



테넌트 그룹 관리

StorageGRID software

NetApp
July 23, 2026

목차

테넌트 그룹 관리	1
StorageGRID에서 S3 테넌트에 대한 그룹 생성	1
그룹 생성 마법사에 액세스합니다.....	1
그룹 유형을 선택합니다	1
그룹 권한 관리.....	2
S3 그룹 정책 설정	2
사용자 추가 (로컬 그룹만 해당).....	3
StorageGRID 테넌트 관리 권한	4
StorageGRID 테넌트 그룹 관리	5
그룹 보기 또는 편집	5
중복 그룹.....	7
그룹 클론 재시도	7
하나 이상의 그룹 삭제	7
AssumeRole 설정	8

테넌트 그룹 관리

StorageGRID에서 S3 테넌트에 대한 그룹 생성

페더레이션 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹의 권한을 관리할 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.
- 연합 그룹을 가져오려는 경우, "[구성된 ID 페더레이션](#)", 해당 연합 그룹이 구성된 ID 소스에 이미 존재합니다.
- 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 워크플로 및 고려 사항을 검토했으며 "[테넌트 그룹 및 사용자 복제](#)", 테넌트의 소스 그리드에 로그인되어 있어야 합니다.

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 그리드에서 생성된 새 그룹이 연결된 다른 그리드의 동일한 테넌트에도 복제된다는 것을 나타내는 파란색 배너가 표시되는지 확인하십시오. 이 배너가 표시되지 않으면 테넌트의 대상 그리드에 로그인되어 있을 수 있습니다.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

[Create group](#) [Actions](#)

1 This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New tenant groups will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

☐	Name	ID	Type	Access mode
No groups found				
Create group				

3. *그룹 생성*을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 연합 그룹을 가져올 수 있습니다.

단계

1. 로컬 그룹을 생성하려면 로컬 그룹 탭을 선택하고, 이전에 구성한 ID 소스에서 그룹을 가져오려면 연합 그룹 탭을 선택하십시오.

StorageGRID 시스템에 단일 로그인(SSO)이 활성화된 경우 로컬 그룹에 속한 사용자는 테넌트 관리자에 로그인할 수 없지만, 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있습니다.

2. 그룹 이름을 입력하세요.

- 로컬 그룹: 표시 이름과 고유 이름을 모두 입력하세요. 표시 이름은 나중에 수정할 수 있습니다.



테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 대상 그리드의 테넌트에 동일한 *고유 이름*이 이미 존재하면 복제 오류가 발생합니다.

- 연합 그룹: 고유한 이름을 입력하십시오. Active Directory의 경우 고유 이름은 sAMAccountName 속성과 연결된 이름입니다. OpenLDAP의 경우 고유 이름은 uid 속성과 연결된 이름입니다.

3. *Continue*를 선택합니다.

그룹 권한 관리

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

단계

1. *액세스 모드*의 경우 다음 중 하나를 선택하십시오.

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



사용자가 여러 그룹에 속해 있고 어떤 그룹이라도 읽기 전용으로 설정되어 있는 경우, 해당 사용자는 선택된 모든 설정 및 기능에 대해 읽기 전용 액세스 권한만 갖게 됩니다.

2. 이 그룹에 대해 하나 이상의 권한을 선택하십시오.

"테넌트 관리 권한"을 참조하십시오.

3. *Continue*를 선택합니다.

S3 그룹 정책 설정

그룹 정책은 사용자가 가질 S3 액세스 권한을 결정합니다.

단계

1. 이 그룹에 적용할 정책을 선택하십시오.

그룹 정책	설명
S3 액세스 불가	기본값입니다. 이 그룹의 사용자는 버킷 정책을 통해 접근 권한이 부여되지 않는 한 S3 리소스에 접근할 수 없습니다. 이 옵션을 선택하면 기본적으로 루트 사용자만 S3 리소스에 접근할 수 있습니다.

그룹 정책	설명
읽기 전용 액세스	이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 갖습니다. 예를 들어, 이 그룹의 사용자는 객체 목록을 보고 객체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책에 대한 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
전체 액세스	이 그룹의 사용자는 버킷을 포함한 S3 리소스에 대한 모든 권한을 갖습니다. 이 옵션을 선택하면 전체 액세스 그룹 정책에 대한 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
랜섬웨어 완화	이 예시 정책은 해당 테넌트의 모든 버킷에 적용됩니다. 이 그룹의 사용자는 일반적인 작업을 수행할 수 있지만, 객체 버전 관리가 활성화된 버킷에서 객체를 영구적으로 삭제할 수는 없습니다. 모든 버킷 관리 권한이 있는 Tenant Manager 사용자는 이 그룹 정책을 재정의할 수 있습니다. 모든 버킷 관리 권한은 신뢰할 수 있는 사용자에게만 부여하고, 가능한 경우 다단계 인증(MFA)을 사용하십시오.
사용자 지정	<code>\${post_edited_translations.segment}</code>

2. *사용자 지정*을 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책의 크기 제한은 5,120바이트입니다. 유효한 JSON 형식의 문자열을 입력해야 합니다.

언어 구문 및 예제를 포함한 그룹 정책에 대한 자세한 내용은 "[예시 그룹 정책](#)"을 참조하십시오.

3. 로컬 그룹을 생성하는 경우 *계속*을 선택하십시오. 연합 그룹을 생성하는 경우 *그룹 생성*을 선택한 다음 *완료*를 선택하십시오.

사용자 추가 (로컬 그룹만 해당)

사용자를 추가하지 않고 그룹을 저장할 수도 있고, 선택적으로 이미 존재하는 로컬 사용자를 추가할 수도 있습니다.



테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 소스 그리드에서 로컬 그룹을 만들 때 선택한 사용자는 해당 그룹이 타겟 클러스터로 복제될 때 포함되지 않습니다. 따라서 그룹을 만들 때 사용자를 선택하지 마십시오. 대신, 사용자를 만들 때 그룹을 선택하십시오.

단계

1. 선택적으로, 이 그룹에 대해 한 명 이상의 로컬 사용자를 선택할 수 있습니다.
2. 그룹 만들기 및 *완료*를 선택합니다.

생성한 그룹이 그룹 목록에 나타납니다.

테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에 있는 경우, 새 그룹이 테넌트의 대상 그리드로 복제됩니다. 그룹 세부 정보 페이지의 개요 섹션에서 *복제 상태*가 *성공*으로 표시됩니다.

StorageGRID 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 사용자는 하나 이상의 권한을 가진 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 설정 및 기능을 보기만 할 수 있는지를 결정합니다.



사용자가 여러 그룹에 속해 있고 어떤 그룹이라도 읽기 전용으로 설정되어 있는 경우, 해당 사용자는 선택된 모든 설정 및 기능에 대해 읽기 전용 액세스 권한만 갖게 됩니다.

그룹에 다음과 같은 권한을 할당할 수 있습니다.

권한	설명	세부 정보
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스 권한을 제공합니다.	
S3 자격 증명 직접 관리	사용자가 자신의 S3 액세스 키를 생성하고 삭제할 수 있도록 합니다.	이 권한이 없는 사용자는 STORAGE (S3) > My S3 access keys 메뉴 옵션을 볼 수 없습니다.
모든 버킷 보기	사용자가 모든 버킷과 버킷 구성을 볼 수 있도록 합니다.	모든 버킷 보기 또는 모든 버킷 관리 권한이 없는 사용자는 버킷 메뉴 옵션을 볼 수 없습니다. 이 권한은 '모든 버킷 관리' 권한으로 대체됩니다. S3 클라이언트 또는 S3 Console에서 사용하는 S3 버킷 또는 그룹 정책에는 영향을 미치지 않습니다.
<code>\$_post_edited_translations.segment</code>	사용자는 테넌트 관리자 및 테넌트 관리 API를 사용하여 S3 버킷을 생성 및 삭제하고, S3 버킷 또는 그룹 정책과 관계없이 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다.	모든 버킷 보기 또는 모든 버킷 관리 권한이 없는 사용자는 버킷 메뉴 옵션을 볼 수 없습니다. 이 권한은 '모든 버킷 보기' 권한보다 우선합니다. S3 클라이언트 또는 S3 Console에서 사용하는 S3 버킷 또는 그룹 정책에는 영향을 미치지 않습니다.

권한	설명	세부 정보
엔드포인트 관리	사용자는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID 플랫폼 서비스의 대상으로 사용되는 플랫폼 서비스 엔드포인트를 생성하거나 편집할 수 있습니다.	이 권한이 없는 사용자는 플랫폼 서비스 엔드포인트 메뉴 옵션을 볼 수 없습니다.
S3 콘솔 탭 사용	'모든 버킷 보기' 또는 '모든 버킷 관리' 권한과 함께 사용하면 사용자는 버킷 세부 정보 페이지의 S3 Console 탭에서 객체를 보고 관리할 수 있습니다.	

StorageGRID 테넌트 그룹 관리

`$(post_edited_translations.segment)`

시작하기 전에

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

그룹 보기 또는 편집

각 그룹의 기본 정보와 세부 정보를 확인하고 편집할 수 있습니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 그룹 페이지에 제공된 정보를 검토하십시오. 이 페이지에는 해당 테넌트 계정에 대한 모든 로컬 및 페더레이션 그룹의 기본 정보가 나열되어 있습니다.

테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 그룹을 보고 있는 경우:

- 배너 메시지에는 그룹을 편집하거나 삭제하면 변경 사항이 다른 그리드에 동기화되지 않는다는 내용이 표시됩니다.
- 필요에 따라, 그룹이 대상 그리드의 테넌트로 복제되지 않은 경우 배너 메시지가 표시됩니다. 실패한 항목을 [그룹 클론 재시도](#) 수 있습니다.

3. 그룹 이름을 변경하려면:
 - a. 해당 그룹의 확인란을 선택합니다.
 - b. *작업* > *그룹 이름 편집*을 선택합니다.
 - c. 새 이름을 입력합니다.
 - d. *변경 사항 저장*을 선택합니다.
4. 더 자세한 내용을 보거나 추가 수정을 하려면 다음 중 하나를 수행하십시오.
 - 그룹 이름을 선택합니다.
 - 해당 그룹의 확인란을 선택한 다음 작업 > *그룹 세부 정보 보기*를 선택합니다.
5. 개요 섹션을 검토하십시오. 이 섹션에는 각 그룹에 대한 다음 정보가 나와 있습니다.

- 표시 이름
- 고유한 이름
- 유형
- 액세스 모드
- 권한
- S3 정책
- 이 그룹의 사용자 수
- 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 그룹을 보고 있는 경우 추가 필드:
 - 클론 생성 상태 (성공 또는 실패)
 - 이 그룹을 편집하거나 삭제하면 변경 사항이 다른 그리드에 동기화되지 않음을 나타내는 파란색 배너가 표시됩니다.

6. 필요에 따라 그룹 설정을 편집하세요. 입력할 내용에 대한 자세한 내용은 "[S3 테넌트에 대한 그룹 생성](#)"을 참조하세요.

- a. 개요 섹션에서 이름 또는 편집 아이콘  을 선택하여 표시 이름을 변경합니다.
- b. 그룹 권한 탭에서 권한을 업데이트하고 *변경 내용 저장*을 선택합니다.
- c. 그룹 정책 탭에서 변경 사항을 적용하고 *변경 내용 저장*을 선택합니다.

선택적으로 다른 S3 그룹 정책을 선택하거나 필요에 따라 사용자 지정 정책에 대한 JSON 문자열을 입력합니다.

7. 기존 로컬 사용자를 하나 이상 그룹에 추가하려면 다음 단계를 따르십시오.

- a. 사용자 탭을 선택합니다.



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

성공 메시지가 오른쪽 상단에 나타납니다.

8. 로컬 사용자를 그룹에서 제거하려면:

- a. 사용자 탭을 선택합니다.
- b. *사용자 제거*를 선택합니다.
- c. 삭제할 사용자를 선택하고 *사용자 삭제*를 선택합니다.

성공 메시지가 오른쪽 상단에 나타납니다.

9. 변경한 각 섹션에 대해 *변경 내용 저장*을 선택했는지 확인하십시오.

중복 그룹

기존 그룹을 복제하면 새 그룹을 더 빠르게 만들 수 있습니다.



테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 원본 그리드에서 그룹을 복제하면 복제된 그룹이 테넌트의 대상 그리드에도 복제됩니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 복제하려는 그룹의 확인란을 선택합니다.
3. 작업 > *그룹 복제*를 선택합니다.
4. 입력할 내용에 대한 자세한 내용은 ["S3 테넌트에 대한 그룹 생성"](#)을 참조하십시오.
5. *그룹 생성*을 선택합니다.

그룹 클론 재시도

실패한 클론을 다시 시도하려면:

1. 그룹 이름 아래에 _(복제 실패)_라고 표시된 각 그룹을 선택하십시오.
2. 작업 > *그룹 복제*를 선택합니다.
3. 복제하려는 각 그룹의 세부 정보 페이지에서 복제 작업의 상태를 확인할 수 있습니다.

자세한 내용은 ["테넌트 그룹 및 사용자 복제"](#)을 참조하십시오.

하나 이상의 그룹 삭제

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



테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 그룹을 삭제하면 StorageGRID는 다른 그리드에서 해당 그룹을 삭제하지 않습니다. 이 정보를 동기화 상태로 유지해야 하는 경우, 양쪽 그리드에서 동일한 그룹을 삭제해야 합니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 삭제하려는 각 그룹의 확인란을 선택합니다.
3. 작업 > 그룹 삭제 또는 작업 > *그룹 삭제*를 선택합니다.

확인 대화 상자가 나타납니다.

4. 그룹 삭제 또는 *그룹 삭제*를 선택합니다.

AssumeRole 설정

시작하기 전에

AssumeRole을 설정하려면 관리자여야 합니다.

이 작업 정보

AssumeRole을 설정하려면 대상 그룹이 없는 경우 인수할 대상 그룹을 생성합니다. 그룹의 S3 정책을 편집하여 이 그룹을 인수할 때 허용되는 작업을 지정합니다. 그룹의 S3 트러스트 정책을 편집하여 AssumeRole API를 사용하여 그룹을 인수할 수 있는 신뢰할 수 있는 사용자를 지정합니다.

이 그룹에 대한 권한을 위임받아 생성된 임시 보안 자격 증명은 제한된 기간 동안만 유효합니다. 세션 지속 시간은 15분에서 12시간 사이이며, 기본 세션 지속 시간은 1시간입니다. 사용자를 그룹의 S3 신뢰 정책에서 제거하면 해당 사용자는 더 이상 이 그룹에 대한 권한을 위임받을 수 없습니다.

단계

1. 액세스 관리 > *그룹*을 선택합니다.
2. 그룹 이름을 클릭합니다.
3. **S3** 신뢰 정책 탭을 선택합니다.
4. S3 신뢰 정책을 추가합니다. 여기에는 AssumeRole을 수행할 수 있는 사용자 목록이 포함됩니다.
5. *변경 사항 저장*을 선택합니다.
6. **S3** 그룹 정책 탭을 선택합니다.
7. 이 그룹의 S3 신뢰 정책에 추가된 신뢰 사용자에게 필요한 S3 작업만 지정하도록 S3 정책을 편집하십시오.
8. *변경 사항 저장*을 선택합니다.

AssumeRole S3 신뢰 정책의 예시

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

구성이 완료되면 S3 신뢰 정책에 등록된 사용자는 AssumeRole을 수행하고 자격 증명을 받을 수 있습니다. 최종 권한은 그룹 정책, 버킷 정책 및 세션 정책에 따라 결정됩니다. 자세한 내용은 ["액세스 정책 사용"](#)을 참조하십시오.

저작권 정보

Copyright © 2026 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.