테넌트 관리

StorageGRID software

NetApp
July 23, 2026

목차

테넌트 관리

StorageGRID의 테넌트 계정

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

Swift 관련 세부 정보는 이 버전의 문서 사이트에서 삭제되었습니다. 참조 "StorageGRID 11.8: 테넌트 관리".

그리드 관리자로서 S3 클라이언트가 객체를 저장하고 검색하는 데 사용하는 테넌트 계정을 생성하고 관리합니다.

각 테넌트 계정에는 연합 또는 로컬 그룹, 사용자, S3 버킷 및 객체가 있습니다.

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**:** 엔터프라이즈 애플리케이션에서 StorageGRID 시스템을 관리하는 경우, 조직 내 여러 부서별로 그리드의 객체 스토리지를 분리하고 싶을 수 있습니다. 이 경우 마케팅 부서, 고객 지원 부서, 인사 부서 등을 위한 테넌트 계정을 생성할 수 있습니다.

  S3 클라이언트 프로토콜을 사용하면 S3 버킷과 버킷 정책을 활용하여 기업 내 부서 간에 객체를 분리할 수 있습니다. 테넌트 계정을 사용할 필요가 없습니다. 자세한 내용은 "S3 버킷 및 버킷 정책" 구현 지침을 참조하십시오.

- 서비스 제공업체 사용 사례**:** StorageGRID 시스템을 서비스 제공업체로서 관리하는 경우, 그리드의 객체 스토리지를 그리드에서 스토리지를 임대할 여러 주체별로 분리할 수 있습니다. 이 경우, 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정을 생성하면 됩니다.

자세한 내용은 "테넌트 계정 사용"을 참조하십시오.

테넌트 계정은 어떻게 만드나요?

그리드 관리자를 사용하여 테넌트 계정을 생성합니다. 테넌트 계정을 생성할 때 다음 정보를 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, S3 테넌트 계정이 규제 요건을 준수해야 하는 경우 StorageGRID 시스템에 S3 객체 잠금 설정을 활성화할 수 있습니다. S3 객체 잠금이 활성화되면 모든 S3 테넌트 계정은 규제를 준수하는 버킷을 생성하고 관리할 수 있습니다.

Tenant Manager는 무엇에 사용되나요?

테넌트 계정을 생성한 후, 테넌트 사용자는 Tenant Manager에 로그인하여 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

S3 테넌트 사용자는 테넌트 관리자를 통해 S3 액세스 키와 버킷을 생성 및 관리할 수 있지만, 객체를 수집하고 관리하려면 S3 클라이언트 애플리케이션을 사용해야 합니다. 자세한 내용은 "S3 REST API 사용"을 참조하십시오.

StorageGRID 테넌트 계정을 생성합니다

StorageGRID 시스템의 스토리지에 대한 액세스를 제어하려면 최소 하나 이상의 테넌트 계정을 생성해야 합니다.

테넌트 계정을 생성하는 단계는 "ID 페더레이션" 및 "싱글 사인온" 구성 여부와 테넌트 계정을 생성하는 데 사용하는 Grid Manager 계정이 루트 액세스 권한이 있는 관리자 그룹에 속해 있는지 여부에 따라 다릅니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 당신은 "루트 액세스 또는 테넌트 계정 권한"을(를) 가지고 있습니다.
- 테넌트 계정이 Grid Manager에 대해 구성된 ID 소스를 사용하고, 페더레이션 그룹에 테넌트 계정에 대한 루트 액세스 권한을 부여하려는 경우, 해당 페더레이션 그룹을 Grid Manager로 가져온 것입니다. 이 관리자 그룹에 Grid Manager 권한을 할당할 필요는 없습니다. "관리자 그룹 관리"을 참조하십시오.
- S3 테넌트가 그리드 페더레이션 연결을 사용하여 계정 데이터를 복제하고 버킷 객체를 다른 그리드로 복제할 수 있도록 허용하려면 다음을 수행합니다.
  - "그리드 페더레이션 연결을 구성했습니다."이(가) 있습니다.
  - 연결 상태는 *연결됨*입니다.
  - 루트 액세스 권한이 있습니다.
  - 귀하는 "그리드 페더레이션에 허용된 테넌트 관리"에 대한 고려 사항을 검토하셨습니다.
  - 테넌트 계정이 Grid Manager에 대해 구성된 ID 소스를 사용하는 경우, 두 그리드 모두에서 동일한 페더레이션 그룹을 Grid Manager로 가져온 것입니다.

    테넌트를 생성할 때 소스 및 대상 테넌트 계정 모두에 대해 초기 루트 액세스 권한을 갖도록 이 그룹을 선택합니다.

    테넌트를 생성하기 전에 이 관리 그룹이 두 그리드 모두에 존재하지 않으면 테넌트가 대상으로 복제되지 않습니다.

마법사에 액세스합니다

단계

1. *테넌트*를 선택합니다.
2. *생성*을 선택합니다.

세부 정보를 입력합니다

단계

1. 테넌트에 대한 세부 정보를 입력합니다.

필드	설명
이름	테넌트 계정의 이름입니다. 테넌트 이름은 고유할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 20자리 계정 ID가 부여됩니다.
설명 (선택 사항)	테넌트를 식별하는 데 도움이 되는 설명입니다. 그리드 페더레이션 연결을 사용할 테넌트를 생성하는 경우, 선택적으로 이 필드를 사용하여 소스 테넌트와 대상 테넌트를 식별할 수 있습니다. 예를 들어, Grid 1에서 생성된 테넌트에 대한 다음 설명은 Grid 2로 복제된 테넌트에도 표시됩니다. "이 테넌트는 Grid 1에서 생성되었습니다."
클라이언트 유형	*S3*이어야 합니다.
스토리지 할당량(선택 사항)	이 테넌트에 스토리지 할당량을 설정하려면 할당량의 숫자 값과 단위를 입력하세요.

2. *Continue*를 선택합니다.

권한 선택

단계

1. 선택적으로, 이 테넌트에게 부여할 기본 권한을 선택합니다.

> 일부 권한에는 추가 요구 사항이 있습니다. 자세한 내용은 각 권한에 대한 도움말 아이콘을 선택하십시오.

권한	선택한 경우...
플랫폼 서비스 허용	테넌트는 CloudMirror와 같은 S3 플랫폼 서비스를 사용할 수 있습니다. 을(를) 참조하십시오."S3 테넌트 계정에 대한 플랫폼 서비스 관리"
자체 ID 소스 사용	테넌트는 페더레이션 그룹 및 사용자에 대한 자체 ID 소스를 구성하고 관리할 수 있습니다. StorageGRID 시스템에 대해 "구성된 SSO"한 경우 이 옵션은 비활성화됩니다.

권한	선택한 경우...
S3 Select 허용	테넌트는 S3 SelectObjectContent API 요청을 통해 객체 데이터를 필터링하고 검색할 수 있습니다. 을 참조하십시오."테넌트 계정에 대한 S3 Select 관리" 중요: SelectObjectContent 요청은 모든 S3 클라이언트와 모든 테넌트의 로드 밸런서 성능을 저하시킬 수 있습니다. 이 기능은 필요한 경우에만, 그리고 신뢰할 수 있는 테넌트에 대해서만 활성화하십시오.

2. 선택적으로, 이 테넌트에게 부여할 고급 권한을 선택합니다.

권한	선택한 경우...
그리드 페더레이션 연결	테넌트는 그리드 페더레이션 연결을 사용할 수 있으며, 이 연결은 다음과 같습니다. • 이 테넌트와 계정에 추가된 모든 테넌트 그룹 및 사용자가 이 그리드(소스 그리드)에서 선택한 연결의 다른 그리드(대상 그리드)로 복제됩니다. • 이 테넌트가 각 그리드의 해당 버킷 간에 그리드 간 복제를 구성할 수 있습니다. "그리드 페더레이션에 허용된 테넌트 관리"을 참조하십시오.
S3 Object Lock	테넌트가 S3 오브젝트 잠금의 특정 기능을 사용할 수 있도록 허용합니다. • *최대 보존 기간*은 이 버킷에 새로 추가된 객체를 수집 시점부터 얼마나 오랫동안 보존할지 정의합니다. • *규정 준수 모드 허용*은 보존 기간 동안 사용자가 보호된 오브젝트 버전을 덮어쓰거나 삭제하지 못하도록 합니다.

3. *Continue*를 선택합니다.

루트 액세스 정의 및 테넌트 생성

단계

1. StorageGRID 시스템에서 ID 페더레이션, 싱글 사인온(SSO) 또는 둘 다를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스 권한을 정의하십시오.

옵션	이렇게 하세요
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 테넌트에 대한 루트 액세스 권한을 부여할 기존 페더레이션 그룹을 선택합니다. b. 선택적으로, 로컬 루트 사용자로 테넌트에 로그인할 때 사용할 암호를 지정합니다.

옵션	이렇게 하세요
ID 페더레이션과 싱글 사인온(SSO)이 모두 활성화된 경우	테넌트에 대한 루트 액세스 권한을 부여할 기존 페더레이션 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

2. *테넌트 생성*을 선택합니다.

   성공 메시지가 표시되고 새 테넌트가 테넌트 페이지에 나열됩니다. 테넌트 세부 정보를 확인하고 테넌트 활동을 모니터링하는 방법에 대한 자세한 내용은 "테넌트 활동 모니터링"을 참조하십시오.

   > 테넌트 그리드 전체에 테넌트 설정을 적용하는 데에는 네트워크 연결 상태, 노드 상태 및 Cassandra 작업에 따라 15분 이상 소요될 수 있습니다.

3. 테넌트에 대해 * 그리드 페더레이션 연결 사용 * 권한을 선택한 경우:

   a. 연결된 다른 그리드에 동일한 테넌트가 복제되었는지 확인하십시오. 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다.

      > "클론 없이 테넌트가 생성되었습니다"라는 오류 메시지가 표시되면 "그리드 페더레이션 오류 해결"의 지침을 참조하십시오.

   b. 루트 액세스를 정의할 때 로컬 루트 사용자 암호를 제공한 경우, 복제된 테넌트에 대해 "로컬 루트 사용자의 암호 변경"합니다.

      > 루트 사용자 암호를 변경하기 전까지는 로컬 루트 사용자가 대상 그리드의 테넌트 관리자에 로그인할 수 없습니다.

테넌트에 로그인(선택 사항)

필요에 따라 지금 새 테넌트에 로그인하여 구성을 완료하거나 나중에 테넌트에 로그인할 수 있습니다. 로그인 단계는 기본 포트(443)를 사용하여 Grid Manager에 로그인했는지 또는 제한된 포트를 사용하여 로그인했는지에 따라 다릅니다. "외부 방화벽에서 액세스 제어"을 참조하십시오.

지금 로그인하세요

사용 중인 경우...	이렇게 하세요...
포트 443 및 로컬 루트 사용자에 대한 암호를 설정합니다	1. *루트로 로그인*을 선택합니다. 로그인하면 버킷, ID 페더레이션, 그룹 및 사용자 구성을 위한 링크가 표시됩니다. 2. 테넌트 계정을 구성하려면 링크를 선택하십시오. 각 링크를 클릭하면 테넌트 관리자의 해당 페이지가 열립니다. 페이지를 완료하려면 "테넌트 계정 사용 지침"을 참조하세요.

사용 중인 경우...	이렇게 하세요...
포트 443을 사용하고 있으며 로컬 루트 사용자의 암호를 설정하지 않은 경우	*로그인*을 선택하고 루트 액세스 페더레이션 그룹에 속한 사용자의 자격 증명을 입력하십시오.
제한된 포트	1. **Finish** 를 선택합니다 2. 테넌트 테이블에서 *제한됨*을 선택하여 해당 테넌트 계정에 액세스하는 방법에 대한 자세한 내용을 확인하십시오. 테넌트 관리자의 URL 형식은 다음과 같습니다. `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다. ◦ `*port*`은(는) 테넌트 전용 포트입니다. ◦ `*20-digit-account-id*`은(는) 테넌트의 고유 계정 ID입니다.

나중에 로그인

사용 중인 경우...	다음 중 하나를 수행하십시오...
포트 443	• 그리드 관리자에서 *테넌트*를 선택하고 테넌트 이름 오른쪽에 있는 *로그인*을 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다. ◦ `*20-digit-account-id*`은(는) 테넌트의 고유 계정 ID입니다.
제한된 포트	• 그리드 관리자에서 *테넌트*를 선택한 다음 *제한됨*을 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `*FQDN_or_Admin_Node_IP*`는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다. ◦ `*port*`는 테넌트 전용 제한 포트입니다. ◦ `*20-digit-account-id*`은(는) 테넌트의 고유 계정 ID입니다.

테넌트 구성

"테넌트 계정 사용"의 지침에 따라 테넌트 그룹 및 사용자, S3 액세스 키, 버킷, 플랫폼 서비스, 계정 복제 및 크로스 그리드 복제를 관리하십시오.

StorageGRID 테넌트 계정 편집

테넌트 계정을 편집하여 표시 이름, 스토리지 할당량 또는 테넌트 권한을 변경할 수 있습니다.

테넌트에게 그리드 페더레이션 연결 사용 권한이 있는 경우, 연결된 두 그리드 중 어느 쪽에서든 테넌트 세부 정보를 편집할 수 있습니다. 단, 한 그리드에서 변경한 내용은 다른 그리드에 복사되지 않습니다. 두 그리드의 테넌트 세부 정보를 정확히 동기화하려면 두 그리드에서 동일한 편집 작업을 수행해야 합니다. "그리드 페더레이션 연결에 허용된 테넌트 관리"을 참조하십시오.

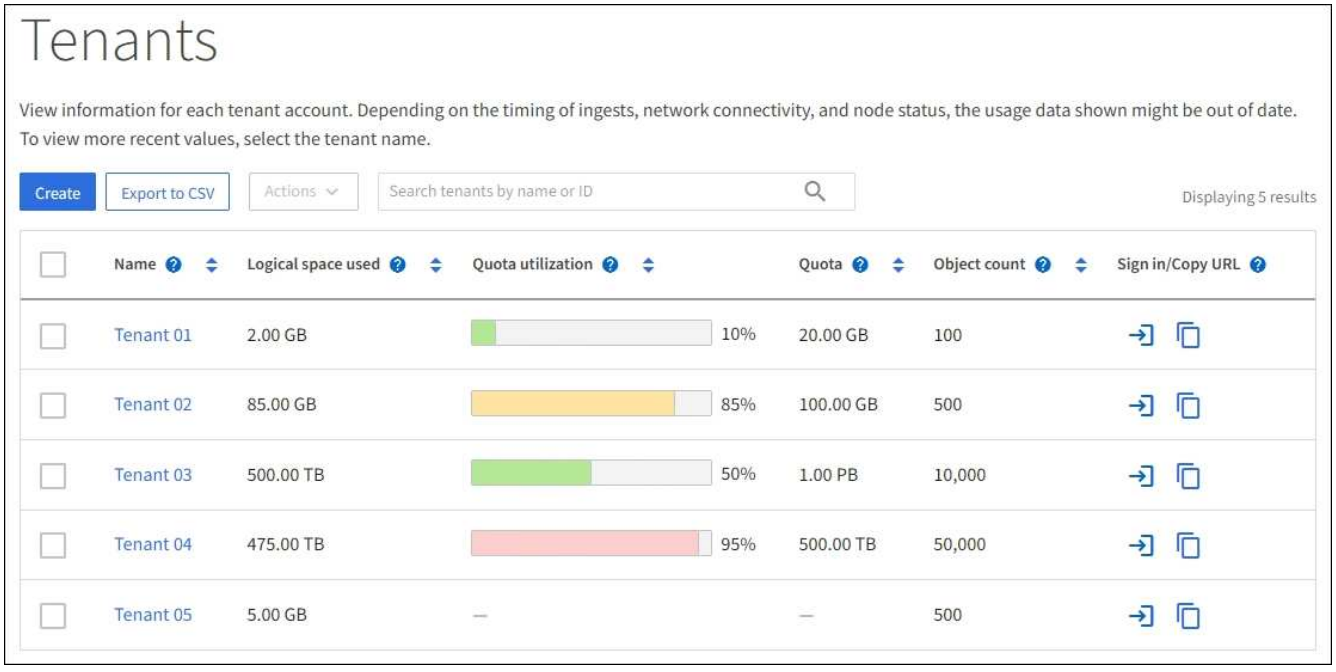
시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 당신은 "루트 액세스 또는 테넌트 계정 권한"을(를) 가지고 있습니다.

테넌트 그리드 전체에 테넌트 설정을 적용하는 데에는 네트워크 연결 상태, 노드 상태 및 Cassandra 작업에 따라 15분 이상 소요될 수 있습니다.

단계

1. *테넌트*를 선택합니다.



2. 수정하려는 테넌트 계정을 찾습니다.

   검색 상자를 사용하여 테넌트 이름 또는 테넌트 ID로 테넌트를 검색하세요.

3. 테넌트를 선택합니다. 다음 두 가지 방법 중 하나를 선택할 수 있습니다.

- 테넌트의 확인란을 선택하고 작업 > *편집*을 선택합니다.
- 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 *편집*을 선택합니다.

4. 필요에 따라 다음 필드의 값을 변경할 수 있습니다.
   - 이름
   - 설명
   - 스토리지 할당량
5. *Continue*를 선택합니다.
6. 테넌트 계정에 대한 권한을 선택하거나 해제합니다.
   - 이미 플랫폼 서비스를 사용 중인 테넌트에 대해 해당 서비스를 비활성화하면 테넌트가 S3 버킷에 대해 구성한 서비스가 작동을 멈춥니다. 테넌트에게 오류 메시지가 전송되지 않습니다. 예를 들어, 테넌트가 S3 버킷에 대해 CloudMirror 복제를 구성한 경우, 해당 버킷에 객체를 계속 저장할 수는 있지만, 엔드포인트로 구성한 외부 S3 버킷에는 더 이상 해당 객체의 복사본이 생성되지 않습니다. "S3 테넌트 계정에 대한 플랫폼 서비스 관리"을 참조하십시오.
   - 테넌트 계정이 자체 ID 소스를 사용할지 아니면 Grid Manager에 구성된 ID 소스를 사용할지 결정하려면 자체 **ID** 소스 사용 설정을 변경하십시오.

     *자체 신원 정보 출처 사용*이 다음과 같은 경우:

     - 비활성화 및 선택된 경우, 테넌트가 이미 자체 ID 소스를 활성화한 것입니다. 테넌트는 Grid Manager에 구성된 ID 소스를 사용하기 전에 먼저 자체 ID 소스를 비활성화해야 합니다.
     - 비활성화되어 선택되지 않은 경우, StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.
   - 필요에 따라 **S3 Select** 허용 권한을 선택하거나 해제하십시오. 을 참조하십시오."테넌트 계정에 대한 S3 Select 관리"
   - 그리드 페더레이션 연결 사용 권한을 제거하려면:
     i. **Grid federation** 탭을 선택합니다.
     ii. *권한 제거*를 선택합니다.
   - 그리드 페더레이션 연결 사용 권한을 추가하려면:
     i. **Grid federation** 탭을 선택합니다.
     ii. 그리드 페더레이션 연결 사용 확인란을 선택하십시오.
     iii. 선택적으로 *기존 로컬 사용자 및 그룹 복제*를 선택하여 원격 그리드로 복제할 수 있습니다. 원하는 경우, 진행 중인 복제를 중지하거나 마지막 복제 작업 완료 후 일부 로컬 사용자 또는 그룹이 복제되지 않은 경우 복제를 다시 시도할 수 있습니다.
   - 최대 보존 기간을 설정하거나 규정 준수 모드를 허용하려면:

     ⓘ 이 설정을 사용하려면 먼저 그리드에서 S3 객체 잠금 기능을 활성화해야 합니다.

     i. **S3** 객체 잠금 탭을 선택합니다.
     ii. 최대 보존 기간 설정의 경우 값을 입력하고 드롭다운에서 기간을 선택합니다.
     iii. *규정 준수 모드 허용*의 경우 확인란을 선택하십시오.

StorageGRID 테넌트의 로컬 루트 사용자 암호 변경

루트 사용자가 계정에서 잠긴 경우 테넌트의 로컬 루트 사용자의 암호를 변경해야 할 수 있습니다.

시작하기 전에

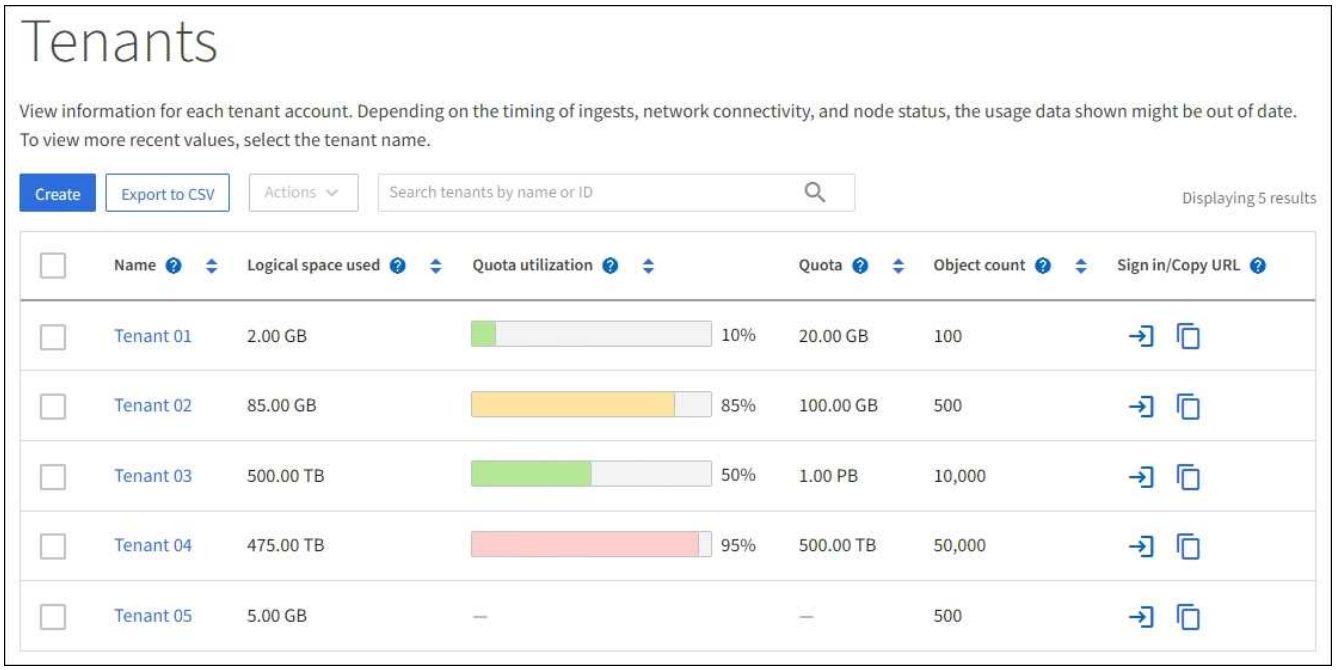
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

이 작업 정보

StorageGRID 시스템에서 SSO(싱글 사인온)가 활성화된 경우 로컬 루트 사용자는 테넌트 계정에 로그인할 수 없습니다. 루트 사용자 작업을 수행하려면 사용자가 테넌트에 대한 루트 액세스 권한이 있는 페더레이션 그룹에 속해 있어야 합니다.

단계

1. *테넌트*를 선택합니다.



2. 테넌트 계정을 선택합니다. 다음 중 하나를 수행할 수 있습니다.
   - 테넌트의 확인란을 선택하고 작업 > *루트 암호 변경*을 선택합니다.
   - 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 작업 > *루트 암호 변경*을 선택합니다.
3. 테넌트 계정의 새 비밀번호를 입력하십시오.
4. *저장*을 선택하세요.

StorageGRID 테넌트 계정 삭제

테넌트의 시스템 액세스 권한을 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 테넌트 계정과 연결된 모든 S3 버킷 및 객체를 제거했습니다.
- 테넌트가 그리드 페더레이션 연결을 사용할 수 있도록 허용된 경우, "그리드 페더레이션 연결 사용 권한이 있는 테넌트 삭제"에 대한 고려 사항을 검토했습니다.

단계

1. *테넌트*를 선택합니다.
2. 삭제하려는 테넌트 계정을 찾습니다.

   검색 상자를 사용하여 테넌트 이름 또는 테넌트 ID로 테넌트를 검색하세요.

3. 여러 테넌트를 삭제하려면 확인란을 선택한 다음 작업 > *삭제*를 선택하십시오.
4. 단일 테넌트를 삭제하려면 다음 중 하나를 수행하십시오.
   - 확인란을 선택한 다음 작업 > *삭제*를 선택합니다.
   - 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 작업 > *삭제*를 선택합니다.
5. *예*를 선택합니다.

플랫폼 서비스 관리

StorageGRID 플랫폼 서비스에 대해 알아보십시오

플랫폼 서비스에는 CloudMirror 복제, 이벤트 알림 및 검색 통합 서비스가 포함됩니다.

S3 테넌트 계정에 플랫폼 서비스를 활성화하는 경우, 테넌트가 이러한 서비스를 사용하는 데 필요한 외부 리소스에 액세스할 수 있도록 그리드를 구성해야 합니다.

플랫폼 서비스는 "브랜치 버킷"에 대해 지원되지 않습니다.

CloudMirror 복제

StorageGRID CloudMirror 복제 서비스는 StorageGRID 버킷의 특정 객체를 지정된 외부 대상으로 미러링하는 데 사용됩니다.

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

CloudMirror 복제는 크로스 그리드 복제 기능과 몇 가지 중요한 유사점과 차이점이 있습니다. 자세한 내용은 "크로스 그리드 복제와 CloudMirror 복제 비교"을 참조하세요.

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

알림

버킷별 이벤트 알림은 객체에 대해 수행된 특정 작업에 대한 알림을 지정된 외부 Kafka 클러스터, 웹훅 엔드포인트 또는 Amazon Simple Notification Service로 전송하는 데 사용됩니다.

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

> S3 객체 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만, 알림 메시지에는 객체의 S3 객체 잠금 메타데이터(보존 기한 및 법적 보존 상태 포함)가 포함되지 않습니다.

검색 통합 서비스

검색 통합 서비스는 S3 객체 메타데이터를 지정된 Elasticsearch 인덱스로 전송하는 데 사용되며, 외부 서비스를 통해 해당 메타데이터를 검색하거나 분석할 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 Object Lock이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만, 객체의 S3 Object Lock 메타데이터(보존 기한 및 법적 보존 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스를 통해 테넌트는 외부 스토리지 리소스, 알림 서비스, 검색 또는 분석 서비스를 자신의 데이터와 함께 사용할 수 있습니다. 플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 환경 외부에 있으므로 테넌트가 이러한 서비스를 사용할 수 있도록 허용할지 여부를 결정해야 합니다. 허용하기로 결정했다면 테넌트 계정을 생성하거나 편집할 때 플랫폼 서비스 사용을 활성화해야 합니다. 또한 테넌트가 생성하는 플랫폼 서비스 메시지가 목적지에 도달할 수 있도록 네트워크를 구성해야 합니다.

플랫폼 서비스 이용 관련 권장 사항

플랫폼 서비스를 이용하기 전에 다음 권장 사항을 숙지하십시오.

- StorageGRID 시스템의 S3 버킷에 버전 관리와 CloudMirror 복제가 모두 활성화된 경우, 대상 엔드포인트에 대해서도 S3 버킷 버전 관리를 활성화해야 합니다. 이렇게 하면 CloudMirror 복제를 통해 엔드포인트에 동일한 객체 버전이 생성됩니다.
- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청에 대해 활성 테넌트를 100개 이상 사용하지 않는 것이 좋습니다. 활성 테넌트가 100개를 초과하면 S3 클라이언트 성능이 저하될 수 있습니다.
- 완료할 수 없는 엔드포인트에 대한 요청은 최대 50만 건까지 대기열에 저장됩니다. 이 제한은 활성 테넌트 간에 균등하게 분배됩니다. 신규 테넌트는 일시적으로 이 50만 건 제한을 초과할 수 있으며, 이를 통해 새로 생성된 테넌트가 불공평하게 불이익을 받지 않도록 합니다.

관련 정보

- "플랫폼 서비스 관리"
- "스토리지 프록시 설정 구성"
- "StorageGRID 모니터링"

StorageGRID 플랫폼 서비스용 네트워크 및 포트

S3 테넌트 플랫폼 서비스를 사용하도록 허용하는 경우, 플랫폼 서비스 메시지가 목적지로 전달될 수 있도록 그리드에 대한 네트워킹을 구성해야 합니다.

S3 테넌트 계정을 생성하거나 업데이트할 때 플랫폼 서비스를 활성화할 수 있습니다. 플랫폼 서비스가 활성화되면 테넌트는 S3 버킷에서 CloudMirror 복제, 이벤트 알림 또는 검색 통합 메시지를 수신할 대상 엔드포인트를 생성할 수 있습니다. 이러한 플랫폼 서비스 메시지는 ADC 서비스를 실행하는 스토리지 노드에서 대상 엔드포인트로 전송됩니다.

예를 들어, 테넌트는 다음과 같은 유형의 대상 엔드포인트를 구성할 수 있습니다.

- 로컬에서 호스팅되는 Elasticsearch 클러스터
- Amazon Simple Notification Service 메시지 수신을 지원하는 로컬 애플리케이션
- 로컬에서 호스팅되는 Kafka 클러스터
- HTTP POST 알림 요청을 지원하는 외부 또는 로컬 호스팅 웹훅 엔드포인트.

  이 엔드포인트는 Fluentd와 같은 다양한 웹 서버, 프레임워크 또는 데이터 처리 도구에서 호스팅될 수 있습니다.

- 동일하거나 다른 StorageGRID 인스턴스에 로컬로 호스팅된 S3 버킷
- Amazon Web Services의 엔드포인트와 같은 외부 엔드포인트.

플랫폼 서비스 메시지가 정상적으로 전달되도록 하려면 ADC 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 대상 엔드포인트로 플랫폼 서비스 메시지를 전송하는 데 다음 포트를 사용할 수 있도록 설정해야 합니다.

기본적으로 플랫폼 서비스 메시지는 다음 포트를 통해 전송됩니다.

- **80**: http로 시작하는 엔드포인트 URI(대부분의 엔드포인트)의 경우
- **443**: https로 시작하는 엔드포인트 URI의 경우(대부분의 엔드포인트)
- **9092**: http 또는 https로 시작하는 엔드포인트 URI의 경우(Kafka 엔드포인트만 해당)

테넌트는 엔드포인트를 생성하거나 편집할 때 다른 포트를 지정할 수 있습니다.

> StorageGRID 배포를 CloudMirror 복제 대상으로 사용하는 경우, 복제 메시지가 80번 또는 443번 포트 이외의 포트로 수신될 수 있습니다. 대상 StorageGRID 배포에서 S3에 사용하는 포트가 엔드포인트에 지정되어 있는지 확인하십시오.

투명하지 않은 프록시 서버를 사용하는 경우 인터넷상의 엔드포인트와 같은 외부 엔드포인트로 메시지를 보낼 수 있도록 "스토리지 프록시 설정 구성"도 해야 합니다.

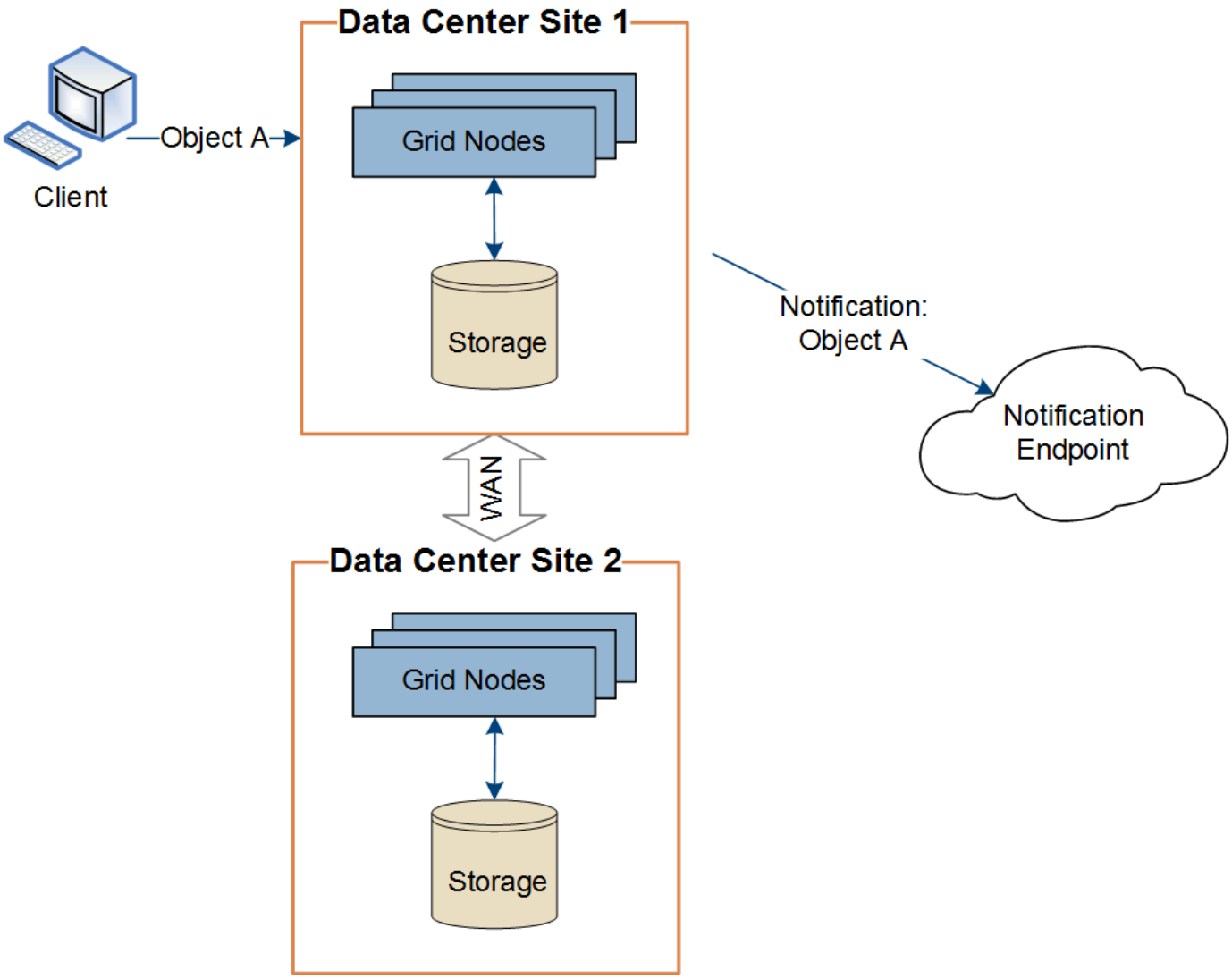
관련 정보

"테넌트 계정 사용"

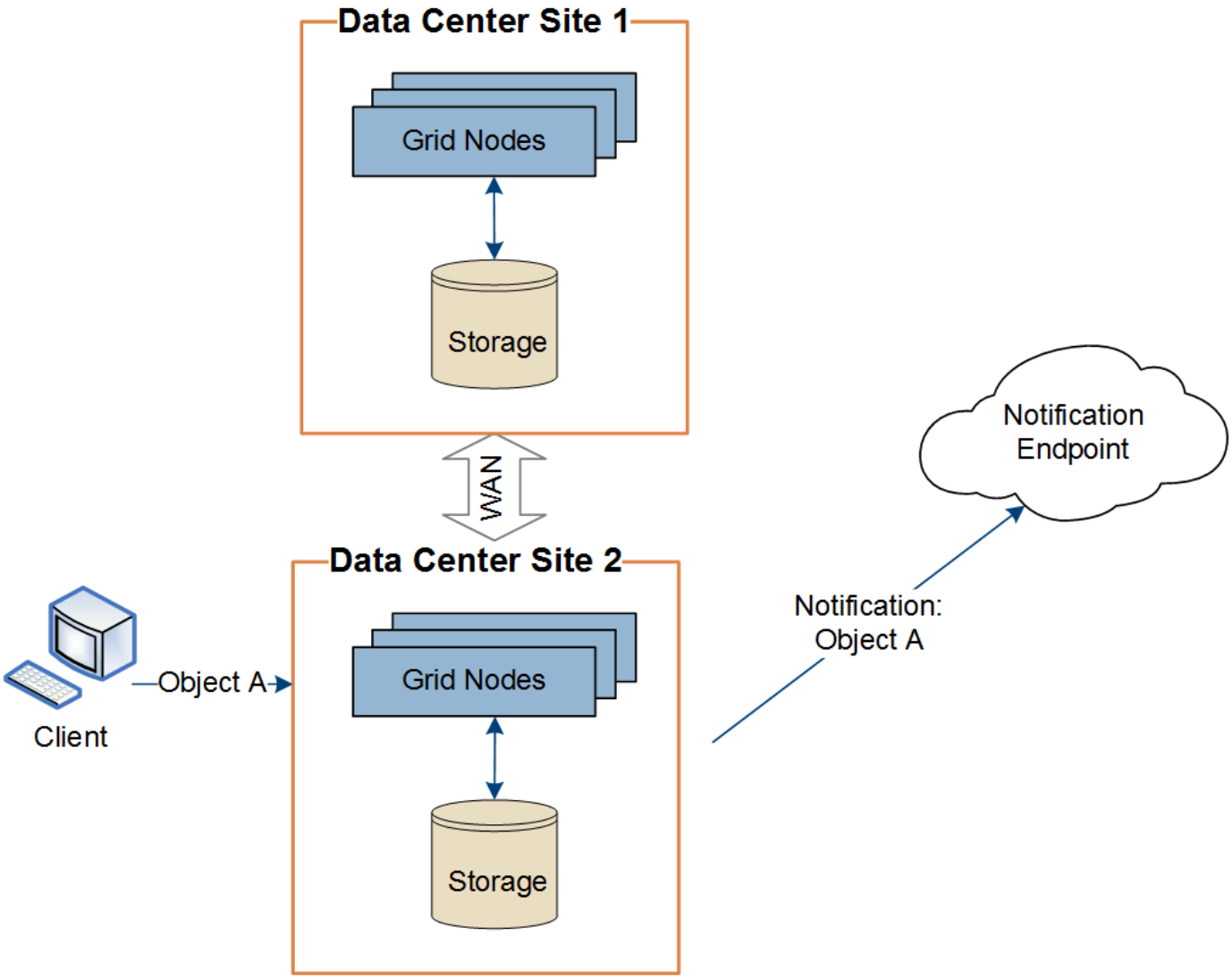
StorageGRID 플랫폼 서비스 메시지의 사이트별 전달

모든 플랫폼 서비스 운영은 사이트별로 수행됩니다.

즉, 테넌트가 클라이언트를 사용하여 데이터 센터 사이트 1의 게이트웨이 노드에 연결하여 객체에 대한 S3 API 생성 작업을 수행하면 해당 작업에 대한 알림이 트리거되어 데이터 센터 사이트 1에서 전송됩니다.



클라이언트가 이후 데이터 센터 사이트 2에서 동일한 객체에 대해 S3 API 삭제 작업을 수행하면 삭제 작업에 대한 알림이 트리거되어 데이터 센터 사이트 2에서 전송됩니다.



각 사이트의 네트워크가 플랫폼 서비스 메시지를 목적지로 전달할 수 있도록 구성되어 있는지 확인하십시오.

StorageGRID 플랫폼 서비스 문제 해결

플랫폼 서비스에서 사용되는 엔드포인트는 테넌트 사용자가 테넌트 관리자에서 생성하고 관리합니다. 하지만 테넌트 플랫폼 서비스 구성 또는 사용에 문제가 있는 경우, 그리드 관리자를 사용하여 문제를 해결할 수 있습니다.

새로운 엔드포인트 관련 문제

테넌트가 플랫폼 서비스를 사용하려면 먼저 테넌트 관리자를 통해 하나 이상의 엔드포인트를 생성해야 합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon Simple Notification Service 토픽, Kafka 토픽 또는 로컬이나 AWS에서 호스팅되는 Elasticsearch 클러스터와 같은 플랫폼 서비스의 외부 대상을 나타냅니다. 각 엔드포인트에는 외부 리소스의 위치와 해당 리소스에 액세스하는 데 필요한 자격 증명이 모두 포함됩니다.

테넌트가 엔드포인트를 생성하면 StorageGRID 시스템은 해당 엔드포인트가 존재하는지, 그리고 지정된 자격 증명을 사용하여 접근할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

엔드포인트 유효성 검사에 실패하면 실패 사유를 설명하는 오류 메시지가 표시됩니다. 테넌트 사용자는 문제를 해결한

후 엔드포인트를 다시 생성해야 합니다.

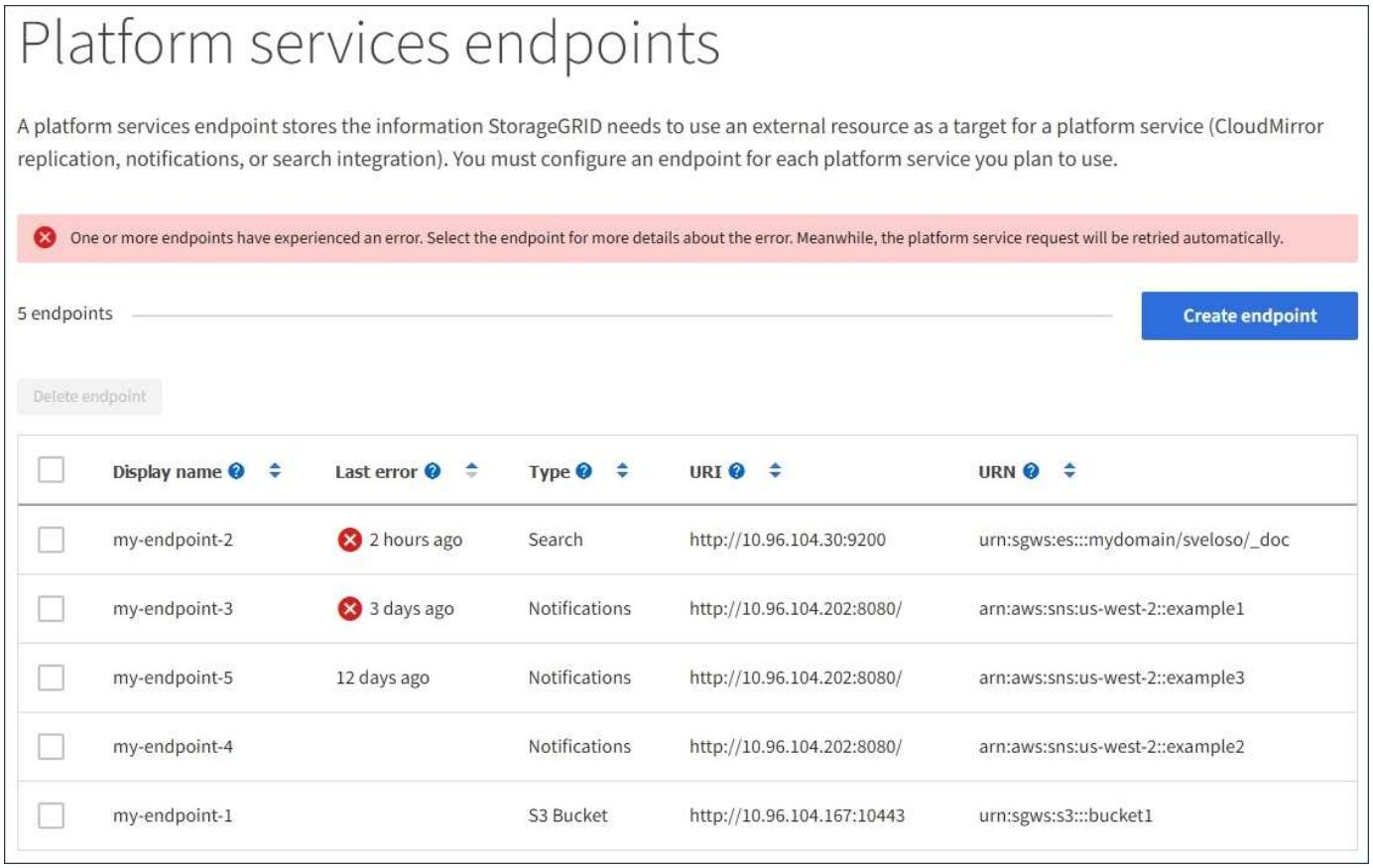
테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트 관련 문제

StorageGRID가 기존 엔드포인트에 연결을 시도하는 동안 오류가 발생하면 테넌트 관리자의 대시보드에 메시지가 표시됩니다.

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

테넌트 사용자는 엔드포인트 페이지에서 각 엔드포인트에 대한 최근 오류 메시지를 확인하고 오류 발생 시점을 파악할 수 있습니다. 마지막 오류 열에는 각 엔드포인트의 최근 오류 메시지와 오류 발생 시점이 표시됩니다. ⊗ 아이콘이 포함된 오류는 지난 7일 이내에 발생한 오류입니다.



마지막 오류 열의 일부 오류 메시지에는 괄호 안에 logID가 포함될 수 있습니다. 그리드 관리자 또는 기술 지원 담당자는 이 ID를 사용하여 bycast.log에서 오류에 대한 자세한 정보를 찾을 수 있습니다.

프록시 서버 관련 문제

스토리지 노드와 플랫폼 서비스 엔드포인트 간에 "스토리지 프록시"를 구성한 경우, 프록시 서비스에서 StorageGRID의 메시지를 허용하지 않으면 오류가 발생할 수 있습니다. 이러한 문제를 해결하려면 프록시 서버의 설정을 확인하여 플랫폼 서비스 관련 메시지가 차단되지 않도록 하십시오.

오류가 발생했는지 확인합니다.

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

클라이언트 작업이 실패합니다.

일부 플랫폼 서비스 문제로 인해 S3 버킷에 대한 클라이언트 작업이 실패할 수 있습니다. 예를 들어, 내부 복제 상태 머신(RSM) 서비스가 중지되거나 전송 대기 중인 플랫폼 서비스 메시지가 너무 많으면 S3 클라이언트 작업이 실패합니다.

서비스 상태를 확인하려면:

1. 노드 > 사이트 > 스토리지 노드 > 개요 를 선택합니다.
2. 알림 테이블에서 활성화된 알림을 확인하십시오.
3. 활성화된 경고를 모두 해결하십시오. 필요한 경우 기술 지원에 문의하십시오.

복구 가능한 엔드포인트 오류 및 복구 불가능한 엔드포인트 오류

엔드포인트가 생성된 후 플랫폼 서비스 요청 오류는 다양한 이유로 발생할 수 있습니다. 일부 오류는 사용자 개입을 통해 복구할 수 있습니다. 예를 들어, 복구 가능한 오류는 다음과 같은 이유로 발생할 수 있습니다.

- 사용자의 자격 증명이 삭제되었거나 만료되었습니다.
- 대상 버킷이 존재하지 않습니다.
- 알림을 전달할 수 없습니다.

StorageGRID에서 복구 가능한 오류가 발생하면 플랫폼 서비스 요청이 성공할 때까지 재시도됩니다.

다른 오류는 복구할 수 없습니다. 예를 들어, 복구 불가능한 오류는 다음과 같은 이유로 발생할 수 있습니다.

- 해당 엔드포인트가 삭제되었습니다.
- 웹훅 엔드포인트 대상이 알림 요청에 `400 Bad Request` 오류로 응답합니다.

StorageGRID에서 복구할 수 없는 엔드포인트 오류가 발생하는 경우:

- Grid Manager에서 지원 > 도구 > 메트릭 > **Grafana** > *플랫폼 서비스 개요*로 이동하여 오류 세부 정보를 확인하십시오.
- 테넌트 관리자에서 **STORAGE (S3)** > *Platform Services Endpoints*로 이동하여 오류 세부 정보를 확인하십시오.
- `/var/local/log/bycast-err.log`관련 오류가 있는지 확인하십시오. ADC 서비스가 있는 스토리지 노드에는 이 로그 파일이 포함되어 있습니다.

플랫폼 서비스 메시지를 전달할 수 없습니다

대상에서 플랫폼 서비스 메시지를 수락할 수 없는 문제가 발생하면 버킷에 대한 클라이언트 작업은 성공하지만 플랫폼 서비스 메시지는 전달되지 않습니다. 예를 들어, 대상의 자격 증명이 업데이트되어 StorageGRID가 더 이상 대상 서비스에 인증할 수 없는 경우 이 오류가 발생할 수 있습니다.

관련 알림을 확인하십시오.

플랫폼 서비스 요청 처리 속도가 느려짐

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.

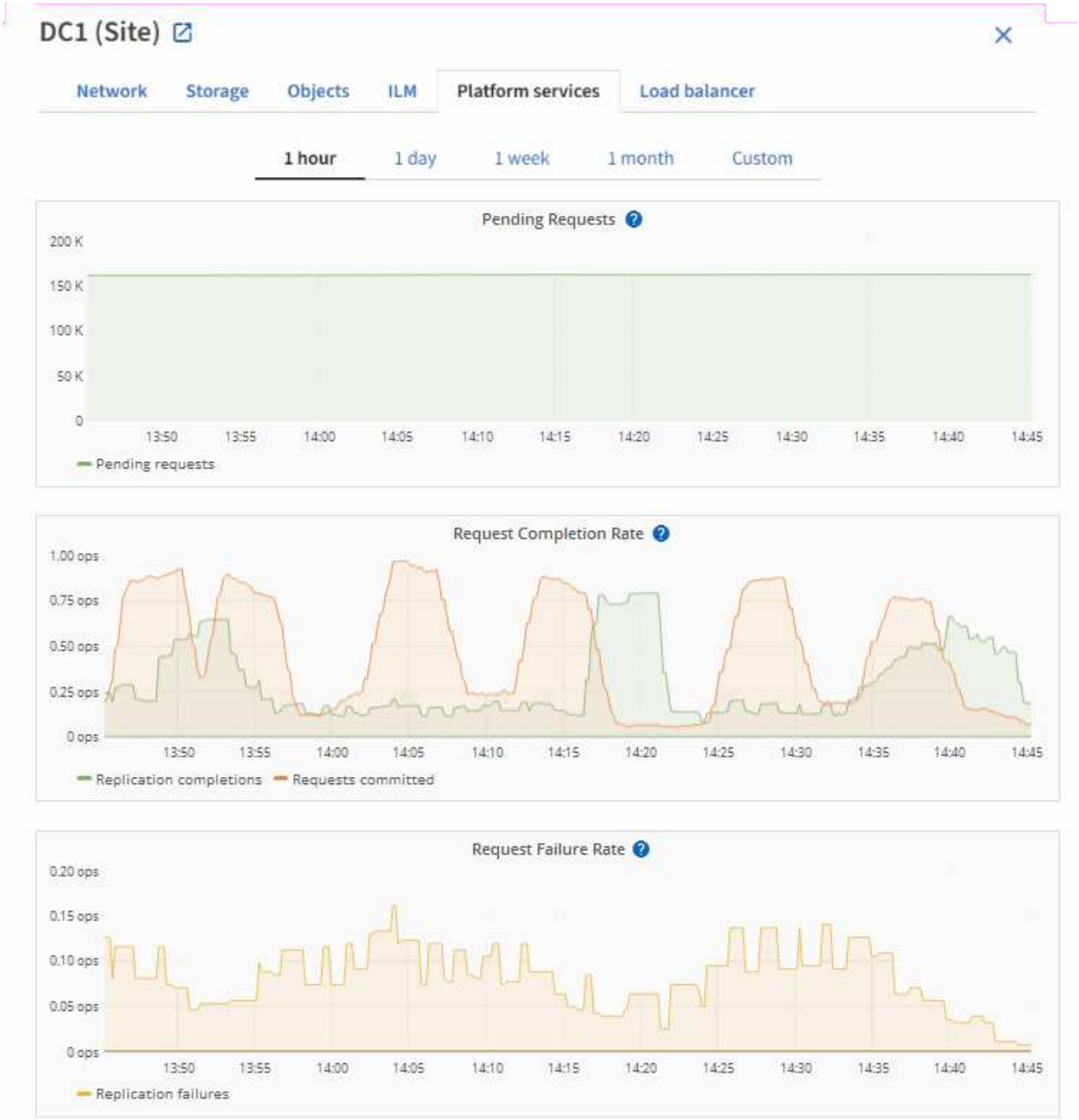
눈에 띄는 유일한 영향은 수신 S3 요청 실행 시간이 더 오래 걸린다는 것입니다. 성능 저하가 현저하게 감지되기 시작하면 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하면 클라이언트의 S3 작업(예: PUT 요청)이 결국 실패하게 됩니다.

CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 더 큰 영향을 받을 가능성이 높습니다.

플랫폼 서비스 요청이 실패합니다

플랫폼 서비스의 요청 실패율을 보려면:

1. *노드*를 선택합니다.
2. 사이트 > *플랫폼 서비스*를 선택합니다.
3. 요청 오류율 차트를 확인합니다.



플랫폼 서비스 이용 불가 알림

플랫폼 서비스 이용 불가 경고는 RSM 서비스를 사용하는 스토리지 노드 중 실행 중이거나 사용 가능한 노드 수가 너무 적어 해당 사이트에서 플랫폼 서비스 작업을 수행할 수 없음을 나타냅니다.

RSM 서비스는 플랫폼 서비스 요청이 각각의 엔드포인트로 전송되도록 보장합니다.

이 경고를 해결하려면 사이트에서 RSM 서비스가 포함된 스토리지 노드를 확인하십시오. (RSM 서비스는 ADC 서비스가 포함된 스토리지 노드에 있습니다.) 그런 다음 해당 스토리지 노드 중 과반수가 실행 중이고 사용 가능한 상태인지 확인하십시오.

한 사이트에서 RSM 서비스를 포함하는 스토리지 노드가 두 개 이상 장애가 발생하면 해당 사이트에 대한 보류 중인 플랫폼 서비스 요청이 모두 손실됩니다.

플랫폼 서비스 엔드포인트에 대한 추가 문제 해결 지침

자세한 내용은 테넌트 계정 사용 › 플랫폼 서비스 엔드포인트 문제 해결을 참조하십시오.

관련 정보

"StorageGRID 시스템 문제 해결"

StorageGRID의 테넌트 계정에 대한 S3 Select 관리

특정 S3 테넌트가 S3 Select를 사용하여 개별 개체에 대한 SelectObjectContent 요청을 실행할 수 있도록 허용할 수 있습니다.

S3 Select는 데이터베이스 및 관련 리소스를 배포하지 않고도 대량의 데이터를 효율적으로 검색할 수 있는 방법을 제공합니다. 또한 데이터 검색 비용과 지연 시간을 줄여줍니다.

S3 Select란 무엇인가요?

S3 Select를 사용하면 S3 클라이언트가 SelectObjectContent 요청을 통해 객체에서 필요한 데이터만 필터링하고 검색할 수 있습니다. StorageGRID 의 S3 Select 구현에는 S3 Select 명령 및 기능의 일부가 포함되어 있습니다.

S3 Select 사용을 위한 고려 사항 및 요구 사항

Grid 관리 요구사항

그리드 관리자는 테넌트에게 S3 Select 권한을 부여해야 합니다. *S3 Select 허용*은 "테넌트 생성" 또는 "테넌트 편집" 할 때 선택합니다.

객체 형식 요구 사항

조회하려는 객체는 다음 형식 중 하나여야 합니다.

- **CSV**. 있는 그대로 사용하거나 GZIP 또는 BZIP2 아카이브로 압축할 수 있습니다.
- **Parquet**. Parquet 객체에 대한 추가 요구사항:
  - S3 Select는 GZIP 또는 Snappy를 사용한 컬럼형 압축만 지원합니다. S3 Select는 Parquet 객체에 대한 전체 객체 압축을 지원하지 않습니다.
  - S3 Select는 Parquet 출력을 지원하지 않습니다. 출력 형식을 CSV 또는 JSON으로 지정해야 합니다.
  - 압축되지 않은 행 그룹의 최대 크기는 512MB입니다.
  - 객체의 스키마에 명시된 데이터 형식을 사용해야 합니다.
  - INTERVAL, JSON, LIST, TIME 또는 UUID 논리 유형은 사용할 수 없습니다.

엔드포인트 요구 사항

SelectObjectContent 요청은 "StorageGRID 로드 밸런서 엔드포인트"으로 전송되어야 합니다.

엔드포인트에서 사용하는 관리 노드 및 게이트웨이 노드는 다음 중 하나여야 합니다.

- 서비스 어플라이언스 노드
- VMware 기반 소프트웨어 노드
- cgroup v2가 활성화된 커널을 실행하는 베어메탈 노드

일반적인 고려 사항

쿼리를 스토리지 노드로 직접 보낼 수 없습니다.

> SelectObjectContent 요청은 모든 S3 클라이언트와 모든 테넌트의 로드 밸런서 성능을 저하시킬 수 있습니다. 이 기능은 필요한 경우에만, 그리고 신뢰할 수 있는 테넌트에 대해서만 활성화하십시오.

"S3 Select 사용 설명서"을 참조하십시오.

시간 경과에 따른 S3 Select 작업의 "Grafana 차트"을(를) 보려면 그리드 관리자에서 지원 > 도구 > *메트릭*을 선택하십시오.