



# 테넌트 그룹을 관리합니다

## StorageGRID 11.7

NetApp  
April 12, 2024

# 목차

테넌트 그룹을 관리합니다.....	1
S3 테넌트에 대한 그룹을 생성합니다 .....	1
Swift 테넌트의 그룹을 생성합니다.....	4
테넌트 관리 권한 .....	5
그룹을 관리합니다 .....	6

# 테넌트 그룹을 관리합니다

## S3 테넌트에 대한 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹에 대한 권한을 관리할 수 있습니다.

시작하기 전에

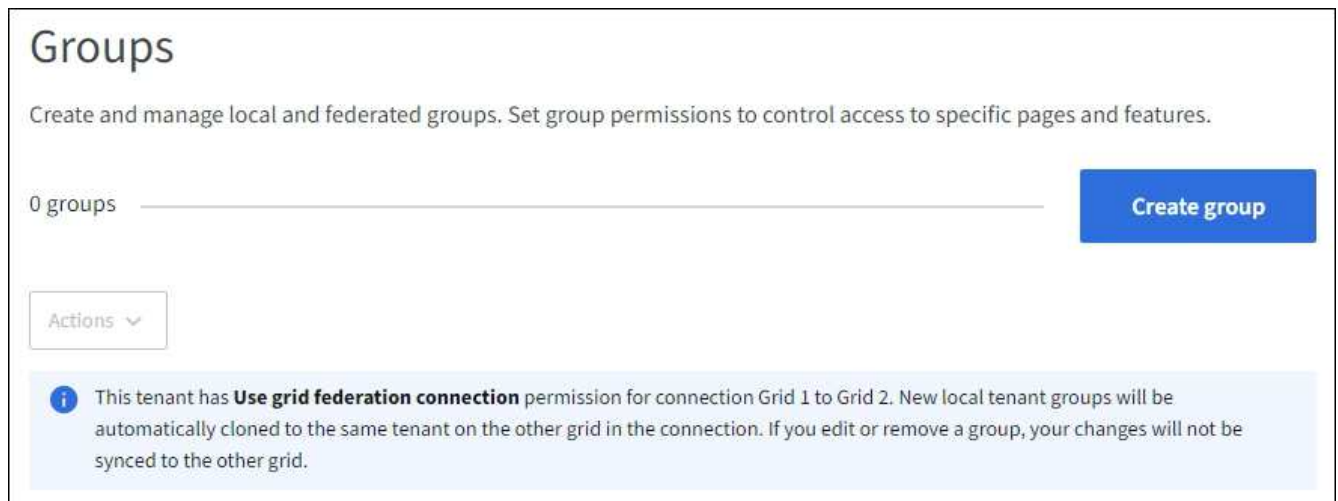
- 를 사용하여 테넌트 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 이 있는 사용자 그룹에 속해 있습니다 ["루트 액세스 권한"](#).
- 통합 그룹을 가져올 계획이라면 이 있습니다 ["ID 페더레이션을 구성했습니다"](#), 및 통합 그룹이 이미 구성된 ID 소스에 있습니다.
- 테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있는 경우 에 대한 워크플로와 고려 사항을 검토했습니다 ["테넌트 그룹 및 사용자를 클론 생성합니다"](#)를 클릭합니다. 그러면 테넌트의 소스 그리드에 로그인됩니다.

### 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 그리드에 생성된 새 그룹이 연결의 다른 그리드에 있는 동일한 테넌트에 복제됨을 나타내는 파란색 배너가 나타나는지 확인합니다. 이 배너가 나타나지 않으면 테넌트의 대상 그리드에 로그인되었을 수 있습니다.



3. Create group \* 을 선택합니다.

### 그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

단계

1. 로컬 그룹을 생성하려면 \* Local group \* 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 \* Federated group \* 탭을 선택합니다.

StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

2. 그룹의 이름을 입력합니다.

- \* 로컬 그룹 \*: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.



테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있는 경우 대상 그리드에 해당 테넌트에 대해 동일한 \* 고유 이름 \* 이 이미 있으면 클론 생성 오류가 발생합니다.

- \* 페더레이션 그룹 \*: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 에 연결된 이름입니다 sAMAccountName 속성. OpenLDAP의 경우 고유한 이름은 에 연결된 이름입니다 uid 속성.

3. Continue \* 를 선택합니다.

## 그룹 권한을 관리합니다

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

단계

1. 액세스 모드 \* 의 경우 다음 중 하나를 선택합니다.

- \* 읽기-쓰기 \* (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
- \* 읽기 전용 \*: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.



사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

2. 이 그룹에 대한 권한을 하나 이상 선택합니다.

을 참조하십시오 "테넌트 관리 권한".

3. Continue \* 를 선택합니다.

## S3 그룹 정책을 설정합니다

그룹 정책은 사용자가 가질 S3 액세스 권한을 결정합니다.

단계

1. 이 그룹에 사용할 정책을 선택합니다.

그룹 정책	설명
S3 액세스 없음	기본값. 버킷 정책을 통해 액세스 권한이 부여되지 않은 한 이 그룹의 사용자는 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.

그룹 정책	설명
읽기 전용 액세스	이 그룹의 사용자는 S3 리소스에 읽기 전용 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열을 편집할 수 없습니다.
전체 액세스	이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열을 편집할 수 없습니다.
랜섬웨어 완화	이 샘플 정책은 이 테넌트의 모든 버킷에 적용됩니다. 이 그룹의 사용자는 일반적인 작업을 수행할 수 있지만 개체 버전 관리가 활성화된 버킷에서 개체를 영구적으로 삭제할 수는 없습니다.  Manage All Bucket * 권한이 있는 테넌트 관리자 사용자는 이 그룹 정책을 재정의할 수 있습니다. 모든 버킷 관리 권한을 신뢰할 수 있는 사용자로 제한하고 가능한 경우 MFA(Multi-Factor Authentication)를 사용합니다.
맞춤형	그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다.

2. 사용자 정의 \* 를 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책은 크기 제한이 5,120바이트입니다. 올바른 JSON 형식 문자열을 입력해야 합니다.

언어 구문 및 예제를 비롯한 그룹 정책에 대한 자세한 내용은 을 참조하십시오 "[그룹 정책의 예](#)".

3. 로컬 그룹을 만드는 경우 \* 계속 \* 을 선택합니다. 통합 그룹을 만드는 경우 \* 그룹 생성 \* 및 \* 마침 \* 을 선택합니다.

## 사용자 추가(로컬 그룹만 해당)

사용자를 추가하지 않고 그룹을 저장하거나 이미 존재하는 로컬 사용자를 선택적으로 추가할 수 있습니다.



테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있는 경우 소스 그리드에 로컬 그룹을 생성할 때 선택한 모든 사용자는 대상 그리드에 그룹이 클론 생성될 때 포함되지 않습니다. 따라서 그룹을 만들 때 사용자를 선택하지 마십시오. 대신 사용자를 생성할 때 그룹을 선택합니다.

### 단계

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.
2. Create group \* 과 \* Finish \* 를 선택합니다.

생성한 그룹이 그룹 목록에 나타납니다.

테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있고 테넌트의 소스 그리드에 있는 경우 새 그룹이 테넌트의 대상 그리드에 복제됩니다. \* 성공 \* 은 그룹 세부 정보 페이지의 개요 섹션에 \* 클론 생성 상태 \* 로 표시됩니다.

# Swift 테넌트의 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 Swift 테넌트 계정에 대한 액세스 권한을 관리할 수 있습니다. 하나 이상의 그룹에 Swift 관리자 권한이 있어야 합니다. 이 권한은 Swift 테넌트 계정의 컨테이너 및 개체를 관리하는 데 필요합니다.



Swift 클라이언트 응용 프로그램에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 이 있는 사용자 그룹에 속해 있습니다 "[루트 액세스 권한](#)".
- 통합 그룹을 가져올 계획이라면 이 있습니다 "[ID 페더레이션을 구성했습니다](#)", 및 통합 그룹이 이미 구성된 ID 소스에 있습니다.

## 그룹 생성 마법사에 액세스합니다

단계

첫 번째 단계로 그룹 생성 마법사에 액세스합니다.

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
2. Create group \* 을 선택합니다.

## 그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

단계

1. 로컬 그룹을 생성하려면 \* Local group \* 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 \* Federated group \* 탭을 선택합니다.

StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

2. 그룹의 이름을 입력합니다.
  - \* 로컬 그룹 \*: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
  - \* 페더레이션 그룹 \*: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 에 연결된 이름입니다 sAMAccountName 속성. OpenLDAP의 경우 고유한 이름은 에 연결된 이름입니다 uid 속성.
3. Continue \* 를 선택합니다.

## 그룹 권한을 관리합니다

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

단계

1. 액세스 모드 \* 의 경우 다음 중 하나를 선택합니다.

- \* 읽기-쓰기 \* (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
- \* 읽기 전용 \*: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.



사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

2. 그룹 사용자가 테넌트 관리자 또는 테넌트 관리 API에 로그인해야 하는 경우 \* Root access \* 확인란을 선택합니다.

3. Continue \* 를 선택합니다.

## Swift 그룹 정책을 설정합니다

Swift 사용자는 컨테이너를 생성하고 오브젝트를 수집하려면 Swift REST API에 인증하는 관리자 권한이 필요합니다.

1. 그룹 사용자가 Swift REST API를 사용하여 컨테이너 및 객체를 관리해야 하는 경우 \* Swift administrator \* 확인란을 선택합니다.
2. 로컬 그룹을 만드는 경우 \* 계속 \* 을 선택합니다. 통합 그룹을 만드는 경우 \* 그룹 생성 \* 및 \* 마침 \* 을 선택합니다.

## 사용자 추가(로컬 그룹만 해당)

사용자를 추가하지 않고 그룹을 저장하거나 이미 존재하는 로컬 사용자를 선택적으로 추가할 수 있습니다.

단계

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.

아직 로컬 사용자를 만들지 않은 경우 사용자 페이지에서 이 그룹을 사용자에게 추가할 수 있습니다. 을 참조하십시오 "[로컬 사용자를 관리합니다](#)".

2. Create group \* 과 \* Finish \* 를 선택합니다.

생성한 그룹이 그룹 목록에 나타납니다.

## 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 사용자가 하나 이상의 권한이 있는 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 설정과 기능만 볼 수 있는지 여부를 결정합니다.



사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

그룹에 다음 권한을 할당할 수 있습니다. S3 테넌트와 Swift 테넌트는 다른 그룹 권한을 가집니다.

권한	설명
루트 액세스	<p>테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다.</p> <ul style="list-style-type: none"> <li>참고: * Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.</li> </ul>
관리자	<p>Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다</p> <ul style="list-style-type: none"> <li>참고: * Swift 사용자는 Swift REST API를 사용하여 모든 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.</li> </ul>
자체 S3 자격 증명을 관리합니다	<p>사용자가 자신의 S3 액세스 키를 생성하고 제거할 수 있습니다. 이 권한이 없는 사용자는 * storage(S3) * &gt; * My S3 access keys * 메뉴 옵션을 볼 수 없습니다.</p>
모든 버킷을 관리합니다	<ul style="list-style-type: none"> <li>S3 테넌트: 사용자가 테넌트 관리자 및 테넌트 관리 API를 사용하여 S3 버킷을 생성 및 삭제하고 S3 버킷 또는 그룹 정책에 관계없이 테넌트 계정의 모든 S3 버킷을 관리할 수 있습니다.</li> <li>이 권한이 없는 사용자는 * Bucket * 메뉴 옵션이 표시되지 않습니다.</li> <li>Swift 테넌트: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 정합성 수준을 제어할 수 있습니다.</li> <li>참고: * 테넌트 관리 API에서 Swift 그룹에 모든 버킷 관리 권한만 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.</li> </ul>
엔드포인트 관리	<p>사용자가 테넌트 관리자 또는 테넌트 관리 API를 사용하여 플랫폼 서비스 엔드포인트를 생성하거나 편집할 수 있습니다. 이 엔드포인트는 StorageGRID 플랫폼 서비스의 대상으로 사용됩니다.</p> <p>이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션이 표시되지 않습니다.</p>
S3 콘솔을 통해 오브젝트 관리	<p>Manage All Bucket(모든 버킷 관리) 권한과 함께 사용하면 사용자가 Bucket(버킷) 페이지에서 실험 S3 콘솔에 액세스할 수 있습니다. 이 권한이 있지만 모든 버킷 관리 권한이 없는 사용자는 여전히 실험 S3 콘솔로 직접 이동할 수 있습니다.</p>

## 그룹을 관리합니다

그룹을 보고, 그룹의 이름, 권한, 정책 및 사용자를 편집하고, 그룹을 복제할 수 있습니다. 또는



## 그룹을 삭제합니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 이 있는 사용자 그룹에 속해 있습니다 ["루트 액세스 권한"](#).

## 그룹을 보거나 편집합니다


각 그룹의 기본 정보와 세부 정보를 보고 편집할 수 있습니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
2. 그룹 페이지에 제공된 정보를 검토하여 이 테넌트 계정의 모든 로컬 및 통합 그룹에 대한 기본 정보를 나열합니다.

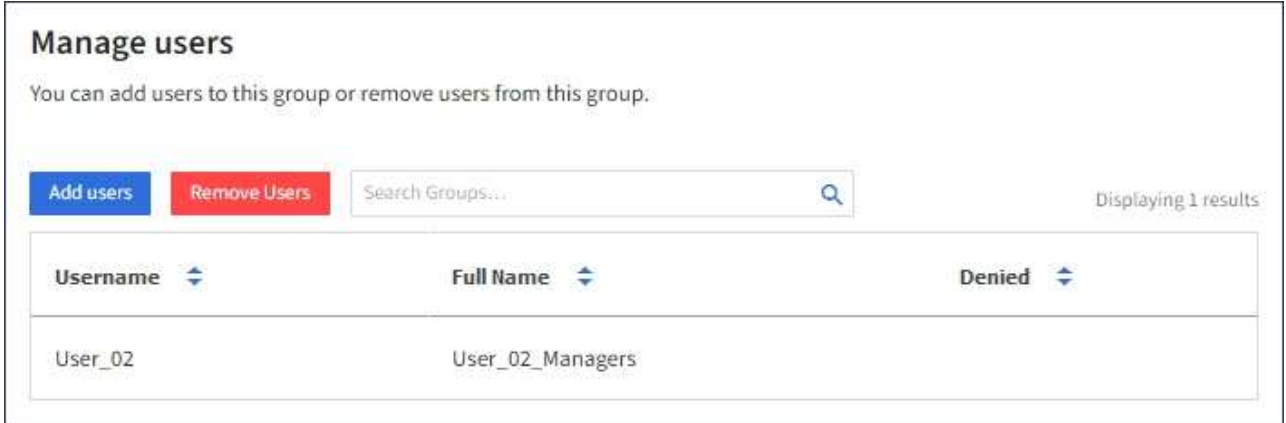
테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있고 테넌트의 소스 격자에서 그룹을 보고 있는 경우 파란색 배너는 그룹을 편집하거나 제거하면 변경 내용이 다른 격자와 동기화되지 않음을 나타냅니다. 을 참조하십시오 ["클론 테넌트 그룹 및 사용자"](#).

3. 그룹 이름을 변경하려면:
  - a. 그룹의 확인란을 선택합니다.
  - b. Actions \* > \* Edit group name \* 을 선택합니다.
  - c. 새 이름을 입력합니다.
  - d. 변경 사항 저장 \* 을 선택합니다
4. 자세한 내용을 보거나 추가로 편집하려면 다음 중 하나를 수행합니다.
  - 그룹 이름을 선택합니다.
  - 그룹의 확인란을 선택하고 \* Actions \* > \* View group details \* 를 선택합니다.
5. 각 그룹에 대해 다음 정보를 보여 주는 개요 섹션을 검토합니다.
  - 표시 이름
  - 고유한 이름입니다
  - 유형
  - 액세스 모드
  - 권한
  - S3 정책
  - 이 그룹의 사용자 수입니다
  - 테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있고 테넌트의 소스 격자에서 그룹을 보고 있는 경우 추가 필드:
    - 복제 상태, \* 성공 \* 또는 \* 실패 \*
    - 이 그룹을 편집하거나 삭제하면 변경 내용이 다른 눈금과 동기화되지 않음을 나타내는 파란색 배너입니다.
6. 필요에 따라 그룹 설정을 편집합니다. 을 참조하십시오 ["S3 테넌트에 대한 그룹을 생성합니다"](#) 및 ["Swift 테넌트의 그룹을 생성합니다"](#) 를 참조하십시오.

- a. 개요 섹션에서 이름 또는 편집 아이콘을 선택하여 표시 이름을 변경합니다 .
- b. 그룹 권한 \* 탭에서 권한을 업데이트하고 \* 변경 사항 저장 \* 을 선택합니다.
- c. 그룹 정책 \* 탭에서 변경을 수행하고 \* 변경 사항 저장 \* 을 선택합니다.
  - S3 그룹을 편집하는 경우 필요에 따라 다른 S3 그룹 정책을 선택하거나 사용자 지정 정책의 JSON 문자열을 입력합니다.
  - Swift 그룹을 편집 중인 경우 \* Swift 관리자 \* 확인란을 선택하거나 선택 취소합니다.

7. 그룹에 기존 로컬 사용자를 하나 이상 추가하려면 다음을 수행합니다.

- a. 사용자 탭을 선택합니다.



- b. 사용자 추가 \* 를 선택합니다.
- c. 추가할 기존 사용자를 선택하고 \* 사용자 추가 \* 를 선택합니다.

오른쪽 위에 성공 메시지가 나타납니다.

8. 그룹에서 로컬 사용자 제거하기:

- a. 사용자 탭을 선택합니다.
- b. 사용자 제거 \* 를 선택합니다.
- c. 제거할 사용자를 선택하고 \* 사용자 제거 \* 를 선택합니다.

오른쪽 위에 성공 메시지가 나타납니다.

9. 변경한 각 섹션에 대해 \* 변경 사항 저장 \* 을 선택했는지 확인합니다.

## 그룹이 중복되었습니다

기존 그룹을 복제하여 새 그룹을 더 빠르게 만들 수 있습니다.



테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있고 테넌트의 소스 그리드에서 그룹을 복제하는 경우 복제된 그룹은 테넌트의 대상 그리드에 복제됩니다.

단계

- 1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
- 2. 복제할 그룹의 확인란을 선택합니다.

3. Actions \* > \* Duplicate group \* 을 선택합니다.
4. 을 참조하십시오 "S3 테넌트에 대한 그룹을 생성합니다" 또는 "Swift 테넌트의 그룹을 생성합니다" 를 참조하십시오.
5. Create group \* 을 선택합니다.

## 하나 이상의 그룹을 삭제합니다

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



테넌트 계정에 \* 그리드 페더레이션 연결 사용 \* 권한이 있고 그룹을 삭제하는 경우 StorageGRID는 다른 그리드에서 해당 그룹을 삭제하지 않습니다. 이 정보를 동기화해야 하는 경우 두 그리드에서 동일한 그룹을 삭제해야 합니다.

### 단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
2. 삭제할 각 그룹의 확인란을 선택합니다.
3. Actions \* > \* Delete group \* 또는 \* Actions \* > \* Delete groups \* 를 선택합니다.

확인 대화 상자가 나타납니다.

4. 그룹 삭제 \* 또는 \* 그룹 삭제 \* 를 선택합니다.

## 저작권 정보

Copyright © 2024 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.