S3 테넌트 계정 관리

StorageGRID

NetApp
April 10, 2024

목차

S3 테넌트 계정 관리 1
S3 액세스 키를 관리합니다 1
S3 버킷을 관리합니다 10

S3 테넌트 계정 관리

S3 액세스 키를 관리합니다

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

이 작업에 대해

S3 액세스 키는 다음과 같이 관리할 수 있습니다.

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

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

자체 S3 액세스 키를 생성합니다

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

필요한 것

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

이 작업에 대해

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

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

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

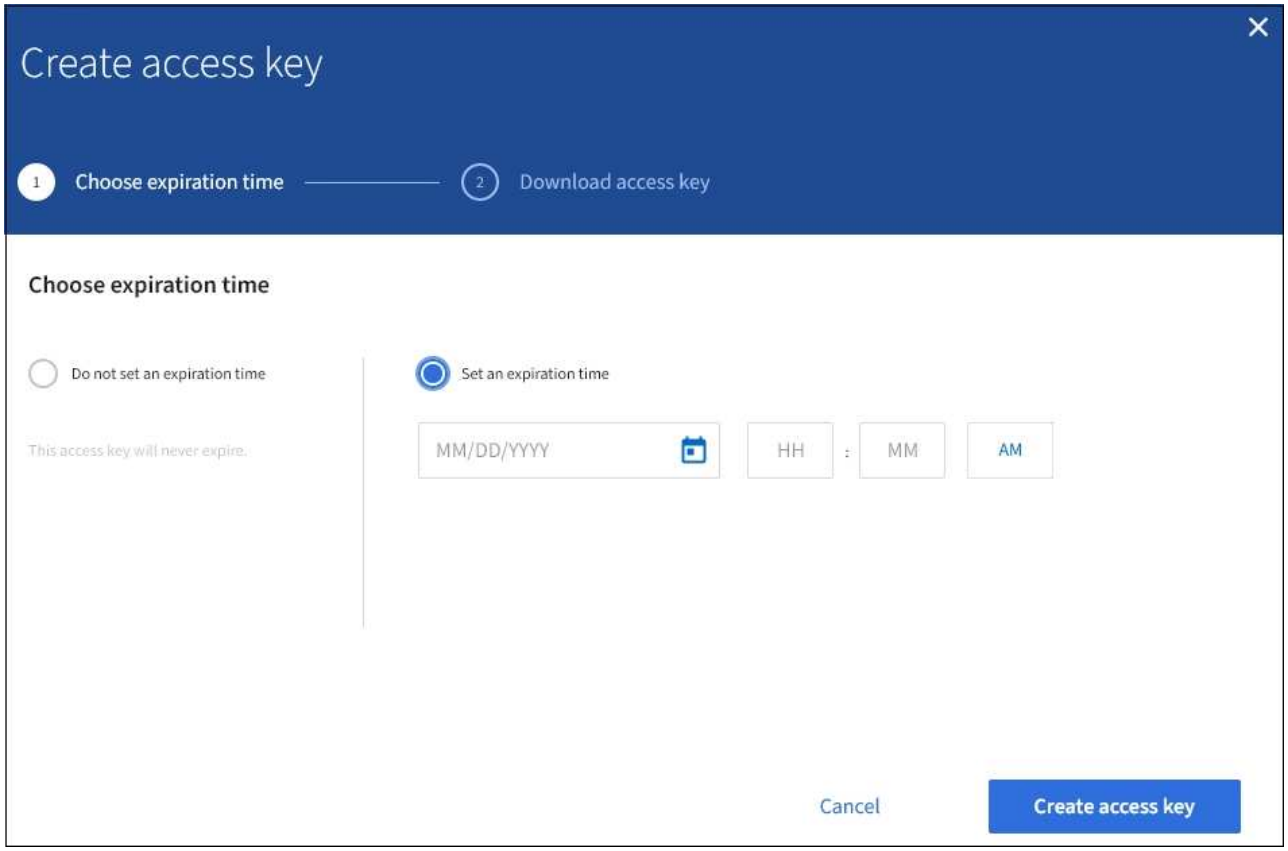
> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

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

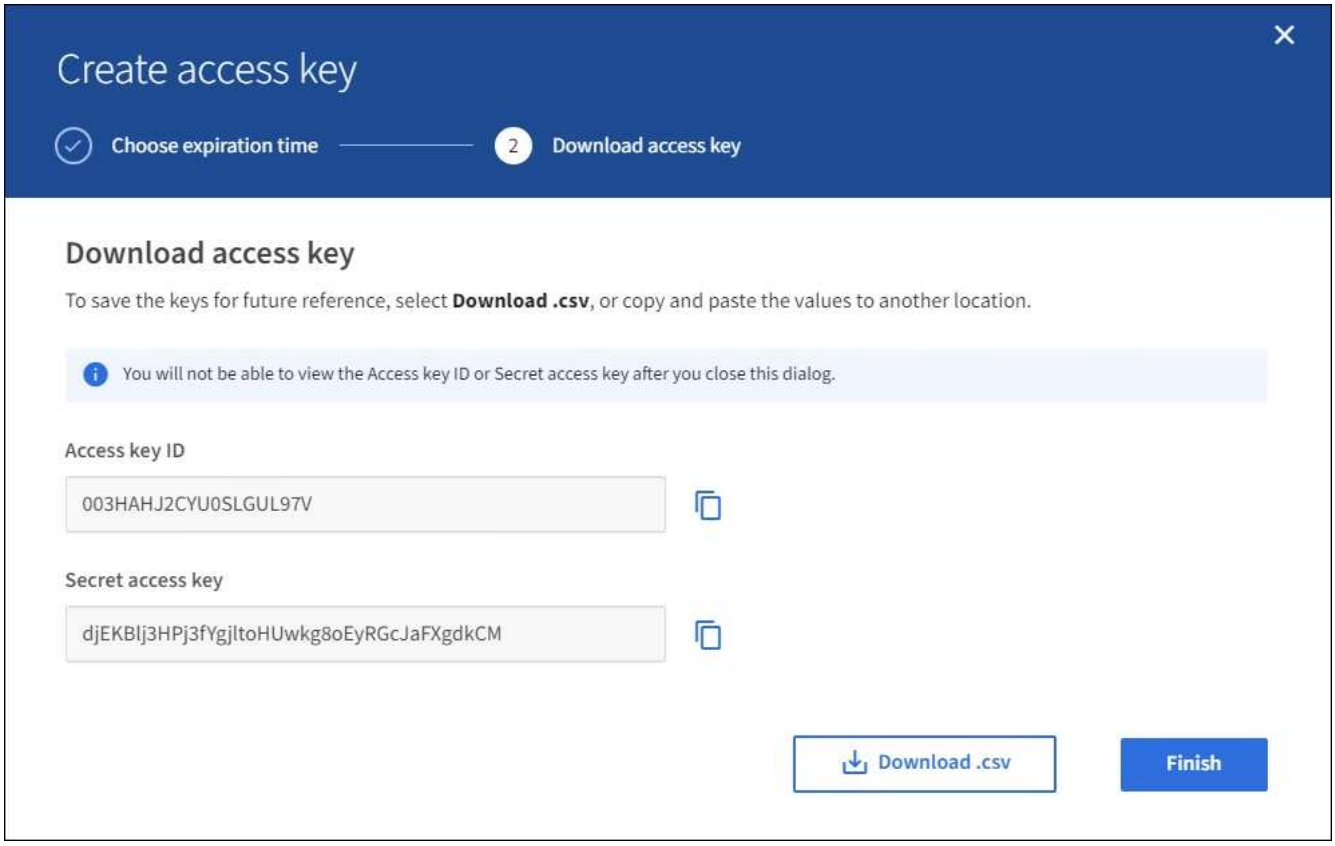


4. Create access key * 를 선택합니다.

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

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

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



6. 마침 * 을 선택합니다.

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

S3 액세스 키를 봅니다

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

필요한 것

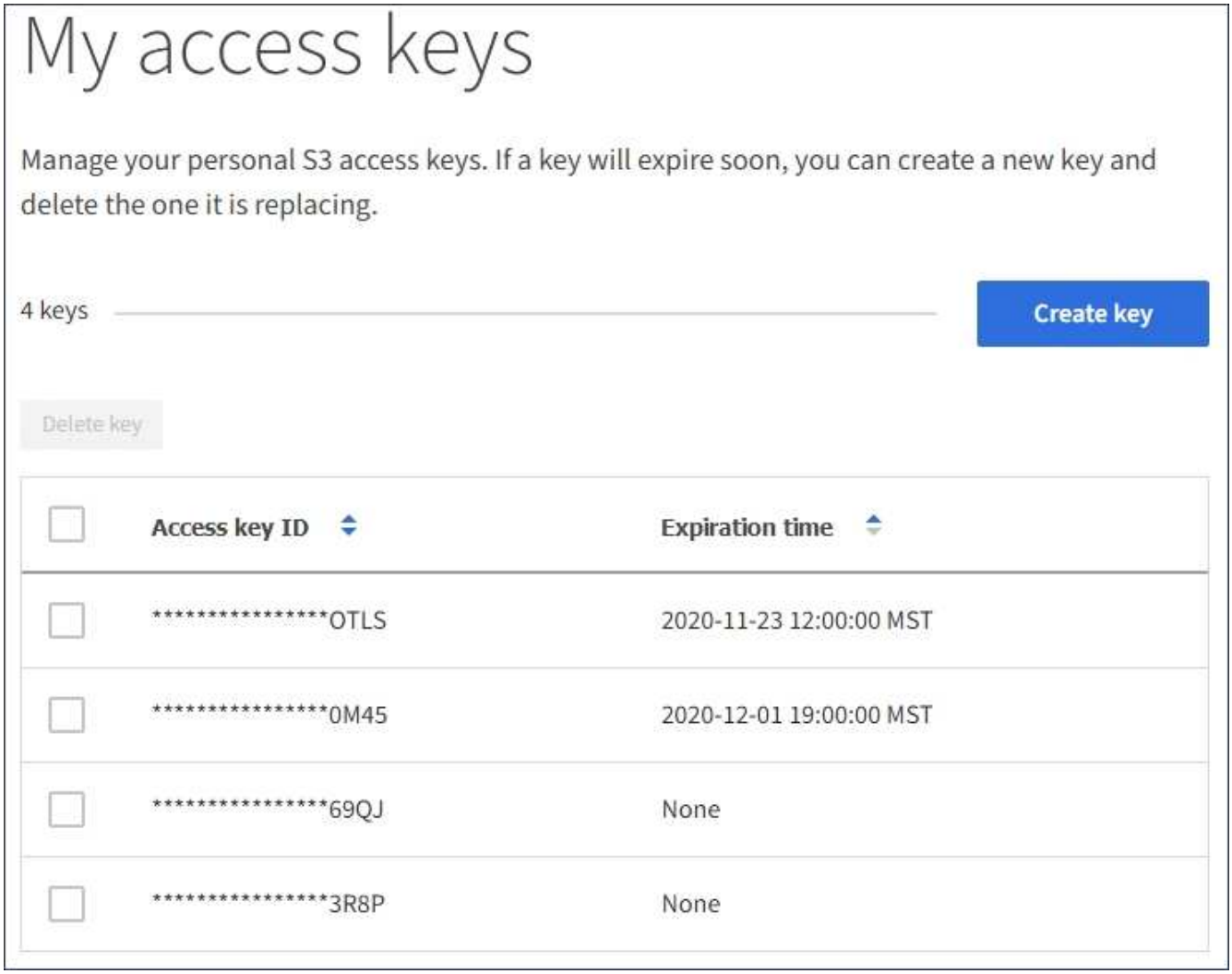
- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있어야 합니다.

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

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.



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

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

   만료된 키는 자동으로 제거됩니다.

관련 정보

자체 S3 액세스 키를 생성합니다

자체 S3 액세스 키를 삭제합니다

자체 **S3** 액세스 키를 삭제합니다

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

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

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

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

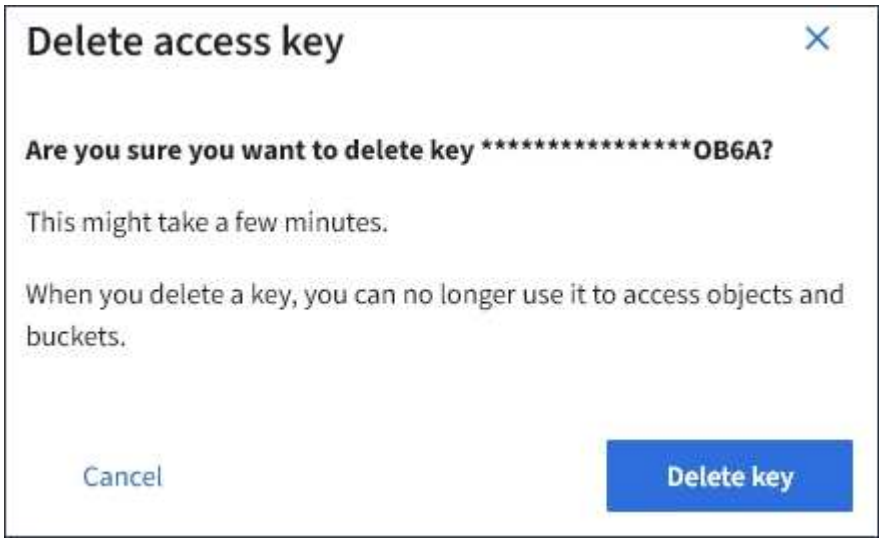
단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

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

   확인 대화 상자가 나타납니다.



4. Delete key * 를 선택합니다.

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

다른 사용자의 **S3** 액세스 키를 생성합니다

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

필요한 것

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

이 작업에 대해

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

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

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

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

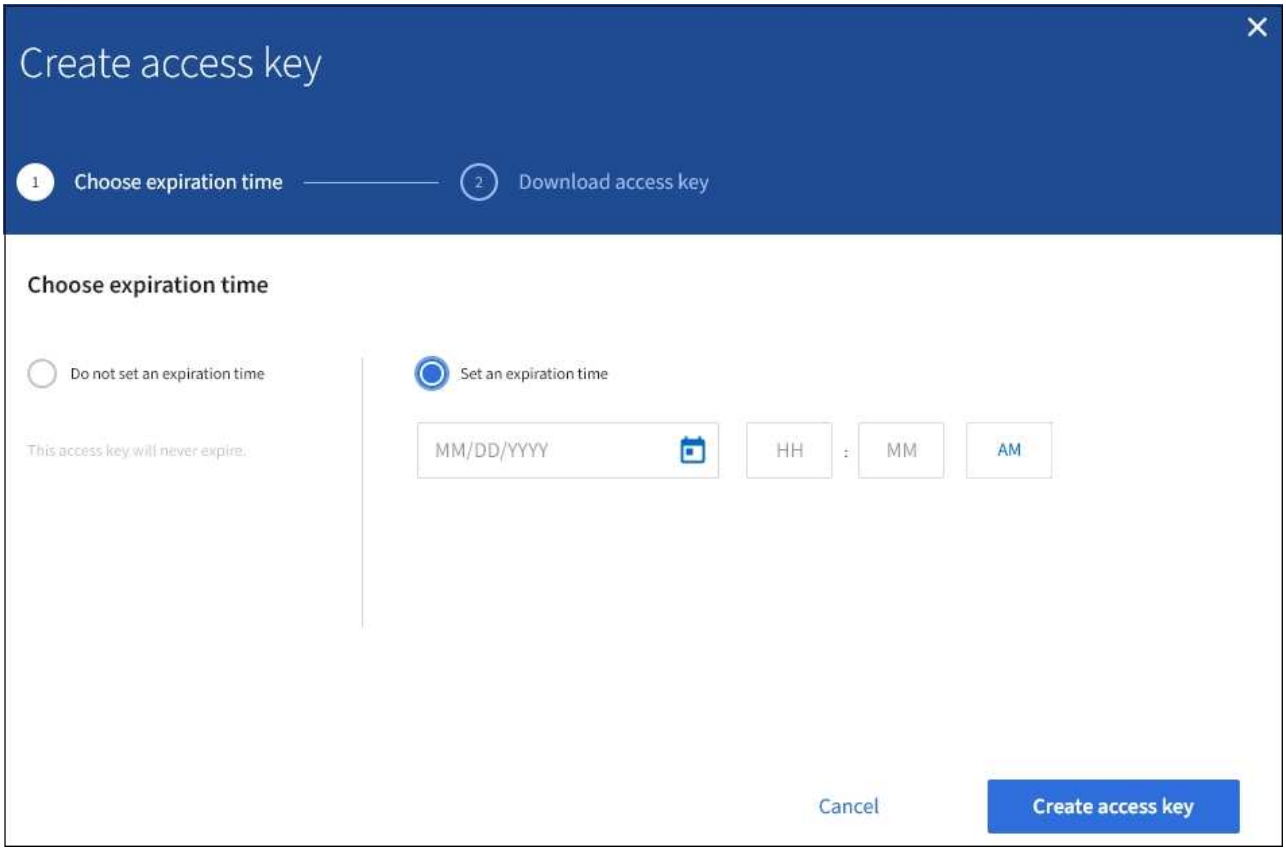
> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

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

   사용자 세부 정보 페이지가 나타납니다.

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

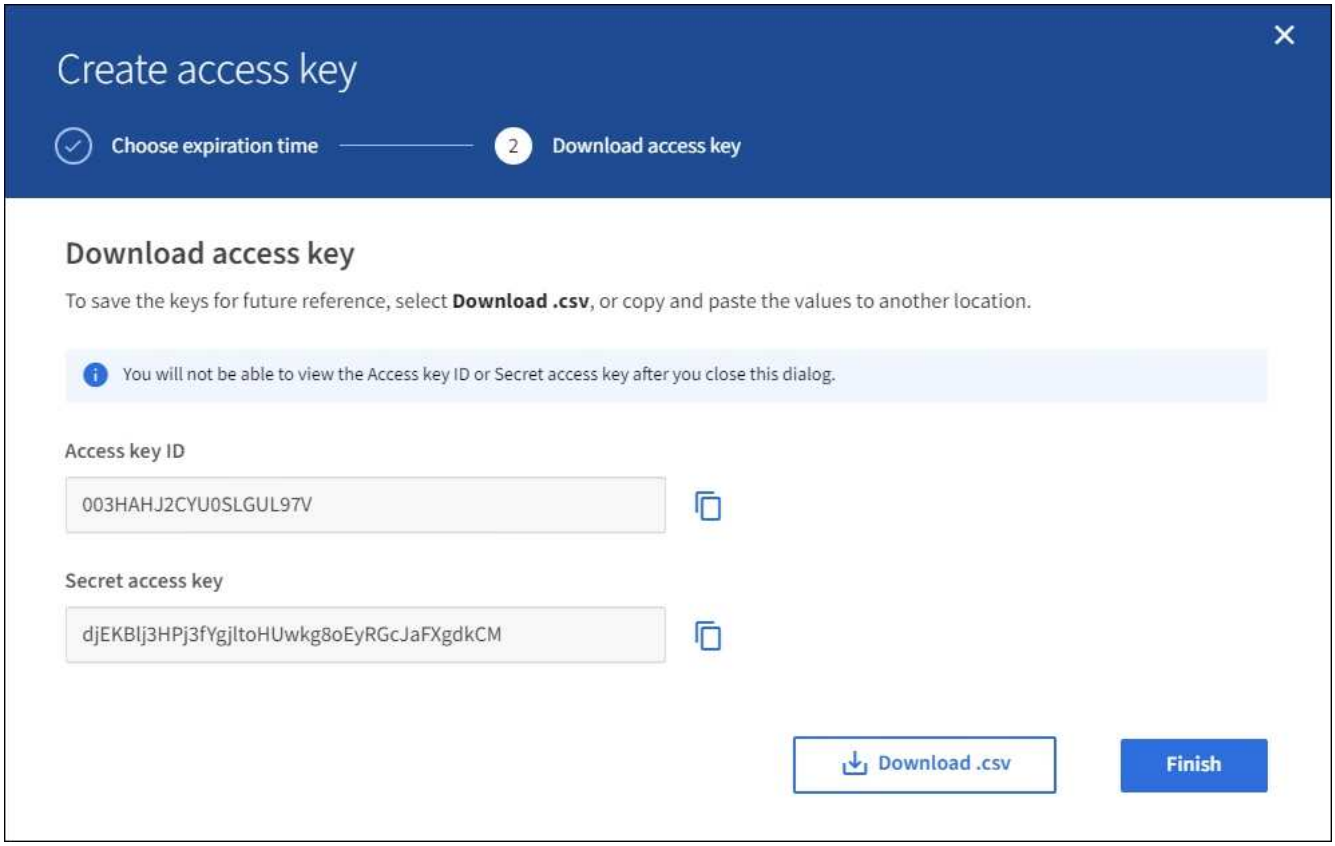


5. Create access key * 를 선택합니다.

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

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

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



7. 마침 * 을 선택합니다.

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

관련 정보

테넌트 관리 권한

다른 사용자의 **S3** 액세스 키를 봅니다

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

필요한 것

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

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

단계

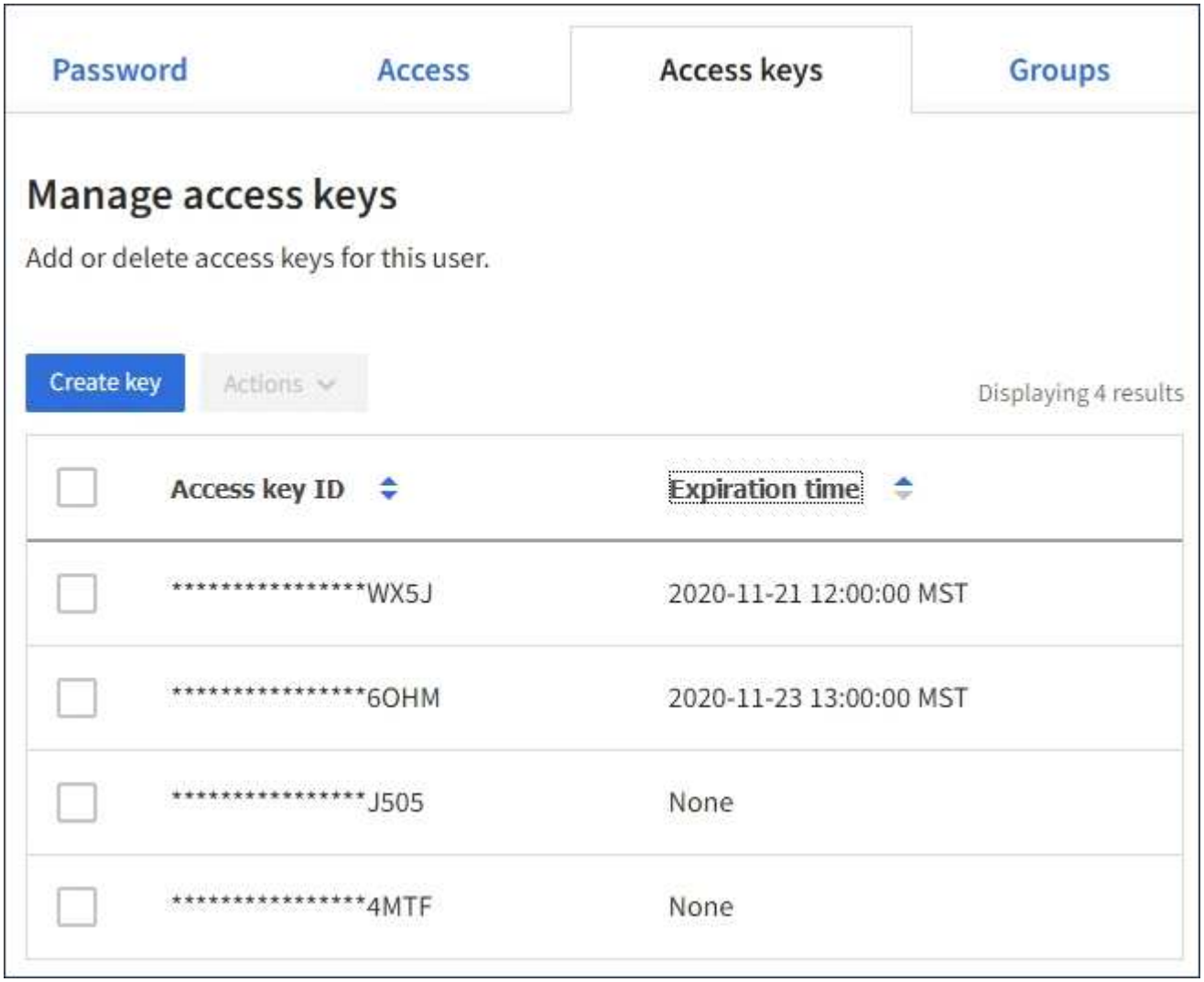
1. 액세스 관리 * > * 사용자 * 를 선택합니다.

   사용자 페이지가 나타나고 기존 사용자가 나열됩니다.

2. S3 액세스 키를 보려는 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택합니다.



4. 키를 * Expiration Time * 또는 * Access key ID * 로 정렬합니다.

5. 필요에 따라 새 키를 생성하고 에서 더 이상 사용하지 않는 키를 수동으로 삭제합니다.

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

   만료된 키는 자동으로 제거됩니다.

관련 정보

다른 사용자의 S3 액세스 키를 생성합니다

다른 사용자의 S3 액세스 키를 삭제합니다

다른 사용자의 **S3** 액세스 키를 삭제합니다

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

필요한 것

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

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

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.

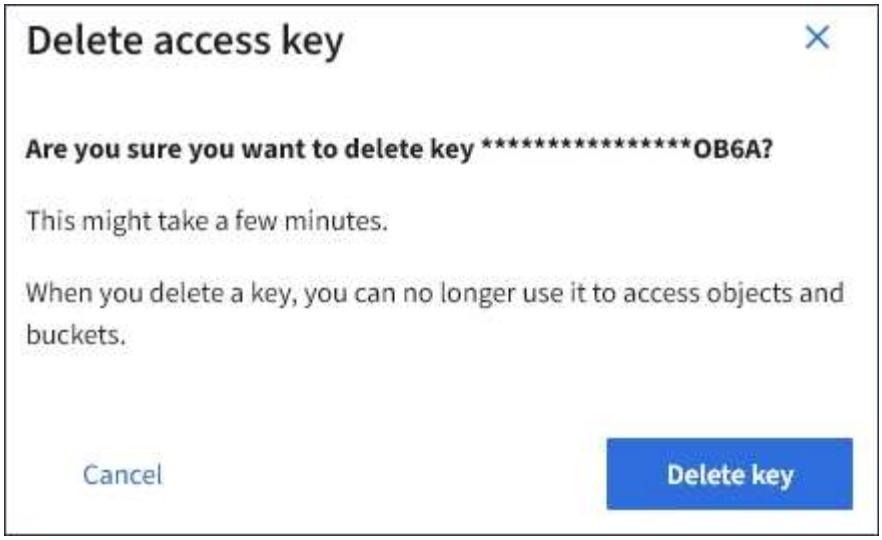
   사용자 페이지가 나타나고 기존 사용자가 나열됩니다.

2. S3 액세스 키를 관리할 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

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

   확인 대화 상자가 나타납니다.



5. Delete key * 를 선택합니다.

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

S3 버킷을 관리합니다

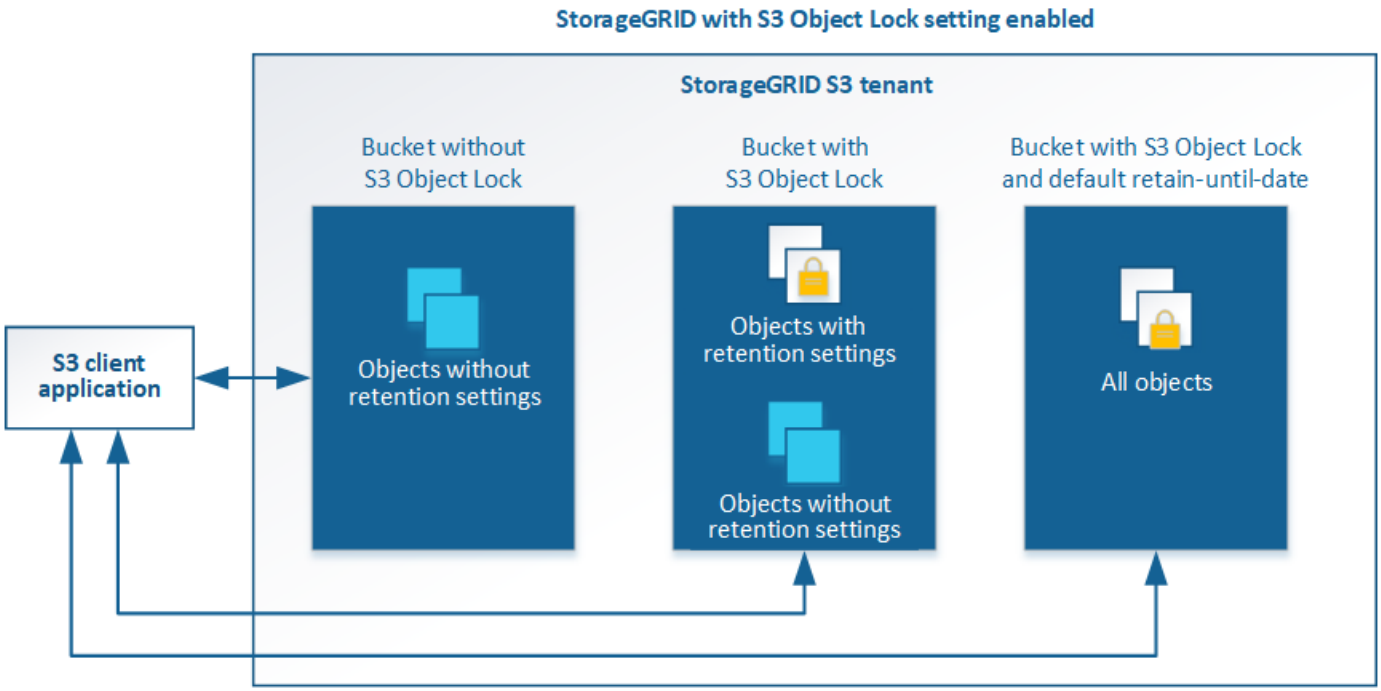
테넌트에 S3 오브젝트 잠금을 사용합니다

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

S3 오브젝트 잠금이란 무엇입니까?

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

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



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

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

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

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

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

레거시 준수 버킷을 관리합니다

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

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

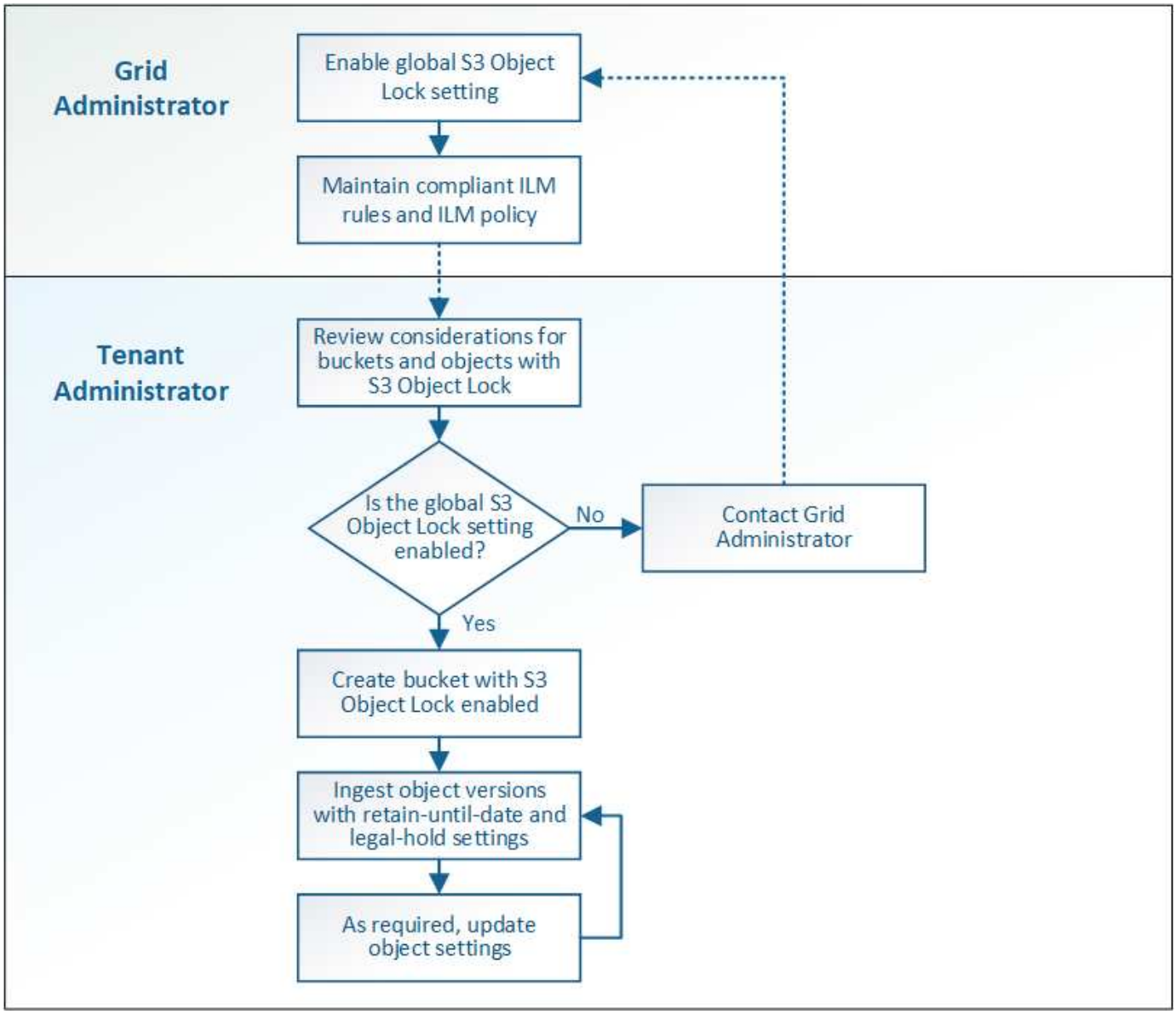
S3 오브젝트 잠금 워크플로

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

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

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

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



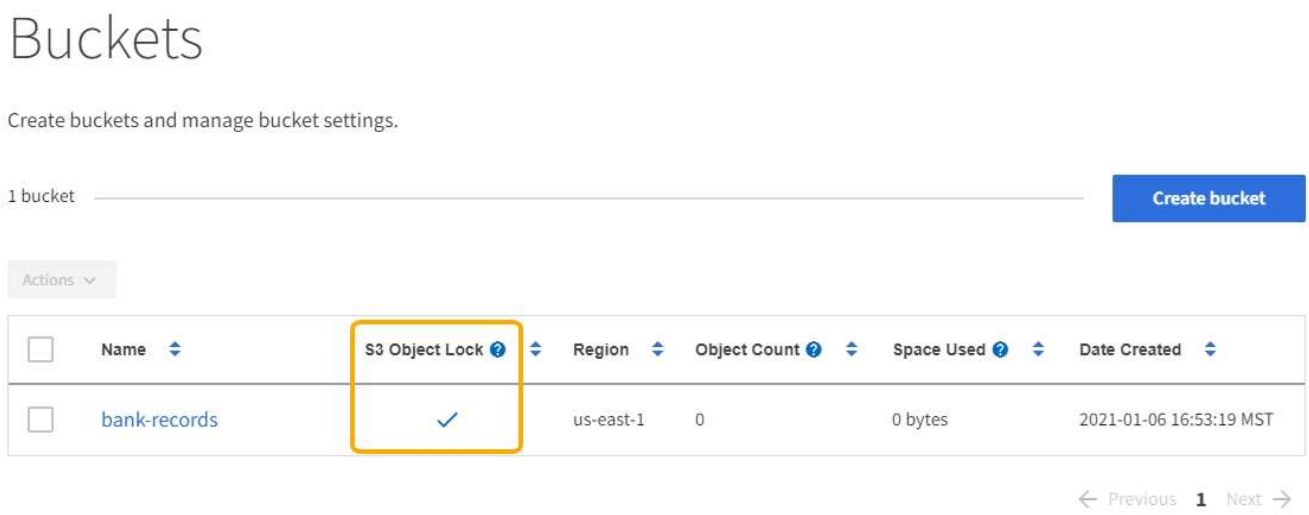
S3 오브젝트 잠금에 대한 요구사항

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

S3 오브젝트 잠금이 설정된 버킷의 요구 사항

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

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



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

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

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

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 라이프사이클

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

1. * 오브젝트 수집 *
    - S3 오브젝트 잠금이 설정된 버킷에 오브젝트 버전을 추가할 경우 S3 클라이언트 애플리케이션이 오브젝트에 대한 보존 설정을 선택적으로 지정할 수 있습니다(보존 기한, 법적 보류 또는 둘 다). 그런 다음 StorageGRID에서는 해당 개체의 메타데이터를 생성하며 고유한 UUID(Object Identifier)와 수집 날짜 및

시간이 포함됩니다.

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

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

S3 버킷을 생성합니다

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

필요한 것

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

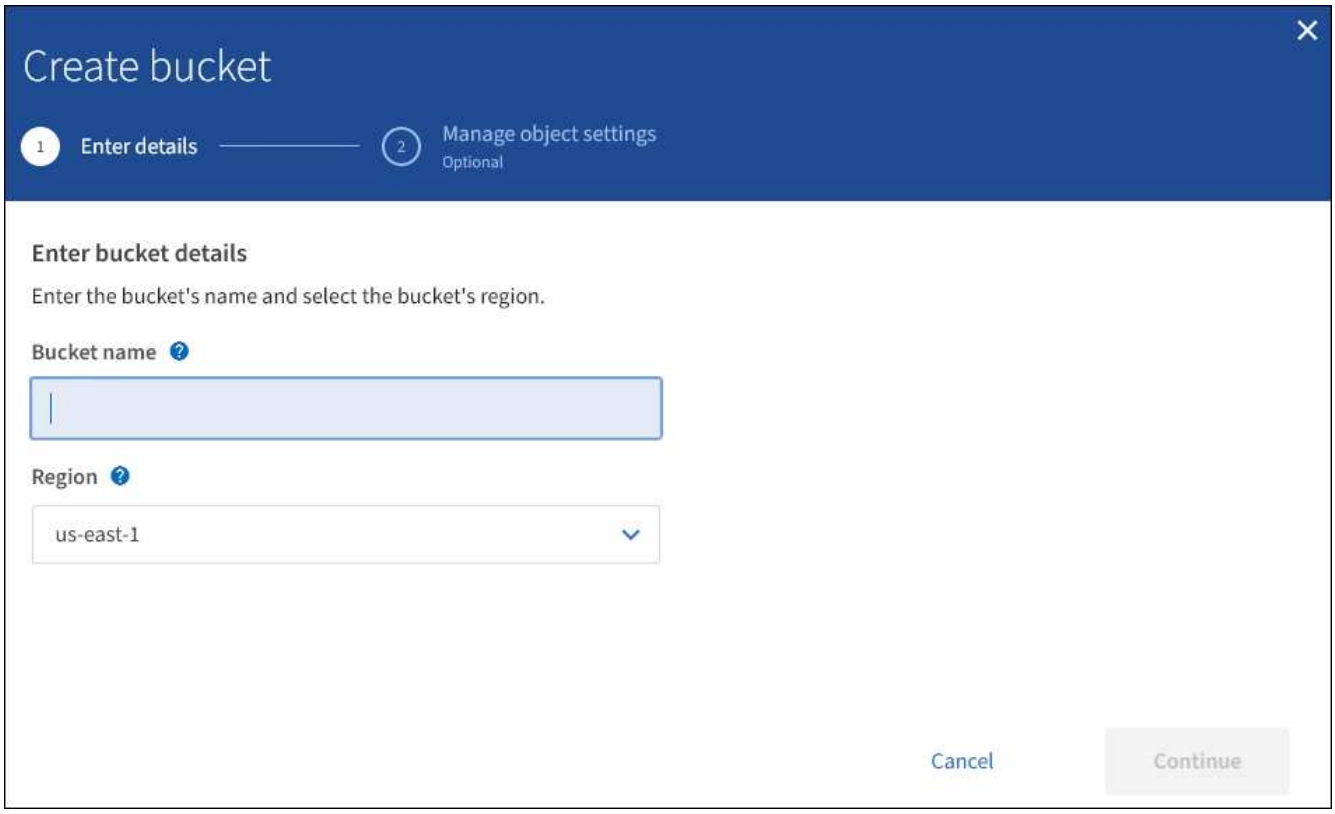
> 에서 버킷 또는 오브젝트의 S3 오브젝트 잠금 속성을 설정하거나 수정하는 권한을 부여할 수 있습니다 버킷 정책 또는 그룹 정책.

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

  S3 오브젝트 잠금을 사용합니다

단계

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



3. 버킷의 고유한 이름을 입력하십시오.

   버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

   버킷 이름은 다음 규칙을 준수해야 합니다.

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

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

4. 이 버킷의 영역을 선택합니다.

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

   버킷을 생성한 후에는 지역을 변경할 수 없습니다.

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

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

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

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

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

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

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

8. Create bucket * 을 선택합니다.

   버킷이 생성되어 버킷 페이지의 테이블에 추가됩니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

테넌트 관리 API 이해

S3을 사용합니다

S3 버킷 세부 정보를 봅니다

테넌트 계정에서 버킷 및 버킷 설정 목록을 볼 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 테넌트 계정에 대한 모든 버킷이 나열됩니다.

2. 각 버킷에 대한 정보를 검토합니다.

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

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

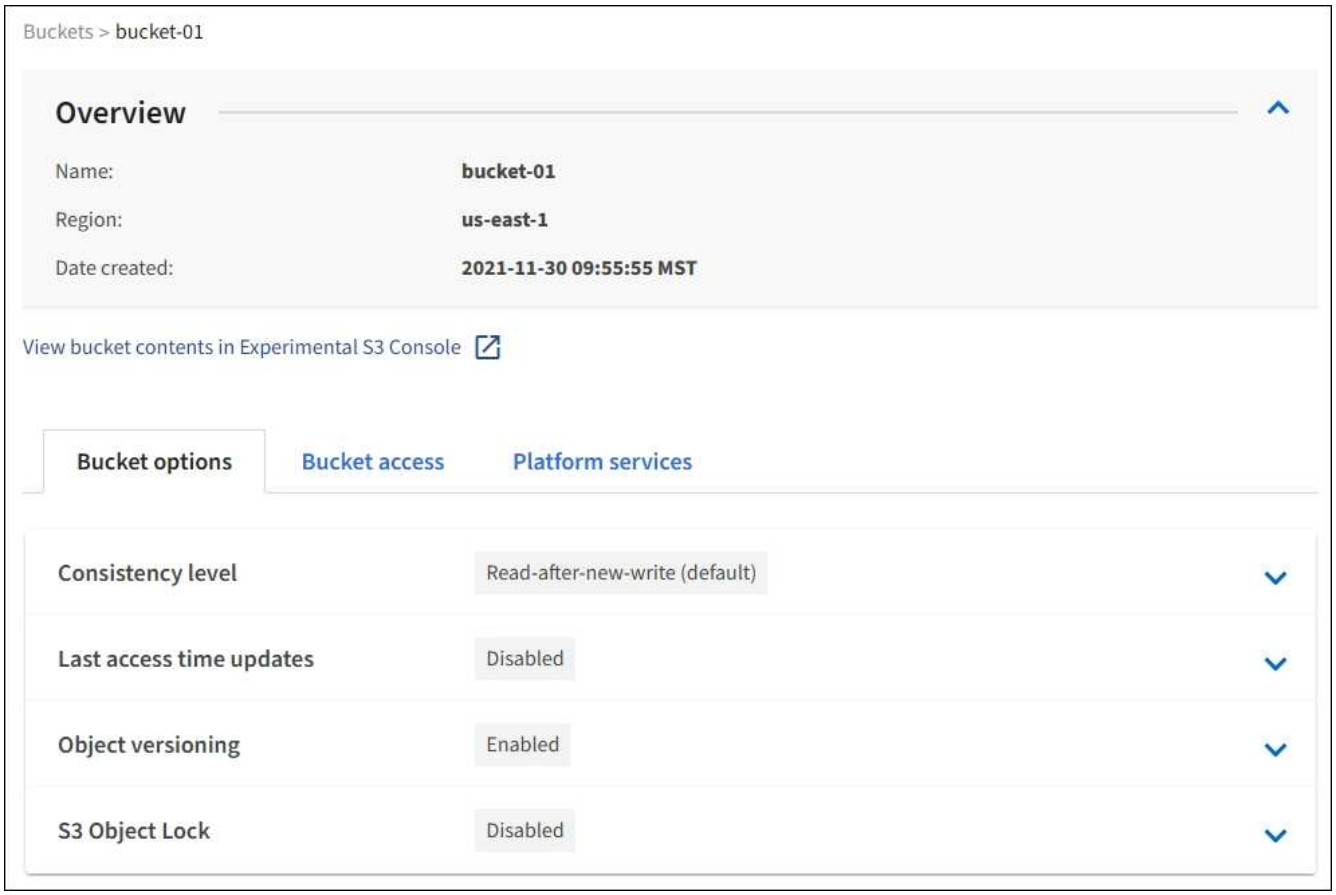
     전역 S3 오브젝트 잠금 설정이 비활성화된 경우 이 열은 표시되지 않습니다. 또한 이 열에는 레거시 준수 버킷에 대한 정보도 표시됩니다.

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

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

3. 버킷의 설정을 보고 관리하려면 버킷 이름을 선택합니다.

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



정합성 보장 수준을 변경합니다

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

필요한 것

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

이 작업에 대해

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

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

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

단계

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

버킷 세부 정보 페이지가 나타납니다.

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

마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다

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

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

필요한 것

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

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

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

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

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

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

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

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

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

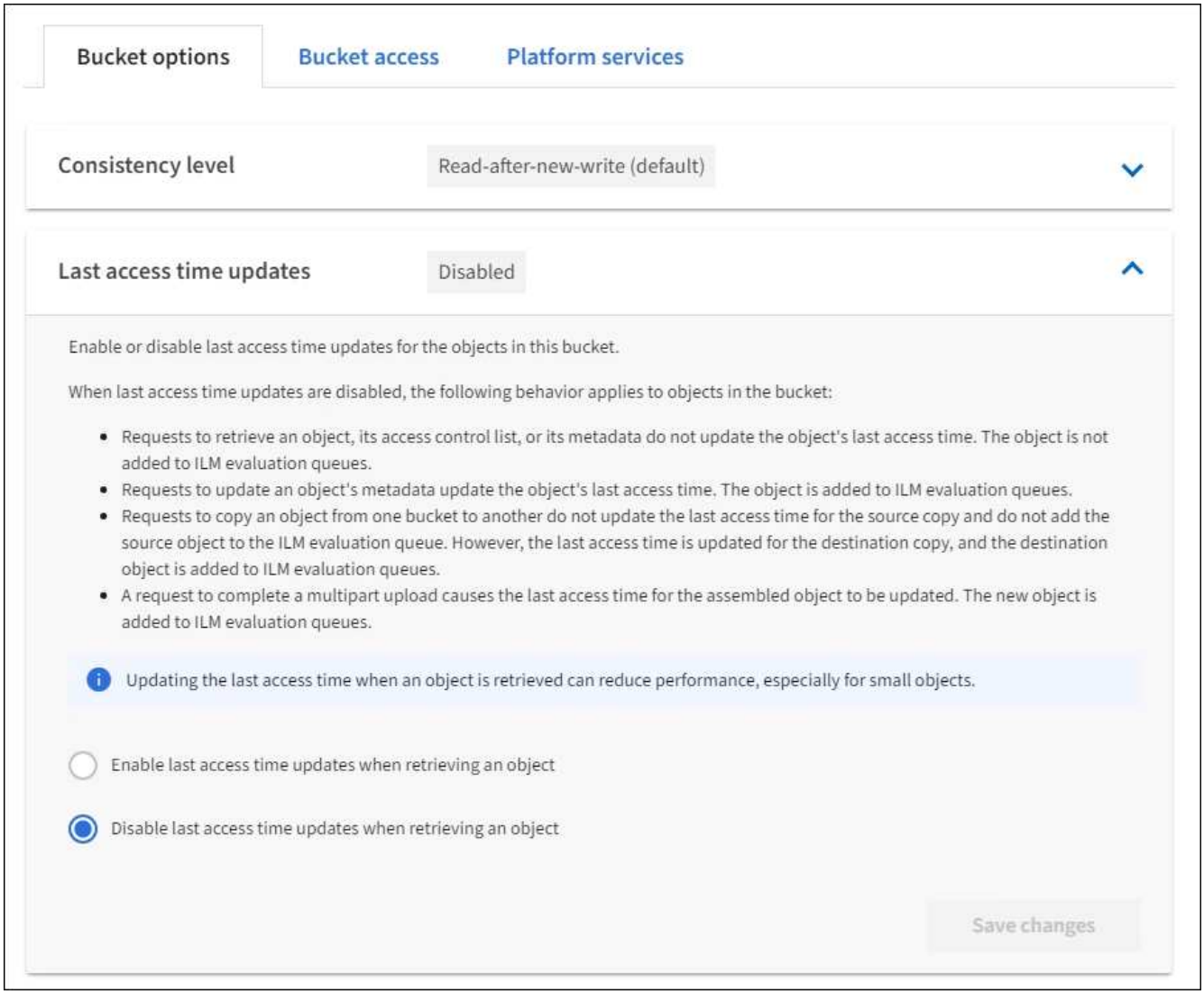
요청 유형입니다	마지막 액세스 시간이 비활성화된 경우의 동작(기본값)		마지막 액세스 시간이 설정된 경우의 동작	
	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?
개체, 해당 액세스 제어 목록 또는 해당 메타데이터를 검색하는 요청입니다	아니요	아니요	예	예
개체의 메타데이터를 업데이트하도록 요청합니다	예	예	예	예
한 버킷에서 다른 버킷으로 오브젝트 복사 요청	• 아니요, 소스 복제본입니다 • 예, 대상 복사본에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

단계

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

   버킷 세부 정보 페이지가 나타납니다.

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



5. 변경 내용 저장 * 을 선택합니다.

관련 정보

테넌트 관리 권한

ILM을 사용하여 개체를 관리합니다

버킷의 오브젝트 버전 관리를 변경합니다

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

필요한 것

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

  테넌트 관리 권한

이 작업에 대해

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

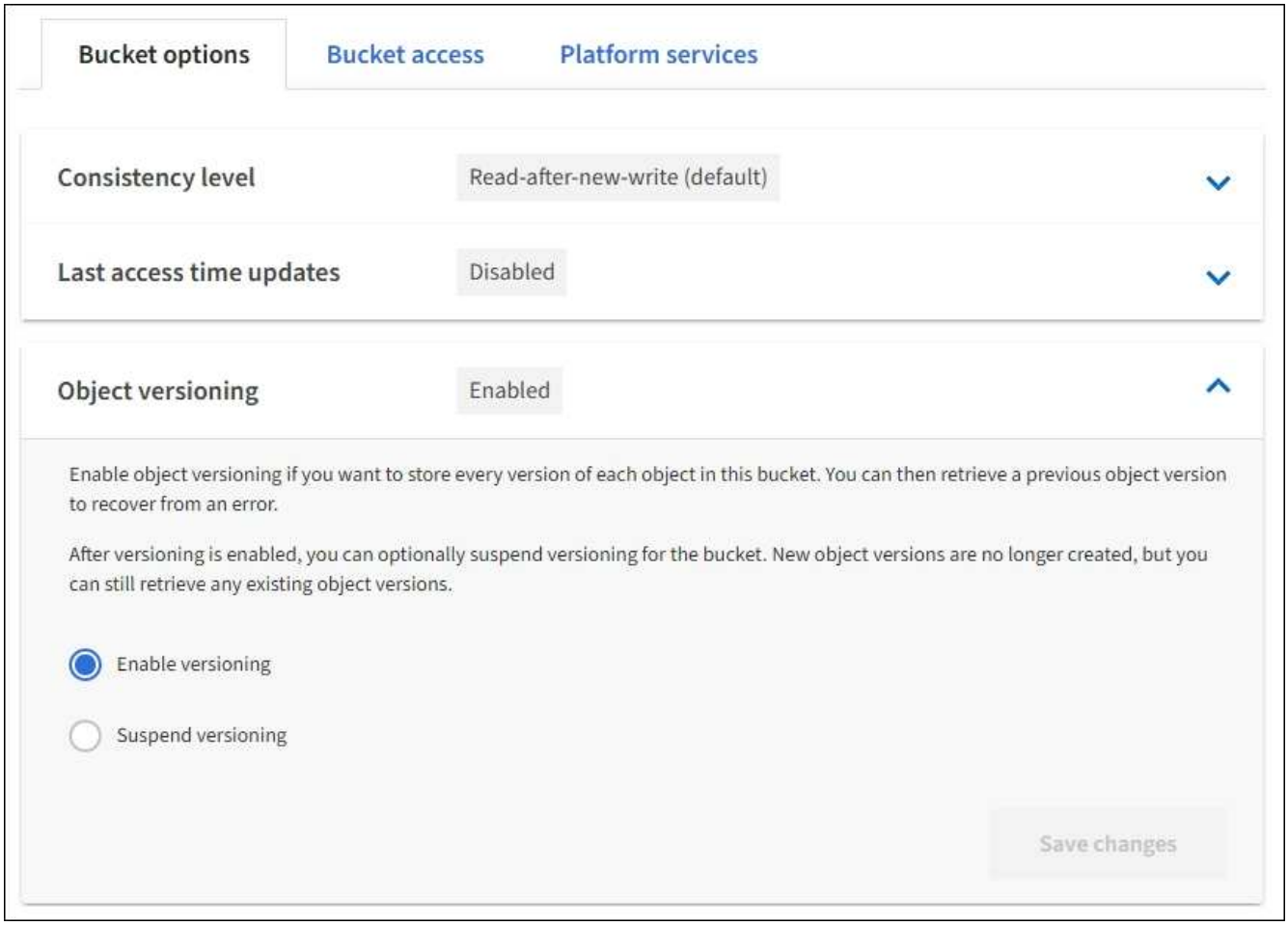
- 사용 안 함: 버전 관리가 활성화되지 않았습니다
- 사용: 버전 관리가 활성화됩니다
- 일시 중단됨: 버전 관리가 이전에 활성화되었으며 일시 중단되었습니다

S3 오브젝트 버전 관리

S3 버전 오브젝트 ILM 규칙 및 정책(예 4)

단계

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



4. 이 버킷의 오브젝트에 대한 버전 관리 상태를 선택합니다.

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

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

5. 변경 내용 저장 * 을 선택합니다.

CORS(Cross-Origin Resource Sharing) 구성

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

필요한 것

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

이 작업에 대해

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

단계

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

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

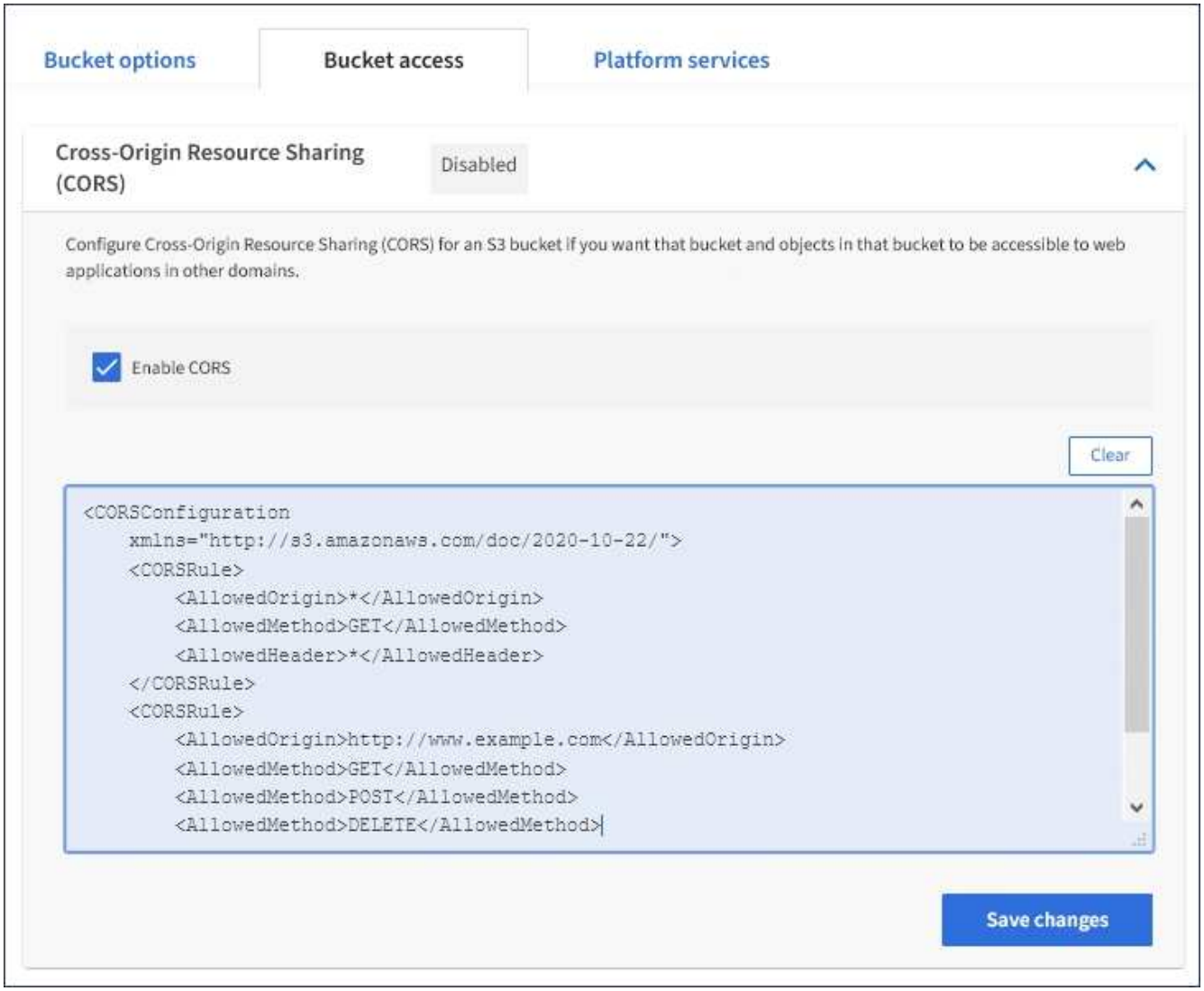
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>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

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

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

   버킷 세부 정보 페이지가 나타납니다.

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



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

S3 버킷을 삭제합니다

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

필요한 것

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

이 작업에 대해

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

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

단계

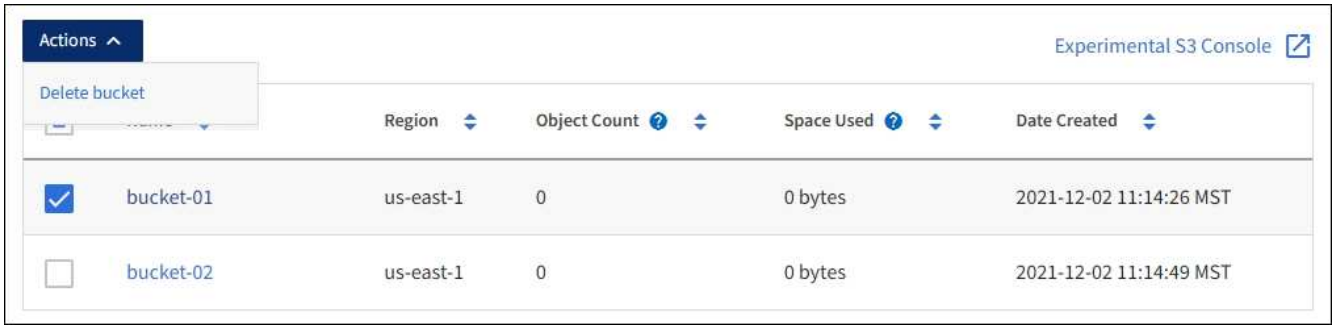
1. 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 기존의 모든 S3 버킷을 표시합니다.

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

   작업 메뉴가 활성화됩니다.

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



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

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

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

Experimental S3 Console을 사용합니다

S3 콘솔을 사용하여 S3 버킷의 오브젝트를 볼 수 있습니다.

S3 콘솔을 사용하여 다음을 수행할 수도 있습니다.

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

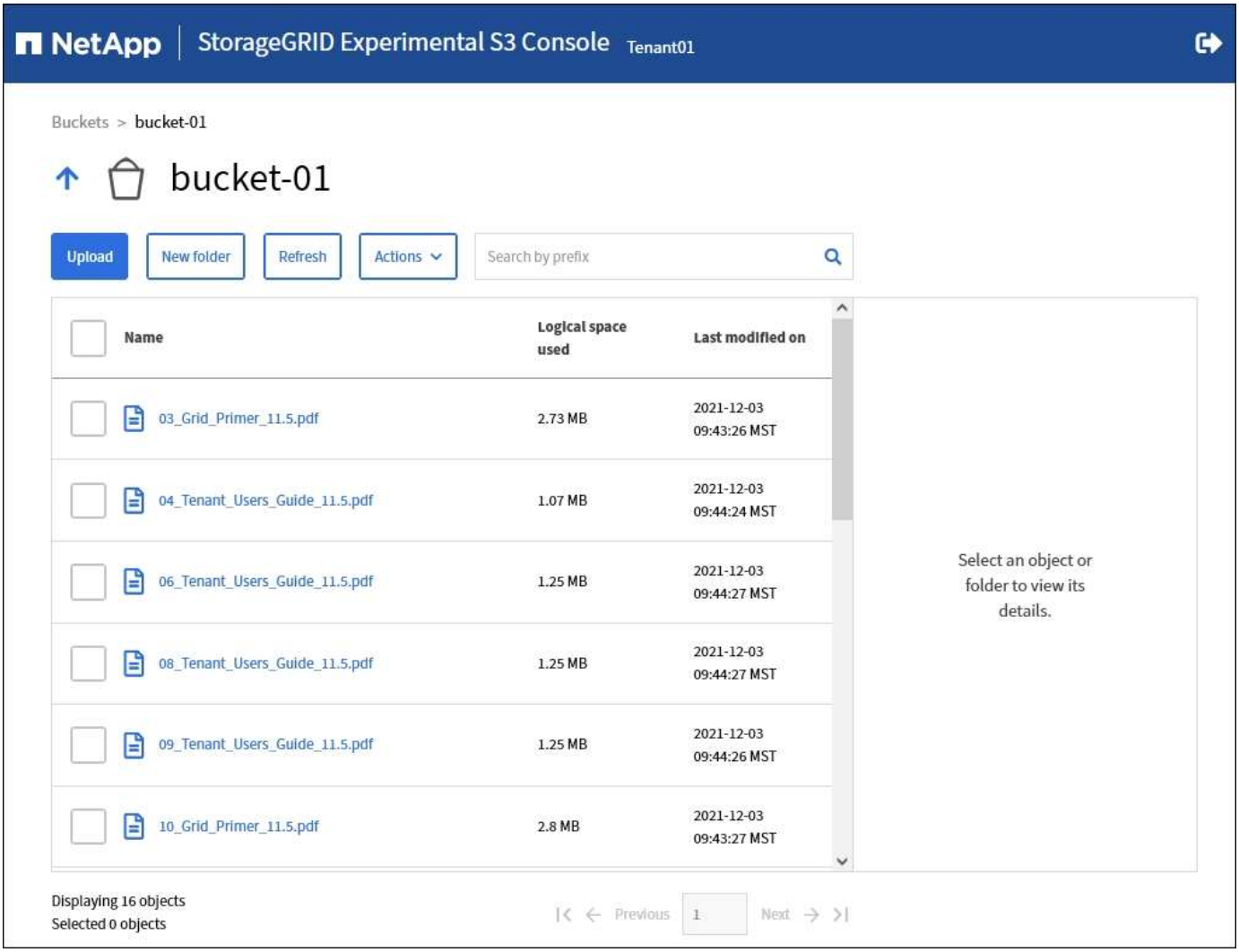
> S3 콘솔이 완전히 테스트되지 않았으며 "Experimental(실험)"으로 표시됩니다. 대량의 오브젝트 관리 또는 운영 환경에서 사용하기 위한 것이 아닙니다. 테넌트는 새로운 ILM 정책을 시뮬레이션하기 위해 개체를 업로드할 때, 수집 문제 해결 또는 개념 증명 또는 비운영 그리드를 사용하는 경우와 같이 소수의 개체에 대한 기능을 수행할 때만 S3 콘솔을 사용해야 합니다.

필요한 것

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

단계

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


NetApp
StorageGRID Experimental S3 Console
Tenant01
Buckets > bucket-01
bucket-01
Upload
New folder
Refresh
Actions
Search by prefix
Name
Logical space used
Last modified on
03_Grid_Primer_11.5.pdf
2.73 MB
2021-12-03 09:43:26 MST
04_Tenant_Users_Guide_11.5.pdf
1.07 MB
2021-12-03 09:44:24 MST
06_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
08_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
09_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:26 MST
10_Grid_Primer_11.5.pdf
2.8 MB
2021-12-03 09:43:27 MST
Select an object or folder to view its details.
Displaying 16 objects
Selected 0 objects
Previous
1
Next