



# 그룹 관리

## StorageGRID 11.5

NetApp  
April 11, 2024

# 목차

그룹 관리	1
테넌트 관리 권한	1
S3 테넌트에 대한 그룹 생성 중	2
Swift 테넌트에 대한 그룹을 생성하는 중입니다	5
그룹 세부 정보 보기 및 편집	7
로컬 그룹에 사용자 추가	9
그룹 이름 편집	11
그룹 복제	12
그룹을 삭제하는 중입니다	13

# 그룹 관리

테넌트 사용자가 수행할 수 있는 작업을 제어하기 위해 사용자 그룹에 권한을 할당합니다. Active Directory 또는 OpenLDAP와 같은 ID 소스에서 통합 그룹을 가져오거나 로컬 그룹을 생성할 수 있습니다.



StorageGRID 시스템에 SSO(Single Sign-On)가 설정되어 있으면 그룹 사용 권한에 따라 S3 및 Swift 리소스에 액세스할 수 있지만 로컬 사용자는 테넌트 관리자에 로그인할 수 없습니다.

## 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. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

권한	설명
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다. <ul style="list-style-type: none"><li>• 참고: * Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.</li></ul>
관리자	Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다. <ul style="list-style-type: none"><li>• 참고: * Swift 사용자는 Swift REST API를 사용하여 모든 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.</li></ul>
자신의 S3 자격 증명을 관리합니다	S3 테넌트만 해당. 사용자가 자신의 S3 액세스 키를 생성하고 제거할 수 있습니다. 이 권한이 없는 사용자는 * storage(S3) * > * My S3 access keys * 메뉴 옵션을 볼 수 없습니다.

권한	설명
모든 버킷 관리	<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> </ul> <p>이 권한이 없는 사용자는 * Bucket * 메뉴 옵션을 볼 수 없습니다.</p> <ul style="list-style-type: none"> <li>• Swift 테넌트: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 정합성 수준을 제어할 수 있습니다.</li> <li>• 참고: * 테넌트 관리 API에서 Swift 그룹에만 모든 버킷 관리 권한을 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.</li> </ul>
엔드포인트 관리	<p>S3 테넌트만 해당. 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID 플랫폼 서비스의 대상으로 사용되는 엔드포인트를 생성하거나 편집할 수 있습니다.</p> <p>이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션을 볼 수 없습니다.</p>

관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

## S3 테넌트에 대한 그룹 생성 중

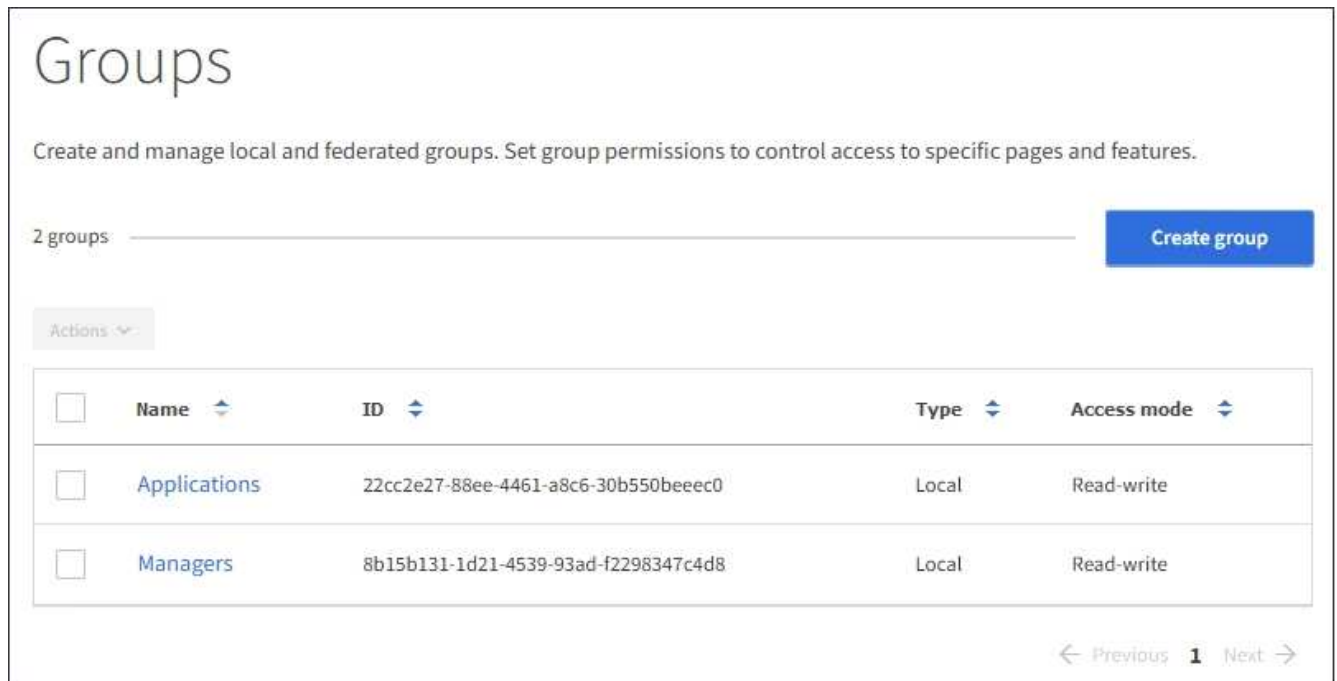
통합 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹에 대한 권한을 관리할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.



2. Create group \* 을 선택합니다.
3. 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.

4. 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.
5. Continue \* 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
  - \* 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.
7. 이 그룹에 대한 그룹 권한을 선택합니다.

테넌트 관리 권한에 대한 정보를 참조하십시오.

8. Continue \* 를 선택합니다.
9. 그룹 정책을 선택하여 이 그룹의 구성원이 가질 S3 액세스 권한을 결정합니다.
  - \* S3 액세스 없음 \*: 기본값. 이 그룹의 사용자는 버킷 정책을 통해 액세스가 부여되지 않는 한 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
  - \* 읽기 전용 액세스 \*: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 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 문자열은 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 문자열은 편집할 수 없습니다.
- \* 사용자 정의 \*: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다. 언어 구문 및 예제를 비롯한 그룹 정책에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

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

이 예제에서 그룹 구성원은 지정된 버킷의 사용자 이름(키 접두사)과 일치하는 폴더만 나열하고 액세스할 수 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.



The screenshot shows the AWS IAM console interface for creating a group policy. On the left, there are four radio button options: 'No S3 Access', 'Read Only Access', 'Full Access', and 'Custom'. The 'Custom' option is selected, with a note below it: '(Must be a valid JSON formatted string.)'. On the right, a text area contains the following JSON policy document:

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

11. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.

- 통합 그룹: \* 그룹 생성 \*
- 로컬 그룹: \* 계속 \*

로컬 그룹을 만드는 경우 \* Continue \* 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

12. 그룹에 추가할 각 사용자에게 대한 확인란을 선택한 다음 \* 그룹 생성 \* 을 선택합니다.

필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 추가할 때 그룹을 선택할 수 있습니다.

13. 마침 \* 을 선택합니다.

생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

["테넌트 관리 권한"](#)

["S3을 사용합니다"](#)

## Swift 테넌트에 대한 그룹을 생성하는 중입니다

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.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.



The screenshot shows a web interface titled "Groups" with the subtitle "Create and manage local and federated groups. Set group permissions to control access to specific pages and features." Below the subtitle, it indicates "2 groups" and has a "Create group" button. An "Actions" dropdown menu is visible. The main content is a table with the following data:

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

At the bottom right of the table, there are navigation arrows: "← Previous 1 Next →".

2. Create group \* 을 선택합니다.
3. 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.

4. 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.
5. Continue \* 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
  - \* 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.
7. 그룹 권한을 설정합니다.
  - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 로그인해야 하는 경우 \* Root Access \* 확인란을 선택합니다. (기본값)
  - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 액세스할 필요가 없는 경우 \* Root Access \* (루트 액세스 \*) 확인란의 선택을 취소합니다. 예를 들어, 테넌트에 액세스할 필요가 없는 응용 프로그램의 확인란을 선택 취소합니다. 그런 다음 이러한 사용자가 컨테이너 및 개체를 관리할 수 있도록 \* Swift 관리자 \* 권한을 할당합니다.
8. Continue \* 를 선택합니다.
9. 사용자가 Swift REST API를 사용할 수 있어야 하는 경우 \* Swift administrator \* 확인란을 선택합니다.
 

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.
10. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.
  - 통합 그룹: \* 그룹 생성 \*
  - 로컬 그룹: \* 계속 \*

로컬 그룹을 만드는 경우 \* Continue \* 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.
11. 그룹에 추가할 각 사용자에게 대한 확인란을 선택한 다음 \* 그룹 생성 \* 을 선택합니다.
 

필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 만들 때 그룹을 선택할 수 있습니다.
12. 마침 \* 을 선택합니다.
 

생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

["테넌트 관리 권한"](#)

["Swift를 사용합니다"](#)



## 그룹 세부 정보 보기 및 편집

그룹의 세부 정보를 볼 때 그룹의 표시 이름, 사용 권한, 정책 및 그룹에 속한 사용자를 변경할 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

### 단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
2. 세부 정보를 보거나 편집할 그룹의 이름을 선택합니다.

또는 \* Actions \* > \* View group details \* 를 선택할 수 있습니다.

그룹 세부 정보 페이지가 나타납니다. 다음 예에서는 S3 그룹 세부 정보 페이지를 보여 줍니다.

## Overview

Display name:	<b>Applications</b> 
Unique name:	<b>group/Applications</b>
Type:	<b>Local</b>
Access mode:	<b>Read-write</b>
Permissions:	<b>Root Access</b>
S3 Policy:	<b>None</b>
Number of users in this group:	<b>0</b>

Group permissions

S3 group policy

Users

## Manage group permissions

Select an access mode for this group and select one or more permissions.

### Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write  Read-only

### Group permissions

Select the tenant account permissions you want to assign to this group.

**Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

**Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

**Manage Endpoints**

Allows users to configure endpoints for platform services.

**Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. 필요에 따라 그룹 설정을 변경합니다.



변경 내용을 저장하려면 각 섹션을 변경한 후 \* 변경 사항 저장 \* 을 선택합니다. 변경 내용이 저장되면 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

a. 선택적으로 표시 이름 또는 편집 아이콘을 선택합니다 표시 이름을 업데이트합니다.

그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

b. 필요에 따라 사용 권한을 업데이트합니다.

c. 그룹 정책의 경우 S3 또는 Swift 테넌트를 적절하게 변경합니다.

- S3 테넌트의 그룹을 편집하는 경우 선택적으로 다른 S3 그룹 정책을 선택합니다. 사용자 지정 S3 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
- Swift 테넌트의 그룹을 편집하는 경우, 필요에 따라 \* Swift 관리자 \* 확인란을 선택하거나 선택 취소합니다.

Swift 관리자 권한에 대한 자세한 내용은 Swift 테넌트에 대한 그룹 생성 지침을 참조하십시오.

d. 필요에 따라 사용자를 추가 또는 제거합니다.

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

캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

["S3 테넌트에 대한 그룹 생성 중"](#)

["Swift 테넌트에 대한 그룹을 생성하는 중입니다"](#)

## 로컬 그룹에 사용자 추가

필요에 따라 로컬 그룹에 사용자를 추가할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.

2. 사용자를 추가할 로컬 그룹의 이름을 선택합니다.

또는 \* Actions \* > \* View group details \* 를 선택할 수 있습니다.

그룹 세부 정보 페이지가 나타납니다.

## Overview

Display name:	<b>Applications</b> 
Unique name:	<b>group/Applications</b>
Type:	<b>Local</b>
Access mode:	<b>Read-write</b>
Permissions:	<b>Root Access</b>
S3 Policy:	<b>None</b>
Number of users in this group:	<b>0</b>

Group permissions

S3 group policy

Users

## Manage group permissions

Select an access mode for this group and select one or more permissions.

### Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write  Read-only

### Group permissions

Select the tenant account permissions you want to assign to this group.

**Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

**Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

**Manage Endpoints**

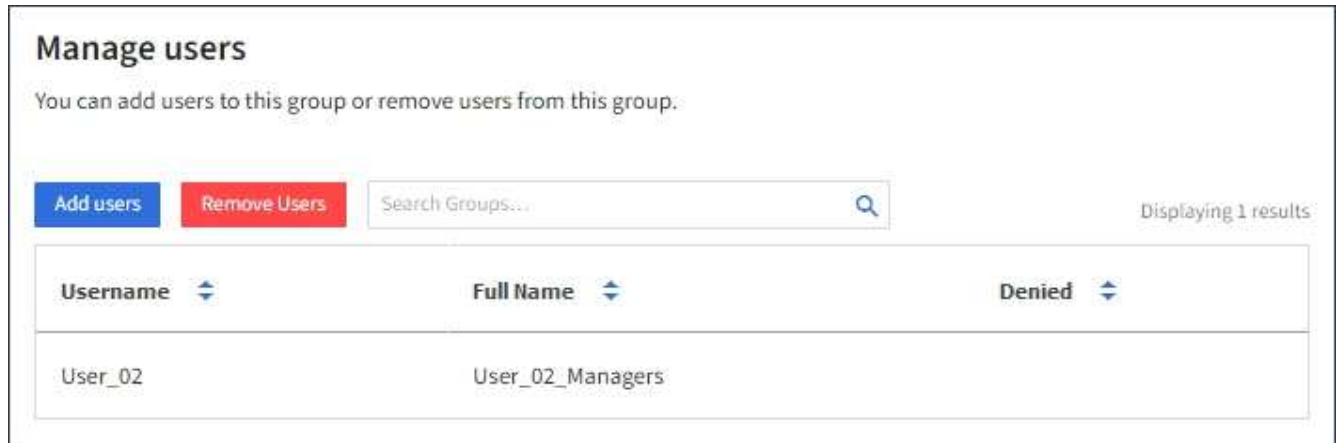
Allows users to configure endpoints for platform services.

**Manage Your Own S3 Credentials**

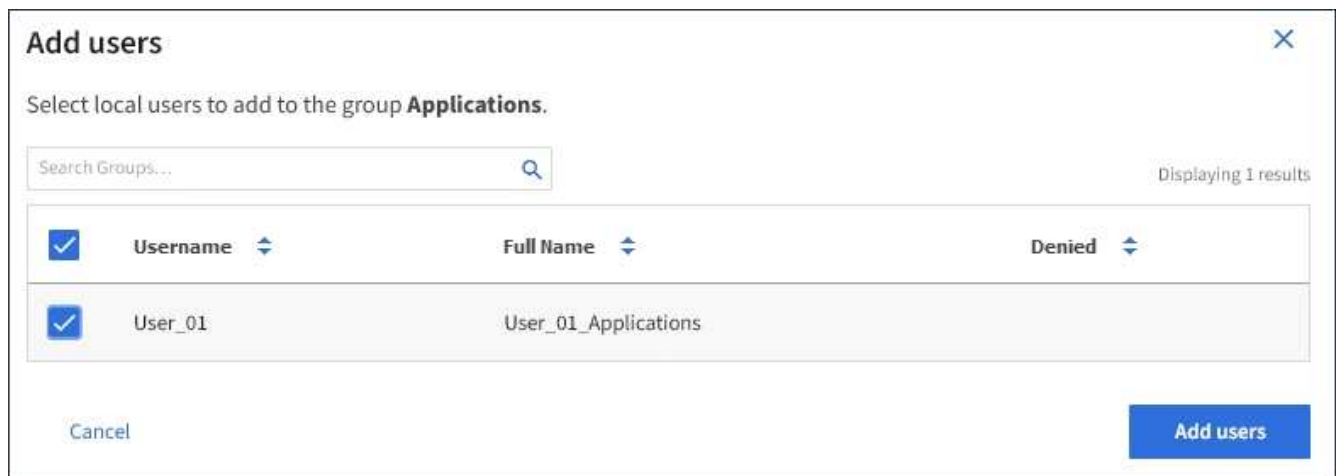
Allows users to create and delete their own S3 access keys.

Save changes

3. 사용자 관리 \* 를 선택한 다음 \* 사용자 추가 \* 를 선택합니다.



4. 그룹에 추가할 사용자를 선택한 다음 \* 사용자 추가 \* 를 선택합니다.



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

## 그룹 이름 편집

그룹의 표시 이름을 편집할 수 있습니다. 그룹의 고유한 이름은 편집할 수 없습니다.

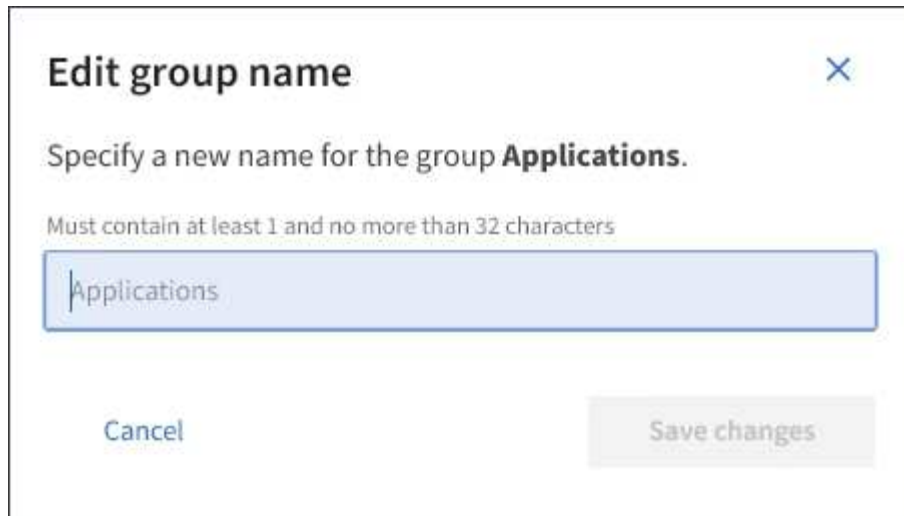
필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
2. 표시 이름을 편집할 그룹의 확인란을 선택합니다.
3. Actions \* > \* Edit group name \* 을 선택합니다.

Edit group name(그룹 이름 편집) 대화 상자가 나타납니다.



4. 로컬 그룹을 편집하는 경우 필요에 따라 표시 이름을 업데이트합니다.

그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

5. 변경 내용 저장 \* 을 선택합니다.

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

관련 정보

["테넌트 관리 권한"](#)

## 그룹 복제

기존 그룹을 복제하면 새 그룹을 더 빠르게 만들 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.
2. 복제할 그룹의 확인란을 선택합니다.
3. Duplicate group \* 을 선택합니다. 그룹을 생성하는 방법에 대한 자세한 내용은 S3 테넌트 또는 Swift 테넌트용 그룹을 생성하는 지침을 참조하십시오.
4. 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.

5. 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.

6. Continue \* 를 선택합니다.
7. 필요에 따라 이 그룹에 대한 권한을 수정합니다.
8. Continue \* 를 선택합니다.
9. 필요에 따라 S3 테넌트에 대한 그룹을 복제할 경우 \* S3 정책 추가 \* 라디오 버튼에서 다른 정책을 선택할 수도 있습니다. 사용자 지정 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
10. Create group \* 을 선택합니다.

관련 정보

["S3 테넌트에 대한 그룹 생성 중"](#)

["Swift 테넌트에 대한 그룹을 생성하는 중입니다"](#)

["테넌트 관리 권한"](#)

## 그룹을 삭제하는 중입니다

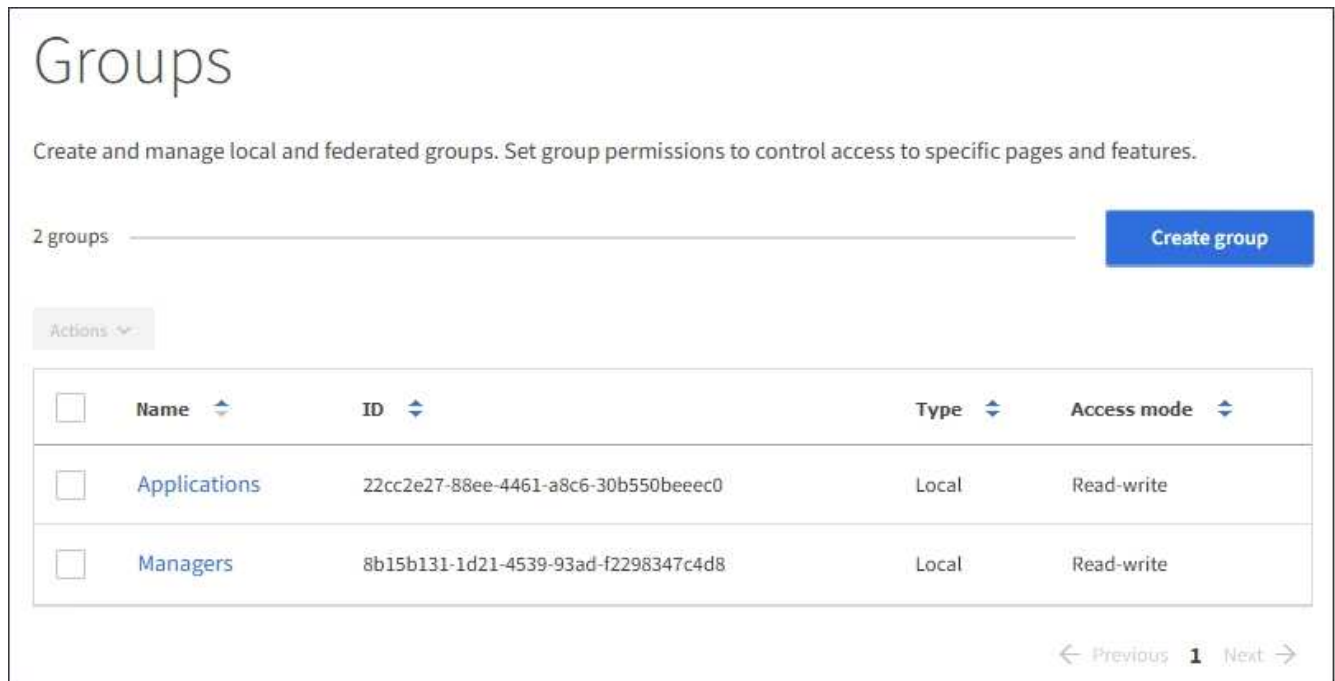
시스템에서 그룹을 삭제할 수 있습니다. 해당 그룹에만 속하는 사용자는 더 이상 테넌트 관리자에 로그인하거나 테넌트 계정을 사용할 수 없습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 \* > \* 그룹 \* 을 선택합니다.



2. 삭제할 그룹의 확인란을 선택합니다.
3. Actions \* > \* Delete group \* 을 선택합니다.

확인 메시지가 나타납니다.

4. 확인 메시지에 표시된 그룹을 삭제하려면 \* Delete group \* 을 선택합니다.

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

관련 정보

["테넌트 관리 권한"](#)



## 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.