 그룹에 속한 사용자는 테넌트 관리자에 로그인할 수 없지만, 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있습니다.

2. 그룹 이름을 입력하세요.
   - 로컬 그룹: 표시 이름과 고유 이름을 모두 입력하세요. 표시 이름은 나중에 수정할 수 있습니다.

     테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 대상 그리드의 테넌트에 동일한 *고유 이름*이 이미 존재하면 복제 오류가 발생합니다.

   - 연합 그룹: 고유한 이름을 입력하십시오. Active Directory의 경우 고유 이름은 `sAMAccountName` 속성과 연결된 이름입니다. OpenLDAP의 경우 고유 이름은 `uid` 속성과 연결된 이름입니다.

3. *Continue*를 선택합니다.

그룹 권한 관리

그룹 권한은 사용자가 테넌트 관리자 및 테넌트 관리 API에서 수행할 수 있는 작업을 제어합니다.

단계

1. *액세스 모드*의 경우 다음 중 하나를 선택하십시오.
   - 읽기-쓰기 (기본값): 사용자는 Tenant Manager에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - 읽기 전용: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 변경하거나 작업을 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 비밀번호를 변경할 수 있습니다.

   > ⓘ 사용자가 여러 그룹에 속해 있고 어떤 그룹이라도 읽기 전용으로 설정되어 있는 경우, 해당 사용자는 선택된 모든 설정 및 기능에 대해 읽기 전용 액세스 권한만 갖게 됩니다.

2. 이 그룹에 대해 하나 이상의 권한을 선택하십시오.

   "테넌트 관리 권한"을 참조하십시오.

3. *Continue*를 선택합니다.

S3 그룹 정책 설정

그룹 정책은 사용자가 가질 S3 액세스 권한을 결정합니다.

단계

1. 이 그룹에 적용할 정책을 선택하십시오.

그룹 정책	설명
S3 액세스 불가	기본값입니다. 이 그룹의 사용자는 버킷 정책을 통해 접근 권한이 부여되지 않는 한 S3 리소스에 접근할 수 없습니다. 이 옵션을 선택하면 기본적으로 루트 사용자만 S3 리소스에 접근할 수 있습니다.
읽기 전용 액세스	이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 갖습니다. 예를 들어, 이 그룹의 사용자는 객체 목록을 보고 객체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책에 대한 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
전체 액세스	이 그룹의 사용자는 버킷을 포함한 S3 리소스에 대한 모든 권한을 갖습니다. 이 옵션을 선택하면 전체 액세스 그룹 정책에 대한 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.

그룹 정책	설명
랜섬웨어 완화	이 예시 정책은 해당 테넌트의 모든 버킷에 적용됩니다. 이 그룹의 사용자는 일반적인 작업을 수행할 수 있지만, 객체 버전 관리가 활성화된 버킷에서 객체를 영구적으로 삭제할 수는 없습니다. 모든 버킷 관리 권한이 있는 Tenant Manager 사용자는 이 그룹 정책을 재정의할 수 있습니다. 모든 버킷 관리 권한은 신뢰할 수 있는 사용자에게만 부여하고, 가능한 경우 다단계 인증(MFA)을 사용하십시오.
사용자 지정	${post_edited_translations.segment}

2. *사용자 지정*을 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책의 크기 제한은 5,120바이트입니다. 유효한 JSON 형식의 문자열을 입력해야 합니다.

   언어 구문 및 예제를 포함한 그룹 정책에 대한 자세한 내용은 "예시 그룹 정책"을 참조하십시오.

3. 로컬 그룹을 생성하는 경우 *계속*을 선택하십시오. 연합 그룹을 생성하는 경우 *그룹 생성*을 선택한 다음 *완료*를 선택하십시오.

사용자 추가 (로컬 그룹만 해당)

사용자를 추가하지 않고 그룹을 저장할 수도 있고, 선택적으로 이미 존재하는 로컬 사용자를 추가할 수도 있습니다.

> ⓘ 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 소스 그리드에서 로컬 그룹을 만들 때 선택한 사용자는 해당 그룹이 타겟 클러스터로 복제될 때 포함되지 않습니다. 따라서 그룹을 만들 때 사용자를 선택하지 마십시오. 대신, 사용자를 만들 때 그룹을 선택하십시오.

단계

1. 선택적으로, 이 그룹에 대해 한 명 이상의 로컬 사용자를 선택할 수 있습니다.
2. 그룹 만들기 및 *완료*를 선택합니다.

   생성한 그룹이 그룹 목록에 나타납니다.

   테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에 있는 경우, 새 그룹이 테넌트의 대상 그리드로 복제됩니다. 그룹 세부 정보 페이지의 개요 섹션에서 *복제 상태*가 *성공*으로 표시됩니다.

StorageGRID 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 사용자는 하나 이상의 권한을 가진 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 설정 및 기능을 보기만 할 수 있는지를 결정합니다.

> 사용자가 여러 그룹에 속해 있고 어떤 그룹이라도 읽기 전용으로 설정되어 있는 경우, 해당 사용자는 선택된 모든 설정 및 기능에 대해 읽기 전용 액세스 권한만 갖게 됩니다.

그룹에 다음과 같은 권한을 할당할 수 있습니다.

권한	설명	세부 정보
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스 권한을 제공합니다.	
S3 자격 증명 직접 관리	사용자가 자신의 S3 액세스 키를 생성하고 삭제할 수 있도록 합니다.	이 권한이 없는 사용자는 **STORAGE (S3)** > **My S3 access keys** 메뉴 옵션을 볼 수 없습니다.
모든 버킷 보기	사용자가 모든 버킷과 버킷 구성을 볼 수 있도록 합니다.	모든 버킷 보기 또는 모든 버킷 관리 권한이 없는 사용자는 버킷 메뉴 옵션을 볼 수 없습니다. 이 권한은 '모든 버킷 관리' 권한으로 대체됩니다. S3 클라이언트 또는 S3 Console에서 사용하는 S3 버킷 또는 그룹 정책에는 영향을 미치지 않습니다.
${post_edited_translations.segment}	사용자는 테넌트 관리자 및 테넌트 관리 API를 사용하여 S3 버킷을 생성 및 삭제하고, S3 버킷 또는 그룹 정책과 관계없이 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다.	모든 버킷 보기 또는 모든 버킷 관리 권한이 없는 사용자는 버킷 메뉴 옵션을 볼 수 없습니다. 이 권한은 '모든 버킷 보기' 권한보다 우선합니다. S3 클라이언트 또는 S3 Console에서 사용하는 S3 버킷 또는 그룹 정책에는 영향을 미치지 않습니다.
엔드포인트 관리	사용자는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID 플랫폼 서비스의 대상으로 사용되는 플랫폼 서비스 엔드포인트를 생성하거나 편집할 수 있습니다.	이 권한이 없는 사용자는 플랫폼 서비스 엔드포인트 메뉴 옵션을 볼 수 없습니다.
S3 콘솔 탭 사용	'모든 버킷 보기' 또는 '모든 버킷 관리' 권한과 함께 사용하면 사용자는 버킷 세부 정보 페이지의 S3 Console 탭에서 객체를 보고 관리할 수 있습니다.	

StorageGRID 테넌트 그룹 관리

${post_edited_translations.segment}

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.

- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.

그룹 보기 또는 편집

각 그룹의 기본 정보와 세부 정보를 확인하고 편집할 수 있습니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 그룹 페이지에 제공된 정보를 검토하십시오. 이 페이지에는 해당 테넌트 계정에 대한 모든 로컬 및 페더레이션 그룹의 기본 정보가 나열되어 있습니다.

   테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 그룹을 보고 있는 경우:

   - 배너 메시지에는 그룹을 편집하거나 삭제하면 변경 사항이 다른 그리드에 동기화되지 않는다는 내용이 표시됩니다.
   - 필요에 따라, 그룹이 대상 그리드의 테넌트로 복제되지 않은 경우 배너 메시지가 표시됩니다. 실패한 항목을 그룹 클론 재시도 수 있습니다.
3. 그룹 이름을 변경하려면:
   a. 해당 그룹의 확인란을 선택합니다.
   b. * 작업 * > * 그룹 이름 편집 * 을 선택합니다.
   c. 새 이름을 입력합니다.
   d. *변경 사항 저장*을 선택합니다.
4. 더 자세한 내용을 보거나 추가 수정을 하려면 다음 중 하나를 수행하십시오.
   - 그룹 이름을 선택합니다.
   - 해당 그룹의 확인란을 선택한 다음 작업 > *그룹 세부 정보 보기*를 선택합니다.
5. 개요 섹션을 검토하십시오. 이 섹션에는 각 그룹에 대한 다음 정보가 나와 있습니다.
   - 표시 이름
   - 고유한 이름
   - 유형
   - 액세스 모드
   - 권한
   - S3 정책
   - 이 그룹의 사용자 수
   - 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 그룹을 보고 있는 경우 추가 필드:
     - 클론 생성 상태 (성공 또는 실패)
     - 이 그룹을 편집하거나 삭제하면 변경 사항이 다른 그리드에 동기화되지 않음을 나타내는 파란색 배너가 표시됩니다.
6. 필요에 따라 그룹 설정을 편집하세요. 입력할 내용에 대한 자세한 내용은 "S3 테넌트에 대한 그룹 생성"을 참조하세요.

a. 개요 섹션에서 이름 또는 편집 아이콘 을 선택하여 표시 이름을 변경합니다.

b. 그룹 권한 탭에서 권한을 업데이트하고 *변경 내용 저장*을 선택합니다.

c. 그룹 정책 탭에서 변경 사항을 적용하고 *변경 내용 저장*을 선택합니다.

선택적으로 다른 S3 그룹 정책을 선택하거나 필요에 따라 사용자 지정 정책에 대한 JSON 문자열을 입력합니다.

7. 기존 로컬 사용자를 하나 이상 그룹에 추가하려면 다음 단계를 따르십시오.

a. 사용자 탭을 선택합니다.

b. *사용자 추가*를 선택합니다.

c. 추가할 기존 사용자를 선택하고 *사용자 추가*를 선택합니다.

성공 메시지가 오른쪽 상단에 나타납니다.

8. 로컬 사용자를 그룹에서 제거하려면:

a. 사용자 탭을 선택합니다.

b. *사용자 제거*를 선택합니다.

c. 삭제할 사용자를 선택하고 *사용자 삭제*를 선택합니다.

성공 메시지가 오른쪽 상단에 나타납니다.

9. 변경한 각 섹션에 대해 *변경 내용 저장*을 선택했는지 확인하십시오.

중복 그룹

기존 그룹을 복제하면 새 그룹을 더 빠르게 만들 수 있습니다.

테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 원본 그리드에서 그룹을 복제하면 복제된 그룹이 테넌트의 대상 그리드에도 복제됩니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 복제하려는 그룹의 확인란을 선택합니다.
3. 작업 > *그룹 복제*를 선택합니다.
4. 입력할 내용에 대한 자세한 내용은 "S3 테넌트에 대한 그룹 생성"을 참조하십시오.
5. *그룹 생성*을 선택합니다.

그룹 클론 재시도

실패한 클론을 다시 시도하려면:

1. 그룹 이름 아래에 _(복제 실패)_라고 표시된 각 그룹을 선택하십시오.
2. 작업 > *그룹 복제*를 선택합니다.
3. 복제하려는 각 그룹의 세부 정보 페이지에서 복제 작업의 상태를 확인할 수 있습니다.

자세한 내용은 "테넌트 그룹 및 사용자 복제"을 참조하십시오.

하나 이상의 그룹 삭제

하나 이상의 그룹을 삭제할 수 있습니다. 삭제된 그룹에만 속한 사용자는 더 이상 테넌트 관리자에 로그인하거나 해당 테넌트 계정을 사용할 수 없습니다.

> 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 그룹을 삭제하면 StorageGRID는 다른 그리드에서 해당 그룹을 삭제하지 않습니다. 이 정보를 동기화 상태로 유지해야 하는 경우, 양쪽 그리드에서 동일한 그룹을 삭제해야 합니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 삭제하려는 각 그룹의 확인란을 선택합니다.
3. 작업 > 그룹 삭제 또는 작업 > *그룹 삭제*를 선택합니다.

   확인 대화 상자가 나타납니다.

4. 그룹 삭제 또는 *그룹 삭제*를 선택합니다.

AssumeRole 설정

시작하기 전에

AssumeRole을 설정하려면 관리자여야 합니다.

이 작업 정보

AssumeRole을 설정하려면 대상 그룹이 없는 경우 인수할 대상 그룹을 생성합니다. 그룹의 S3 정책을 편집하여 이 그룹을 인수할 때 허용되는 작업을 지정합니다. 그룹의 S3 트러스트 정책을 편집하여 AssumeRole API를 사용하여 그룹을 인수할 수 있는 신뢰할 수 있는 사용자를 지정합니다.

이 그룹에 대한 권한을 위임받아 생성된 임시 보안 자격 증명은 제한된 기간 동안만 유효합니다. 세션 지속 시간은 15분에서 12시간 사이이며, 기본 세션 지속 시간은 1시간입니다. 사용자를 그룹의 S3 신뢰 정책에서 제거하면 해당 사용자는 더 이상 이 그룹에 대한 권한을 위임받을 수 없습니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 그룹 이름을 클릭합니다.
3. **S3** 신뢰 정책 탭을 선택합니다.
4. S3 신뢰 정책을 추가합니다. 여기에는 AssumeRole을 수행할 수 있는 사용자 목록이 포함됩니다.

5. *변경 사항 저장*을 선택합니다.
6. **S3** 그룹 정책 탭을 선택합니다.
7. 이 그룹의 S3 신뢰 정책에 추가된 신뢰 사용자에게 필요한 S3 작업만 지정하도록 S3 정책을 편집하십시오.
8. *변경 사항 저장*을 선택합니다.

AssumeRole S3 신뢰 정책의 예시

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

구성이 완료되면 S3 신뢰 정책에 등록된 사용자는 AssumeRole을 수행하고 자격 증명을 받을 수 있습니다. 최종 권한은 그룹 정책, 버킷 정책 및 세션 정책에 따라 결정됩니다. 자세한 내용은 "액세스 정책 사용"을 참조하십시오.

StorageGRID 테넌트 사용자 관리

로컬 사용자를 생성하고 로컬 그룹에 할당하여 해당 사용자가 액세스할 수 있는 기능을 지정할 수 있습니다. 페더레이션된 사용자를 가져올 수도 있습니다. 테넌트 관리자에는 "root"라는 이름의 미리 정의된 로컬 사용자가 하나 포함되어 있습니다. 로컬 사용자는 추가 및 삭제할 수 있지만, 루트 사용자는 삭제할 수 없습니다.

> StorageGRID 시스템에 단일 로그인(SSO)이 활성화된 경우 로컬 사용자는 Tenant Manager 또는 테넌트 관리 API에 로그인할 수 없지만, 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.
- 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 워크플로 및 고려 사항을 검토했으며 "테넌트 그룹 및 사용자 복제", 테넌트의 소스 그리드에 로그인되어 있어야 합니다.

로컬 사용자 생성

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

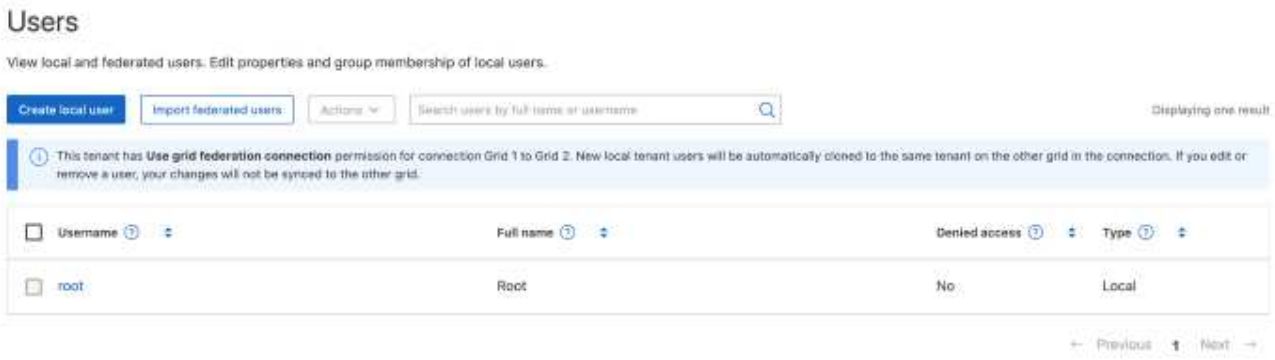
어떤 그룹에도 속하지 않은 S3 사용자는 관리 권한이 없으며 S3 그룹 정책도 적용되지 않습니다. 이러한 사용자는 버킷 정책을 통해 S3 버킷 액세스 권한을 부여받았을 수 있습니다.

사용자 생성 마법사에 액세스합니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.

   테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 파란색 배너가 표시되어 해당 테넌트의 소스 그리드임을 나타냅니다. 이 그리드에서 생성하는 모든 로컬 사용자는 연결된 다른 그리드로 복제됩니다.



2. *사용자 생성*을 선택합니다.

자격 증명을 입력합니다

단계

1. 사용자 자격 증명 입력 단계에서 다음 필드를 입력합니다.

필드	설명
성명	이 사용자의 전체 이름입니다. 예를 들어, 사람의 이름과 성 또는 애플리케이션 이름일 수 있습니다.
사용자 이름	이 사용자가 로그인할 때 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다. 참고: 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 동일한 *사용자 이름*이 대상 그리드의 테넌트에 이미 존재하면 복제 오류가 발생합니다.
비밀번호 및 비밀번호 확인	사용자가 처음 로그인할 때 사용할 비밀번호입니다.

필드	설명
액세스 거부	이 사용자가 하나 이상의 그룹에 속해 있더라도 테넌트 계정에 로그인하지 못하도록 하려면 *예*를 선택하십시오. 예를 들어, 사용자의 로그인 기능을 일시적으로 중단하려면 *예*를 선택하세요.

2. *Continue*를 선택합니다.

그룹에 할당

단계

1. 사용자를 하나 이상의 로컬 그룹에 할당하여 수행할 수 있는 작업을 결정합니다.

   사용자를 그룹에 할당하는 것은 선택 사항입니다. 원하시는 경우, 그룹을 생성하거나 편집할 때 사용자를 선택할 수 있습니다.

   어떤 그룹에도 속하지 않은 사용자는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다. "테넌트 관리 권한"을 참조하십시오.

2. *사용자 생성*을 선택합니다.

   테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에 있는 경우, 새 로컬 사용자가 테넌트의 대상 그리드로 복제됩니다. 사용자 세부 정보 페이지의 개요 섹션에서 *복제 상태*가 *성공*으로 표시됩니다.

3. *완료*를 선택하여 사용자 페이지로 돌아갑니다.

로컬 사용자 보기 또는 편집

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 사용자 페이지에 제공된 정보를 검토하십시오. 이 페이지에는 해당 테넌트 계정의 모든 로컬 및 연합 사용자에 대한 기본 정보가 나열되어 있습니다.

   테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 사용자를 보고 있는 경우:

   - 배너 메시지에는 사용자를 편집하거나 삭제해도 변경 사항이 다른 그리드에 동기화되지 않는다는 내용이 표시됩니다.
   - 필요에 따라, 대상 그리드의 테넌트로 사용자가 복제되지 않은 경우 배너 메시지가 표시됩니다. 실패한 사용자 복제 작업을 다시 시도합니다..

3. 사용자의 전체 이름을 변경하려면:
   a. 사용자의 확인란을 선택합니다.
   b. 작업 > *전체 이름 편집*을 선택합니다.
   c. 새 이름을 입력합니다.
   d. *변경 사항 저장*을 선택합니다.
4. 더 자세한 내용을 보거나 추가 수정을 하려면 다음 중 하나를 수행하십시오.

- 사용자 이름을 선택합니다.
- 해당 사용자의 확인란을 선택한 다음 작업 > *사용자 세부 정보 보기*를 선택합니다.

5. 개요 섹션을 검토하십시오. 이 섹션에는 각 사용자에 대한 다음 정보가 표시됩니다.
   - 성명
   - 사용자 이름
   - 사용자 유형
   - 액세스 거부됨
   - 액세스 모드
   - 그룹 멤버십
   - 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 사용자를 보고 있는 경우 추가 필드:
     - 클론 생성 상태 (성공 또는 실패)
     - 이 사용자의 정보를 수정해도 다른 그리드에 변경 사항이 동기화되지 않음을 나타내는 파란색 배너가 표시됩니다.
6. 필요에 따라 사용자 설정을 편집합니다. 입력할 내용에 대한 자세한 내용은 로컬 사용자 생성을 참조하십시오.
   a. 개요 섹션에서 이름 또는 편집 아이콘 을 선택하여 전체 이름을 변경하세요.

      사용자 이름은 변경할 수 없습니다.

   b. 암호 탭에서 사용자의 암호를 변경하고 *변경 사항 저장*을 선택합니다.
   c. 액세스 탭에서 사용자가 로그인할 수 있도록 허용하려면 *아니요*를 선택하고, 로그인을 차단하려면 *예*를 선택합니다. 그런 다음 *변경 사항 저장*을 선택합니다.
   d. 액세스 키 탭에서 *키 생성*을 선택하고 "다른 사용자의 S3 액세스 키 생성"에 대한 지침을 따르십시오.
   e. 그룹 탭에서 *그룹 편집*을 선택하여 사용자를 그룹에 추가하거나 그룹에서 제거합니다. 그런 다음 *변경 내용 저장*을 선택합니다.
7. 변경한 각 섹션에 대해 *변경 내용 저장*을 선택했는지 확인하십시오.

연합 사용자 가져오기

최대 100명까지 연합 사용자를 하나 이상 사용자 페이지로 직접 가져올 수 있습니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. *연합 사용자 가져오기*를 선택합니다.
3. 연합 사용자 한 명 이상의 UUID 또는 사용자 이름을 입력하십시오.

   여러 항목을 입력하려면 각 UUID 또는 사용자 이름을 새 줄에 추가하십시오.

4. *가져오기*를 선택합니다.

   사용자 필드로의 가져오기가 한 명 이상의 사용자에 대해 실패하는 경우 다음 단계를 수행하십시오.

a. *가져오지 않은 사용자*를 확장하고 *사용자 복사*를 선택합니다.

b. 이전*을 선택하고 복사한 사용자를 *연합 사용자 가져오기 대화 상자에 붙여넣어 가져오기를 다시 시도하십시오.

연합 사용자 가져오기 대화 상자를 닫으면 성공적으로 가져온 사용자에 대한 연합 사용자 정보가 사용자 페이지에 표시됩니다.

로컬 사용자 중복

로컬 사용자를 복제하면 새 사용자를 더 빠르게 생성할 수 있습니다.

> 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 사용자를 복제하면 복제된 사용자가 테넌트의 대상 그리드에도 복제됩니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 복제하려는 사용자의 확인란을 선택합니다.
3. 작업 > *사용자 복제*를 선택합니다.
4. 입력할 내용에 대한 자세한 내용은 로컬 사용자 생성을 참조하십시오.
5. *사용자 생성*을 선택합니다.

사용자 클론 재시도

실패한 클론을 다시 시도하려면:

1. 사용자 이름 아래에 _(복제 실패)_라고 표시된 사용자를 각각 선택하십시오.
2. 작업 > *사용자 복제*를 선택합니다.
3. 복제 대상 사용자 각각의 상세 페이지에서 복제 작업의 상태를 확인할 수 있습니다.

자세한 내용은 "테넌트 그룹 및 사용자 복제"을 참조하십시오.

로컬 사용자 한 명 이상 삭제

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

> 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 로컬 사용자를 삭제하면 StorageGRID는 다른 그리드에서 해당 사용자를 삭제하지 않습니다. 이 정보를 동기화해야 하는 경우 두 그리드에서 동일한 사용자를 모두 삭제해야 합니다.

> 페더레이션 사용자를 삭제하려면 페더레이션 ID 소스를 사용해야 합니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 삭제하려는 각 사용자의 확인란을 선택하십시오.
3. 작업 > 사용자 삭제 또는 작업 > *사용자 삭제*를 선택합니다.

확인 대화 상자가 나타납니다.

4. 사용자 삭제 또는 *사용자 삭제*를 선택합니다.

S3 액세스 키 관리

StorageGRID에서 S3 액세스 키 관리

S3 테넌트 계정의 각 사용자는 StorageGRID 시스템에 객체를 저장하고 검색하기 위해 액세스 키를 보유해야 합니다. 액세스 키는 액세스 키 ID와 비밀 액세스 키로 구성됩니다.

S3 액세스 키는 다음과 같이 관리할 수 있습니다.

- **S3** 자격 증명 관리 권한이 있는 사용자는 자신의 S3 액세스 키를 생성하거나 삭제할 수 있습니다.
- 루트 액세스 권한이 있는 사용자는 S3 루트 계정 및 기타 모든 사용자의 액세스 키를 관리할 수 있습니다. 루트 액세스 키는 버킷 정책에서 명시적으로 비활성화하지 않는 한 테넌트의 모든 버킷 및 객체에 대한 전체 액세스 권한을 제공합니다.

StorageGRID는 서명 버전 2 및 서명 버전 4 인증을 지원합니다. 버킷 정책에서 명시적으로 허용하지 않는 한 계정 간 액세스는 허용되지 않습니다.

StorageGRID에서 자체 S3 액세스 키 생성

S3 테넌트를 사용 중이고 적절한 권한이 있는 경우, S3 액세스 키를 직접 생성할 수 있습니다. 버킷과 객체에 액세스하려면 액세스 키가 필요합니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "S3 자격 증명 또는 루트 액세스 권한을 직접 관리합니다."이(가) 있는 사용자 그룹에 속해 있습니다.

이 작업 정보

테넌트 계정에 대한 버킷을 생성하고 관리할 수 있는 S3 액세스 키를 하나 이상 생성할 수 있습니다. 새 액세스 키를 생성한 후에는 애플리케이션에 새 액세스 키 ID와 비밀 액세스 키를 업데이트하십시오. 보안을 위해 필요한 것보다 많은 키를 생성하지 말고 사용하지 않는 키는 삭제하십시오. 키가 하나만 있고 만료일이 임박한 경우, 만료 전에 새 키를 생성한 다음 기존 키를 삭제하십시오.

각 키에는 특정 만료 시간을 설정하거나 만료 시간을 설정하지 않을 수 있습니다. 만료 시간 설정 시 다음 지침을 따르십시오.

- 액세스 키에 만료 시간을 설정하여 특정 기간 동안만 액세스할 수 있도록 제한하세요. 만료 시간을 짧게 설정하면 액세스 키 ID와 비밀 액세스 키가 실수로 노출될 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 삭제됩니다.
- 보안 위험이 낮아 주기적으로 새 키를 생성할 필요가 없다면 키 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 생성하기로 결정했다면 이전 키는 수동으로 삭제하세요.

계정에 속한 S3 버킷과 객체는 테넌트 관리자에서 계정에 표시된 액세스 키 ID와 비밀 액세스 키를 사용하여 접근할 수 있습니다. 따라서 액세스 키는 비밀번호처럼 안전하게 보호해야 합니다. 액세스 키는 정기적으로 교체하고, 사용하지 않는 키는 계정에서 삭제하며, 다른 사용자와 절대 공유하지 마십시오.

단계

1. **STORAGE (S3)** > *My access keys*를 선택합니다.

   '내 액세스 키' 페이지가 나타나고 기존 액세스 키 목록이 표시됩니다.

2. *키 생성*을 선택합니다.
3. 다음 중 하나를 수행하십시오.
   - 만료되지 않는 키를 생성하려면 *만료 시간 설정 안 함*을 선택하세요. (기본값)
   - *만료 시간 설정*을 선택하고 만료 날짜와 시간을 설정합니다.

   > 만료일은 현재 날짜로부터 최대 5년까지 가능합니다. 만료 시간은 현재 시간으로부터 최소 1분부터 가능합니다.

4. *액세스 키 생성*을 선택합니다.

   액세스 키 다운로드 대화 상자가 나타나고, 액세스 키 ID와 비밀 액세스 키가 표시됩니다.

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

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

6. *완료*를 선택합니다.

   새 키는 내 액세스 키 페이지에 표시됩니다.

7. 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 선택적으로 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제할 수 있습니다. "API를 사용하여 S3 액세스 키 복제"을 참조하십시오.

StorageGRID에서 S3 액세스 키 보기

S3 테넌트를 사용 중이고 "적절한 권한"을(를) 보유하고 있는 경우, S3 액세스 키 목록을 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬하여 어떤 키가 곧 만료되는지 확인할 수 있습니다. 필요에 따라 더 이상 사용하지 않는 키를 "${post_edited_translations.segment}"하거나 "키 삭제"할 수 있습니다.

> 계정에 속한 S3 버킷과 객체는 테넌트 관리자에서 계정에 표시된 액세스 키 ID와 비밀 액세스 키를 사용하여 접근할 수 있습니다. 따라서 액세스 키는 비밀번호처럼 안전하게 보호해야 합니다. 액세스 키는 정기적으로 교체하고, 사용하지 않는 키는 계정에서 삭제하며, 다른 사용자와 절대 공유하지 마십시오.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 S3 자격 증명을 직접 관리할 수 있는 사용자 그룹에 속해 있습니다"권한".

단계

1. **STORAGE (S3)** > *My access keys*를 선택합니다.
2. '내 액세스 키' 페이지에서 기존 액세스 키를 만료 시간 또는 *액세스 키 ID*별로 정렬할 수 있습니다.
3. 필요에 따라 새 키를 생성하거나 더 이상 사용하지 않는 키를 삭제하세요.

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

   만료된 키는 자동으로 삭제됩니다.

StorageGRID에서 자체 S3 액세스 키 삭제

S3 테넌트를 사용 중이고 적절한 권한이 있는 경우, 본인의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키를 삭제하면 해당 키를 사용하여 테넌트 계정의 객체 및 버킷에 더 이상 액세스할 수 없습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 당신은 "S3 자격 증명 권한 직접 관리"을(를) 가지고 있습니다.

> 계정에 속한 S3 버킷과 객체는 테넌트 관리자에서 계정에 표시된 액세스 키 ID와 비밀 액세스 키를 사용하여 접근할 수 있습니다. 따라서 액세스 키는 비밀번호처럼 안전하게 보호해야 합니다. 액세스 키는 정기적으로 교체하고, 사용하지 않는 키는 계정에서 삭제하며, 다른 사용자와 절대 공유하지 마십시오.

단계

1. **STORAGE (S3)** > *My access keys*를 선택합니다.
2. '내 액세스 키' 페이지에서 제거하려는 각 액세스 키의 확인란을 선택합니다.
3. *삭제 키*를 선택합니다.
4. 확인 대화 상자에서 *Delete key*를 선택합니다.

   페이지 오른쪽 상단에 확인 메시지가 나타납니다.

StorageGRID에서 다른 사용자의 S3 액세스 키 생성

S3 테넌트를 사용 중이고 적절한 권한이 있는 경우, 버킷 및 객체에 액세스해야 하는 애플리케이션과 같은 다른 사용자를 위해 S3 액세스 키를 생성할 수 있습니다.

시작하기 전에

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

이 작업 정보

다른 사용자가 자신의 테넌트 계정에 대한 버킷을 생성하고 관리할 수 있도록 하나 이상의 S3 액세스 키를 생성할 수 있습니다. 새 액세스 키를 생성한 후에는 애플리케이션에 새 액세스 키 ID와 비밀 액세스 키를 업데이트해야 합니다. 보안을 위해 사용자가 필요로 하는 것보다 많은 키를 생성하지 말고, 사용하지 않는 키는 삭제하십시오. 키가 하나만

있고 만료일이 임박한 경우, 만료 전에 새 키를 생성하고 기존 키를 삭제하십시오.

각 키에는 특정 만료 시간을 설정하거나 만료 시간을 설정하지 않을 수 있습니다. 만료 시간 설정 시 다음 지침을 따르십시오.

- 사용자의 액세스 권한을 특정 기간으로 제한하려면 키 만료 시간을 설정하세요. 만료 시간을 짧게 설정하면 액세스 키 ID와 비밀 액세스 키가 실수로 노출될 경우 발생할 수 있는 위험을 줄일 수 있습니다. 만료된 키는 자동으로 삭제됩니다.
- 보안 위험이 낮아 주기적으로 새 키를 생성할 필요가 없다면 키 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 생성하기로 결정했다면 이전 키는 수동으로 삭제하세요.

> 사용자가 소유한 S3 버킷과 객체는 테넌트 관리자에서 해당 사용자에게 표시되는 액세스 키 ID와 비밀 액세스 키를 사용하여 접근할 수 있습니다. 따라서 액세스 키는 비밀번호처럼 안전하게 보호해야 합니다. 액세스 키는 정기적으로 교체하고, 사용하지 않는 키는 계정에서 삭제하며, 다른 사용자와 절대 공유하지 마십시오.

단계

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

   사용자 상세 정보 페이지가 나타납니다.
3. *액세스 키*를 선택한 다음 *키 생성*을 선택합니다.
4. 다음 중 하나를 수행하십시오.
   - 만료되지 않는 키를 생성하려면 *만료 시간 설정 안 함*을 선택하세요. (기본값)
   - *만료 시간 설정*을 선택하고 만료 날짜와 시간을 설정합니다.

     > 만료일은 현재 날짜로부터 최대 5년까지 가능합니다. 만료 시간은 현재 시간으로부터 최소 1분부터 가능합니다.
5. *액세스 키 생성*을 선택합니다.

   액세스 키 다운로드 대화 상자가 나타나고, 액세스 키 ID와 비밀 액세스 키가 표시됩니다.
6. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나, *.csv 다운로드*를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

   > 이 정보를 복사하거나 다운로드하기 전까지는 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.
7. *완료*를 선택합니다.

   새 키는 사용자 세부 정보 페이지의 액세스 키 탭에 표시됩니다.
8. 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 선택적으로 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제할 수 있습니다. "API를 사용하여 S3 액세스 키 복제"을 참조하십시오.

StorageGRID에서 다른 사용자의 S3 액세스 키 보기

S3 테넌트를 사용 중이고 적절한 권한이 있는 경우, 다른 사용자의 S3 액세스 키를 볼 수 있습니다. 만료 시간순으로 목록을 정렬하여 곧 만료될 키를 확인할 수 있습니다. 필요에 따라 새 키를 생성하거나 더 이상 사용하지 않는 키를 삭제할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 다음이 있습니다. "루트 액세스 권한".

> 사용자가 소유한 S3 버킷과 객체는 테넌트 관리자에서 해당 사용자에게 표시되는 액세스 키 ID와 비밀 액세스 키를 사용하여 접근할 수 있습니다. 따라서 액세스 키는 비밀번호처럼 안전하게 보호해야 합니다. 액세스 키는 정기적으로 교체하고, 사용하지 않는 키는 계정에서 삭제하며, 다른 사용자와 절대 공유하지 마십시오.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 사용자 페이지에서 S3 액세스 키를 보려는 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 *액세스 키*를 선택합니다.
4. 키를 만료 시간 또는 액세스 키 **ID** 순으로 정렬하세요.
5. 필요에 따라 새 키를 생성하고 더 이상 사용하지 않는 키는 수동으로 삭제하십시오.

   기존 키가 만료되기 전에 새 키를 생성하면 사용자는 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용하여 작업을 시작할 수 있습니다.

   만료된 키는 자동으로 삭제됩니다.

관련 정보

- "다른 사용자의 S3 액세스 키 생성"
- "다른 사용자의 S3 액세스 키 삭제"

StorageGRID에서 다른 사용자의 S3 액세스 키 삭제

S3 테넌트를 사용 중이고 적절한 권한이 있는 경우, 다른 사용자의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제되면 해당 테넌트 계정의 객체 및 버킷에 더 이상 액세스할 수 없습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 다음이 있습니다. "루트 액세스 권한".

사용자가 소유한 S3 버킷과 객체는 테넌트 관리자에서 해당 사용자에게 표시되는 액세스 키 ID와 비밀 액세스 키를 사용하여 접근할 수 있습니다. 따라서 액세스 키는 비밀번호처럼 안전하게 보호해야 합니다. 액세스 키는 정기적으로 교체하고, 사용하지 않는 키는 계정에서 삭제하며, 다른 사용자와 절대 공유하지 마십시오.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 사용자 페이지에서 S3 액세스 키를 관리하려는 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 *액세스 키*를 선택한 다음 삭제하려는 각 액세스 키의 확인란을 선택합니다.
4. 작업 > *선택한 키 삭제*를 선택합니다.
5. 확인 대화 상자에서 *Delete key*를 선택합니다.

   페이지 오른쪽 상단에 확인 메시지가 나타납니다.

S3 버킷 관리

StorageGRID S3 버킷을 생성합니다

테넌트 관리자를 사용하여 객체 데이터용 S3 버킷을 생성할 수 있습니다.

시작하기 전에

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

  버킷 또는 객체의 S3 Object Lock 속성을 설정하거나 수정할 수 있는 권한은 "버킷 정책 또는 그룹 정책"을(를) 통해 부여할 수 있습니다.

- 버킷에 S3 객체 잠금을 활성화하려는 경우, 그리드 관리자가 StorageGRID 시스템에 대한 전역 S3 객체 잠금 설정을 활성화했으며 S3 객체 잠금 버킷 및 객체에 대한 요구 사항을 검토한 상태여야 합니다.
- 각 테넌트가 5,000개의 버킷을 보유하게 될 경우, 그리드의 각 스토리지 노드에는 최소 64GB의 RAM이 필요합니다.

  각 그리드는 최대 100,000개의 버킷을 가질 수 있으며, 여기에는 "브랜치 버킷"이(가) 포함됩니다.

마법사에 액세스합니다

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
2. *버킷 생성*을 선택합니다.

세부 정보를 입력합니다

단계

1. 버킷에 대한 세부 정보를 입력합니다.

필드	설명
버킷 이름	이 규칙을 준수하는 버킷의 이름: • 각 StorageGRID 시스템 전체에서 고유해야 합니다(테넌트 계정 내에서만 고유한 것이 아님). • DNS 규정을 준수해야 합니다. • 최소 3자, 최대 63자여야 합니다. • 각 라벨은 소문자 또는 숫자로 시작하고 끝나야 하며, 소문자, 숫자 및 하이픈만 사용할 수 있습니다. • 가상 호스팅 스타일 요청에는 마침표를 포함해서는 안 됩니다. 마침표는 서버 와일드카드 인증서 검증에 문제를 일으킬 수 있습니다. 자세한 내용은 "Amazon Web Services(AWS) 버킷 이름 지정 규칙에 대한 문서"를 참조하십시오. 참고: 버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.
지역	버킷의 영역. StorageGRID 관리자가 사용 가능한 리전을 관리합니다. 버킷의 리전은 객체에 적용되는 데이터 보호 정책에 영향을 줄 수 있습니다. 기본적으로 모든 버킷은 `us-east-1` 리전에 생성됩니다. 기본 리전이 `us-east-1` 이외의 다른 리전으로 구성된 경우, 드롭다운에서 해당 다른 리전이 처음에 선택됩니다. 참고: 버킷 생성 후에는 지역을 변경할 수 없습니다.

2. *Continue*를 선택합니다.

설정 관리

단계

1. 선택적으로 버킷에 대한 객체 버전 관리를 활성화할 수 있습니다.

   이 버킷에 각 객체의 모든 버전을 저장하려면 객체 버전 관리를 활성화하십시오. 그러면 필요에 따라 객체의 이전 버전을 검색할 수 있습니다.

   다음과 같은 경우 객체 버전 관리를 활성화해야 합니다.

   ◦ 해당 버킷은 그리드 간 복제에 사용됩니다.
   ◦ 이 버킷에서 "브랜치 버킷"을(를) 생성하려고 합니다.

2. 전역 S3 Object Lock 설정이 활성화된 경우, 쓰기 1회-읽기 다수(WORM) 모델을 사용하여 객체를 저장하기 위해 버킷에 대해 S3 Object Lock을 선택적으로 활성화할 수 있습니다.

특정 규제 요건을 충족하는 등 일정 기간 동안 객체를 보존해야 하는 경우에만 버킷에 S3 Object Lock을 활성화하십시오. S3 Object Lock은 객체가 일정 기간 또는 무기한으로 삭제되거나 덮어쓰이는 것을 방지하는 영구적인 설정입니다.

> 버킷에 대해 S3 Object Lock 설정을 활성화하면 비활성화할 수 없습니다. 올바른 권한을 가진 사용자는 해당 버킷에 변경할 수 없는 객체를 추가할 수 있습니다. 이러한 객체 또는 버킷 자체를 삭제하지 못할 수도 있습니다.

버킷에 S3 객체 잠금을 활성화하면 버킷 버전 관리가 자동으로 활성화됩니다.

3. *S3 객체 잠금 사용*을 선택한 경우, 선택적으로 이 버킷에 대해 *기본 보존*을 사용 설정할 수 있습니다.

> 그리드 관리자가 "S3 Object Lock의 특정 기능 사용"할 수 있는 권한을 부여해야 합니다.

기본 보존*이 활성화되면 버킷에 새로 추가된 객체는 삭제되거나 덮어쓰기되지 않도록 자동으로 보호됩니다**.** *기본 보존 설정은 자체 보존 기간이 있는 객체에는 적용되지 않습니다.

a. *기본 보존*이 활성화된 경우 버킷에 대한 *기본 보존 모드*를 지정하십시오.

기본 보존 모드	설명
거버넌스	• `s3:BypassGovernanceRetention` 권한이 있는 사용자는 `x-amz-bypass-governance-retention: true` 요청 헤더를 사용하여 보존 설정을 우회할 수 있습니다. • 이러한 사용자는 보존 기한이 도래하기 전에 개체 버전을 삭제할 수 있습니다. • 이러한 사용자는 개체의 보존 기간을 늘리거나 줄이거나 없앨 수 있습니다.
규정 준수	• 해당 객체는 지정된 보존 기간이 만료될 때까지 삭제할 수 없습니다. • 객체의 보존 기간은 늘릴 수는 있지만 줄일 수는 없습니다. • 해당 날짜에 도달할 때까지 객체의 보존 기한을 제거할 수 없습니다. 참고: 그리드 관리자가 규정 준수 모드 사용을 허용해야 합니다.

b. *기본 보존*이 활성화된 경우 버킷의 *기본 보존 기간*을 지정하십시오.

*기본 보존 기간*은 이 버킷에 새로 추가된 객체를 수집 시점부터 보존할 기간을 나타냅니다. 그리드 관리자가 설정한 테넌트의 최대 보존 기간 이하의 값을 지정하십시오.

최대 보존 기간은 1일에서 100년까지의 값으로 설정할 수 있으며, 그리드 관리자가 테넌트를 생성할 때 설정됩니다. 기본 보존 기간을 설정할 때는 최대 보존 기간에 설정된 값을 초과할 수 없습니다. 필요한 경우 그리드 관리자에게 최대 보존 기간을 늘리거나 줄이도록 요청하십시오.

4. 선택적으로 *용량 제한 활성화*를 선택하고 값을 입력한 다음 용량 단위를 선택합니다.

용량 제한은 해당 버킷의 객체에 사용할 수 있는 최대 용량입니다. 이 값은 물리적 용량(디스크 용량)이 아닌 논리적 용량(객체 크기)을 나타냅니다.

제한이 설정되지 않은 경우 이 버킷의 용량은 무제한입니다. 자세한 내용은 "용량 제한 사용량"을 참조하십시오.

5. 선택적으로 *객체 개수 제한 활성화*를 선택합니다.

   객체 개수 제한은 이 버킷에 포함될 수 있는 최대 객체 수입니다. 이 값은 논리적 양(객체 개수)을 나타냅니다. 제한이 설정되지 않은 경우 객체 개수는 무제한입니다.

6. *버킷 생성*을 선택합니다.

   버킷이 생성되어 버킷 페이지의 표에 추가됩니다.

7. 필요에 따라 *버킷 세부 정보 페이지로 이동*을 선택하여 "버킷 세부 정보 보기" 추가 구성을 수행합니다.

또한 필요에 따라 "브랜치 버킷 생성"할 수 있습니다.

StorageGRID에서 S3 버킷 세부 정보 보기

버킷은 테넌트 계정에서 확인할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스, 모든 버킷 관리 또는 모든 버킷 보기 권한"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지(S3) > *버킷*을 선택합니다.

   버킷 페이지가 나타납니다.

2. 각 버킷의 요약 테이블을 검토하십시오.

   필요에 따라 원하는 열을 기준으로 정보를 정렬하거나 목록을 앞뒤로 넘겨볼 수 있습니다.

   > 표시되는 객체 개수, 사용 공간 및 사용량 값은 추정치입니다. 이러한 추정치는 데이터 수집 시간, 네트워크 연결 상태 및 노드 상태의 영향을 받습니다. 버킷에 버전 관리가 활성화된 경우 삭제된 객체 버전도 객체 개수에 포함됩니다.

   이름
   : 버킷의 고유 이름이며 변경할 수 없습니다.

   활성화된 기능
   : 버킷에 대해 활성화된 기능 목록입니다.

   S3 Object Lock
   : 버킷에 대해 S3 객체 잠금이 활성화되어 있는지 여부입니다.

     이 열은 그리드에 S3 Object Lock이 활성화된 경우에만 표시됩니다. 또한 이 열에는 기존 규정 준수 버킷에 대한 정보도 표시됩니다.

지역

버킷의 리전은 변경할 수 없습니다. 이 열은 기본적으로 숨겨져 있습니다.

객체 개수

이 버킷에 있는 객체의 개수입니다. 버킷에 버전 관리가 활성화된 경우, 현재 버전이 아닌 객체 버전도 이 값에 포함됩니다.

객체가 추가되거나 삭제될 때 이 값이 즉시 업데이트되지 않을 수 있습니다.

사용된 공간

버킷에 있는 모든 객체의 논리적 크기입니다. 논리적 크기에는 복제본이나 이레이저 코딩된 복사본 또는 객체 메타데이터에 필요한 실제 공간이 포함되지 않습니다.

이 값이 업데이트되는 데 최대 10분이 소요될 수 있습니다.

사용법

버킷 용량 제한이 설정된 경우, 해당 용량 제한에서 사용된 비율입니다.

사용량 값은 내부 추정치를 기반으로 하며 경우에 따라 초과될 수 있습니다. 예를 들어, StorageGRID는 테넌트가 객체 업로드를 시작할 때 용량 제한(설정된 경우)을 확인하고, 테넌트가 용량 제한을 초과한 경우 해당 버킷으로의 새로운 객체 업로드를 거부합니다. 하지만 StorageGRID는 용량 제한 초과 여부를 판단할 때 현재 업로드 중인 객체의 크기는 고려하지 않습니다. 객체가 삭제되면 테넌트는 용량 제한 사용량이 다시 계산될 때까지 해당 버킷에 새로운 객체를 업로드할 수 없게 될 수 있습니다. 계산에는 10분 이상 소요될 수 있습니다.

이 값은 객체와 해당 메타데이터를 저장하는 데 필요한 물리적 크기가 아닌 논리적 크기를 나타냅니다.

용량

설정된 경우, 버킷의 용량 제한입니다.

생성일

버킷이 생성된 날짜 및 시간입니다. 이 열은 기본적으로 숨겨져 있습니다.

3. 특정 버킷의 세부 정보를 보려면 표에서 버킷 이름을 선택하십시오.
   a. 버킷에 대한 자세한 정보(예: 지역 및 객체 수)를 확인하려면 웹 페이지 상단의 요약 정보를 참조하십시오.
   b. 용량 제한 사용량 및 객체 개수 제한 사용량 막대를 확인하십시오. 사용량이 100%이거나 100%에 가까운 경우 제한을 늘리거나 일부 객체를 삭제하는 것을 고려하십시오.
   c. 필요에 따라 버킷의 객체 삭제 및 *버킷 삭제*를 선택하십시오.

      각 옵션을 선택할 때 나타나는 주의 사항을 주의 깊게 살펴보십시오. 자세한 내용은 다음을 참조하십시오.

      - "버킷의 모든 객체를 삭제합니다"
      - "버킷 삭제" (버킷은 비어 있어야 합니다)

   d. 필요에 따라 각 탭에서 버킷 설정을 확인하거나 변경할 수 있습니다.
      - **S3** 콘솔: 버킷의 객체를 볼 수 있습니다. 자세한 내용은 "S3 콘솔 사용"을 참조하십시오.
      - 버킷 옵션: 옵션 설정을 보거나 변경할 수 있습니다. S3 Object Lock과 같은 일부 설정은 버킷 생성 후에는

변경할 수 없습니다.

- "버킷 일관성 관리"
- "최근 액세스 시간 업데이트"
- "용량 제한"
- "객체 개수 제한"
- "객체 버전 관리"
- "S3 Object Lock"
- "기본 버킷 보존 기간"
- "그리드 간 복제 관리" (테넌트에 허용된 경우)

- 플랫폼 서비스: "플랫폼 서비스 관리"(테넌트에 허용된 경우)
- 버킷 접근: 옵션 설정을 보거나 변경할 수 있습니다. 특정 접근 권한이 필요합니다.
  - "버킷 및 객체에 대한 CORS"을 구성하여 버킷과 버킷 내의 객체가 다른 도메인의 웹 애플리케이션에서 액세스할 수 있도록 합니다.
  - "사용자 접근 제어" S3 버킷 및 해당 버킷에 있는 객체에 대한 정보입니다.
- **Branches**: 해당 버킷에 대한 분기 버킷 목록을 봅니다. "새 브랜치 버킷을 생성하거나 브랜치 버킷을 관리합니다.".

StorageGRID 브랜치 버킷에 대해 알아보세요

브랜치 버킷은 특정 시점의 버킷 내 객체에 대한 접근을 제공합니다.

기존 버킷에서 브랜치 버킷을 생성할 수 있습니다. 브랜치 버킷을 생성한 후에는 해당 버킷이 생성된 원래 버킷을 _기본 버킷_이라고 합니다. 또한 다른 브랜치 버킷에서 브랜치 버킷을 생성할 수도 있습니다.

브랜치 버킷은 보호된 데이터에 대한 접근을 제공하지만 백업 역할은 하지 않습니다. 데이터를 계속 보호하려면 기본 버킷에서 다음 기능을 사용하십시오.

- "S3 Object Lock"
- "교차 그리드 복제" 기본 버킷용
- "버킷 정책" 버전 관리 버킷에서 오래된 객체 버전을 정리하려면

브랜치 버킷의 다음 특성에 유의하십시오.

- "S3 콘솔에서 객체 다운로드"을 사용하여 브랜치 버킷의 객체에 액세스할 수 있습니다.
- 클라이언트가 브랜치 버킷의 객체에 접근할 때, 기본 버킷의 정책이 아닌 브랜치 버킷의 "${post_edited_translations.segment}"에 따라 접근 허용 여부가 결정됩니다.
- 기본 버킷에서 생성된 객체는 "ILM 규칙"이(가) 기본 버킷에 적용되는 방식을 기반으로 평가됩니다. 브랜치 버킷에서 생성된 객체는 ILM 규칙이 브랜치 버킷에 적용되는 방식을 기반으로 평가됩니다.
- ${post_edited_translations.segment}
- 브랜치 버킷에서는 플랫폼 서비스가 지원되지 않습니다.

${post_edited_translations.segment}

- 손상된 객체를 제거하려면 손상 발생 이전 시점을 기준으로 브랜치 버킷을 생성한 다음, 애플리케이션이 손상된 객체가 포함된 기본 버킷 대신 브랜치 버킷을 가리키도록 설정하면 됩니다.
- 버전 관리 버킷에 데이터를 저장하고 있습니다. 예기치 않은 취약점으로 인해 시간 *T* 이후에 원치 않는 많은 오브젝트가 수집되었습니다. Before 시간 값인 _T_에 대한 브랜치 버킷을 생성하고 클라이언트 작업을 해당 브랜치 버킷으로 재지정할 수 있습니다. 그러면 Before 시간 _T_보다 이전에 수집된 오브젝트만 클라이언트에 노출됩니다.

${post_edited_translations.segment}

- 브랜치 버킷에 대한 PUT 객체 작업은 해당 브랜치에 객체를 생성합니다.
- 브랜치 버킷에 대한 GET 객체 작업은 브랜치에서 객체를 가져옵니다. 객체가 브랜치 버킷에 존재하지 않는 경우, 베이스 버킷에서 객체를 가져옵니다.
- 브랜치 버킷에서 객체가 삭제되는 과정은 다음과 같습니다.

작업	대상	결과	기본 버킷에서의 객체 가시성	브랜치 버킷에서의 객체 가시성
버전 ID 없이 삭제	베이스 버킷	삭제 표시는 기본 버킷에만 생성됩니다.	HEAD/GET 시 객체가 존재하지 않음을 반환하지만 특정 버전에는 여전히 액세스할 수 있습니다	HEAD/GET 반환 시 객체가 존재하며 특정 버전에 계속 액세스할 수 있습니다. 삭제 표시는 브랜치 버킷의 `beforeTime` 이후에 생성되었을 것입니다.
버전 ID로 삭제	베이스 버킷	특정 객체 버전이 기본 버킷과 분기 버킷 모두에서 삭제됩니다.	HEAD/GET이 객체 버전이 존재하지 않음을 반환합니다	HEAD/GET이 객체 버전이 존재하지 않음을 반환합니다
버전 ID 없이 삭제	브랜치 버킷	삭제 표시는 브랜치 버킷에만 생성됩니다.	HEAD/GET 요청은 객체를 반환합니다(기본 버킷 객체는 영향을 받지 않음)	HEAD/GET가 개체가 존재하지 않음을 반환합니다
버전 ID로 삭제	브랜치 버킷	${post_edited_translations.segment}	${post_edited_translations.segment}	HEAD/GET이 객체 버전이 존재하지 않음을 반환합니다

또한 "S3 버전 관리 객체가 삭제되는 방법"을(를) 참조하십시오.

StorageGRID 브랜치 버킷 관리

테넌트 관리자를 사용하여 브랜치 버킷을 생성하고 세부 정보를 볼 수 있습니다.

시작하기 전에

- "지원되는 웹 브라우저"을 사용하여 테넌트 관리자에 로그인했습니다.
- 루트 액세스 또는 "모든 버킷 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷

정책의 권한 설정을 재정의합니다.

- 브랜치를 생성하려는 기본 버킷에는 "버전 관리가 활성화됨"이(가) 있습니다.
- 기본 버킷의 소유자입니다.

이 작업 정보

브랜치 버킷에 대한 다음 정보를 참고하십시오.

- 버킷 또는 객체의 S3 Object Lock 속성을 설정하는 권한은 "버킷 정책 또는 그룹 정책"을(를) 통해 부여할 수 있습니다.
- 기본 버킷의 버전 관리를 일시 중지하면 기본 버킷의 내용이 해당 브랜치 버킷에서 더 이상 표시되지 않습니다.

브랜치 버킷을 구성하고 생성한 후에는 구성을 변경할 수 없습니다.

브랜치 버킷 생성

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
2. 브랜치를 생성할 버킷("기본 버킷")을 선택합니다.
3. 버킷 세부 정보 페이지에서 **Branches** > *Create branch bucket*을 선택합니다.

   기본 버킷에 버전 관리가 활성화되어 있지 않으면 브랜치 버킷 생성 버튼이 비활성화됩니다.

세부 정보를 입력합니다

단계

1. 브랜치 버킷에 대한 세부 정보를 입력하세요.

필드	설명
브랜치 버킷 이름	다음 규칙을 준수하는 브랜치 버킷의 이름: • 각 StorageGRID 시스템 전체에서 고유해야 합니다(테넌트 계정 내에서만 고유한 것이 아님). • DNS 규정을 준수해야 합니다. • 최소 3자, 최대 63자여야 합니다. • 각 라벨은 소문자 또는 숫자로 시작하고 끝나야 하며, 소문자, 숫자 및 하이픈만 사용할 수 있습니다. • 가상 호스팅 스타일 요청에는 마침표를 포함해서는 안 됩니다. 마침표는 서버 와일드카드 인증서 검증에 문제를 일으킬 수 있습니다. 자세한 내용은 "Amazon Web Services(AWS) 버킷 이름 지정 규칙에 대한 문서"를 참조하십시오. 참고: 브랜치 버킷을 생성한 후에는 이름을 변경할 수 없습니다.

필드	설명
지역 (브랜치 버킷의 경우 수정할 수 없음)	브랜치 버킷의 리전. 브랜치 버킷의 지역은 베이스 버킷의 지역과 일치해야 하므로, 브랜치 버킷의 경우 이 필드는 비활성화되어 있습니다.
시간 이전	기본 버킷에서 생성된 객체 버전이 브랜치 버킷에서 액세스 가능해지는 마감 시간입니다. 브랜치 버킷은 Before 시간보다 이전에 생성된 객체 버전에 대한 액세스를 제공합니다. '이전' 시간은 반드시 이미 지난 날짜와 시간이어야 합니다. 미래의 날짜는 될 수 없습니다.
브랜치 버킷 유형	• **Read-write**: 브랜치 버킷에서 객체 또는 객체 버전을 추가하거나 삭제할 수 있습니다. • 읽기 전용: 브랜치 버킷의 객체는 수정할 수 없습니다. 참고: 브랜치 버킷이 비어 있는 경우에만 브랜치 버킷 유형을 읽기 전용으로 설정할 수 있습니다. 기존 브랜치 버킷의 유형이 읽기/쓰기로 설정되어 있고 아직 데이터를 쓰지 않은 경우, 유형을 읽기 전용으로 변경할 수 있습니다.

2. *Continue*를 선택합니다.

객체 설정 관리(선택 사항)

브랜치 버킷의 객체 설정은 기본 버킷의 객체 버전에 영향을 미치지 않습니다.

단계

1. 전역 S3 객체 잠금 설정이 활성화된 경우, 선택적으로 브랜치 버킷에 대해 S3 객체 잠금을 활성화할 수 있습니다. S3 객체 잠금을 활성화하려면 브랜치 버킷은 읽기/쓰기 가능한 버킷이어야 합니다.

   특정 규제 요건을 충족하는 등 일정 기간 동안 객체를 보존해야 하는 경우에만 브랜치 버킷에 S3 Object Lock을 활성화하십시오. S3 Object Lock은 객체가 일정 기간 또는 무기한으로 삭제되거나 덮어쓰이는 것을 방지하는 영구 설정입니다.

   > 버킷에 S3 객체 잠금 설정이 활성화되면 비활성화할 수 없습니다. 올바른 권한을 가진 사용자는 브랜치 버킷에 객체를 추가할 수 있지만, 추가된 객체는 변경할 수 없습니다. 이러한 객체 또는 브랜치 버킷 자체를 삭제하지 못할 수도 있습니다.

2. *S3 객체 잠금 활성화*를 선택한 경우, 선택적으로 브랜치 버킷에 대해 *기본 보존*을 활성화할 수 있습니다.

   > 그리드 관리자가 "S3 Object Lock의 특정 기능 사용"할 수 있는 권한을 부여해야 합니다.

   기본 보존*이 활성화되면 브랜치 버킷에 새로 추가된 객체는 삭제되거나 덮어쓰기되지 않도록 자동으로 보호됩니다. *기본 보존 설정은 자체 보존 기간이 있는 객체에는 적용되지 않습니다.

   a. *기본 보존*이 활성화된 경우, 브랜치 버킷에 대한 *기본 보존 모드*를 지정하십시오.

기본 보존 모드	설명
거버넌스	• `s3:BypassGovernanceRetention` 권한이 있는 사용자는 `x-amz-bypass-governance-retention: true` 요청 헤더를 사용하여 보존 설정을 우회할 수 있습니다. • 이러한 사용자는 보존 기한이 도래하기 전에 개체 버전을 삭제할 수 있습니다. • 이러한 사용자는 개체의 보존 기간을 늘리거나 줄이거나 없앨 수 있습니다.
규정 준수	• 해당 객체는 지정된 보존 기간이 만료될 때까지 삭제할 수 없습니다. • 객체의 보존 기간은 늘릴 수는 있지만 줄일 수는 없습니다. • 해당 날짜에 도달할 때까지 객체의 보존 기한을 제거할 수 없습니다. 참고: 그리드 관리자가 규정 준수 모드 사용을 허용해야 합니다.

b. *기본 보존*이 활성화된 경우, 브랜치 버킷에 대한 *기본 보존 기간*을 지정하십시오.

*기본 보존 기간*은 브랜치 버킷에 새로 추가된 객체를 수집 시점부터 보존할 기간을 나타냅니다. 그리드 관리자가 설정한 테넌트의 최대 보존 기간 이하의 값을 지정하십시오.

최대 보존 기간은 1일에서 100년까지의 값으로 설정할 수 있으며, 그리드 관리자가 테넌트를 생성할 때 설정됩니다. 기본 보존 기간을 설정할 때는 최대 보존 기간에 설정된 값을 초과할 수 없습니다. 필요한 경우 그리드 관리자에게 최대 보존 기간을 늘리거나 줄이도록 요청하십시오.

3. 필요에 따라 *용량 제한 활성화*를 선택합니다.

용량 제한은 브랜치 버킷에 사용할 수 있는 최대 용량입니다. 이 값은 물리적 용량(디스크 용량)이 아닌 논리적 용량(객체 크기)을 나타냅니다.

제한을 설정하지 않으면 브랜치 버킷의 용량은 무제한입니다. 자세한 내용은 "용량 제한 사용량"을 참조하십시오.

> ⓘ 이 설정은 브랜치 버킷에 직접 수집된 객체에만 적용되며, 기본 버킷에서 브랜치 버킷을 통해 볼 수 있는 객체에는 적용되지 않습니다.

4. 선택적으로 *객체 개수 제한 활성화*를 선택합니다.

객체 개수 제한은 브랜치 버킷에 포함될 수 있는 최대 객체 수입니다. 이 값은 논리적 양(객체 개수)을 나타냅니다. 제한이 설정되지 않은 경우 객체 개수는 무제한입니다.

> ⓘ 이 설정은 브랜치 버킷에 직접 수집된 객체에만 적용되며, 기본 버킷에서 브랜치 버킷을 통해 볼 수 있는 객체에는 적용되지 않습니다.

5. *버킷 생성*을 선택합니다.

브랜치 버킷이 생성되어 버킷 페이지의 표에 추가됩니다.

6. 필요에 따라 *버킷 세부 정보 페이지로 이동*을 선택하여 "브랜치 버킷 세부 정보 보기" 추가 구성을 수행합니다.

버킷 세부 정보 페이지에서 읽기 전용 버킷의 경우 객체 수정과 관련된 일부 구성 옵션이 비활성화됩니다.

StorageGRID 버킷에 ILM 정책 태그를 적용합니다

객체 스토리지 요구 사항에 따라 버킷에 적용할 ILM 정책 태그를 선택하십시오.

ILM 정책은 객체 데이터가 저장되는 위치와 특정 기간 후 삭제 여부를 제어합니다. 그리드 관리자는 ILM 정책을 생성하고 여러 활성 정책을 사용하는 경우 ILM 정책 태그에 할당합니다.

버킷의 정책 태그를 자주 변경하지 마십시오. 그렇지 않으면 성능 문제가 발생할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스, 모든 버킷 관리 또는 모든 버킷 보기 권한"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지(S3) > *버킷*을 선택합니다.

   버킷 페이지가 나타납니다. 필요에 따라 원하는 열을 기준으로 정보를 정렬하거나 목록을 앞뒤로 넘겨볼 수 있습니다.

2. ILM 정책 태그를 할당할 버킷 이름을 선택하십시오.

   이미 태그가 할당된 버킷에 대해 ILM 정책 태그 할당을 변경할 수도 있습니다.

   표시되는 객체 개수 및 사용 공간 값은 추정치입니다. 이러한 추정치는 데이터 수집 시간, 네트워크 연결 상태 및 노드 상태의 영향을 받습니다. 버킷에 버전 관리가 활성화된 경우 삭제된 객체 버전도 객체 개수에 포함됩니다.

3. 버킷 옵션 탭에서 ILM 정책 태그 아코디언을 확장합니다. 이 아코디언은 그리드 관리자가 사용자 지정 정책 태그 사용을 활성화한 경우에만 나타납니다.
4. 각 정책 태그의 설명을 읽고 버킷에 적용할 태그를 결정하십시오.

   버킷의 ILM 정책 태그를 변경하면 버킷 내 모든 객체에 대한 ILM 재평가가 수행됩니다. 새 정책에서 객체를 일정 기간 동안 보존하는 경우, 이전 객체는 삭제됩니다.

5. 버킷에 할당할 태그에 해당하는 라디오 버튼을 선택하십시오.
6. *변경 사항 저장*을 선택합니다. 키 `NTAP-SG-ILM-BUCKET-TAG`와 ILM 정책 태그 이름의 값을 가진 새 S3 버킷 태그가 버킷에 설정됩니다.

   S3 애플리케이션이 실수로 새 버킷 태그를 덮어쓰거나 삭제하지 않도록 하십시오. 버킷에 새 TagSet을 적용할 때 이 태그를 누락하면 버킷의 객체는 기본 ILM 정책에 따라 평가됩니다.

ILM 정책 태그는 테넌트 관리자 또는 테넌트 관리자 API를 통해서만 설정하고 수정해야 하며, 이때 ILM 정책 태그의 유효성을 검사해야 합니다. `NTAP-SG-ILM-BUCKET-TAG`S3 PutBucketTagging API 또는 S3 DeleteBucketTagging API를 사용하여 ILM 정책 태그를 수정하지 마십시오.

버킷에 할당된 정책 태그를 변경하면 새 ILM 정책을 사용하여 객체를 재평가하는 동안 일시적인 성능 영향이 발생합니다.

StorageGRID 버킷 정책 관리

S3 버킷 및 해당 버킷에 있는 객체에 대한 사용자 액세스를 제어할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다. 모든 버킷 보기 및 모든 버킷 관리 권한은 보기만 허용합니다.
- 필요한 스토리지 노드 및 사이트 수가 확보되었는지 확인했습니다. 사이트 내에서 두 개 이상의 스토리지 노드를 사용할 수 없거나 사이트를 사용할 수 없는 경우, 이러한 설정을 변경하지 못할 수 있습니다.

단계

1. *버킷*을 선택한 다음 관리할 버킷을 선택합니다.
2. ${post_edited_translations.segment}
3. 다음 중 하나를 수행하십시오.
   - 정책 활성화 확인란을 선택하여 버킷 정책을 입력합니다. 그런 다음 유효한 JSON 형식의 문자열을 입력합니다.

     각 버킷 정책에는 20,480바이트의 크기 제한이 있습니다.
   - 기존 정책을 수정하려면 문자열을 편집하세요.
   - *정책 활성화*를 선택 해제하여 정책을 비활성화합니다.

버킷 정책에 대한 자세한 내용(언어 구문 및 예제 포함)은 "예시 버킷 정책"을 참조하십시오.

StorageGRID 버킷 일관성 관리

일관성 값은 버킷 설정 변경의 가용성을 지정하는 데 사용될 수 있으며, 버킷 내 객체의 가용성과 여러 스토리지 노드 및 사이트 간 객체의 일관성 간의 균형을 유지하는 데에도 사용될 수 있습니다. 클라이언트 애플리케이션의 운영 요구 사항에 맞춰 일관성 값을 기본값과 다르게 변경할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

버킷 일관성 지침

버킷 일관성은 해당 S3 버킷 내의 객체에 영향을 미치는 클라이언트 애플리케이션의 일관성을 결정하는 데 사용됩니다. 일반적으로 버킷에는 새 쓰기 후 읽기 일관성을 사용하는 것이 좋습니다.

버킷 일관성 변경

새 쓰기 후 읽기 일관성이 클라이언트 애플리케이션의 요구 사항을 충족하지 못하는 경우, 버킷 일관성을 설정하거나 `Consistency-Control` 헤더를 사용하여 일관성을 변경할 수 있습니다. `Consistency-Control` 헤더를 사용하면 버킷 일관성 설정이 재정의됩니다.

> 버킷의 일관성을 변경하면 변경 이후에 수집된 객체만 수정된 설정을 충족하는 것으로 보장됩니다.

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
2. 표에서 버킷 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.
3. 버킷 옵션 탭에서 ** 아코디언을 선택합니다.
4. ${post_edited_translations.segment}
   - 모두: 최고 수준의 일관성을 제공합니다. 모든 노드가 데이터를 즉시 수신하며, 그렇지 않을 경우 요청이 실패합니다.
   - **Strong-global**: 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
   - **Strong-site**: 사이트 내 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
   - **Read-after-new-write** (기본값): 새 객체에 대한 read-after-write 일관성 및 객체 업데이트에 대한 최종 일관성을 제공합니다. 높은 가용성 및 데이터 보호 보장을 제공합니다. 대부분의 경우에 권장됩니다.
   - 사용 가능: 새 객체 생성 및 객체 업데이트 모두에 대해 최종 일관성을 제공합니다. S3 버킷의 경우, 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷 또는 존재하지 않는 키에 대한 HEAD 또는 GET 작업). S3 FabricPool 버킷에서는 지원되지 않습니다.
5. *변경 사항 저장*을 선택합니다.

버킷 설정을 변경하면 어떻게 되나요**?**

버킷에는 버킷 및 버킷 내 객체의 동작에 영향을 미치는 여러 설정이 있습니다.

다음 버킷 설정은 기본적으로 강력한 일관성을 사용합니다. 사이트 내에서 두 개 이상의 스토리지 노드를 사용할 수 없거나 사이트를 사용할 수 없는 경우 이러한 설정을 변경해도 적용되지 않을 수 있습니다.

- "${post_edited_translations.segment}"
- "최종 액세스 시간"
- "버킷 수명 주기"
- "버킷 정책"
- "버킷 태깅"
- "버킷 버전 관리"

- "S3 Object Lock"
- "버킷 암호화"

> 버킷 버전 관리, S3 Object Lock 및 버킷 암호화의 일관성 값은 강력한 일관성을 보장하지 않는 값으로 설정할 수 없습니다.

다음 버킷 설정은 강력한 일관성을 사용하지 않으며 변경 사항에 대한 가용성이 더 높습니다. 이러한 설정의 변경 사항이 적용되는 데는 어느 정도 시간이 걸릴 수 있습니다.

- "플랫폼 서비스 구성: 알림, 복제 또는 검색 통합"
- "버킷 및 객체에 대한 StorageGRID CORS 구성"
- 버킷 일관성 변경

> 버킷 설정을 변경할 때 사용되는 기본 일관성이 클라이언트 애플리케이션의 요구사항을 충족하지 않는 경우, "S3 REST API"에 대한 `Consistency-Control` 헤더를 사용하거나 "테넌트 관리 API"의 `reducedConsistency` 또는 `force` 옵션을 사용하여 일관성을 변경할 수 있습니다.

StorageGRID에서 마지막 액세스 시간 업데이트 활성화 또는 비활성화

그리드 관리자가 StorageGRID 시스템의 정보 라이프사이클 관리(ILM) 규칙을 생성할 때, 객체의 마지막 액세스 시간을 기준으로 해당 객체를 다른 스토리지 위치로 이동할지 여부를 결정하도록 선택적으로 지정할 수 있습니다. S3 테넌트를 사용하는 경우, S3 버킷에 있는 객체의 마지막 액세스 시간 업데이트를 활성화하여 이러한 규칙을 활용할 수 있습니다.

이 지침은 고급 필터 또는 참조 시간으로 마지막 액세스 시간 옵션을 사용하는 ILM 규칙이 하나 이상 포함된 StorageGRID 시스템에만 적용됩니다. StorageGRID 시스템에 이러한 규칙이 없는 경우 이 지침을 무시해도 됩니다. 자세한 내용은 "ILM 규칙에서 마지막 액세스 시간 사용"을 참조하십시오.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

마지막 액세스 시간*은 **ILM** 규칙의 *참조 시간 배치 지침에 사용할 수 있는 옵션 중 하나입니다. 규칙의 참조 시간을 마지막 액세스 시간으로 설정하면 그리드 관리자는 객체가 마지막으로 검색(읽기 또는 보기)된 시간을 기준으로 특정 스토리지 위치에 객체를 배치하도록 지정할 수 있습니다.

예를 들어, 최근에 본 객체가 더 빠른 스토리지에 유지되도록 하려면 그리드 관리자가 다음과 같이 지정하는 ILM 규칙을 만들 수 있습니다.

- 지난 한 달 동안 검색된 객체는 로컬 스토리지 노드에 유지되어야 합니다.
- 지난 한 달 동안 검색되지 않은 오브젝트는 오프사이트 위치로 이동해야 합니다.

기본적으로 마지막 액세스 시간 업데이트는 비활성화되어 있습니다. StorageGRID 시스템에 마지막 액세스 시간 옵션을 사용하는 ILM 규칙이 포함되어 있고 이 옵션을 해당 버킷의 객체에 적용하려면 해당 규칙에 지정된 S3 버킷에 대해 마지막 액세스 시간 업데이트를 활성화해야 합니다.

객체를 검색할 때 마지막 액세스 시간을 업데이트하면 특히 작은 객체의 경우 StorageGRID 성능이 저하될 수 있습니다.

마지막 액세스 시간 업데이트로 인해 성능 영향이 발생합니다. StorageGRID가 객체를 검색할 때마다 이러한 추가 단계를 수행해야 하기 때문입니다.

- 새 타임스탬프로 객체를 업데이트합니다
- 해당 객체를 ILM 큐에 추가하여 현재 ILM 규칙 및 정책에 따라 재평가될 수 있도록 합니다.

이 표는 마지막 액세스 시간 기능이 비활성화 또는 활성화되었을 때 버킷 내 모든 객체에 적용되는 동작을 요약합니다.

요청 유형	마지막 액세스 시간이 비활성화된 경우의 동작(기본값)		마지막 액세스 시간이 활성화된 경우의 동작	
	마지막 액세스 시간 업데이트 여부?	해당 객체가 ILM 평가 대기열에 추가되었습니까?	마지막 액세스 시간 업데이트 여부?	해당 객체가 ILM 평가 대기열에 추가되었습니까?
HEAD 작업이 실행될 때 객체의 메타데이터를 검색하기 위한 요청입니다.	아니요	아니요	아니요	아니요
객체, 해당 객체의 액세스 제어 목록 또는 메타데이터를 검색하는 요청	아니요	아니요	예	예
객체의 메타데이터 업데이트 요청	예	예	예	예
객체 또는 객체 버전 목록 요청	아니요	아니요	아니요	아니요
한 버킷에서 다른 버킷으로 객체를 복사하는 요청입니다.	• 아니요, 원본 복사본에 대해서입니다. • 예, 대상 복사본에 대해서입니다.	• 아니요, 원본 복사본에 대해서입니다. • 예, 대상 복사본에 대해서입니다.	• 예, 소스 복사본의 경우 • 예, 대상 복사본에 대해서입니다.	• 예, 소스 복사본의 경우 • 예, 대상 복사본에 대해서입니다.
다중 파트 업로드 완료 요청	네, 조립된 객체에 대해서입니다.	네, 조립된 객체에 대해서입니다.	네, 조립된 객체에 대해서입니다.	네, 조립된 객체에 대해서입니다.

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.

2. 표에서 버킷 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

3. 버킷 옵션 탭에서 마지막 액세스 시간 업데이트 아코디언을 선택합니다.
4. 마지막 액세스 시간 업데이트를 활성화 또는 비활성화합니다.
5. *변경 사항 저장*을 선택합니다.

StorageGRID에서 S3 버킷에 대한 객체 버전 관리 변경

S3 테넌트를 사용하는 경우 S3 버킷의 버전 관리 상태를 변경할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.
- 필요한 스토리지 노드 및 사이트 수가 확보되었는지 확인했습니다. 사이트 내에서 두 개 이상의 스토리지 노드를 사용할 수 없거나 사이트를 사용할 수 없는 경우, 이러한 설정을 변경하지 못할 수 있습니다.

이 작업 정보

버킷에 대해 객체 버전 관리를 활성화하거나 일시 중지할 수 있습니다. 버킷에 대해 버전 관리를 활성화하면 버전 관리가 해제된 상태로 되돌릴 수 없습니다. 하지만 버킷에 대해 버전 관리를 일시 중지할 수는 있습니다.

- 비활성화됨: 버전 관리가 활성화된 적이 없습니다.
- 활성화됨: 버전 관리가 활성화되었습니다.
- 일시 중단됨: 이전에 버전 관리가 활성화되었으나 현재 일시 중단되었습니다.

자세한 내용은 다음을 참조하십시오.

- "객체 버전 관리"
- "S3 버전 관리 객체에 대한 ILM 규칙 및 정책(예제 4)"
- "객체가 삭제되는 방법"

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지(S3) > *버킷*을 선택합니다.
2. 표에서 버킷 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

3. 버킷 옵션 탭에서 객체 버전 관리 아코디언을 선택합니다.
4. 이 버킷에 있는 객체에 대한 버전 관리 상태를 선택하십시오.

   그리드 간 복제에 사용되는 버킷의 경우 객체 버전 관리가 활성화된 상태로 유지되어야 합니다. S3 객체 잠금 또는 레거시 규정 준수가 활성화된 경우 * 객체 버전 관리 * 옵션은 비활성화됩니다.

옵션	설명
버전 관리 활성화	이 버킷에 각 객체의 모든 버전을 저장하려면 객체 버전 관리를 활성화하십시오. 그러면 필요에 따라 객체의 이전 버전을 검색할 수 있습니다. 버킷에 이미 있는 객체는 사용자가 수정할 때 버전이 관리됩니다.
버전 관리 일시 중단	새로운 객체 버전 생성을 더 이상 원하지 않는 경우 객체 버전 관리를 일시 중지하세요. 기존 객체 버전은 언제든지 조회할 수 있습니다.

5. *변경 사항 저장*을 선택합니다.

S3 오브젝트 잠금을 사용하여 StorageGRID에서 오브젝트 보존

버킷과 객체가 보존에 관한 규제 요건을 준수해야 하는 경우 S3 객체 잠금을 사용할 수 있습니다.

S3 Object Lock의 특정 기능을 사용하려면 그리드 관리자의 권한이 필요합니다.

S3 객체 잠금이란 무엇입니까**?**

StorageGRID S3 객체 잠금 기능은 Amazon Simple Storage Service(Amazon S3)의 S3 객체 잠금과 동일한 객체 보호 솔루션입니다.

StorageGRID 시스템에 대해 전역 S3 객체 잠금 설정이 활성화된 경우, S3 테넌트 계정은 S3 객체 잠금 활성화 여부와 관계없이 버킷을 생성할 수 있습니다. 버킷에 S3 객체 잠금이 활성화된 경우 버킷 버전 관리가 필요하며 자동으로 활성화됩니다.

*S3 객체 잠금이 없는 버킷*에는 보존 설정이 지정되지 않은 객체만 저장할 수 있습니다. 수집된 객체에는 보존 설정이 적용되지 않습니다.

*S3 객체 잠금이 설정된 버킷*에는 S3 클라이언트 애플리케이션에서 지정한 보존 설정이 있는 객체와 없는 객체가 모두 포함될 수 있습니다. 수집된 객체 중 일부에는 보존 설정이 적용됩니다.

*S3 객체 잠금 및 기본 보존 설정이 구성된 버킷*에는 보존 설정이 지정된 업로드된 객체와 보존 설정이 없는 새 객체가 모두 존재할 수 있습니다. 새 객체는 객체 수준에서 보존 설정이 구성되지 않았기 때문에 기본 설정을 사용합니다.

기본 보존 설정이 구성된 경우, 새로 수집되는 모든 객체에는 보존 설정이 적용됩니다. 객체 보존 설정이 없는 기존 객체는 영향을 받지 않습니다.

보존 모드

StorageGRID S3 객체 잠금 기능은 객체에 서로 다른 수준의 보호를 적용할 수 있는 두 가지 보존 모드를 지원합니다. 이러한 모드는 Amazon S3의 보존 모드와 동일합니다.

- 규정 준수 모드:
  - 해당 객체는 지정된 보존 기간이 만료될 때까지 삭제할 수 없습니다.
  - 객체의 보존 기간은 늘릴 수는 있지만 줄일 수는 없습니다.
  - 해당 날짜에 도달할 때까지 객체의 보존 기한을 제거할 수 없습니다.

- 거버넌스 모드에서:
  - 특별 권한을 가진 사용자는 요청에 바이패스 헤더를 사용하여 특정 보존 설정을 수정할 수 있습니다.
  - 이러한 사용자는 보존 기한이 도래하기 전에 개체 버전을 삭제할 수 있습니다.
  - 이러한 사용자는 개체의 보존 기간을 늘리거나 줄이거나 없앨 수 있습니다.

객체 버전 보존 설정

S3 객체 잠금이 활성화된 상태로 버킷이 생성된 경우, 사용자는 S3 클라이언트 애플리케이션을 사용하여 버킷에 추가되는 각 객체에 대해 다음과 같은 보존 설정을 선택적으로 지정할 수 있습니다.

- 보존 모드: 규정 준수 또는 거버넌스 중 하나.
- 보존 기한: 객체 버전의 보존 기한이 미래 날짜로 설정되어 있으면 해당 객체를 검색할 수는 있지만 삭제할 수는 없습니다.
- 법적 보류: 객체 버전에 법적 보류를 적용하면 해당 객체가 즉시 잠깁니다. 예를 들어, 조사 또는 법적 분쟁과 관련된 객체에 법적 보류를 적용해야 할 수 있습니다. 법적 보류에는 만료일이 없으며 명시적으로 해제될 때까지 유지됩니다. 법적 보류는 보존 기한과 무관합니다.

  법적 보존 조치가 적용된 객체는 보존 모드와 관계없이 누구도 삭제할 수 없습니다.

  객체 설정에 대한 자세한 내용은 "S3 REST API를 사용하여 S3 Object Lock 구성"을 참조하십시오.

버킷에 대한 기본 보존 설정

S3 객체 잠금이 활성화된 상태로 버킷을 생성하는 경우, 사용자는 선택적으로 버킷에 대해 다음과 같은 기본 설정을 지정할 수 있습니다.

- 기본 보존 모드: 규정 준수 또는 거버넌스 중 하나.
- 기본 보존 기간: 이 버킷에 추가된 새 객체 버전을 추가된 날로부터 보존할 기간입니다.

기본 버킷 설정은 자체 보존 설정이 없는 새 객체에만 적용됩니다. 기존 버킷 객체는 이러한 기본 설정을 추가하거나 변경해도 영향을 받지 않습니다.

"S3 버킷 생성" 및 "S3 객체 잠금 기본 보존 기간 업데이트"을(를) 참조하십시오.

S3 객체 잠금 작업

다음은 그리드 관리자와 테넌트 사용자를 위한 S3 객체 잠금 기능 사용에 필요한 주요 작업 목록입니다.

그리드 관리자

- 전체 StorageGRID 시스템에 대한 글로벌 S3 오브젝트 잠금 설정을 활성화합니다.
- 정보 라이프사이클 관리(ILM) 정책이 규정을 준수하는지 확인하십시오. 즉, 정책이 "S3 객체 잠금이 활성화된 버킷의 요구 사항"을 충족하는지 확인하십시오.
- 필요에 따라 테넌트가 Compliance를 보존 모드로 사용할 수 있도록 허용하십시오. 그렇지 않으면 Governance 모드만 허용됩니다.
- 필요에 따라 테넌트의 최대 보존 기간을 설정합니다.

테넌트 사용자

- S3 객체 잠금을 사용할 때 버킷 및 객체에 대한 고려 사항을 검토하십시오.
- 필요한 경우 그리드 관리자에게 문의하여 전역 S3 오브젝트 잠금 설정을 활성화하고 권한을 설정하십시오.
- S3 객체 잠금이 활성화된 버킷을 생성합니다.
- 선택적으로 버킷의 기본 보존 설정을 구성할 수 있습니다.
  - 기본 보존 모드: 그리드 관리자가 허용하는 경우 Governance 또는 Compliance.
  - 기본 보존 기간: 그리드 관리자가 설정한 최대 보존 기간보다 작거나 같아야 합니다.
- S3 클라이언트 애플리케이션을 사용하여 객체를 추가하고 필요에 따라 객체별 보존 기간을 설정할 수 있습니다.
  - 보존 모드. 그리드 관리자가 허용하는 경우 거버넌스 또는 규정 준수.
  - 보존 기한: 그리드 관리자가 설정한 최대 보존 기간에서 허용하는 날짜보다 작거나 같아야 합니다.

S3 객체 잠금이 활성화된 버킷에 대한 요구 사항

- StorageGRID 시스템에 대해 전역 S3 객체 잠금 설정이 활성화된 경우, 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 S3 객체 잠금이 활성화된 버킷을 생성할 수 있습니다.
- S3 객체 잠금을 사용하려면 버킷 생성 시 S3 객체 잠금을 활성화해야 합니다. 기존 버킷에는 S3 객체 잠금을 활성화할 수 없습니다.
- 버킷에 대해 S3 객체 잠금이 활성화되면 StorageGRID가 해당 버킷에 대한 버전 관리를 자동으로 활성화합니다. 버킷에 대해 S3 객체 잠금을 비활성화하거나 버전 관리를 일시 중지할 수는 없습니다.
- 선택적으로 Tenant Manager, 테넌트 관리 API 또는 S3 REST API를 사용하여 각 버킷에 대한 기본 보존 모드와 보존 기간을 지정할 수 있습니다. 버킷의 기본 보존 설정은 자체 보존 설정이 없는 버킷에 새로 추가되는 객체에만 적용됩니다. 객체 업로드 시 각 객체 버전에 대한 보존 모드와 보존 만료일을 지정하여 이러한 기본 설정을 재정의할 수 있습니다.
- S3 Object Lock이 활성화된 버킷에 대해 버킷 수명 주기 구성이 지원됩니다.
- CloudMirror S3 객체 잠금이 활성화된 버킷의 경우 CloudMirror 복제가 지원되지 않습니다.

S3 객체 잠금이 활성화된 버킷의 객체에 대한 요구 사항

- 객체 버전을 보호하려면 버킷에 대한 기본 보존 설정을 지정하거나 각 객체 버전에 대한 보존 설정을 지정할 수 있습니다. 객체 수준의 보존 설정은 S3 클라이언트 애플리케이션 또는 S3 REST API를 사용하여 지정할 수 있습니다.
- 보존 설정은 개별 객체 버전에 적용됩니다. 객체 버전은 보존 기간 설정과 법적 보존 설정을 모두 가질 수도 있고, 둘 중 하나만 가질 수도 있으며, 둘 다 가지지 않을 수도 있습니다. 객체에 보존 기간 설정 또는 법적 보존 설정을 지정하면 요청에 지정된 버전만 보호됩니다. 객체의 새 버전을 생성할 수 있지만 이전 버전은 계속 잠금 상태로 유지됩니다.

S3 객체 잠금이 활성화된 버킷의 객체 수명 주기

S3 객체 잠금이 활성화된 버킷에 저장되는 각 객체는 다음 단계를 거칩니다.

1. 오브젝트 수집

   S3 객체 잠금이 활성화된 버킷에 객체 버전이 추가되면 보존 설정이 다음과 같이 적용됩니다.

   - 객체에 대한 보존 설정이 지정된 경우 객체 수준 설정이 적용됩니다. 기본 버킷 설정은 무시됩니다.

- 객체에 대한 보존 설정이 지정되지 않은 경우, 기본 버킷 설정이 존재하면 해당 설정이 적용됩니다.
- 객체 또는 버킷에 대한 보존 설정이 지정되지 않은 경우 해당 객체는 S3 Object Lock으로 보호되지 않습니다.

보존 설정이 적용된 경우 객체와 S3 사용자 정의 메타데이터가 모두 보호됩니다.

2. 객체 보존 및 삭제

   보호된 각 객체의 여러 복사본은 지정된 보존 기간 동안 StorageGRID에 저장됩니다. 객체 복사본의 정확한 개수, 유형 및 저장 위치는 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다. 보호 대상 객체를 보존 기한 이전에 삭제할 수 있는지 여부는 해당 객체의 보존 모드에 따라 다릅니다.

   - 법적 보존 조치가 적용된 객체는 보존 모드와 관계없이 누구도 삭제할 수 없습니다.

기존 규정 준수 버킷을 계속 관리할 수 있나요**?**

S3 객체 잠금 기능은 이전 StorageGRID 버전에서 제공되었던 규정 준수 기능을 대체합니다. 이전 버전의 StorageGRID를 사용하여 규정 준수 버킷을 생성한 경우 해당 버킷의 설정을 계속 관리할 수 있지만, 더 이상 새로운 규정 준수 버킷을 생성할 수 없습니다. 자세한 내용은 "NetApp 기술 자료: StorageGRID 11.5에서 기존 규정 준수 버킷을 관리하는 방법"을 참조하십시오.

StorageGRID에서 S3 오브젝트 잠금 기본 보존 업데이트

버킷 생성 시 S3 객체 잠금을 활성화한 경우, 버킷을 편집하여 기본 보존 설정을 변경할 수 있습니다. 기본 보존을 활성화(또는 비활성화)하고 기본 보존 모드 및 보존 기간을 설정할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.
- StorageGRID 시스템에 대해 S3 객체 잠금이 전역적으로 활성화되어 있으며, 버킷을 생성할 때 S3 객체 잠금을 활성화했습니다. 을 참조하십시오. "S3 객체 잠금을 사용하여 객체 보존".

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
2. 표에서 버킷 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

3. 버킷 옵션 탭에서 **S3** 객체 잠금 아코디언을 선택합니다.
4. 선택적으로 이 버킷에 대해 *기본 보존*을 활성화 또는 비활성화할 수 있습니다.

   이 설정 변경 사항은 버킷에 이미 있는 객체나 자체 보존 기간이 있는 객체에는 적용되지 않습니다.

5. *기본 보존*이 활성화된 경우 버킷에 대한 *기본 보존 모드*를 지정하십시오.

기본 보존 모드	설명
거버넌스	• `s3:BypassGovernanceRetention` 권한이 있는 사용자는 `x-amz-bypass-governance-retention: true` 요청 헤더를 사용하여 보존 설정을 우회할 수 있습니다. • 이러한 사용자는 보존 기한이 도래하기 전에 개체 버전을 삭제할 수 있습니다. • 이러한 사용자는 개체의 보존 기간을 늘리거나 줄이거나 없앨 수 있습니다.
규정 준수	• 해당 객체는 지정된 보존 기간이 만료될 때까지 삭제할 수 없습니다. • 객체의 보존 기간은 늘릴 수는 있지만 줄일 수는 없습니다. • 해당 날짜에 도달할 때까지 객체의 보존 기한을 제거할 수 없습니다. 참고: 그리드 관리자가 규정 준수 모드 사용을 허용해야 합니다.

6. *기본 보존*이 활성화된 경우 버킷의 *기본 보존 기간*을 지정하십시오.

   *기본 보존 기간*은 이 버킷에 새로 추가된 객체를 수집 시점부터 보존할 기간을 나타냅니다. 그리드 관리자가 설정한 테넌트의 최대 보존 기간 이하의 값을 지정하십시오.

   최대 보존 기간은 1일에서 100년까지의 값으로 설정할 수 있으며, 그리드 관리자가 테넌트를 생성할 때 설정됩니다. 기본 보존 기간을 설정할 때는 최대 보존 기간에 설정된 값을 초과할 수 없습니다. 필요한 경우 그리드 관리자에게 최대 보존 기간을 늘리거나 줄이도록 요청하십시오.

7. *변경 사항 저장*을 선택합니다.

StorageGRID에서 S3 버킷에 대한 CORS 구성

S3 버킷과 해당 버킷의 객체가 다른 도메인의 웹 애플리케이션에서 액세스할 수 있도록 하려면 CORS(교차 출처 리소스 공유)를 구성할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- GET CORS 구성 요청의 경우, 귀하는 "모든 버킷 관리 또는 모든 버킷 보기 권한"이(가) 있는 사용자 그룹에 속해 있어야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.
- PUT CORS 구성 요청의 경우, "모든 버킷 권한 관리"이 있는 사용자 그룹에 속해 있어야 합니다. 이 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.
- "루트 액세스 권한"은(는) 모든 CORS 구성 요청에 대한 액세스를 제공합니다.

이 작업 정보

CORS(교차 출처 리소스 공유)는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, `Images`이라는 S3 버킷을 사용하여 그래픽을 저장한다고 가정해 보겠습니다. `Images` 버킷에 대해 CORS를 구성하면 해당 버킷의 이미지를 웹사이트 `http://www.example.com`에 표시할 수 있습니다.

버킷에 **CORS** 활성화

단계

1. 텍스트 편집기를 사용하여 필요한 XML을 생성합니다. 이 예시는 S3 버킷에 CORS를 활성화하는 데 사용되는 XML을 보여줍니다. 구체적으로 다음과 같습니다.
   - 모든 도메인이 버킷에 GET 요청을 보낼 수 있도록 허용합니다.
   - 해당 `http://www.example.com` 도메인은 GET, POST 및 DELETE 요청만 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 "Amazon Web Services(AWS) 문서: Amazon Simple Storage Service 사용자 가이드"을 참조하십시오.

2. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
3. 표에서 버킷 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

4. 버킷 액세스 탭에서 **CORS(**교차 출처 리소스 공유**)** 아코디언을 선택합니다.
5. **CORS** 활성화 확인란을 선택합니다.
6. CORS 구성 XML을 텍스트 상자에 붙여넣습니다.
7. *변경 사항 저장*을 선택합니다.

CORS 설정 수정

단계

1. 텍스트 상자에서 CORS 구성 XML을 업데이트하거나 *지우기*를 선택하여 처음부터 다시 시작하세요.
2. *변경 사항 저장*을 선택합니다.

CORS 설정 비활성화

단계

1. **CORS** 활성화 확인란의 선택을 해제합니다.
2. *변경 사항 저장*을 선택합니다.

관련 정보

"관리 인터페이스에 대한 StorageGRID CORS 구성"

StorageGRID S3 버킷에서 객체 삭제

테넌트 관리자를 사용하여 하나 이상의 버킷에 있는 객체를 삭제할 수 있습니다.

고려사항 및 요구사항

다음 단계를 수행하기 전에 다음 사항에 유의하십시오.

- 버킷에서 객체를 삭제하면 StorageGRID는 선택한 각 버킷의 모든 객체와 모든 객체 버전을 StorageGRID 시스템의 모든 노드 및 사이트에서 영구적으로 제거합니다. StorageGRID는 또한 관련 객체 메타데이터를 제거합니다. 이 정보는 복구할 수 없습니다.
- 버킷에 있는 모든 객체를 삭제하는 데는 객체 수, 객체 복사본 수, 동시 작업 수에 따라 몇 분, 며칠 또는 몇 주가 걸릴 수 있습니다.
- 버킷에 "S3 객체 잠금 활성화됨"이(가) 있으면 해당 버킷은 수년 동안 객체 삭제 중**:** 읽기 전용 상태로 유지될 수 있습니다.

  S3 Object Lock을 사용하는 버킷은 모든 객체의 보존 날짜가 도래하고 모든 법적 보류가 해제될 때까지 객체 삭제 중**:** 읽기 전용 상태를 유지합니다.

- 객체가 삭제되는 동안 버킷의 상태는 *객체 삭제 중: 읽기 전용*이 됩니다. 이 상태에서는 버킷에 새 객체를 추가할 수 없습니다.
- 모든 객체가 삭제되면 버킷은 읽기 전용 상태로 유지됩니다. 다음 중 하나를 수행할 수 있습니다.
  - 버킷을 쓰기 모드로 되돌리고 새 객체에 대해 재사용하십시오.
  - 버킷을 삭제합니다
  - 버킷의 이름을 향후 사용을 위해 예약하려면 읽기 전용 모드로 유지하십시오.
- 버킷에 객체 버전 관리가 활성화된 경우, StorageGRID 11.8 이상에서 생성된 삭제 마커는 버킷의 객체 삭제 작업을 사용하여 제거할 수 있습니다.
- 버킷에 객체 버전 관리가 활성화된 경우, 객체 삭제 작업은 StorageGRID 11.7 이하 버전에서 생성된 삭제 마커를 제거하지 않습니다. 버킷에서 객체를 삭제하는 방법에 대한 자세한 내용은 "S3 버전 관리 객체가 삭제되는 방법"을 참조하십시오.
- "교차 그리드 복제"를 사용하는 경우 다음 사항에 유의하십시오.
  - 이 옵션을 사용해도 다른 그리드의 버킷에서 객체가 삭제되지는 않습니다.
  - 소스 버킷에 대해 이 옵션을 선택하면 다른 그리드의 대상 버킷에 객체를 추가할 경우 그리드 간 복제 실패 경고가 발생합니다. 다른 그리드의 버킷에 아무도 객체를 추가하지 않도록 보장할 수 없는 경우, "그리드 간 복제 비활성화" 모든 버킷 객체를 삭제하기 전에 해당 버킷에 대해 이 옵션을 선택하십시오.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다. 이 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.

   버킷 페이지가 나타나고 기존의 모든 S3 버킷이 표시됩니다.

2. 작업 메뉴 또는 특정 버킷의 세부 정보 페이지를 사용합니다.

   작업 메뉴

   a. 객체를 삭제할 각 버킷에 대한 확인란을 선택하십시오.

   b. 작업 > *버킷에서 객체 삭제*를 선택합니다.

   상세 정보 페이지

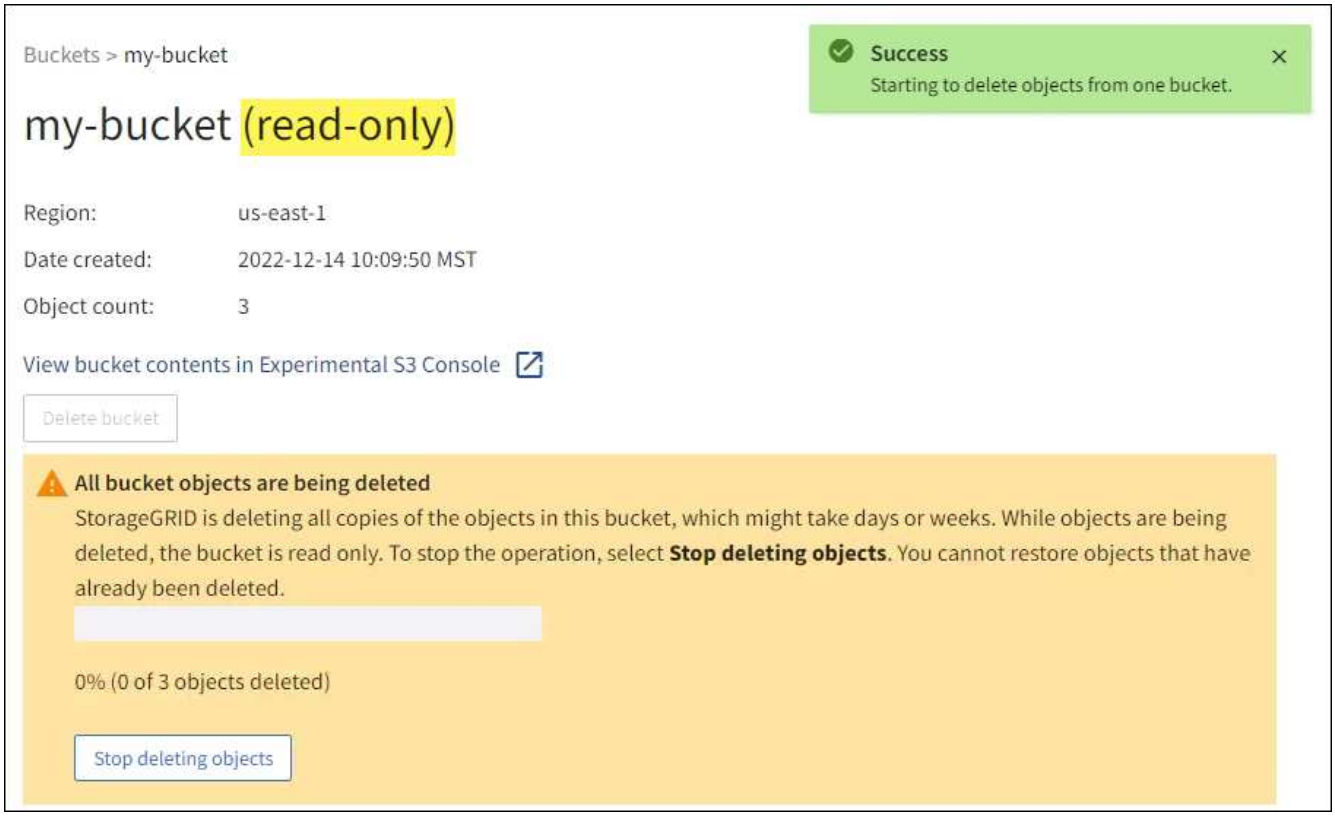
   a. 버킷 이름을 선택하여 세부 정보를 표시합니다.

   b. *버킷에서 객체 삭제*를 선택합니다.

3. 확인 대화 상자가 나타나면 세부 정보를 검토하고 *Yes*를 입력한 다음 *OK*를 선택하십시오.
4. 삭제 작업이 시작될 때까지 기다리십시오.

   몇 분 후:

   - 버킷 세부 정보 페이지에 노란색 상태 배너가 나타납니다. 진행률 표시줄은 삭제된 객체의 비율을 나타냅니다.
   - 버킷 세부 정보 페이지에서 버킷 이름 뒤에 *(읽기 전용)*이 표시됩니다.
   - 버킷 페이지에서 버킷 이름 옆에 *(객체 삭제: 읽기 전용)*이 표시됩니다.

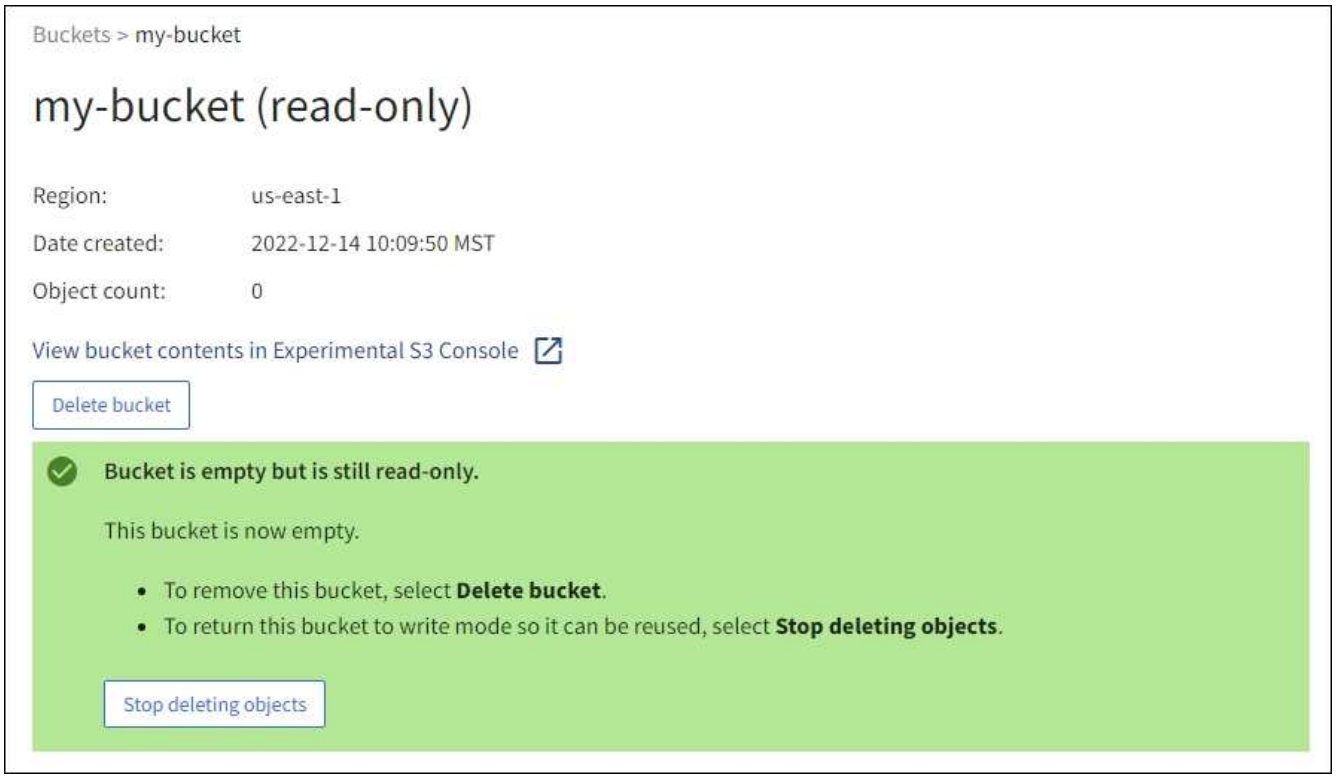


5. 작업 실행 중에 필요에 따라 *객체 삭제 중지*를 선택하여 프로세스를 중지할 수 있습니다. 그런 다음 선택적으로 *버킷에서 객체 삭제*를 선택하여 프로세스를 다시 시작할 수 있습니다.

   *객체 삭제 중지*를 선택하면 버킷이 쓰기 모드로 돌아가지만, 삭제된 객체에 액세스하거나 복원할 수는 없습니다.

6. 작업이 완료될 때까지 기다리세요.

   버킷이 비어 있으면 상태 배너가 업데이트되지만 버킷은 읽기 전용 상태로 유지됩니다.



7. 다음 중 하나를 수행하십시오.
   - 페이지를 종료하면 버킷이 읽기 전용 모드로 유지됩니다. 예를 들어, 나중에 사용할 버킷 이름을 예약하기 위해 빈 버킷을 읽기 전용 모드로 유지할 수 있습니다.
   - 버킷을 삭제합니다. 버킷 하나를 삭제하려면 버킷 삭제*를 선택하고, 여러 버킷을 삭제하려면 버킷 페이지로 돌아가서 *작업 > *버킷 삭제*를 선택합니다.

     모든 객체를 삭제한 후에도 버전 관리 버킷을 삭제할 수 없는 경우 삭제 마커가 남아 있을 수 있습니다. 버킷을 삭제하려면 남아 있는 모든 삭제 마커를 제거해야 합니다.

   - 버킷을 쓰기 모드로 되돌리고 필요에 따라 새 객체에 재사용할 수 있습니다. 단일 버킷에 대해 객체 삭제 중지*를 선택하거나, 버킷 페이지로 돌아가서 여러 버킷에 대해 *작업 > *객체 삭제 중지*를 선택할 수 있습니다.

StorageGRID S3 버킷 삭제

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

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.
- 삭제하려는 버킷이 비어 있습니다. 삭제하려는 버킷이 비어 있지 않은 경우, "버킷에서 객체를 삭제합니다".

이 작업 정보

이 지침에서는 테넌트 관리자를 사용하여 S3 버킷을 삭제하는 방법을 설명합니다. "테넌트 관리 API" 또는 "S3 REST API"를 사용하여 S3 버킷을 삭제할 수도 있습니다.

객체, 현재 버전이 아닌 객체 버전 또는 삭제 마커가 포함된 S3 버킷은 삭제할 수 없습니다. S3 버전 관리 객체 삭제 방법에 대한 자세한 내용은 "객체가 삭제되는 방법"을 참조하십시오.

단계

1. 대시보드에서 버킷 보기*를 선택하거나 *스토리지(S3) > *버킷*을 선택합니다.

   버킷 페이지가 나타나고 기존의 모든 S3 버킷이 표시됩니다.

2. 작업 메뉴 또는 특정 버킷의 세부 정보 페이지를 사용합니다.

   작업 메뉴

   a. 삭제하려는 각 버킷의 확인란을 선택합니다.

   b. 작업 > *버킷 삭제*를 선택합니다.

   상세 정보 페이지

   a. 버킷 이름을 선택하여 세부 정보를 표시합니다.

   b. *버킷 삭제*를 선택합니다.

3. 확인 대화 상자가 나타나면 *예*를 선택하십시오.

   StorageGRID는 각 버킷이 비어 있는지 확인한 후 각 버킷을 삭제합니다. 이 작업은 몇 분 정도 소요될 수 있습니다.

   버킷이 비어 있지 않으면 오류 메시지가 표시됩니다. 버킷을 삭제하려면 먼저 "버킷에 있는 모든 객체와 삭제 표시를 삭제합니다."해야 합니다.

StorageGRID에서 S3 콘솔 사용

S3 콘솔을 사용하여 S3 버킷의 객체를 보고 관리할 수 있습니다.

S3 콘솔을 사용하면 다음을 수행할 수 있습니다.

- 객체 업로드, 다운로드, 이름 변경, 복사, 이동 및 삭제
- 객체 버전 보기, 되돌리기, 다운로드 및 삭제
- 접두사로 객체 검색
- 객체 태그 관리
- 객체 메타데이터 보기
- 폴더를 보고, 만들고, 이름을 바꾸고, 복사하고, 이동하고, 삭제할 수 있습니다.

S3 Console은 가장 일반적인 경우에 대해 향상된 사용자 인터페이스 환경을 제공합니다. 모든 상황에서 CLI 또는 API 작업을 대체하도록 설계된 것은 아닙니다.

S3 콘솔을 사용하여 작업하는 데 시간이 너무 오래 걸리는 경우(예: 몇 분 또는 몇 시간) 다음 사항을 고려하십시오.

- 선택된 객체 수 줄이기
- 그래픽 방식이 아닌 (API 또는 CLI) 방법을 사용하여 데이터에 액세스

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 객체를 관리하려면 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 또는 S3 콘솔 탭 사용 권한과 모든 버킷 보기 권한 또는 모든 버킷 관리 권한 중 하나를 가진 사용자 그룹에 속해야 합니다. "테넌트 관리 권한"을 참조하십시오.
- 사용자에게 S3 그룹 또는 버킷 정책이 구성되었습니다. "버킷 및 그룹 액세스 정책 사용"을 참조하십시오.
- 사용자 액세스 키 ID와 비밀 액세스 키를 알고 있습니다. 선택적으로, `.csv` 이 정보가 포함된 파일이 있을 수도 있습니다. "액세스 키 생성 지침"을 참조하십시오.

단계

1. 스토리지 > 버킷 > *버킷 이름*을 선택합니다.
2. S3 콘솔 탭을 선택합니다.
3. 액세스 키 ID와 비밀 액세스 키를 해당 필드에 붙여넣으세요. 또는 *액세스 키 업로드*를 선택하고 사용자의 `.csv` 파일을 선택하세요.
4. *로그인*을 선택합니다.
5. 버킷 객체 목록이 표시됩니다. 필요에 따라 객체를 관리할 수 있습니다.

추가 정보

- 접두사로 검색: 접두사 검색 기능은 현재 폴더를 기준으로 특정 단어로 시작하는 개체만 검색합니다. 해당 단어가 다른 곳에 포함된 개체는 검색에서 제외됩니다. 이 규칙은 폴더 내의 개체에도 적용됩니다. 예를 들어, `folder1/folder2/somefile-`를 검색하면 `folder1/folder2/`폴더 내에 있고 `somefile-`단어로 시작하는 개체가 반환됩니다.
- 드래그 앤 드롭: 컴퓨터의 파일 관리자에서 S3 콘솔로 파일을 드래그 앤 드롭할 수 있습니다. 단, 폴더는 업로드할 수 없습니다.
- 폴더 작업: 폴더를 이동, 복사 또는 이름을 변경하면 폴더 안의 모든 개체가 하나씩 순차적으로 업데이트되므로 시간이 다소 걸릴 수 있습니다.
- 버킷 버전 관리가 비활성화된 경우 영구 삭제: 버전 관리가 비활성화된 버킷에서 객체를 덮어쓰거나 삭제하면 해당 작업은 영구적으로 적용됩니다. "버킷의 객체 버전 관리 변경"을 참조하십시오.

S3 플랫폼 서비스 관리

S3 플랫폼 서비스

StorageGRID용 플랫폼 서비스에 대해 알아보십시오

플랫폼 서비스를 구현하기 전에 해당 서비스 사용에 대한 개요 및 고려 사항을 검토하십시오.

S3에 대한 자세한 내용은 "S3 REST API 사용"을 참조하십시오.

플랫폼 서비스 개요

StorageGRID 플랫폼 서비스를 이용하면 이벤트 알림과 S3 객체 및 객체 메타데이터의 복사본을 외부 대상으로 전송할 수 있으므로 하이브리드 클라우드 전략을 구현하는 데 도움이 됩니다.

플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 환경 외부에 있기 때문에, 플랫폼 서비스를 통해 외부 스토리지 리소스, 알림 서비스, 데이터 검색 또는 분석 서비스를 활용하여 강력한 기능과 유연성을 확보할 수 있습니다.

하나의 S3 버킷에 대해 다양한 플랫폼 서비스를 조합하여 구성할 수 있습니다. 예를 들어, StorageGRID S3 버킷에서 "CloudMirror 서비스" 및 "알림"를 모두 구성하여 특정 객체를 Amazon Simple Storage Service(S3)에 미러링하는 동시에 각 객체에 대한 알림을 타사 모니터링 애플리케이션으로 전송하여 AWS 비용을 추적할 수 있습니다.

플랫폼 서비스 사용은 StorageGRID 관리자가 Grid Manager 또는 Grid Management API를 사용하여 각 테넌트 계정에 대해 활성화해야 합니다.

플랫폼 서비스 구성 방법

플랫폼 서비스는 "테넌트 관리자" 또는 "테넌트 관리 API"를 사용하여 구성한 외부 엔드포인트와 통신합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon SNS 토픽, 웹훅 엔드포인트 또는 로컬, AWS 또는 다른 곳에 호스팅된 Elasticsearch 클러스터와 같은 외부 대상을 나타냅니다.

외부 엔드포인트를 생성한 후 버킷에 XML 구성을 추가하여 버킷에 대한 플랫폼 서비스를 활성화할 수 있습니다. XML 구성은 버킷이 처리해야 할 객체, 버킷이 수행해야 할 작업, 그리고 서비스에 사용할 엔드포인트를 지정합니다.

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

- 키가 `/images`로 시작하는 모든 객체를 Amazon S3 버킷으로 복제하려면 소스 버킷에 복제 구성을 추가해야 합니다.
- 이러한 객체가 버킷에 저장될 때 알림을 보내려면 알림 구성을 추가해야 합니다.
- 이러한 객체의 메타데이터를 색인화하려면 검색 통합을 구현하는 데 사용되는 메타데이터 알림 구성을 추가해야 합니다.

구성 XML의 형식은 StorageGRID 플랫폼 서비스를 구현하는 데 사용되는 S3 REST API에 의해 결정됩니다.

플랫폼 서비스	**S3 REST API**	참조하십시오
CloudMirror 복제	• GetBucketReplication • PutBucketReplication	• "CloudMirror 복제" • "버킷에 대한 작업"
알림	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "알림" • "버킷에 대한 작업"

플랫폼 서비스	**S3 REST API**	참조하십시오
검색 통합	• GET 버킷 메타데이터 알림 구성 • PUT 버킷 메타데이터 알림 구성	• "검색 통합" • "StorageGRID 사용자 지정 작업"

플랫폼 서비스 사용 시 고려 사항

고려 사항	세부 정보
대상 엔드포인트 모니터링	각 대상 엔드포인트의 가용성을 모니터링해야 합니다. 대상 엔드포인트에 대한 연결이 장시간 끊어지고 요청이 대량으로 누적된 경우, StorageGRID에 대한 추가 클라이언트 요청(예: PUT 요청)이 실패할 수 있습니다. 엔드포인트에 다시 연결할 수 있게 되면 이러한 실패한 요청을 재시도해야 합니다.
대상 엔드포인트 스로틀링	StorageGRID 소프트웨어는 버킷으로 들어오는 S3 요청 속도가 대상 엔드포인트가 요청을 수신할 수 있는 속도를 초과하는 경우 해당 요청 속도를 제한할 수 있습니다. 속도 제한은 대상 엔드포인트로 전송될 요청이 누적되어 대기 중인 경우에만 발생합니다. 눈에 띄는 유일한 영향은 수신 S3 요청 실행 시간이 더 오래 걸린다는 것입니다. 성능 저하가 현저하게 감지되기 시작하면 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하면 클라이언트의 S3 작업(예: PUT 요청)이 결국 실패하게 됩니다. CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 더 큰 영향을 받을 가능성이 높습니다.
순서 보장	StorageGRID는 사이트 내 객체에 대한 작업 순서를 보장합니다. 객체에 대한 모든 작업이 동일한 사이트 내에서 이루어지는 한, 최종 객체 상태(복제용)는 항상 StorageGRID의 상태와 동일합니다. StorageGRID는 StorageGRID 사이트 간 작업 시 요청 순서를 최대한 정확하게 유지하려고 노력합니다. 예를 들어, 처음에 A 사이트에 객체를 기록한 후 나중에 B 사이트에서 동일한 객체를 덮어쓰는 경우, CloudMirror가 대상 버킷에 복제하는 최종 객체가 최신 객체라는 보장은 없습니다.
ILM 기반 객체 삭제	AWS CRR 및 Amazon Simple Notification Service의 삭제 동작과 일치하도록, StorageGRID ILM 규칙으로 인해 소스 버킷의 객체가 삭제될 경우 CloudMirror 및 이벤트 알림 요청이 전송되지 않습니다. 예를 들어, ILM 규칙에 따라 객체가 14일 후에 삭제되는 경우 CloudMirror 또는 이벤트 알림 요청이 전송되지 않습니다. 이와 대조적으로, ILM으로 인해 객체가 삭제될 때 검색 통합 요청이 전송됩니다.

고려 사항	세부 정보
Kafka 엔드포인트 사용	Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 따라서 Kafka 브로커 구성에서 `ssl.client.auth`을(를) `required`로 설정한 경우 Kafka 엔드포인트 구성 문제가 발생할 수 있습니다. Kafka 엔드포인트 인증에는 다음과 같은 인증 유형이 사용됩니다. 이러한 유형은 Amazon SNS와 같은 다른 엔드포인트 인증에 사용되는 유형과 다르며, 사용자 이름과 암호 자격 증명이 필요합니다. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 참고**:** 구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에는 적용되지 않습니다.

CloudMirror 복제 서비스 사용 시 고려 사항

고려 사항	세부 정보
복제 상태	StorageGRID는 `x-amz-replication-status` 헤더를 지원하지 않습니다.
객체 크기	CloudMirror 복제 서비스를 통해 대상 버킷으로 복제할 수 있는 객체의 최대 크기는 5TiB이며, 이는 지원되는 최대 객체 크기와 동일합니다. 참고: 단일 PutObject 작업의 최대 권장 크기는 5GiB(5,368,709,120바이트)입니다. 객체 크기가 5GiB보다 큰 경우 멀티파트 업로드를 사용하십시오.
버킷 버전 관리 및 버전 ID	StorageGRID의 소스 S3 버킷에 버전 관리가 활성화되어 있는 경우 대상 버킷에도 버전 관리를 활성화해야 합니다. 버전 관리를 사용할 때, S3 프로토콜의 제한 사항으로 인해 대상 버킷에서 객체 버전의 순서는 CloudMirror 서비스에서 보장되지 않고 최선을 다해 유지된다는 점에 유의하십시오. 참고: StorageGRID의 소스 버킷에 대한 버전 ID는 대상 버킷의 버전 ID와 관련이 없습니다.
객체 버전에 대한 태깅	CloudMirror 서비스는 S3 프로토콜의 제한 사항으로 인해 버전 ID를 제공하는 PutObjectTagging 또는 DeleteObjectTagging 요청을 복제하지 않습니다. 소스와 대상의 버전 ID가 서로 관련이 없기 때문에 특정 버전 ID에 대한 태그 업데이트가 복제되도록 보장할 방법이 없습니다. 반면, CloudMirror 서비스는 버전 ID를 지정하지 않는 PutObjectTagging 요청이나 DeleteObjectTagging 요청은 복제합니다. 이러한 요청은 최신 키(또는 버킷에 버전이 지정된 경우 최신 버전)에 대한 태그를 업데이트합니다. 태그가 포함된 일반적인 데이터 수집(태그 업데이트 제외)도 복제됩니다.

고려 사항	세부 정보
멀티파트 업로드 및 `ETag` 값	멀티파트 업로드를 사용하여 업로드된 객체를 미러링할 때 CloudMirror 서비스는 파트를 보존하지 않습니다. 따라서 미러링된 객체의 `ETag` 값은 원본 객체의 `ETag` 값과 다릅니다.
SSE-C로 암호화된 객체(고객이 제공한 키를 사용한 서버 측 암호화)	CloudMirror 서비스는 SSE-C로 암호화된 객체를 지원하지 않습니다. CloudMirror 복제를 위해 소스 버킷에 객체를 수집하려고 할 때 요청에 SSE-C 요청 헤더가 포함되어 있으면 작업이 실패합니다.
S3 객체 잠금이 활성화된 버킷	S3 객체 잠금이 활성화된 소스 또는 대상 버킷의 경우 복제가 지원되지 않습니다.

StorageGRID CloudMirror 복제 서비스에 대해 알아보세요

StorageGRID 버킷에 추가된 특정 객체를 하나 이상의 외부 대상 버킷으로 복제하도록 하려면 S3 버킷에 대해 CloudMirror 복제를 활성화할 수 있습니다.

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

CloudMirror 소스 버킷에 S3 객체 잠금이 활성화된 경우 CloudMirror 복제가 지원되지 않습니다.

CloudMirror 및 **ILM**

CloudMirror 복제는 그리드의 활성 ILM 정책과 독립적으로 작동합니다. CloudMirror 서비스는 객체가 소스 버킷에 저장되는 즉시 복제하여 가능한 한 빨리 대상 버킷으로 전달합니다. 복제된 객체의 전달은 객체 수집이 성공했을 때 시작됩니다.

CloudMirror 및 크로스그리드 복제

CloudMirror 복제는 크로스 그리드 복제 기능과 중요한 유사점과 차이점을 가지고 있습니다. 자세한 내용은 "크로스 그리드 복제와 CloudMirror 복제 비교"을 참조하십시오.

CloudMirror 및 **S3** 버킷

CloudMirror 복제는 일반적으로 외부 S3 버킷을 대상으로 구성됩니다. 하지만 다른 StorageGRID 배포 또는 S3 호환 서비스를 대상으로 복제를 구성할 수도 있습니다.

기존 버킷

CloudMirror 복제를 기존 버킷에 대해 활성화하면 해당 버킷에 새로 추가된 객체만 복제됩니다. 버킷에 이미 있는 객체는 복제되지 않습니다. 기존 객체를 강제로 복제하려면 객체 복사를 수행하여 기존 객체의 메타데이터를 업데이트하면 됩니다.

CloudMirror 복제를 사용하여 객체를 Amazon S3 대상으로 복사하는 경우, Amazon S3는 각 PUT 요청 헤더 내 사용자 정의 메타데이터의 크기를 2KB로 제한한다는 점에 유의하십시오. 객체의 사용자 정의 메타데이터가 2KB를 초과하는 경우 해당 객체는 복제되지 않습니다.

여러 대상 버킷

단일 버킷의 객체를 여러 대상 버킷으로 복제하려면 복제 구성 XML에서 각 규칙에 대한 대상을 지정해야 합니다. 객체를 동시에 두 개 이상의 버킷으로 복제할 수는 없습니다.

버전 관리 버킷 또는 버전 관리되지 않는 버킷

버전 관리되는 버킷 또는 버전 관리되지 않는 버킷에서 CloudMirror 복제를 구성할 수 있습니다. 대상 버킷은 버전 관리되는 버킷이거나 버전 관리되지 않는 버킷일 수 있습니다. 버전 관리되는 버킷과 버전 관리되지 않는 버킷의 어떠한 조합도 사용할 수 있습니다. 예를 들어, 버전 관리되지 않는 소스 버킷의 대상으로 버전 관리되는 버킷을 지정하거나 그 반대로 지정할 수 있습니다. 버전 관리되지 않는 버킷 간에 복제할 수도 있습니다.

삭제, 복제 루프 및 이벤트

삭제 동작

이는 Amazon S3 서비스의 교차 리전 복제(CRR)와 동일한 삭제 동작입니다. 소스 버킷에서 객체를 삭제해도 대상 버킷의 복제된 객체는 삭제되지 않습니다. 소스 및 대상 버킷 모두 버전 관리가 적용된 경우 삭제 마커가 복제됩니다. 대상 버킷에 버전 관리가 적용되지 않은 경우 소스 버킷에서 객체를 삭제해도 삭제 마커가 대상 버킷으로 복제되지 않으며 대상 객체도 삭제되지 않습니다.

복제 루프로부터의 보호

객체가 대상 버킷으로 복제될 때 StorageGRID는 해당 객체를 "복제본"으로 표시합니다. 대상 StorageGRID 버킷은 복제본으로 표시된 객체를 다시 복제하지 않으므로 의도치 않은 복제 루프를 방지할 수 있습니다. 이 복제본 표시는 StorageGRID 내부적으로 처리되며, Amazon S3 버킷을 대상으로 사용할 때 AWS CRR을 활용하는 데 영향을 미치지 않습니다.

> 복제본을 표시하는 데 사용되는 사용자 지정 헤더는 `x-ntap-sg-replica`입니다. 이 표시는 계단식 미러링을 방지합니다. StorageGRID는 두 그리드 간의 양방향 CloudMirror를 지원합니다.

대상 버킷의 이벤트

대상 버킷의 이벤트 고유성 및 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행되는 작업으로 인해 소스 객체의 동일한 복사본이 대상에 두 개 이상 전달될 수 있습니다. 드물지만, 동일한 객체가 두 개 이상의 StorageGRID 사이트에서 동시에 업데이트되는 경우 대상 버킷의 작업 순서가 소스 버킷의 이벤트 순서와 일치하지 않을 수 있습니다.

S3 버킷에 대한 **StorageGRID** 이벤트 알림에 대해 알아보십시오

StorageGRID가 지정된 이벤트에 대한 알림을 대상 Kafka 클러스터, 웹훅 엔드포인트 또는 Amazon Simple Notification Service로 전송하도록 하려면 S3 버킷에 대한 이벤트 알림을 활성화할 수 있습니다.

예를 들어, 버킷에 추가되는 각 객체에 대해 관리자에게 알림을 보내도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 관련된 로그 파일을 나타냅니다.

이벤트 알림은 알림 구성에 지정된 대로 소스 버킷에서 생성되어 대상으로 전달됩니다. 객체와 관련된 이벤트가 성공적으로 처리되면 해당 이벤트에 대한 알림이 생성되어 전달 대기열에 추가됩니다.

알림의 고유성과 순서는 보장되지 않습니다. 전달 성공을 보장하기 위해 수행되는 작업으로 인해 동일한 이벤트에 대한 알림이 대상에 두 개 이상 전달될 수 있습니다. 또한 전달이 비동기적으로 이루어지기 때문에, 특히 서로 다른 StorageGRID 사이트에서 시작된 작업의 경우, 대상에서의 알림 시간 순서가 소스 버킷의 이벤트 순서와 일치한다는 보장은 없습니다. Amazon S3 설명서에 설명된 대로 이벤트 메시지의 `sequencer` 키를 사용하여 특정 객체에 대한 이벤트 순서를 확인할 수 있습니다.

StorageGRID 이벤트 알림은 일부 제한 사항이 있지만 Amazon S3 API를 따릅니다.

- 지원되는 이벤트 유형은 다음과 같습니다.
  - s3:ObjectCreated:
  - s3:ObjectCreated:Put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:
  - s3:ObjectRemoved:Delete
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- StorageGRID에서 전송된 이벤트 알림은 표준 JSON 형식을 사용하지만, 아래 표와 같이 일부 키는 포함하지 않고 다른 키에는 특정 값을 사용합니다.

키 이름	**StorageGRID** 값
eventSource	`sgws:s3`
awsRegion	포함되지 않음
x-amz-id-2	포함되지 않음
arn	`urn:sgws:s3:::bucket_name`

StorageGRID 검색 통합 서비스에 대해 알아보십시오

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

검색 통합 서비스는 StorageGRID 의 사용자 지정 서비스로, 객체가 생성되거나 삭제될 때, 또는 메타데이터나 태그가 업데이트될 때마다 S3 객체 메타데이터를 대상 엔드포인트로 자동으로 비동기 전송합니다. 대상 서비스에서 제공하는 정교한 검색, 데이터 분석, 시각화 또는 머신러닝 도구를 사용하여 객체 데이터를 검색, 분석하고 유용한 정보를 얻을 수 있습니다.

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

S3 객체 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만, 객체의 S3 객체 잠금 메타데이터(보존 기한 및 법적 보존 상태 포함)는 Elasticsearch로 전송되는 메타데이터에 포함되지 않습니다.

> 검색 통합 서비스는 객체 메타데이터를 대상으로 전송하기 때문에 해당 구성 XML을 "메타데이터 알림 구성 XML"이라고 합니다. 이 구성 XML은 이벤트 알림을 활성화하는 데 사용되는 "알림 구성 XML"과는 다릅니다.

검색 통합 및 **S3** 버킷

버전 관리 여부와 관계없이 모든 버킷에 대해 검색 통합 서비스를 활성화할 수 있습니다. 검색 통합은 작업할 객체와 객체 메타데이터의 대상을 지정하는 메타데이터 알림 구성 XML을 버킷에 연결하여 구성합니다.

메타데이터 알림은 버킷 이름, 객체 이름, 그리고 버전 ID(있는 경우)로 구성된 JSON 문서 형식으로 생성됩니다. 각 메타데이터 알림에는 객체의 모든 태그 및 사용자 메타데이터 외에도 객체에 대한 표준 시스템 메타데이터 세트가 포함됩니다.

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

검색 알림

메타데이터 알림은 다음과 같은 경우에 생성되어 전송 대기열에 추가됩니다.

- 객체가 생성되었습니다.
- 객체가 삭제됩니다. 여기에는 그리드의 ILM 정책 작동으로 인해 객체가 삭제되는 경우도 포함됩니다.
- 객체 메타데이터 또는 태그가 추가, 업데이트 또는 삭제됩니다. 메타데이터 업데이트 시에는 변경된 값뿐만 아니라 전체 메타데이터 및 태그 세트가 항상 전송됩니다.

버킷에 메타데이터 알림 구성 XML을 추가하면 새로 생성하는 모든 객체와 데이터, 사용자 메타데이터 또는 태그를 업데이트하여 수정하는 모든 객체에 대해 알림이 전송됩니다. 그러나 버킷에 이미 있는 객체에 대해서는 알림이 전송되지 않습니다. 버킷에 있는 모든 객체의 객체 메타데이터가 대상으로 전송되도록 하려면 다음 중 하나를 수행해야 합니다.

- 버킷을 생성한 직후, 그리고 객체를 추가하기 전에 검색 통합 서비스를 구성하십시오.
- 버킷에 이미 있는 모든 객체에 대해 메타데이터 알림 메시지가 대상으로 전송되도록 하는 작업을 수행합니다.

검색 통합 서비스 및 **Elasticsearch**

StorageGRID 검색 통합 서비스는 Elasticsearch 클러스터를 대상으로 지원합니다. 다른 플랫폼 서비스와 마찬가지로, 대상은 서비스의 구성 XML에서 URN이 사용되는 엔드포인트에 지정됩니다. "NetApp 상호 운용성 매트릭스 도구"을 사용하여 지원되는 Elasticsearch 버전을 확인하십시오.

플랫폼 서비스 엔드포인트 관리

StorageGRID에서 플랫폼 서비스 엔드포인트 구성

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

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

플랫폼 서비스 엔드포인트란 무엇인가요?

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

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

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

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

CloudMirror 복제용 엔드포인트

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

알림 엔드포인트

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

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

검색 통합 서비스의 엔드포인트

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

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

관련 정보

"StorageGRID 관리"

StorageGRID 플랫폼 서비스 엔드포인트에 대한 **URN**을 지정하십시오

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

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

URN 요소

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

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

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

URN의 다음 요소는 다음과 같이 플랫폼 서비스 유형을 지정합니다.

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

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

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

웹훅 엔드포인트의 경우 대상 리소스는 대상 URI 자체입니다.

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

AWS 및 GCP에서 호스팅되는 서비스에 대한 URN

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

- CloudMirror 복제:

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

- 알림:

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

- 검색 통합:

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

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

로컬에서 호스팅되는 서비스에 대한 **URN**

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

- CloudMirror 복제:

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

StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 경우, 다음으로 시작하는 유효한 URN을 지정할 수 있습니다 `urn:sgws`:

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

- 알림:

Amazon Simple Notification Service 엔드포인트를 지정하십시오.

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

Kafka 엔드포인트를 지정합니다:

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

웹훅 엔드포인트를 지정합니다.

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

- 검색 통합:

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

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

StorageGRID 플랫폼 서비스 엔드포인트를 생성합니다.

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

시작하기 전에

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

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

  - 고유 리소스 이름(URN)

    "플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오."

  - 인증 자격 증명(필요한 경우):

검색 통합 엔드포인트

검색 통합 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

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

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

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

Amazon SNS 엔드포인트

Amazon SNS 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키

Kafka 엔드포인트

${post_edited_translations.segment}

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

◦ 보안 인증서(인증서 확인이 필요한 경우)

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

단계

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

   ${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

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

   포트를 지정하지 않으면 다음 기본 포트가 사용됩니다.

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

예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같을 수 있습니다.

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

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

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

마찬가지로 AWS에서 호스팅되는 버킷의 URI는 다음과 같을 수 있습니다.

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

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

5. 엔드포인트의 고유 리소스 이름(URN)을 입력하십시오.

> 엔드포인트가 생성된 후에는 해당 엔드포인트의 URN을 변경할 수 없습니다.

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

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

검색 통합 엔드포인트

검색 통합 엔드포인트에 대한 자격 증명을 입력하거나 업로드하십시오.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

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

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트에 대한 자격 증명을 입력하거나 업로드하세요.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

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

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

Amazon SNS 엔드포인트

Amazon SNS 엔드포인트에 대한 자격 증명을 입력하거나 업로드하십시오.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

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

Kafka 엔드포인트

Kafka 엔드포인트에 대한 자격 증명을 입력하거나 업로드합니다.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

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

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

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

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

대부분의 엔드포인트

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

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

웹훅 엔드포인트만 해당

웹훅 엔드포인트에 대한 TLS 연결을 확인하십시오.

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

${post_edited_translations.segment}

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

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

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

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

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

관련 정보

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

StorageGRID 플랫폼 서비스 엔드포인트의 연결을 테스트합니다

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

시작하기 전에

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

이 작업 정보

StorageGRID는 자격 증명에 올바른 권한이 있는지 검증하지 않습니다.

단계

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

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

2. 연결을 테스트할 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

3. *연결 테스트*를 선택합니다.

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

◦ 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하기 위해 엔드포인트를 수정해야 하는 경우, *구성*을 선택하고 정보를 업데이트합니다. 그런 다음 *테스트 및 변경 사항 저장*을 선택합니다.

StorageGRID에서 플랫폼 서비스 엔드포인트 편집

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

시작하기 전에

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

단계

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

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

2. 편집할 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

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

   엔드포인트가 생성된 후에는 해당 엔드포인트의 URN을 변경할 수 없습니다.

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

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

   d. 필요에 따라 인증서 확인 방법을 변경하십시오.
5. *테스트 후 변경 사항 저장*을 선택합니다.
   ◦ 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

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

StorageGRID 플랫폼 서비스 엔드포인트를 삭제합니다

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

시작하기 전에

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

단계

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

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

2. 삭제하려는 각 엔드포인트의 확인란을 선택합니다.

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

3. 작업 > *엔드포인트 삭제*를 선택합니다.

   확인 메시지가 나타납니다.

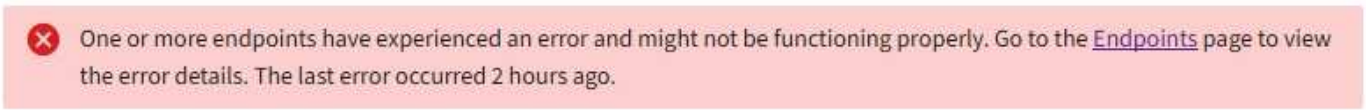
4. *엔드포인트 삭제*를 선택합니다.

StorageGRID 플랫폼 서비스 엔드포인트 오류 해결

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

오류가 발생했는지 확인합니다.

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



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

단계

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

오류가 여전히 유효한지 확인하십시오.

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

단계

1. 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

2. * 연결* > *연결 테스트*를 선택합니다.

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

엔드포인트 오류 해결

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

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

단계

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

${post_edited_translations.segment}

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

관련 정보

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

- "플랫폼 서비스 엔드포인트 편집"

StorageGRID에서 CloudMirror 복제 구성

버킷에 대한 CloudMirror 복제를 활성화하려면 유효한 버킷 복제 구성 XML을 생성하여 적용해야 합니다.

시작하기 전에

- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 이미 복제 소스 역할을 할 버킷을 생성했습니다.
- CloudMirror 복제 대상으로 사용하려는 엔드포인트가 이미 존재하며 해당 URN을 알고 있습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

CloudMirror 복제는 소스 버킷의 객체를 엔드포인트에 지정된 대상 버킷으로 복사합니다.

버킷 복제 및 구성 방법에 대한 일반 정보는 "Amazon Simple Storage Service (S3) 문서: 객체 복제"을 참조하십시오. StorageGRID가 GetBucketReplication, DeleteBucketReplication 및 PutBucketReplication을 구현하는 방법에 대한 자세한 내용은 "버킷에 대한 작업"을 참조하십시오.

> CloudMirror 복제는 크로스 그리드 복제 기능과 중요한 유사점과 차이점을 가지고 있습니다. 자세한 내용은 "크로스 그리드 복제와 CloudMirror 복제 비교"을 참조하십시오.

CloudMirror 복제를 구성할 때 다음 요구 사항 및 특징에 유의하십시오.

- 유효한 버킷 복제 구성 XML을 생성하고 적용할 때는 각 대상에 대해 S3 버킷 엔드포인트의 URN을 사용해야 합니다.
- S3 객체 잠금이 활성화된 소스 또는 대상 버킷의 경우 복제가 지원되지 않습니다.
- CloudMirror 복제를 객체가 포함된 버킷에서 활성화하면 버킷에 새로 추가된 객체는 복제되지만, 버킷에 이미 있는 객체는 복제되지 않습니다. 복제를 시작하려면 기존 객체를 업데이트해야 합니다.
- 복제 구성 XML에서 스토리지 클래스를 지정하면 StorageGRID는 대상 S3 엔드포인트에 대한 작업을 수행할 때 해당 클래스를 사용합니다. 대상 엔드포인트 또한 지정된 스토리지 클래스를 지원해야 합니다. 대상 시스템 공급업체에서 제공하는 권장 사항을 반드시 따르십시오.

단계

1. 원본 버킷에 대한 복제를 활성화합니다.
   - S3 복제 API에 명시된 대로 복제를 활성화하는 데 필요한 복제 구성 XML을 텍스트 편집기를 사용하여 생성합니다.
   - XML을 구성할 때:
     - StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 대한 `Filter`요소 사용을 지원하지 않으며, 객체 버전 삭제 시 V1 규칙을 따릅니다. 자세한 내용은 Amazon의 복제 구성 관련 문서를 참조하십시오.
     - 대상으로 S3 버킷 엔드포인트의 URN을 사용합니다.

- 선택적으로 `<StorageClass>` 요소를 추가하고 다음 중 하나를 지정하십시오.
  - `STANDARD`: 기본 스토리지 클래스입니다. 객체를 업로드할 때 스토리지 클래스를 지정하지 않으면 `STANDARD` 스토리지 클래스가 사용됩니다.
  - `STANDARD_IA`: (Standard - infrequent access.) 액세스 빈도는 낮지만 필요할 때 신속한 액세스가 필요한 데이터에 이 스토리지 클래스를 사용하십시오.
  - `REDUCED_REDUNDANCY`: 이 스토리지 클래스는 중요하지 않고 재현 가능한 데이터, 즉 `STANDARD` 스토리지 클래스보다 중복성을 줄여도 되는 데이터에 사용하십시오.
- 구성 XML에 `Role`을 지정하더라도 해당 값은 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. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.
4. 플랫폼 서비스 > *복제*를 선택합니다.
5. 복제 활성화 확인란을 선택하십시오.
6. 복제 구성 XML을 텍스트 상자에 붙여넣고 *변경 내용 저장*을 선택합니다.

   > 각 테넌트 계정에 대해 플랫폼 서비스를 활성화하려면 Grid Manager 또는 Grid Management API를 사용하는 StorageGRID 관리자가 필요합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 복제 구성이 올바르게 되어 있는지 확인하십시오.
   a. 복제 구성에 지정된 복제 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞서 보여드린 예시에서처럼 접두사 "2020"과 일치하는 객체가 복제됩니다.
   b. 객체가 대상 버킷에 복제되었는지 확인하십시오.

      작은 오브젝트의 경우 복제가 빠르게 이루어집니다.

관련 정보

"플랫폼 서비스 엔드포인트 생성"

StorageGRID에서 이벤트 알림을 구성합니다

버킷에 대한 알림을 활성화하려면 알림 구성 XML을 생성하고 Tenant Manager를 사용하여 해당 XML을 버킷에 적용하면 됩니다.

시작하기 전에

- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 이미 알림 소스로 사용할 버킷을 생성했습니다.
- 이벤트 알림 대상으로 사용하려는 엔드포인트가 이미 존재하며, 해당 URN을 알고 있습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

이벤트 알림은 알림 구성 XML을 소스 버킷과 연결하여 구성합니다. 알림 구성 XML은 버킷 알림 구성을 위한 S3 규칙을 따르며, 대상 Amazon SNS 토픽, Kafka 토픽 또는 웹훅 엔드포인트는 엔드포인트의 URN으로 지정됩니다.

이벤트 알림 및 구성 방법에 대한 일반 정보는 "Amazon 문서"을 참조하십시오. StorageGRID가 S3 버킷 알림 구성 API를 구현하는 방법에 대한 자세한 내용은 "S3 클라이언트 애플리케이션 구현 지침"을 참조하십시오.

버킷에 대한 이벤트 알림을 구성할 때 다음 요구 사항 및 특징을 참고하십시오.

- 유효한 알림 구성 XML을 생성하고 적용할 때는 각 대상에 대해 이벤트 알림 엔드포인트의 URN을 사용해야 합니다.
- S3 Object Lock이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만, 알림 메시지에는 객체의 S3 Object Lock 메타데이터(보존 기한 및 법적 보존 상태 포함)가 포함되지 않습니다.
- 이벤트 알림을 구성하면 소스 버킷의 객체에 대해 지정된 이벤트가 발생할 때마다 알림이 생성되어 대상으로 사용된 Amazon SNS 토픽, Kafka 토픽 또는 웹훅 엔드포인트로 전송됩니다.
- 객체가 포함된 버킷에 대해 이벤트 알림을 활성화하면 알림 구성이 저장된 후에 수행된 작업에 대해서만 알림이 전송됩니다.

단계

1. 소스 버킷에 대한 알림을 활성화합니다.
    - 텍스트 편집기를 사용하여 S3 알림 API에 명시된 대로 이벤트 알림을 활성화하는 데 필요한 알림 구성 XML을 생성합니다.
    - XML을 구성할 때 대상 토픽으로 이벤트 알림 엔드포인트의 URN을 사용하십시오.

```
<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 **STORAGE (S3)** > *Buckets*를 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

4. 플랫폼 서비스 > *이벤트 알림*을 선택합니다.
5. 이벤트 알림 활성화 확인란을 선택합니다.
6. 알림 구성 XML을 텍스트 상자에 붙여넣고 *변경 사항 저장*을 선택합니다.

   각 테넌트 계정에 대해 플랫폼 서비스를 활성화하려면 Grid Manager 또는 Grid Management API를 사용하는 StorageGRID 관리자가 필요합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 이벤트 알림이 올바르게 구성되었는지 확인하십시오.

   a. 구성 XML에 설정된 대로 알림을 트리거하기 위한 요구 사항을 충족하는 소스 버킷의 객체에 대해 작업을 수행합니다.

      예시에서는 `images/` 접두사가 붙은 객체가 생성될 때마다 이벤트 알림이 전송됩니다.

   b. 알림이 대상 Amazon SNS 토픽, Kafka 토픽 또는 웹훅 엔드포인트로 전달되었는지 확인하십시오.

      예를 들어, 대상 주제가 Amazon SNS에 호스팅되어 있는 경우, 알림이 전달될 때 이메일을 보내도록 서비스를 구성할 수 있습니다.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+ 대상 토픽에서 알림을 수신하면 StorageGRID 알림에 대한 소스 버킷 구성이 성공적으로 완료된 것입니다.

관련 정보

- "버킷에 대한 알림 이해"
- "S3 REST API 사용"
- "플랫폼 서비스 엔드포인트 생성"

StorageGRID에서 검색 통합 서비스 구성

버킷에 대한 검색 통합을 활성화하려면 검색 통합 XML을 생성하고 Tenant Manager를 사용하여 해당 XML을 버킷에 적용하면 됩니다.

시작하기 전에

- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 이미 S3 버킷을 생성했으며, 해당 버킷의 콘텐츠를 인덱싱하려고 합니다.
- 검색 통합 서비스의 대상으로 사용하려는 엔드포인트가 이미 존재하며, 해당 URN을 가지고 있습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

소스 버킷에 대한 검색 통합 서비스를 구성한 후 객체를 생성하거나 객체의 메타데이터 또는 태그를 업데이트하면 객체 메타데이터가 대상 엔드포인트로 전송됩니다.

이미 객체가 포함된 버킷에 대해 검색 통합 서비스를 활성화하면 기존 객체에 대한 메타데이터 알림이 자동으로 전송되지 않습니다. 대상 검색 인덱스에 메타데이터가 추가되도록 하려면 기존 객체를 업데이트해야 합니다.

단계

1. 버킷에 대한 검색 통합을 활성화합니다.

   - 메타데이터 검색 통합을 활성화하는 데 필요한 메타데이터 알림 XML을 생성하려면 텍스트 편집기를 사용하십시오.
   - XML을 구성할 때 대상으로는 검색 통합 엔드포인트의 URN을 사용하십시오.

     객체는 객체 이름의 접두사를 기준으로 필터링할 수 있습니다. 예를 들어, 접두사가 `images`인 객체의 메타데이터는 한 대상으로 보내고, 접두사가 `videos`인 객체의 메타데이터는 다른 대상으로 보낼 수 있습니다. 접두사가 중복되는 구성은 유효하지 않으며 제출 시 거부됩니다. 예를 들어, 접두사가 `test`인 객체에 대한 규칙 하나와 접두사가 `test2`인 객체에 대한 두 번째 규칙이 포함된 구성은 허용되지 않습니다.

     필요에 따라 메타데이터 구성 XML의 예시를 참조하십시오.

     ```
     <MetadataNotificationConfiguration>
      <Rule>
         <Status>Enabled</Status>
         <Prefix></Prefix>
         <Destination>
            <Urn>/Urn>
            </Destination>
      </Rule>
     </MetadataNotificationConfiguration>
     ```

     메타데이터 알림 구성 XML의 요소:

이름	설명	필수
MetadataNotificationConfiguration	메타데이터 알림의 객체와 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 Rule 요소를 포함합니다.	예
규칙	지정된 인덱스에 메타데이터를 추가해야 하는 객체를 식별하는 규칙에 대한 컨테이너 태그입니다. 접두사가 겹치는 규칙은 허용되지 않습니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID	규칙에 대한 고유 식별자입니다. 규칙 요소에 포함됩니다.	아니요
상태	상태는 '활성화됨' 또는 '비활성화됨'일 수 있습니다. 비활성화된 규칙에 대해서는 아무런 조치도 취해지지 않습니다. 규칙 요소에 포함됩니다.	예
접두사	접두사와 일치하는 객체는 해당 규칙의 영향을 받으며, 해당 객체의 메타데이터가 지정된 대상으로 전송됩니다. 모든 객체와 일치시키려면 빈 접두사를 지정하십시오. 규칙 요소에 포함됩니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. 규칙 요소에 포함됩니다.	예

이름	설명	필수
Urn	객체 메타데이터가 전송되는 대상의 URN입니다. 다음 속성을 가진 StorageGRID 엔드포인트의 URN이어야 합니다. • `es`세 번째 요소여야 합니다. • URN은 메타데이터가 저장된 인덱스와 유형으로 끝나야 하며, 형식은 `domain-name/myindex/mytype`입니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 사용합니다. • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 엔드포인트는 구성 XML을 제출하기 전에 구성되어야 합니다. 그렇지 않으면 구성이 실패하고 404 오류가 발생합니다. URN은 Destination 요소에 포함되어 있습니다.	예

2. 테넌트 관리자에서 **STORAGE (S3)** > *Buckets*를 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 검색 통합 * 을 선택합니다.
5. 검색 통합 활성화 확인란을 선택합니다.
6. 메타데이터 알림 구성을 텍스트 상자에 붙여넣고 *변경 사항 저장*을 선택합니다.

   각 테넌트 계정에 대한 플랫폼 서비스는 StorageGRID 관리자가 Grid Manager 또는 관리 API를 사용하여 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

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

      앞서 보여드린 예시에서처럼 버킷에 추가되는 모든 객체는 메타데이터 알림을 트리거합니다.

   b. 해당 객체의 메타데이터와 태그가 포함된 JSON 문서가 엔드포인트에 지정된 검색 인덱스에 추가되었는지 확인하십시오.

완료한 후

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

- **STORAGE (S3)** > **Buckets***를 선택하고 ***Enable search integration** 확인란을 선택 해제합니다.

- S3 API를 직접 사용하는 경우, DELETE Bucket 메타데이터 알림 요청을 사용하십시오. S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

예시: 모든 객체에 적용되는 메타데이터 알림 구성

이 예시에서는 모든 객체의 객체 메타데이터가 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>
```

예시: 두 개의 규칙이 포함된 메타데이터 알림 구성

이 예시에서는 접두사 `/images`와 일치하는 객체의 객체 메타데이터는 한 대상으로 전송되고, 접두사 `/videos`와 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>
```

메타데이터 알림 형식

버킷에 대한 검색 통합 서비스를 활성화하면 객체 메타데이터 또는 태그가 추가, 업데이트 또는 삭제될 때마다 JSON 문서가 생성되어 대상 엔드포인트로 전송됩니다.

이 예시는 키가 `SGWS/Tagging.txt`인 객체가 `test`라는 이름의 버킷에 생성될 때 생성될 수 있는 JSON의 예시를 보여줍니다. 해당 `test` 버킷은 버전 관리가 되지 않으므로 `versionId` 태그는 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"
  }
}
```

JSON 문서에 포함된 필드

문서 이름에는 버킷 이름, 객체 이름, 그리고 있는 경우 버전 ID가 포함됩니다.

버킷 및 객체 정보

`bucket`: 버킷 이름

`key`: 객체 키 이름

`versionID`: 버전 관리 버킷에 있는 객체의 객체 버전입니다.

`region`: 버킷 영역, 예를 들어 `us-east-1`

시스템 메타데이터

`size`: HTTP 클라이언트에 표시되는 객체 크기(바이트)

`md5`: 객체 해시

사용자 메타데이터

`metadata`: 객체에 대한 모든 사용자 메타데이터(키-값 쌍 형식)

`key:value`

태그

`tags`: 키-값 쌍으로 나타낸 객체에 대해 정의된 모든 객체 태그

```
key:value
```

Elasticsearch에서 결과를 보는 방법

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