그룹 및 사용자 관리

StorageGRID software

NetApp
July 23, 2026

목차

그룹 및 사용자 관리

StorageGRID에서 ID 페더레이션 사용

ID 페더레이션을 사용하면 테넌트 그룹 및 사용자 설정이 더 빨라지고, 테넌트 사용자는 익숙한 자격 증명을 사용하여 테넌트 계정에 로그인할 수 있습니다.

테넌트 관리자에 대한 ID 페더레이션 구성

테넌트 그룹 및 사용자를 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하려면 테넌트 관리자에 대한 ID 페더레이션을 구성할 수 있습니다.

시작하기 전에

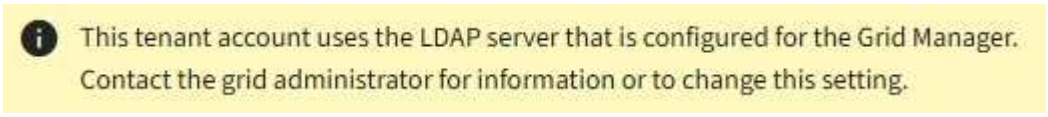
- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.
- 현재 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

  목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

- OpenLDAP을 사용하려면 OpenLDAP 서버를 구성해야 합니다. OpenLDAP 서버 구성 지침을 참조하십시오.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다. "TLS 발신 연결에 지원되는 암호화 방식"을 참조하십시오.

이 작업 정보

테넌트에 대한 ID 페더레이션 서비스 구성 가능 여부는 테넌트 계정 설정 방식에 따라 다릅니다. 테넌트는 Grid Manager에 구성된 ID 페더레이션 서비스를 공유할 수도 있습니다. ID 페더레이션 페이지에 액세스할 때 이 메시지가 표시되면 해당 테넌트에 대해 별도의 페더레이션 ID 소스를 구성할 수 없습니다.

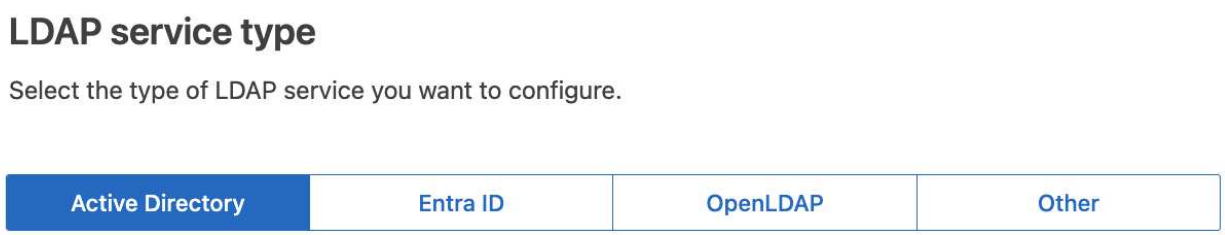


구성 입력

ID 페더레이션을 구성할 때 StorageGRID가 LDAP 서비스에 연결하는 데 필요한 값을 제공합니다.

단계

1. 액세스 관리 > *ID 페더레이션*을 선택합니다.
2. *ID 페더레이션 활성화*를 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성하려는 LDAP 서비스 유형을 선택합니다.



Oracle Directory Server를 사용하는 LDAP 서버의 값을 구성하려면 *기타*를 선택하십시오.

4. *기타*를 선택한 경우 LDAP 속성 섹션의 필드를 작성하십시오. 그렇지 않으면 다음 단계로 진행하십시오.
   - 사용자 고유 이름: LDAP 사용자의 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `sAMAccountName`, OpenLDAP의 경우 `uid`와 동일합니다. Oracle Directory Server를 구성하는 경우 `uid`를 입력합니다.
   - 사용자 **UUID**: LDAP 사용자의 영구 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `objectGUID`와, OpenLDAP의 경우 `entryUUID`와 동일합니다. Oracle Directory Server를 구성하는 경우 `nsuniqueid`를 입력하십시오. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.
   - 그룹 고유 이름: LDAP 그룹의 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `sAMAccountName`, OpenLDAP의 경우 `cn`와 동일합니다. Oracle Directory Server를 구성하는 경우 `cn`를 입력합니다.
   - 그룹 **UUID**: LDAP 그룹의 영구 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `objectGUID`, OpenLDAP의 경우 `entryUUID`와 동일합니다. Oracle Directory Server를 구성하는 경우 `nsuniqueid`를 입력합니다. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.
5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에서 필요한 LDAP 서버 및 네트워크 연결 정보를 입력하십시오.
   - 호스트 이름: LDAP 서버의 정규화된 도메인 이름(FQDN) 또는 IP 주소.
   - 포트: LDAP 서버에 연결하는 데 사용되는 포트입니다.

     STARTTLS의 기본 포트는 389이고, LDAPS의 기본 포트는 636입니다. 하지만 방화벽이 올바르게 구성되어 있다면 어떤 포트든 사용할 수 있습니다.

   - 사용자 이름: LDAP 서버에 연결할 사용자의 고유 이름(DN) 전체 경로입니다.

     Active Directory의 경우 하위 레벨 로그온 이름 또는 사용자 주체 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자 목록을 볼 수 있는 권한과 다음 속성에 접근할 수 있는 권한이 있어야 합니다.

     - `sAMAccountName` 또는 `uid`
     - `objectGUID`, `entryUUID` 또는 `nsuniqueid`
     - `cn`
     - `memberOf` 또는 `isMemberOf`
     - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, 및

`userPrincipalName`

- **Entra ID**: `accountEnabled` 및 `userPrincipalName`

◦ **Password**: 사용자 이름과 연결된 비밀번호입니다.

> 향후 비밀번호를 변경하는 경우, 반드시 이 페이지에서 업데이트해야 합니다.

◦ 그룹 기본 **DN**: 그룹을 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다. 아래 Active Directory 예시에서 고유 이름이 기본 DN(DC=storagegrid,DC=example,DC=com)을 기준으로 하는 모든 그룹은 페더레이션 그룹으로 사용할 수 있습니다.

> 그룹 고유 이름 값은 해당 그룹 기본 **DN** 내에서 고유해야 합니다.

◦ 사용자 기본 **DN**: 사용자를 검색하려는 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

> 사용자 고유 이름 값은 해당 사용자 기본 **DN** 내에서 고유해야 합니다.

◦ 바인드 사용자 이름 형식 (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 사용할 기본 사용자 이름 패턴입니다.

*바인딩 사용자 이름 형식*을 제공하는 것이 좋습니다. 이렇게 하면 StorageGRID 서비스 계정과 바인딩할 수 없는 경우에도 사용자가 로그인할 수 있습니다.

다음 패턴 중 하나를 입력하세요:

- **UserPrincipalName 패턴(AD 및 Entra ID)**: `[USERNAME]@example.com`
- 하위 레벨 로그온 이름 패턴**(AD 및 Entra ID)**: `example\[USERNAME]`
- 고유 이름 패턴: `CN=[USERNAME],CN=Users,DC=example,DC=com`

*[USERNAME]*을 정확히 입력하세요.

6. 전송 계층 보안(TLS) 섹션에서 보안 설정을 선택합니다.

◦ **STARTTLS** 사용: STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. Active Directory, OpenLDAP 또는 기타 시스템에는 이 옵션을 권장하지만, Microsoft Entra ID에서는 이 옵션이 지원되지 않습니다.

◦ **LDAPS** 사용: LDAPS(SSL을 통한 LDAP) 옵션은 TLS를 사용하여 LDAP 서버에 연결을 설정합니다. Microsoft Entra ID를 사용하려면 이 옵션을 선택해야 합니다.

◦ **TLS**를 사용하지 마십시오: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Microsoft Entra ID에서 지원되지 않습니다.

> Active Directory 서버에서 LDAP 서명을 강제하는 경우 **TLS**를 사용하지 않음 옵션은 지원되지 않습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결을 보호하는 데 사용되는 인증서를 선택하십시오.

◦ 운영체제 **CA** 인증서 사용: 연결을 보호하기 위해 운영체제에 설치된 기본 Grid CA 인증서를 사용합니다.

◦ 사용자 지정 **CA** 인증서 사용: 사용자 지정 보안 인증서를 사용합니다.

이 설정을 선택한 경우 사용자 지정 보안 인증서를 CA 인증서 텍스트 상자에 복사하여 붙여넣으세요.

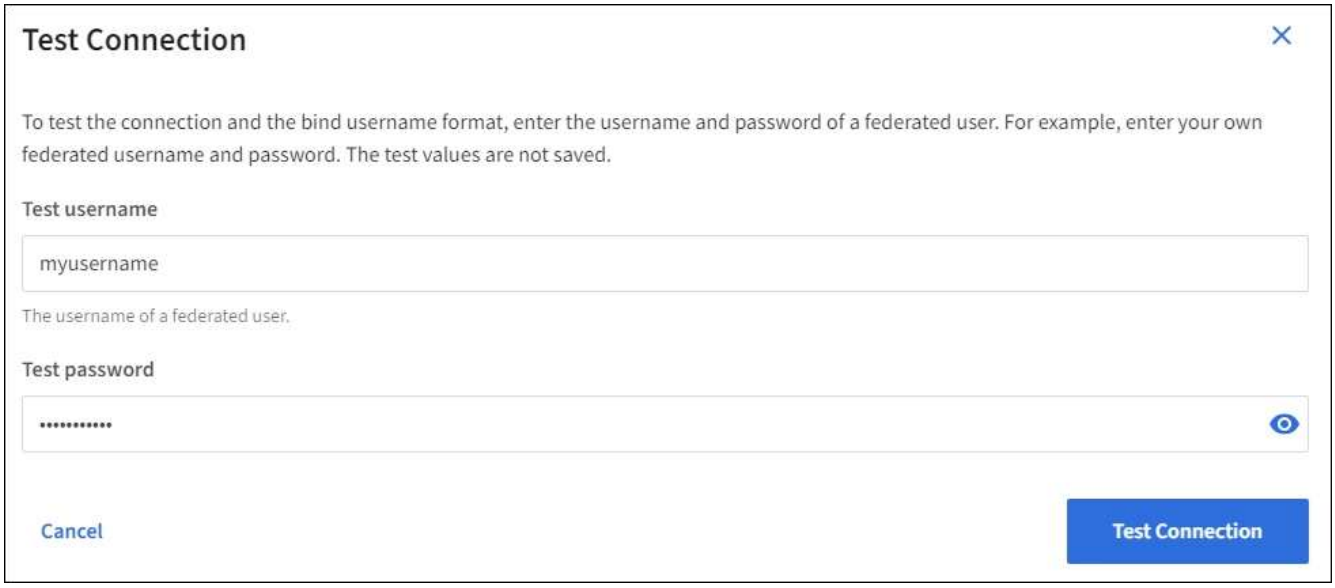
연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버의 연결 설정과 바인드 사용자 이름 형식(제공한 경우)을 확인합니다.

단계

1. *연결 테스트*를 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "연결 테스트 성공" 메시지가 나타납니다. *저장*을 선택하여 구성을 저장합니다.
   - 연결 설정이 올바르지 않으면 "테스트 연결을 설정할 수 없습니다"라는 메시지가 나타납니다. *닫기*를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트하십시오.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 페더레이션 사용자의 사용자 이름과 암호를 입력하십시오.

   예를 들어, 본인의 사용자 이름과 비밀번호를 입력하십시오. 사용자 이름에 @ 또는 /와 같은 특수 문자를 포함하지 마십시오.



   - 연결 설정이 유효하면 "연결 테스트 성공" 메시지가 나타납니다. *저장*을 선택하여 구성을 저장합니다.
   - 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름 및 암호가 유효하지 않으면 오류 메시지가 나타납니다. 문제를 해결한 후 연결을 다시 테스트하십시오.

ID 소스와의 강제 동기화

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹 및 사용자를 주기적으로 동기화합니다. 사용자 권한을 최대한 빨리 활성화하거나 제한하려면 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 연동 페이지로 이동합니다.
2. 페이지 상단에서 *동기화 서버*를 선택합니다.

   동기화 과정은 사용 환경에 따라 다소 시간이 걸릴 수 있습니다.

ID 페더레이션 동기화 실패 경고는 ID 소스에서 페더레이션된 그룹 및 사용자를 동기화하는 데 문제가 발생할 경우 발생합니다.

ID 연동 비활성화

그룹 및 사용자에 대한 ID 페더레이션을 일시적 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션이 비활성화되면 StorageGRID 와 ID 소스 간의 통신이 중단됩니다. 하지만 구성한 설정은 모두 유지되므로 나중에 ID 페더레이션을 쉽게 다시 활성화할 수 있습니다.

이 작업 정보

ID 페더레이션을 비활성화하기 전에 다음 사항을 숙지해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인 중인 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 계속 액세스할 수 있지만, 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 발생하지 않으며, 동기화되지 않은 계정에 대한 알림도 표시되지 않습니다.
- 싱글 사인온(SSO) 상태가 '사용' 또는 '샌드박스 모드'인 경우 'ID 페더레이션 사용' 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 싱글 사인온 페이지의 SSO 상태가 '사용 안 함'이어야 합니다. "싱글 사인온 비활성화"을 참조하십시오.

단계

1. ID 연동 페이지로 이동합니다.
2. **ID** 페더레이션 활성화 확인란의 선택을 해제합니다.

OpenLDAP 서버 구성 지침

ID 페더레이션을 위해 OpenLDAP 서버를 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

Active Directory 또는 Microsoft Entra ID가 아닌 ID 소스의 경우, StorageGRID는 외부에서 사용이 중지된 사용자의 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 해당 사용자의 S3 키를 삭제하거나 모든 그룹에서 해당 사용자를 제거하십시오.

Memberof 및 **refint** 오버레이

memberof 및 refint 오버레이를 활성화해야 합니다. 자세한 내용은 "OpenLDAP 문서: 버전 2.4 관리자 가이드"의 역방향 그룹 멤버십 유지 관리 지침을 참조하십시오.

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

또한, 최적의 성능을 위해 사용자 이름에 대한 도움말에 언급된 필드가 색인화되었는지 확인하십시오.

역방향 그룹 멤버십 유지 관리에 대한 정보는 "OpenLDAP 문서: 버전 2.4 관리자 가이드"을 참조하십시오.

테넌트 그룹 관리

StorageGRID에서 S3 테넌트에 대한 그룹 생성

페더레이션 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹의 권한을 관리할 수 있습니다.

시작하기 전에

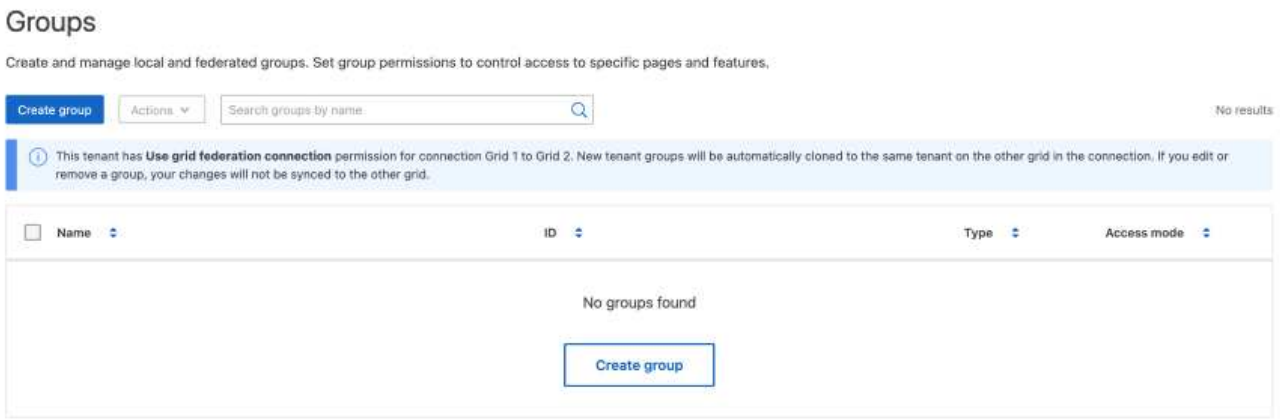
- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "루트 액세스 권한"이(가) 있는 사용자 그룹에 속해 있습니다.
- 연합 그룹을 가져오려는 경우, "구성된 ID 페더레이션", 해당 연합 그룹이 구성된 ID 소스에 이미 존재합니다.
- 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 워크플로 및 고려 사항을 검토했으며 "테넌트 그룹 및 사용자 복제", 테넌트의 소스 그리드에 로그인되어 있어야 합니다.

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.



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.
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	${post_edited_translations.segment}

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.
${post_edited_translations.segment}	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.

StorageGRID 테넌트 사용자 관리

로컬 사용자를 생성하고 로컬 그룹에 할당하여 해당 사용자가 액세스할 수 있는 기능을 지정할 수 있습니다. 페더레이션된 사용자를 가져올 수도 있습니다. 테넌트 관리자에는 "root"라는 이름의 미리 정의된 로컬 사용자가 하나 포함되어 있습니다. 로컬 사용자는 추가 및 삭제할 수 있지만, 루트 사용자는 삭제할 수 없습니다.

StorageGRID 시스템에 단일 로그인(SSO)이 활성화된 경우 로컬 사용자는 Tenant Manager 또는 테넌트 관리 API에 로그인할 수 없지만, 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 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.
- 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.

로컬 사용자 생성

로컬 사용자를 생성하고 하나 이상의 로컬 그룹에 할당하여 액세스 권한을 제어할 수 있습니다.

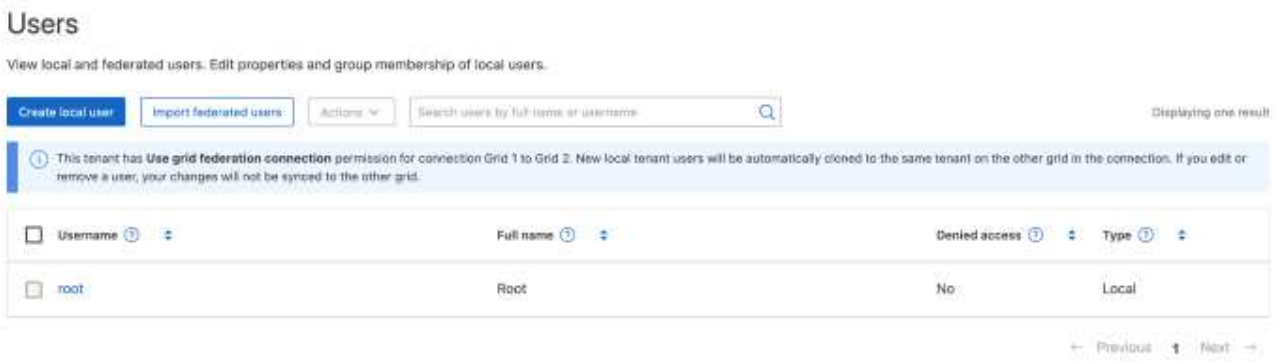
어떤 그룹에도 속하지 않은 S3 사용자는 관리 권한이 없으며 S3 그룹 정책도 적용되지 않습니다. 이러한 사용자는 버킷 정책을 통해 S3 버킷 액세스 권한을 부여받았을 수 있습니다.

사용자 생성 마법사에 액세스합니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.

   테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 파란색 배너가 표시되어 해당 테넌트의 소스 그리드임을 나타냅니다. 이 그리드에서 생성하는 모든 로컬 사용자는 연결된 다른 그리드로 복제됩니다.



2. *사용자 생성*을 선택합니다.

자격 증명을 입력합니다

단계

1. 사용자 자격 증명 입력 단계에서 다음 필드를 입력합니다.

필드	설명
성명	이 사용자의 전체 이름입니다. 예를 들어, 사람의 이름과 성 또는 애플리케이션 이름일 수 있습니다.
사용자 이름	이 사용자가 로그인할 때 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다. 참고: 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우, 동일한 *사용자 이름*이 대상 그리드의 테넌트에 이미 존재하면 복제 오류가 발생합니다.
비밀번호 및 비밀번호 확인	사용자가 처음 로그인할 때 사용할 비밀번호입니다.
액세스 거부	이 사용자가 하나 이상의 그룹에 속해 있더라도 테넌트 계정에 로그인하지 못하도록 하려면 *예*를 선택하십시오. 예를 들어, 사용자의 로그인 기능을 일시적으로 중단하려면 *예*를 선택하세요.

2. *Continue*를 선택합니다.

그룹에 할당

단계

1. 사용자를 하나 이상의 로컬 그룹에 할당하여 수행할 수 있는 작업을 결정합니다.

   사용자를 그룹에 할당하는 것은 선택 사항입니다. 원하시는 경우, 그룹을 생성하거나 편집할 때 사용자를 선택할 수 있습니다.

   어떤 그룹에도 속하지 않은 사용자는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다. "테넌트 관리 권한"을 참조하십시오.

2. *사용자 생성*을 선택합니다.

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

3. *완료*를 선택하여 사용자 페이지로 돌아갑니다.

로컬 사용자 보기 또는 편집

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 사용자 페이지에 제공된 정보를 검토하십시오. 이 페이지에는 해당 테넌트 계정의 모든 로컬 및 연합 사용자에 대한

기본 정보가 나열되어 있습니다.

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

- 배너 메시지에는 사용자를 편집하거나 삭제해도 변경 사항이 다른 그리드에 동기화되지 않는다는 내용이 표시됩니다.
- 필요에 따라, 대상 그리드의 테넌트로 사용자가 복제되지 않은 경우 배너 메시지가 표시됩니다. 실패한 사용자 복제 작업을 다시 시도합니다..

3. 사용자의 전체 이름을 변경하려면:
   a. 사용자의 확인란을 선택합니다.
   b. 작업 > *전체 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.
   - 사용자 이름을 선택합니다.
   - 해당 사용자의 확인란을 선택한 다음 작업 > *사용자 세부 정보 보기*를 선택합니다.
5. 개요 섹션을 검토하십시오. 이 섹션에는 각 사용자에 대한 다음 정보가 표시됩니다.
   - 성명
   - 사용자 이름
   - 사용자 유형
   - 액세스 거부됨
   - 액세스 모드
   - 그룹 멤버십
   - 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 사용자를 보고 있는 경우 추가 필드:
     - 클론 생성 상태 (성공 또는 실패)
     - 이 사용자의 정보를 수정해도 다른 그리드에 변경 사항이 동기화되지 않음을 나타내는 파란색 배너가 표시됩니다.
6. 필요에 따라 사용자 설정을 편집합니다. 입력할 내용에 대한 자세한 내용은 로컬 사용자 생성을 참조하십시오.
   a. 개요 섹션에서 이름 또는 편집 아이콘 을 선택하여 전체 이름을 변경하세요.

      사용자 이름은 변경할 수 없습니다.

   b. 암호 탭에서 사용자의 암호를 변경하고 *변경 사항 저장*을 선택합니다.
   c. 액세스 탭에서 사용자가 로그인할 수 있도록 허용하려면 *아니요*를 선택하고, 로그인을 차단하려면 *예*를 선택합니다. 그런 다음 *변경 사항 저장*을 선택합니다.
   d. 액세스 키 탭에서 *키 생성*을 선택하고 "다른 사용자의 S3 액세스 키 생성"에 대한 지침을 따르십시오.
   e. 그룹 탭에서 *그룹 편집*을 선택하여 사용자를 그룹에 추가하거나 그룹에서 제거합니다. 그런 다음 *변경 내용 저장*을 선택합니다.

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

연합 사용자 가져오기

최대 100명까지 연합 사용자를 하나 이상 사용자 페이지로 직접 가져올 수 있습니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. *연합 사용자 가져오기*를 선택합니다.
3. 연합 사용자 한 명 이상의 UUID 또는 사용자 이름을 입력하십시오.

   여러 항목을 입력하려면 각 UUID 또는 사용자 이름을 새 줄에 추가하십시오.

4. *가져오기*를 선택합니다.

   사용자 필드로의 가져오기가 한 명 이상의 사용자에 대해 실패하는 경우 다음 단계를 수행하십시오.

   a. *가져오지 않은 사용자*를 확장하고 *사용자 복사*를 선택합니다.
   b. 이전*을 선택하고 복사한 사용자를 *연합 사용자 가져오기 대화 상자에 붙여넣어 가져오기를 다시 시도하십시오.

   연합 사용자 가져오기 대화 상자를 닫으면 성공적으로 가져온 사용자에 대한 연합 사용자 정보가 사용자 페이지에 표시됩니다.

로컬 사용자 중복

로컬 사용자를 복제하면 새 사용자를 더 빠르게 생성할 수 있습니다.

> ⓘ 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있고 테넌트의 소스 그리드에서 사용자를 복제하면 복제된 사용자가 테넌트의 대상 그리드에도 복제됩니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 복제하려는 사용자의 확인란을 선택합니다.
3. 작업 > *사용자 복제*를 선택합니다.
4. 입력할 내용에 대한 자세한 내용은 로컬 사용자 생성을 참조하십시오.
5. *사용자 생성*을 선택합니다.

사용자 클론 재시도

실패한 클론을 다시 시도하려면:

1. 사용자 이름 아래에 _(복제 실패)_라고 표시된 사용자를 각각 선택하십시오.
2. 작업 > *사용자 복제*를 선택합니다.
3. 복제 대상 사용자 각각의 상세 페이지에서 복제 작업의 상태를 확인할 수 있습니다.

자세한 내용은 "테넌트 그룹 및 사용자 복제"을 참조하십시오.

로컬 사용자 한 명 이상 삭제

StorageGRID 테넌트 계정에 더 이상 액세스할 필요가 없는 로컬 사용자를 하나 이상 영구적으로 삭제할 수 있습니다.

> 테넌트 계정에 그리드 페더레이션 연결 사용 권한이 있는 경우 로컬 사용자를 삭제하면 StorageGRID는 다른 그리드에서 해당 사용자를 삭제하지 않습니다. 이 정보를 동기화해야 하는 경우 두 그리드에서 동일한 사용자를 모두 삭제해야 합니다.

> 페더레이션 사용자를 삭제하려면 페더레이션 ID 소스를 사용해야 합니다.

단계

1. 액세스 관리 > *사용자*를 선택합니다.
2. 삭제하려는 각 사용자의 확인란을 선택하십시오.
3. 작업 > 사용자 삭제 또는 작업 > *사용자 삭제*를 선택합니다.

   확인 대화 상자가 나타납니다.

4. 사용자 삭제 또는 *사용자 삭제*를 선택합니다.