# S3 액세스 키 관리

StorageGRID software

NetApp
July 23, 2026

# 목차

# 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.