Verwalten von Gruppen und Benutzern

StorageGRID

NetApp
March 12, 2025

Inhalt

Verwalten von Gruppen und Benutzern

Verwenden Sie den Identitätsverbund

Durch die Verwendung eines Identitätsverbunds können Mandantengruppen und Benutzer schneller eingerichtet werden, und Mandantenbenutzer können sich dann mithilfe der vertrauten Anmeldedaten beim Mandantenkonto anmelden.

Konfigurieren Sie die Identitätsföderation für Mandanten-Manager

Sie können eine Identitätsföderation für den Mandanten-Manager konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System, z. B. Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server, gemanagt werden sollen.

Bevor Sie beginnen

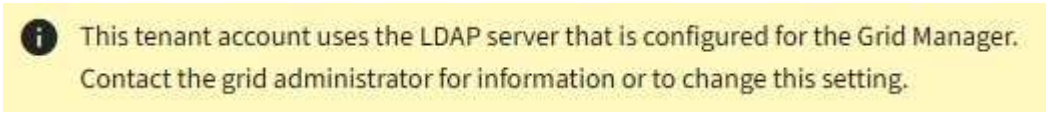
- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitäts-Provider.

> ⓘ Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, wenden Sie sich an den technischen Support.

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Siehe Richtlinien für die Konfiguration von OpenLDAP-Server.
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitäts-Provider TLS 1.2 oder 1.3 verwenden. Siehe "Unterstützte Chiffren für ausgehende TLS-Verbindungen".

Über diese Aufgabe

Ob Sie einen Identitätsföderationsdienst für Ihren Mandanten konfigurieren können, hängt davon ab, wie Ihr Mandantenkonto eingerichtet wurde. Der Mandant kann sich möglicherweise den für den Grid Manager konfigurierten Identitätsföderationsdienst teilen. Wenn diese Meldung angezeigt wird, wenn Sie auf die Seite Identity Federation zugreifen, können Sie keine separate föderierte Identitätsquelle für diesen Mandanten konfigurieren.



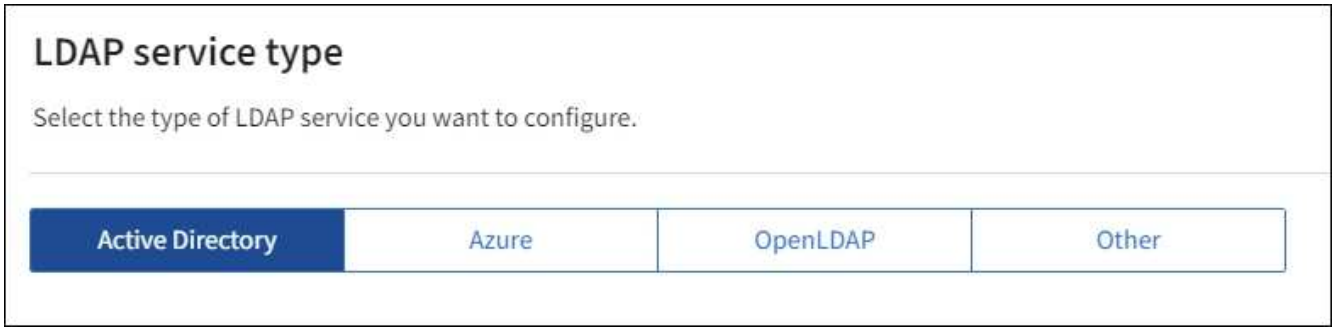
Konfiguration eingeben

Wenn Sie Identifizieren Verbund konfigurieren, geben Sie die Werte an, die StorageGRID für die Verbindung mit einem LDAP-Dienst benötigt.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
2. Wählen Sie **Identitätsföderation aktivieren**.

3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.



   Wählen Sie **Other** aus, um Werte für einen LDAP-Server zu konfigurieren, der Oracle Directory Server verwendet.

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
   - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut entspricht `sAMAccountName` für Active Directory und `uid` OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid`.
   - **Benutzer-UUID**: Der Name des Attributs, das den permanenten eindeutigen Identifier eines LDAP-Benutzers enthält. Dieses Attribut entspricht `objectGUID` für Active Directory und `entryUUID` OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
   - **Group Unique Name**: Der Name des Attributs, das den eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut entspricht `sAMAccountName` für Active Directory und `cn` OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn`.
   - **Group UUID**: Der Name des Attributs, das den permanenten eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut entspricht `objectGUID` für Active Directory und `entryUUID` OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Servicetypen die Informationen zum erforderlichen LDAP-Server und zur Netzwerkverbindung im Abschnitt LDAP-Server konfigurieren ein.
   - **Hostname**: Der vollständig qualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
   - **Port**: Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird.

     > Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden beliebigen Port verwenden, solange Ihre Firewall korrekt konfiguriert ist.

   - **Benutzername**: Der vollständige Pfad des Distinguished Name (DN) für den Benutzer, der eine Verbindung zum LDAP-Server herstellt.

     Für Active Directory können Sie auch den unten angegebenen Anmeldenamen oder den Benutzerprinzipalnamen festlegen.

     Der angegebene Benutzer muss über die Berechtigung zum Auflisten von Gruppen und Benutzern

sowie zum Zugriff auf die folgenden Attribute verfügen:

- `sAMAccountName` Oder `uid`
- `objectGUID`, `entryUUID` Oder `nsuniqueid`
- `cn`
- `memberOf` Oder `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl` Und `userPrincipalName`
- **Azure**: `accountEnabled` Und `userPrincipalName`

◦ **Passwort**: Das mit dem Benutzernamen verknüpfte Passwort.

> Wenn Sie das Passwort in Zukunft ändern, müssen Sie es auf dieser Seite aktualisieren.

◦ **Group Base DN**: Der vollständige Pfad des Distinguished Name (DN) für einen LDAP-Unterbaum, nach dem Sie nach Gruppen suchen möchten. Im Active Directory-Beispiel (unten) können alle Gruppen, deren Distinguished Name relativ zum Basis-DN (DC=storagegrid,DC=example,DC=com) ist, als föderierte Gruppen verwendet werden.

> Die **Group Unique Name**-Werte müssen innerhalb des **Group Base DN**, zu dem sie gehören, eindeutig sein.

◦ **User Base DN**: Der vollständige Pfad des Distinguished Name (DN) eines LDAP-Unterbaums, nach dem Sie nach Benutzern suchen möchten.

> Die **Benutzer-eindeutigen Namen**-Werte müssen innerhalb des **User Base DN**, zu dem sie gehören, eindeutig sein.

◦ **Bind username Format** (optional): Das Standard-Username Muster StorageGRID sollte verwendet werden, wenn das Muster nicht automatisch ermittelt werden kann.

Es wird empfohlen, **Bind username Format** bereitzustellen, da Benutzer sich anmelden können, wenn StorageGRID nicht mit dem Servicekonto verknüpft werden kann.

Geben Sie eines der folgenden Muster ein:

- **UserPrincipalNamensmuster (Active Directory und Azure)**: `[USERNAME]@*example*.com`
- **Logon Name Pattern (Active Directory und Azure)**: `*example*\[USERNAME]`
- **Distinguished Namensmuster**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Fügen Sie **[USERNAME]** genau wie geschrieben ein.

6. Wählen Sie im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung aus.
   ◦ **Verwenden Sie STARTTLS**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder andere, diese Option wird jedoch für Azure nicht unterstützt.
   ◦ **LDAPS verwenden**: Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.

- **Verwenden Sie keine TLS**: Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.

> Die Verwendung der Option **keine TLS** verwenden wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signatur erzwingt. Sie müssen STARTTLS oder LDAPS verwenden.

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.
   - **Verwenden Sie das Betriebssystem CA-Zertifikat**: Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat.

     Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat und fügen Sie es ein.

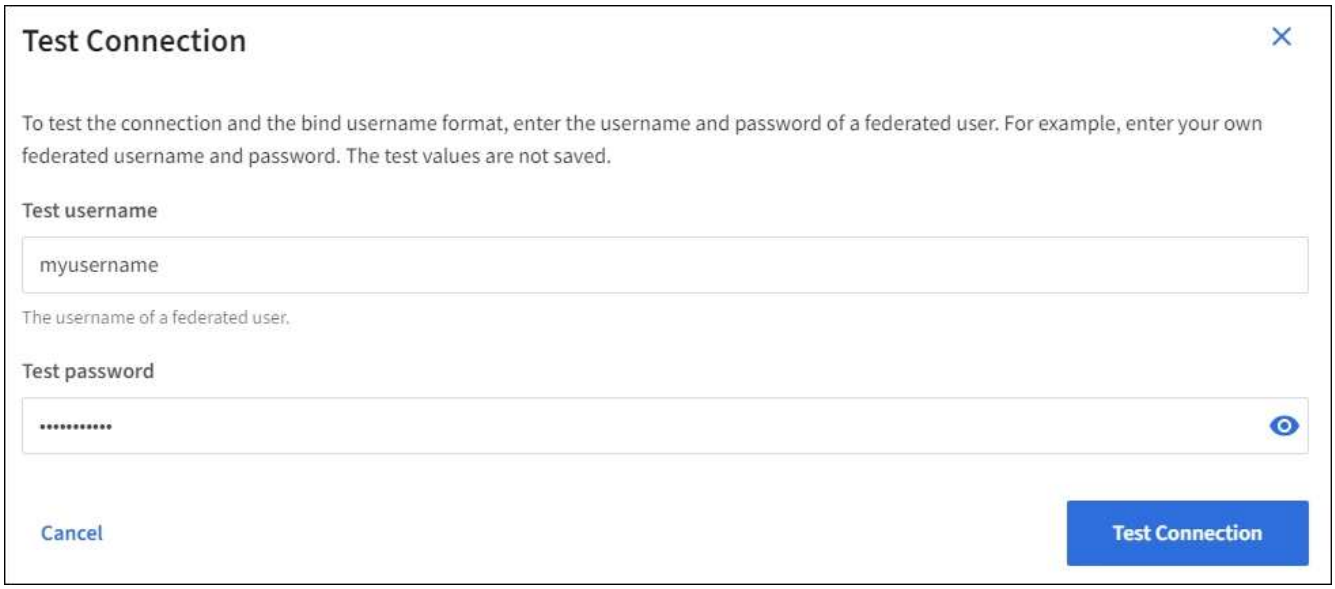
Testen Sie die Verbindung und speichern Sie die Konfiguration

Nachdem Sie alle Werte eingegeben haben, müssen Sie die Verbindung testen, bevor Sie die Konfiguration speichern können. StorageGRID überprüft die Verbindungseinstellungen für den LDAP-Server und das BIND-Username-Format, wenn Sie es angegeben haben.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein bind username Format angegeben haben:
   - Wenn die Verbindungseinstellungen gültig sind, wird die Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
   - Wenn die Verbindungseinstellungen ungültig sind, wird die Meldung „Testverbindung konnte nicht hergestellt werden“ angezeigt. Wählen Sie **Schließen**. Beheben Sie anschließend alle Probleme, und testen Sie die Verbindung erneut.
3. Wenn Sie ein bind username Format angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen föderierten Benutzers ein.

   Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr Kennwort ein. Geben Sie keine Sonderzeichen in den Benutzernamen ein, z. B. @ oder /.



- Wenn die Verbindungseinstellungen gültig sind, wird die Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Es wird eine Fehlermeldung angezeigt, wenn die Verbindungseinstellungen, das Bind-Username-Format oder der Test-Benutzername und das Kennwort ungültig sind. Beheben Sie alle Probleme, und testen Sie die Verbindung erneut.

Synchronisierung mit Identitätsquelle erzwingen

Das StorageGRID-System synchronisiert regelmäßig föderierte Gruppen und Benutzer von der Identitätsquelle aus. Sie können die Synchronisierung erzwingen, wenn Sie Benutzerberechtigungen so schnell wie möglich aktivieren oder einschränken möchten.

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Wählen Sie oben auf der Seite **Sync Server** aus.

   Der Synchronisierungsprozess kann je nach Umgebung einige Zeit in Anspruch nehmen.

   Die Warnmeldung * Identity Federation Failure* wird ausgelöst, wenn es ein Problem gibt, das die Synchronisierung von föderierten Gruppen und Benutzern aus der Identitätsquelle verursacht.

Deaktivieren Sie den Identitätsverbund

Sie können den Identitätsverbund für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen StorageGRID und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.

- Föderierte Benutzer, die sich derzeit anmelden, erhalten bis zu ihrem Ablauf Zugriff auf das StorageGRID-System, können sich jedoch nach Ablauf der Sitzung nicht anmelden.
- Die Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle wird nicht durchgeführt, und für Konten, die nicht synchronisiert wurden, werden keine Warnmeldungen ausgegeben.
- Das Kontrollkästchen **Enable Identity Federation** ist deaktiviert, wenn Single Sign-On (SSO) auf **enabled** oder **Sandbox Mode** eingestellt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Siehe "Deaktivieren Sie Single Sign-On".

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Deaktivieren Sie das Kontrollkästchen **Enable Identity Federation**.

Richtlinien für die Konfiguration von OpenLDAP-Server

Wenn Sie einen OpenLDAP-Server für die Identitätsföderation verwenden möchten, müssen Sie bestimmte Einstellungen auf dem OpenLDAP-Server konfigurieren.

> Bei Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff nicht automatisch für Benutzer, die extern deaktiviert sind. Löschen Sie zum Blockieren des S3-Zugriffs alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur Pflege der umgekehrten Gruppenmitgliedschaft im "OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch".

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Stichwörtern für den Index konfigurieren:

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

Stellen Sie außerdem sicher, dass die in der Hilfe für den Benutzernamen genannten Felder für eine optimale Leistung indiziert sind.

Weitere Informationen zur Pflege der umgekehrten Gruppenmitgliedschaft finden Sie im "OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch".

Managen von Mandantengruppen

Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen managen, indem Sie föderierte

Gruppen importieren oder lokale Gruppen erstellen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Wenn Sie planen, eine föderierte Gruppe "Konfigurierte Identitätsföderation"zu importieren, haben Sie , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, haben Sie den Workflow und die Überlegungen für überprüft "Klonen von Mandantengruppen und Benutzern"und Sie sind im Quellraster des Mandanten angemeldet.

Rufen Sie den Assistenten zum Erstellen von Gruppen auf

Rufen Sie als ersten Schritt den Assistenten zum Erstellen von Gruppen auf.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verfügt, bestätigen Sie, dass ein blaues Banner erscheint, das anzeigt, dass neue Gruppen, die in diesem Raster erstellt werden, auf demselben Mandanten auf dem anderen Raster der Verbindung geklont werden. Wenn dieses Banner nicht angezeigt wird, werden Sie möglicherweise im Zielraster des Mandanten angemeldet.

3. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

   Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

2. Geben Sie den Namen der Gruppe ein.
   - **Lokale Gruppe**: Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.

     Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, tritt ein Klonfehler auf, wenn der gleiche **eindeutige Name** bereits für den Mandanten im Zielraster vorhanden ist.

   - **Federated Group**: Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der Name, der dem Attribut zugeordnet `sAMAccountName` ist. Bei OpenLDAP ist der eindeutige Name der dem Attribut zugeordnete Name `uid`.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer in Tenant Manager und Tenant Management API durchführen können.

Schritte

1. Wählen Sie für **Access Mode** eine der folgenden Optionen aus:
   - **Lesen-Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Konfiguration des Mandanten verwalten.
   - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder keine Vorgänge in der Tenant Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

     Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.
2. Wählen Sie eine oder mehrere Berechtigungen für diese Gruppe aus.

   Siehe "Mandantenmanagement-Berechtigungen".
3. Wählen Sie **Weiter**.

Legen Sie die S3-Gruppenrichtlinie fest

Die Gruppenrichtlinie legt fest, über welche S3-Zugriffsberechtigungen Benutzer verfügen.

Schritte

1. Wählen Sie die Richtlinie aus, die Sie für diese Gruppe verwenden möchten.

Gruppenrichtlinie	Beschreibung
Kein S3-Zugriff	Standard. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird über eine Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.

Gruppenrichtlinie	Beschreibung
Schreibgeschützter Zugriff	Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
Voller Zugriff	Benutzer in dieser Gruppe haben vollständigen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
Ransomware-Minimierung	Diese Beispielrichtlinie gilt für alle Buckets für diesen Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber Objekte aus Buckets, für die die Objektversionierung aktiviert ist, nicht dauerhaft löschen. Tenant Manager-Benutzer mit der Berechtigung **Alle Buckets verwalten** können diese Gruppenrichtlinie überschreiben. Beschränken Sie die Berechtigung zum Verwalten aller Buckets auf vertrauenswürdige Benutzer und verwenden Sie die Multi-Faktor-Authentifizierung (MFA), sofern verfügbar.
Individuell	Benutzer in der Gruppe erhalten die Berechtigungen, die Sie im Textfeld angeben.

2. Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie die Gruppenrichtlinie ein. Jede Gruppenrichtlinie hat eine Größenbeschränkung von 5,120 Byte. Sie müssen einen gültigen JSON-formatierten String eingeben.

   Ausführliche Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispiele, finden Sie unter "Beispiel für Gruppenrichtlinien".

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional alle bereits vorhandenen lokalen Benutzer hinzufügen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verfügt, werden alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, nicht berücksichtigt, wenn die Gruppe im Zielraster geklont wird. Wählen Sie aus diesem Grund keine Benutzer aus, wenn Sie die Gruppe erstellen. Wählen Sie stattdessen die Gruppe aus, wenn Sie die Benutzer erstellen.

Schritte

1. Wählen Sie optional einen oder mehrere lokale Benutzer für diese Gruppe aus.
2. Wählen Sie **Gruppe erstellen** und **Fertig stellen**.

   Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

   Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie sich im Quellraster des Mandanten befinden, wird die neue Gruppe im Zielraster des Mandanten geklont. **Success** erscheint als **Klonstatus** im Abschnitt Übersicht der Detailseite der Gruppe.

Erstellen von Gruppen für einen Swift Mandanten

Sie können Zugriffsberechtigungen für ein Swift-Mandantenkonto verwalten, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen. Mindestens eine Gruppe muss über die Swift-Administratorberechtigung verfügen, die zur Verwaltung der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.

Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Wenn Sie planen, eine föderierte Gruppe "Konfigurierte Identitätsföderation"zu importieren, haben Sie , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Rufen Sie den Assistenten zum Erstellen von Gruppen auf

Schritte

Rufen Sie als ersten Schritt den Assistenten zum Erstellen von Gruppen auf.

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

   Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

2. Geben Sie den Namen der Gruppe ein.
   - **Lokale Gruppe**: Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.

- **Federated Group**: Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der Name, der dem Attribut zugeordnet `sAMAccountName` ist. Bei OpenLDAP ist der eindeutige Name der dem Attribut zugeordnete Name `uid`.

3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer in Tenant Manager und Tenant Management API durchführen können.

Schritte

1. Wählen Sie für **Access Mode** eine der folgenden Optionen aus:
   - **Lesen-Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Konfiguration des Mandanten verwalten.
   - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder keine Vorgänge in der Tenant Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

   > Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Aktivieren Sie das Kontrollkästchen **Root Access**, wenn Gruppenbenutzer sich beim Tenant Manager oder der Tenant Management API anmelden müssen.
3. Wählen Sie **Weiter**.

Swift-Gruppenrichtlinie festlegen

Swift-Benutzer benötigen Administratorberechtigungen, um sich bei der Swift-REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen.

1. Aktivieren Sie das Kontrollkästchen **Swift Administrator**, wenn Gruppenbenutzer die Swift REST API zum Verwalten von Containern und Objekten verwenden müssen.
2. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional alle bereits vorhandenen lokalen Benutzer hinzufügen.

Schritte

1. Wählen Sie optional einen oder mehrere lokale Benutzer für diese Gruppe aus.

   Wenn Sie noch keine lokalen Benutzer erstellt haben, können Sie diese Gruppe dem Benutzer auf der Seite Benutzer hinzufügen. Siehe "Managen Sie lokale Benutzer".

2. Wählen Sie **Gruppe erstellen** und **Fertig stellen**.

   Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Mandantenmanagement-Berechtigungen

Bevor Sie eine Mandantengruppe erstellen, überlegen Sie, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Über die Mandantenmanagement-Berechtigungen wird festgelegt, welche Aufgaben Benutzer mit dem Tenant Manager oder der Mandantenmanagement-API durchführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen werden kumulativ, wenn ein Benutzer zu mehreren Gruppen gehört.

Um sich beim Tenant Manager anzumelden oder die Mandantenmanagement-API zu verwenden, müssen Benutzer einer Gruppe mit mindestens einer Berechtigung angehören. Alle Benutzer, die sich anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Eigenes Kennwort ändern (für lokale Benutzer)

Für alle Berechtigungen legt die Einstellung Zugriffsmodus der Gruppe fest, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie nur die zugehörigen Einstellungen und Funktionen anzeigen können.

> Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

Sie können einer Gruppe die folgenden Berechtigungen zuweisen. Beachten Sie, dass S3-Mandanten und Swift-Mandanten unterschiedliche Gruppenberechtigungen haben.

Berechtigung	Beschreibung	Details
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API.	Swift-Benutzer müssen über Root-Zugriffsberechtigungen verfügen, um sich beim Mandantenkonto anzumelden.
Verwalter	Nur Swift Mandanten. Bietet vollständigen Zugriff auf die Swift Container und Objekte für dieses Mandantenkonto	Swift-Benutzer müssen über die Swift-Administrator-Berechtigung verfügen, um alle Vorgänge mit der Swift-REST-API auszuführen.
Management Ihrer eigenen S3 Zugangsdaten	Benutzer können ihre eigenen S3-Zugriffsschlüssel erstellen und entfernen.	Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption **STORAGE (S3)** > **Meine S3-Zugriffstasten** nicht.

Berechtigung	Beschreibung	Details
Alle Buckets anzeigen	**S3 Tenants**: Ermöglicht es Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen. **Swift Tenants**: Ermöglicht Swift-Benutzern, alle Container und Container-Konfigurationen über die Tenant Management API anzuzeigen.	Benutzer, die weder die Berechtigung Alle Buckets anzeigen noch die Berechtigung Alle Buckets verwalten haben, sehen die Menüoption **Buckets** nicht. Diese Berechtigung wird durch die Berechtigung zum Verwalten aller Buckets ersetzt. Dies hat keine Auswirkungen auf S3-Bucket oder Gruppenrichtlinien, die von S3-Clients oder S3-Konsole verwendet werden. Diese Berechtigung können Sie Swift-Gruppen nur über die Mandanten-Management-API zuweisen. Diese Berechtigung können Swift-Gruppen nicht mit dem Tenant Manager zugewiesen werden.
Managen aller Buckets	**S3-Mandanten**: Ermöglicht Benutzern die Verwendung des Tenant Manager und der Tenant Management API, um S3-Buckets zu erstellen und zu löschen sowie die Einstellungen für alle S3-Buckets im Mandantenkonto zu managen, unabhängig von S3-Bucket oder Gruppenrichtlinien. **Swift Tenants**: Ermöglicht Swift-Benutzern die Kontrolle der Konsistenz für Swift-Container mithilfe der Mandanten-Management-API.	Benutzer, die weder die Berechtigung Alle Buckets anzeigen noch die Berechtigung Alle Buckets verwalten haben, sehen die Menüoption **Buckets** nicht. Diese Berechtigung ersetzt die Berechtigung Alle Planungsperioden anzeigen. Dies hat keine Auswirkungen auf S3-Bucket oder Gruppenrichtlinien, die von S3-Clients oder S3-Konsole verwendet werden. Diese Berechtigung können Sie Swift-Gruppen nur über die Mandanten-Management-API zuweisen. Diese Berechtigung können Swift-Gruppen nicht mit dem Tenant Manager zugewiesen werden.
Verwalten von Endpunkten	Ermöglicht Benutzern die Verwendung des Tenant Managers oder der Mandanten-Management-API zum Erstellen oder Bearbeiten von Plattformdienstendpunkten, die als Ziel für StorageGRID-Plattformdienste verwendet werden.	Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption **Plattform-Dienste-Endpunkte** nicht.
Verwenden Sie die Registerkarte S3 Console	In Kombination mit der Berechtigung Alle Buckets anzeigen oder alle Buckets verwalten können Benutzer Objekte über die Registerkarte S3 Console auf der Detailseite für einen Bucket anzeigen und managen.	

Gruppen managen

Managen Sie die Mandantengruppen nach Bedarf, um eine Gruppe anzuzeigen, zu

bearbeiten oder zu duplizieren und vieles mehr.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".

Gruppe anzeigen oder bearbeiten

Sie können die grundlegenden Informationen und Details für jede Gruppe anzeigen und bearbeiten.

Schritte

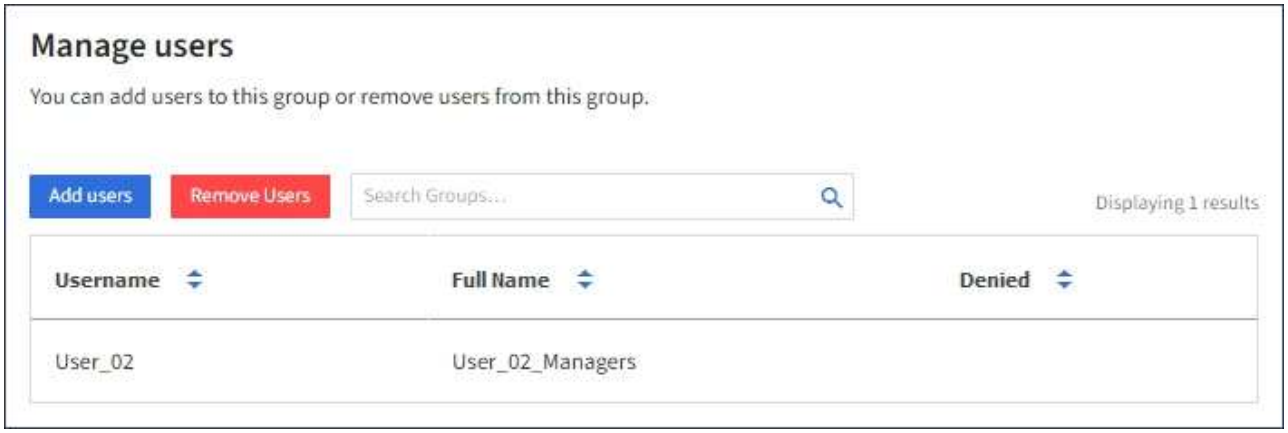
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Überprüfen Sie die Informationen auf der Seite Gruppen, auf der grundlegende Informationen für alle lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

   Wenn das Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie Gruppen im Quellraster des Mandanten anzeigen:

   - Eine Banner-Meldung zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie eine Gruppe bearbeiten oder entfernen.
   - Bei Bedarf gibt eine Banner-Meldung an, ob Gruppen nicht für den Mandanten im Zielraster geklont wurden. Sie können Wiederholen Sie einen Gruppenklon das gescheitert.
3. Wenn Sie den Namen der Gruppe ändern möchten:
   a. Aktivieren Sie das Kontrollkästchen für die Gruppe.
   b. Wählen Sie **Aktionen** > **Gruppenname bearbeiten**.
   c. Geben Sie den neuen Namen ein.
   d. Wählen Sie **Änderungen speichern.**
4. Wenn Sie weitere Details anzeigen oder weitere Änderungen vornehmen möchten, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie den Gruppennamen aus.
   - Aktivieren Sie das Kontrollkästchen für die Gruppe und wählen Sie **actions** > **View Group Details**.
5. Lesen Sie den Abschnitt „Übersicht“, in dem die folgenden Informationen für jede Gruppe angezeigt werden:
   - Anzeigename
   - Eindeutiger Name
   - Typ
   - Zugriffsmodus
   - Berechtigungen
   - S3-Richtlinie
   - Anzahl der Benutzer in dieser Gruppe
   - Zusätzliche Felder, wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie die Gruppe im Quellraster des Mandanten anzeigen:
     - Klonstatus, entweder **success** oder **failure**
     - Ein blaues Banner, das darauf hinweist, dass Ihre Änderungen nicht mit dem anderen Raster

synchronisiert werden, wenn Sie diese Gruppe bearbeiten oder löschen.

6. Bearbeiten Sie die Gruppeneinstellungen nach Bedarf. Weitere Informationen zu den Eingeben finden Sie unter "Erstellen von Gruppen für einen S3-Mandanten" und"Erstellen von Gruppen für einen Swift Mandanten".
   a. Ändern Sie im Abschnitt Übersicht den Anzeigenamen, indem Sie den Namen oder das Bearbeiten-Symbol auswählen.
   b. Aktualisieren Sie auf der Registerkarte **Gruppenberechtigungen** die Berechtigungen und wählen Sie **Änderungen speichern**.
   c. Nehmen Sie auf der Registerkarte **Gruppenrichtlinie** Änderungen vor und wählen Sie **Änderungen speichern**.
      - Wenn Sie eine S3-Gruppe bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus, oder geben Sie bei Bedarf den JSON-String für eine benutzerdefinierte Richtlinie ein.
      - Wenn Sie eine Swift-Gruppe bearbeiten, aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Swift Administrator**.
7. So fügen Sie der Gruppe einen oder mehrere vorhandene lokale Benutzer hinzu:
   a. Wählen Sie die Registerkarte Benutzer aus.



   b. Wählen Sie **Benutzer hinzufügen**.
   c. Wählen Sie die vorhandenen Benutzer aus, die Sie hinzufügen möchten, und wählen Sie **Benutzer hinzufügen**.

      Oben rechts wird eine Erfolgsmeldung angezeigt.

8. So entfernen Sie lokale Benutzer aus der Gruppe:
   a. Wählen Sie die Registerkarte Benutzer aus.
   b. Wählen Sie **Benutzer entfernen**.
   c. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und wählen Sie **Benutzer entfernen**.

      Oben rechts wird eine Erfolgsmeldung angezeigt.

9. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Gruppe duplizieren

Sie können eine vorhandene Gruppe duplizieren, um neue Gruppen schneller zu erstellen.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie eine Gruppe aus dem Quellraster des Mandanten duplizieren, wird die duplizierte Gruppe im Zielraster des Mandanten geklont.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Aktionen** > **Gruppe duplizieren**.
4. Weitere Informationen zu den Eingeben finden Sie unter "Erstellen von Gruppen für einen S3-Mandanten" oder"Erstellen von Gruppen für einen Swift Mandanten".
5. Wählen Sie **Gruppe erstellen**.

Gruppenklone erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klon:

1. Wählen Sie jede Gruppe aus, die *(Klonen fehlgeschlagen)* unter dem Gruppennamen anzeigt.
2. Wählen Sie **actions** > **Clone groups**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jeder Gruppe an, die Sie klonen.

Weitere Informationen finden Sie unter "Klonen von Mandantengruppen und Benutzern".

Löschen Sie eine oder mehrere Gruppen

Sie können eine oder mehrere Gruppen löschen. Alle Benutzer, die nur zu einer Gruppe gehören, die gelöscht wurde, können sich nicht mehr beim Tenant Manager anmelden oder das Mandantenkonto verwenden.

Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie eine Gruppe löschen, wird StorageGRID die entsprechende Gruppe im anderen Raster nicht löschen. Wenn Sie diese Informationen synchron halten müssen, müssen Sie dieselbe Gruppe aus beiden Rastern löschen.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für jede Gruppe, die Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Gruppe löschen** oder **Aktionen** > **Gruppen löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **Gruppe löschen** oder **Gruppen löschen**.

Managen Sie lokale Benutzer

Sie können lokale Benutzer erstellen und lokalen Gruppen zuweisen, um zu bestimmen, auf welche Funktionen diese Benutzer zugreifen können. Der Tenant Manager enthält einen vordefinierten lokalen Benutzer mit dem Namen „root“. Obwohl Sie lokale Benutzer hinzufügen und entfernen können, können Sie den Root-Benutzer nicht entfernen.

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Tenant Manager oder der Mandanten-Management-API anmelden, obwohl sie Clientanwendungen verwenden können, um basierend auf Gruppenberechtigungen auf die Ressourcen des Mandanten zuzugreifen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, haben Sie den Workflow und die Überlegungen für überprüft "Klonen von Mandantengruppen und Benutzern"und Sie sind im Quellraster des Mandanten angemeldet.

Erstellen Sie einen lokalen Benutzer

Sie können einen lokalen Benutzer erstellen und diesen einer oder mehreren lokalen Gruppen zuweisen, um ihre Zugriffsberechtigungen zu steuern.

S3-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder S3-Gruppenrichtlinien, die auf sie angewendet werden. Diese Benutzer haben möglicherweise S3-Bucket-Zugriff, der über eine Bucket-Richtlinie gewährt wird.

Swift-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder Swift-Container-Zugriff.

Rufen Sie den Assistenten zum Erstellen von Benutzern auf

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.

   Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, zeigt ein blaues Banner an, dass dies das Quellraster des Mandanten ist. Alle lokalen Benutzer, die Sie in diesem Raster erstellen, werden in das andere Raster der Verbindung geklont.

2. Wählen Sie **Benutzer erstellen**.

Geben Sie die Anmeldedaten ein

Schritte

1. Füllen Sie für den Schritt **Enter user credentials** die folgenden Felder aus.

Feld	Beschreibung
Vollständiger Name	Der vollständige Name für diesen Benutzer, z. B. der vor- und Nachname einer Person oder der Name einer Anwendung.

Feld	Beschreibung
Benutzername	Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden. **Hinweis**: Wenn Ihr Mieterkonto die Berechtigung **Grid Federation connection** verwenden hat, tritt ein Klonfehler auf, wenn der gleiche **Benutzername** bereits für den Mieter im Zielraster vorhanden ist.
Passwort und Passwort bestätigen	Das Passwort, das der Benutzer beim Anmelden verwendet.
Zugriff verweigern	Wählen Sie **Ja**, um zu verhindern, dass sich dieser Benutzer beim Mandantenkonto anmeldet, obwohl er noch zu einer oder mehreren Gruppen gehört. Wählen Sie zum Beispiel **Ja**, um die Anmelde-Fähigkeit eines Benutzers vorübergehend zu unterbrechen.

2. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

1. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu, um zu bestimmen, welche Aufgaben er ausführen kann.

   Das Zuweisen eines Benutzers zu Gruppen ist optional. Wenn Sie möchten, können Sie Benutzer auswählen, wenn Sie Gruppen erstellen oder bearbeiten.

   Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören. Siehe "Mandantenmanagement-Berechtigungen".

2. Wählen Sie **Benutzer erstellen**.

   Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie sich im Quellraster des Mandanten befinden, wird der neue lokale Benutzer im Zielraster des Mandanten geklont. **Success** erscheint als **Klonstatus** im Abschnitt Übersicht der Detailseite des Benutzers.

3. Wählen Sie **Fertig**, um zur Benutzerseite zurückzukehren.

Lokalen Benutzer anzeigen oder bearbeiten

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Überprüfen Sie die Informationen auf der Seite Benutzer, auf der grundlegende Informationen für alle lokalen und föderierten Benutzer dieses Mandantenkontos aufgeführt sind.

   Wenn das Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie den Benutzer im Quellraster des Mandanten anzeigen:

- Wenn Sie einen Benutzer bearbeiten oder entfernen, werden Ihre Änderungen nicht mit dem anderen Raster synchronisiert.
- Bei Bedarf gibt eine Banner-Meldung an, ob Benutzer nicht für den Mandanten im Zielraster geklont wurden. Sie können Wiederholen Sie einen fehlgeschlagenen Benutzerklon.

3. Wenn Sie den vollständigen Namen des Benutzers ändern möchten:
   a. Aktivieren Sie das Kontrollkästchen für den Benutzer.
   b. Wählen Sie **Aktionen** > **vollständigen Namen bearbeiten**.
   c. Geben Sie den neuen Namen ein.
   d. Wählen Sie **Änderungen speichern.**
4. Wenn Sie weitere Details anzeigen oder weitere Änderungen vornehmen möchten, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie den Benutzernamen aus.
   - Aktivieren Sie das Kontrollkästchen für den Benutzer, und wählen Sie **Aktionen** > **Benutzerdetails anzeigen**.
5. Lesen Sie den Abschnitt Übersicht, in dem die folgenden Informationen für jeden Benutzer angezeigt werden:
   - Vollständiger Name
   - Benutzername
   - Benutzertyp
   - Zugriff verweigert
   - Zugriffsmodus
   - Gruppenmitgliedschaft
   - Zusätzliche Felder, wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie den Benutzer im Quellraster des Mandanten anzeigen:
     - Klonstatus, entweder **success** oder **failure**
     - Ein blaues Banner, das darauf hinweist, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diesen Benutzer bearbeiten.
6. Bearbeiten Sie die Benutzereinstellungen nach Bedarf. Einzelheiten dazu, was Sie eingeben müssen, finden Sie unterErstellen Sie einen lokalen Benutzer.
   a. Ändern Sie im Abschnitt Übersicht den vollständigen Namen, indem Sie den Namen oder das Bearbeiten-Symbol auswählen.

      Sie können den Benutzernamen nicht ändern.

   b. Ändern Sie auf der Registerkarte **Passwort** das Passwort des Benutzers und wählen Sie **Änderungen speichern**.
   c. Wählen Sie auf der Registerkarte **Access No** aus, damit sich der Benutzer anmelden kann, oder wählen Sie **Yes**, um die Anmeldung des Benutzers zu verhindern. Wählen Sie dann **Änderungen speichern**.
   d. Wählen Sie auf der Registerkarte **Access Keys Create key** aus und folgen Sie den Anweisungen für "Erstellen der S3-Zugriffsschlüssel eines anderen Benutzers".
   e. Wählen Sie auf der Registerkarte **Gruppen** die Option **Gruppen bearbeiten**, um den Benutzer zu Gruppen hinzuzufügen oder ihn aus Gruppen zu entfernen. Wählen Sie dann **Änderungen speichern**.

7. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Doppelter lokaler Benutzer

Sie können einen lokalen Benutzer duplizieren, um einen neuen Benutzer schneller zu erstellen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie einen Benutzer aus dem Quellraster des Mandanten duplizieren, wird der duplizierte Benutzer im Zielraster des Mandanten geklont.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Aktivieren Sie das Kontrollkästchen für den Benutzer, den Sie duplizieren möchten.
3. Wählen Sie **Aktionen** > **Benutzer duplizieren**.
4. Einzelheiten dazu, was Sie eingeben müssen, finden Sie unterErstellen Sie einen lokalen Benutzer.
5. Wählen Sie **Benutzer erstellen**.

Benutzerklon wiederholen

So wiederholen Sie einen fehlgeschlagenen Klon:

1. Wählen Sie jeden Benutzer aus, der *(Klonen fehlgeschlagen)* unter dem Benutzernamen anzeigt.
2. Wählen Sie **actions** > **Clone users**.
3. Den Status des Klonvorgangs können Sie auf der Detailseite jedes Benutzers, den Sie klonen, anzeigen.

Weitere Informationen finden Sie unter "Klonen von Mandantengruppen und Benutzern".

Löschen Sie einen oder mehrere lokale Benutzer

Sie können einen oder mehrere lokale Benutzer, die nicht mehr auf das StorageGRID-Mandantenkonto zugreifen müssen, dauerhaft löschen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie einen lokalen Benutzer löschen, wird StorageGRID den entsprechenden Benutzer im anderen Raster nicht löschen. Wenn Sie diese Informationen synchron halten müssen, müssen Sie denselben Benutzer aus beiden Rastern löschen.

> Sie müssen die föderierte Identitätsquelle verwenden, um verbundene Benutzer zu löschen.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Benutzer löschen** oder **Aktionen** > **Benutzer löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **Benutzer löschen** oder **Benutzer löschen**.