그룹 및 사용자를 관리합니다

StorageGRID 11.7

NetApp
April 12, 2024

목차

그룹 및 사용자를 관리합니다

ID 페더레이션을 사용합니다

ID 페더레이션을 사용하면 테넌트 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 테넌트 사용자는 익숙한 자격 증명을 사용하여 테넌트 계정에 로그인할 수 있습니다.

테넌트 관리자에 대한 ID 페더레이션을 구성합니다

테넌트 그룹 및 사용자를 Active Directory, Azure Active Directory(Azure AD), OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하도록 하려면 테넌트 관리자에 대한 ID 페더레이션을 구성할 수 있습니다.

시작하기 전에

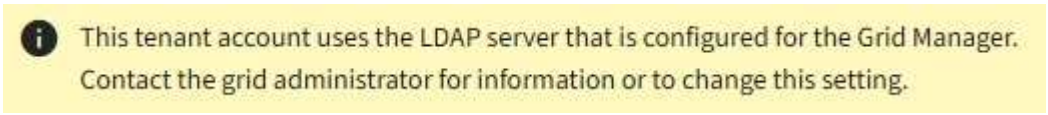
- 를 사용하여 테넌트 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 이 있는 사용자 그룹에 속해 있습니다 "루트 액세스 권한".
- Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

  목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

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

이 작업에 대해

테넌트의 ID 페더레이션 서비스를 구성할 수 있는지 여부는 테넌트 계정 설정 방법에 따라 달라집니다. 테넌트가 Grid Manager용으로 구성된 ID 페더레이션 서비스를 공유할 수 있습니다. ID 페더레이션 페이지에 액세스할 때 이 메시지가 표시되면 이 테넌트에 대해 별도의 통합 ID 소스를 구성할 수 없습니다.

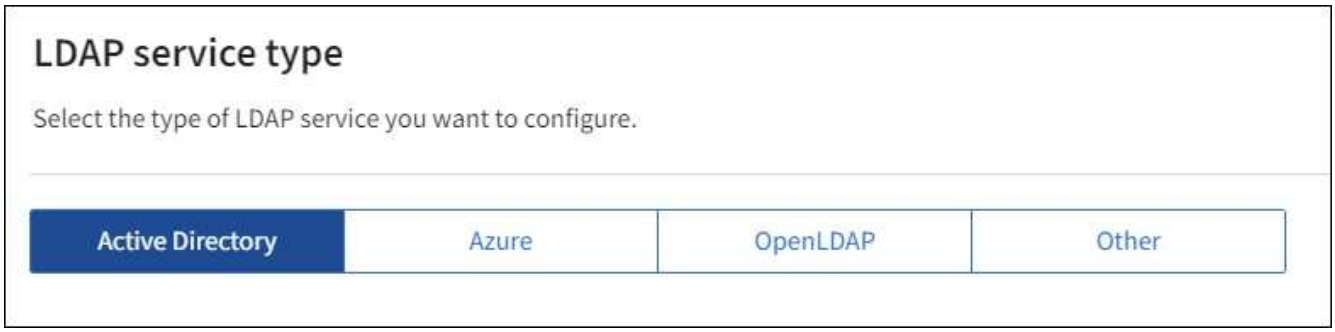


구성을 입력합니다

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

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.



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

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다. 그렇지 않으면 다음 단계로 이동합니다.
   - * 사용자 고유 이름 *: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 `sAMAccountName` Active Directory 및 의 경우 `uid` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `uid`.
   - * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 `objectGUID` Active Directory 및 의 경우 `entryUUID` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
   - * 그룹 고유 이름 *: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 `sAMAccountName` Active Directory 및 의 경우 `cn` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `cn`.
   - * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 `objectGUID` Active Directory 및 의 경우 `entryUUID` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.
   - * 호스트 이름 *: LDAP 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
   - * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다.

     STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.

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

     Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

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

- * Azure *: `accountEnabled` 및 `userPrincipalName`

◦ * 암호 *: 사용자 이름과 연결된 암호입니다.

◦ * Group Base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.

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

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

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

◦ * 사용자 이름 형식 바인딩 * (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 기본 사용자 이름 패턴을 사용해야 합니다.

StorageGRID가 서비스 계정에 바인딩할 수 없는 경우 사용자가 로그인할 수 있으므로 * 사용자 이름 형식 바인딩 * 을 제공하는 것이 좋습니다.

다음 패턴 중 하나를 입력합니다.

- * UserPrincipalName 패턴(Active Directory 및 Azure) *: `[USERNAME]@example.com`
- * 하위 수준 로그온 이름 패턴(Active Directory 및 Azure) *: `example\[USERNAME]`
- * 고유 이름 패턴 *: `CN=[USERNAME],CN=Users,DC=example,DC=com`

[UserName] * 을 서면 그대로 포함합니다.

6. TLS(전송 계층 보안) 섹션에서 보안 설정을 선택합니다.

◦ * STARTTLS 사용 *: STARTTLS를 사용하여 LDAP 서버와의 통신 보안을 설정합니다. 이 옵션은 Active Directory, OpenLDAP 또는 기타 에 대해 권장되지만 Azure에서는 지원되지 않습니다.

◦ * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. Azure의 경우 이 옵션을 선택해야 합니다.

◦ * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Azure에서 지원되지 않습니다.

> Active Directory 서버가 LDAP 서명을 적용하는 경우 * TLS 사용 안 함 * 옵션을 사용할 수 없습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.

◦ * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.

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

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

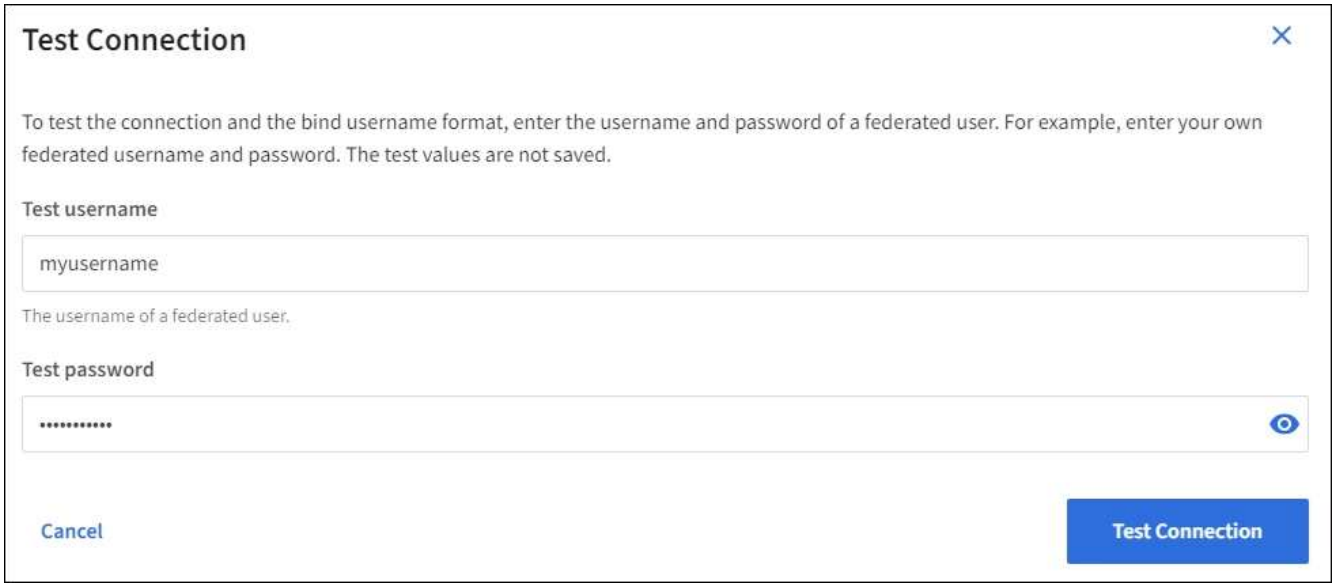
연결을 테스트하고 구성을 저장합니다

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

단계

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정이 잘못된 경우 ""테스트 연결을 설정할 수 없습니다"" 메시지가 나타납니다. 닫기 * 를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트합니다.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 통합 사용자의 사용자 이름과 암호를 입력합니다.

   예를 들어 사용자 이름과 암호를 입력합니다. @ 또는 / 같은 특수 문자를 사용자 이름에 포함하지 마십시오.



   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름과 암호가 올바르지 않으면 오류 메시지가 나타납니다. 모든 문제를 해결하고 연결을 다시 테스트합니다.

ID 소스와 강제로 동기화합니다

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹과 사용자를 정기적으로 동기화합니다. 사용자 권한을 최대한 빨리 설정하거나 제한하려는 경우 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 페더레이션 페이지로 이동합니다.
2. 페이지 맨 위에서 * 서버 동기화 * 를 선택합니다.

   동기화 프로세스는 환경에 따라 다소 시간이 걸릴 수 있습니다.

ID 소스에서 페더레이션 그룹과 사용자를 동기화하는 데 문제가 있는 경우 * ID 페더레이션 동기화 실패 * 경고가 트리거됩니다.

ID 페더레이션을 비활성화합니다

그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 사용하지 않도록 설정하면 StorageGRID와 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않으며 동기화되지 않은 계정에 대해 알림 또는 경보가 발생하지 않습니다.
- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable identity federation * 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 참조하십시오 "SSO(Single Sign-On)를 비활성화합니다".

단계

1. ID 페더레이션 페이지로 이동합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.

OpenLDAP 서버 구성 지침

OpenLDAP 서버를 ID 페더레이션에 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

ActiveDirectory 또는 Azure가 아닌 ID 소스의 경우 StorageGRID는 외부에서 비활성화된 사용자에 대한 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 사용자의 S3 키를 삭제하거나 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 의 역방향 그룹 구성원 유지 관리 지침을 참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

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 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

에서 역방향 그룹 구성원 유지 관리에 대한 정보를
참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

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.
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	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다. • 참고: * Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.
관리자	Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다 • 참고: * Swift 사용자는 Swift REST API를 사용하여 모든 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.
자체 S3 자격 증명을 관리합니다	사용자가 자신의 S3 액세스 키를 생성하고 제거할 수 있습니다. 이 권한이 없는 사용자는 * storage(S3) * > * My S3 access keys * 메뉴 옵션을 볼 수 없습니다.
모든 버킷을 관리합니다	• 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. 이 권한이 없는 사용자는 * Bucket * 메뉴 옵션이 표시되지 않습니다. • Swift 테넌트: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 정합성 수준을 제어할 수 있습니다. • 참고: * 테넌트 관리 API에서 Swift 그룹에 모든 버킷 관리 권한만 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.
엔드포인트 관리	사용자가 테넌트 관리자 또는 테넌트 관리 API를 사용하여 플랫폼 서비스 엔드포인트를 생성하거나 편집할 수 있습니다. 이 엔드포인트는 StorageGRID 플랫폼 서비스의 대상으로 사용됩니다. 이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션이 표시되지 않습니다.
S3 콘솔을 통해 오브젝트 관리	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.

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".

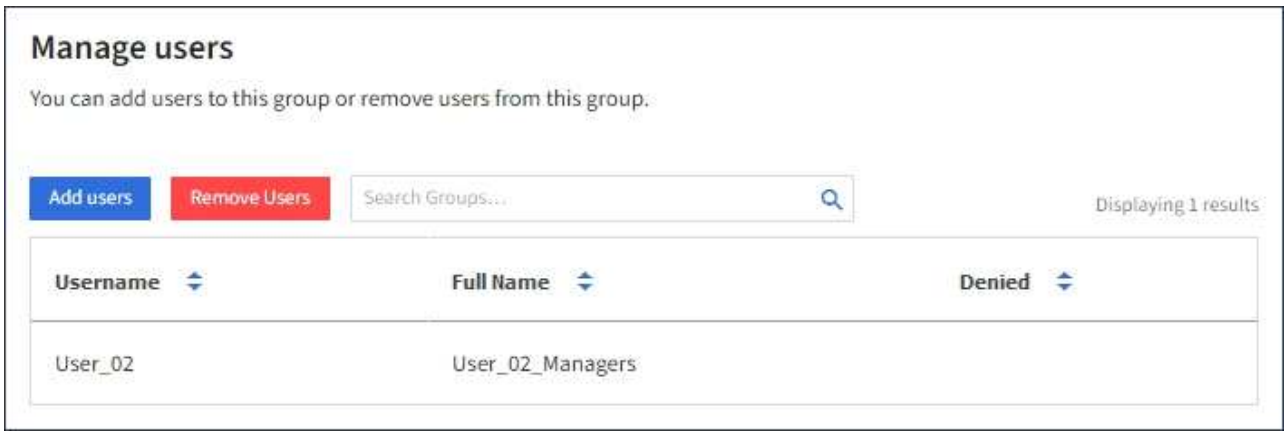
3. 그룹 이름을 변경하려면:
   a. 그룹의 확인란을 선택합니다.
   b. Actions * > * Edit group name * 을 선택합니다.
   c. 새 이름을 입력합니다.
   d. 변경 사항 저장 * 을 선택합니다
4. 자세한 내용을 보거나 추가로 편집하려면 다음 중 하나를 수행합니다.
   - 그룹 이름을 선택합니다.
   - 그룹의 확인란을 선택하고 * Actions * > * View group details * 를 선택합니다.
5. 각 그룹에 대해 다음 정보를 보여 주는 개요 섹션을 검토합니다.
   - 표시 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.

로컬 사용자를 관리합니다

로컬 사용자를 만들고 로컬 그룹에 할당하여 사용자가 액세스할 수 있는 기능을 결정할 수 있습니다. Tenant Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 한 명 있습니다. 로컬 사용자를 추가 및 제거할 수는 있지만 루트 사용자는 제거할 수 없습니다.

> StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 수 있지만 테넌트 관리자 또는 테넌트 관리 API에 로그인할 수 없습니다.

시작하기 전에

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

로컬 사용자를 생성합니다

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

그룹에 속하지 않은 S3 사용자는 관리 권한이나 S3 그룹 정책이 적용되지 않습니다. 이러한 사용자는 버킷 정책을 통해 S3 버킷 액세스가 부여될 수 있습니다.

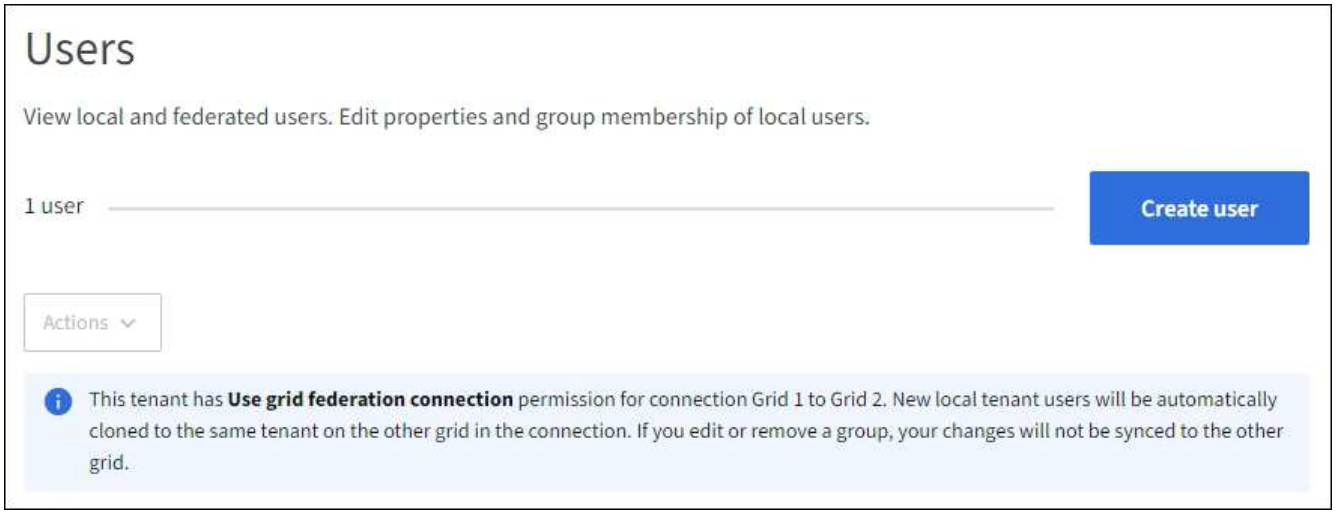
그룹에 속하지 않는 Swift 사용자는 관리 권한이나 Swift 컨테이너 액세스 권한이 없습니다.

사용자 생성 마법사에 액세스합니다

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.

   테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 파란색 배너는 해당 테넌트의 소스 그리드임을 나타냅니다. 이 그리드에서 만드는 모든 로컬 사용자는 연결의 다른 그리드에 복제됩니다.



2. 사용자 생성 * 을 선택합니다.

자격 증명을 입력합니다

단계

1. 사용자 자격 증명 입력 * 단계에 대해 다음 필드를 입력합니다.

필드에 입력합니다	설명
전체 이름	이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램의 이름).
사용자 이름	이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다. • 참고 *: 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 대상 그리드에 해당 테넌트에 대해 동일한 * 사용자 이름 * 이 이미 있으면 클론 생성 오류가 발생합니다.
암호 및 암호 확인	사용자가 로그인할 때 처음 사용할 암호입니다.
액세스를 거부합니다	이 사용자가 하나 이상의 그룹에 속해 있더라도 테넌트 계정에 로그인하지 못하도록 하려면 * 예 * 를 선택합니다. 예를 들어, * 예 * 를 선택하여 사용자의 로그인 기능을 일시적으로 중단시킵니다.

2. Continue * 를 선택합니다.

그룹에 할당합니다

단계

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

   그룹에 사용자를 할당하는 것은 선택 사항입니다. 원하는 경우 그룹을 만들거나 편집할 때 사용자를 선택할 수 있습니다.

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

2. 사용자 생성 * 을 선택합니다.

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

3. 사용자 페이지로 돌아가려면 * 마침 * 을 선택합니다.

로컬 사용자를 보거나 편집합니다

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 사용자 페이지에 제공된 정보를 검토하여 이 테넌트 계정에 대한 모든 로컬 및 통합 사용자의 기본 정보를 나열합니다.

   테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 격자에서 사용자를 보고 있는 경우 파란색 배너는 사용자를 편집하거나 제거하면 변경 내용이 다른 격자와 동기화되지 않음을 나타냅니다.

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. 자세한 내용을 보거나 추가로 편집하려면 다음 중 하나를 수행합니다.
   - 사용자 이름을 선택합니다.
   - 사용자의 확인란을 선택하고 * Actions * > * View user details * 를 선택합니다.
5. 각 사용자에 대해 다음 정보를 보여 주는 개요 섹션을 검토합니다.
   - 전체 이름
   - 사용자 이름
   - 사용자 유형
   - 액세스가 거부되었습니다
   - 액세스 모드
   - 그룹 구성원 자격

◦ 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 격자에서 사용자를 보는 경우 추가 필드:

▪ 복제 상태, * 성공 * 또는 * 실패 *

▪ 이 사용자를 편집하면 변경 내용이 다른 눈금과 동기화되지 않음을 나타내는 파란색 배너입니다.

6. 필요에 따라 사용자 설정을 편집합니다. 을 참조하십시오 로컬 사용자를 생성합니다 를 참조하십시오.

   a. 개요 섹션에서 이름 또는 편집 아이콘을 선택하여 전체 이름을 변경합니다 .

      사용자 이름은 변경할 수 없습니다.

   b. 암호 * 탭에서 사용자 암호를 변경하고 * 변경 사항 저장 * 을 선택합니다.

   c. 액세스 * 탭에서 * 아니오 * 를 선택하여 사용자가 로그인할 수 있도록 하거나 * 예 * 를 선택하여 사용자가 로그인하지 못하도록 합니다. 그런 다음 * 변경 사항 저장 * 을 선택합니다.

   d. 액세스 키 * 탭에서 * 키 만들기 * 를 선택하고 의 지침을 따릅니다 "다른 사용자의 S3 액세스 키 생성".

   e. 그룹 * 탭에서 * 그룹 편집 * 을 선택하여 사용자를 그룹에 추가하거나 그룹에서 제거합니다. 그런 다음 * 변경 사항 저장 * 을 선택합니다.

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

로컬 사용자를 복제하십시오

로컬 사용자를 복제하면 새 사용자를 보다 빠르게 만들 수 있습니다.

> 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 그리드에서 사용자를 복제하면 복제된 사용자는 테넌트의 대상 그리드에 복제됩니다.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 복제할 사용자의 확인란을 선택합니다.
3. Actions * > * Duplicate user * 를 선택합니다.
4. 을 참조하십시오 로컬 사용자를 생성합니다 를 참조하십시오.
5. 사용자 생성 * 을 선택합니다.

하나 이상의 로컬 사용자를 삭제합니다

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

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

> 통합 사용자를 삭제하려면 통합 ID 소스를 사용해야 합니다.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.

2. 삭제할 각 사용자에 대한 확인란을 선택합니다.
3. Actions * > * Delete user * 또는 * Actions * > * Delete users * 를 선택합니다.

   확인 대화 상자가 나타납니다.

4. 사용자 삭제 * 또는 * 사용자 삭제 * 를 선택합니다.