



Managen des Systemzugriffs für Mandantenbenutzer

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Managen des Systemzugriffs für Mandantenbenutzer 1
 - Identitätsföderation verwenden 1
 - Verwalten von Gruppen 5
 - Verwalten von lokalen Benutzern 20

Managen des Systemzugriffs für Mandantenbenutzer

Sie gewähren Benutzern Zugriff auf ein Mandantenkonto, indem Sie Gruppen von einer föderierten Identitätsquelle importieren und Verwaltungsberechtigungen zuweisen. Außerdem können lokale Mandantengruppen und Benutzer erstellt werden, es sei denn, Single Sign On (SSO) gilt für das gesamte StorageGRID System.

- ["Identitätsföderation verwenden"](#)
- ["Verwalten von Gruppen"](#)
- ["Verwalten von lokalen Benutzern"](#)

Identitätsföderation verwenden

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 einer föderierten Identitätsquelle"](#)
- ["Synchronisierung mit der Identitätsquelle erzwingen"](#)
- ["Identitätsföderation deaktivieren"](#)

Konfigurieren einer föderierten Identitätsquelle

Sie können eine Identitätsföderation konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System wie Active Directory, OpenLDAP oder Oracle Directory Server verwaltet werden sollen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen Active Directory, OpenLDAP oder Oracle Directory Server als Identitäts-Provider verwenden. Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, müssen Sie sich an den technischen Support wenden.
- 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.

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 für diesen Mandanten keine separate föderierte Identitätsquelle konfigurieren.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Diensttyp **Active Directory**, **OpenLDAP** oder **Other** aus.

Wenn Sie **OpenLDAP** wählen, konfigurieren Sie den OpenLDAP-Server. Weitere Informationen zur Konfiguration eines OpenLDAP-Servers finden Sie in den Richtlinien.

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.
 - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `uid` Für 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 ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für 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 ist äquivalent zu `sAMAccountName` Für Active Directory und `cn` Für 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 ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für 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 im Abschnitt LDAP-Server konfigurieren die erforderlichen Informationen zum LDAP-Server und zur Netzwerkverbindung ein.
 - **Hostname**: Der Server-Hostname 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`

- **Passwort:** Das mit dem Benutzernamen verknüpfte Passwort.
- **Gruppenbasis 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 der **Group-Basis-DN**, zu der 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 **User Unique Name**-Werte müssen innerhalb der **User Base DN**, zu der sie gehören, eindeutig sein.

6. Wählen Sie im Abschnitt **Transport Layer Security (TLS)** eine Sicherheitseinstellung aus.

- **Verwenden Sie STARTTLS (empfohlen):** Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option.
- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Diese Option wird aus Kompatibilitätsgründen unterstützt.
- **Verwenden Sie keine TLS:** Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert.

Diese Option 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-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.

8. Wählen Sie **Verbindung testen**, um die Verbindungseinstellungen für den LDAP-Server zu validieren.

Wenn die Verbindung gültig ist, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.

9. Wenn die Verbindung gültig ist, wählen Sie **Speichern**.

Der folgende Screenshot zeigt Beispielfeldkonfigurationen für einen LDAP-Server, der Active Directory verwendet.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Richtlinien für die Konfiguration eines OpenLDAP-Servers"](#)

Richtlinien für die Konfiguration eines OpenLDAP-Servers

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

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie im Administratorhandbuch für OpenLDAP in den Anweisungen zur Wartung der Reverse-Group-Mitgliedschaft.

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 Wartung der Umkehrgruppenmitgliedschaft finden Sie im Administratorhandbuch für OpenLDAP.

Synchronisierung mit der 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die gespeicherte Identitätsquelle muss aktiviert sein.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.

Die Seite Identitätsföderation wird angezeigt. Die Schaltfläche **Sync Server** befindet sich oben rechts auf der Seite.



Wenn die gespeicherte Identitätsquelle nicht aktiviert ist, ist die Schaltfläche **Sync Server** nicht aktiv.

2. Wählen Sie **Sync Server**.

Eine Bestätigungsmeldung zeigt an, dass die Synchronisierung erfolgreich gestartet wurde.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Identitätsföderation deaktivieren

Wenn Sie einen Identitätsföderationsdienst für diesen Mandanten konfiguriert haben, können Sie die Identitätsföderation für Mandanten und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen dem StorageGRID-System und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die derzeit angemeldet sind, erhalten bis zum Ablauf ihrer Sitzung Zugriff auf das Mandantenkonto, können sich jedoch nach Ablauf ihrer Sitzung nicht anmelden.
- Es erfolgt keine Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle.

Schritte

1. Wählen Sie *** ACCESS MANAGEMENT* > Identity Federation**.
2. Deaktivieren Sie das Kontrollkästchen *** Identitätsföderation aktivieren***.
3. Wählen Sie **Speichern**.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Verwalten von Gruppen

Sie weisen Benutzergruppen Berechtigungen zu, um zu steuern, welche Aufgaben Mandantenbenutzer durchführen können. Sie können föderierte Gruppen aus einer Identitätsquelle importieren, z. B. Active Directory oder OpenLDAP, oder Sie können lokale Gruppen erstellen.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager anmelden, obwohl sie auf Basis der Gruppenberechtigungen auf S3- und Swift-Ressourcen zugreifen können.

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. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

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

Berechtigung	Beschreibung
Alle Buckets Verwalten	<ul style="list-style-type: none"> S3-Mandanten: Ermöglicht Benutzern die Nutzung des Mandanten-Manager und der Mandanten-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. <p>Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption Buckets nicht.</p> <ul style="list-style-type: none"> Swift Mandanten: Ermöglicht Swift Benutzern die Kontrolle der Konsistenzstufe für Swift Container mithilfe der Mandanten-Management-API. <p>Hinweis: Sie können Swift-Gruppen nur die Berechtigung Alle Buckets verwalten aus der Mandantenmanagement-API zuweisen. Sie können diese Berechtigung nicht Swift-Gruppen mit dem Tenant Manager zuweisen.</p>
Endpunkte Managen	<p>Nur S3-Mandanten. Ermöglicht Benutzern, Endpunkte mithilfe des Mandanten-Managers oder der Mandanten-Management-API zu erstellen oder zu bearbeiten, die als Ziel für StorageGRID-Platformservices verwendet werden.</p> <p>Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption Platform Services Endpunkte.</p>

Verwandte Informationen

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen managen, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Schritte

- Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

Groups

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

2 groups Create group

Actions ▼

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

← Previous **1** Next →

2. Wählen Sie **Gruppe erstellen**.

3. 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.

4. 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 dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.

5. Wählen Sie **Weiter**.

6. Wählen Sie einen Zugriffsmodus aus. 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.

- **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.
- **Schreibgeschützt:** Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

7. Wählen Sie die Gruppenberechtigungen für diese Gruppe aus.

Weitere Informationen zu Berechtigungen für die Mandantenverwaltung finden Sie unter.

8. Wählen Sie **Weiter**.

9. Wählen Sie eine Gruppenrichtlinie aus, um zu bestimmen, über welche S3-Zugriffsrechte die Mitglieder dieser Gruppe verfügen.
- **Kein S3-Zugriff:** Standard. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.
 - **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. Sie können diesen String nicht bearbeiten.
 - **Vollzugriff:** Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Sie können diesen String nicht bearbeiten.
 - **Benutzerdefiniert:** Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben. Anweisungen zur Implementierung einer S3-Client-Applikation finden Sie in den detaillierten Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispielen.
10. 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.

In diesem Beispiel dürfen Mitglieder der Gruppe nur einen Ordner auflisten und darauf zugreifen, der ihrem Benutzernamen (Schlüsselpräfix) im angegebenen Bucket entspricht. Beachten Sie, dass bei der Festlegung der Privatsphäre dieser Ordner Zugriffsberechtigungen aus anderen Gruppenrichtlinien und der Bucket-Richtlinie berücksichtigt werden sollten.

No S3 Access
 Read Only Access
 Full Access
 Custom
 (Must be a valid JSON formatted string.)

```

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

11. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:

- Verbundgruppe: **Gruppe erstellen**
- Lokale Gruppe: **Weiter**

Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

12. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können der Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer hinzufügen.

13. Wählen Sie **Fertig**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["S3 verwenden"](#)

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

Groups

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

2 groups Create group

Actions ▾

<input type="checkbox"/>	Name ↕	ID ↕	Type ↕	Access mode ↕
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beee0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

2. Wählen Sie **Gruppe erstellen**.

3. 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.

4. 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 dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.

5. Wählen Sie **Weiter**.

6. Wählen Sie einen Zugriffsmodus aus. 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.

- **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.
- **Schreibgeschützt:** Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

7. Legen Sie die Gruppenberechtigung fest.

- Aktivieren Sie das Kontrollkästchen **Root Access**, wenn sich Benutzer bei der Tenant Manager- oder Mandantenmanagement-API anmelden müssen. (Standard)
- Deaktivieren Sie das Kontrollkästchen **Root Access**, wenn Benutzer keinen Zugriff auf die Tenant Manager- oder Mandantenmanagement-API benötigen. Deaktivieren Sie beispielsweise das

Kontrollkästchen für Anwendungen, die nicht auf den Mandanten zugreifen müssen. Weisen Sie dann die **Swift Administrator**-Berechtigung zu, damit diese Benutzer Container und Objekte verwalten können.

8. Wählen Sie **Weiter**.

9. Aktivieren Sie das Kontrollkästchen **Swift Administrator**, wenn der Benutzer die Swift REST API verwenden muss.

Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

10. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:

- Verbundgruppe: **Gruppe erstellen**
- Lokale Gruppe: **Weiter**

Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

11. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können die Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer erstellen.

12. Wählen Sie **Fertig**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Verwenden Sie Swift"](#)

Anzeigen und Bearbeiten von Gruppendetails

Wenn Sie die Details für eine Gruppe anzeigen, können Sie den Anzeigenamen, Berechtigungen, Richtlinien und die Benutzer, die zu der Gruppe gehören, ändern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie den Namen der Gruppe aus, deren Details Sie anzeigen oder bearbeiten möchten.

Alternativ können Sie **Aktionen > Gruppendetails anzeigen** wählen.

Die Seite Gruppendetails wird angezeigt. Im folgenden Beispiel wird die Seite mit den S3-Gruppendetails angezeigt.

Overview

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

Group permissions

S3 group policy

Users

Manage group permissions

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

Access mode

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

Read-write Read-only

Group permissions

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

Root Access

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

Manage All Buckets

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

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

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

Save changes

3. Nehmen Sie bei Bedarf Änderungen an den Gruppeneinstellungen vor.



Um sicherzustellen, dass Ihre Änderungen gespeichert werden, wählen Sie **Änderungen speichern** aus, nachdem Sie Änderungen in jedem Abschnitt vorgenommen haben. Wenn Ihre Änderungen gespeichert sind, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.

a. Wählen Sie optional den Anzeigenamen oder das Bearbeitungssymbol aus  Um den Anzeigenamen zu aktualisieren.

Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

b. Optional können Sie die Berechtigungen aktualisieren.

c. Nehmen Sie für die Gruppenrichtlinie die entsprechenden Änderungen für Ihren S3- oder Swift-Mandanten vor.

- Wenn Sie eine Gruppe für einen S3-Mandanten bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus. Wenn Sie eine benutzerdefinierte S3-Richtlinie auswählen, aktualisieren Sie den JSON-String wie erforderlich.
- Wenn Sie eine Gruppe für einen Swift-Mandanten bearbeiten, aktivieren oder deaktivieren Sie das Kontrollkästchen **Swift Administrator**.

Weitere Informationen zum Swift Administrator erhalten Sie in den Anweisungen zum Erstellen von Gruppen für einen Swift-Mandanten.

d. Optional können Benutzer hinzugefügt oder entfernt werden.

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

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Erstellen von Gruppen für einen S3-Mandanten"](#)

["Erstellen von Gruppen für einen Swift Mandanten"](#)

Hinzufügen von Benutzern zu einer lokalen Gruppe

Sie können bei Bedarf Benutzer zu einer lokalen Gruppe hinzufügen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie den Namen der lokalen Gruppe aus, der Sie Benutzer hinzufügen möchten.

Alternativ können Sie **Aktionen > Gruppendetails anzeigen** wählen.

Die Seite Gruppendetails wird angezeigt.

Overview

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

Group permissions

S3 group policy

Users

Manage group permissions

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

Access mode

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

Read-write Read-only

Group permissions

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

Root Access

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

Manage All Buckets

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

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

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

Save changes

3. Wählen Sie **Benutzer verwalten** und dann **Benutzer hinzufügen**.

Username	Full Name	Denied
User_02	User_02_Managers	

4. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Benutzer hinzufügen**.

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	User_01	User_01_Applications	
<input type="checkbox"/>			

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Gruppennamen bearbeiten

Sie können den Anzeigenamen für eine Gruppe bearbeiten. Sie können den eindeutigen Namen für eine Gruppe nicht bearbeiten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, deren Anzeigename Sie bearbeiten möchten.
3. Wählen Sie **Aktionen > Gruppenname bearbeiten**.

Das Dialogfeld Gruppenname bearbeiten wird angezeigt.

Edit group name ✕

Specify a new name for the group **Applications**.

Must contain at least 1 and no more than 32 characters

Applications

Cancel Save changes

4. Wenn Sie eine lokale Gruppe bearbeiten, aktualisieren Sie den Anzeigenamen nach Bedarf.

Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

5. Wählen Sie **Änderungen speichern**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Duplizieren einer Gruppe

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Gruppe duplizieren**. Weitere Details zum Erstellen einer Gruppe finden Sie in den Anweisungen zum Erstellen von Gruppen für einen S3-Mandanten oder für einen Swift-Mandanten.
4. 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.

5. 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 dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.

6. Wählen Sie **Weiter**.

7. Ändern Sie bei Bedarf die Berechtigungen für diese Gruppe.

8. Wählen Sie **Weiter**.

9. Wenn Sie eine Gruppe für einen S3-Mandanten duplizieren, wählen Sie bei Bedarf aus den Optionsfeldern **S3-Richtlinie hinzufügen** eine andere Richtlinie aus. Wenn Sie eine benutzerdefinierte Richtlinie ausgewählt haben, aktualisieren Sie den JSON-String wie erforderlich.

10. Wählen Sie **Gruppe erstellen**.

Verwandte Informationen

["Erstellen von Gruppen für einen S3-Mandanten"](#)

["Erstellen von Gruppen für einen Swift Mandanten"](#)

["Mandantenmanagement-Berechtigungen"](#)

Löschen einer Gruppe

Sie können eine Gruppe aus dem System löschen. Benutzer, die nur zu dieser Gruppe gehören, können sich nicht mehr beim Mandantenmanager anmelden oder das Mandantenkonto verwenden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

Groups

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

2 groups Create group

Actions ▼

<input type="checkbox"/>	Name ↕	ID ↕	Type ↕	Access mode ↕
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beee0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

2. Aktivieren Sie die Kontrollkästchen für die Gruppen, die Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Gruppe löschen**.

Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie **Gruppe löschen**, um zu bestätigen, dass Sie die in der Bestätigungsmeldung angegebenen Gruppen löschen möchten.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Verwalten von lokalen Benutzern

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen zu einer Lese-/Schreib-Benutzergruppe mit Root Access-Berechtigung gehören.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager oder bei der Mandantenmanagement-API anmelden, auch wenn sie mithilfe von S3- oder Swift-Client-Applikationen auf die Ressourcen des Mandanten zugreifen können, basierend auf Gruppenberechtigungen.

Zugriff auf die Seite Benutzer

Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.

Users

View local and federated users. Edit properties and group membership of local users.

3 users Create user

Actions ▾

<input type="checkbox"/>	Username ▾	Full Name ▾	Denied ▾	Type ▾
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

Erstellen lokaler Benutzer

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

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

Swift-Benutzer, die keiner Gruppe angehören, haben weder Managementberechtigungen noch Swift-Container-Zugriff.

Schritte

1. Wählen Sie **Benutzer erstellen**.
2. Füllen Sie die folgenden Felder aus.
 - **Vollständiger Name:** Der vollständige Name für diesen Benutzer, zum Beispiel der vor- und Nachname einer Person oder der Name einer Anwendung.
 - **Benutzername:** Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden.
 - **Passwort:** Ein Passwort, das bei der Anmeldung des Benutzers verwendet wird.
 - **Passwort bestätigen:** Geben Sie dasselbe Passwort ein, das Sie im Feld Passwort eingegeben

haben.

- **Zugriff verweigern:** Wenn Sie **Ja** wählen, kann sich dieser Benutzer nicht beim Mandantenkonto anmelden, obwohl der Benutzer noch zu einer oder mehreren Gruppen gehört.

Als Beispiel können Sie diese Funktion verwenden, um die Fähigkeit eines Benutzers, sich anzumelden, vorübergehend auszusetzen.

3. Wählen Sie **Weiter**.

4. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu.

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

5. Wählen Sie **Benutzer erstellen**.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Benutzerdetails werden bearbeitet


Wenn Sie die Details für einen Benutzer bearbeiten, können Sie den vollständigen Namen und das Kennwort des Benutzers ändern, den Benutzer zu verschiedenen Gruppen hinzufügen und verhindern, dass der Benutzer auf den Mandanten zugreift.

Schritte

1. Wählen Sie in der Liste Benutzer den Namen des Benutzers aus, dessen Details Sie anzeigen oder bearbeiten möchten.

Alternativ können Sie das Kontrollkästchen für den Benutzer aktivieren und dann **Aktionen > Benutzerdetails anzeigen** wählen.

2. Nehmen Sie bei Bedarf Änderungen an den Benutzereinstellungen vor.

- a. Ändern Sie den vollständigen Namen des Benutzers nach Bedarf, indem Sie den vollständigen Namen oder das Bearbeiten-Symbol auswählen  Im Abschnitt Übersicht.

Sie können den Benutzernamen nicht ändern.

- b. Ändern Sie auf der Registerkarte **Passwort** das Kennwort des Benutzers nach Bedarf.
- c. Auf der Registerkarte **Zugriff** können Sie sich anmelden (wählen Sie **Nein**) oder verhindern, dass sich der Benutzer bei Bedarf anmelden kann (wählen Sie **Ja**).
- d. Fügen Sie auf der Registerkarte **Groups** den Benutzer zu Gruppen hinzu, oder entfernen Sie den Benutzer aus Gruppen nach Bedarf.
- e. Wählen Sie nach Bedarf für jeden Abschnitt **Änderungen speichern**.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Lokale Benutzer werden dupliziert

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

Schritte

1. Wählen Sie in der Liste Benutzer den Benutzer aus, den Sie duplizieren möchten.
2. Wählen Sie **Benutzer duplizieren**.
3. Ändern Sie die folgenden Felder für den neuen Benutzer.
 - **Vollständiger Name**: Der vollständige Name für diesen Benutzer, zum Beispiel der vor- und Nachname einer Person oder der Name einer Anwendung.
 - **Benutzername**: Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden.
 - **Passwort**: Ein Passwort, das bei der Anmeldung des Benutzers verwendet wird.
 - **Passwort bestätigen**: Geben Sie dasselbe Passwort ein, das Sie im Feld Passwort eingegeben haben.
 - **Zugriff verweigern**: Wenn Sie **Ja** wählen, kann sich dieser Benutzer nicht beim Mandantenkonto anmelden, obwohl der Benutzer noch zu einer oder mehreren Gruppen gehört.

Als Beispiel können Sie diese Funktion verwenden, um die Fähigkeit eines Benutzers, sich anzumelden, vorübergehend auszusetzen.

4. Wählen Sie **Weiter**.
5. Wählen Sie eine oder mehrere lokale Gruppen aus.

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

6. Wählen Sie **Benutzer erstellen**.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Lokale Benutzer werden gelöscht

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

Mit dem Tenant Manager können Sie lokale Benutzer löschen, aber keine föderierten Benutzer. Sie müssen die föderierte Identitätsquelle verwenden, um verbundene Benutzer zu löschen.

Schritte

1. Aktivieren Sie in der Liste Benutzer das Kontrollkästchen für den lokalen Benutzer, den Sie löschen möchten.
2. Wählen Sie **Aktionen > Benutzer löschen**.
3. Wählen Sie im Bestätigungsdialogfeld **Benutzer löschen** aus, um zu bestätigen, dass Sie den Benutzer aus dem System löschen möchten.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.