



테넌트 관리 StorageGRID

NetApp
October 03, 2025

목차

테넌트 관리	1
테넌트 관리	1
테넌트 계정이란 무엇입니까?	1
테넌트 계정을 생성하고 구성합니다	1
S3 테넌트를 구성합니다	2
Swift 테넌트를 구성합니다	2
테넌트 계정을 생성합니다	3
테넌트의 로컬 루트 사용자에게 대한 암호를 변경합니다	7
테넌트 계정을 편집합니다	8
테넌트 계정을 삭제합니다	11
플랫폼 서비스 관리	11
S3 테넌트 계정에 대한 플랫폼 서비스 관리	11
플랫폼 서비스를 위한 네트워크 및 포트	12
플랫폼 서비스 메시지를 사이트별로 전달	13
플랫폼 서비스 문제 해결	15
관리 S3 테넌트 계정에 대해 선택	20
S3 Select란 무엇입니까?	20
S3 Select 사용에 대한 고려 사항 및 요구 사항	20

테넌트 관리

테넌트 관리

그리드 관리자는 S3 및 Swift 클라이언트가 StorageGRID 시스템을 사용하여 오브젝트를 저장 및 검색하고, 스토리지 사용량을 모니터링하고, 클라이언트가 수행할 수 있는 작업을 관리하는 데 사용하는 테넌트 계정을 생성하고 관리합니다.

테넌트 계정이란 무엇입니까?

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API 또는 Swift REST API를 사용하는 클라이언트 애플리케이션이 StorageGRID에 개체를 저장하고 검색할 수 있습니다.

각 테넌트 계정은 계정을 생성할 때 지정하는 단일 프로토콜 사용을 지원합니다. 두 프로토콜을 모두 사용하는 StorageGRID 시스템에 오브젝트를 저장하고 검색하려면 S3 버킷 및 오브젝트, Swift 컨테이너 및 오브젝트, 두 개의 테넌트 계정을 만들어야 합니다. 각 테넌트 계정에는 고유한 계정 ID, 인증된 그룹 및 사용자, 버킷 또는 컨테이너 및 객체가 있습니다.

필요에 따라 시스템에 저장된 객체를 다른 엔터티로 분리하려는 경우 추가 테넌트 계정을 생성할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 설정할 수 있습니다.

- * 기업 활용 사례: * 엔터프라이즈 애플리케이션에서 StorageGRID 시스템을 관리하는 경우 조직의 여러 부서에서 그리드의 객체 스토리지를 분리할 수 있습니다. 이 경우 마케팅 부서, 고객 지원 부서, 인사 부서 등에 대한 테넌트 계정을 만들 수 있습니다.



S3 클라이언트 프로토콜을 사용하는 경우 S3 버킷 및 버킷 정책을 사용하여 엔터프라이즈의 부서 간에 오브젝트를 분리할 수 있습니다. 테넌트 계정은 사용할 필요가 없습니다. 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

- * 서비스 공급자 활용 사례: * StorageGRID 시스템을 서비스 공급자로 관리하는 경우 그리드의 객체 스토리지를 그리드의 스토리지를 임대할 다른 엔터티로 분리할 수 있습니다. 이 경우 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정을 생성합니다.

테넌트 계정을 생성하고 구성합니다

테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트 계정의 표시 이름입니다.
- 테넌트 계정(S3 또는 Swift)에서 사용할 클라이언트 프로토콜입니다.
- S3 테넌트 계정의 경우: 테넌트 계정에 S3 버킷을 포함하는 플랫폼 서비스를 사용할 수 있는 권한이 있는지 여부
테넌트 계정에서 플랫폼 서비스를 사용하도록 허용하는 경우 해당 사용자의 사용을 지원하도록 그리드가 구성되어 있는지 확인해야 합니다. "플랫폼 서비스"를 참조하십시오.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 할당량이 초과되면 테넌트가 새 객체를 생성할 수 없습니다.



테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.

- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

테넌트 계정이 생성된 후 다음 작업을 수행할 수 있습니다.

- * GRID용 플랫폼 서비스 관리 *: 테넌트 계정에 대해 플랫폼 서비스를 사용하는 경우, 플랫폼 서비스 메시지가 전달되는 방법과 StorageGRID 배포에서 플랫폼 서비스를 사용하는 데 필요한 네트워킹 요구 사항을 이해해야 합니다.
- * 테넌트 계정의 스토리지 사용량 모니터링 *: 테넌트가 해당 계정을 사용하기 시작한 후 Grid Manager를 사용하여 각 테넌트가 사용하는 스토리지 양을 모니터링할 수 있습니다.



노드가 그리드의 다른 노드로부터 격리되면 테넌트의 스토리지 사용량 값이 최신 상태가 아닐 수 있습니다. 네트워크 연결이 복원되면 합계가 업데이트됩니다.

테넌트에 대해 할당량을 설정한 경우 * 테넌트 할당량 사용량 높음 * 알림을 설정하여 테넌트가 할당량을 사용하고 있는지 확인할 수 있습니다. 활성화된 경우 테넌트가 할당량의 90%를 사용한 경우 이 경고가 트리거됩니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 설명서의 경고 참조를 참조하십시오.

- * 클라이언트 작업 구성 *: 일부 클라이언트 작업이 금지되는지 여부를 구성할 수 있습니다.

S3 테넌트를 구성합니다

S3 테넌트 계정이 생성된 후 테넌트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

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



S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 액세스 키 및 버킷을 생성 및 관리할 수 있지만, S3 클라이언트 애플리케이션을 사용하여 오브젝트를 수집 및 관리해야 합니다.

Swift 테넌트를 구성합니다

Swift 테넌트 계정이 생성된 후 테넌트의 루트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

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



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

테넌트 계정을 생성합니다

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

테넌트 계정을 생성할 때 이름, 클라이언트 프로토콜 및 선택적으로 스토리지 할당량을 지정합니다. StorageGRID에 대해 SSO(Single Sign-On)를 사용하는 경우 테넌트 계정을 구성할 루트 액세스 권한이 있는 통합 그룹도 지정합니다. StorageGRID에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정에서 자체 ID 소스를 사용할지 여부를 지정하고 테넌트의 로컬 루트 사용자에게 대한 초기 암호를 구성해야 합니다.

Grid Manager는 테넌트 계정 생성 단계를 안내하는 마법사를 제공합니다. 단계는 에 따라 다릅니다 [ID 제휴](#) 및 [SSO\(Single Sign-On\)](#) 테넌트 계정을 만드는 데 사용하는 Grid Manager 계정이 루트 액세스 권한이 있는 관리자 그룹에 속하는지 여부 및 가 구성됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 [지원되는 웹 브라우저](#).
- 특정 액세스 권한이 있습니다.
- 테넌트 계정에서 Grid Manager에 대해 구성된 ID 소스를 사용하고 테넌트 계정에 대한 루트 액세스 권한을 통합 그룹에 부여하려는 경우 해당 통합 그룹을 Grid Manager로 가져온 것입니다. 이 관리 그룹에 그리드 관리자 권한을 할당할 필요는 없습니다. 를 참조하십시오 [관리 그룹 관리 지침](#).

단계

1. Tenants * 를 선택합니다.
2. Create * 를 선택하고 테넌트에 대해 다음 정보를 입력합니다.
 - a. * 이름 *: 테넌트 계정의 이름을 입력합니다. 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.
 - b. * Description * (선택 사항): 테넌트를 식별하는 데 도움이 되는 설명을 입력합니다.
 - c. * 클라이언트 유형 *: * S3 * 또는 * Swift * 의 클라이언트 유형을 선택합니다.
 - d. * 스토리지 할당량 * (선택 사항): 이 테넌트에 스토리지 할당량을 지정하려면 할당량에 대한 숫자 값을 입력하고 올바른 단위(GB, TB 또는 PB)를 선택합니다.

×

Create a tenant

1

Enter details

2

Select permissions

3

Define root access

Enter tenant details

Name ?

Description (optional) ?

Description

Client type ?

☒ S3
 ☐ Swift

Storage quota (optional) ?

GB ▼

Cancel

Continue

3. 계속 * 을 선택하고 S3 또는 Swift 테넌트를 구성합니다.

S3 테넌트

테넌트에 대한 적절한 권한을 선택합니다. 이러한 권한 중 일부는 추가 요구 사항이 있습니다. 자세한 내용은 각 권한에 대한 온라인 도움말을 참조하십시오.

- 플랫폼 서비스를 허용합니다
- 자체 ID 소스 사용(SSO를 사용하지 않는 경우에만 선택 가능)
- S3 선택 허용(참조 [관리 S3 테넌트 계정에 대해 선택](#))

Swift 테넌트

테넌트가 자체 ID 소스를 사용할 경우 * 고유 ID 소스 사용 * 을 선택합니다(SSO를 사용하지 않는 경우에만 선택 가능).

1. Continue * 를 선택하고 테넌트 계정에 대한 루트 액세스를 정의합니다.

ID 페더레이션이 구성되지 않았습니다

1. 로컬 루트 사용자의 암호를 입력합니다.
2. 테넌트 생성 * 을 선택합니다.

SSO가 활성화되었습니다

StorageGRID에 대해 SSO가 활성화된 경우 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용해야 합니다. 로컬 사용자는 로그인할 수 없습니다. 테넌트 계정을 구성할 루트 액세스 권한이 있는 통합 그룹을 지정합니다.

1. 테넌트에 대한 초기 루트 액세스 권한을 가지려면 그리드 관리자에서 기존 통합 그룹을 선택합니다.



적절한 권한이 있는 경우 필드를 선택하면 그리드 관리자의 기존 통합 그룹이 나열됩니다. 그렇지 않으면 그룹의 고유 이름을 입력합니다.

2. 테넌트 생성 * 을 선택합니다.

SSO가 활성화되지 않았습니다

1. 테넌트가 자신의 그룹 및 사용자를 관리하는지 또는 Grid Manager에 대해 구성된 ID 소스를 사용하는지에 따라 표에 설명된 단계를 완료합니다.

테넌트가...	수행할 작업...
자체 그룹 및 사용자를 관리합니다	a. Use own identity source * 를 선택합니다. ◦ 참고 *: 이 확인란을 선택하고 테넌트 그룹 및 사용자에 대해 ID 페더레이션을 사용하려면 테넌트가 자체 ID 소스를 구성해야 합니다. 를 참조하십시오 테넌트 계정 사용 지침. b. 테넌트의 로컬 루트 사용자에 대한 암호를 지정한 다음 * Create tenant * 를 선택합니다. c. 테넌트를 구성하려면 * root * 로 로그인 * 을 선택하고, 나중에 테넌트를 구성하려면 * 마침 * 을 선택합니다.
Grid Manager에 대해 구성된 그룹 및 사용자를 사용합니다	a. 다음 중 하나 또는 모두를 수행합니다. ◦ 테넌트에 대한 초기 루트 액세스 권한이 있어야 하는 기존 통합 그룹을 그리드 관리자에서 선택합니다. ▪ 참고 *: 적절한 권한이 있으면 필드를 선택할 때 그리드 관리자의 기존 통합 그룹이 나열됩니다. 그렇지 않으면 그룹의 고유 이름을 입력합니다. ◦ 테넌트의 로컬 루트 사용자에 대한 암호를 지정합니다. b. 테넌트 생성 * 을 선택합니다.

1. 지금 테넌트에 로그인하려면:

- 제한된 포트에서 그리드 관리자에 액세스하는 경우 테넌트 테이블에서 * 제한된 * 를 선택하여 이 테넌트 계정에 액세스하는 방법에 대해 자세히 알아보십시오.

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'는 테넌트 전용 포트입니다
- '20-digit-account-id'는 테넌트의 고유 계정 ID입니다
- 포트 443에서 그리드 관리자에 액세스하지만 로컬 루트 사용자의 암호를 설정하지 않은 경우 그리드 관리자의 테넌트 테이블에서 * 로그인 * 을 선택하고 루트 액세스 통합 그룹에 사용자의 자격 증명을 입력합니다.
- 포트 443에서 Grid Manager에 액세스하고 로컬 루트 사용자의 암호를 설정하는 경우:
 - i. 지금 테넌트를 구성하려면 * root로 로그인 * 을 선택합니다.

로그인하면 버킷 또는 컨테이너, ID 페더레이션, 그룹 및 사용자를 구성하기 위한 링크가 표시됩니다.

Create a tenant

Enter details — Select permissions — Define root access

The tenant Tenant02 was created.

If you're ready to configure the tenant, select Sign in as root.

[Sign in as root](#) Signed in

You can now access the Tenant Manager to configure these settings:

- **Buckets** : Create and manage buckets.
- **Identity federation** : Configure an external identity source to use federated groups.
- **Groups** : Manage groups and assign permissions.
- **Users** : Manage local users and assign users to groups.

Finish

- i. 테넌트 계정을 구성할 링크를 선택합니다.

각 링크는 테넌트 관리자에서 해당 페이지를 엽니다. 페이지를 완료하려면 을 참조하십시오 [테넌트 계정 사용 지침](#).

- ii. 그렇지 않으면 * 마침 * 을 선택하여 나중에 테넌트에 액세스하십시오.

2. 나중에 테넌트에 액세스하려면 다음을 수행합니다.

사용 중인 경우...	다음 중 하나를 수행합니다.
포트 443	• Grid Manager에서 * Tenants * 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'는 테넌트의 고유 계정 ID입니다
제한된 포트	• Grid Manager에서 * Tenants * 를 선택하고 * Restricted * 를 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'는 테넌트의 고유 계정 ID입니다

관련 정보

- [방화벽을 통한 액세스 제어](#)
- [S3 테넌트 계정에 대한 플랫폼 서비스 관리](#)

테넌트의 로컬 루트 사용자에게 암호를 변경합니다

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

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 [지원되는 웹 브라우저](#).
- 특정 액세스 권한이 있습니다.

이 작업에 대해

StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 루트 사용자는 테넌트 계정에 로그인할 수 없습니다. 루트 사용자 작업을 수행하려면 사용자가 테넌트에 대한 루트 액세스 권한이 있는 통합 그룹에 속해야 합니다.

단계

1. Tenants * 를 선택합니다.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. 편집할 테넌트 계정을 선택합니다.

작업 단추가 활성화됩니다.

3. Actions * 드롭다운에서 * Change root password * 를 선택합니다.

4. 테넌트 계정의 새 암호를 입력합니다.

5. 저장 * 을 선택합니다.

테넌트 계정을 편집합니다

테넌트 계정을 편집하여 표시 이름을 변경하거나, ID 소스 설정을 변경하거나, 플랫폼 서비스를 허용 또는 금지하거나, 스토리지 할당량을 입력할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 [지원되는 웹 브라우저](#).
- 특정 액세스 권한이 있습니다.

단계

1. Tenants * 를 선택합니다.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Create

Export to CSV

Actions

Search tenants by name or ID

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. 편집할 테넌트 계정을 선택합니다.

검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

3. 작업 드롭다운에서 * 편집 * 을 선택합니다.

이 예제는 SSO(Single Sign-On)를 사용하지 않는 그리드에 대한 것입니다. 이 테넌트 계정은 자체 ID 소스를 구성하지 않았습니다.

×

Edit the tenant

1 Enter details

✓ Select permissions

Enter tenant details

Name ?

Tenant 01

Description (optional) ?

Description

Client type ?

☒ S3
☐ Swift

Storage quota (optional) ?

GB ▼

Cancel

Continue

4. 필요에 따라 다음 필드의 값을 변경합니다.

- * 이름 *
- * 설명 *
- * 클라이언트 유형 *
- * 스토리지 할당량 *

5. Continue * 를 선택합니다.

6. 테넌트 계정에 대한 사용 권한을 선택하거나 선택 취소합니다.

- 이미 사용 중인 테넌트에 대해 * 플랫폼 서비스 * 를 비활성화하면 해당 S3 버킷에 대해 구성된 서비스가 작동을 멈춥니다. 테넌트에 오류 메시지가 전송되지 않습니다. 예를 들어, 테넌트가 S3 버킷에 대해 CloudMirror 복제를 구성한 경우 버킷에 오브젝트를 저장할 수 있지만 해당 오브젝트의 복사본은 더 이상 엔드포인트로 구성된 외부 S3 버킷에서 생성할 수 없습니다.
- 사용자 지정 ID 소스 사용 * 확인란의 설정을 변경하여 테넌트 계정에서 자체 ID 소스를 사용할지 또는 Grid Manager용으로 구성된 ID 소스를 사용할지 여부를 결정합니다.

고유 ID 원본 사용 * 확인란이 다음과 같은 경우:

- 비활성화된 후 선택한 경우 테넌트는 이미 자체 ID 소스를 사용하도록 설정되어 있습니다. 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용하기 전에 해당 ID 소스를 비활성화해야 합니다.
- 비활성화되고 선택 취소되며 StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.

◦ 필요에 따라 * S3 Select * 를 활성화 또는 비활성화합니다. 을 참조하십시오 [관리 S3 테넌트 계정에 대해 선택](#).

7. 저장 * 을 선택합니다.

관련 정보

- [S3 테넌트 계정에 대한 플랫폼 서비스 관리](#)
- [테넌트 계정을 사용합니다](#)

테넌트 계정을 삭제합니다

테넌트의 시스템 액세스를 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 [지원되는 웹 브라우저](#).
- 특정 액세스 권한이 있어야 합니다.
- 테넌트 계정과 연결된 모든 버킷(S3), 컨테이너(Swift) 및 개체를 제거해야 합니다.

단계

1. Tenants * 를 선택합니다.
2. 삭제할 테넌트 계정을 선택합니다.

검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

3. 작업 * 드롭다운에서 * 삭제 * 를 선택합니다.
4. OK * 를 선택합니다.

플랫폼 서비스 관리

S3 테넌트 계정에 대한 플랫폼 서비스 관리

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

플랫폼 서비스란 무엇입니까?

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

이러한 서비스를 통해 테넌트는 자신의 S3 버킷에서 다음 기능을 사용할 수 있습니다.

- * CloudMirror 복제 *: StorageGRID CloudMirror 복제 서비스는 StorageGRID 버킷에서 지정된 외부 대상으로 특정 객체를 미러링하는 데 사용됩니다.

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



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

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

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



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

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

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



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

플랫폼 서비스를 통해 테넌트는 외부 스토리지 리소스, 알림 서비스 및 데이터에 대한 검색 또는 분석 서비스를 사용할 수 있습니다. 플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 외부에 있으므로 테넌트가 이러한 서비스를 사용하도록 허용할지 여부를 결정해야 합니다. 이 경우 테넌트 계정을 만들거나 편집할 때 플랫폼 서비스 사용을 활성화해야 합니다. 또한 테넌트가 생성하는 플랫폼 서비스 메시지가 대상에 도달할 수 있도록 네트워크를 구성해야 합니다.

플랫폼 서비스 사용을 위한 권장 사항

플랫폼 서비스를 사용하기 전에 다음 권장 사항을 숙지하십시오.

- StorageGRID 시스템의 S3 버킷에서 버전 관리 및 CloudMirror 복제가 모두 활성화된 경우 대상 엔드포인트에 대해 S3 버킷 버전을 활성화해야 합니다. 이를 통해 CloudMirror 복제가 엔드포인트에 비슷한 개체 버전을 생성할 수 있습니다.
- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청이 있는 100개 이상의 활성 테넌트를 사용해서는 안 됩니다. 활성 테넌트가 100개 이상인 경우 S3 클라이언트 성능이 저하될 수 있습니다.
- 완료할 수 없는 엔드포인트에 대한 요청은 최대 500,000개의 요청에 대해 대기됩니다. 이 제한은 활성 테넌트 간에 동일하게 공유됩니다. 새 테넌트는 이 500,000개 제한을 일시적으로 초과할 수 있으므로 새로 생성된 테넌트가 불공평하게 처벌되지 않습니다.

관련 정보

- [테넌트 계정을 사용합니다](#)
- [스토리지 프록시 설정을 구성합니다](#)
- [모니터링하고 문제를 해결합니다](#)

플랫폼 서비스를 위한 네트워크 및 포트

S3 테넌트가 플랫폼 서비스를 사용할 수 있도록 허용하는 경우 플랫폼 서비스 메시지가 대상으로 전달될 수 있도록 그리드에 대한 네트워킹을 구성해야 합니다.

테넌트 계정을 생성하거나 업데이트할 때 S3 테넌트 계정에 대해 플랫폼 서비스를 활성화할 수 있습니다. 플랫폼 서비스가 설정된 경우 테넌트는 CloudMirror 복제, 이벤트 알림 또는 S3 버킷에서 통합 메시지를 검색할 대상으로 사용되는 엔드포인트를 생성할 수 있습니다. 이러한 플랫폼 서비스 메시지는 ADC 서비스를 실행하는 스토리지 노드에서 대상 끝점으로 전송됩니다.

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

- 로컬로 호스팅되는 Elasticsearch 클러스터입니다
- SNS(Simple Notification Service) 메시지 수신을 지원하는 로컬 애플리케이션입니다
- StorageGRID의 동일한 인스턴스 또는 다른 인스턴스에서 로컬로 호스팅되는 S3 버킷
- Amazon Web Services의 엔드포인트와 같은 외부 엔드포인트입니다.

플랫폼 서비스 메시지가 전달될 수 있도록 ADC 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 다음 포트를 사용하여 플랫폼 서비스 메시지를 대상 끝점에 보낼 수 있는지 확인해야 합니다.

기본적으로 플랫폼 서비스 메시지는 다음 포트로 전송됩니다.

- * 80 *: http로 시작하는 끝점 URI입니다
- * 443 *: https로 시작하는 끝점 URI의 경우

테넌트는 끝점을 만들거나 편집할 때 다른 포트를 지정할 수 있습니다.



StorageGRID 배포를 CloudMirror 복제의 대상으로 사용하는 경우 80 또는 443 이외의 포트에서 복제 메시지를 받을 수 있습니다. 대상 StorageGRID 배포에서 S3에 사용 중인 포트가 끝점에 지정되었는지 확인합니다.

투명하지 않은 프록시 서버를 사용하는 경우에도 필요합니다 [스토리지 프록시 설정을 구성합니다](#) 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 합니다.

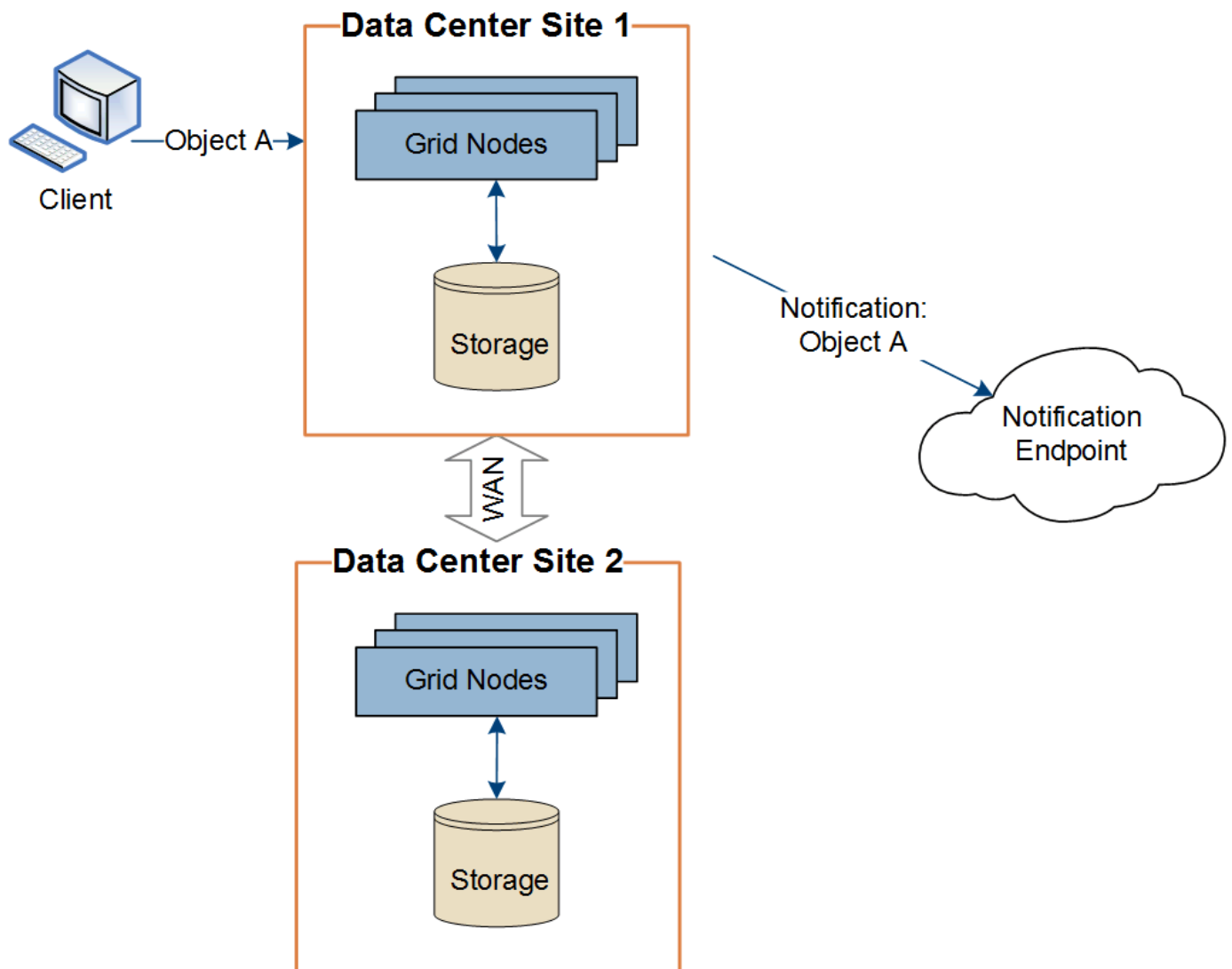
관련 정보

- [테넌트 계정을 사용합니다](#)

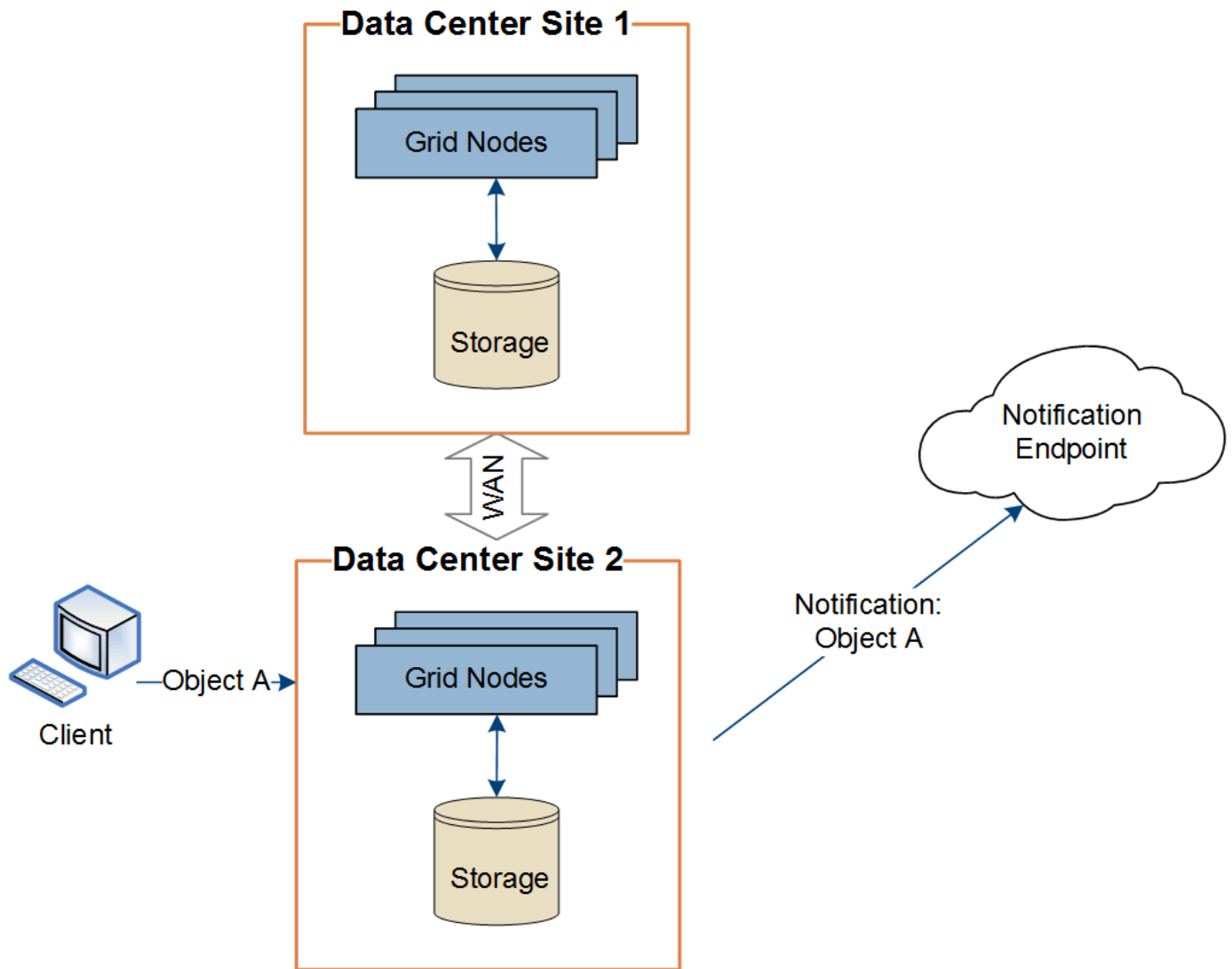
플랫폼 서비스 메시지를 사이트별로 전달

모든 플랫폼 서비스 작업은 사이트별로 수행됩니다.

즉, 테넌트가 클라이언트를 사용하여 데이터 센터 사이트 1의 게이트웨이 노드에 연결하여 오브젝트에 대해 S3 API 생성 작업을 수행하는 경우 해당 작업에 대한 알림이 트리거되고 데이터 센터 사이트 1에서 전송됩니다.



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



각 사이트의 네트워킹이 플랫폼 서비스 메시지를 해당 대상에 전달할 수 있도록 구성되어 있는지 확인합니다.

플랫폼 서비스 문제 해결

플랫폼 서비스에 사용되는 엔드포인트는 테넌트 관리자의 테넌트 사용자가 생성 및 유지 관리합니다. 그러나 테넌트에 플랫폼 서비스를 구성하거나 사용하는 데 문제가 있는 경우 Grid Manager를 사용하여 문제를 해결할 수 있습니다.

새 끝점에 문제가 있습니다

테넌트가 플랫폼 서비스를 사용하려면 먼저 테넌트 관리자를 사용하여 하나 이상의 엔드포인트를 생성해야 합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon 웹 서비스 버킷, 간단한 알림 서비스 주제 또는 로컬 또는 AWS에서 호스팅되는 Elasticsearch 클러스터와 같은 단일 플랫폼 서비스의 외부 대상을 나타냅니다. 각 끝점에는 외부 리소스의 위치와 해당 리소스에 액세스하는 데 필요한 자격 증명이 모두 포함됩니다.

테넌트가 끝점을 만들 때 StorageGRID 시스템은 끝점이 있는지, 그리고 지정된 자격 증명을 사용하여 해당 끝점에 도달할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 유효성 검사에 실패하면 끝점 유효성 검사가 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 테넌트 사용자가 문제를 해결한 다음 엔드포인트를 다시 생성해 보십시오.



테넌트 계정에 대해 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트에 문제가 있습니다

StorageGRID가 기존 엔드포인트에 도달하려고 할 때 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 끝점 페이지로 이동하여 각 끝점에 대한 가장 최근의 오류 메시지를 검토하고 오류가 발생한 시간을 확인할 수 있습니다. 마지막 오류 * 열은 각 끝점에 대한 가장 최근 오류 메시지를 표시하고 오류가 발생한 시간을

나타냅니다. 에 포함된 오류  지난 7일 내에 아이콘이 발생했습니다.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

☐	Display name  	Last error  	Type  	URI  	URN  
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



마지막 오류 * 열에 있는 일부 오류 메시지에는 괄호 안에 로그 ID가 포함될 수 있습니다. 그리드 관리자 또는 기술 지원에서는 이 ID를 사용하여 bycast.log의 오류에 대한 자세한 정보를 찾을 수 있습니다.

프록시 서버와 관련된 문제

스토리지 노드와 플랫폼 서비스 엔드포인트 간에 스토리지 프록시를 구성한 경우 프록시 서비스에서 StorageGRID의 메시지를 허용하지 않으면 오류가 발생할 수 있습니다. 이러한 문제를 해결하려면 프록시 서버의 설정을 확인하여 플랫폼 서비스 관련 메시지가 차단되지 않았는지 확인합니다.

오류가 발생했는지 확인합니다

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

클라이언트 작업이 실패했습니다

일부 플랫폼 서비스 문제로 인해 S3 버킷의 클라이언트 작업이 실패할 수 있습니다. 예를 들어 RSM(Internal Replicated State Machine) 서비스가 중지되거나 너무 많은 플랫폼 서비스 메시지가 배달 대기 중인 경우 S3 클라이언트 작업이 실패합니다.

서비스 상태를 확인하려면

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > * Storage Node * > * SSM * > * Services * 를 선택합니다.

복구할 수 없는 끝점 오류입니다

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

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

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

다른 오류는 복구할 수 없습니다. 예를 들어, 끝점이 삭제되면 복구할 수 없는 오류가 발생합니다.

StorageGRID에서 복구할 수 없는 끝점 오류가 발생하면 그리드 관리자에서 SMTT(Total Events) 레거시 경보가 트리거됩니다. Total Events Legacy(총 이벤트 레거시) 알람을 보려면

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > * node * > * SSM * > * Events * 를 선택합니다.
3. 테이블 상단의 마지막 이벤트 보기

이벤트 메시지는 '/var/local/log/bycast-err.log'에도 나열됩니다.

4. SMTT 알람 내용물에 제공된 지침을 따라 문제를 해결하십시오.
5. 구성 * 탭을 선택하여 이벤트 수를 재설정합니다.
6. 플랫폼 서비스 메시지가 전달되지 않은 객체를 테넌트에 알립니다.
7. 테넌트에게 객체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 다시 트리거하도록 지시합니다.

테넌트는 불필요한 변경을 방지하기 위해 기존 값을 다시 제출할 수 있습니다.

플랫폼 서비스 메시지를 전달할 수 없습니다

대상에 플랫폼 서비스 메시지를 수락하지 못하는 문제가 발생하면 버킷에 대한 클라이언트 작업은 성공하지만 플랫폼

서비스 메시지는 전달되지 않습니다. 예를 들어, StorageGRID가 더 이상 대상 서비스에 인증할 수 없도록 대상에서 자격 증명이 업데이트되는 경우 이 오류가 발생할 수 있습니다.

복구할 수 없는 오류로 인해 플랫폼 서비스 메시지를 전달할 수 없는 경우 그리드 관리자에서 SMTT(Total Events) 레거시 경보가 트리거됩니다.

플랫폼 서비스 요청에 대한 성능 저하

요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다.

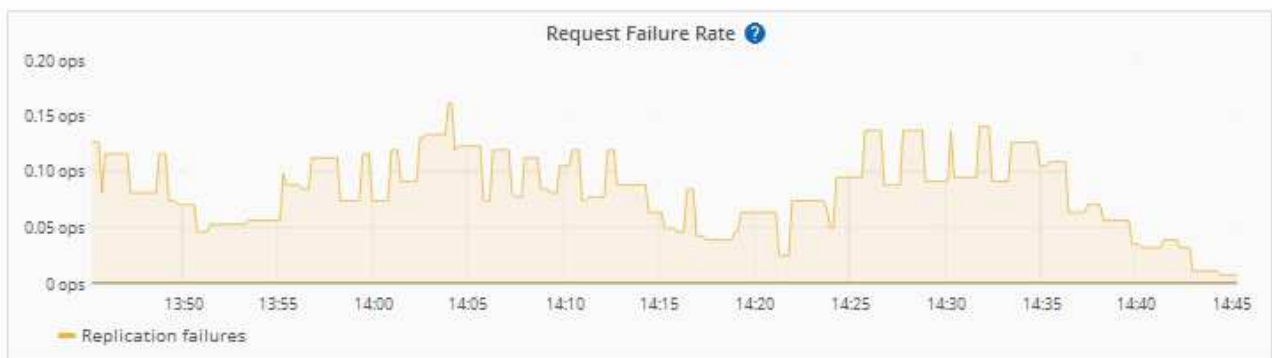
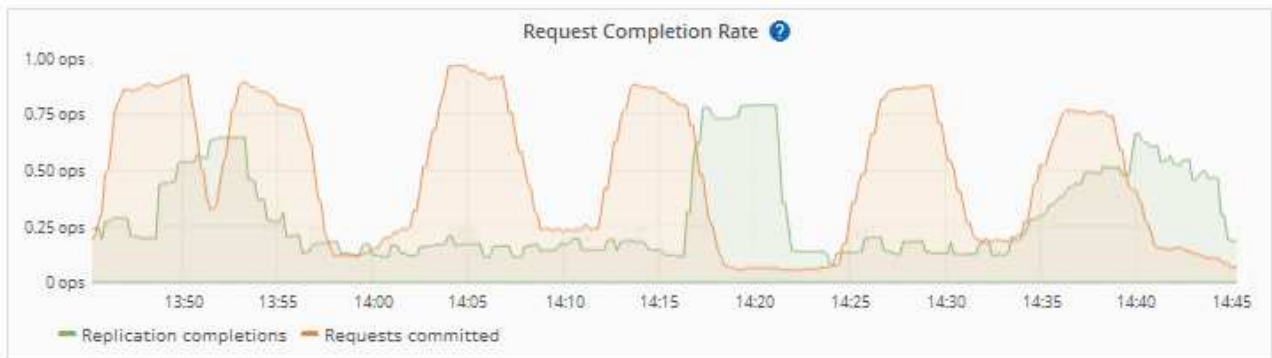
단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다.

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

플랫폼 서비스 요청에 실패했습니다

플랫폼 서비스에 대한 요청 실패율을 보려면

1. 노드 * 를 선택합니다.
2. `_site * > * 플랫폼 서비스 *` 를 선택합니다.
3. 요청 오류율 차트를 봅니다.

[1 hour](#) [1 day](#) [1 week](#) [1 month](#) [Custom](#)

플랫폼 서비스를 사용할 수 없음 경고

플랫폼 서비스 사용 불가 * 경고는 RSM 서비스가 실행 중이거나 사용 가능한 스토리지 노드가 너무 적어서 사이트에서 플랫폼 서비스 작업을 수행할 수 없음을 나타냅니다.

RSM 서비스는 플랫폼 서비스 요청이 각 끝점으로 전송되도록 합니다.

이 경고를 해결하려면 사이트에서 RSM 서비스를 포함하는 스토리지 노드를 확인합니다. (RSM 서비스는 ADC 서비스도 포함하는 스토리지 노드에 있습니다.) 그런 다음 이러한 스토리지 노드 중 대부분이 실행 중이고 사용 가능한지 확인합니다.



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

플랫폼 서비스 끝점에 대한 추가 문제 해결 지침

플랫폼 서비스 끝점 문제 해결에 대한 자세한 내용은 의 지침을 참조하십시오 [테넌트 계정 사용](#).

관련 정보

- [모니터링하고 문제를 해결합니다](#)
- [스토리지 프록시 설정을 구성합니다](#)

관리 S3 테넌트 계정에 대해 선택

특정 S3 테넌트가 S3 선택을 사용하여 개별 오브젝트에 SelectObjectContent 요청을 발급하도록 허용할 수 있습니다.

S3 Select를 사용하면 데이터베이스와 관련 리소스를 배치하지 않고도 대량의 데이터를 효율적으로 검색할 수 있습니다. 또한, 데이터를 검색하는 데 드는 비용과 대기 시간도 줄어듭니다.

S3 Select란 무엇입니까?

S3 Select를 사용하면 S3 클라이언트가 SelectObjectContent 요청을 사용하여 오브젝트에서 필요한 데이터만 필터링 및 검색할 수 있습니다. S3 Select의 StorageGRID 구현에는 S3 Select 명령 및 기능의 하위 집합이 포함됩니다.

S3 Select 사용에 대한 고려 사항 및 요구 사항

StorageGRID에서 S3 선택 쿼리에 대해 다음을 수행해야 합니다.

- 쿼리할 객체가 CSV 형식이거나 CSV 형식 파일이 포함된 GZIP 또는 BZIP2 압축 파일입니다.
- 테넌트는 그리드 관리자가 S3 선택 기능을 부여해야 합니다. Allow S3 Select * When(S3 선택 허용 * 시기) 을 선택합니다 [테넌트 생성](#) 또는 [테넌트 편집](#).
- SelectObjectContent 요청은 로 보내야 합니다 [StorageGRID 로드 밸런서 엔드포인트](#). 엔드포인트에서 사용하는 관리 및 게이트웨이 노드는 SG100 또는 SG1000 어플라이언스 노드 또는 VMware 기반 소프트웨어 노드여야 합니다.

다음 제한 사항을 참고하십시오.

- 베어 메탈 로드 밸런서 노드는 지원되지 않습니다.
- 쿼리는 스토리지 노드로 직접 보낼 수 없습니다.
- 더 이상 사용되지 않는 CLB 서비스를 통해 전송된 쿼리는 지원되지 않습니다.



SelectObjectContent 요청은 모든 S3 클라이언트 및 모든 테넌트의 로드 밸런서 성능을 줄일 수 있습니다. 신뢰할 수 있는 테넌트에만 필요한 경우에만 이 기능을 사용하도록 설정합니다.

를 참조하십시오 [S3 Select 사용에 대한 지침](#).

를 눌러 봅니다 [Grafana 차트](#) 시간의 경과에 따른 S3 Select 작업의 경우 Grid Manager에서 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.