Verwalten von Gruppen und Benutzern

StorageGRID software

NetApp
October 21, 2025

Inhalt

Verwalten von Gruppen und Benutzern . . . 1
- Verwenden der Identitätsföderation . . . 1
  - Konfigurieren der Identitätsföderation für den Mandantenmanager . . . 1
  - Synchronisierung mit Identitätsquelle erzwingen . . . 5
  - Identitätsföderation deaktivieren . . . 5
  - Richtlinien zum Konfigurieren des OpenLDAP-Servers . . . 5
- Verwalten von Mandantengruppen . . . 6
  - Erstellen von Gruppen für einen S3-Mandanten . . . 6
  - Erstellen Sie Gruppen für einen Swift-Mandanten . . . 9
  - Berechtigungen zur Mandantenverwaltung . . . 11
  - Verwalten von Gruppen . . . 13
- Lokale Benutzer verwalten . . . 16
  - Erstellen Sie einen lokalen Benutzer . . . 17
  - Lokalen Benutzer anzeigen oder bearbeiten . . . 18
  - Duplizieren Sie den lokalen Benutzer . . . 19
    - Benutzerklon erneut versuchen . . . 20
  - Löschen eines oder mehrerer lokaler Benutzer . . . 20

Verwalten von Gruppen und Benutzern

Verwenden der Identitätsföderation

Durch die Verwendung der Identitätsföderation lässt sich das Einrichten von Mandantengruppen und Benutzern beschleunigen und Mandantenbenutzer können sich mit vertrauten Anmeldeinformationen beim Mandantenkonto anmelden.

Konfigurieren der Identitätsföderation für den Mandantenmanager

Sie können die Identitätsföderation für den Mandantenmanager konfigurieren, wenn Sie Mandantengruppen und Benutzer in einem anderen System wie Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server verwalten möchten.

Bevor Sie beginnen

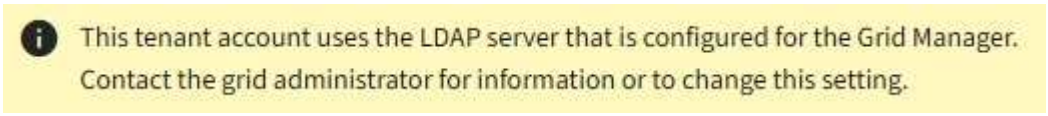
- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.

> Wenn Sie einen LDAP v3-Dienst verwenden möchten, der nicht aufgeführt ist, wenden Sie sich an den technischen Support.

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Sehen Richtlinien zum Konfigurieren des OpenLDAP-Servers .
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitätsanbieter TLS 1.2 oder 1.3 verwenden. Sehen "Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen" .

Informationen zu diesem Vorgang

Ob Sie einen Identitätsföderationsdienst für Ihren Mandanten konfigurieren können, hängt davon ab, wie Ihr Mandantenkonto eingerichtet wurde. Ihr Mandant nutzt möglicherweise den für den Grid Manager konfigurierten Identitätsföderationsdienst gemeinsam. Wenn diese Meldung beim Zugriff auf die Seite „Identitätsföderation“ angezeigt wird, können Sie für diesen Mandanten keine separate föderierte Identitätsquelle konfigurieren.

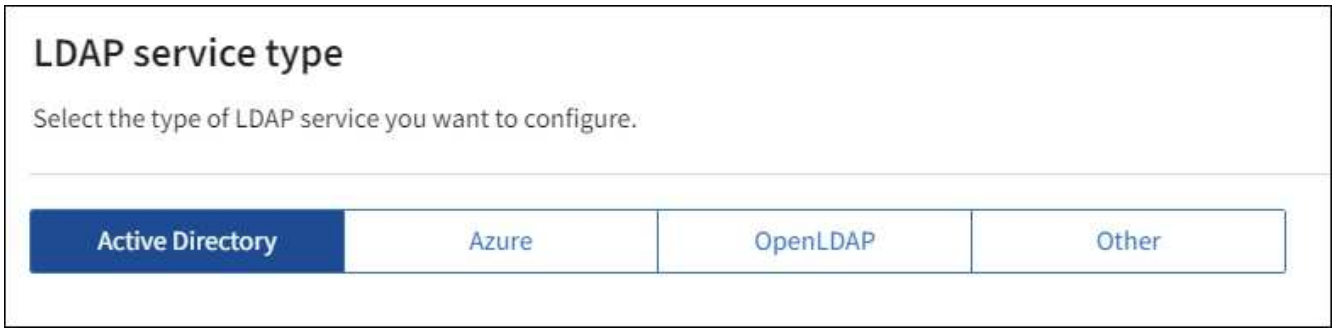


Konfiguration eingeben

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

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Identitätsföderation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt „LDAP-Diensttyp“ den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.



Wählen Sie **Andere** 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 ist gleichbedeutend mit `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 die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `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 Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
   - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `cn` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn` .
   - **Gruppen-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `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 Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Diensttypen die erforderlichen LDAP-Server- und Netzwerkverbindungsinformationen im Abschnitt „LDAP-Server konfigurieren“ ein.
   - **Hostname**: Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des LDAP-Servers.
   - **Port**: Der Port, der für die Verbindung mit dem LDAP-Server verwendet wird.

     Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden Port verwenden, solange Ihre Firewall richtig 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 Down-Level-Anmeldenamen oder den Benutzerprinzipalnamen angeben.

     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`
- **Azurblau**: `accountEnabled` Und `userPrincipalName`

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

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

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

> Die Werte für den **eindeutigen Gruppennamen** müssen innerhalb des **Gruppen-Basis-DN**, zu dem sie gehören, eindeutig sein.

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

> Die Werte für den **Eindeutigen Benutzernamen** müssen innerhalb des **Benutzerbasis-DN**, zu dem sie gehören, eindeutig sein.

◦ **Bind-Benutzernamenformat** (optional): Das Standardbenutzernamenmuster, das StorageGRID verwenden soll, wenn das Muster nicht automatisch ermittelt werden kann.

Es wird empfohlen, das **Bind-Benutzernamenformat** anzugeben, da dies Benutzern die Anmeldung ermöglichen kann, wenn StorageGRID keine Bindung mit dem Dienstkonto herstellen kann.

Geben Sie eines dieser Muster ein:

- **UserPrincipalName-Muster (Active Directory und Azure)**: `[USERNAME]@*example*.com`
- **Downlevel-Anmeldenamenmuster (Active Directory und Azure)**: `*example*\[USERNAME]`
- **Muster für eindeutige Namen**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

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

6. Wählen Sie im Abschnitt „Transport Layer Security (TLS)“ eine Sicherheitseinstellung aus.
   ◦ **STARTLS verwenden**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese Option wird 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.
   ◦ **TLS nicht verwenden**: Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.

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

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, das zum Sichern der Verbindung verwendet wird.
   - **CA-Zertifikat des Betriebssystems verwenden**: Verwenden Sie das standardmäßig auf dem Betriebssystem installierte 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 und fügen Sie es in das Textfeld „CA-Zertifikat“ ein.

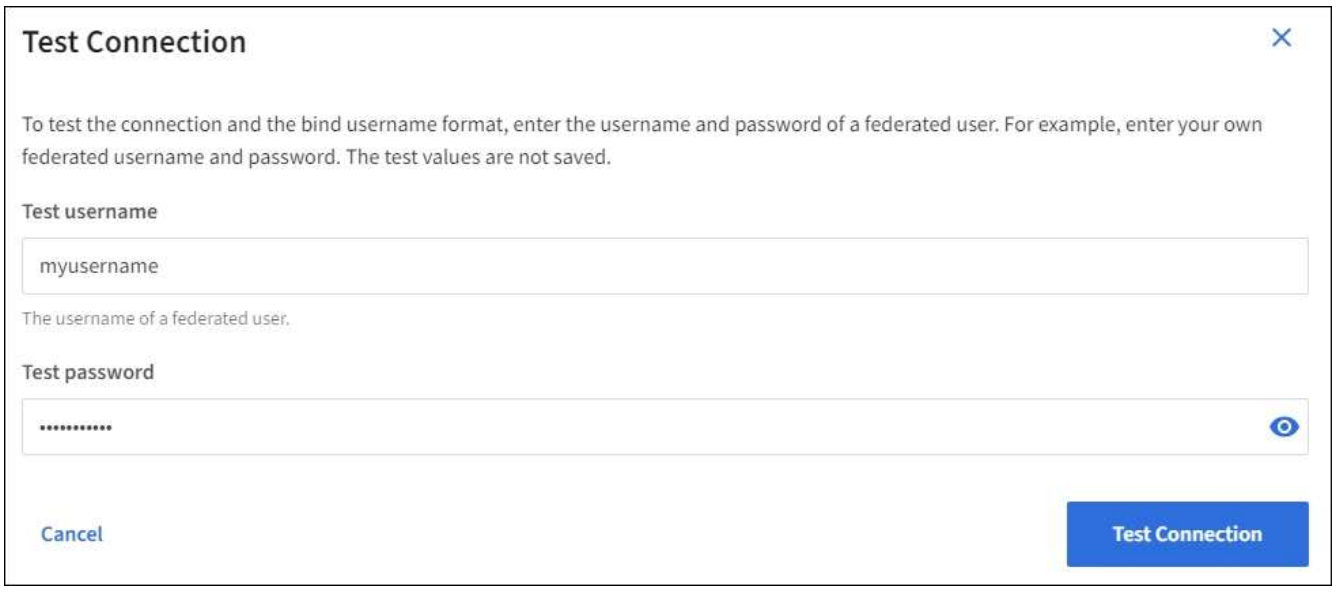
Testen Sie die Verbindung und speichern Sie die Konfiguration

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-Benutzernamenformat, falls Sie eines angegeben haben.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein Bind-Benutzernamenformat angegeben haben:
   - Bei gültigen Verbindungseinstellungen wird die Meldung „Verbindungstest erfolgreich“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
   - Bei ungültigen Verbindungseinstellungen erscheint die Meldung „Testverbindung konnte nicht hergestellt werden“. Wählen Sie **Schließen**. Beheben Sie dann alle Probleme und testen Sie die Verbindung erneut.
3. Wenn Sie ein Bind-Benutzernamenformat angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen Verbundbenutzers ein.

   Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr eigenes Passwort ein. Verwenden Sie im Benutzernamen keine Sonderzeichen wie @ oder /.



- Bei gültigen Verbindungseinstellungen wird die Meldung „Verbindungstest erfolgreich“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Wenn die Verbindungseinstellungen, das Bind-Benutzernamenformat oder der Testbenutzername und das Testkennwort ungültig sind, wird eine Fehlermeldung angezeigt. Beheben Sie alle Probleme und testen Sie die Verbindung erneut.

Synchronisierung mit Identitätsquelle erzwingen

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

Schritte

1. Gehen Sie zur Seite „Identitätsföderation“.
2. Wählen Sie oben auf der Seite **Sync-Server** aus.

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

> Die Warnung **Fehler bei der Synchronisierung der Identitätsföderation** wird ausgelöst, wenn beim Synchronisieren föderierter Gruppen und Benutzer aus der Identitätsquelle ein Problem auftritt.

Identitätsföderation deaktivieren

Sie können die Identitätsföderation für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, findet keine Kommunikation zwischen StorageGRID und der Identitätsquelle statt. Alle von Ihnen konfigurierten Einstellungen bleiben jedoch erhalten, sodass Sie die Identitätsföderation in Zukunft problemlos wieder aktivieren können.

Informationen zu diesem Vorgang

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundbenutzer können sich nicht anmelden.
- Verbundbenutzer, die derzeit angemeldet sind, behalten den Zugriff auf das StorageGRID -System, bis ihre Sitzung abläuft, können sich nach Ablauf ihrer Sitzung jedoch nicht mehr anmelden.
- Es findet keine Synchronisierung zwischen dem StorageGRID -System und der Identitätsquelle statt und es werden keine Warnungen für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn Single Sign-On (SSO) auf **Aktiviert** oder **Sandbox-Modus** eingestellt ist. Der SSO-Status auf der Single Sign-On-Seite muss **Deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Sehen "Deaktivieren der einmaligen Anmeldung" .

Schritte

1. Gehen Sie zur Seite „Identitätsföderation“.
2. Deaktivieren Sie das Kontrollkästchen **Identitätsföderation aktivieren**.

Richtlinien zum Konfigurieren des OpenLDAP-Servers

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 für extern deaktivierte Benutzer nicht automatisch. Um den S3-Zugriff zu blockieren, löschen Sie alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Memberof- und Refint-Overlays

Die Memberof- und Refint-Overlays sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur umgekehrten Pflege von Gruppenmitgliedschaften imhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP-Dokumentation: Administratorhandbuch Version 2.4"^] .

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Indexschlüsselwörtern 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.

Informationen zur umgekehrten Pflege von Gruppenmitgliedschaften finden Sie imhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP-Dokumentation: Administratorhandbuch Version 2.4"^] .

Verwalten von Mandantengruppen

Erstellen von Gruppen für einen S3-Mandanten

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie"konfigurierte Identitätsföderation" , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, haben Sie den Workflow und die Überlegungen für"Klonen von Mandantengruppen und Benutzern" , und Sie sind beim Quellraster des Mandanten angemeldet.

Greifen Sie auf den Assistenten „Gruppe erstellen“ zu

Rufen Sie als ersten Schritt den Assistenten „Gruppe erstellen“ auf.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, bestätigen Sie, dass ein blaues Banner angezeigt wird, das darauf hinweist, dass neue Gruppen, die in diesem Grid erstellt werden, in denselben Mandanten im anderen Grid in der Verbindung geklont werden. Wenn dieses Banner nicht angezeigt wird, sind Sie möglicherweise beim Zielraster des Mandanten angemeldet.

3. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp

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

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe**, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Verbundgruppe**, 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 Tenant Manager anmelden, obwohl sie Clientanwendungen verwenden können, um die Ressourcen des Mandanten basierend auf Gruppenberechtigungen zu verwalten.

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

     Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, tritt ein Klonfehler auf, wenn derselbe **eindeutige Name** für den Mandanten im Zielgrid bereits vorhanden ist.

   - **Föderierte Gruppe**: Geben Sie den eindeutigen Namen ein. Für Active Directory ist der eindeutige Name der Name, der mit dem `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der mit dem `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer im Tenant Manager und in der Tenant Management API ausführen können.

Schritte

1. Wählen Sie für **Zugriffsmodus** eine der folgenden Optionen aus:
   - **Lesen/Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Tenant-Konfiguration verwalten.
   - **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Tenant Manager oder in der Tenant Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.

   > Wenn ein Benutzer mehreren Gruppen angehört und für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Wählen Sie eine oder mehrere Berechtigungen für diese Gruppe aus.

   Sehen "Berechtigungen zur Mandantenverwaltung" .

3. Wählen Sie **Weiter**.

S3-Gruppenrichtlinie festlegen

Die Gruppenrichtlinie bestimmt, welche S3-Zugriffsberechtigungen Benutzer haben.

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 mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat standardmäßig nur der Root-Benutzer Zugriff auf S3-Ressourcen.
Nur-Lese-Zugriff	Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Beispielsweise können Benutzer dieser Gruppe Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine schreibgeschützte Gruppenrichtlinie im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
Vollzugriff	Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine Gruppenrichtlinie mit vollem Zugriff im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.

Gruppenrichtlinie	Beschreibung
Ransomware-Minderung	Diese Beispielrichtlinie gilt für alle Buckets dieses Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber keine Objekte dauerhaft aus Buckets löschen, für die die Objektversionierung aktiviert ist. Tenant Manager-Benutzer mit der Berechtigung **Alle Buckets verwalten** können diese Gruppenrichtlinie außer Kraft setzen. Beschränken Sie die Berechtigung „Alle Buckets verwalten“ auf vertrauenswürdige Benutzer und verwenden Sie, sofern verfügbar, die Multi-Faktor-Authentifizierung (MFA).
Brauch	Den Benutzern in der Gruppe werden die Berechtigungen erteilt, 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 eine gültige Zeichenfolge im JSON-Format eingeben.

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

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine föderierte Gruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig**.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional bereits vorhandene lokale Benutzer hinzufügen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, werden alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quell-Grid auswählen, nicht einbezogen, wenn die Gruppe in das Ziel-Grid geklont wird. Wählen Sie aus diesem Grund beim Erstellen der Gruppe keine Benutzer aus. 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**.

   Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

   Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie sich im Quell-Grid des Mandanten befinden, wird die neue Gruppe in das Ziel-Grid des Mandanten geklont. **Erfolg** wird als **Klonstatus** im Abschnitt „Übersicht“ der Detailseite der Gruppe angezeigt.

Erstellen Sie 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 Berechtigung „Swift-Administrator“ verfügen, die zum Verwalten der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.

> Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie"konfigurierte Identitätsföderation" , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Greifen Sie auf den Assistenten „Gruppe erstellen“ zu

Schritte

Rufen Sie als ersten Schritt den Assistenten „Gruppe erstellen“ auf.

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

Wählen Sie einen Gruppentyp

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

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe**, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Verbundgruppe**, 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 Tenant Manager anmelden, obwohl sie Clientanwendungen verwenden können, um die Ressourcen des Mandanten basierend auf Gruppenberechtigungen zu verwalten.

2. Geben Sie den Namen der Gruppe ein.
   - **Lokale Gruppe**: Geben Sie sowohl einen Anzeigenamen als auch einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
   - **Föderierte Gruppe**: Geben Sie den eindeutigen Namen ein. Für Active Directory ist der eindeutige Name der Name, der mit dem `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der mit dem `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer im Tenant Manager und in der Tenant Management API ausführen können.

Schritte

1. Wählen Sie für **Zugriffsmodus** eine der folgenden Optionen aus:

- **Lesen/Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Tenant-Konfiguration verwalten.
- **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Tenant Manager oder in der Tenant Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.

> Wenn ein Benutzer mehreren Gruppen angehört und für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Aktivieren Sie das Kontrollkästchen **Root-Zugriff**, wenn sich Gruppenbenutzer 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, 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 föderierte Gruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig**.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional bereits vorhandene lokale 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 auf der Seite „Benutzer“ zum Benutzer hinzufügen. Sehen "Lokale Benutzer verwalten" .

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

   Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Berechtigungen zur Mandantenverwaltung

Überlegen Sie vor dem Erstellen einer Mandantengruppe, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Die Berechtigungen zur Mandantenverwaltung legen fest, welche Aufgaben Benutzer mit dem Mandantenmanager oder der Mandantenverwaltungs-API ausführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen sind kumulativ, wenn ein Benutzer mehreren Gruppen angehört.

Um sich beim Tenant Manager anzumelden oder die Tenant Management API zu verwenden, müssen Benutzer einer Gruppe angehören, die über mindestens eine Berechtigung verfügt. Alle Benutzer, die sich

anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Das eigene Passwort ändern (für lokale Benutzer)

Bei allen Berechtigungen bestimmt die Einstellung „Zugriffsmodus“ der Gruppe, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie die zugehörigen Einstellungen und Funktionen nur anzeigen können.

> Wenn ein Benutzer mehreren Gruppen angehört und für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff 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.

Erlaubnis	Beschreibung	Details
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Tenant Management API.	Swift-Benutzer müssen über Root-Zugriffsberechtigungen verfügen, um sich beim Mandantenkonto anmelden zu können.
Administrator	Nur Swift-Mieter. Bietet vollständigen Zugriff auf die Swift-Container und -Objekte für dieses Mandantenkonto	Swift-Benutzer müssen über die Berechtigung „Swift-Administrator“ verfügen, um Vorgänge mit der Swift-REST-API ausführen zu können.
Verwalten Sie Ihre eigenen S3-Anmeldeinformationen	Ermöglicht Benutzern das Erstellen und Entfernen eigener S3-Zugriffsschlüssel.	Benutzer ohne diese Berechtigung sehen die Menüoption **STORAGE (S3)** > **Meine S3-Zugriffsschlüssel** nicht.
Alle Eimer anzeigen	**S3-Mandanten**: Ermöglicht Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen. **Swift-Mandanten**: Ermöglicht Swift-Benutzern, alle Container und Containerkonfigurationen mithilfe der Tenant Management API anzuzeigen.	Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption **Buckets** nicht sehen. Diese Berechtigung wird durch die Berechtigung „Alle Buckets verwalten“ ersetzt. Es hat keine Auswirkungen auf S3-Bucket- oder Gruppenrichtlinien, die von S3-Clients oder der S3-Konsole verwendet werden. Sie können diese Berechtigung nur Swift-Gruppen über die Tenant Management API zuweisen. Sie können diese Berechtigung nicht mithilfe des Mandanten-Managers Swift-Gruppen zuweisen.

Erlaubnis	Beschreibung	Details
Alle Buckets verwalten	**S3-Mandanten**: Ermöglicht Benutzern die Verwendung des Mandantenmanagers und der Mandantenverwaltungs-API zum Erstellen und Löschen von S3-Buckets und zum Verwalten der Einstellungen für alle S3-Buckets im Mandantenkonto, unabhängig von S3-Bucket- oder Gruppenrichtlinien. **Swift-Mandanten**: Ermöglicht Swift-Benutzern, die Konsistenz für Swift-Container mithilfe der Tenant Management API zu steuern.	Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption **Buckets** nicht sehen. Diese Berechtigung ersetzt die Berechtigung „Alle Buckets anzeigen“. Es hat keine Auswirkungen auf S3-Bucket- oder Gruppenrichtlinien, die von S3-Clients oder der S3-Konsole verwendet werden. Sie können diese Berechtigung nur Swift-Gruppen über die Tenant Management API zuweisen. Sie können diese Berechtigung nicht mithilfe des Mandanten-Managers Swift-Gruppen zuweisen.
Verwalten von Endpunkten	Ermöglicht Benutzern die Verwendung des Tenant Managers oder der Tenant Management API zum Erstellen oder Bearbeiten von Plattformdienst-Endpunkten, die als Ziel für StorageGRID -Plattformdienste verwendet werden.	Benutzern ohne diese Berechtigung wird die Menüoption **Plattformdienst-Endpunkte** nicht angezeigt.
Registerkarte „S3-Konsole verwenden“	In Kombination mit der Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ können Benutzer Objekte über die Registerkarte „S3-Konsole“ auf der Detailseite für einen Bucket anzeigen und verwalten.	

Verwalten von Gruppen

Verwalten Sie Ihre Mandantengruppen nach Bedarf, um eine Gruppe anzuzeigen, zu bearbeiten oder zu duplizieren und mehr.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .

Gruppe anzeigen oder bearbeiten

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

Schritte

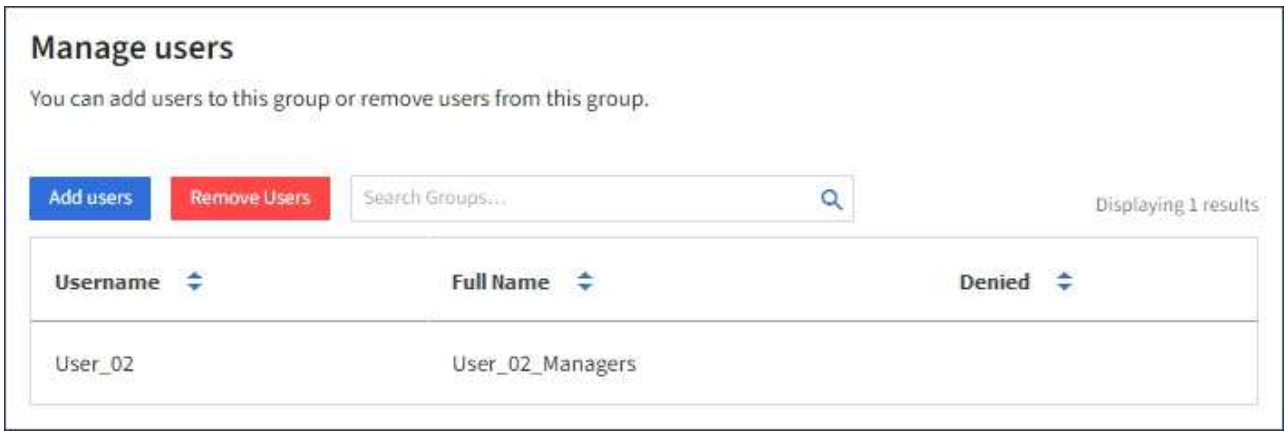
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Überprüfen Sie die Informationen auf der Seite „Gruppen“, auf der grundlegende Informationen zu allen lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

Wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie Gruppen im Quell-Grid des Mandanten anzeigen:

- Eine Bannermeldung weist darauf hin, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie eine Gruppe bearbeiten oder entfernen.
- Bei Bedarf zeigt eine Bannermeldung an, ob Gruppen nicht auf den Mandanten im Zielraster geklont wurden. Du kannstErneuter Versuch eines Gruppenklons das ist fehlgeschlagen.

3. Wenn Sie den Namen der Gruppe ändern möchten:
   a. Aktivieren Sie das Kontrollkästchen für die Gruppe.
   b. Wählen Sie **Aktionen** > **Gruppennamen bearbeiten**.
   c. Geben Sie den neuen Namen ein.
   d. Wählen Sie **Änderungen speichern**.
4. Wenn Sie weitere Details anzeigen oder zusätzliche 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 **Aktionen** > **Gruppendetails anzeigen**.
5. Sehen Sie sich den Abschnitt „Übersicht“ an, der für jede Gruppe die folgenden Informationen enthält:
   - Anzeigename
   - Eindeutiger Name
   - Typ
   - Zugriffsmodus
   - Berechtigungen
   - S3-Richtlinie
   - Anzahl der Benutzer in dieser Gruppe
   - Zusätzliche Felder, wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie die Gruppe im Quell-Grid des Mandanten anzeigen:
     - Klonstatus, entweder **Erfolg** oder **Fehler**
     - Ein blaues Banner zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diese Gruppe bearbeiten oder löschen.
6. Bearbeiten Sie die Gruppeneinstellungen nach Bedarf. Sehen"Erstellen von Gruppen für einen S3-Mandanten" Und"Erstellen Sie Gruppen für einen Swift-Mandanten" für Details zu den einzugebenden Informationen.
   a. Ändern Sie im Abschnitt „Übersicht“ den Anzeigenamen, indem Sie den Namen oder das Bearbeitungssymbol auswählen .
   b. Aktualisieren Sie auf der Registerkarte **Gruppenberechtigungen** die Berechtigungen und wählen Sie **Änderungen speichern**.
   c. Nehmen Sie auf der Registerkarte **Gruppenrichtlinie** die gewünschten 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 die JSON-Zeichenfolge 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 erscheint eine Erfolgsmeldung.

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 erscheint eine Erfolgsmeldung.

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

Gruppe duplizieren

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

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie eine Gruppe aus dem Quell-Grid des Mandanten duplizieren, wird die duplizierte Gruppe in das Ziel-Grid 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. Sehen"Erstellen von Gruppen für einen S3-Mandanten" oder"Erstellen Sie Gruppen für einen Swift-Mandanten" für Details zu den einzugebenden Informationen.
5. Wählen Sie **Gruppe erstellen**.

Gruppenklon erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klonvorgang:

1. Wählen Sie jede Gruppe aus, bei der unter dem Gruppennamen *(Klonen fehlgeschlagen)* angezeigt wird.
2. Wählen Sie **Aktionen** > **Gruppen klonen**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jeder Gruppe an, die Sie klonen.

Weitere Informationen finden Sie unter"Mandantengruppen und Benutzer klonen" .

Löschen einer oder mehrerer Gruppen

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

> ⓘ Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie eine Gruppe löschen, löscht StorageGRID die entsprechende Gruppe im anderen Grid nicht. 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**.

Lokale Benutzer verwalten

Sie können lokale Benutzer erstellen und sie lokalen Gruppen zuweisen, um festzulegen, auf welche Funktionen diese Benutzer zugreifen können. Der Tenant Manager umfasst einen vordefinierten lokalen Benutzer namens „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 Tenant Management API anmelden, obwohl sie basierend auf Gruppenberechtigungen Clientanwendungen verwenden können, um auf die Ressourcen des Mandanten zuzugreifen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, haben Sie den Workflow und die Überlegungen für"Klonen von Mandantengruppen und Benutzern" , und Sie sind beim Quellraster des Mandanten angemeldet.

Erstellen Sie einen lokalen Benutzer

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

Auf S3-Benutzer, die keiner Gruppe angehören, werden keine Verwaltungsberechtigungen oder S3-Gruppenrichtlinien angewendet. Diesen Benutzern wird möglicherweise über eine Bucket-Richtlinie Zugriff auf den S3-Bucket gewährt.

Swift-Benutzer, die keiner Gruppe angehören, verfügen weder über Verwaltungsberechtigungen noch über Zugriff auf Swift-Container.

Greifen Sie auf den Assistenten „Benutzer erstellen“ zu

Schritte

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

   Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, zeigt ein blaues Banner an, dass dies das Quell-Grid des Mandanten ist. Alle lokalen Benutzer, die Sie in diesem Raster erstellen, werden in das andere Raster in der Verbindung geklont.

2. Wählen Sie **Benutzer erstellen**.

Anmeldeinformationen eingeben

Schritte

1. Füllen Sie für den Schritt **Benutzeranmeldeinformationen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Vollständiger Name	Der vollständige Name dieses Benutzers, beispielsweise der Vor- und Nachname einer Person oder der Name einer Anwendung.
Benutzername	Der Name, den dieser Benutzer zum Anmelden verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden. **Hinweis**: Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, tritt ein Klonfehler auf, wenn derselbe **Benutzername** für den Mandanten im Zielgrid bereits vorhanden ist.
Passwort und Passwort bestätigen	Das Kennwort, das der Benutzer zunächst bei der Anmeldung verwendet.
Zugriff verweigern	Wählen Sie **Ja** aus, um zu verhindern, dass sich dieser Benutzer beim Mandantenkonto anmeldet, auch wenn er möglicherweise noch einer oder mehreren Gruppen angehört. Wählen Sie beispielsweise **Ja** aus, um die Anmeldemöglichkeit eines Benutzers vorübergehend zu sperren.

2. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

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

   Die Zuweisung eines Benutzers zu Gruppen ist optional. Wenn Sie möchten, können Sie beim Erstellen oder Bearbeiten von Gruppen Benutzer auswählen.

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

2. Wählen Sie **Benutzer erstellen**.

   Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie sich im Quell-Grid des Mandanten befinden, wird der neue lokale Benutzer in das Ziel-Grid des Mandanten geklont. **Erfolg** wird als **Klonstatus** im Abschnitt „Übersicht“ der Detailseite des Benutzers angezeigt.

3. Wählen Sie **Fertig**, um zur Seite „Benutzer“ 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 zu allen lokalen und föderierten Benutzern für dieses Mandantenkonto aufgeführt sind.

   Wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie den Benutzer im Quell-Grid des Mandanten anzeigen:

   - Eine Bannermeldung weist darauf hin, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie einen Benutzer bearbeiten oder entfernen.
   - Bei Bedarf zeigt eine Bannermeldung an, ob Benutzer nicht in den Mandanten im Zielraster geklont wurden. Sie können Wiederholen Sie den Versuch, einen fehlgeschlagenen Benutzerklon auszuführen .

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 zusätzliche 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. Sehen Sie sich den Abschnitt „Übersicht“ an, in dem für jeden Benutzer die folgenden Informationen angezeigt werden:

- Vollständiger Name
- Benutzername
- Benutzertyp
- Zugriff verweigert
- Zugriffsmodus
- Gruppenmitgliedschaft
- Zusätzliche Felder, wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie den Benutzer im Quell-Grid des Mandanten anzeigen:
  - Klonstatus, entweder **Erfolg** oder **Fehler**
  - Ein blaues Banner zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diesen Benutzer bearbeiten.

6. Bearbeiten Sie die Benutzereinstellungen nach Bedarf. SehenLokalen Benutzer erstellen für Details zu den einzugebenden Informationen.
   a. Ändern Sie im Abschnitt „Übersicht“ den vollständigen Namen, indem Sie den Namen oder das Bearbeitungssymbol 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 **Zugriff Nein** aus, um dem Benutzer die Anmeldung zu erlauben, oder wählen Sie **Ja** aus, um die Anmeldung des Benutzers zu verhindern. Wählen Sie dann **Änderungen speichern** aus.
   d. Wählen Sie auf der Registerkarte **Zugriffsschlüssel** die Option **Schlüssel erstellen** und folgen Sie den Anweisungen für"Erstellen der S3-Zugriffsschlüssel eines anderen Benutzers" .
   e. Wählen Sie auf der Registerkarte **Gruppen** die Option **Gruppen bearbeiten** aus, um den Benutzer zu Gruppen hinzuzufügen oder aus Gruppen zu entfernen. Wählen Sie dann **Änderungen speichern**.
7. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt die Option **Änderungen speichern** ausgewählt haben.

Duplizieren Sie den lokalen Benutzer

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

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie einen Benutzer aus dem Quell-Grid des Mandanten duplizieren, wird der duplizierte Benutzer in das Ziel-Grid 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. SehenLokalen Benutzer erstellen für Details zu den einzugebenden Informationen.
5. Wählen Sie **Benutzer erstellen**.

Benutzerklon erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klonvorgang:

1. Wählen Sie jeden Benutzer aus, bei dem unter dem Benutzernamen *(Klonen fehlgeschlagen)* angezeigt wird.
2. Wählen Sie **Aktionen** > **Benutzer klonen**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jedes Benutzers an, den Sie klonen.

Weitere Informationen finden Sie unter"Mandantengruppen und Benutzer klonen" .

Löschen eines oder mehrerer lokaler Benutzer

Sie können einen oder mehrere lokale Benutzer dauerhaft löschen, die keinen Zugriff mehr auf das StorageGRID Mandantenkonto benötigen.

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

> Sie müssen die Verbundidentitätsquelle verwenden, um Verbundbenutzer 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**.