



Kontrolle des Zugriffs auf StorageGRID

StorageGRID software

NetApp

February 12, 2026

Inhalt

Kontrolle des Zugriffs auf StorageGRID	1
Kontrolle über den StorageGRID-Zugriff	1
Den Zugriff auf den Grid Manager steuern	1
Aktivieren Sie Single Sign On	1
Provisionierungs-Passphrase ändern	1
Ändern der Passwörter für die Node-Konsole	1
Ändern Sie die Provisionierungs-Passphrase	2
Ändern der Passwörter für die Node-Konsole	3
Greifen Sie auf den Assistenten zu	3
Laden Sie das aktuelle Wiederherstellungspaket herunter	3
Neue Passwörter bereitstellen	4
Schließen Sie die Passwortänderung ab	4
Ändern Sie die SSH-Zugriffskennwörter für Admin-Nodes	5
Greifen Sie auf den Assistenten zu	6
Laden Sie das aktuelle Wiederherstellungspaket herunter	6
Ändern Sie die SSH-Zugriffsschlüssel	6
Verwenden Sie den Identitätsverbund	7
Konfigurieren Sie die Identitätsföderation für Grid Manager	7
Synchronisierung mit der Identitätsquelle erzwingen	11
Deaktivieren Sie den Identitätsverbund	12
Richtlinien für die Konfiguration eines OpenLDAP-Servers	12
Managen von Admin-Gruppen	13
Erstellen einer Admin-Gruppe	13
Anzeigen und Bearbeiten von Admin-Gruppen	15
Duplizieren einer Gruppe	16
Gruppe löschen	16
Berechtigungen für Admin-Gruppen	16
Interaktion zwischen Berechtigungen und Zugriffsmodus	16
Root-Zugriff	17
Root-Passwort des Mandanten ändern	17
ILM	17
Wartung	17
Verwalten von Meldungen	18
Abfrage von Kennzahlen	18
Suche nach Objektmetadaten	18
Andere Grid-Konfiguration	18
Storage Appliance-Administrator	19
Mandantenkonten	19
Benutzer managen	19
Erstellen Sie einen lokalen Benutzer	19
Lokale Benutzer anzeigen und bearbeiten	20
Importieren von Verbundbenutzern	22
Duplizieren eines Benutzers	22

Löschen Sie einen Benutzer	23
Single Sign On (SSO) verwenden	23
So funktioniert SSO	23
Anforderungen und Überlegungen für SSO	25
Bestätigen Sie, dass verbundene Benutzer sich anmelden können	27
SSO konfigurieren	28
Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS	35
Erstellen Sie Unternehmensanwendungen in Entra ID	40
Erstellen von SP-Verbindungen (Service Provider) in PingFederate	42
SSO deaktivieren	47
SSO für einen Admin-Knoten vorübergehend deaktivieren und wieder aktivieren	47

Kontrolle des Zugriffs auf StorageGRID

Kontrolle über den StorageGRID-Zugriff

Sie steuern, wer auf StorageGRID zugreifen kann und welche Aufgaben Benutzer ausführen können, indem Sie Gruppen und Benutzer erstellen oder importieren und jeder Gruppe Berechtigungen zuweisen. Optional können Sie Single Sign On (SSO) aktivieren, Client-Zertifikate erstellen und Grid-Passwörter ändern.

Den Zugriff auf den Grid Manager steuern

Sie bestimmen, wer auf den Grid Manager und die Grid Management API zugreifen kann, indem Sie Gruppen und Benutzer von einem Identitätsverbundservice aus importieren oder lokale Gruppen und lokale Benutzer einrichten.

Mit "[Identitätsföderation](#)" wird die Einrichtung "[Gruppen](#)" beschleunigt und "[Benutzer](#)" Benutzer können sich mit vertrauten Anmeldeinformationen bei StorageGRID anmelden. Sie können die Identitätsföderation konfigurieren, wenn Sie Active Directory, OpenLDAP oder Oracle Directory Server verwenden.



Wenden Sie sich an den technischen Support, wenn Sie einen anderen LDAP v3-Dienst verwenden möchten.

Sie legen fest, welche Aufgaben jeder Benutzer durchführen kann, indem Sie jeder Gruppe unterschiedliche Aufgaben zuweisen "[Berechtigungen](#)". Beispielsweise können Benutzer in einer Gruppe in der Lage sein, ILM-Regeln und Benutzer in einer anderen Gruppe zu verwalten, um Wartungsaufgaben durchzuführen. Ein Benutzer muss mindestens einer Gruppe angehören, um auf das System zuzugreifen.

Optional können Sie eine Gruppe als schreibgeschützt konfigurieren. Benutzer in einer schreibgeschützten Gruppe können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen an der Grid Manager- oder Grid-Management-API vornehmen oder Vorgänge ausführen.

Aktivieren Sie Single Sign On

Das StorageGRID -System unterstützt Single Sign-On (SSO) mithilfe des Standards Security Assertion Markup Language 2.0 (SAML 2.0). Nach Ihnen "[Konfigurieren und aktivieren Sie SSO](#)" müssen alle Benutzer von einem externen Identitätsanbieter authentifiziert werden, bevor sie auf den Grid Manager, den Tenant Manager, die Grid Management API oder die Tenant Management API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

Provisionierungs-Passphrase ändern

Die Bereitstellungspassphrase wird für viele Installations- und Wartungsverfahren sowie zum Herunterladen des StorageGRID -Wiederherstellungspakets benötigt. Die Passphrase ist auch zum Herunterladen von Backups der Grid-Topologieinformationen und Verschlüsselungsschlüssel für das StorageGRID -System erforderlich. Du kannst "[Ändern Sie die Passphrase](#)" nach Bedarf.

Ändern der Passwörter für die Node-Konsole

Jeder Knoten in Ihrem Grid verfügt über ein Knotenkonsolenkennwort, das Sie benötigen, um sich per SSH als „Admin“ beim Knoten oder bei einer VM-/physischen Konsolenverbindung als Root-Benutzer anzumelden. Bei Bedarf können Sie "[Ändern Sie das Passwort für die Node-Konsole](#)" für jeden Knoten.

Ändern Sie die Provisionierungs-Passphrase

Verwenden Sie dieses Verfahren, um die Passphrase für die StorageGRID Bereitstellung zu ändern. Die Passphrase wird für Wiederherstellungs-, Erweiterungs- und Wartungsverfahren benötigt. Die Passphrase ist auch zum Herunterladen von Backups des Wiederherstellungspakets erforderlich, die Informationen zur Grid-Topologie, Passwörter für die Grid-Knotenkonsole und Verschlüsselungsschlüssel für das StorageGRID System enthalten.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

Die Bereitstellungspassphrase wird für viele Installations- und Wartungsverfahren benötigt, sowie für "[Herunterladen des Wiederherstellungspakets](#)". Die Bereitstellungspassphrase ist nicht aufgeführt in der `Passwords.txt` Datei. Dokumentieren Sie die Bereitstellungspassphrase und bewahren Sie sie an einem sicheren Ort auf.

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Grid-Passwörter**.
2. Wählen Sie unter **Change Provisioning Passphrase** die Option **make a change** aus
3. Geben Sie Ihre aktuelle Provisionierungs-Passphrase ein.
4. Geben Sie die neue Passphrase ein. Die Passphrase muss mindestens 8 und maximal 32 Zeichen enthalten. Passphrases sind Groß-/Kleinschreibung.



Bewahren Sie die Bereitstellungspassphrase an einem sicheren Ort auf. Es wird für Installations-, Erweiterungs- und Wartungsverfahren benötigt.

5. Geben Sie die neue Passphrase erneut ein, und wählen Sie **Speichern**.

Das System zeigt ein grünes Erfolgsbanner an, wenn die Änderung der Provisionierungs-Passphrase abgeschlossen ist.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Wählen Sie **Wiederherstellungspaket**.
7. Geben Sie die neue Bereitstellungspassphrase ein, um das neue Wiederherstellungspaket herunterzuladen.



Nach dem Ändern der Bereitstellungspassphrase müssen Sie sofort ein neues Wiederherstellungspaket herunterladen. Mit der Wiederherstellungspaketdatei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

Ändern der Passwörter für die Node-Konsole

Jeder Knoten in Ihrem Grid verfügt über ein Knotenkonsolenkennwort, mit dem Sie sich beim Knoten anmelden. Standardmäßig hat jeder Knoten ein eindeutiges Passwort. Sie können jedes Kennwort in ein neues, eindeutiges Kennwort ändern oder das Kennwort für jeden Knoten ändern, um ein globales Kennwort zu verwenden. Die Passwörter werden im Wiederherstellungspaket gespeichert.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Berechtigung für Wartung oder Root-Zugriff"](#).
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

Sie verwenden ein Knotenkonsolenkennwort, um sich per SSH als „Administrator“ bei einem Knoten oder als Root-Benutzer bei einer VM-/physischen Konsolenverbindung anzumelden. Sie können die Passwörter der Knotenkonsole mit einer der folgenden Optionen ändern:

- Wenden Sie automatisch zufällige Passwörter auf jeden Knoten an
- Ein globales Passwort für alle Knoten festlegen und anwenden
- Geben Sie ein eindeutiges Kennwort an und wenden Sie es auf einen oder mehrere Knoten an.

Die Passwörter werden in einer aktualisierten `Passwords.txt` Datei im Wiederherstellungspaket. Die Passwörter sind in der Spalte „Passwort“ der Datei aufgeführt.



Der ["SSH-Zugriffspasswörter"](#) denn die für die Kommunikation zwischen Knoten verwendeten SSH-Schlüssel sind von den Passwörtern der Knotenkonsole getrennt. Dieses Verfahren ändert die SSH-Zugriffskennwörter nicht.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Grid-Passwörter**.
2. Wählen Sie unter **Change Node Console passwords** die Option **make a change** aus.

Laden Sie das aktuelle Wiederherstellungspaket herunter

Laden Sie das aktuelle Wiederherstellungspaket herunter, bevor Sie die Passwörter der Knotenkonsole ändern. Sie können die Passwörter in dieser Datei verwenden, wenn der Passwortänderungsprozess für einen beliebigen Knoten fehlschlägt.

Schritte

1. Geben Sie die Provisionierungs-Passphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.
3. Kopieren Sie die Wiederherstellungspaketdatei (`.zip`) an zwei sichere und getrennte Orte.



Die Wiederherstellungspaketdatei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

4. Wählen Sie **Weiter**.

Neue Passwörter bereitstellen

1. Wählen Sie die gewünschte Methode zum Ändern des Kennworts aus.

- **Automatisch:** StorageGRID weist allen Knoten automatisch ein neues zufälliges Konsolenkennwort zu.
- **Benutzerdefiniert:** Sie geben Konsolenkennwörter an.

Automatisch

1. Wählen Sie **Weiter**.

Individuell

1. Wählen Sie eine der folgenden Optionen:

- **Globales Konsolenkennwort:** Wenden Sie auf allen Knoten dasselbe Konsolenkennwort an.
- **Eindeutige Konsolenkennwörter:** Wenden Sie auf einem oder mehreren Knoten ein anderes Kennwort an.

2. Wenn Sie **Globales Konsolenkennwort** ausgewählt haben, geben Sie das Kennwort ein, das Sie für alle Knoten verwenden möchten.

3. Wenn Sie **Eindeutige Konsolenkennwörter** ausgewählt haben, geben Sie ein eindeutiges Kennwort für einen oder mehrere Knoten ein.

4. Wählen Sie **Weiter**.

Schließen Sie die Passwortänderung ab

1. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**, wenn Sie bereit sind, dass StorageGRID mit der Änderung der Knotenkonsolenkennwörter beginnt.



Sie können diesen Vorgang nach dem Start nicht abbrechen.

StorageGRID generiert ein neues Wiederherstellungspaket, das das neue Passwort enthält.

2. Wenn das neue Wiederherstellungspaket fertig ist, wählen Sie **Neues Wiederherstellungspaket herunterladen** und speichern Sie das Wiederherstellungspaket.

3. Öffnen Sie die `.zip` Datei.

4. Vergewissern Sie sich, dass Sie auf den Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen Kennwörter der Node-Konsole enthält.

5. Kopieren Sie die neue Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.



Überschreiben Sie nicht das alte Wiederherstellungspaket.

Sie müssen die Wiederherstellungsdatei sichern, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

6. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie das neue Wiederherstellungspaket heruntergeladen und den Inhalt überprüft haben.
7. Wählen Sie **Weiter**.

StorageGRID aktualisiert das Passwort für jeden Knoten.

Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in der Fortschrittsleiste die Anzahl der Knoten aufgeführt, deren Passwörter nicht geändert werden konnten. Das System wiederholt den Vorgang automatisch auf jedem Knoten, dessen Kennwort nicht geändert werden konnte. Wenn der Vorgang endet und einige Knoten immer noch kein geändertes Kennwort haben, wird die Schaltfläche **Wiederholen** angezeigt.

8. Wenn die Kennwortaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:
 - a. Überprüfen Sie die in der Tabelle aufgeführten Fehlermeldungen.
 - b. Beheben Sie die Probleme.
 - c. Wählen Sie **Wiederholen**.



Beim erneuten Versuch werden nur die Kennwörter der Knotenkonsole auf den Knoten geändert, die bei früheren Kennwortänderungsversuchen fehlgeschlagen sind.

9. Wenn der Fortschrittsbalken anzeigt, dass keine Updates mehr verfügbar sind, wählen Sie **Fertig**.
10. Nachdem die Passwörter der Knotenkonsole für alle Knoten geändert wurden, löschen Sie [dieses erste Wiederherstellungspaket, das Sie heruntergeladen haben](#).

Ändern Sie die SSH-Zugriffskennwörter für Admin-Nodes

Wenn Sie die SSH-Zugriffskennwörter für Admin-Nodes ändern, werden auch die eindeutigen Sätze interner SSH-Schlüssel für jeden Node im Grid aktualisiert. Der primäre Admin-Node verwendet diese SSH-Schlüssel, um mit einer sicheren Authentifizierung ohne Kennwort auf Knoten zuzugreifen.

Verwenden Sie einen SSH-Schlüssel, um sich bei einem Node als `admin` oder beim Root-Benutzer auf einer VM- oder physischen Konsolenverbindung anzumelden.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Berechtigung für Wartung oder Root-Zugriff"](#).
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

Die neuen Zugangspasswörter für Admin-Knoten und die neuen internen Schlüssel für jeden Knoten werden im `Passwords.txt` Datei im Wiederherstellungspaket. Die Schlüssel sind in der Spalte „Passwort“ dieser Datei aufgeführt.

Separate SSH-Zugriffskennwörter für die SSH-Schlüssel, die für die Kommunikation zwischen den Nodes verwendet werden. Diese werden durch dieses Verfahren nicht geändert.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Grid-Passwörter**.
2. Wählen Sie unter **SSH-Schlüssel ändern** **Änderung vornehmen**.

Laden Sie das aktuelle Wiederherstellungspaket herunter

Laden Sie vor dem Ändern der SSH-Zugriffsschlüssel das aktuelle Wiederherstellungspaket herunter. Sie können die Schlüssel in dieser Datei verwenden, wenn der Schlüsseländerungsprozess für einen beliebigen Knoten fehlschlägt.

Schritte

1. Geben Sie die Provisionierungs-Passphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.
3. Kopieren Sie die Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.



Die Wiederherstellungspaketdatei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

4. Wählen Sie **Weiter**.
5. Wenn das Bestätigungsdiaologfeld angezeigt wird, wählen Sie **Yes** aus, wenn Sie bereit sind, die SSH-Zugriffsschlüssel zu ändern.



Sie können diesen Vorgang nach dem Start nicht abbrechen.

Ändern Sie die SSH-Zugriffsschlüssel

Wenn der Prozess zum Ändern der SSH-Zugriffsschlüssel beginnt, wird ein neues Wiederherstellungspaket generiert, das die neuen Schlüssel enthält. Anschließend werden die Schlüssel auf jedem Knoten aktualisiert.

Schritte

1. Warten Sie, bis das neue Wiederherstellungspaket generiert wurde. Dies kann einige Minuten dauern.
2. Wenn die Schaltfläche „Neues Wiederherstellungspaket herunterladen“ aktiviert ist, wählen Sie „Neues Wiederherstellungspaket herunterladen“ und speichern Sie die neue Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.
3. Wenn der Download abgeschlossen ist:
 - a. Öffnen Sie die `.zip` Datei.
 - b. Bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen SSH-Zugriffsschlüssel enthält.
 - c. Kopieren Sie die neue Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.



Überschreiben Sie nicht das alte Wiederherstellungspaket.

Die Wiederherstellungspaketdatei muss gesichert werden, da sie Verschlüsselungsschlüssel und

Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

4. Warten Sie, bis die Schlüssel auf jedem Node aktualisiert werden. Dies kann einige Minuten dauern.

Wenn die Schlüssel für alle Nodes geändert werden, wird ein grünes Success-Banner angezeigt.

Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in einer Banner-Meldung die Anzahl der Knoten aufgeführt, bei denen die Schlüssel nicht geändert wurden. Das System wiederholt den Prozess automatisch auf jedem Node, bei dem der Schlüssel nicht geändert wurde. Wenn der Prozess mit einigen Knoten endet, die noch keinen geänderten Schlüssel haben, wird die Schaltfläche **Wiederholen** angezeigt.

Wenn das Schlüsselupdate für einen oder mehrere Nodes fehlgeschlagen ist:

- a. Überprüfen Sie die in der Tabelle aufgeführten Fehlermeldungen.
- b. Beheben Sie die Probleme.
- c. Wählen Sie **Wiederholen**.

Durch die erneute Versuche werden nur die SSH-Zugriffsschlüssel auf den Nodes geändert, die bei vorherigen Versuchen mit Schlüsseländerungen fehlgeschlagen sind.

5. Nachdem die SSH-Zugriffsschlüssel für alle Knoten geändert wurden, löschen Sie die [das erste Wiederherstellungspaket, das Sie heruntergeladen haben](#) .
6. Wählen Sie optional **Wartung > System > Wiederherstellungspaket**, um eine zusätzliche Kopie des neuen Wiederherstellungspakets herunterzuladen.

Verwenden Sie den Identitätsverbund

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

Konfigurieren Sie die Identitätsföderation für Grid Manager

Sie können die Identitätsföderation im Grid Manager konfigurieren, wenn Sie möchten, dass Administratorgruppen und Benutzer in einem anderen System wie Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server verwaltet werden.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["Unterstützter Webbrowser"](#) .
- Du hast ["Bestimmte Zugriffsberechtigungen"](#) .
- Sie verwenden Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.



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

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Siehe [Richtlinien für die Konfiguration eines OpenLDAP-Servers](#).
- Wenn Sie Single Sign-On (SSO) aktivieren möchten, haben Sie die ["Voraussetzungen und Überlegungen"](#)

für Single Sign-On" .

- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, verwendet der Identitäts-Provider TLS 1.2 oder 1.3. Siehe "[Unterstützte Chiffren für ausgehende TLS-Verbindungen](#)".

Über diese Aufgabe

Sie können eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie Gruppen aus einem anderen System wie Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server importieren möchten. Sie können die folgenden Gruppentypen importieren:

- Admin-Gruppen. Die Benutzer in Admin-Gruppen können sich beim Grid Manager anmelden und anhand der Verwaltungsberechtigungen, die der Gruppe zugewiesen sind, Aufgaben ausführen.
- Mandantenbenutzergruppen für Mandanten, die keine eigene Identitätsquelle 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. Weitere Informationen finden Sie unter "[Erstellen eines Mandantenkontos](#)" und "[Verwenden Sie ein Mandantenkonto](#)".

Geben Sie die Konfiguration ein

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Identitätsföderation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other
------------------	----------	----------	-------

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

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
 - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `uid` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `uid` .
 - **Benutzer-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `nsuniqueid` . Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
 - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `cn` für

OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `cn` .

- **Gruppen-UUID:** Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `nsuniqueid` . Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.

5. Geben Sie für alle LDAP-Servicetypen die Informationen zum erforderlichen LDAP-Server und zur Netzwerkverbindung im Abschnitt LDAP-Server konfigurieren ein.

- **Hostname:** Der vollständig qualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
- **Port:** Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird.



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

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

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

Der angegebene Benutzer muss über die Berechtigung zum Auflisten von Gruppen und Benutzern sowie zum Zugriff auf die folgenden Attribute verfügen:

- `sAMAccountName` Oder `uid`
 - `objectGUID`, `entryUUID` Oder `nsuniqueid`
 - `cn`
 - `memberOf` Oder `isMemberOf`
 - **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl` Und `userPrincipalName`
 - **Eintritts-ID:** `accountEnabled` Und `userPrincipalName`
- **Passwort:** Das mit dem Benutzernamen verknüpfte Passwort.



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

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



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

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



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

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

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

Geben Sie eines der folgenden Muster ein:

- **UserPrincipalName-Muster (AD- und Entra-ID):** [USERNAME]@example.com
- **Anmeldenamenmuster auf niedrigerer Ebene (AD- und Entra-ID):** example\[USERNAME]
- **Distinguished Namensmuster:** CN=[USERNAME], CN=Users, DC=example, DC=com

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

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

- **STARTTLS verwenden:** Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese Option wird für Microsoft Entra ID nicht unterstützt.
- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für die Microsoft Entra ID auswählen.
- **TLS nicht verwenden:** Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für die Microsoft Entra ID nicht unterstützt.



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

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.

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

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

Testen Sie die Verbindung und speichern Sie die Konfiguration

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

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein Bind-Benutzernamenformat angegeben haben:

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

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

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

Synchronisierung mit 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.

Schritte

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

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



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

Deaktivieren Sie den Identitätsverbund

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

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.
- Es findet keine Synchronisierung zwischen dem StorageGRID -System und der Identitätsquelle statt und es werden keine Warnungen für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn der Single Sign-On-Status (SSO) **Aktiviert** oder **Sandbox-Modus** ist. Der SSO-Status auf der Single Sign-On-Seite muss **Deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Sehen "[Deaktivieren Sie Single Sign-On](#)".

Schritte

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

Richtlinien für die Konfiguration eines OpenLDAP-Servers

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



Bei Identitätsquellen, bei denen es sich nicht um Active Directory oder Microsoft Entra ID handelt, blockiert StorageGRID den S3-Zugriff für extern deaktivierte Benutzer nicht automatisch. Um den S3-Zugriff zu blockieren, löschen Sie alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Überlagerungen in Memberof und Refint

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

Indizierung

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

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

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

Weitere Informationen zur Pflege der umgekehrten Gruppenmitgliedschaft finden Sie im ["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"](#).

Managen von 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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben ["Bestimmte Zugriffsberechtigungen"](#).
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Erstellen einer Admin-Gruppe

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

Greifen Sie auf den Assistenten zu

Schritte

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

Wählen Sie einen Gruppentyp aus

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

- Erstellen Sie eine lokale Gruppe, wenn Sie lokalen Benutzern Berechtigungen zuweisen möchten.
- Erstellen Sie eine föderierte Gruppe, um Benutzer aus der Identitätsquelle zu importieren.

Lokale Gruppe

Schritte

1. Wählen Sie **Lokale Gruppe**.
2. Geben Sie einen Anzeigenamen für die Gruppe ein, den Sie bei Bedarf später aktualisieren können.
Beispiel: „Maintenance Users“ oder „ILM Administrators“.
3. Geben Sie einen eindeutigen Namen für die Gruppe ein, den Sie später nicht mehr aktualisieren können.
4. Wählen Sie **Weiter**.

Föderierte Gruppe

Schritte

1. Wählen Sie **Federated Group**.
2. Geben Sie den Namen der Gruppe ein, die importiert werden soll, genau so, wie sie in der konfigurierten Identitätsquelle angezeigt wird.
 - Verwenden Sie für Active Directory und Microsoft Entra ID den sAMAccountName.
 - Verwenden Sie für OpenLDAP das CN (Common Name).
 - Verwenden Sie für einen anderen LDAP den entsprechenden eindeutigen Namen für den LDAP-Server.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Schritte

1. 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 an der Grid Manager- oder Grid-Management-API vornehmen oder Vorgänge 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.

2. Wählen Sie eine oder mehrere "**Berechtigungen für Administratorgruppen**".

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

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

Benutzer hinzufügen (nur lokale Gruppen)

Schritte

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


Wenn Sie noch keine lokalen Benutzer erstellt haben, können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können diese Gruppe dem Benutzer auf der Seite Benutzer hinzufügen. Weitere Informationen finden Sie unter ["Benutzer managen"](#).

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

Anzeigen und Bearbeiten von Admin-Gruppen

Sie können Details für vorhandene Gruppen anzeigen, eine Gruppe ändern oder eine Gruppe duplizieren.

- Um grundlegende Informationen für alle Gruppen anzuzeigen, überprüfen Sie die Tabelle auf der Seite Gruppen.
- Um alle Details für eine bestimmte Gruppe anzuzeigen oder eine Gruppe zu bearbeiten, verwenden Sie das Menü **Aktionen** oder die Detailseite.

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Gruppendetails an	<ol style="list-style-type: none">a. Aktivieren Sie das Kontrollkästchen für die Gruppe.b. Wählen Sie Aktionen > Gruppendetails anzeigen.	Wählen Sie den Gruppennamen in der Tabelle aus.
Anzeigenname bearbeiten (nur lokale Gruppen)	<ol style="list-style-type: none">a. Aktivieren Sie das Kontrollkästchen für die Gruppe.b. Wählen Sie Aktionen > Gruppenname bearbeiten.c. Geben Sie den neuen Namen ein.d. Wählen Sie Änderungen speichern.	<ol style="list-style-type: none">a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen.b. Wählen Sie das Symbol Bearbeiten .c. Geben Sie den neuen Namen ein.d. Wählen Sie Änderungen speichern.
Zugriffsmodus oder Berechtigungen bearbeiten	<ol style="list-style-type: none">a. Aktivieren Sie das Kontrollkästchen für die Gruppe.b. Wählen Sie Aktionen > Gruppendetails anzeigen.c. Ändern Sie optional den Zugriffsmodus der Gruppe.d. Wählen oder löschen Sie optional "Berechtigungen für Administratorgruppen".e. Wählen Sie Änderungen speichern.	<ol style="list-style-type: none">a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen.b. Ändern Sie optional den Zugriffsmodus der Gruppe.c. Wählen oder löschen Sie optional "Berechtigungen für Administratorgruppen".d. Wählen Sie Änderungen speichern.

Duplizieren einer Gruppe

Schritte

1. Aktivieren Sie das Kontrollkästchen für die Gruppe.
2. Wählen Sie **Aktionen** > **Gruppe duplizieren**.
3. Schließen Sie den Assistenten für die doppelte Gruppe ab.

Gruppe löschen

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 Benutzer aus der Gruppe entfernt, die Benutzer jedoch nicht gelöscht.

Schritte

1. Aktivieren Sie auf der Seite Gruppen das Kontrollkästchen für jede Gruppe, die Sie entfernen möchten.
2. Wählen Sie **Aktionen** > **Gruppe löschen**.
3. Wählen Sie **Gruppen löschen**.

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 oder der Grid Management API 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
- Dashboard anzeigen
- Zeigen Sie die Seiten Knoten an
- Anzeige aktueller und aufgelöster Warnmeldungen
- Eigenes Kennwort ändern (nur lokale Benutzer)
- Zeigen Sie bestimmte Informationen auf den Seiten Konfiguration und Wartung an

Interaktion zwischen Berechtigungen und Zugriffsmodus

Für alle Berechtigungen bestimmt die Einstellung **Zugriffsmodus** der Gruppe, 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.

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Admin-Gruppe zuweisen können. Jede Funktion, die nicht explizit erwähnt wird, erfordert die **Root**

Access-Berechtigung.

Root-Zugriff

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

Root-Passwort des Mandanten ändern

Diese Berechtigung bietet Zugriff auf die Option **Root-Passwort ändern** auf der Seite der Mieter, so dass Sie steuern können, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern kann. Diese Berechtigung wird auch für die Migration von S3-Schlüsseln verwendet, wenn die S3-Key-Importfunktion aktiviert ist. Benutzer, die diese Berechtigung nicht besitzen, können die Option **root-Passwort ändern** nicht sehen.



Um Zugriff auf die Seite Mieter zu gewähren, die die Option **Root Passwort ändern** enthält, weisen Sie auch die Berechtigung **Mandantenkonten** zu.

ILM

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Storage-Pools
- Lagergütern
- Regionen
- Suche nach Objektmetadaten



Benutzer müssen über die Berechtigung **Andere Rasterkonfiguration** verfügen, um Speicherklassen verwalten zu können.

Wartung

Benutzer müssen über die Berechtigung zur Wartung verfügen, um folgende Optionen verwenden zu können:

- **Konfiguration > Zugriffskontrolle:**
 - Grid-Passwörter
- **Konfiguration > Netzwerk:**
 - Domännennamen des S3-Endpunkts
- **Wartung > Aufgaben:**
 - Ausmustern
 - Erweiterung
 - Überprüfung der Objektexistenz
 - Recovery

- **Wartung > System:**

- Recovery-Paket
- Software-Update

- **Support > Tools:**

- Protokolle

Benutzer, die nicht über die Berechtigung Wartung verfügen, können diese Seiten anzeigen, aber nicht bearbeiten:

- **Wartung > Netzwerk:**

- DNS-Server
- Grid-Netzwerk
- NTP-Server

- **Wartung > System:**

- Lizenz

- **Konfiguration > Netzwerk:**

- Domännennamen des S3-Endpunkts

- **Konfiguration > Sicherheit:**

- Zertifikate

- **Konfiguration > Überwachung:**

- Audit- und Syslog-Server

Verwalten von Meldungen

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.

Abfrage von Kennzahlen

Diese Berechtigung bietet Zugriff auf:

- **Support > Tools > Metriken-Seite**
- Benutzerdefinierte Prometheus-Metrikabfragen mit dem Abschnitt **Metrics** der Grid Management API
- Dashboard-Karten von Grid Manager, die Metriken enthalten

Suche nach Objektmetadaten

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **ILM > Objekt-Metadaten-Lookup**.

Andere Grid-Konfiguration

Diese Berechtigung bietet Zugriff auf diese zusätzlichen Rasterkonfigurationsoptionen:

- **ILM:**

- Lagergüten

- **Konfiguration > System:**
- **Support > Sonstiges:**
 - Verbindungskosten

Storage Appliance-Administrator

Diese Berechtigung bietet:

- Zugriff auf den E-Series SANtricity System Manager auf Storage Appliances über den Grid Manager
- Die Möglichkeit zur Durchführung von Fehlerbehebungs- und Wartungsaufgaben auf der Registerkarte Laufwerke managen für Appliances, die diese Vorgänge unterstützen.

Mandantenkonten

Mit dieser Berechtigung können Sie:

- Öffnen Sie die Seite Tenants, auf der Sie Mandantenkonten erstellen, bearbeiten und entfernen können
- Zeigen Sie vorhandene Richtlinien zur Verkehrsklassifizierung an
- Dashboard-Karten von Grid Manager anzeigen, die Mandantendetails enthalten

Benutzer managen

Sie können lokale und föderierte Benutzer anzeigen. Sie können auch lokale Benutzer erstellen und lokalen Administratorgruppen zuordnen, um zu bestimmen, auf welche Grid Manager-Funktionen diese Benutzer zugreifen können.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".

Erstellen Sie einen lokalen Benutzer

Sie können einen oder mehrere lokale Benutzer erstellen und jedem Benutzer einer oder mehreren lokalen Gruppen zuweisen. Die Berechtigungen der Gruppe steuern, auf welche Grid Manager- und Grid Management API-Funktionen der Benutzer zugreifen kann.

Sie können nur lokale Benutzer erstellen. Verwenden Sie die externe Identitätsquelle, um verbundene Benutzer und Gruppen zu verwalten.

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



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

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Benutzer**.
2. Wählen Sie **Benutzer erstellen**.

Geben Sie die Anmeldedaten des Benutzers ein

Schritte

1. Geben Sie den vollständigen Namen des Benutzers, einen eindeutigen Benutzernamen und ein Kennwort ein.
2. Wählen Sie optional **Ja** aus, wenn dieser Benutzer keinen Zugriff auf den Grid Manager oder die Grid Management API haben soll.
3. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

1. Weisen Sie den Benutzer optional einer oder mehreren Gruppen zu, um die Berechtigungen des Benutzers zu ermitteln.

Wenn Sie noch keine Gruppen erstellt haben, können Sie den Benutzer speichern, ohne Gruppen auszuwählen. Sie können diesen Benutzer einer Gruppe auf der Seite Gruppen hinzufügen.

Wenn ein Benutzer zu mehreren Gruppen gehört, werden die Berechtigungen kumulativ. Weitere Informationen finden Sie unter ["Managen von Admin-Gruppen"](#) .

2. Wählen Sie **Benutzer erstellen** und wählen Sie **Fertig**.

Lokale Benutzer anzeigen und bearbeiten

Details zu vorhandenen lokalen und föderierten Benutzern können angezeigt werden. Sie können einen lokalen Benutzer ändern, um den vollständigen Namen, das Kennwort oder die Gruppenmitgliedschaft des Benutzers zu ändern. Sie können auch vorübergehend verhindern, dass ein Benutzer auf den Grid Manager und die Grid Management API zugreift.


Sie können nur lokale Benutzer bearbeiten. Verwenden Sie die externe Identitätsquelle, um verbundene Benutzer zu verwalten.

- Um grundlegende Informationen für alle lokalen und föderierten Benutzer anzuzeigen, lesen Sie die Tabelle auf der Benutzer-Seite.
- Um alle Details für einen bestimmten Benutzer anzuzeigen, einen lokalen Benutzer zu bearbeiten oder das Passwort eines lokalen Benutzers zu ändern, verwenden Sie das Menü **Aktionen** oder die Detailseite.

Bei der nächsten Abmeldet sich der Benutzer an und meldet sich dann wieder beim Grid Manager an.



Lokale Benutzer können ihre eigenen Passwörter über die Option **Passwort ändern** im Grid Manager Banner ändern.

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Benutzerdetails an	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. 	Wählen Sie den Benutzernamen in der Tabelle aus.
Vollständigen Namen bearbeiten (nur lokale Benutzer)	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > vollständigen Namen bearbeiten. c. Geben Sie den neuen Namen ein. d. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie das Symbol Bearbeiten . c. Geben Sie den neuen Namen ein. d. Wählen Sie Änderungen speichern.
StorageGRID-Zugriff verweigern oder zulassen	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. c. Wählen Sie die Registerkarte Zugriff aus. d. Wählen Sie Ja aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie Nein aus, damit der Benutzer sich anmelden kann. e. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Zugriff aus. c. Wählen Sie Ja aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie Nein aus, damit der Benutzer sich anmelden kann. d. Wählen Sie Änderungen speichern.
Passwort ändern (nur lokale Benutzer)	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. c. Wählen Sie die Registerkarte Kennwort aus. d. Geben Sie ein neues Passwort ein. e. Wählen Sie Passwort ändern. 	<ul style="list-style-type: none"> a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Kennwort aus. c. Geben Sie ein neues Passwort ein. d. Wählen Sie Passwort ändern.

Aufgabe	Menü „Aktionen“	Detailseite
Gruppen ändern (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen . c. Wählen Sie die Registerkarte Gruppen aus. d. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. e. Wählen Sie Gruppen bearbeiten , um verschiedene Gruppen auszuwählen. f. Wählen Sie Änderungen speichern .	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Gruppen aus. c. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. d. Wählen Sie Gruppen bearbeiten , um verschiedene Gruppen auszuwählen. e. Wählen Sie Änderungen speichern .

Importieren von Verbundbenutzern

Sie können einen oder mehrere Verbundbenutzer (bis zu maximal 100 Benutzer) direkt in die Seite „Benutzer“ importieren.

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Admin-Benutzer**.
2. Wählen Sie **Verbundbenutzer importieren**.
3. Geben Sie die UUID oder den Benutzernamen für einen oder mehrere Verbundbenutzer ein.

Fügen Sie bei mehreren Einträgen jede UUID oder jeden Benutzernamen in einer neuen Zeile hinzu.

4. Wählen Sie **Importieren**.

Wenn der Import in das Feld „Benutzer“ für einen oder mehrere Benutzer fehlschlägt, führen Sie die folgenden Schritte aus:

- a. Erweitern Sie **Nicht importierte Benutzer** und wählen Sie **Benutzer kopieren**.
- b. Versuchen Sie den Import erneut, indem Sie **Zurück** auswählen und die kopierten Benutzer in das Dialogfeld **Verbundbenutzer importieren** einfügen.

Nachdem Sie das Dialogfeld **Verbundbenutzer importieren** geschlossen haben, werden die Verbundbenutzerinformationen für die erfolgreich importierten Benutzer auf der Seite „Benutzer“ angezeigt.

Duplizieren eines Benutzers

Sie können einen vorhandenen Benutzer duplizieren, um einen neuen Benutzer mit denselben Berechtigungen zu erstellen.

Schritte

1. Aktivieren Sie das Kontrollkästchen für den Benutzer.

2. Wählen Sie **Aktionen** > **Benutzer duplizieren**.
3. Schließen Sie den Assistenten für doppelte Benutzer ab.

Löschen Sie einen Benutzer

Sie können einen lokalen Benutzer löschen, um diesen Benutzer dauerhaft aus dem System zu entfernen.



Sie können den Root-Benutzer nicht löschen.

Schritte

1. Aktivieren Sie auf der Seite Benutzer das Kontrollkästchen für jeden Benutzer, den Sie entfernen möchten.
2. Wählen Sie **Aktionen** > **Benutzer löschen**.
3. Wählen Sie **Benutzer löschen**.

Single Sign On (SSO) verwenden

So funktioniert SSO

Wenn Single Sign-On (SSO) aktiviert ist, können Benutzer nur dann auf den Grid Manager, den Tenant Manager, die Grid Management API oder die Tenant Management API zugreifen, wenn ihre Anmeldeinformationen mithilfe des von Ihrer Organisation implementierten SSO-Anmeldevorgangs autorisiert sind. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

Das StorageGRID-System unterstützt Single Sign-On (SSO) unter Verwendung des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards.

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

Melden Sie sich an, wenn SSO aktiviert ist

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 die URL zum ersten Mal in diesem Browser aufrufen, werden Sie zur Eingabe einer Konto-ID aufgefordert.
- 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 StorageGRID-Anmeldeseite wird nicht angezeigt, wenn Sie die vollständige URL für ein Mandantenkonto eingeben (d. h. einen vollständig qualifizierten Domännennamen oder eine IP-Adresse gefolgt von `?accountId=20-digit-account-id`). Stattdessen werden Sie sofort zur SSO-Anmeldeseite Ihres Unternehmens weitergeleitet, auf der Sie die Möglichkeit haben [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** aus, 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. Wählen Sie **Anmelden**

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

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 zu einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen gehören, werden Sie je nach ausgewähltem Konto beim Grid Manager oder dem Mandanten-Manager angemeldet.



Wenn das Dienstkonto nicht zugänglich ist, können Sie sich trotzdem anmelden, solange Sie ein vorhandener Benutzer sind, der zu einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen gehört.

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. Suchen Sie den Link **Abmelden** in der oberen rechten Ecke der Benutzeroberfläche.
2. Wählen Sie **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.



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.

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 Hinweis: Wenn Sie die Entra-ID für SSO verwenden, kann es einige Minuten dauern, bis Sie von allen Admin-Knoten abgemeldet sind.
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.

Anforderungen und Überlegungen für SSO

Bevor Sie Single Sign-On (SSO) für ein StorageGRID-System aktivieren, lesen Sie die Anforderungen und Überlegungen.

Anforderungen an Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

- Active Directory Federation Service (AD FS)
- Microsoft Entra ID
- PingFederate

Sie müssen die Identitätsföderation für Ihr StorageGRID-System konfigurieren, bevor Sie einen SSO-Identitätsanbieter konfigurieren können. Der Typ des LDAP-Service, den Sie für die Identitätsföderation verwenden, steuert, welcher SSO-Typ Sie implementieren können.

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory	<ul style="list-style-type: none">• Active Directory• Entra-ID• PingFederate
Entra-ID	Entra-ID

AD-FS-Anforderungen

Sie können eine der folgenden Versionen von AD FS verwenden:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS



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

Zusätzlichen Anforderungen

- Transport Layer Security (TLS) 1.2 oder 1.3
- Microsoft .NET Framework, Version 3.5.1 oder höher

Überlegungen zur Entra-ID

Wenn Sie Entra ID als SSO-Typ verwenden und Benutzer über Benutzerprinzipalnamen verfügen, die nicht sAMAccountName als Präfix verwenden, können Anmeldeprobleme auftreten, wenn StorageGRID die Verbindung zum LDAP-Server verliert. Um Benutzern die Anmeldung zu ermöglichen, müssen Sie die Verbindung zum LDAP-Server wiederherstellen.

Serverzertifikate-Anforderungen

Standardmäßig verwendet StorageGRID auf jedem Admin-Knoten ein Verwaltungsschnittstellenzertifikat, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern. Wenn Sie Vertrauensstellungen der vertrauenden Seite (AD FS), Unternehmensanwendungen (Entra ID) oder Dienstanbieterverbindungen (PingFederate) für StorageGRID konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID Anfragen.

Wenn Sie noch nicht ["Ein benutzerdefiniertes Zertifikat für die Managementoberfläche konfiguriert"](#), 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, Unternehmensanwendungen oder SP-Verbindungen verwenden.



Es wird nicht empfohlen, das Standardserverzertifikat eines Admin Node in einer Vertrauensstelle, einer Unternehmensanwendungen oder einer SP-Verbindung 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 zu bestellenden Partei, die Enterprise-Anwendung oder die SP-Verbindung mit dem neuen Zertifikat aktualisieren.

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich bei der Befehlsshell des Knotens anmelden und zum Verzeichnis wechseln `/var/local/mgmt-api`. Ein benutzerdefiniertes Serverzertifikat wird benannt `custom-server.crt`. Das Standardserverzertifikat des Knotens lautet `server.crt`.

Port-Anforderungen

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. Siehe ["Kontrolle des Zugriffs über externe Firewall"](#).

Bestätigen Sie, dass verbundene Benutzer sich anmelden können

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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben ["Bestimmte Zugriffsberechtigungen"](#).
- Sie haben bereits einen Identitätsverbund konfiguriert.

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 **Zugriffsverwaltung > Identitätsföderation**.
 - c. Bestätigen Sie, dass das Kontrollkästchen **Enable Identity Federation** nicht aktiviert ist.
 - d. Wenn dies der Fall ist, bestätigen Sie, dass keine föderierten Gruppen mehr für dieses Mandantenkonto benötigt werden, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.
2. Bestätigen Sie, dass ein verbundener Benutzer auf den Grid Manager zugreifen kann:
 - a. Wählen Sie im Grid Manager **Konfiguration > Zugriffskontrolle > Admingruppen**.
 - 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 bestehende Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root-Zugriffsberechtigung anmelden kann:
 - a. Wählen Sie im Grid Manager **Mandanten** aus.
 - b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen > Bearbeiten**.
 - c. Wählen Sie auf der Registerkarte Details eingeben die Option **Weiter**.
 - d. Wenn das Kontrollkästchen **eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern** aus.

Die Seite Mandant wird angezeigt.

- e. Wählen Sie das Mandantenkonto aus, wählen Sie **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
- f. Wählen Sie im Mandanten-Manager **Zugriffsverwaltung > Gruppen**.

- g. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus dem Grid Manager die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.
- h. Abmelden.
- i. Bestätigen Sie, dass Sie sich wieder bei dem Mandanten als Benutzer in der föderierten Gruppe anmelden können.

Verwandte Informationen

- ["Voraussetzungen und Überlegungen für Single Sign-On"](#)
- ["Managen von Admin-Gruppen"](#)
- ["Verwenden Sie ein Mandantenkonto"](#)

SSO konfigurieren

Sie können dem Assistenten „SSO konfigurieren“ folgen und in den Sandbox-Modus wechseln, um Single Sign-On (SSO) zu konfigurieren und zu testen, bevor Sie es für alle StorageGRID Benutzer aktivieren. Nachdem SSO aktiviert wurde, können Sie bei Bedarf in den Sandbox-Modus zurückkehren, um die Konfiguration zu ändern oder erneut zu testen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Root-Zugriffsberechtigung"](#).
- Sie haben eine Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für den Identitätsverbund **LDAP-Diensttyp** haben Sie je nach dem SSO-Identitätsanbieter, den Sie verwenden möchten, entweder Active Directory oder Entra ID ausgewählt.

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory Federation Service (AD FS)	<ul style="list-style-type: none"> • Active Directory • Entra-ID • PingFederate
Entra-ID	Entra-ID

Über diese Aufgabe

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an den SSO-Identitäts-Provider. Der SSO-Identitäts-Provider sendet wiederum eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Authentifizierungsanforderung erfolgreich war. Für erfolgreiche Anfragen:

- Die Antwort von Active Directory oder PingFederate enthält eine Universally Unique Identifier (UUID) für den Benutzer.
- Die Antwort von Entra ID enthält einen User Principal Name (UPN).

Damit StorageGRID (der Dienstanbieter) und der SSO-Identitätsanbieter sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, führen Sie die folgenden Aufgaben aus:

1. Konfigurieren Sie die Einstellungen in StorageGRID.
2. Verwenden Sie die Software des SSO-Identitätsanbieters, um für jeden Admin-Knoten eine Vertrauensstellung der vertrauenden Partei (AD FS), eine Unternehmensanwendung (Entra ID) oder einen Dienstanbieter (PingFederate) zu erstellen.
3. Kehren Sie zu StorageGRID zurück, um SSO zu aktivieren.

Der Sandbox-Modus erleichtert die Durchführung dieser Hin- und Her-Konfiguration und das Testen aller Ihrer Einstellungen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht per SSO anmelden.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Einmaliges Anmelden**. Die Seite „Single Sign-On“ wird angezeigt.



Wenn die Schaltfläche „SSO-Einstellungen konfigurieren“ deaktiviert ist, bestätigen Sie, dass Sie den Identitätsanbieter als Verbundidentitätsquelle konfiguriert haben. Weitere Informationen finden Sie unter ["Voraussetzungen und Überlegungen für Single Sign-On"](#).

2. Wählen Sie **SSO-Einstellungen konfigurieren**. Die Seite „Identitätsanbieterdetails angeben“ wird angezeigt.

Geben Sie die Details des Identitätsanbieters an

Schritte

1. Wählen Sie aus der Dropdown-Liste den **SSO-Typ** aus.
2. Wenn Sie Active Directory als SSO-Typ ausgewählt haben, geben Sie den **Verbunddienstnamen** für den Identitätsanbieter genau so ein, wie er im Active Directory Federation Service (AD FS) angezeigt wird.



Um den Namen des Föderationsdienstes 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.

3. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, 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 den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

- **Verwenden Sie keine TLS:** Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.



Wenn Sie das Zertifizierungsstellenzertifikat ändern, führen Sie sofort ["Starten Sie den Management-API-Service auf den Admin-Nodes neu"](#) eine erfolgreiche SSO-Prüfung im Grid Manager durch.

4. Wählen Sie **Weiter**. Die Seite „Relying Party Identifier angeben“ wird angezeigt.

Geben Sie die Kennung der vertrauenden Partei an

1. Füllen Sie die Felder auf der Seite „Identifikator der vertrauenden Seite angeben“ basierend auf dem von Ihnen ausgewählten SSO-Typ aus.

Active Directory

- a. Geben Sie die **Relying Party Identifier** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Vertrauensstellung der vertrauenden Seite in AD FS verwenden.
- Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder ``StorageGRID`` ein.
 - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Durch Einfügen dieser Zeichenfolge wird eine Tabelle erstellt, die die Kennung der vertrauenden Partei für jeden Admin-Knoten im Raster basierend auf dem Hostnamen des Knotens anzeigt.



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.

- b. Wählen Sie **Speichern und Sandbox-Modus aufrufen**.

Entra-ID

- a. Geben Sie im Abschnitt „Unternehmensanwendung“ den **Namen der Unternehmensanwendung** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Unternehmensanwendung in Entra ID verwenden.
- Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder ``StorageGRID`` ein.
 - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Durch Einfügen dieser Zeichenfolge wird eine Tabelle erstellt, die basierend auf dem Hostnamen des Knotens einen Unternehmensanwendungsnamen für jeden Admin-Knoten in Ihrem System anzeigt.



Sie müssen eine Enterprise-Anwendung für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Enterprise-Anwendung für jeden Admin-Node wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Node anmelden können.

- b. Befolgen Sie die Schritte in ["Erstellen Sie Unternehmensanwendungen in Entra ID"](#) um für jeden in der Tabelle aufgeführten Admin-Knoten eine Unternehmensanwendung zu erstellen.
- c. Kopieren Sie aus der Entra-ID die URL der Verbundmetadaten für jede Unternehmensanwendung. Fügen Sie diese URL dann in das entsprechende Feld **Federation metadata URL** in StorageGRID ein.
- d. Nachdem Sie eine Föderationsmetadaten-URL für alle Admin-Knoten kopiert und eingefügt haben, wählen Sie **Speichern und in den Sandbox-Modus wechseln**.

PingFederate

- a. Geben Sie im Abschnitt Dienstanbieter (SP) die **SP-Verbindungs-ID** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede SP-Verbindung in PingFederate verwenden.
- Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder ``StorageGRID`` ein.
 - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Durch Einfügen dieser

Zeichenfolge wird eine Tabelle erstellt, die die SP Verbindungs-ID für jeden Admin-Knoten in Ihrem System basierend auf dem Hostnamen des Knotens anzeigt.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System eine SP-Verbindung erstellen. Durch eine SP-Verbindung für jeden Admin-Node wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Node anmelden können.

- b. Geben Sie im Feld **Federation Metadaten-URL** die URL der Federation Metadaten für jeden Admin-Node an.

Verwenden Sie das folgende Format:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- c. Wählen Sie **Speichern und Sandbox-Modus aufrufen**.

Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen

Nachdem Sie die Konfiguration gespeichert und in den Sandbox-Modus gewechselt haben, können Sie die Konfiguration für den ausgewählten SSO-Typ abschließen und testen.

StorageGRID kann so lange wie nötig im Sandbox-Modus bleiben. Allerdings können sich nur Verbundbenutzer und lokale Benutzer anmelden.

Active Directory

Schritte

1. Wechseln Sie zu Active Directory Federation Services (AD FS).
2. Erstellen Sie eine oder mehrere Vertrauensstellungen der vertrauenden Seite für StorageGRID und verwenden Sie dabei die einzelnen Kennungen der vertrauenden Seite, die in der Tabelle auf der Seite „SSO konfigurieren“ angezeigt werden.

Sie müssen für jeden in der Tabelle aufgeführten Admin-Node ein Vertrauen erstellen.

Anweisungen hierzu finden Sie unter ["Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS"](#).

Entra-ID

Schritte

1. Wählen Sie auf der Seite Single Sign-On für den Admin-Node, bei dem Sie sich aktuell angemeldet haben, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster die folgenden Schritte:
 - a. Melden Sie sich beim Knoten an.
 - b. Wählen Sie **Konfiguration > Zugriffskontrolle > Einmaliges Anmelden**.
 - c. Laden Sie die SAML-Metadaten für diesen Node herunter, und speichern Sie sie.
3. Wechseln Sie zum Azure-Portal.
4. Befolgen Sie die Schritte in ["Erstellen Sie Unternehmensanwendungen in Entra ID"](#) um die SAML-Metadatendatei für jeden Admin-Knoten in die entsprechende Entra ID-Unternehmensanwendung hochzuladen.

PingFederate

Schritte

1. Wählen Sie auf der Seite Single Sign-On für den Admin-Node, bei dem Sie sich aktuell angemeldet haben, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster die folgenden Schritte:
 - a. Melden Sie sich beim Knoten an.
 - b. Wählen Sie **Konfiguration > Zugriffskontrolle > Einmaliges Anmelden**.
 - c. Laden Sie die SAML-Metadaten für diesen Node herunter, und speichern Sie sie.
3. Fahren Sie zur PingFederate.
4. ["Erstellen Sie eine oder mehrere SP-Verbindungen \(Service-Provider\) für StorageGRID"](#) . Verwenden Sie die SP Verbindungs-ID für jeden Admin-Knoten (angezeigt in der Tabelle auf der Seite „SSO konfigurieren“) und die SAML-Metadaten, die Sie für diesen Admin-Knoten heruntergeladen haben.

Für jeden in der Tabelle aufgeführten Admin-Node müssen Sie eine SP-Verbindung erstellen.

Testkonfiguration

Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID System erzwingen, bestätigen Sie, dass Single Sign-On und Single Logout für jeden Admin-Knoten richtig konfiguriert sind.

Active Directory

Schritte

1. Suchen Sie auf der Seite „SSO konfigurieren“ den Link zum Schritt „Konfiguration testen“ des Assistenten.

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

2. Wählen Sie den Link aus, oder kopieren Sie die URL in einen Browser, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
3. Um zu bestätigen, dass Sie SSO zur Anmeldung bei StorageGRID verwenden können, wählen Sie **Anmelden bei einer der folgenden Sites**, wählen Sie die vertrauenswürdigen Partei-ID für Ihren primären Admin-Knoten und wählen Sie **Anmelden**.
4. Geben Sie Ihren föderierten Benutzernamen und Ihr Kennwort ein.
 - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.
 - 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.
5. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

Entra-ID

Schritte

1. Wechseln Sie im Azure-Portal zur Seite Single Sign On.
2. Wählen Sie **Diese Anwendung testen**.
3. Geben Sie die Anmeldeinformationen eines föderierten Benutzers ein.
 - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.
 - 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.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

PingFederate

Schritte

1. Wählen Sie auf der Seite „SSO konfigurieren“ den ersten Link in der Sandbox-Modus-Nachricht aus.

Wählen Sie jeweils einen Link aus, und testen Sie ihn.
2. Geben Sie die Anmeldeinformationen eines föderierten Benutzers ein.
 - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.
 - 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.
3. Wählen Sie den nächsten Link aus, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

Wenn eine Nachricht mit abgelaufener Seite angezeigt wird, wählen Sie in Ihrem Browser die Schaltfläche **Zurück** aus, und senden Sie Ihre Anmeldedaten erneut.

Aktivieren Sie Single Sign On

Wenn Sie bestätigt haben, dass Sie sich mit SSO bei jedem Admin-Node anmelden können, können Sie SSO für Ihr gesamtes StorageGRID System aktivieren.



Wenn SSO aktiviert ist, müssen alle Benutzer 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.

Schritte

1. Wählen Sie im Schritt „Testkonfiguration“ des SSO-Konfigurationsassistenten die Option „SSO aktivieren“ aus.
2. Überprüfen Sie die Warnmeldung und wählen Sie **SSO aktivieren**.

Single Sign-On ist jetzt aktiviert. Die Seite „Single Sign-On“ wird angezeigt und enthält jetzt die Details für das gerade konfigurierte SSO.

3. Um die Konfiguration zu bearbeiten, wählen Sie **Bearbeiten**.
4. Um die einmalige Anmeldung zu deaktivieren, wählen Sie **SSO deaktivieren**.



Wenn Sie das Azure-Portal verwenden und von demselben Computer aus auf StorageGRID zugreifen, den Sie für den Zugriff auf Entra ID verwenden, stellen Sie sicher, dass der Azure-Portalbenutzer auch ein autorisierter StorageGRID Benutzer ist (ein Benutzer in einer Verbundgruppe, der in StorageGRID importiert wurde, oder melden Sie sich vom Azure-Portal ab, bevor Sie versuchen, sich bei StorageGRID anzumelden).

Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien 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.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ **AD FS** ausgewählt.
- Du hast "[Sandbox-Modus aufgerufen](#)" im Grid Manager.
- Sie kennen den vollqualifizierten Domännennamen (oder die IP-Adresse) und die Kennung der vertrauenden Partei für jeden Admin-Knoten in Ihrem System. Sie finden diese Werte in der Detailtabelle „Admin-Knoten“ auf der StorageGRID -Seite „SSO konfigurieren“.



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.
- Wenn Sie das Vertrauen der Vertrauensstelle manuell erstellen, haben Sie das benutzerdefinierte Zertifikat, das für die StorageGRID-Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich von der Eingabeaufforderung-Shell bei einem Admin-Knoten anmelden.

Über diese Aufgabe

Diese Anweisungen gelten für Windows Server 2016 AD FS. Wenn Sie eine andere Version von AD FS verwenden, werden Sie kleine Unterschiede im Verfahren bemerken. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Erstellen Sie mit Windows PowerShell ein Vertrauensverhältnis, das sich auf die Kunden stützt

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

Schritte

1. Wählen Sie im Windows-Startmenü mit der rechten Maustaste das PowerShell-Symbol aus 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"
```

- Geben Sie für *Admin_Node_Identifier* die ID der aussetzenden Partei für den Admin-Knoten genau so ein, wie sie auf der Seite Single Sign-On angezeigt wird. `SG-DC1-ADM1` Beispiel: .
- Geben Sie für *Admin_Node_FQDN* den vollständig qualifizierten Domännennamen 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. Wählen Sie **Anwenden**, und wählen Sie **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. Wählen Sie **Regel hinzufügen**.
- d. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
- e. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

- f. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
 - g. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
 - h. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
 - i. Wählen Sie **Fertig**, und wählen Sie **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, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie 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 zurück und "[Testen Sie alle Vertrauensstellungen der vertrauenden Parteien](#)" um zu bestätigen, dass sie richtig konfiguriert sind.

Erstellen Sie durch den Import von Federationmetadaten ein Vertrauen von Kunden

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

Schritte

- 1. Wählen Sie im Windows Server Manager **Tools** aus, und wählen Sie dann **AD FS Management** aus.
- 2. Wählen Sie unter Aktionen **Vertrauensstellung hinzufügen** aus.
- 3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus, und wählen Sie **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`

Geben Sie für *Admin_Node_FQDN* den vollständig qualifizierten Domännennamen 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 zu

vertrauenden Partei und schließen Sie den Assistenten.



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

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. Wählen Sie **Regel hinzufügen**:
- c. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
- d. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

- e. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
- f. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
- g. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
- h. Wählen Sie **Fertig**, und wählen Sie **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, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie 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 zurück und "[Testen Sie alle Vertrauensstellungen der vertrauenden Parteien](#)" um zu bestätigen, dass sie richtig konfiguriert sind.

Erstellen Sie manuell ein Vertrauen der Vertrauensbasis

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

Schritte

1. Wählen Sie im Windows Server Manager **Tools** aus, und wählen Sie dann **AD FS Management** aus.
2. Wählen Sie unter Aktionen **Vertrauensstellung hinzufügen** aus.
3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus, und wählen Sie **Start**.
4. Wählen Sie **Geben Sie Daten über den Besteller manuell** ein, und wählen Sie **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. `SG-DC1-ADM1` Beispiel: .

- 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`

Geben Sie für *Admin_Node_FQDN* den vollständig qualifizierten Domännennamen 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

Geben Sie für *Admin_Node_Identifier* die ID der aussetzenden Partei für den Admin-Knoten genau so ein, wie sie auf der Seite Single Sign-On angezeigt wird. `SG-DC1-ADM1` Beispiel: .

- 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, wählen Sie **Regel hinzufügen**:

- a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
- b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

- c. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
- d. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
- e. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
- f. Wählen Sie **Fertig**, und wählen Sie **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. Wählen Sie **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
```

Geben Sie für *Admin_Node_FQDN* 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. Wählen Sie **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 in das `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie die Zertifikatdatei hinzu `custom-server.crt`.



Die Verwendung des Standardzertifikats des Admin-Knotens (`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. Wählen Sie **Anwenden**, und wählen Sie **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 zurück und "[Testen Sie alle Vertrauensstellungen der vertrauenden Parteien](#)" um zu bestätigen, dass sie richtig konfiguriert sind.

Erstellen Sie Unternehmensanwendungen in Entra ID

Sie verwenden die Entra-ID, um für jeden Admin-Knoten in Ihrem System eine Unternehmensanwendung zu erstellen.

Bevor Sie beginnen

- Sie haben mit der Konfiguration der einmaligen Anmeldung für StorageGRID begonnen und **Entra ID** als SSO-Typ ausgewählt.
- Du hast "[Sandbox-Modus aufgerufen](#)" im Grid Manager.
- Sie haben den **Namen der Unternehmensanwendung** für jeden Admin-Knoten in Ihrem System. Sie können diese Werte aus der Detailtabelle des Admin-Knotens auf der Seite „SSO konfigurieren“ kopieren.



Sie müssen eine Enterprise-Anwendung für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Enterprise-Anwendung für jeden Admin-Node wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Node anmelden können.

- Sie haben Erfahrung mit der Erstellung von Unternehmensanwendungen in Entra ID.
- Sie haben ein Entra-ID-Konto mit einem aktiven Abonnement.
- Sie haben eine der folgenden Rollen im Entra ID-Konto: Globaler Administrator, Cloud-Anwendungsadministrator, Anwendungsadministrator oder Besitzer des Dienstprinzipals.

Zugang zur Entra-ID

Schritte

1. Melden Sie sich beim an ["Azure-Portal"](#).
2. Navigieren Sie zu ["Entra-ID"](#).
3. Wählen Sie ["Enterprise-Applikationen"](#).

Erstellen von Enterprise-Applikationen und Speichern von StorageGRID SSO-Konfiguration

Um die SSO-Konfiguration für Entra ID in StorageGRID zu speichern, müssen Sie Entra ID verwenden, um für jeden Admin-Knoten eine Unternehmensanwendung zu erstellen. Sie kopieren die URLs der Föderationsmetadaten von Entra ID und fügen sie in die entsprechenden Felder **Föderationsmetadaten-URL** auf der Seite „SSO konfigurieren“ ein.

Schritte

1. Wiederholen Sie die folgenden Schritte für jeden Admin-Node.
 - a. Wählen Sie im Bereich „Entra ID Enterprise-Anwendungen“ **Neue Anwendung** aus.
 - b. Wählen Sie **Erstellen Sie Ihre eigene Anwendung**.
 - c. Geben Sie als Namen den **Namen der Unternehmensanwendung** ein, den Sie aus der Tabelle mit den Admin-Knotendetails auf der Seite „SSO konfigurieren“ kopiert haben.
 - d. Lassen Sie das * eine andere Anwendung integrieren, die Sie nicht in der Galerie finden (nicht-Galerie)* Optionsfeld ausgewählt.
 - e. Wählen Sie **Erstellen**.
 - f. Wählen Sie im **2 den Link *Get Started** aus. Aktivieren Sie das Feld Single Sign On*, oder wählen Sie den Link **Single Sign-On** im linken Rand.
 - g. Wählen Sie das Feld **SAML** aus.
 - h. Kopieren Sie die **App Federation Metadaten-URL**, die Sie unter **Step 3 SAML-Signierungszertifikat** finden können.
 - i. Gehen Sie zur Seite „SSO konfigurieren“ und fügen Sie die URL in das Feld „URL der Verbundmetadaten“ ein, die dem von Ihnen verwendeten „Namen der Unternehmensanwendung“ entspricht.
2. Nachdem Sie für jeden Admin-Knoten eine URL mit Verbundmetadaten eingefügt und alle anderen erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, wählen Sie auf der Seite „SSO konfigurieren“ **Speichern** aus.

Laden Sie für jeden Admin-Node SAML-Metadaten herunter

Nachdem die SSO-Konfiguration gespeichert ist, können Sie für jeden Admin-Node in Ihrem StorageGRID-System eine SAML-Metadatendatei herunterladen.

Schritte

1. Wiederholen Sie diese Schritte für jeden Admin-Node.
 - a. Melden Sie sich über den Admin-Node bei StorageGRID an.
 - b. Wählen Sie **Konfiguration > Zugriffskontrolle > Einmaliges Anmelden**.
 - c. Wählen Sie die Schaltfläche, um die SAML-Metadaten für diesen Admin-Node herunterzuladen.
 - d. Speichern Sie die Datei, die Sie in Entra ID hochladen.

Hochladen von SAML-Metadaten in jede Enterprise-Applikation

Nachdem Sie für jeden StorageGRID Admin-Knoten eine SAML-Metadatendatei heruntergeladen haben, führen Sie in Entra ID die folgenden Schritte aus:

Schritte

1. Zurück zum Azure-Portal.
2. Wiederholen Sie diese Schritte für jede Enterprise-Applikation:



Möglicherweise müssen Sie die Seite Enterprise-Applikationen aktualisieren, um Anwendungen anzuzeigen, die Sie zuvor in der Liste hinzugefügt haben.

- a. Gehen Sie zur Seite Eigenschaften für die Enterprise-Anwendung.
 - b. Legen Sie **Zuweisung erforderlich** auf **Nein** fest (es sei denn, Sie möchten Aufgaben separat konfigurieren).
 - c. Rufen Sie die Seite Single Sign-On auf.
 - d. Schließen Sie die SAML-Konfiguration ab.
 - e. Wählen Sie die Schaltfläche **Metadatendatei hochladen** aus, und wählen Sie die SAML-Metadatendatei aus, die Sie für den entsprechenden Admin-Node heruntergeladen haben.
 - f. Nachdem die Datei geladen wurde, wählen Sie **Speichern** und dann **X** aus, um das Fenster zu schließen. Sie gelangen zurück zur Seite Single Sign-On mit SAML einrichten.
3. ["Testen Sie jede Anwendung"](#) .

Erstellen von SP-Verbindungen (Service Provider) in PingFederate

Sie verwenden PingFederate, um für jeden Admin-Node in Ihrem System eine SP-Verbindung (Service Provider) zu erstellen. Um den Prozess zu beschleunigen, importieren Sie die SAML-Metadaten aus StorageGRID.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ * Ping föderate* ausgewählt.
- Du hast ["Sandbox-Modus aufgerufen"](#) im Grid Manager.
- Sie haben die * SP Verbindungs-ID* für jeden Admin-Knoten in Ihrem System. Sie finden diese Werte in der Detailtabelle „Admin-Knoten“ auf der Seite „SSO konfigurieren“.

- Sie haben die **SAML-Metadaten** für jeden Admin-Knoten in Ihrem System heruntergeladen.
- Sie haben Erfahrung beim Erstellen von SP-Verbindungen in PingFederate Server.
- Sie haben den "[Administrator's Reference Guide](#)" für PingFederate Server. Die PingFederate-Dokumentation bietet detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben die "[Administratorberechtigung](#)" für PingFederate Server.

Über diese Aufgabe

Mit diesen Anweisungen wird zusammengefasst, wie PingFederate Server Version 10.3 als SSO-Anbieter für StorageGRID konfiguriert wird. Wenn Sie eine andere Version von PingFederate verwenden, müssen Sie diese Anweisungen möglicherweise anpassen. Detaillierte Anweisungen für Ihre Version finden Sie in der Dokumentation zu PingFederate Server.

Alle Voraussetzungen in PingFederate

Bevor Sie die SP-Verbindungen erstellen können, die Sie für StorageGRID verwenden, müssen Sie die erforderlichen Aufgaben in PingFederate ausführen. Beim Konfigurieren der SP-Verbindungen verwenden Sie Informationen aus diesen Voraussetzungen.

Datenspeicher erstellen

Falls noch nicht, erstellen Sie einen Datenspeicher, um PingFederate mit dem AD FS LDAP-Server zu verbinden. Verwenden Sie die Werte, die Sie in StorageGRID verwendet "[Identitätsföderation wird konfiguriert](#)" haben.

- **Typ:** Verzeichnis (LDAP)
- **LDAP-Typ:** Active Directory
- **Binärattribut Name:** Geben Sie **objectGUID** auf der Registerkarte LDAP Binärattribute genau wie dargestellt ein.

Passwortvalididator[[Password-Validator] erstellen

Wenn Sie noch nicht vorhanden sind, erstellen Sie einen Validierer für Kennwortausweise.

- **Typ:** LDAP Benutzername Passwort Zugangsdaten Validierer
- **Datenspeicher:** Wählen Sie den von Ihnen erstellten Datenspeicher aus.
- **Search base:** Geben Sie Informationen aus LDAP ein (z. B. DC=saml,DC=sgws).
- **Suchfilter:** SAMAccountName=€{username}
- **Umfang:** Unterbaum

IdP-Adapterinstanz erstellen

Wenn Sie noch nicht, erstellen Sie eine IdP-Adapterinstanz.

Schritte

1. Gehen Sie zu **Authentifizierung > Integration > IdP-Adapter**.
2. Wählen Sie **Neue Instanz Erstellen**.
3. Wählen Sie auf der Registerkarte Typ die Option **HTML-Formular-IdP-Adapter** aus.
4. Wählen Sie auf der Registerkarte IdP-Adapter **Neue Zeile zu 'Credential Validators'** hinzufügen.

5. Wählen Sie die [Gültigkeitsprüfung für Kennwortausweise](#) Sie erstellt haben.
6. Wählen Sie auf der Registerkarte Adapterattribute das Attribut **Benutzername** für **Pseudonym** aus.
7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

Wenn Sie noch nicht, erstellen oder importieren Sie das Signierungszertifikat.

Schritte

1. Gehen Sie zu **Sicherheit > Signieren & Entschlüsseln Schlüssel & Zertifikate**.
2. Erstellen oder importieren Sie das Signieren-Zertifikat.

Erstellen Sie eine SP-Verbindung in PingFederate

Wenn Sie eine SP-Verbindung in PingFederate erstellen, importieren Sie die SAML-Metadaten, die Sie für den Admin-Node von StorageGRID heruntergeladen haben. Die Metadatendatei enthält viele der spezifischen Werte, die Sie benötigen.



Sie müssen für jeden Admin-Node in Ihrem StorageGRID-System eine SP-Verbindung erstellen, damit sich Benutzer sicher bei und aus einem beliebigen Node anmelden können. Erstellen Sie anhand dieser Anweisungen die erste SP-Verbindung. Gehen Sie dann zu, um zusätzliche Verbindungen zu [Erstellen Sie zusätzliche SP-Verbindungen](#) erstellen, die Sie benötigen.

Wählen Sie den SP-Verbindungstyp

Schritte

1. Gehen Sie zu **Anwendungen > Integration > SP-Verbindungen**.
2. Wählen Sie **Verbindung Erstellen**.
3. Wählen Sie **Verwenden Sie keine Vorlage für diese Verbindung**.
4. Wählen Sie als Protokoll **Browser SSO Profile** und **SAML 2.0** aus.

Importieren der SP-Metadaten

Schritte

1. Wählen Sie auf der Registerkarte Metadaten importieren die Option **Datei**.
2. Wählen Sie die SAML-Metadatendatei aus, die Sie von der Seite „SSO konfigurieren“ für den Admin-Knoten heruntergeladen haben.
3. Überprüfen Sie die Metadatenübersicht und die Informationen auf der Registerkarte Allgemeine Informationen.

Die Entity-ID des Partners und der Verbindungsname werden auf die Verbindungs-ID des StorageGRID-SP festgelegt. (Z. B. 10.96.105.200-DC1-ADM1-105-200). Die Basis-URL ist die IP des StorageGRID-Admin-Knotens.

4. Wählen Sie **Weiter**.

Konfigurieren Sie SSO für den IdP-Browser

Schritte

1. Wählen Sie auf der Registerkarte Browser-SSO * die Option * Browser-SSO konfigurieren* aus.
2. Wählen Sie auf der Registerkarte SAML-Profil die Optionen **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** und **IdP-initiated SLO** aus.
3. Wählen Sie **Weiter**.
4. Nehmen Sie auf der Registerkarte Assertion Lifetime keine Änderungen vor.
5. Wählen Sie auf der Registerkarte Assertion Creation die Option **Assertion Creation konfigurieren** aus.
 - a. Wählen Sie auf der Registerkarte Identitätszuordnung die Option **Standard**.
 - b. Verwenden Sie auf der Registerkarte „Attributvertrag“ die Registerkarte **SAML_SUBJECT** als Attributvertrag und das undefinierte Namensformat, das importiert wurde.
6. Wählen Sie unter Vertrag verlängern die Option **Löschen**, um das nicht verwendete , zu entfernen
urn:oid.

Adapterinstanz zuordnen

Schritte

1. Wählen Sie auf der Registerkarte Authentication Source Mapping die Option **Map New Adapter Instance**.
2. Wählen Sie auf der Registerkarte Adapterinstanz die erstellte aus [Adapterinstanz](#).
3. Wählen Sie auf der Registerkarte Zuordnungsmethode die Option **Weitere Attribute aus einem Datenspeicher abrufen** aus.
4. Wählen Sie auf der Registerkarte Attributquelle und Benutzersuche die Option **Attributquelle hinzufügen** aus.
5. Geben Sie auf der Registerkarte Datenspeicher eine Beschreibung ein, und wählen Sie die hinzugefügte aus [Datastore](#).
6. Auf der Registerkarte LDAP-Verzeichnissuche:
 - Geben Sie den **Basis-DN** ein, der exakt mit dem Wert übereinstimmt, den Sie in StorageGRID für den LDAP-Server eingegeben haben.
 - Wählen Sie für den Suchumfang die Option **Subtree** aus.
 - Suchen und fügen Sie für die Root-Objektklasse eines der folgenden Attribute hinzu: **ObjectGUID** oder **userPrincipalName**.
7. Wählen Sie auf der Registerkarte LDAP Binary Attribute Encoding Types **Base64** für das Attribut **objectGUID** aus.
8. Geben Sie auf der Registerkarte LDAP-Filter **sAMAccountName={username}** ein.
9. Wählen Sie auf der Registerkarte Contract Fulfillment die Option **LDAP (Attribut)** aus der Dropdown-Liste Source aus und wählen Sie entweder **objectGUID** oder **userPrincipalName** aus der Dropdown-Liste Value aus.
10. Überprüfen und speichern Sie dann die Attributquelle.
11. Wählen Sie auf der Registerkarte Attributquelle failsave die Option **SSO-Transaktion abbrechen** aus.
12. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**.
13. Wählen Sie * Fertig*.

Konfigurieren von Protokolleinstellungen

Schritte

1. Wählen Sie auf der Registerkarte **SP-Verbindung** > **Browser SSO** > **Protokolleinstellungen** die Option **Protokolleinstellungen konfigurieren** aus.
2. Akzeptieren Sie auf der Registerkarte Assertion Consumer Service URL die Standardwerte, die aus den StorageGRID SAML-Metadaten (**POST** für Bindung und für Endpunkt-URL) importiert wurden `/api/saml-response`.
3. Akzeptieren Sie auf der Registerkarte SLO Service URLs die Standardwerte, die aus den StorageGRID SAML-Metadaten (**REDIRECT** für Bindung und für Endpunkt-URL importiert wurden `/api/saml-logout`.
4. Deaktivieren Sie auf der Registerkarte Allowable SAML Bindings **ARTIFACT** und **SOAP**. Es sind nur **POST** und **REDIRECT** erforderlich.
5. Lassen Sie auf der Registerkarte Signature Policy die Kontrollkästchen **require AUTHN Requests to be signed** und **always Sign Assertion** ausgewählt.
6. Wählen Sie auf der Registerkarte Verschlüsselungsrichtlinie die Option **Keine** aus.
7. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**, um die Protokolleinstellungen zu speichern.
8. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**, um die SSO-Einstellungen des Browsers zu speichern.

Anmeldedaten konfigurieren

Schritte

1. Wählen Sie auf der Registerkarte SP-Verbindung die Option **Anmeldeinformationen** aus.
2. Wählen Sie auf der Registerkarte Anmeldeinformationen die Option **Anmeldeinformationen konfigurieren**.
3. Wählen Sie die [Signieren des Zertifikats](#) Sie haben erstellt oder importiert.
4. Wählen Sie **Weiter** aus, um zu **Einstellungen zur Signature-Verifizierung verwalten** zu gelangen.
 - a. Wählen Sie auf der Registerkarte Vertrauensmodell die Option **nicht verankert** aus.
 - b. Überprüfen Sie auf der Registerkarte Signaturverifizierungszertifikat die Signature Certificate-Informationen, die aus den StorageGRID SAML-Metadaten importiert wurden.
5. Prüfen Sie die Übersichtsbildschirme und wählen Sie **Speichern**, um die SP-Verbindung zu speichern.

Erstellen Sie zusätzliche SP-Verbindungen

Sie können die erste SP-Verbindung kopieren, um die für jeden Admin-Node in Ihrem Raster erforderlichen SP-Verbindungen zu erstellen. Sie laden für jede Kopie neue Metadaten hoch.



Die SP-Verbindungen für verschiedene Admin-Nodes verwenden identische Einstellungen, mit Ausnahme der Entity-ID des Partners, der Basis-URL, der Verbindungs-ID, des Verbindungsnamens, der Signaturverifizierung, Und SLO Response-URL.

Schritte

1. Wählen Sie **Aktion** > **Kopieren** aus, um für jeden zusätzlichen Admin-Node eine Kopie der anfänglichen SP-Verbindung zu erstellen.
2. Geben Sie die Verbindungs-ID und den Verbindungsnamen für die Kopie ein, und wählen Sie **Speichern**.
3. Wählen Sie die dem Admin-Node entsprechende Metadatendatei:
 - a. Wählen Sie **Aktion** > **Aktualisieren mit Metadaten**.
 - b. Wählen Sie **Datei auswählen** und laden Sie die Metadaten hoch.

- c. Wählen Sie **Weiter**.
 - d. Wählen Sie **Speichern**.
4. Beheben Sie den Fehler aufgrund des nicht verwendeten Attributs:
- a. Wählen Sie die neue Verbindung aus.
 - b. Wählen Sie **Browser-SSO konfigurieren > Assertion-Erstellung konfigurieren > Attributvertrag** aus.
 - c. Löschen Sie den Eintrag für **Urne:oid**.
 - d. Wählen Sie **Speichern**.

SSO deaktivieren

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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Einmaliges Anmelden**.

Die Seite Single Sign-On wird angezeigt.

2. Wählen Sie **SSO deaktivieren**.
3. Wählen Sie **Ja**.

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

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.

SSO für einen Admin-Knoten vorübergehend deaktivieren und wieder aktivieren

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.

Bevor Sie beginnen

- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".
- Sie haben die `Passwords.txt` Datei.
- Sie kennen das Passwort für den lokalen Root-Benutzer.

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 werden beibehalten, sofern Sie sie nicht aktualisieren.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:

- Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
- Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
- Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
- Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von \$ zu #.

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:

- Wählen Sie **Konfiguration > Zugriffskontrolle > Einmaliges Anmelden**.
- Ändern Sie die falschen oder veralteten SSO-Einstellungen.
- Wählen Sie **Speichern**.

Wenn Sie auf der Seite Single Sign-On **Save** wählen, 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:

- Führen Sie alle Aufgaben oder Aufgaben aus, die Sie ausführen müssen.
- Wählen Sie **Abmelden**, und schließen Sie den Grid Manager.
- 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.

- Grid-Node neu booten: `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.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.