



# **Kontrolle des Administratorzugriffs auf StorageGRID**

StorageGRID 11.5

NetApp  
April 11, 2024

# Inhalt

- Kontrolle des Administratorzugriffs auf StorageGRID ..... 1
  - Zugriffskontrolle durch Firewalls ..... 1
  - Identitätsföderation verwenden ..... 2
  - Verwalten von Admin-Gruppen ..... 7
  - Verwalten von lokalen Benutzern ..... 15
  - Verwenden von Single Sign On (SSO) für StorageGRID ..... 18
  - Administrator-Client-Zertifikate werden konfiguriert ..... 36

# Kontrolle des Administratorzugriffs auf StorageGRID

Sie können den Administratorzugriff auf das StorageGRID-System steuern, indem Sie Firewall-Ports öffnen oder schließen, Administratorgruppen und Benutzer verwalten, SSO konfigurieren und Client-Zertifikate für den sicheren externen Zugriff auf StorageGRID-Metriken bereitstellen.

- ["Zugriffskontrolle durch Firewalls"](#)
- ["Identitätsföderation verwenden"](#)
- ["Verwalten von Admin-Gruppen"](#)
- ["Verwalten von lokalen Benutzern"](#)
- ["Verwenden von Single Sign On \(SSO\) für StorageGRID"](#)
- ["Administrator-Client-Zertifikate werden konfiguriert"](#)

## Zugriffskontrolle durch Firewalls

Wenn Sie den Zugriff über Firewalls steuern möchten, öffnen oder schließen Sie bestimmte Ports an der externen Firewall.

### Kontrolle des Zugriffs an der externen Firewall

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise möchten Sie verhindern, dass Mandanten sich an der Firewall mit dem Grid Manager verbinden können, und zwar zusätzlich über andere Methoden zur Steuerung des Systemzugriffs.

Port	Beschreibung	Port offen...
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen.  <b>Hinweis:</b> Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	<ul style="list-style-type: none"><li>• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen.</li><li>• Webbrowser und Management-API-Clients können nicht auf den Mandanten-Manager oder die Mandanten-Management-API zugreifen.</li><li>• Anfragen nach internen Inhalten werden abgelehnt.</li></ul>

Port	Beschreibung	Port offen...
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	<ul style="list-style-type: none"> <li>• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Mandanten-Manager und die Mandanten-Management-API zugreifen.</li> <li>• Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid Management API zugreifen.</li> <li>• Anfragen nach internen Inhalten werden abgelehnt.</li> </ul>



Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

### Verwandte Informationen

["Melden Sie sich beim Grid Manager an"](#)

["Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet"](#)

["Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen"](#)

["Verwalten von nicht vertrauenswürdigen Client-Netzwerken"](#)

["Installieren Sie Ubuntu oder Debian"](#)

["VMware installieren"](#)

["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)

## Identitätsföderation verwenden

Durch die Verwendung von Identity Federation lassen sich Gruppen und Benutzer schneller einrichten, und Benutzer können sich mithilfe vertrauter Anmeldedaten bei StorageGRID anmelden.

### Identitätsföderation wird konfiguriert

Sie können einen Identitätsverbund konfigurieren, wenn Administratorgruppen 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 Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie Single Sign-On (SSO) aktivieren möchten, müssen Sie Active Directory als föderierte Identitätsquelle und AD FS als Identitäts-Provider verwenden. Siehe „Anforderungen für die Verwendung von Single Sign-On.“
- 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

Sie müssen eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie die folgenden Typen von föderierten Gruppen importieren möchten:

- Verwaltungsgruppen. Die Benutzer in Admin-Gruppen können sich beim Grid Manager anmelden und anhand der Verwaltungsberechtigungen, die der Gruppe zugewiesen sind, Aufgaben ausführen.
- Mandanten-Benutzergruppen für Mandanten, die ihre eigene Identitätsquelle nicht verwenden Benutzer in Mandantengruppen können sich beim Mandanten-Manager anmelden und Aufgaben ausführen, basierend auf den Berechtigungen, die der Gruppe im Mandanten-Manager zugewiesen sind.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Identitätsföderation**.
2. Wählen Sie **Identitätsföderation aktivieren**.

Die Felder zum Konfigurieren des LDAP-Servers werden angezeigt.

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

Sie können **Active Directory**, **OpenLDAP** oder **Other** auswählen.



Wenn Sie **OpenLDAP** auswählen, müssen Sie den OpenLDAP-Server konfigurieren. 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.



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

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.
  - **Verwenden Sie das Betriebssystem CA-Zertifikat:** Verwenden Sie das auf dem Betriebssystem installierte Standard-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 optional **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 Beispielkonfigurationswerte für einen LDAP-Server, der Active Directory verwendet.

## Verwandte Informationen

["Unterstützte Chiffren für ausgehende TLS-Verbindungen"](#)

["Anforderungen für die Nutzung von Single Sign On"](#)

["Erstellen eines Mandantenkontos"](#)

["Verwenden Sie ein Mandantenkonto"](#)

## 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.

### Verwandte Informationen

["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"](#)

## 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 Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die Identitätsquelle muss aktiviert sein.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Identitätsföderation**.

Die Seite Identity Federation wird angezeigt. Die Schaltfläche **Synchronisieren** befindet sich am unteren Rand der Seite.

#### Synchronize

---

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. Klicken Sie Auf **Synchronisieren**.

Eine Bestätigungsmeldung gibt an, dass die Synchronisierung erfolgreich gestartet wurde. Der Synchronisierungsprozess kann je nach Umgebung einige Zeit in Anspruch nehmen.



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

## Identitätsföderation deaktivieren

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

### Was Sie benötigen



- Sie müssen über einen unterstützten Browser beim Grid 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 sich derzeit anmelden, erhalten bis zu ihrem Ablauf Zugriff auf das StorageGRID-System, können sich jedoch nach Ablauf der Sitzung nicht anmelden.
- Die Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle erfolgt nicht, und Warnmeldungen oder Alarme werden nicht für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn Single Sign-On (SSO) auf **Enabled** oder **Sandbox Mode** gesetzt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Identitätsföderation**.
2. Deaktivieren Sie das Kontrollkästchen \* Identitätsföderation aktivieren\*.
3. Klicken Sie Auf **Speichern**.

### Verwandte Informationen

["Deaktivieren der Einzelanmeldung"](#)

## Verwalten von Admin-Gruppen

Sie können Administratorgruppen erstellen, um die Sicherheitsberechtigungen für einen oder mehrere Admin-Benutzer zu verwalten. Benutzer müssen zu einer Gruppe gehören, die Zugriff auf das StorageGRID-System gewährt.

### Erstellen von Admin-Gruppen

Administratorgruppen ermöglichen es Ihnen, festzulegen, welche Benutzer auf welche Funktionen und Vorgänge im Grid Manager und in der Grid Management API zugreifen können.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie einen Identitätsverbund konfiguriert haben, und die föderierte Gruppe muss bereits in der konfigurierten Identitätsquelle vorhanden sein.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Gruppen**.

Die Seite Admin Groups wird angezeigt und enthält alle vorhandenen Admin-Gruppen.

## Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.

+ Add Clone Edit Remove			
Name	ID	Group Type ?	Access Mode ?
<input checked="" type="radio"/> Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/> Simpson	cc8ad11f-68d0-f84a-af29-e7a6fc63a2	Federated	Read-only
<input type="radio"/> ILM (read-only_group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/> API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/> ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/> Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write

Group Type  Show  rows per page

### 2. Wählen Sie **Hinzufügen**.

Das Dialogfeld Gruppe hinzufügen wird angezeigt.

## Add Group

Create a new local group or import a group from the external identity source.

Group Type ?  Local  Federated

Display Name

Unique Name ?

Access Mode ?  Read-write  Read-only

### Management Permissions

- |  |   |
|--|---|
| <input type="checkbox"/> Root Access ?                 | <input type="checkbox"/> Manage Alerts ?                    |
| <input type="checkbox"/> Acknowledge Alarms ?          | <input type="checkbox"/> Grid Topology Page Configuration ? |
| <input type="checkbox"/> Other Grid Configuration ?    | <input type="checkbox"/> Tenant Accounts ?                  |
| <input type="checkbox"/> Change Tenant Root Password ? | <input type="checkbox"/> Maintenance ?                      |
| <input type="checkbox"/> Metrics Query ?               | <input type="checkbox"/> ILM ?                              |
| <input type="checkbox"/> Object Metadata Lookup ?      | <input type="checkbox"/> Storage Appliance Administrator ?  |

Cancel

Save

3. Wählen Sie für den Gruppentyp **Lokal** aus, wenn Sie eine Gruppe erstellen möchten, die nur innerhalb von StorageGRID verwendet werden soll, oder wählen Sie **föderiert** aus, wenn Sie eine Gruppe aus der Identitätsquelle importieren möchten.
4. Wenn Sie **Lokal** ausgewählt haben, geben Sie einen Anzeigenamen für die Gruppe ein. Der Anzeigename ist der Name, der im Grid Manager angezeigt wird. Zum Beispiel: „MWartung Benutzer“ oder „ILM-Administratoren“
5. Geben Sie einen eindeutigen Namen für die Gruppe ein.
  - **Lokal**: Geben Sie einen eindeutigen Namen ein. Beispiel: „ILM-Administratoren“
  - **Federated**: Geben Sie den Namen der Gruppe genau so ein, wie er in der konfigurierten Identitätsquelle angezeigt wird.
6. Wählen Sie unter **Zugriffsmodus** aus, ob Benutzer in der Gruppe Einstellungen ändern und Vorgänge im Grid Manager und der Grid Management API ausführen können oder ob sie nur Einstellungen und Funktionen anzeigen können.
  - **Lesen-Schreiben** (Standard): Benutzer können Einstellungen ändern und die Operationen durchführen, die durch ihre Verwaltungsberechtigungen erlaubt sind.
  - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge im Grid Manager oder der Grid Management API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf **schreibgeschützt** gesetzt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Features.

7. Wählen Sie eine oder mehrere Verwaltungsberechtigungen aus.

Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen. Andernfalls können sich Benutzer der Gruppe nicht bei StorageGRID anmelden.

8. Wählen Sie **Speichern**.

Die neue Gruppe wird erstellt. Wenn es sich um eine lokale Gruppe handelt, können Sie jetzt einen oder mehrere Benutzer hinzufügen. Wenn es sich um eine föderierte Gruppe handelt, verwaltet die Identitätsquelle, welche Benutzer der Gruppe angehören.

## Verwandte Informationen

["Verwalten von lokalen Benutzern"](#)

## Berechtigungen für Admin-Gruppen

Beim Erstellen von Admin-Benutzergruppen wählen Sie eine oder mehrere Berechtigungen, um den Zugriff auf bestimmte Funktionen des Grid Manager zu steuern. Sie können dann jeden Benutzer einer oder mehreren dieser Admin-Gruppen zuweisen, um zu bestimmen, welche Aufgaben der Benutzer ausführen kann.

Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen. Andernfalls können sich Benutzer, die dieser Gruppe angehören, nicht beim Grid Manager anmelden.

Standardmäßig kann jeder Benutzer, der zu einer Gruppe mit mindestens einer Berechtigung gehört, die folgenden Aufgaben ausführen:

- Melden Sie sich beim Grid Manager an

- Zeigen Sie das Dashboard an
- Zeigen Sie die Seiten Knoten an
- Monitoring der Grid-Topologie
- Anzeige aktueller und aufgelöster Warnmeldungen
- Aktuelle und historische Alarme anzeigen (Legacy-System)
- Eigenes Kennwort ändern (nur lokale Benutzer)
- Zeigen Sie bestimmte Informationen auf den Seiten Konfiguration und Wartung an

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Admin-Gruppe zuweisen können. Für alle nicht explizit genannten Funktionen ist die Root-Zugriffsberechtigung erforderlich.

### Root-Zugriff

Mit dieser Berechtigung erhalten Sie Zugriff auf alle Grid-Administrationsfunktionen.

### Verwalten Von Warnmeldungen

Mit dieser Berechtigung erhalten Sie Zugriff auf Optionen zum Verwalten von Warnmeldungen. Benutzer müssen über diese Berechtigung verfügen, um Stille, Warnmeldungen und Alarmregeln zu verwalten.

### Quittierung von Alarmen (Altsystem)

Diese Berechtigung ermöglicht den Zugriff auf Quittierung und Reaktion auf Alarme (Altsystem). Alle Benutzer, die angemeldet sind, können aktuelle und historische Alarme anzeigen.

Wenn ein Benutzer die Grid-Topologie überwachen und nur Alarme quittieren soll, sollten Sie diese Berechtigung zuweisen.

### Konfiguration Der Seite Grid Topology

Mit dieser Berechtigung haben Sie Zugriff auf die folgenden Menüoptionen:

- Konfigurationsregisterkarten auf den Seiten **Support > Tools > Grid Topology**.
- **Ereignisanzahl zurücksetzen**-Link auf der Registerkarte **Knoten > Ereignisse**.

### Andere Grid-Konfiguration

Diese Berechtigung ermöglicht den Zugriff auf zusätzliche Grid-Konfigurationsoptionen.



Um diese zusätzlichen Optionen zu sehen, müssen Benutzer auch über die Berechtigung für die Konfiguration der Grid Topology-Seite verfügen.

- **Alarme (Altsystem):**
  - Globale Alarme
  - Einrichtung Alter E-Mail-Adresse
- **ILM:**
  - Storage-Pools

- Storage-Klasse
- **Konfiguration > Netzwerkeinstellungen**
  - Verbindungskosten
- **Konfiguration > Systemeinstellungen:**
  - Anzeigeoptionen
  - Grid-Optionen
  - Storage-Optionen
- **Konfiguration > Überwachung:**
  - Veranstaltungen
- \* Support\*:
  - AutoSupport

## Mandantenkonten

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **Mieter > Mandantenkonten**.



Version 1 der Grid Management API (die veraltet ist) verwendet diese Berechtigung, um Mandantengruppenrichtlinien zu managen, Swift-Admin-Passwörter zurückzusetzen und S3-Zugriffsschlüssel für den Root-Benutzer zu verwalten.

## Root-Passwort Des Mandanten Ändern

Mit dieser Berechtigung erhalten Sie Zugriff auf die Option **Root Passwort ändern** auf der Seite Mandantenkonten, mit der Sie steuern können, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern kann. Benutzer, die diese Berechtigung nicht besitzen, können die Option **Root Passwort ändern** nicht sehen.



Sie müssen der Gruppe die Berechtigungen für Mandantenkonten zuweisen, bevor Sie diese Berechtigung zuweisen können.

## Wartung

Mit dieser Berechtigung haben Sie Zugriff auf die folgenden Menüoptionen:

- **Konfiguration > Systemeinstellungen:**
  - Domain-Namen\*
  - Server-Zertifikate\*
- **Konfiguration > Überwachung:**
  - Audit\*
- **Konfiguration > Zugangskontrolle:**
  - Grid-Passwörter
- **Wartung > Wartungsaufgaben**
  - Ausmustern
  - Erweiterung

- Recovery
- **Wartung > Netzwerk:**
  - DNS-Server\*
  - Grid-Netzwerk\*
  - NTP-Server\*
- **Wartung > System:**
  - Lizenz\*
  - Wiederherstellungspaket
  - Software-Update
- **Support > Tools:**
  - Protokolle
- Benutzer, die nicht über die Wartungsberechtigung verfügen, können die mit einem Sternchen gekennzeichneten Seiten anzeigen, jedoch nicht bearbeiten.

### Abfrage Von Kennzahlen

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **Support > Tools > Metriken**. Diese Berechtigung bietet auch Zugriff auf benutzerdefinierte Prometheus-metrische Abfragen unter Verwendung des Abschnitts **Metriken** der Grid Management API.

### ILM

Diese Berechtigung bietet Zugriff auf die folgenden **ILM** Menüoptionen:

- \* Erasure Coding\*
- **Regeln**
- **Richtlinien**
- **Regionen**



Der Zugriff auf die Menüoptionen **ILM > Storage Pools** und **ILM > Storage Klasse** wird über die anderen Berechtigungen für die Konfiguration der Grid-Konfiguration und Grid-Topologie-Seite gesteuert.

### Lookup Von Objektmetadaten

Mit dieser Berechtigung haben Sie Zugriff auf das Menü **ILM > Object Metadaten Lookup**.

### Storage Appliance Administrator

Mit dieser Berechtigung erhalten Sie über den Grid Manager Zugriff auf den SANtricity System Manager der E-Series auf Storage Appliances.

### Interaktion zwischen Berechtigungen und Zugriffsmodus

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**

gesetzt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Features.

## Deaktivieren von Funktionen über die Grid Management API

Mithilfe der Grid Management API können Sie bestimmte Funktionen im StorageGRID-System komplett deaktivieren. Wenn ein Feature deaktiviert ist, kann niemand Berechtigungen zum Ausführen der Aufgaben zugewiesen werden, die mit diesem Feature verbunden sind.

### Über diese Aufgabe

Mit dem deaktivierten Features-System können Sie den Zugriff auf bestimmte Funktionen im StorageGRID-System verhindern. Die Deaktivierung einer Funktion ist die einzige Möglichkeit, zu verhindern, dass der Root-Benutzer oder Benutzer, die zu Administratorgruppen mit Root Access-Berechtigung gehören, diese Funktion verwenden können.

Um zu verstehen, wie diese Funktionalität nützlich sein kann, gehen Sie folgendermaßen vor:

*Unternehmen A ist ein Service Provider, der durch die Erstellung von Mandantenkonten die Storage-Kapazität ihres StorageGRID Systems leaset. Um die Sicherheit der Objekte ihrer Eigentümer zu schützen, möchte Unternehmen A sicherstellen, dass die eigenen Mitarbeiter nach der Bereitstellung des Kontos niemals auf ein Mandantenkonto zugreifen können.*

*Unternehmen A kann dieses Ziel mithilfe des Systems Funktionen deaktivieren in der Grid Management API erreichen. Durch die vollständige Deaktivierung der Funktion **Ändern des Mandantenstammpassworts** im Grid Manager (sowohl der UI als auch der API) kann Unternehmen A sicherstellen, dass kein Admin-Benutzer - einschließlich des Stammbenutzers und der Benutzer, die zu Gruppen mit Root Access-Berechtigung gehören - das Passwort für den Root-Benutzer eines Mandantenkontos ändern kann.*

### Deaktivieren von Funktionen erneut aktivieren

Standardmäßig können Sie mit der Grid Management API eine deaktivierte Funktion reaktivieren. Wenn Sie jedoch verhindern möchten, dass deaktivierte Funktionen jemals wieder aktiviert werden, können Sie die **activateFeatures**-Funktion selbst deaktivieren.



Die **activateFeatures**-Funktion kann nicht reaktiviert werden. Wenn Sie sich entscheiden, diese Funktion zu deaktivieren, beachten Sie, dass Sie die Möglichkeit verlieren, alle anderen deaktivierten Funktionen dauerhaft zu reaktivieren. Sie müssen sich an den technischen Support wenden, um verlorene Funktionen wiederherzustellen.

Details finden Sie in der Anleitung zur Implementierung von S3- oder Swift-Client-Applikationen.

### Schritte

1. Rufen Sie die Swagger-Dokumentation für die Grid Management API auf.
2. Suchen Sie den Endpunkt zum Deaktivieren von Funktionen.
3. Um eine Funktion, wie z. B. **Ändern des Mandantenwurzelkennworts**, zu deaktivieren, senden Sie einen Text wie folgt an die API:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Wenn die Anforderung abgeschlossen ist, ist die Funktion Mandantenstammpasswort ändern deaktiviert. Die Berechtigung zum Ändern des Stammkennworts für Mandanten erscheint nicht mehr in der Benutzeroberfläche, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu

ändern, schlägt mit „403 Verbotenen“ fehl.

4. Um alle Funktionen erneut zu aktivieren, senden Sie einen Text wie folgt an die API:

```
{ "grid": null }
```

Wenn diese Anforderung abgeschlossen ist, werden alle Funktionen, einschließlich der Funktion „Mandantenstammpasswort ändern“, erneut aktiviert. Die Berechtigung zum Ändern des Root-Kennworts für Mandanten erscheint jetzt in der Benutzeroberfläche. Jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, wird erfolgreich sein, vorausgesetzt, der Benutzer hat die Berechtigung zum Verwalten des Root-Zugriffs oder zum Ändern des Root-Kennworts für Mandanten.



Das vorherige Beispiel führt dazu, dass *all* deaktivierte Funktionen reaktiviert werden. Wenn andere Features deaktiviert wurden, die deaktiviert bleiben sollen, müssen Sie diese explizit in der PUT-Anforderung angeben. Wenn Sie beispielsweise die Funktion „Mandantenstammpasswort ändern“ erneut aktivieren und die Funktion „Alarm Acknowledgement“ deaktivieren möchten, senden Sie diese PUT-Anforderung:

```
{ "grid": { "alarmAcknowledgment": true } }
```

## Verwandte Informationen

["Verwenden der Grid-Management-API"](#)

## Ändern einer Admin-Gruppe

Sie können eine Admin-Gruppe ändern, um die Berechtigungen zu ändern, die der Gruppe zugeordnet sind. Für lokale Admin-Gruppen können Sie auch den Anzeigenamen aktualisieren.

### Was Sie benötigen

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

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Gruppen**.
2. Wählen Sie die Gruppe aus.

Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Bearbeiten**.
4. Optional geben Sie für lokale Gruppen den Gruppennamen ein, der Benutzern angezeigt wird, z. B. „Maintual users“.

Sie können den eindeutigen Namen, d. h. den internen Gruppennamen, nicht ändern.

5. Ändern Sie optional den Zugriffsmodus der Gruppe.



- **Lesen-Schreiben** (Standard): Benutzer können Einstellungen ändern und die Operationen durchführen, die durch ihre Verwaltungsberechtigungen erlaubt sind.
- **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge im Grid Manager oder der Grid Management API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf **schreibgeschützt** gesetzt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Features.

6. Optional können Sie Gruppenberechtigungen hinzufügen oder entfernen.

Weitere Informationen zu Administratorgruppenberechtigungen finden Sie unter.

7. Wählen Sie **Speichern**.

### Verwandte Informationen

[Berechtigungen für Admin-Gruppen](#)

## Löschen einer Admin-Gruppe

Sie können eine Admin-Gruppe löschen, wenn Sie die Gruppe aus dem System entfernen möchten, und alle mit der Gruppe verknüpften Berechtigungen entfernen. Durch das Löschen einer Admin-Gruppe werden alle Admin-Benutzer aus der Gruppe entfernt, die Admin-Benutzer jedoch nicht gelöscht.

### Was Sie benötigen

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

### Über diese Aufgabe

Wenn Sie eine Gruppe löschen, verlieren Benutzer, die dieser Gruppe zugewiesen sind, alle Zugriffsberechtigungen für den Grid Manager, es sei denn, sie werden von einer anderen Gruppe Berechtigungen erteilt.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Gruppen**.
2. Wählen Sie den Namen der Gruppe aus.

Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Wählen Sie **Entfernen**.
4. Wählen Sie **OK**.

## Verwalten von lokalen Benutzern

Sie können lokale Benutzer erstellen und lokalen Admin-Gruppen zuweisen, um zu bestimmen, auf welche Grid Manager-Funktionen diese Benutzer zugreifen können.

Der Grid Manager enthält einen vordefinierten lokalen Benutzer mit dem Namen „root“. Obwohl Sie lokale Benutzer hinzufügen und entfernen können, können Sie den Root-Benutzer nicht entfernen.



Wenn Single Sign-On (SSO) aktiviert ist, können sich lokale Benutzer nicht bei StorageGRID anmelden.

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

## Erstellen eines lokalen Benutzers

Wenn Sie lokale Administratorgruppen erstellt haben, können Sie einen oder mehrere lokale Benutzer erstellen und jeden Benutzer einer oder mehreren Gruppen zuweisen. Die Berechtigungen der Gruppe steuern, auf welche Grid Manager den Benutzer zugreifen kann.

### Über diese Aufgabe

Sie können nur lokale Benutzer erstellen und diese Benutzer nur lokalen Admin-Gruppen zuweisen. Verbundene Benutzer und Gruppen werden über die externe Identitätsquelle verwaltet.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Benutzer**.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie den Anzeigenamen, den eindeutigen Namen und das Kennwort des Benutzers ein.
4. Weisen Sie den Benutzer einer oder mehreren Gruppen zu, die die Zugriffsberechtigungen regeln.

Die Liste der Gruppennamen wird aus der Tabelle Gruppen generiert.

5. Klicken Sie Auf **Speichern**.

### Verwandte Informationen

["Verwalten von Admin-Gruppen"](#)

## Ändern des Kontos eines lokalen Benutzers

Sie können das Konto eines lokalen Administratorbenutzers ändern, um den Anzeigenamen oder die Gruppenmitgliedschaft des Benutzers zu aktualisieren. Sie können auch vorübergehend verhindern, dass ein Benutzer auf das System zugreift.

### Über diese Aufgabe

Sie können nur lokale Benutzer bearbeiten. Verbundene Benutzerdetails werden automatisch mit der externen Identitätsquelle synchronisiert.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Benutzer**.
2. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten.

Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Bearbeiten**.
4. Ändern Sie optional den Namen oder die Gruppenmitgliedschaft.
5. Um den Benutzer vorübergehend nicht auf das System zugreifen zu können, aktivieren Sie **Zugriff verweigern**.
6. Klicken Sie Auf **Speichern**.

Die neuen Einstellungen werden angewendet, wenn sich der Benutzer beim nächsten Mal abmeldet und sich dann wieder beim Grid Manager anmeldet.

## Löschen eines lokalen Benutzerkontos

Sie können Konten für lokale Benutzer löschen, die keinen Zugriff mehr auf den Grid Manager benötigen.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Benutzer**.
2. Wählen Sie den lokalen Benutzer aus, den Sie löschen möchten.



Der vordefinierte lokale Root-Benutzer kann nicht gelöscht werden.

Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Entfernen**.
4. Klicken Sie auf **OK**.

## Ändern des Kennworts eines lokalen Benutzers

Lokale Benutzer können ihre eigenen Passwörter mit der Option **Passwort ändern** im Banner Grid Manager ändern. Darüber hinaus können Benutzer, die Zugriff auf die Seite Admin-Benutzer haben, Passwörter für andere lokale Benutzer ändern.

### Über diese Aufgabe

Sie können Passwörter nur für lokale Benutzer ändern. Verbundene Benutzer müssen ihre eigenen Passwörter in der externen Identitätsquelle ändern.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Benutzer**.
2. Wählen Sie auf der Seite Benutzer den Benutzer aus.

Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Passwort Ändern**.
4. Geben Sie das Passwort ein und bestätigen Sie es, und klicken Sie auf **Speichern**.

# Verwenden von Single Sign On (SSO) für StorageGRID

Das StorageGRID-System unterstützt Single Sign-On (SSO) unter Verwendung des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards. Wenn SSO aktiviert ist, müssen alle Benutzer von einem externen Identitäts-Provider authentifiziert werden, bevor sie auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

- ["Funktionsweise von Single Sign-On"](#)
- ["Anforderungen für die Nutzung von Single Sign On"](#)
- ["Konfigurieren der Single Sign-On-Konfiguration"](#)

## Funktionsweise von Single Sign-On

Prüfen Sie vor der Aktivierung von Single Sign-On (SSO), wie sich die StorageGRID-Anmelde- und -Abmelde-Prozesse bei Aktivierung von SSO auswirken.

### Anmeldung bei aktiviertem SSO

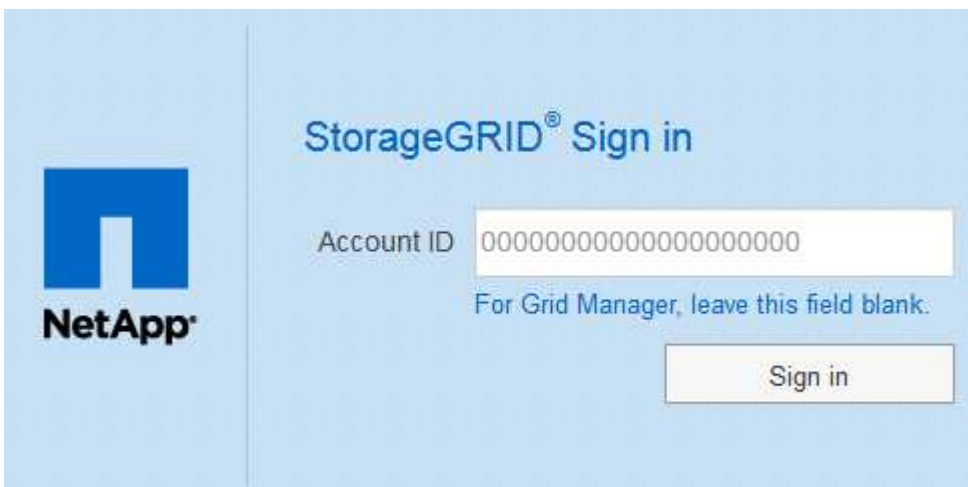
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur SSO-Seite Ihres Unternehmens weitergeleitet, um Ihre Anmeldedaten zu validieren.

#### Schritte

1. Geben Sie in einem Webbrowser den vollständig qualifizierten Domännennamen oder die IP-Adresse eines beliebigen StorageGRID-Admin-Knotens ein.

Die Seite StorageGRID-Anmeldung wird angezeigt.

- Wenn Sie in diesem Browser zum ersten Mal auf die URL zugegriffen haben, werden Sie aufgefordert, eine Konto-ID einzugeben:



StorageGRID® Sign in

Account ID

For Grid Manager, leave this field blank.

Sign in

- Wenn Sie zuvor entweder auf den Grid Manager oder den Tenant Manager zugegriffen haben, werden Sie aufgefordert, ein aktuelles Konto auszuwählen oder eine Konto-ID einzugeben:



Die Seite „StorageGRID-Anmeldung“ wird nicht angezeigt, wenn Sie die vollständige URL für ein Mandantenkonto eingeben (d. h. einen vollständig qualifizierten Domain-Namen oder eine IP-Adresse, gefolgt von `/?accountId=20-digit-account-id`). Stattdessen werden Sie sofort auf die SSO-Anmeldeseite Ihres Unternehmens umgeleitet, auf der Sie sich befinden können [melden Sie sich mit Ihren SSO-Anmeldedaten an](#).

2. Geben Sie an, ob Sie auf den Grid Manager oder den Tenant Manager zugreifen möchten:
  - Um auf den Grid Manager zuzugreifen, lassen Sie das Feld **Konto-ID** leer, geben Sie **0** als Konto-ID ein, oder wählen Sie **Grid-Manager**, wenn es in der Liste der letzten Konten angezeigt wird.
  - Um auf den Mandantenmanager zuzugreifen, geben Sie die 20-stellige Mandantenkonto-ID ein, oder wählen Sie einen Mandanten nach Namen aus, wenn er in der Liste der letzten Konten angezeigt wird.
3. Klicken Sie auf **Anmelden**

StorageGRID leitet Sie zur SSO-Anmeldeseite Ihres Unternehmens weiter. Beispiel:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Melden Sie sich mit Ihren SSO-Anmeldedaten an.

Falls Ihre SSO-Anmeldedaten korrekt sind:

  - a. Der Identitäts-Provider (IdP) stellt eine Authentifizierungsantwort für StorageGRID bereit.
  - b. StorageGRID validiert die Authentifizierungsantwort.
  - c. Wenn die Antwort gültig ist und Sie einer Gruppe angehören, die über ausreichende Zugriffsberechtigungen verfügt, werden Sie je nach ausgewähltem Konto beim Grid Manager oder dem Tenant Manager angemeldet.
5. Wenn Sie über ausreichende Berechtigungen verfügen, können Sie optional auf andere Admin-Nodes zugreifen oder auf den Grid Manager oder den Tenant Manager zugreifen.

Sie müssen Ihre SSO-Anmeldedaten nicht erneut eingeben.

### Abmelden, wenn SSO aktiviert ist

Wenn SSO für StorageGRID aktiviert ist, hängt dies davon ab, ab, bei welchem Anmeldefenster Sie sich angemeldet haben und von wo Sie sich abmelden.

#### Schritte

1. Klicken Sie oben rechts auf der Benutzeroberfläche auf den Link **Abmelden**.

## 2. Klicken Sie Auf **Abmelden**.

Die Seite StorageGRID-Anmeldung wird angezeigt. Das Drop-Down **Recent Accounts** wird aktualisiert und enthält **Grid Manager** oder den Namen des Mandanten, sodass Sie in Zukunft schneller auf diese Benutzeroberflächen zugreifen können.

Wenn Sie bei angemeldet sind...	Und Sie melden sich ab von...	Sie sind abgemeldet von...
Grid Manager auf einem oder mehreren Admin-Nodes	Grid Manager auf jedem Admin-Node	Grid Manager auf allen Admin-Nodes
Mandantenmanager auf einem oder mehreren Admin-Nodes	Mandanten-Manager auf jedem Admin-Node	Mandantenmanager auf allen Admin-Nodes
Sowohl Grid Manager als auch Tenant Manager	Grid Manager	Nur Grid Manager. Sie müssen sich auch vom Tenant Manager abmelden, um SSO abzumelden.



Die Tabelle fasst zusammen, was passiert, wenn Sie sich abmelden, wenn Sie eine einzelne Browser-Sitzung verwenden. Wenn Sie sich bei StorageGRID über mehrere Browser-Sitzungen hinweg angemeldet haben, müssen Sie sich von allen Browser-Sitzungen separat anmelden.

## Anforderungen für die Nutzung von Single Sign On

Bevor Sie Single Sign On (SSO) für ein StorageGRID-System aktivieren, überprüfen Sie die Anforderungen in diesem Abschnitt.



Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

## Anforderungen an Identitätsanbieter

Der Identitäts-Provider (IdP) für SSO muss die folgenden Anforderungen erfüllen:

- Eine der folgenden Versionen des Active Directory Federation Service (AD FS):
  - AD FS 4.0, im Lieferumfang von Windows Server 2016 enthalten



Windows Server 2016 sollte den verwenden "[KB3201845-Update](#)", Oder höher.

- AD FS 3.0, im Lieferumfang von Windows Server 2012 R2 Update oder höher enthalten.
- Transport Layer Security (TLS) 1.2 oder 1.3
- Microsoft .NET Framework, Version 3.5.1 oder höher

## Serverzertifikate-Anforderungen

StorageGRID verwendet auf jedem Admin-Node ein Zertifikat für die Managementschnittstelle, um den Zugriff auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandantenmanagement-

API zu sichern. Wenn Sie SSO-Vertrauensstellen für StorageGRID in AD FS konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID-Anforderungen an AD FS.

Falls Sie noch kein benutzerdefiniertes Serverzertifikat für die Managementoberfläche installiert haben, sollten Sie dies jetzt tun. Wenn Sie ein benutzerdefiniertes Serverzertifikat installieren, wird es für alle Administratorknoten verwendet, und Sie können es in allen StorageGRID-Vertrauensstellungen verwenden.



Es wird nicht empfohlen, das Standardserverzertifikat eines Admin-Knotens im AD FS-Vertrauensverhältnis zu verwenden. Wenn der Knoten ausfällt und Sie ihn wiederherstellen, wird ein neues Standard-Serverzertifikat generiert. Bevor Sie sich beim wiederhergestellten Knoten anmelden können, müssen Sie das Vertrauensverhältnis der betreffenden Partei in AD FS mit dem neuen Zertifikat aktualisieren.

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich bei der Befehlshülle des Knotens anmelden und auf die zugreifen `/var/local/mgmt-api` Verzeichnis. Ein benutzerdefiniertes Serverzertifikat ist benannt `custom-server.crt`. Das Standardserverzertifikat des Node wird mit benannt `server.crt`.

### Verwandte Informationen

["Zugriffskontrolle durch Firewalls"](#)

["Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"](#)

## Konfigurieren der Single Sign-On-Konfiguration

Wenn Single Sign-On (SSO) aktiviert ist, können Benutzer nur auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen, wenn ihre Anmeldedaten über den von Ihrem Unternehmen implementierten SSO-Anmeldeprozess autorisiert sind.

- ["Bestätigung der föderierten Benutzer kann sich anmelden"](#)
- ["Sandbox-Modus verwenden"](#)
- ["Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS"](#)
- ["Testen von Vertrauen von Vertrauensstellen"](#)
- ["Aktivieren von Single Sign On"](#)
- ["Deaktivieren der Einzelanmeldung"](#)
- ["Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten"](#)

### Bestätigung der föderierten Benutzer kann sich anmelden

Bevor Sie Single Sign-On (SSO) aktivieren, müssen Sie bestätigen, dass sich mindestens ein verbundener Benutzer beim Grid Manager und beim Tenant Manager für alle bestehenden Mandantenkonten anmelden kann.

### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie verwenden Active Directory als föderierte Identitätsquelle und AD FS als Identitätsanbieter.

## "Anforderungen für die Nutzung von Single Sign On"

### Schritte

1. Falls bereits vorhandene Mandantenkonten vorhanden sind, bestätigen Sie, dass kein Mandant seine eigene Identitätsquelle verwendet.



Wenn Sie SSO aktivieren, wird eine im Mandantenmanager konfigurierte Identitätsquelle von der im Grid Manager konfigurierten Identitätsquelle außer Kraft gesetzt. Benutzer, die zur Identitätsquelle des Mandanten gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Identitätsquelle des Grid Manager.

- a. Melden Sie sich für jedes Mandantenkonto bei Tenant Manager an.
  - b. Wählen Sie **Zugriffskontrolle > Identitätsföderation**.
  - c. Bestätigen Sie, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht aktiviert ist.
  - d. Wenn dies der Fall ist, bestätigen Sie, dass alle föderierten Gruppen, die für dieses Mandantenkonto verwendet werden, nicht mehr erforderlich sind. Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Speichern**.
2. Bestätigen Sie, dass ein verbundener Benutzer auf den Grid Manager zugreifen kann:
    - a. Wählen Sie im Grid Manager die Option **Konfiguration > Zugriffskontrolle > Admin-Gruppen** aus.
    - b. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
    - c. Abmelden.
    - d. Bestätigen Sie, dass Sie sich wieder bei Grid Manager als Benutzer in der föderierten Gruppe anmelden können.
  3. Wenn es bereits vorhandene Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root Access-Berechtigung anmelden kann:
    - a. Wählen Sie im Grid Manager die Option **Miters** aus.
    - b. Wählen Sie das Mandantenkonto aus und klicken Sie auf **Konto bearbeiten**.
    - c. Wenn das Kontrollkästchen \* verwendet eigene Identitätsquelle\* aktiviert ist, deaktivieren Sie das Kontrollkästchen und klicken Sie auf **Speichern**.

### Edit Tenant Account

#### Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional)

Cancel

Save



Die Seite Mandantenkonten wird angezeigt.

- a. Wählen Sie das Mandantenkonto aus, klicken Sie auf **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
- b. Klicken Sie im Mandantenmanager auf **Zugriffskontrolle > Gruppen**.
- c. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus dem Grid Manager der Root Access-Berechtigung für diesen Mandanten zugewiesen wurde.
- d. Abmelden.
- e. Bestätigen Sie, dass Sie sich wieder bei dem Mandanten als Benutzer in der föderierten Gruppe anmelden können.

### **Verwandte Informationen**

["Anforderungen für die Nutzung von Single Sign On"](#)

["Verwalten von Admin-Gruppen"](#)

["Verwenden Sie ein Mandantenkonto"](#)

### **Sandbox-Modus verwenden**

Sie können den Sandbox-Modus verwenden, um Active Directory Federation Services (AD FS) zu konfigurieren und zu testen, die auf Vertrauen von Parteien basieren, bevor Sie SSO für StorageGRID-Benutzer durchsetzen. Nachdem SSO aktiviert ist, können Sie den Sandbox-Modus erneut aktivieren, um neue und vorhandene Vertrauensstellen zu konfigurieren oder zu testen. Im Sandbox-Modus wird SSO für StorageGRID-Benutzer vorübergehend deaktiviert.

### **Was Sie benötigen**

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

### **Über diese Aufgabe**

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an AD FS. Wiederum sendet AD FS eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Autorisierungsanforderung erfolgreich war. Für erfolgreiche Anforderungen enthält die Antwort eine universell eindeutige Kennung (UUID) für den Benutzer.

Damit StorageGRID (der Service Provider) und AD FS (der Identitäts-Provider) sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, müssen Sie bestimmte Einstellungen in StorageGRID konfigurieren. Als Nächstes müssen Sie AD FS verwenden, um für jeden Admin-Knoten ein Vertrauensverhältnis zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, um SSO zu aktivieren.

Im Sandbox-Modus ist es einfach, diese Rückkehrkonfiguration durchzuführen und alle Einstellungen zu testen, bevor Sie SSO aktivieren.



Die Verwendung des Sandbox-Modus ist sehr empfehlenswert, aber nicht unbedingt erforderlich. Wenn Sie bereit sind, AD FS zu erstellen, auf denen die Teilnehmer vertrauen, unmittelbar nach der Konfiguration von SSO in StorageGRID, Und Sie müssen die SSO- und SLO-Prozesse (Single Logout) für jeden Admin-Knoten nicht testen, klicken Sie auf **aktiviert**, geben Sie die StorageGRID-Einstellungen ein, erstellen Sie für jeden Admin-Knoten in AD FS ein Vertrauensverhältnis, und klicken Sie dann auf **Speichern**, um SSO zu aktivieren.

## Schritte

### 1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt, wobei die Option **deaktiviertes** ausgewählt ist.

#### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status  Disabled  Sandbox Mode  Enabled

Save



Wenn die Optionen für den SSO-Status nicht angezeigt werden, bestätigen Sie, dass Sie Active Directory als föderierte Identitätsquelle konfiguriert haben. Siehe „Anforderungen für die Verwendung von Single Sign-On.“

### 2. Wählen Sie die Option **Sandbox Mode**.

Die Einstellungen für Identitäts-Provider und vertrauende Partei werden angezeigt. Im Abschnitt „Identitätsanbieter“ wird das Feld **Diensttyp** schreibgeschützt angezeigt. Es zeigt den Typ des Services zur Identitätsföderation an, den Sie verwenden (z. B. Active Directory).

### 3. Im Abschnitt „Identitätsanbieter“:

- Geben Sie den Namen des Föderationsdienstes ein, genau wie er in AD FS angezeigt wird.



Um den Federationsdienstnamen zu finden, gehen Sie zu Windows Server Manager. Wählen Sie **Tools > AD FS Management**. Wählen Sie im Menü Aktion die Option **Eigenschaften des Föderationsdienstes bearbeiten** aus. Der Name des Föderationsdienstes wird im zweiten Feld angezeigt.

- Geben Sie an, ob Sie die Verbindung mit Transport Layer Security (TLS) sichern möchten, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.

- **Verwenden Sie das Betriebssystem CA-Zertifikat:** Verwenden Sie das auf dem Betriebssystem installierte Standard-CA-Zertifikat, um die Verbindung zu sichern.
- **Benutzerdefiniertes CA-Zertifikat verwenden:** Verwenden Sie ein benutzerdefiniertes CA-Zertifikat, um die Verbindung zu sichern.

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

- **Verwenden Sie keine TLS:** Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.
4. Geben Sie im Abschnitt „Vertrauenspartei“ die ID der betreffenden Partei an, die Sie für StorageGRID-Admin-Knoten verwenden, wenn Sie Vertrauensstellungen der betreffenden Partei konfigurieren.
- Wenn Ihr Grid beispielsweise nur einen Admin-Node hat und Sie nicht erwarten, dass künftig weitere Admin-Nodes hinzugefügt werden, geben Sie ein `SG Oder StorageGRID`.
  - Wenn Ihr Grid mehr als einen Admin-Node enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` In der Kennung. Beispiel: `SG-[HOSTNAME]`. Dadurch wird eine Tabelle mit einer auf den Hostnamen des Knotens beruhenden Partei-ID für jeden Admin-Node generiert. + HINWEIS: Sie müssen eine Vertrauensbasis für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

5. Klicken Sie Auf **Speichern**.

- Ein grünes Häkchen wird für einige Sekunden auf der Schaltfläche **Speichern** angezeigt.



- Der Bestätigungshinweis zum Sandbox-Modus wird angezeigt und bestätigt, dass der Sandbox-Modus nun aktiviert ist. Sie können diesen Modus verwenden, während Sie AD FS verwenden, um ein Vertrauensverhältnis von Vertrauensstellen für jeden Admin-Node zu konfigurieren und die Single Sign-in (SSO)- und SLO-Prozesse (Single Logout) zu testen.

### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

### Verwandte Informationen

["Anforderungen für die Nutzung von Single Sign On"](#)

## Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS

Sie müssen Active Directory Federation Services (AD FS) verwenden, um ein Vertrauensverhältnis für jeden Admin-Knoten in Ihrem System zu erstellen. Sie können vertraut mit PowerShell-Befehlen erstellen, SAML-Metadaten von StorageGRID importieren oder die Daten manuell eingeben.

### Erstellen eines Vertrauensverhältnisses mit Windows PowerShell

Mit Windows PowerShell können Sie schnell ein oder mehrere Vertrauensstellen von vertrauenswürdigen Parteien erstellen.

#### Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domänennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.

#### Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

#### Schritte

1. Klicken Sie im Windows-Startmenü mit der rechten Maustaste auf das PowerShell-Symbol und wählen Sie **als Administrator ausführen** aus.
2. Geben Sie an der PowerShell-Eingabeaufforderung den folgenden Befehl ein:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Für *Admin\_Node\_Identifer*, Geben Sie die ID für den Admin-Knoten auf, die sich auf der Seite Single Sign-On befindet, genau so ein, wie sie auf der Seite „Single Sign-On“ angezeigt wird. Beispiel: SG-DC1-ADM1.
- Für *Admin\_Node\_FQDN*, Geben Sie den vollständig qualifizierten Domänennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

3. Wählen Sie im Windows Server Manager **Tools > AD FS Management** aus.

Das AD FS Management Tool wird angezeigt.

4. Wählen Sie **AD FS > vertraut auf Partei**.

Die Liste der Vertrauensstellen wird angezeigt.

5. Fügen Sie eine Zugriffskontrollrichtlinie zum neu erstellten Vertrauen der Vertrauensstellenden Partei hinzu:
  - a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
  - b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
  - c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
  - d. Klicken Sie auf **Anwenden** und klicken Sie auf **OK**
  
6. Fügen Sie dem neu erstellten Treuhandgesellschaft eine Richtlinie zur Ausstellung von Forderungen hinzu:
  - a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
  - b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
  - c. Klicken Sie auf **Regel hinzufügen**.
  - d. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
  - e. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.  
  
 Beispiel: **ObjectGUID an Name ID**.
  - f. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
  - g. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
  - h. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
  - i. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.
  
7. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.
  - a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
  - b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifizier** und **Signatur** ausgefüllt sind.  
  
 Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach die Werte manuell ein.
  
8. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
9. Wenn Sie fertig sind, kehren Sie zu StorageGRID und zurück ["Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen"](#) Um sicherzustellen, dass sie richtig konfiguriert sind.

#### **Schaffung eines Vertrauensverhältnisses durch den Import von Federationmetadaten**

Sie können die Werte für jedes Vertrauen der betreffenden Anbieter importieren, indem Sie für jeden Admin-Node auf die SAML-Metadaten zugreifen.

#### **Was Sie benötigen**

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domännennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.

### Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

### Schritte

1. Klicken Sie im Windows Server Manager auf **Tools** und wählen Sie dann **AD FS Management** aus.
2. Klicken Sie unter Aktionen auf **Vertrauensstellung hinzufügen**.
3. Wählen Sie auf der Begrüßungsseite \* Claims Aware\* aus und klicken Sie auf **Start**.
4. Wählen Sie **Daten über die online veröffentlichte oder auf einem lokalen Netzwerk** importieren.
5. Geben Sie unter **Federation Metadatenadresse (Hostname oder URL)** den Speicherort der SAML-Metadaten für diesen Admin-Node ein:

```
https://Admin_Node_FQDN/api/saml-metadata
```

Für *Admin\_Node\_FQDN*, Geben Sie den vollständig qualifizierten Domänennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

6. Schließen Sie den Assistenten „Vertrauen in die Vertrauensstellung“, speichern Sie das Vertrauen der vertrauenden Partei und schließen Sie den Assistenten.



Verwenden Sie bei der Eingabe des Anzeigenamens die vertrauende Partei-ID für den Admin-Node genau so, wie sie auf der Seite Single Sign-On im Grid Manager angezeigt wird. Beispiel: SG-DC1-ADM1.

7. Fügen Sie eine Antragsregel hinzu:
  - a. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
  - b. Klicken Sie auf **Regel hinzufügen**:
  - c. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
  - d. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.  
  
Beispiel: **ObjectGUID an Name ID**.
  - e. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
  - f. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
  - g. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name**

ID aus.

h. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.

8. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.

- a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
- b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifizier** und **Signatur** ausgefüllt sind.

Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach die Werte manuell ein.

9. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.

10. Wenn Sie fertig sind, kehren Sie zu StorageGRID und zurück "[Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen](#)" Um sicherzustellen, dass sie richtig konfiguriert sind.

### Manuelles Erstellen eines Vertrauensverhältnisses mit einer Vertrauensbasis

Wenn Sie sich entscheiden, die Daten für die Treuhanddienste des Treuhandteils nicht zu importieren, können Sie die Werte manuell eingeben.

### Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domännennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben das benutzerdefinierte Zertifikat, das für die StorageGRID Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich von der Command Shell bei einem Admin-Node einloggen.
- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.

### Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

### Schritte

1. Klicken Sie im Windows Server Manager auf **Tools** und wählen Sie dann **AD FS Management** aus.
2. Klicken Sie unter Aktionen auf **Vertrauensstellung hinzufügen**.
3. Wählen Sie auf der Begrüßungsseite \* Claims Aware\* aus und klicken Sie auf **Start**.
4. Wählen Sie **Geben Sie Daten über den Kunden manuell** ein, und klicken Sie auf **Weiter**.
5. Schließen Sie den Assistenten für Vertrauen in die vertrauende Partei ab:
  - a. Geben Sie einen Anzeigenamen für diesen Admin-Node ein.



Verwenden Sie für Konsistenz den Admin-Node mit der bewirtenden Partei-Kennung, genau wie er auf der Seite Single Sign-On im Grid Manager angezeigt wird. Beispiel: SG-DC1-ADM1.

- b. Überspringen Sie den Schritt, um ein optionales Token-Verschlüsselungszertifikat zu konfigurieren.
- c. Aktivieren Sie auf der Seite „URL konfigurieren“ das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll** aktivieren.
- d. Geben Sie die Endpunkt-URL des SAML-Service für den Admin-Node ein:

`https://Admin_Node_FQDN/api/saml-response`

Für `Admin_Node_FQDN` Geben Sie den vollständig qualifizierten Domänennamen für den Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

- e. Geben Sie auf der Seite Configure Identifiers die befolgende Partei-ID für denselben Admin-Node an:

`Admin_Node_Identifier`

Für `Admin_Node_Identifier`, Geben Sie die ID für den Admin-Knoten auf, die sich auf der Seite Single Sign-On befindet, genau so ein, wie sie auf der Seite „Single Sign-On“ angezeigt wird. Beispiel: SG-DC1-ADM1.

- f. Überprüfen Sie die Einstellungen, speichern Sie das Vertrauen der Vertrauensstellungsgesellschaft, und schließen Sie den Assistenten.

Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.



Wenn das Dialogfeld nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.

6. Um den Assistenten für die Antragsregel zu starten, klicken Sie auf **Regel hinzufügen**:
  - a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
  - b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.  
  
Beispiel: **ObjectGUID an Name ID**.
  - c. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
  - d. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
  - e. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
  - f. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.
7. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
8. Konfigurieren Sie auf der Registerkarte **Endpunkte** den Endpunkt für einzelne Abmeldung (SLO):
  - a. Klicken Sie auf **SAML hinzufügen**.
  - b. Wählen Sie **Endpunkttyp > SAML Logout**.



c. Wählen Sie **Bindung > Umleiten**.

d. Geben Sie im Feld **Trusted URL** die URL ein, die für Single Logout (SLO) von diesem Admin-Node verwendet wird:

```
https://Admin_Node_FQDN/api/saml-logout
```

Für *Admin\_Node\_FQDN*, Geben Sie den vollständig qualifizierten Domännennamen des Admin-Knotens ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

a. Klicken Sie auf **OK**.

9. Geben Sie auf der Registerkarte **Signatur** das Signaturzertifikat für dieses Vertrauen der bevertrauenden Partei an:

a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:

- Wenn Sie über das benutzerdefinierte Managementzertifikat verfügen, das Sie in StorageGRID hochgeladen haben, wählen Sie dieses Zertifikat aus.
- Wenn Sie nicht über das benutzerdefinierte Zertifikat verfügen, melden Sie sich beim Admin-Knoten an, gehen Sie zu `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie das hinzu `custom-server.crt` Zertifikatdatei.

**Hinweis:** das Standardzertifikat des Admin-Knotens verwenden (`server.crt`) Wird nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat neu generiert, wenn Sie den Knoten wiederherstellen, und Sie müssen das Vertrauen der Vertrauensstelle aktualisieren.

b. Klicken Sie auf **Anwenden** und klicken Sie auf **OK**.

Die Eigenschaften der zu vertrauenden Partei werden gespeichert und geschlossen.

10. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.

11. Wenn Sie fertig sind, kehren Sie zu StorageGRID und zurück "[Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen](#)" Um sicherzustellen, dass sie richtig konfiguriert sind.

## Testen von Vertrauen von Vertrauensstellen

Bevor Sie die Verwendung von Single Sign On (SSO) für StorageGRID durchsetzen, müssen Sie sicherstellen, dass Single Sign On und Single Logout (SLO) korrekt konfiguriert sind. Wenn Sie für jeden Admin-Node eine Vertrauensbasis erstellt haben, bestätigen Sie, dass Sie SSO und SLO für jeden Admin-Node verwenden können.

### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie haben eine oder mehrere Vertrauensstellen in AD FS konfiguriert.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt, wobei die Option **Sandbox Mode** ausgewählt ist.

- Suchen Sie in den Anweisungen für den Sandbox-Modus den Link zur Anmeldeseite Ihres Identitätsanbieters.

Die URL wird aus dem Wert abgeleitet, den Sie im Feld **Federated Service Name** eingegeben haben.

**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

- Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
- Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
- From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

- Klicken Sie auf den Link oder kopieren Sie die URL in einen Browser, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
- Um zu bestätigen, dass Sie SSO zur Anmeldung bei StorageGRID verwenden können, wählen Sie **Anmelden bei einer der folgenden Sites**, wählen Sie die vertrauenswürdige Partei-ID für Ihren primären Admin-Knoten und klicken Sie auf **Anmelden**.

You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben.

- Geben Sie Ihren föderierten Benutzernamen und Ihr Kennwort ein.
  - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

✓ Single sign-on authentication and logout test completed successfully.

- Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.

- Wiederholen Sie die vorherigen Schritte, um zu bestätigen, dass Sie sich bei anderen Admin-Nodes

anmelden können.

Wenn alle SSO-Anmelde- und Abmeldevorgänge erfolgreich sind, können Sie SSO aktivieren.

## Aktivieren von Single Sign On

Nachdem Sie den Sandbox-Modus verwendet haben, um alle Trusts von StorageGRID-Kunden zu testen, sind Sie bereit, Single Sign-On (SSO) zu aktivieren.

### Was Sie benötigen

- Sie müssen mindestens eine föderierte Gruppe aus der Identitätsquelle importiert und der Gruppe Root Access Management-Berechtigungen zugewiesen haben. Sie müssen bestätigen, dass mindestens ein verbundener Benutzer Root Access-Berechtigung für den Grid Manager und den Tenant Manager für alle bestehenden Mandantenkonten hat.
- Sie müssen alle Vertrauensstellen der Vertrauensbesteller mit Sandbox-Modus getestet haben.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt, wobei **Sandbox-Modus** ausgewählt ist.

2. Ändern Sie den SSO-Status in **aktiviert**.
3. Klicken Sie Auf **Speichern**.

Es wird eine Warnmeldung angezeigt.

### Warning

#### Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Überprüfen Sie die Warnung und klicken Sie auf **OK**.

Single Sign-On ist jetzt aktiviert.



Alle Benutzer müssen SSO verwenden, um auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandanten-Management-API zuzugreifen. Lokale Benutzer können nicht mehr auf StorageGRID zugreifen.

## Deaktivieren der Einzelanmeldung

Sie können Single Sign-On (SSO) deaktivieren, wenn Sie diese Funktion nicht mehr verwenden möchten. Sie müssen Single Sign-On deaktivieren, bevor Sie die Identitätsföderation deaktivieren können.

### Was Sie benötigen

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

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt.

2. Wählen Sie die Option **deaktiviert** aus.
3. Klicken Sie Auf **Speichern**.

Es wird eine Warnmeldung angezeigt, die darauf hinweist, dass lokale Benutzer sich jetzt anmelden können.

### Warning

Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel

OK

4. Klicken Sie auf **OK**.

Wenn Sie sich das nächste Mal bei StorageGRID anmelden, wird die Seite StorageGRID-Anmeldung angezeigt. Sie müssen den Benutzernamen und das Kennwort für einen lokalen oder föderierten StorageGRID-Benutzer eingeben.

## Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten

Sie können sich möglicherweise nicht beim Grid-Manager anmelden, wenn das SSO-System (Single Sign-On) ausfällt. In diesem Fall können Sie SSO für einen Admin-Node vorübergehend deaktivieren und erneut aktivieren. Um SSO zu deaktivieren und dann erneut zu aktivieren, müssen Sie auf die Befehlshaber des Node zugreifen.

## Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen das Passwort für den lokalen Root-Benutzer kennen.

## Über diese Aufgabe

Nachdem Sie SSO für einen Admin-Node deaktiviert haben, können Sie sich beim Grid-Manager als lokaler Root-Benutzer anmelden. Zum Sichern Ihres StorageGRID-Systems müssen Sie die Befehlshaber des Node verwenden, um SSO auf dem Admin-Node erneut zu aktivieren, sobald Sie sich abmelden.



Das Deaktivieren von SSO für einen Admin-Node wirkt sich nicht auf die SSO-Einstellungen für andere Admin-Nodes im Raster aus. Das Kontrollkästchen **SSO aktivieren** auf der Seite Single Sign-On im Grid Manager bleibt aktiviert, und alle vorhandenen SSO-Einstellungen bleiben erhalten, wenn Sie sie nicht aktualisieren.

## Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
  - a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
  - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
  - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
  - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie den folgenden Befehl aus:`disable-saml`

Eine Meldung gibt an, dass der Befehl nur für diesen Admin-Knoten gilt.

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

Eine Meldung gibt an, dass Single Sign-On auf dem Knoten deaktiviert ist.

4. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.

Die Anmeldeseite für den Grid Manager wird jetzt angezeigt, weil SSO deaktiviert wurde.

5. Melden Sie sich mit dem Benutzernamen root und dem Passwort des lokalen Root-Benutzers an.
6. Wenn Sie SSO vorübergehend deaktiviert haben, da Sie die SSO-Konfiguration korrigieren mussten:
  - a. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.
  - b. Ändern Sie die falschen oder veralteten SSO-Einstellungen.
  - c. Klicken Sie Auf **Speichern**.

Wenn Sie auf der Seite Single Sign-On auf **Save** klicken, wird SSO für das gesamte Raster automatisch wieder aktiviert.

7. Wenn Sie SSO vorübergehend deaktiviert haben, weil Sie aus einem anderen Grund auf den Grid Manager zugreifen mussten:

- a. Führen Sie alle Aufgaben oder Aufgaben aus, die Sie ausführen müssen.
- b. Klicken Sie auf **Abmelden** und schließen Sie den Grid Manager.
- c. SSO auf dem Admin-Node erneut aktivieren. Sie können einen der folgenden Schritte ausführen:
  - Führen Sie den folgenden Befehl aus: `enable-saml`

Eine Meldung gibt an, dass der Befehl nur für diesen Admin-Knoten gilt.

Bestätigen Sie, dass Sie SSO aktivieren möchten.

Eine Meldung gibt an, dass Single Sign-On auf dem Knoten aktiviert ist.

- Booten Sie den Grid-Node neu: `reboot`

8. Greifen Sie über einen Webbrowser über denselben Admin-Node auf den Grid-Manager zu.
9. Vergewissern Sie sich, dass die Seite StorageGRID-Anmeldung angezeigt wird und Sie Ihre SSO-Anmeldedaten für den Zugriff auf den Grid-Manager eingeben müssen.

### Verwandte Informationen

["Konfigurieren der Single Sign-On-Konfiguration"](#)

## Administrator-Client-Zertifikate werden konfiguriert

Sie können Clientzertifikate verwenden, um autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank zu ermöglichen. Clientzertifikate bieten eine sichere Möglichkeit zur Verwendung externer Tools zur Überwachung von StorageGRID.

Wenn Sie mit einem externen Monitoring-Tool auf StorageGRID zugreifen müssen, müssen Sie mithilfe des Grid Managers ein Clientzertifikat hochladen oder generieren und die Zertifikatsinformationen in das externe Tool kopieren.

### Hinzufügen von Administrator-Client-Zertifikaten

Zum Hinzufügen eines Clientzertifikats können Sie Ihr eigenes Zertifikat bereitstellen oder mit dem Grid Manager ein Zertifikat erstellen.

#### Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen die IP-Adresse oder den Domännennamen des Admin-Knotens kennen.
- Sie müssen das Zertifikat für den StorageGRID-Verwaltungsserver konfiguriert haben und über das entsprechende CA-Paket verfügen
- Wenn Sie Ihr eigenes Zertifikat hochladen möchten, müssen der öffentliche Schlüssel und der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer verfügbar sein.

#### Schritte

1. Wählen Sie im Grid Manager die Option **Konfiguration > Zugriffskontrolle > Clientzertifikate** aus.

Die Seite Clientzertifikate wird angezeigt.

## Client Certificates

You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.

Name	Allow Prometheus	Expiration Date
No client certificates configured.		

### 2. Wählen Sie **Hinzufügen**.

Die Seite Zertifikat hochladen wird angezeigt.

### Upload Certificate

Name

Allow Prometheus

---

#### Certificate Details


Upload the public key for the client certificate.

- Geben Sie einen Namen zwischen 1 und 32 Zeichen für das Zertifikat ein.
- Um über Ihr externes Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, aktivieren Sie das Kontrollkästchen **Prometheus erlauben**.
- Hochladen oder Generieren eines Zertifikats:
  - Um ein Zertifikat hochzuladen, gehen Sie [Hier](#).
  - Gehen Sie zum Generieren eines Zertifikats [Hier](#).
- ] zum Hochladen eines Zertifikats:
  - Wählen Sie **Client-Zertifikat Hochladen**.
  - Suchen Sie nach dem öffentlichen Schlüssel für das Zertifikat.

Nachdem Sie den öffentlichen Schlüssel für das Zertifikat hochgeladen haben, werden die Felder **Certificate Metadaten** und **Certificate PEM** ausgefüllt.

## Upload Certificate

Name  test-certificate-upload

Allow Prometheus 


### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwDELMAkGA1UEBhMCVVMxZzARBgNVBAgMCkNhbg1mb3JuaWEuXzAQBgNVBAcM
CVN1bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDby4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1LmV4MDYx
OTIyMTE1LmV4DELMAkGA1UEBhMCVVMxZzARBgNVBAgMCkNhbg1mb3JuaWEuXzAQBg
NVBAcMNVN1bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDby4xCzAJBgNVBAsM
Ak1UMRkwFwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAzVqq2MnjvVotLeStq1Co4coJmsQ2ygrhuwSza0bgMnjf
cwUgHNVFXGuGlzY/Tl37r3Dk5bu2fyGYAeJ6mqbQA6cE3yp0p5Hx7Cm/AWJknFw6
```

Copy certificate to clipboard

Cancel


Save


- a. Wählen Sie **Zertifikat in Zwischenablage kopieren** und fügen Sie das Zertifikat in Ihr externes Überwachungstool ein.
  - b. Verwenden Sie ein Bearbeitungswerkzeug, um den privaten Schlüssel in Ihr externes Überwachungstool zu kopieren und einzufügen.
  - c. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.
7. ] zum Generieren eines Zertifikats:
- a. Wählen Sie **Client-Zertifikat Erstellen**.
  - b. Geben Sie den Domännennamen oder die IP-Adresse des Admin-Knotens ein.
  - c. Geben Sie optional einen X.509-Studienteilnehmer ein, der auch als Distinguished Name (DN) bezeichnet wird, um den Administrator zu identifizieren, der das Zertifikat besitzt.
  - d. Wählen Sie optional die Anzahl der Tage aus, an denen das Zertifikat gültig ist. Der Standardwert ist 730 Tage.
  - e. Wählen Sie **Erzeugen**.

Die Felder **Certificate Metadaten**, **Certificate PEM** und **Certificate Private Key** sind ausgefüllt.



## Upload Certificate

Name  test-certificate-generate

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

[Upload Client Certificate](#)

[Generate Client Certificate](#)

Certificate metadata 

```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:0F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:68:E4:C6:42:52:5F:32:7E:E7:93:66:89:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

Certificate PEM 


```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUUCFj7dxITSN9Ugs01Vm8qA1Ow4gowDQYJKoZIhvcNAQEL
BQAwEwERMA8GA1UEAwIzIGVudC5jb20wHhcNMjIwMjE1MDQyMjI0NDQ2WWhcMjIw
MjIwMjE1MDQyMjI0NDQ2WjATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAR02dS9mx2jFrGuBb22Mjcidf/tCkKtL8Gm+4vI
wt1glvrXgHZ31B9YIQn/Vo729R2mNKKyBwkyQTkGCO2Ixvv0STBLEIWFb3eTgcIcMyt1V1F
OseBWFYs402xxjnR3/X+AX+6s2WZIsVe+3CDjGu4ie0V/uVQxx4yA1T9SoKnjBmOa
LCVjL6iVnkUGB8GbkYUPeOaoMjsL6TN1QsoFv9VEB0xBKCP4D7FDbaIy2f9Ng8rS
FEOQoLN=N=XCasLO4D7j2qFqOVUpFJ3M0oh1x0n5pQ78Z5KEYwV=DKg6v52P8UBM
1o6GeuoFaW+dbpLZKp09N1V=FlghXe9AxxN8s+kCAwEAAaMXMBUwEwYDVR0RBBAww
-----
```

[Copy certificate to clipboard](#)

Certificate private key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArT20H2bHaM+sa4Fv2kyNyJ1/+1NwzEu0Eab7i8jC2KNC/BFe
AdneUH1ghCf9Wjvb1HaY0oxIHCTUBOQYI5kjG+/RJMEb4h29eKxOBwiczK2VWUU7
OwF2jPg7bPGoOrf9f4Bf7xN1ZkixV751IOMa7iJaRX+5VDPHjIDVP1KggelMGY5oe
JWmVqJWeRQYFI2uTJQ946qgyOwvpm2VDOgW/1UQHTZEoKngFeUNtojL2/02DmtJ8
QSCge202x0JrMe7gFuNmoWo5hS8kUncw6iHXHSfm1Dvxnkp9jBWMqDm/nY/xQEzW
jw266h9pbS1ukt2k703VW0WGCfD7GDPE2yyQIDAQABoIBAQCfEUfY4pE0Hqtv
2uEL6De4yXMTwg/3Gn+W3mvtcdgQB4xWEGQrk1kEUG+HTYrFJen6XX0vACDYAC/
Hh1Q67xDVpwrjdpuK0ctr1W3ervzEmpBx99MqH9Y2UGx6Yub3UBJaqfDvja4Nvaon
MxaYJRFBLvAR7f2z2xXVY3b0zRPA+rnoYCrslLct5Y0K73e0G8naTmwIdm2YM6EE
-----
```

[Copy private key to clipboard](#)

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

[Cancel](#)

[Save](#)

- Wählen Sie **Zertifikat in Zwischenablage kopieren** und fügen Sie das Zertifikat in Ihr externes Überwachungstool ein.
- Wählen Sie **Privatschlüssel in Zwischenablage kopieren** und fügen Sie den Schlüssel in Ihr externes Überwachungstool ein.

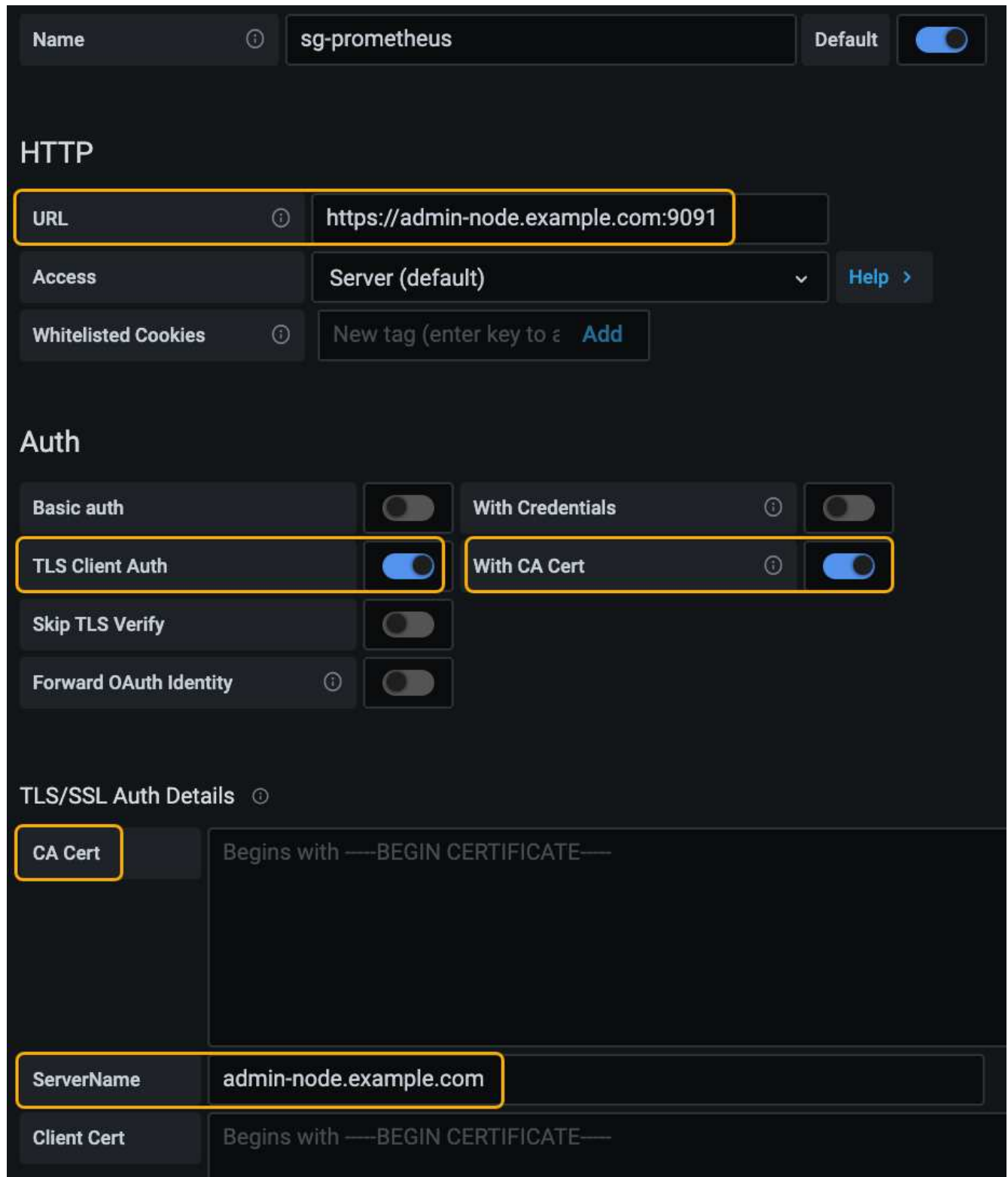


Nach dem Schließen des Dialogfelds können Sie den privaten Schlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einen sicheren Ort.

- Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.

8. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.

Ein Grafana-Beispiel ist im folgenden Screenshot dargestellt:



a. **Name:** Geben Sie einen Namen für die Verbindung ein.

StorageGRID benötigt diese Informationen nicht, Sie müssen jedoch einen Namen angeben, um die Verbindung zu testen.

- b. **URL:** Geben Sie den Domain-Namen oder die IP-Adresse für den Admin-Node ein. Geben Sie HTTPS und Port 9091 an.

Beispiel: `https://admin-node.example.com:9091`

- c. Aktivieren Sie **TLS Client Authorization** und **mit CA Cert**.
- d. Kopieren Sie das Zertifikat des Management Interface Server oder CA-Pakets unter TLS/SSL-Auth-Details auf das **CA-Zertifikat**.
- e. **ServerName:** Geben Sie den Domainnamen des Admin-Knotens ein.

Servername muss mit dem Domännennamen übereinstimmen, wie er im Management Interface Server Certificate angezeigt wird.

- f. Speichern und testen Sie das Zertifikat und den privaten Schlüssel, das Sie aus StorageGRID oder einer lokalen Datei kopiert haben.

Sie können jetzt mit Ihrem externen Monitoring Tool auf die Prometheus Kennzahlen von StorageGRID zugreifen.

Weitere Informationen zu den Metriken finden Sie in den Anweisungen für das Monitoring und die Fehlerbehebung von StorageGRID.

## Verwandte Informationen

["StorageGRID-Sicherheitszertifikate werden verwendet"](#)

["Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"](#)

["Monitor Fehlerbehebung"](#)

## Bearbeiten von Administrator-Clientzertifikaten

Sie können ein Zertifikat bearbeiten, um seinen Namen zu ändern, Prometheus-Zugriff zu aktivieren oder zu deaktivieren oder ein neues Zertifikat hochzuladen, wenn das aktuelle abgelaufen ist.

### Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen die IP-Adresse oder den Domännennamen des Admin-Knotens kennen.
- Wenn Sie ein neues Zertifikat und einen privaten Schlüssel hochladen möchten, müssen diese auf Ihrem lokalen Computer verfügbar sein.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Client-Zertifikate**.

Die Seite Clientzertifikate wird angezeigt. Die vorhandenen Zertifikate sind aufgelistet.

In der Tabelle sind die Daten zum Ablauf des Zertifikats aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Wählen Sie das Optionsfeld links neben dem Zertifikat, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten**.

Das Dialogfeld Zertifikat bearbeiten wird angezeigt.

Edit Certificate test-certificate-generate

Name

Allow Prometheus

---

**Certificate Details**

Upload the public key for the client certificate.

Certificate metadata

```

Subject DN: /CN=test.com
Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53
Issuer DN: /CN=test.com
Issued On: 2020-11-23T15:53:33.000Z
Expires On: 2022-11-23T15:53:33.000Z
SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7
SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:9
0:EC:7A:7B:EF:23:14:55:3D:56

```

Certificate PEM

```

-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzUzWhcNMjAxMTIz
MTU1MzUzWjATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKdGfEneCDFDsljvlnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkW05a2Mym7EhbNrfwOt2nMjQkcaKIrK8OAmutRgG6N1N12FIW0qYQouzFQ0QddLq
n7ymFz6wSa9zYSu7Lp84Yn0/LSDPk+h3Jio7Mrt2X70It52DRwFmbLNvEvYEtTS
h+FbNh885AIRO2eLxvC0IRij1bySe76wK+Wmc97HdxRSgyxIWk6BD47XC+d0rv55
wvtjc/41qc5xsE6Xm7s2yJg4VARr10y8Icwa9fz00+xPwIdC0NwXkpWJXeBnCoXx
YqQxbWzjz+iVLJqLTMxU8zTTT30zUgN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw

```

4. Nehmen Sie die gewünschten Änderungen am Zertifikat vor.
5. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.
6. Wenn Sie ein neues Zertifikat hochgeladen haben:
  - a. Wählen Sie **Zertifikat in Zwischenablage kopieren** aus, um das Zertifikat in Ihr externes Überwachungstool einzufügen.
  - b. Verwenden Sie ein Bearbeitungswerkzeug, um den neuen privaten Schlüssel in Ihr externes Überwachungstool zu kopieren und einzufügen.

- c. Speichern und testen Sie das Zertifikat und den privaten Schlüssel in Ihrem externen Monitoring-Tool.
7. Wenn Sie ein neues Zertifikat generiert haben:
- a. Wählen Sie **Zertifikat in Zwischenablage kopieren** aus, um das Zertifikat in Ihr externes Überwachungstool einzufügen.
  - b. Wählen Sie **Privatschlüssel in Zwischenablage kopieren**, um das Zertifikat in Ihr externes Überwachungstool einzufügen.



Nach dem Schließen des Dialogfelds können Sie den privaten Schlüssel nicht anzeigen oder kopieren. Kopieren Sie den Schlüssel an einen sicheren Ort.

- c. Speichern und testen Sie das Zertifikat und den privaten Schlüssel in Ihrem externen Monitoring-Tool.

## Entfernen von Administrator-Client-Zertifikaten

Wenn Sie kein Zertifikat mehr benötigen, können Sie es entfernen.

### Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

### Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Client-Zertifikate**.

Die Seite Clientzertifikate wird angezeigt. Die vorhandenen Zertifikate sind aufgelistet.

<input type="button" value="+ Add"/> <input type="button" value="✎ Edit"/> <input type="button" value="✕ Remove"/>			
	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Wählen Sie das Optionsfeld links neben dem Zertifikat, das Sie entfernen möchten.
3. Wählen Sie **Entfernen**.

Ein Bestätigungsdialogfeld wird angezeigt.

**⚠ Warning**

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

4. Wählen Sie **OK**.

Das Zertifikat wird entfernt.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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.