



Kontrollieren Sie den Zugriff auf StorageGRID

StorageGRID software

NetApp
October 21, 2025

Inhalt

Kontrollieren Sie den Zugriff auf StorageGRID	1
Steuern Sie den StorageGRID Zugriff	1
Kontrollieren Sie den Zugriff auf den Grid Manager	1
Aktivieren der einmaligen Anmeldung	1
Bereitstellungspassphrase ändern	1
Ändern der Knotenkonsolenkennwörter	2
Ändern der Bereitstellungspassphrase	2
Ändern der Knotenkonsolenkennwörter	3
Zugriff auf den Assistenten	3
Geben Sie die Bereitstellungspassphrase ein	3
Laden Sie das aktuelle Wiederherstellungspaket herunter	3
Ändern der Knotenkonsolenkennwörter	4
SSH-Zugriffskennwörter für Admin-Knoten ändern	5
Zugriff auf den Assistenten	5
Laden Sie das aktuelle Wiederherstellungspaket herunter	5
SSH-Zugriffsschlüssel ändern	6
Verwenden der Identitätsföderation	7
Konfigurieren der Identitätsföderation für Grid Manager	7
Erzwingen der Synchronisierung mit der Identitätsquelle	11
Identitätsföderation deaktivieren	11
Richtlinien zum Konfigurieren eines OpenLDAP-Servers	12
Verwalten von Administratorgruppen	12
Erstellen einer Administratorgruppe	13
Anzeigen und Bearbeiten von Administratorgruppen	14
Duplizieren einer Gruppe	15
Löschen einer Gruppe	15
Berechtigungen der Administratorgruppe	15
Interaktion zwischen Berechtigungen und Zugriffsmodus	16
Root-Zugriff	16
Ändern des Root-Passworts des Mandanten	16
Konfiguration der Grid-Topologieseite	16
ILM	16
Wartung	17
Verwalten von Warnungen	18
Metrikabfrage	18
Objektmetadatenuche	18
Andere Netzkonfiguration	18
Speichergeräteadministrator	18
Mandantenkonten	18
Benutzer verwalten	19
Erstellen eines lokalen Benutzers	19
Anzeigen und Bearbeiten lokaler Benutzer	20
Duplizieren eines Benutzers	21

Löschen eines Benutzers	22
Verwenden Sie Single Sign-On (SSO).	22
Konfigurieren der einmaligen Anmeldung	22
Anforderungen und Überlegungen zur einmaligen Anmeldung	25
Bestätigen, dass sich Verbundbenutzer anmelden können	27
Sandbox-Modus verwenden	28
Erstellen von Vertrauensstellungen der vertrauenden Seite in AD FS	38
Erstellen von Unternehmensanwendungen in Azure AD	43
Erstellen Sie Service Provider (SP)-Verbindungen in PingFederate	45
Deaktivieren der einmaligen Anmeldung	50
Deaktivieren und aktivieren Sie Single Sign-On für einen Admin-Knoten vorübergehend.	50

Kontrollieren Sie den Zugriff auf StorageGRID

Steuern Sie 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.

Kontrollieren Sie den Zugriff auf den Grid Manager

Sie legen fest, wer auf den Grid Manager und die Grid Management API zugreifen kann, indem Sie Gruppen und Benutzer aus einem Identitätsföderationsdienst importieren oder lokale Gruppen und lokale Benutzer einrichten.

Verwenden "[Identitätsföderation](#)" macht das Einrichten "[Gruppen](#)" Und "[Benutzer](#)" schneller und ermöglicht Benutzern die Anmeldung bei StorageGRID mit vertrauten Anmeldeinformationen. 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 bestimmen, welche Aufgaben jeder Benutzer ausführen kann, indem Sie ihm unterschiedliche "[Berechtigungen](#)" zu jeder Gruppe. Beispielsweise möchten Sie möglicherweise, dass Benutzer einer Gruppe ILM-Regeln verwalten können und Benutzer einer anderen Gruppe Wartungsaufgaben ausführen können. Ein Benutzer muss mindestens einer Gruppe angehören, um auf das System zugreifen zu können.

Optional können Sie eine Gruppe so konfigurieren, dass sie schreibgeschützt ist. Benutzer in einer schreibgeschützten Gruppe können Einstellungen und Funktionen nur anzeigen. Sie können im Grid Manager oder in der Grid Management API keine Änderungen vornehmen oder Vorgänge ausführen.

Aktivieren der einmaligen Anmeldung

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 von 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.

Bereitstellungspassphrase 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 Knotenkonsolenkennwörter

Jeder Knoten in Ihrem Grid verfügt über ein eindeutiges 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 Kennwort der Knotenkonsole"](#) für jeden Knoten.

Ändern der Bereitstellungspassphrase

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 Recovery Package-Backups erforderlich, die Informationen zur Grid-Topologie, Passwörter für die Grid-Knotenkonsole und Verschlüsselungsschlüssel für das StorageGRID System enthalten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie verfügen über die aktuelle Bereitstellungspassphrase.

Informationen zu diesem Vorgang

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 **Bereitstellungspassphrase ändern** die Option **Änderung vornehmen** aus.
3. Geben Sie Ihre aktuelle Bereitstellungspassphrase ein.
4. Geben Sie die neue Passphrase ein. Die Passphrase muss mindestens 8 und darf nicht mehr als 32 Zeichen enthalten. Bei Passphrasen wird zwischen Groß- und Kleinschreibung unterschieden.
5. Bewahren Sie die neue Bereitstellungspassphrase an einem sicheren Ort auf. Es wird für Installations-, Erweiterungs- und Wartungsverfahren benötigt.
6. Geben Sie die neue Passphrase erneut ein und wählen Sie **Speichern**.

Das System zeigt ein grünes Erfolgsbanner an, wenn die Änderung der Bereitstellungspassphrase abgeschlossen ist.



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

7. Wählen Sie **Wiederherstellungspaket**.
8. 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 Knotenkonsolenkennwörter

Jeder Knoten in Ihrem Grid verfügt über ein eindeutiges Knotenkonsolenkennwort, das Sie zum Anmelden am Knoten benötigen. Verwenden Sie diese Schritte, um jedes eindeutige Knotenkonsolenkennwort für jeden Knoten in Ihrem Raster zu ändern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Sie haben die ["Wartungs- oder Root-Zugriffsberechtigung"](#) .
- Sie verfügen über die aktuelle Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Verwenden Sie das Kennwort der Knotenkonsole, um sich per SSH als „Administrator“ bei einem Knoten oder als Root-Benutzer bei einer VM-/physischen Konsolenverbindung anzumelden. Der Prozess zum Ändern des Knotenkonsolenkennworts erstellt neue Kennwörter für jeden Knoten in Ihrem Raster und speichert die Kennwörter in einer aktualisierten `passwords.txt` Datei im Wiederherstellungspaket. Die Passwörter sind in der Spalte „Passwort“ in der Datei „passwords.txt“ aufgeführt.



Für die SSH-Schlüssel, die für die Kommunikation zwischen Knoten verwendet werden, gibt es separate SSH-Zugriffskennwörter. Die SSH-Zugangspasswörter werden durch dieses Verfahren nicht geändert.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Grid-Passwörter**.
2. Wählen Sie unter **Passwörter der Knotenkonsole ändern** die Option **Änderung vornehmen** aus.

Geben Sie die Bereitstellungspassphrase ein

Schritte

1. Geben Sie die Bereitstellungspassphrase für Ihr Grid ein.
2. Wählen Sie **Weiter**.

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. Wählen Sie **Wiederherstellungspaket herunterladen**.
2. Kopieren Sie die Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.



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

3. Wählen Sie **Weiter**.
4. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**, wenn Sie bereit sind, mit der Änderung der Knotenkonsolenkennwörter zu beginnen.

Sie können diesen Vorgang nach dem Start nicht mehr abbrechen.

Ändern der Knotenkonsolenkennwörter

Wenn der Kennwortprozess der Knotenkonsole startet, wird ein neues Wiederherstellungspaket generiert, das die neuen Kennwörter enthält. Anschließend werden die Passwörter auf jedem Knoten aktualisiert.

Schritte

1. Warten Sie, bis das neue Wiederherstellungspaket generiert wurde. Dies kann einige Minuten dauern.
2. Wählen Sie **Neues Wiederherstellungspaket herunterladen**.
3. Wenn der Download abgeschlossen ist:
 - a. Öffnen Sie die `.zip` Datei.
 - b. Bestätigen Sie, dass Sie auf die Inhalte zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen Passwörter für die Knotenkonsole enthält.
 - c. Kopieren Sie die neue Wiederherstellungspaketdatei (`.zip`) an zwei sichere und getrennte Orte.



Überschreiben Sie nicht das alte Wiederherstellungspaket.

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

4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie das neue Wiederherstellungspaket heruntergeladen und den Inhalt überprüft haben.
5. Wählen Sie **Passwörter der Knotenkonsole ändern** und warten Sie, bis alle Knoten mit den neuen Passwörtern aktualisiert wurden. Dies kann einige Minuten dauern.

Wenn die Passwörter für alle Knoten geändert werden, wird ein grünes Erfolgsbanner angezeigt. Fahren Sie mit dem nächsten Schritt fort.

Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in einer Bannermeldung die Anzahl der Knoten aufgelistet, 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.

Wenn die Kennwortaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

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



Durch einen erneuten Versuch werden nur die Knotenkonsolenkennwörter auf den Knoten geändert, bei denen bei vorherigen Kennwortänderungsversuchen ein Fehler aufgetreten ist.

6. Nachdem die Passwörter der Knotenkonsole für alle Knoten geändert wurden, löschen Sie die [erstes Wiederherstellungspaket, das Sie heruntergeladen haben](#).
7. Verwenden Sie optional den Link **Wiederherstellungspaket**, um eine zusätzliche Kopie des neuen Wiederherstellungspakets herunterzuladen.

SSH-Zugriffskennwörter für Admin-Knoten ändern

Durch das Ändern der SSH-Zugriffskennwörter für Admin-Knoten werden auch die eindeutigen Sätze interner SSH-Schlüssel für jeden Knoten im Raster aktualisiert. Der primäre Admin-Knoten verwendet diese SSH-Schlüssel, um mithilfe einer sicheren, passwortlosen Authentifizierung auf Knoten zuzugreifen.

Verwenden Sie einen SSH-Schlüssel, um sich bei einem Knoten anzumelden als `admin` oder an den Root-Benutzer einer VM oder einer physischen Konsolenverbindung.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Sie haben die ["Wartungs- oder Root-Zugriffsberechtigung"](#).
- Sie verfügen über die aktuelle Bereitstellungspassphrase.

Informationen zu diesem Vorgang

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.

Für die SSH-Schlüssel, die für die Kommunikation zwischen Knoten verwendet werden, gibt es separate SSH-Zugriffskennwörter. Diese werden durch dieses Verfahren nicht verändert.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Grid-Passwörter**.
2. Wählen Sie unter **SSH-Schlüssel ändern** die Option **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 Bereitstellungspassphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.
3. Kopieren Sie die Wiederherstellungspaketdatei (`.zip`) an zwei sichere und getrennte Orte.



Die Datei des Wiederherstellungspakets 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 Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**, wenn Sie bereit sind, mit der Änderung der SSH-Zugriffsschlüssel zu beginnen.



Sie können diesen Vorgang nach dem Start nicht mehr abbrechen.

SSH-Zugriffsschlüssel ändern

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 die Inhalte 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 Datei des Wiederherstellungspakets 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 Knoten aktualisiert wurden. Dies kann einige Minuten dauern.

Wenn die Schlüssel für alle Knoten geändert werden, wird ein grünes Erfolgsbanner angezeigt.

Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in einer Bannermeldung die Anzahl der Knoten aufgelistet, deren Schlüssel nicht geändert werden konnten. Das System wiederholt den Vorgang automatisch auf jedem Knoten, dessen Schlüssel nicht geändert werden konnte. Wenn der Vorgang endet und einige Knoten immer noch keinen geänderten Schlüssel haben, wird die Schaltfläche **Wiederholen** angezeigt.

Wenn die Schlüsselaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

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

Durch einen erneuten Versuch werden nur die SSH-Zugriffsschlüssel auf den Knoten geändert, bei

denen bei vorherigen Schlüsseländerungsversuchen ein Fehler aufgetreten ist.

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

Verwenden der Identitätsföderation

Durch die Verwendung der Identitätsföderation wird das Einrichten von Gruppen und Benutzern beschleunigt und Benutzer können sich mit vertrauten Anmeldeinformationen bei StorageGRID anmelden.

Konfigurieren der 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, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server verwaltet werden.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.



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

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Sehen [Richtlinien zum Konfigurieren eines OpenLDAP-Servers](#) .
- Wenn Sie Single Sign-On (SSO) aktivieren möchten, haben Sie die ["Anforderungen und Überlegungen für Single Sign-On"](#) .
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, verwendet der Identitätsanbieter TLS 1.2 oder 1.3. Sehen ["Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen"](#) .

Informationen zu diesem Vorgang

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

- Administratorgruppen. Die Benutzer in Administratorgruppen können sich beim Grid Manager anmelden und Aufgaben basierend auf den der Gruppe zugewiesenen Verwaltungsberechtigungen ausführen.
- Mandantenbenutzergruppen für Mandanten, die keine eigene Identitätsquelle verwenden. Benutzer in Mandantengruppen können sich beim Mandantenmanager anmelden und Aufgaben basierend auf den der Gruppe im Mandantenmanager zugewiesenen Berechtigungen ausführen. Sehen ["Mieterkonto erstellen"](#) Und ["Verwenden eines Mandantenkontos"](#) für Details.

Geben Sie die Konfiguration ein

Schritte

1. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Identitätsföderation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt „LDAP-Diensttyp“ 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	Azure	OpenLDAP	Other
------------------	-------	----------	-------

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

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt „LDAP-Attribute“ aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
 - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `uid` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid`.
 - **Benutzer-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
 - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `cn` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn`.
 - **Gruppen-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Diensttypen die erforderlichen LDAP-Server- und Netzwerkverbindungsinformationen im Abschnitt „LDAP-Server konfigurieren“ ein.
 - **Hostname**: Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des LDAP-Servers.
 - **Port**: Der Port, der für die Verbindung mit dem LDAP-Server verwendet wird.



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

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

Für Active Directory können Sie auch den Down-Level-Anmeldenamen oder den Benutzerprinzipalnamen angeben.

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

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



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

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



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

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



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

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

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

Geben Sie eines dieser Muster ein:

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

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

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

- **STARTLS verwenden:** Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese

Option wird für Azure nicht unterstützt.

- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.
- **TLS nicht verwenden:** Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.



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

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, das zum Sichern der Verbindung verwendet wird.

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

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

Testen Sie die Verbindung und speichern Sie die Konfiguration

Nachdem Sie alle Werte eingegeben haben, müssen Sie die Verbindung testen, bevor Sie die Konfiguration speichern können. StorageGRID überprüft die Verbindungseinstellungen für den LDAP-Server und das Bind-Benutzernamenformat, falls Sie eines angegeben haben.

Schritte

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

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

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel

Test Connection

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

Erzwingen der Synchronisierung mit der Identitätsquelle

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

Schritte

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

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



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

Identitätsföderation deaktivieren

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

Informationen zu diesem Vorgang

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundbenutzer können sich nicht anmelden.

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

Schritte

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

Richtlinien zum Konfigurieren eines OpenLDAP-Servers

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



Bei Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff für extern deaktivierte Benutzer nicht automatisch. Um den S3-Zugriff zu blockieren, löschen Sie alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Memberof- und Refint-Overlays

Die Memberof- und Refint-Overlays sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur umgekehrten Pflege von Gruppenmitgliedschaften

im <http://www.openldap.org/doc/admin24/index.html> ["OpenLDAP-Dokumentation: Administratorhandbuch Version 2.4"] .

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Indexschlüsselwörtern konfigurieren:

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

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

Informationen zur umgekehrten Pflege von Gruppenmitgliedschaften finden Sie

im <http://www.openldap.org/doc/admin24/index.html> ["OpenLDAP-Dokumentation: Administratorhandbuch Version 2.4"] .

Verwalten von Administratorgruppen

Sie können Administratorgruppen erstellen, um die Sicherheitsberechtigungen für einen

oder mehrere Administratorbenutzer zu verwalten. Benutzer müssen einer Gruppe angehören, um Zugriff auf das StorageGRID -System zu erhalten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie die Identitätsföderation konfiguriert und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Erstellen einer Administratorgruppe

Mithilfe von Administratorgruppen können Sie festlegen, welche Benutzer auf welche Funktionen und Vorgänge im Grid Manager und der Grid Management API zugreifen können.

Zugriff auf den Assistenten

Schritte

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

Wählen Sie einen Gruppentyp

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** aus.
2. Geben Sie einen Anzeigenamen für die Gruppe ein, den Sie später bei Bedarf aktualisieren können. Beispielsweise „Wartungsbenutzer“ oder „ILM-Administratoren“.
3. Geben Sie einen eindeutigen Namen für die Gruppe ein, den Sie später nicht mehr ändern können.
4. Wählen Sie **Weiter**.

Föderierte Gruppe

Schritte

1. Wählen Sie **Verbundgruppe** aus.
2. Geben Sie den Namen der Gruppe, die Sie importieren möchten, genau so ein, wie er in der konfigurierten Identitätsquelle angezeigt wird.
 - Verwenden Sie für Active Directory und Azure den sAMAccountName.
 - Verwenden Sie für OpenLDAP den CN (Common Name).
 - Verwenden Sie für ein anderes LDAP den entsprechenden eindeutigen Namen für den LDAP-Server.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Schritte

1. Wählen Sie für den **Zugriffsmodus** aus, ob Benutzer der Gruppe Einstellungen ändern und Vorgänge im Grid Manager und der Grid Management API ausführen können oder ob sie Einstellungen und Funktionen nur anzeigen können.
 - **Lesen/Schreiben** (Standard): Benutzer können Einstellungen ändern und die Vorgänge ausführen, die ihnen durch ihre Verwaltungsberechtigungen gestattet sind.
 - **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Grid Manager oder in der Grid Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.



Wenn ein Benutzer mehreren Gruppen angehört und eine der Gruppen auf **Schreibgeschützt** eingestellt ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Wählen Sie eine oder mehrere ["Berechtigungen der Administratorgruppe"](#) .

Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen, da sich die Benutzer der Gruppe sonst nicht bei StorageGRID anmelden können.

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

Benutzer hinzufügen (nur lokale Gruppen)

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. Sehen ["Benutzer verwalten"](#) für Details.

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

Anzeigen und Bearbeiten von Administratorgruppen

Sie können Details zu vorhandenen Gruppen anzeigen, eine Gruppe ändern oder eine Gruppe duplizieren.

- Um grundlegende Informationen zu allen Gruppen anzuzeigen, sehen Sie sich die Tabelle auf der Seite „Gruppen“ an.
- 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
Gruppendetails anzeigen	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie Aktionen > Gruppendetails anzeigen .	Wählen Sie den Gruppennamen in der Tabelle aus.

Aufgabe	Menü „Aktionen“	Detailseite
Anzeigenamen bearbeiten (nur lokale Gruppen)	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie Aktionen > Gruppennamen bearbeiten . c. Geben Sie den neuen Namen ein. d. Wählen Sie Änderungen speichern .	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol  . c. Geben Sie den neuen Namen ein. d. Wählen Sie Änderungen speichern .
Zugriffsmodus oder Berechtigungen bearbeiten	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie Aktionen > Gruppendetails anzeigen . c. Ändern Sie optional den Zugriffsmodus der Gruppe. d. Optional können Sie auswählen oder löschen " Berechtigungen der Administratorgruppe ". e. Wählen Sie Änderungen speichern .	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Ändern Sie optional den Zugriffsmodus der Gruppe. c. Optional können Sie auswählen oder löschen " Berechtigungen der Administratorgruppe ". 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 zum Duplizieren von Gruppen ab.

Löschen einer Gruppe

Sie können eine Administratorgruppe löschen, wenn Sie die Gruppe aus dem System entfernen möchten, und alle mit der Gruppe verknüpften Berechtigungen entfernen. Durch das Löschen einer Administratorgruppe werden alle Benutzer aus der Gruppe entfernt, die Benutzer selbst werden 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 der Administratorgruppe

Beim Erstellen von Administratorbenutzergruppen wählen Sie eine oder mehrere Berechtigungen aus, um den Zugriff auf bestimmte Funktionen des Grid Managers zu steuern. Sie können dann jeden Benutzer einer oder mehreren dieser Administratorgruppen zuweisen, um festzulegen, welche Aufgaben der Benutzer ausführen kann.

Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen. Andernfalls können sich die Benutzer dieser Gruppe nicht beim Grid Manager oder der Grid Management API anmelden.

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

- Sign in
- Dashboard anzeigen
- Anzeigen der Knotenseiten
- Aktuelle und gelöste Warnmeldungen anzeigen
- Das eigene Passwort ändern (nur lokale Benutzer)
- Zeigen Sie bestimmte Informationen auf den Konfigurations- und Wartungsseiten an

Interaktion zwischen Berechtigungen und Zugriffsmodus

Bei allen Berechtigungen bestimmt die Einstellung **Zugriffsmodus** der Gruppe, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie die zugehörigen Einstellungen und Funktionen nur anzeigen können. Wenn ein Benutzer mehreren Gruppen angehört und eine der Gruppen auf **Schreibgeschützt** eingestellt ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Administratorgruppe zuweisen können. Für alle nicht ausdrücklich genannten Funktionen ist die Berechtigung **Root-Zugriff** erforderlich.

Root-Zugriff

Diese Berechtigung bietet Zugriff auf alle Grid-Verwaltungsfunktionen.

Ändern des Root-Passworts des Mandanten

Diese Berechtigung bietet Zugriff auf die Option **Root-Passwort ändern** auf der Seite „Mandanten“, sodass Sie steuern können, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern kann. Diese Berechtigung wird auch zum Migrieren von S3-Schlüsseln verwendet, wenn die Funktion zum Importieren von S3-Schlüsseln aktiviert ist. Benutzer ohne diese Berechtigung können die Option **Root-Passwort ändern** nicht sehen.



Um Zugriff auf die Seite „Mandanten“ zu gewähren, die die Option „Root-Passwort ändern“ enthält, weisen Sie auch die Berechtigung „Mandantenkonten“ zu.

Konfiguration der Grid-Topologieseite

Diese Berechtigung bietet Zugriff auf die Konfigurationsregisterkarten auf der Seite **SUPPORT > Tools > Grid-Topologie**.



Die Seite „Grid-Topologie“ ist veraltet und wird in einer zukünftigen Version entfernt.

ILM

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Speicherpools
- Lagerqualitäten
- Regionen
- Objektmetadatenuche



Benutzer müssen über die Berechtigungen **Andere Rasterkonfiguration** und **Rastertopologieseitenkonfiguration** verfügen, um Speicherklassen verwalten zu können.

Wartung

Benutzer müssen über die Berechtigung „Wartung“ verfügen, um diese Optionen verwenden zu können:

- **KONFIGURATION > Zugriffskontrolle:**
 - Grid-Passwörter
- **KONFIGURATION > Netzwerk:**
 - S3-Endpunktdomännennamen
- **WARTUNG > Aufgaben:**
 - Außerbetriebnahme
 - Erweiterung
 - Objektexistenzprüfung
 - Erholung
- **WARTUNG > System:**
 - Wiederherstellungspaket
 - Software-Update
- **SUPPORT > Tools:**
 - Protokolle

Benutzer ohne Wartungsberechtigung können die folgenden Seiten anzeigen, aber nicht bearbeiten:

- **WARTUNG > Netzwerk:**
 - DNS-Server
 - Netznetzwerk
 - NTP-Server
- **WARTUNG > System:**
 - Lizenz
- **KONFIGURATION > Netzwerk:**
 - S3-Endpunktdomännennamen
- **KONFIGURATION > Sicherheit:**

- Zertifikate
- **KONFIGURATION > Überwachung:**
 - Audit- und Syslog-Server

Verwalten von Warnungen

Diese Berechtigung bietet Zugriff auf Optionen zum Verwalten von Warnungen. Benutzer müssen über diese Berechtigung verfügen, um Stummschaltungen, Warnbenachrichtigungen und Warnregeln zu verwalten.

Metrikabfrage

Diese Berechtigung bietet Zugriff auf:

- **SUPPORT > Tools > Metriken-Seite**
- Benutzerdefinierte Prometheus-Metrikabfragen mithilfe des Abschnitts **Metriken** der Grid Management API
- Grid Manager-Dashboardkarten mit Metriken

Objektmetadatensuche

Diese Berechtigung bietet Zugriff auf die Seite **ILM > Objektmetadatensuche**.

Andere Netzkonfiguration

Diese Berechtigung bietet Zugriff auf zusätzliche Rasterkonfigurationsoptionen.



Um diese zusätzlichen Optionen anzuzeigen, müssen Benutzer auch über die Berechtigung **Konfiguration der Grid-Topologieseite** verfügen.

- **ILM:**
 - Lagerqualitäten
- **KONFIGURATION > System:**
- **SUPPORT > Sonstiges:**
 - Linkkosten

Speichergeräteadministrator

Diese Berechtigung bietet:

- Zugriff auf den E-Series SANtricity System Manager auf Speichergeräten über den Grid Manager.
- Die Möglichkeit, auf der Registerkarte „Laufwerke verwalten“ Fehlerbehebungs- und Wartungsaufgaben für Appliances durchzuführen, die diese Vorgänge unterstützen.

Mandantenkonten

Diese Berechtigung bietet die Möglichkeit:

- Greifen Sie auf die Seite „Mandanten“ zu, auf der Sie Mandantenkonten erstellen, bearbeiten und entfernen können.

- Vorhandene Richtlinien zur Verkehrsklassifizierung anzeigen
- Zeigen Sie Grid Manager-Dashboardkarten an, die Mieterdetails enthalten

Benutzer verwalten

Sie können lokale und föderierte Benutzer anzeigen. Sie können auch lokale Benutzer erstellen und sie lokalen Administratorgruppen zuweisen, um festzulegen, auf welche Grid Manager-Funktionen diese Benutzer zugreifen können.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .

Erstellen eines lokalen Benutzers

Sie können einen oder mehrere lokale Benutzer erstellen und jeden 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 föderierte Benutzer und Gruppen zu verwalten.

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



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

Zugriff auf den Assistenten

Schritte

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

Benutzeranmeldeinformationen eingeben

Schritte

1. Geben Sie den vollständigen Namen des Benutzers, einen eindeutigen Benutzernamen und ein Passwort 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. Optional können Sie den Benutzer einer oder mehreren Gruppen zuweisen, um die Berechtigungen des Benutzers festzulegen.

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

Wenn ein Benutzer mehreren Gruppen angehört, sind die Berechtigungen kumulativ. Sehen "[Verwalten von Administratorgruppen](#)" für Details.

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

Anzeigen und Bearbeiten lokaler Benutzer

Sie können Details zu vorhandenen lokalen und föderierten Benutzern anzeigen. Sie können einen lokalen Benutzer ändern, um den vollständigen Namen, das Kennwort oder die Gruppenmitgliedschaft des Benutzers zu ändern. Sie können einem Benutzer auch vorübergehend den Zugriff auf den Grid Manager und die Grid Management API verweigern.

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

- Um grundlegende Informationen zu allen lokalen und föderierten Benutzern anzuzeigen, sehen Sie sich die Tabelle auf der Seite „Benutzer“ an.
- Um alle Details für einen bestimmten Benutzer anzuzeigen, einen lokalen Benutzer zu bearbeiten oder das Kennwort eines lokalen Benutzers zu ändern, verwenden Sie das Menü **Aktionen** oder die Detailseite.

Alle Änderungen werden angewendet, wenn sich der Benutzer das nächste Mal abmeldet und sich dann wieder beim Grid Manager anmeldet.



Lokale Benutzer können ihre eigenen Passwörter mit der Option **Passwort ändern** im Grid Manager-Banner ändern.

Aufgabe	Menü „Aktionen“	Detailseite
Benutzerdetails anzeigen	- Aktivieren Sie das Kontrollkästchen für den Benutzer. - Wählen Sie Aktionen > Benutzerdetails anzeigen.	Wählen Sie den Namen des Benutzers in der Tabelle aus.
Vollständigen Namen bearbeiten (nur lokale Benutzer)	- Aktivieren Sie das Kontrollkästchen für den Benutzer. - Wählen Sie Aktionen > Vollständigen Namen bearbeiten. - Geben Sie den neuen Namen ein. - Wählen Sie Änderungen speichern.	- Wählen Sie den Namen des Benutzers aus, um die Details anzuzeigen. - Wählen Sie das Bearbeitungssymbol . - Geben Sie den neuen Namen ein. - Wählen Sie Änderungen speichern.

Aufgabe	Menü „Aktionen“	Detailseite
StorageGRID Zugriff verweigern oder zulassen	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, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie Nein, um dem Benutzer die Anmeldung zu ermöglichen. e. Wählen Sie Änderungen speichern.	a. Wählen Sie den Namen des Benutzers aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte „Zugriff“ aus. c. Wählen Sie Ja, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie Nein, um dem Benutzer die Anmeldung zu ermöglichen. d. Wählen Sie Änderungen speichern.
Passwort ändern (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. c. Wählen Sie die Registerkarte „Passwort“. d. Geben Sie ein neues Passwort ein. e. Wählen Sie Passwort ändern.	a. Wählen Sie den Namen des Benutzers aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte „Passwort“. c. Geben Sie ein neues Passwort ein. d. Wählen Sie Passwort ändern.
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 einem neuen Browser-Tab anzuzeigen. e. Wählen Sie Gruppen bearbeiten, um andere Gruppen auszuwählen. f. Wählen Sie Änderungen speichern.	a. Wählen Sie den Namen des Benutzers 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 einem neuen Browser-Tab anzuzeigen. d. Wählen Sie Gruppen bearbeiten, um andere Gruppen auszuwählen. e. Wählen Sie Änderungen speichern.

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 zum Duplizieren von Benutzern ab.

Löschen eines Benutzers

Sie können einen lokalen Benutzer löschen, um ihn 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**.

Verwenden Sie Single Sign-On (SSO).

Konfigurieren der einmaligen Anmeldung

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.

So funktioniert Single Sign-On

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

Bevor Sie Single Sign-On (SSO) aktivieren, prüfen Sie, wie sich die Aktivierung von SSO auf die Anmelde- und Abmeldeprozesse von StorageGRID auswirkt.

Sign in, wenn SSO aktiviert ist

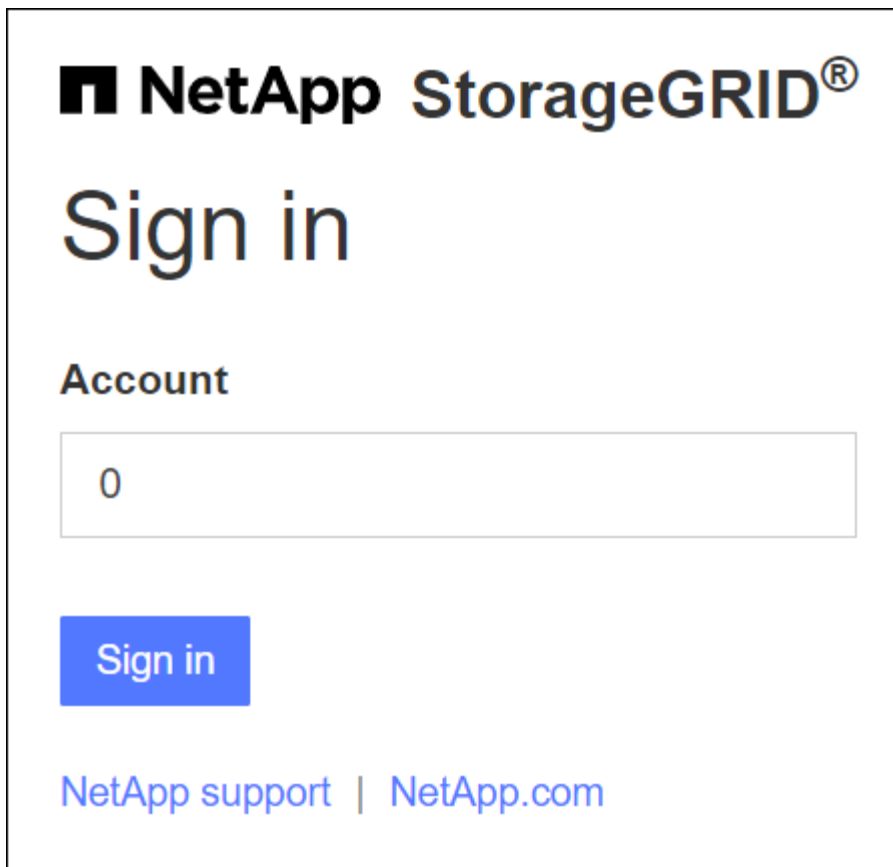
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur Validierung Ihrer Anmeldeinformationen auf die SSO-Seite Ihrer Organisation weitergeleitet.

Schritte

1. Geben Sie den vollqualifizierten Domännennamen oder die IP-Adresse eines beliebigen StorageGRID Admin-Knotens in einen Webbrowser ein.

Die StorageGRID Sign in 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 Sign in wird nicht angezeigt, wenn Sie die vollständige URL für ein Mandantenkonto eingeben (d. h. einen vollqualifizierten Domännennamen oder eine IP-Adresse gefolgt von `/?accountId=20-digit-account-id`). Stattdessen werden Sie sofort auf die SSO-Anmeldeseite Ihrer Organisation weitergeleitet, wo Sie [Melden Sie sich mit Ihren SSO-Anmeldeinformationen an](#).

- 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 dieser 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 dieser in der Liste der letzten Konten angezeigt wird.
- Wählen Sie * Sign in*

StorageGRID leitet Sie zur SSO-Anmeldeseite Ihrer Organisation weiter. Beispiel:

Sign in with your organizational account

Sign in

4. Sign in .

Wenn Ihre SSO-Anmeldeinformationen korrekt sind:

- Der Identitätsanbieter (IdP) stellt StorageGRID eine Authentifizierungsantwort bereit.
- StorageGRID validiert die Authentifizierungsantwort.
- Wenn die Antwort gültig ist und Sie zu einer föderierten Gruppe mit StorageGRID Zugriffsberechtigungen gehören, werden Sie beim Grid Manager oder beim Tenant Manager angemeldet, je nachdem, welches Konto Sie ausgewählt haben.



Wenn auf das Dienstkonto nicht zugegriffen werden kann, können Sie sich trotzdem anmelden, solange Sie ein bestehender Benutzer sind, der zu einer föderierten Gruppe mit StorageGRID Zugriffsberechtigungen gehört.

5. Greifen Sie optional auf andere Admin-Knoten zu oder greifen Sie auf den Grid Manager oder den Tenant Manager zu, wenn Sie über die entsprechenden Berechtigungen verfügen.

Sie müssen Ihre SSO-Anmeldeinformationen nicht erneut eingeben.

Abmelden, wenn SSO aktiviert ist

Wenn SSO für StorageGRID aktiviert ist, hängt das Geschehen beim Abmelden davon ab, bei was Sie angemeldet sind und von wo aus Sie sich abmelden.

Schritte

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

Die StorageGRID Sign in wird angezeigt. Das Dropdown-Menü **Letzte Konten** wurde aktualisiert und enthält jetzt **Grid Manager** oder den Namen des Mandanten, sodass Sie in Zukunft schneller auf diese Benutzeroberflächen zugreifen können.

Wenn Sie angemeldet sind bei...	Und Sie melden sich ab von...	Sie sind abgemeldet von...
Grid Manager auf einem oder mehreren Admin-Knoten	Grid Manager auf jedem Admin-Knoten	Grid Manager auf allen Admin-Knoten Hinweis: Wenn Sie Azure für SSO verwenden, kann es einige Minuten dauern, bis Sie von allen Admin-Knoten abgemeldet sind.
Mandantenmanager auf einem oder mehreren Admin-Knoten	Mandantenmanager auf jedem Admin-Knoten	Mandantenmanager auf allen Admin-Knoten
Sowohl Grid Manager als auch Tenant Manager	Grid-Manager	Nur der Grid Manager. Sie müssen sich auch vom Tenant Manager abmelden, um sich von SSO abzumelden.



Die Tabelle fasst zusammen, was passiert, wenn Sie sich abmelden, wenn Sie eine einzelne Browsersitzung verwenden. Wenn Sie über mehrere Browsersitzungen hinweg bei StorageGRID angemeldet sind, müssen Sie sich von allen Browsersitzungen separat abmelden.

Anforderungen und Überlegungen zur einmaligen Anmeldung

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

Anforderungen an den Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

- Active Directory-Verbunddienst (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

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

Konfigurierter LDAP-Diensttyp	Optionen für SSO-Identitätsanbieter
Active Directory	• Active Directory • Azurblau • PingFederate
Azurblau	Azurblau

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 die ["Update KB3201845"](#) oder höher.

Zusätzliche Anforderungen

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

Überlegungen zu Azure

Wenn Sie Azure 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.

Serverzertifikatanforderungen

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 (Azure) oder Dienstanbieterverbindungen (PingFederate) für StorageGRID konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID Anfragen.

Wenn Sie dies noch nicht getan haben ["ein benutzerdefiniertes Zertifikat für die Verwaltungsschnittstelle konfiguriert"](#), sollten Sie dies jetzt tun. Wenn Sie ein benutzerdefiniertes Serverzertifikat installieren, wird es für alle Admin-Knoten verwendet und Sie können es in allen StorageGRID -Vertrauensstellungen, Unternehmensanwendungen oder SP Verbindungen verwenden.



Die Verwendung des Standardserverzertifikats eines Admin-Knotens in einer Vertrauensstellung der vertrauenden Partei, einer Unternehmensanwendung oder einer SP Verbindung wird nicht empfohlen. Wenn der Knoten ausfällt und Sie ihn wiederherstellen, wird ein neues Standardserverzertifikat generiert. Bevor Sie sich beim wiederhergestellten Knoten anmelden können, müssen Sie die Vertrauensstellung der vertrauenden Seite, die Unternehmensanwendung 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 zu `/var/local/mgmt-api` Verzeichnis. Ein benutzerdefiniertes Serverzertifikat heißt `custom-server.crt`. Das Standardserverzertifikat des Knotens heißt `server.crt`.

Portanforderungen

Single Sign-On (SSO) ist auf den eingeschränkten Grid Manager- oder Tenant Manager-Ports nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Sie möchten, dass sich Benutzer per Single Sign-On authentifizieren. Sehen ["Zugriffskontrolle an externer Firewall"](#).

Bestätigen, dass sich Verbundbenutzer anmelden können

Bevor Sie Single Sign-On (SSO) aktivieren, müssen Sie bestätigen, dass sich mindestens ein Verbundbenutzer beim Grid Manager und beim Tenant Manager für alle vorhandenen Tenant-Konten anmelden kann.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .
- Sie haben die Identitätsföderation bereits konfiguriert.

Schritte

1. Wenn bereits Mandantenkonten vorhanden sind, vergewissern Sie sich, dass keiner der Mandanten eine eigene Identitätsquelle verwendet.



Wenn Sie SSO aktivieren, wird eine im Tenant Manager konfigurierte Identitätsquelle durch die im Grid Manager konfigurierte Identitätsquelle überschrieben. Benutzer, die zur Identitätsquelle des Mandanten gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Identitätsquelle Grid Manager.

- a. Sign in .
 - b. Wählen Sie **ZUGRIFFSVERWALTUNG > Identitätsföderation**.
 - c. Vergewissern Sie sich, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht aktiviert ist.
 - d. Wenn dies der Fall ist, bestätigen Sie, dass alle möglicherweise für dieses Mandantenkonto verwendeten Verbundgruppen nicht mehr benötigt werden, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.
2. Bestätigen Sie, dass ein Verbundbenutzer auf den Grid Manager zugreifen kann:
 - a. Wählen Sie im Grid Manager **KONFIGURATION > Zugriffskontrolle > Admin-Gruppen**.
 - b. Stellen Sie sicher, dass mindestens eine Verbundgruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
 - c. Abmelden.
 - d. Bestätigen Sie, dass Sie sich als Benutzer der Verbundgruppe erneut beim Grid Manager anmelden können.
 3. Wenn vorhandene Mandantenkonten vorhanden sind, bestätigen Sie, dass sich ein Verbundbenutzer mit Root-Zugriffsberechtigung anmelden kann:
 - a. Wählen Sie im Grid Manager **MIETER** aus.
 - b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen > Bearbeiten**.
 - c. Wählen Sie auf der Registerkarte „Details eingeben“ die Option „Weiter“ aus.
 - d. Wenn das Kontrollkästchen **Eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.

Edit the tenant

Enter details ————— 2 Select permissions

Select permissions

Select the permissions for this tenant account.

- ☐ Allow platform services ?
- ☐ Use own identity source ?
- ☐ Allow S3 Select ?

Die Mandantenseite wird angezeigt.

- Wählen Sie das Mandantenkonto aus, wählen Sie * Sign in* und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
- Wählen Sie im Mandanten-Manager **ZUGRIFFSVERWALTUNG > Gruppen**.
- Stellen Sie sicher, dass mindestens einer föderierten Gruppe aus dem Grid Manager die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.
- Abmelden.
- Bestätigen Sie, dass Sie sich als Benutzer der Verbundgruppe erneut beim Mandanten anmelden können.

Ähnliche Informationen

- ["Anforderungen und Überlegungen zur einmaligen Anmeldung"](#)
- ["Verwalten von Administratorgruppen"](#)
- ["Verwenden eines Mandantenkontos"](#)

Sandbox-Modus verwenden

Sie können den Sandbox-Modus verwenden, um Single Sign-On (SSO) zu konfigurieren und zu testen, bevor Sie es für alle StorageGRID Benutzer aktivieren. Nachdem SSO aktiviert wurde, können Sie jederzeit in den Sandbox-Modus zurückkehren, wenn Sie die Konfiguration ändern oder erneut testen müssen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#).

- Sie haben die "[Root-Zugriffsberechtigung](#)".
- Sie haben die Identitätsföderation für Ihr StorageGRID -System konfiguriert.
- Für den **LDAP-Diensttyp** der Identitätsföderation haben Sie je nach dem SSO-Identitätsanbieter, den Sie verwenden möchten, entweder Active Directory oder Azure ausgewählt.

Konfigurierter LDAP-Diensttyp	Optionen für SSO-Identitätsanbieter
Active Directory	• Active Directory • Azurblau • PingFederate
Azurblau	Azurblau

Informationen zu diesem Vorgang

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Knoten anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an den SSO-Identitätsanbieter. Im Gegenzug sendet der SSO-Identitätsanbieter eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Authentifizierungsanforderung erfolgreich war. Für erfolgreiche Anfragen:

- Die Antwort von Active Directory oder PingFederate enthält eine universell eindeutige Kennung (UUID) für den Benutzer.
- Die Antwort von Azure enthält einen User Principal Name (UPN).

Damit StorageGRID (der Dienstanbieter) und der SSO-Identitätsanbieter sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, müssen Sie bestimmte Einstellungen in StorageGRID konfigurieren. Als Nächstes müssen Sie die Software des SSO-Identitätsanbieters verwenden, um für jeden Admin-Knoten eine Vertrauensstellung der vertrauenden Seite (AD FS), eine Unternehmensanwendung (Azure) oder einen Dienstanbieter (PingFederate) zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, 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.

Zugriff auf den Sandbox-Modus

Schritte

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

Die Seite „Single Sign-On“ wird mit der ausgewählten Option **Deaktiviert** angezeigt.

Single Sign-on

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

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Wenn die SSO-Statusoptionen nicht angezeigt werden, bestätigen Sie, dass Sie den Identitätsanbieter als Verbundidentitätsquelle konfiguriert haben. Sehen ["Anforderungen und Überlegungen zur einmaligen Anmeldung"](#) .

2. Wählen Sie **Sandbox-Modus**.

Der Abschnitt „Identitätsanbieter“ wird angezeigt.

Geben Sie die Details des Identitätsanbieters ein

Schritte

1. Wählen Sie den **SSO-Typ** aus der Dropdown-Liste aus.
2. Füllen Sie die Felder im Abschnitt „Identitätsanbieter“ basierend auf dem von Ihnen ausgewählten SSO-Typ aus.

Active Directory

- a. 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 Verbunddienstes zu finden, gehen Sie zum Windows Server-Manager. Wählen Sie **Tools > AD FS-Verwaltung**. Wählen Sie im Aktionsmenü **Eigenschaften des Verbunddienstes bearbeiten** aus. Der Name des Verbunddienstes wird im zweiten Feld angezeigt.

- b. Geben Sie an, welches TLS-Zertifikat zum Sichern der Verbindung verwendet wird, wenn der Identitätsanbieter als Antwort auf StorageGRID -Anfragen SSO-Konfigurationsinformationen sendet.

- **CA-Zertifikat des Betriebssystems verwenden:** 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.

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



Wenn Sie das CA-Zertifikat ändern, sofort "[Starten Sie den mgmt-api-Dienst auf den Admin-Knoten neu](#)" und testen Sie, ob eine erfolgreiche einmalige Anmeldung beim Grid Manager erfolgt.

- c. Geben Sie im Abschnitt „Relying Party“ die **Relying Party-Kennung** 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 einen Admin-Knoten hat und Sie nicht beabsichtigen, in Zukunft weitere Admin-Knoten hinzuzufügen, geben Sie `SG` oder `StorageGRID` .
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Dadurch wird eine Tabelle generiert, die die Kennung der vertrauenden Partei 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 Vertrauensstellung der vertrauenden Partei erstellen. Durch die Einrichtung einer Vertrauensstellung der vertrauenden Partei für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten an- und abmelden können.

- d. Wählen Sie **Speichern**.

Auf der Schaltfläche **Speichern** wird für einige Sekunden ein grünes Häkchen angezeigt.



Azurblau

- a. Geben Sie an, welches TLS-Zertifikat zum Sichern der Verbindung verwendet wird, wenn der Identitätsanbieter als Antwort auf StorageGRID -Anfragen SSO-Konfigurationsinformationen sendet.

- **CA-Zertifikat des Betriebssystems verwenden:** 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.

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



Wenn Sie das CA-Zertifikat ändern, sofort "[Starten Sie den mgmt-api-Dienst auf den Admin-Knoten neu](#)" und testen Sie, ob eine erfolgreiche einmalige Anmeldung beim Grid Manager erfolgt.

- b. Geben Sie im Abschnitt „Unternehmensanwendung“ den **Namen der Unternehmensanwendung** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Unternehmensanwendung in Azure AD verwenden.

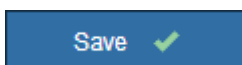
- Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und Sie nicht beabsichtigen, in Zukunft weitere Admin-Knoten hinzuzufügen, geben Sie `SG` oder `StorageGRID` .
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Dadurch wird eine Tabelle generiert, die basierend auf dem Hostnamen des Knotens einen Unternehmensanwendungsnamen für jeden Admin-Knoten in Ihrem System anzeigt.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Durch die Bereitstellung einer Unternehmensanwendung für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten anmelden und abmelden können.

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

Auf der Schaltfläche **Speichern** wird für einige Sekunden ein grünes Häkchen angezeigt.



PingFederate

- a. Geben Sie an, welches TLS-Zertifikat zum Sichern der Verbindung verwendet wird, wenn der Identitätsanbieter als Antwort auf StorageGRID -Anfragen SSO-Konfigurationsinformationen

sendet.

- **CA-Zertifikat des Betriebssystems verwenden:** 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.

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



Wenn Sie das CA-Zertifikat ändern, sofort "[Starten Sie den mgmt-api-Dienst auf den Admin-Knoten neu](#)" und testen Sie, ob eine erfolgreiche einmalige Anmeldung beim Grid Manager erfolgt.

- b. Geben Sie im Abschnitt „Service Provider (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 einen Admin-Knoten hat und Sie nicht beabsichtigen, in Zukunft weitere Admin-Knoten hinzuzufügen, geben Sie `SG` oder `StorageGRID` .
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Dadurch wird eine Tabelle generiert, 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-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten anmelden und abmelden können.

- c. Geben Sie die URL der Verbundmetadaten für jeden Admin-Knoten im Feld **URL der Verbundmetadaten** an.

Verwenden Sie das folgende Format:

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

- d. Wählen Sie **Speichern**.

Auf der Schaltfläche **Speichern** wird für einige Sekunden ein grünes Häkchen angezeigt.

Save ✓

Konfigurieren von Vertrauensstellungen der vertrauenden Seite, Unternehmensanwendungen oder SP Verbindungen

Wenn die Konfiguration gespeichert ist, wird die Bestätigungsmeldung für den Sandbox-Modus angezeigt. Dieser Hinweis bestätigt, dass der Sandbox-Modus jetzt aktiviert ist, und bietet eine Übersichtsanleitung.

StorageGRID kann so lange wie nötig im Sandbox-Modus bleiben. Wenn jedoch auf der Single Sign-On-Seite der **Sandbox-Modus** ausgewählt ist, wird SSO für alle StorageGRID Benutzer deaktiviert. Nur lokale Benutzer können sich anmelden.

Befolgen Sie diese Schritte, um Vertrauensstellungen der vertrauenden Seite (Active Directory) zu konfigurieren, Unternehmensanwendungen zu vervollständigen (Azure) oder SP Verbindungen zu konfigurieren (PingFederate).

Active Directory

Schritte

1. Gehen Sie zu Active Directory-Verbindungsdienste (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 „StorageGRID Single Sign-on“ angezeigt werden.

Sie müssen für jeden in der Tabelle angezeigten Admin-Knoten eine Vertrauensstellung erstellen.

Anweisungen finden Sie unter ["Erstellen von Vertrauensstellungen der vertrauenden Seite in AD FS"](#) .

Azurblau

Schritte

1. Wählen Sie auf der Single Sign-On-Seite für den Admin-Knoten, bei dem Sie derzeit angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster diese Schritte:
 - a. Sign in .
 - b. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Einmaliges Anmelden**.
 - c. Laden Sie die SAML-Metadaten für diesen Knoten herunter und speichern Sie sie.
3. Gehen Sie zum Azure-Portal.
4. Befolgen Sie die Schritte in ["Erstellen von Unternehmensanwendungen in Azure AD"](#) um die SAML-Metadatei für jeden Admin-Knoten in die entsprechende Azure-Unternehmensanwendung hochzuladen.

PingFederate

Schritte

1. Wählen Sie auf der Single Sign-On-Seite für den Admin-Knoten, bei dem Sie derzeit angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster diese Schritte:
 - a. Sign in .
 - b. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Einmaliges Anmelden**.
 - c. Laden Sie die SAML-Metadaten für diesen Knoten herunter und speichern Sie sie.
3. Gehen Sie zu PingFederate.
4. ["Erstellen Sie eine oder mehrere Service Provider \(SP\)-Verbindungen für StorageGRID"](#) . Verwenden Sie die SP Verbindungs-ID für jeden Admin-Knoten (angezeigt in der Tabelle auf der StorageGRID Single-Sign-On-Seite) und die SAML-Metadaten, die Sie für diesen Admin-Knoten heruntergeladen haben.

Sie müssen für jeden in der Tabelle angezeigten Admin-Knoten eine SP Verbindung erstellen.

Testen Sie SSO-Verbindungen

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

Active Directory

Schritte

1. Suchen Sie auf der StorageGRID Single Sign-On-Seite den Link in der Sandbox-Modus-Nachricht.

Die URL wird aus dem Wert abgeleitet, den Sie in das Feld **Name des Verbunddienstes** eingegeben haben.

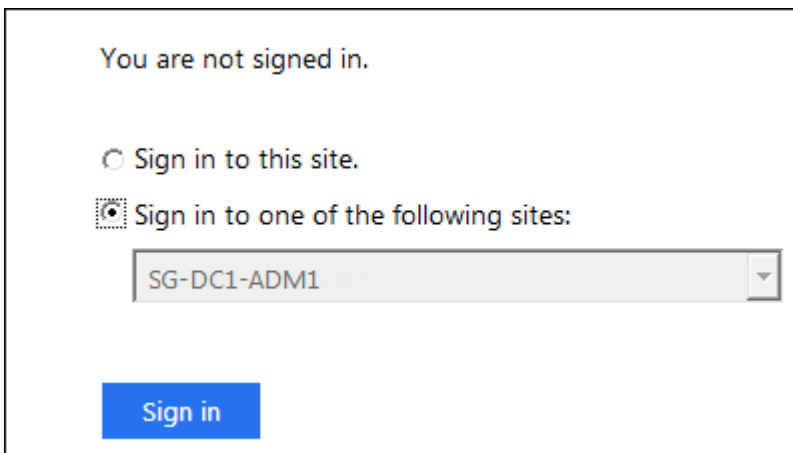
Sandbox mode

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

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

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

2. Wählen Sie den Link aus oder kopieren Sie die URL und fügen Sie sie in einen Browser ein, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
3. Um zu bestätigen, dass Sie sich mit SSO bei StorageGRID anmelden können, wählen Sie * Bei einer der folgenden Sites Sign in , **wählen Sie die Kennung der vertrauenden Partei für Ihren primären Admin-Knoten und wählen Sie * Sign in.**



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

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

- Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers und versuchen Sie es erneut.
5. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Knoten in Ihrem Raster zu überprüfen.

Azurblau

Schritte

1. Wechseln Sie im Azure-Portal zur Seite „Einmaliges Anmelden“.
2. Wählen Sie **Diese Anwendung testen**.
3. Geben Sie die Anmeldeinformationen eines Verbundbenutzers ein.
 - Wenn die SSO-An- und Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

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

- Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers und versuchen Sie es erneut.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Knoten in Ihrem Raster zu überprüfen.

PingFederate

Schritte

1. Wählen Sie auf der StorageGRID Single Sign-On-Seite den ersten Link in der Sandbox-Modus-Nachricht aus.

Wählen und testen Sie jeweils einen Link.

Sandbox mode

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

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Geben Sie die Anmeldeinformationen eines Verbundbenutzers ein.
 - Wenn die SSO-An- und Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

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

- Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers und versuchen Sie es erneut.
3. Wählen Sie den nächsten Link aus, um die SSO-Verbindung für jeden Admin-Knoten in Ihrem Raster zu überprüfen.

Wenn die Meldung „Seite abgelaufen“ angezeigt wird, wählen Sie in Ihrem Browser die Schaltfläche **Zurück** und senden Sie Ihre Anmeldeinformationen erneut.

Aktivieren der einmaligen Anmeldung

Wenn Sie bestätigt haben, dass Sie sich mit SSO bei jedem Admin-Knoten 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 Tenant Manager, die Grid Management API und die Tenant Management API zuzugreifen. Lokale Benutzer können nicht mehr auf StorageGRID zugreifen.

Schritte

1. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Einmaliges Anmelden**.
2. Ändern Sie den SSO-Status in **Aktiviert**.
3. Wählen Sie **Speichern**.
4. Überprüfen Sie die Warnmeldung und wählen Sie **OK**.

Single Sign-On ist jetzt aktiviert.



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

Erstellen von Vertrauensstellungen der vertrauenden Seite in AD FS

Sie müssen Active Directory Federation Services (AD FS) verwenden, um für jeden Admin-Knoten in Ihrem System eine Vertrauensstellung der vertrauenden Seite zu erstellen. Sie können Vertrauensstellungen der vertrauenden Seite mithilfe von PowerShell-Befehlen erstellen, indem Sie SAML-Metadaten aus StorageGRID importieren oder die Daten manuell eingeben.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **AD FS** als SSO-Typ ausgewählt.
- Der **Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Sehen "[Sandbox-Modus verwenden](#)".
- 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 Single-Sign-On-Seite.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID -System eine Vertrauensstellung der vertrauenden Partei erstellen. Durch die Einrichtung einer Vertrauensstellung der vertrauenden Partei für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten an- und abmelden können.

- Sie haben Erfahrung mit der Erstellung von Vertrauensstellungen vertrauender Parteien in AD FS oder Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das AD FS-Verwaltungs-Snap-In und gehören zur Gruppe „Administratoren“.

- Wenn Sie die Vertrauensstellung der vertrauenden Seite manuell erstellen, verfügen Sie über das benutzerdefinierte Zertifikat, das für die StorageGRID Verwaltungsschnittstelle hochgeladen wurde, oder Sie wissen, wie Sie sich über die Befehlsshell bei einem Admin-Knoten anmelden.

Informationen zu diesem Vorgang

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

Erstellen einer Vertrauensstellung der vertrauenden Seite mithilfe von Windows PowerShell

Sie können Windows PowerShell verwenden, um schnell eine oder mehrere Vertrauensstellungen der vertrauenden Seite zu erstellen.

Schritte

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

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

- Für *Admin_Node_Identifier* Geben Sie die Relying Party Identifier für den Admin-Knoten genau so ein, wie sie auf der Single Sign-On-Seite angezeigt wird. Beispiel: SG-DC1-ADM1 .
- Für *Admin_Node_FQDN* , geben Sie den vollqualifizierten Domännennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Knotens verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der vertrauenden Partei aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse jemals ändert.)

3. Wählen Sie im Windows Server Manager **Tools > AD FS-Verwaltung**.

Das AD FS-Verwaltungstool wird angezeigt.

4. Wählen Sie **AD FS > Vertrauensstellungen der vertrauenden Seite**.

Die Liste der Vertrauensstellungen der vertrauenden Seite wird angezeigt.

5. Fügen Sie der neu erstellten Vertrauensstellung der vertrauenden Seite eine Zugriffskontrollrichtlinie hinzu:
 - a. Suchen Sie nach der Vertrauensstellung der vertrauenden Partei, die Sie gerade erstellt haben.
 - b. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
 - c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
 - d. Wählen Sie **Übernehmen** und dann **OK**
6. Fügen Sie dem neu erstellten Relying Party Trust eine Claim Issuance Policy hinzu:
 - a. Suchen Sie nach der Vertrauensstellung der vertrauenden Partei, die Sie gerade erstellt haben.
 - b. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Richtlinie zur Anspruchsausstellung bearbeiten**.
 - c. Wählen Sie **Regel hinzufügen**.
 - d. Wählen Sie auf der Seite „Regelvorlage auswählen“ aus der Liste „LDAP-Attribute als Ansprüche

senden“ aus und klicken Sie auf „Weiter“.

e. Geben Sie auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel ein.

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

f. Wählen Sie für den Attributspeicher **Active Directory** aus.

g. Geben Sie in der Spalte „LDAP-Attribut“ der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.

h. Wählen Sie in der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle aus der Dropdownliste „**Namens-ID**“ aus.

i. Wählen Sie **Fertig** und dann **OK**.

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

a. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite, um ihre Eigenschaften zu öffnen.

b. Bestätigen Sie, dass die Felder auf den Registerkarten **Endpunkte**, **Kennungen** und **Signatur** ausgefüllt sind.

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

8. Wiederholen Sie diese Schritte, um eine Vertrauensstellung der vertrauenden Partei für alle Admin-Knoten 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. Sehen ["Sandbox-Modus verwenden"](#) Anweisungen hierzu finden Sie unter.

Erstellen einer Vertrauensstellung der vertrauenden Seite durch Importieren von Verbundmetadaten

Sie können die Werte für jede Vertrauensstellung der vertrauenden Partei importieren, indem Sie auf die SAML-Metadaten für jeden Admin-Knoten zugreifen.

Schritte

1. Wählen Sie im Windows Server-Manager **Tools** und dann **AD FS-Verwaltung** aus.

2. Wählen Sie unter „Aktionen“ die Option „Vertrauensstellung der vertrauenden Partei hinzufügen“ aus.

3. Wählen Sie auf der Willkommensseite **Claims aware** und dann **Start**.

4. Wählen Sie **Online oder in einem lokalen Netzwerk veröffentlichte Daten über die vertrauende Partei importieren**.

5. Geben Sie unter **Federation metadata address (host name or URL)** den Speicherort der SAML-Metadaten für diesen Admin-Knoten ein:

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

Für *Admin_Node_FQDN*, geben Sie den vollqualifizierten Domännennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Knotens verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der vertrauenden Partei aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse jemals ändert.)

6. Schließen Sie den Assistenten „Vertrauensstellung der vertrauenden Seite“ ab, speichern Sie die Vertrauensstellung der vertrauenden Seite und schließen Sie den Assistenten.



Verwenden Sie beim Eingeben des Anzeigenamens die Relying Party Identifier für den Admin-Knoten, genau so, wie sie auf der Single Sign-On-Seite im Grid Manager angezeigt wird. Beispiel: SG-DC1-ADM1 .

7. Fügen Sie eine Anspruchsregel hinzu:

- a. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Richtlinie zur Anspruchsausstellung bearbeiten**.
- b. Wählen Sie **Regel hinzufügen**:
- c. Wählen Sie auf der Seite „Regelvorlage auswählen“ aus der Liste „LDAP-Attribute als Ansprüche senden“ aus und klicken Sie auf „Weiter“.
- d. Geben Sie auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel ein.

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

- e. Wählen Sie für den Attributspeicher **Active Directory** aus.
- f. Geben Sie in der Spalte „LDAP-Attribut“ der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
- g. Wählen Sie in der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle aus der Dropdownliste **„Namens-ID“** aus.
- h. Wählen Sie **Fertig** und dann **OK**.

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

- a. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite, um ihre Eigenschaften zu öffnen.
- b. Bestätigen Sie, dass die Felder auf den Registerkarten **Endpunkte**, **Kennungen** und **Signatur** ausgefüllt sind.

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

9. Wiederholen Sie diese Schritte, um eine Vertrauensstellung der vertrauenden Partei für alle Admin-Knoten 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. Sehen ["Sandbox-Modus verwenden"](#) Anweisungen hierzu finden Sie unter.

Manuelles Erstellen einer Vertrauensstellung der vertrauenden Seite

Wenn Sie die Daten für die Vertrauensstellungen des vertrauenden Teils nicht importieren möchten, können Sie die Werte manuell eingeben.

Schritte

1. Wählen Sie im Windows Server-Manager **Tools** und dann **AD FS-Verwaltung** aus.
2. Wählen Sie unter „Aktionen“ die Option „Vertrauensstellung der vertrauenden Partei hinzufügen“ aus.
3. Wählen Sie auf der Willkommensseite **Claims aware** und dann **Start**.
4. Wählen Sie **Daten zur vertrauenden Partei manuell eingeben** und wählen Sie **Weiter**.
5. Schließen Sie den Assistenten „Relying Party Trust“ ab:

- a. Geben Sie einen Anzeigenamen für diesen Admin-Knoten ein.

Verwenden Sie aus Konsistenzgründen die Relying Party Identifier für den Admin-Knoten genau so, wie sie auf der Single Sign-On-Seite im Grid Manager angezeigt wird. Beispiel: SG-DC1-ADM1 .

- b. Überspringen Sie den Schritt zum Konfigurieren eines optionalen Token-Verschlüsselungszertifikats.
c. Aktivieren Sie auf der Seite „URL konfigurieren“ das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll aktivieren**.
d. Geben Sie die SAML-Dienstendpunkt-URL für den Admin-Knoten ein:

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

Für *Admin_Node_FQDN* Geben Sie den vollqualifizierten Domännennamen für den Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Knotens verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der vertrauenden Partei aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse jemals ändert.)

- e. Geben Sie auf der Seite „Kennungen konfigurieren“ die Kennung der vertrauenden Partei für denselben Admin-Knoten an:

Admin_Node_Identifier

Für *Admin_Node_Identifier* Geben Sie die Relying Party Identifier für den Admin-Knoten genau so ein, wie sie auf der Single Sign-On-Seite angezeigt wird. Beispiel: SG-DC1-ADM1 .

- f. Überprüfen Sie die Einstellungen, speichern Sie die Vertrauensstellung der vertrauenden Seite und schließen Sie den Assistenten.

Das Dialogfeld „Richtlinie zur Anspruchsausstellung bearbeiten“ wird angezeigt.



Wenn das Dialogfeld nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Richtlinie zur Anspruchsausstellung bearbeiten**.

6. Um den Anspruchsregel-Assistenten zu starten, wählen Sie **Regel hinzufügen**:

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

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

- c. Wählen Sie für den Attributspeicher **Active Directory** aus.
d. Geben Sie in der Spalte „LDAP-Attribut“ der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
e. Wählen Sie in der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle aus der Dropdownliste **„Namens-ID“** aus.
f. Wählen Sie **Fertig** und dann **OK**.

7. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite, um ihre Eigenschaften zu öffnen.
8. Konfigurieren Sie auf der Registerkarte **Endpunkte** den Endpunkt für Single Logout (SLO):

- a. Wählen Sie **SAML hinzufügen**.
- b. Wählen Sie **Endpunkttyp > SAML-Abmeldung**.
- c. Wählen Sie **Bindung > Umleitung**.
- d. Geben Sie im Feld **Vertrauenswürdige URL** die URL ein, die für die einmalige Abmeldung (SLO) von diesem Admin-Knoten verwendet wird:

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

Für *Admin_Node_FQDN* Geben Sie den vollqualifizierten Domännennamen des Admin-Knotens ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Knotens verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der vertrauenden Partei aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse jemals ändert.)

- a. Wählen Sie **OK**.
9. Geben Sie auf der Registerkarte **Signatur** das Signaturzertifikat für diese Vertrauensstellung der vertrauenden Seite an:
- a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:
 - Wenn Sie über das benutzerdefinierte Verwaltungszertifikat verfügen, das Sie in StorageGRID hochgeladen haben, wählen Sie dieses Zertifikat aus.
 - Wenn Sie nicht über das benutzerdefinierte Zertifikat verfügen, melden Sie sich beim Admin-Knoten an, gehen Sie zu `/var/local/mgmt-api` Verzeichnis des Admin-Knotens und fügen Sie die `custom-server.crt` Zertifikatsdatei.



Verwenden 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 vertrauenden Seite aktualisieren.

- b. Wählen Sie **Übernehmen** und dann **OK**.

Die Eigenschaften der vertrauenden Partei werden gespeichert und geschlossen.

10. Wiederholen Sie diese Schritte, um eine Vertrauensstellung der vertrauenden Partei für alle Admin-Knoten 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. Sehen ["Sandbox-Modus verwenden"](#) Anweisungen hierzu finden Sie unter.

Erstellen von Unternehmensanwendungen in Azure AD

Sie verwenden Azure AD, 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 **Azure** als SSO-Typ ausgewählt.
- Der **Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Sehen ["Sandbox-Modus verwenden"](#).

- Sie haben den **Namen der Unternehmensanwendung** für jeden Admin-Knoten in Ihrem System. Sie können diese Werte aus der Tabelle mit den Admin-Knotendetails auf der StorageGRID Single-Sign-On-Seite kopieren.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Durch die Bereitstellung einer Unternehmensanwendung für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten anmelden und abmelden können.

- Sie haben Erfahrung mit der Erstellung von Unternehmensanwendungen in Azure Active Directory.
- Sie verfügen über ein Azure-Konto mit einem aktiven Abonnement.
- Sie haben eine der folgenden Rollen im Azure-Konto: Globaler Administrator, Cloud-Anwendungsadministrator, Anwendungsadministrator oder Besitzer des Dienstprinzips.

Zugriff auf Azure AD

Schritte

1. Melden Sie sich an bei ["Azure-Portal"](#) .
2. Navigieren Sie zu ["Azure Active Directory"](#) .
3. Wählen ["Unternehmensanwendungen"](#) .

Erstellen Sie Unternehmensanwendungen und speichern Sie die StorageGRID SSO-Konfiguration

Um die SSO-Konfiguration für Azure in StorageGRID zu speichern, müssen Sie mit Azure eine Unternehmensanwendung für jeden Admin-Knoten erstellen. Sie kopieren die URLs der Verbundmetadaten aus Azure und fügen sie in die entsprechenden Felder **URL der Verbundmetadaten** auf der StorageGRID Single-Sign-On-Seite ein.

Schritte

1. Wiederholen Sie die folgenden Schritte für jeden Admin-Knoten.
 - a. Wählen Sie im Bereich „Azure Enterprise-Anwendungen“ **Neue Anwendung** aus.
 - b. Wählen Sie **Eigene Anwendung erstellen**.
 - c. Geben Sie als Namen den **Namen der Unternehmensanwendung** ein, den Sie aus der Tabelle mit den Admin-Knotendetails auf der StorageGRID Single-Sign-On-Seite kopiert haben.
 - d. Lassen Sie das Optionsfeld **Alle anderen Anwendungen integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie)** aktiviert.
 - e. Wählen Sie **Erstellen**.
 - f. Wählen Sie den Link **Erste Schritte** in **2. Setzen Sie das Feld „Single Sign-On einrichten“** ein oder wählen Sie den Link **Single Sign-On** im linken Rand aus.
 - g. Wählen Sie das Feld **SAML** aus.
 - h. Kopieren Sie die **App Federation Metadata Url**, die Sie unter **Schritt 3 SAML-Signaturzertifikat** finden.
 - i. Gehen Sie zur StorageGRID Single Sign-On-Seite und fügen Sie die URL in das Feld **Federation metadata URL** 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

StorageGRID Single Sign-On-Seite **Speichern** aus.

Laden Sie SAML-Metadaten für jeden Admin-Knoten herunter

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

Schritte

1. Wiederholen Sie diese Schritte für jeden Admin-Knoten.
 - a. Sign in bei StorageGRID an.
 - b. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Einmaliges Anmelden**.
 - c. Wählen Sie die Schaltfläche aus, um die SAML-Metadaten für diesen Admin-Knoten herunterzuladen.
 - d. Speichern Sie die Datei, die Sie in Azure AD hochladen.

Laden Sie SAML-Metadaten in jede Unternehmensanwendung hoch

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

Schritte

1. Kehren Sie zum Azure-Portal zurück.
2. Wiederholen Sie diese Schritte für jede Unternehmensanwendung:



Möglicherweise müssen Sie die Seite „Unternehmensanwendungen“ aktualisieren, um die Anwendungen anzuzeigen, die Sie zuvor zur Liste hinzugefügt haben.

- a. Gehen Sie zur Eigenschaftenseite der Unternehmensanwendung.
 - b. Setzen Sie **Zuweisung erforderlich** auf **Nein** (es sei denn, Sie möchten Zuweisungen separat konfigurieren).
 - c. Gehen Sie zur Seite „Single Sign-On“.
 - d. Schließen Sie die SAML-Konfiguration ab.
 - e. Wählen Sie die Schaltfläche **Metadatendatei hochladen** und wählen Sie die SAML-Metadatendatei aus, die Sie für den entsprechenden Admin-Knoten heruntergeladen haben.
 - f. Nachdem die Datei geladen wurde, wählen Sie **Speichern** und dann **X**, um den Bereich zu schließen. Sie werden zur Seite „Single Sign-On mit SAML einrichten“ zurückgeleitet.
3. Befolgen Sie die Schritte in ["Sandbox-Modus verwenden"](#) um jede Anwendung zu testen.

Erstellen Sie Service Provider (SP)-Verbindungen in PingFederate

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

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **Ping Federate** als SSO-Typ ausgewählt.
- Der **Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Sehen ["Sandbox-Modus verwenden"](#).

- Sie haben die * SP Verbindungs-ID* für jeden Admin-Knoten in Ihrem System. Sie finden diese Werte in der Detailtabelle „Admin-Knoten“ auf der StorageGRID Single-Sign-On-Seite.
- Sie haben die **SAML-Metadaten** für jeden Admin-Knoten in Ihrem System heruntergeladen.
- Sie haben Erfahrung mit der Erstellung von SP Verbindungen im PingFederate Server.
- Sie haben
die https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html [Referenzhandbuch für Administratoren"] für PingFederate Server. Die PingFederate-Dokumentation bietet detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben die "[Administratorberechtigung](#)" für PingFederate Server.

Informationen zu diesem Vorgang

Diese Anweisungen fassen zusammen, 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. Ausführliche Anweisungen zu Ihrer Version finden Sie in der Dokumentation zum PingFederate-Server.

Erfüllen Sie die Voraussetzungen in PingFederate

Bevor Sie die SP Verbindungen erstellen können, die Sie für StorageGRID verwenden, müssen Sie die erforderlichen Aufgaben in PingFederate abschließen. Sie verwenden die Informationen aus diesen Voraussetzungen, wenn Sie die SP Verbindungen konfigurieren.

Datenspeicher erstellen

Erstellen Sie, falls noch nicht geschehen, einen Datenspeicher, um PingFederate mit dem AD FS-LDAP-Server zu verbinden. Verwenden Sie die Werte, die Sie verwendet haben, "[Konfigurieren der Identitätsföderation](#)" im StorageGRID.

- **Typ:** Verzeichnis (LDAP)
- **LDAP-Typ:** Active Directory
- **Name des binären Attributs:** Geben Sie **objectGUID** auf der Registerkarte „LDAP-Binärattribute“ genau wie angezeigt ein.

Erstellen Sie einen Validator für Kennwortanmeldeinformationen

Erstellen Sie einen Kennwort-Anmeldeinformationsvalidator, sofern Sie dies noch nicht getan haben.

- **Typ:** LDAP-Benutzername-Passwort-Anmeldeinformationsvalidator
- **Datenspeicher:** Wählen Sie den von Ihnen erstellten Datenspeicher aus.
- **Suchbasis:** Geben Sie Informationen aus LDAP ein (z. B. DC=saml,DC=sgws).
- **Suchfilter:** sAMAccountName=\${username}
- **Umfang:** Teilbaum

IdP-Adapterinstanz erstellen

Erstellen Sie eine IdP-Adapterinstanz, falls Sie dies noch nicht getan haben.

Schritte

1. Gehen Sie zu **Authentifizierung > Integration > IdP-Adapter**.

2. Wählen Sie **Neue Instanz erstellen**.
3. Wählen Sie auf der Registerkarte „Typ“ **HTML-Formular-IdP-Adapter** aus.
4. Wählen Sie auf der Registerkarte „IdP-Adapter“ die Option „Neue Zeile zu ‚Credential Validators‘ hinzufügen“ aus.
5. Wählen Sie die [Kennwort-Anmeldeinformationsvalidator](#) Sie erstellt haben.
6. Wählen Sie auf der Registerkarte „Adapterattribute“ das Attribut „**Benutzername**“ für „**Pseudonym**“ aus.
7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

Erstellen oder importieren Sie das Signaturzertifikat, sofern Sie dies noch nicht getan haben.

Schritte

1. Gehen Sie zu **Sicherheit > Signatur- und Entschlüsselungsschlüssel und -zertifikate**.
2. Erstellen oder importieren Sie das Signaturzertifikat.

Erstellen einer SP Verbindung in PingFederate

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



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine SP Verbindung erstellen, damit sich Benutzer sicher bei jedem Knoten an- und abmelden können. Verwenden Sie diese Anweisungen, um die erste SP Verbindung herzustellen. Gehen Sie dann zu [Erstellen Sie zusätzliche SP Verbindungen](#) um alle zusätzlichen Verbindungen herzustellen, 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 **Für diese Verbindung keine Vorlage verwenden**.
4. Wählen Sie **Browser-SSO-Profile** und **SAML 2.0** als Protokoll.

SP Metadaten importieren

Schritte

1. Wählen Sie auf der Registerkarte „Metadaten importieren“ die Option „Datei“ aus.
2. Wählen Sie die SAML-Metadatendatei aus, die Sie von der StorageGRID Single-Sign-On-Seite für den Admin-Knoten heruntergeladen haben.
3. Überprüfen Sie die Metadatenzusammenfassung und die auf der Registerkarte „Allgemeine Informationen“ bereitgestellten Informationen.

Die Entitäts-ID des Partners und der Verbindungsname werden auf die StorageGRID SP Verbindungs-ID eingestellt. (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 des einmaligen Anmeldens im 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-initiiertes SSO*, * SP-initiales SLO*, * IdP-initiiertes SSO* und * IdP-initiiertes SLO* aus.
3. Wählen Sie **Weiter**.
4. Nehmen Sie auf der Registerkarte „Assertion Lifetime“ keine Änderungen vor.
5. Wählen Sie auf der Registerkarte „Assertion-Erstellung“ die Option „Assertion-Erstellung konfigurieren“ aus.
 - a. Wählen Sie auf der Registerkarte „Identitätszuordnung“ **Standard** aus.
 - b. Verwenden Sie auf der Registerkarte „Attributvertrag“ **SAML_SUBJECT** als Attributvertrag und das importierte, nicht angegebene Namensformat.
6. Wählen Sie zum Verlängern des Vertrags **Löschen**, um den `urn:oid`, das nicht verwendet wird.

Adapterinstanz zuordnen

Schritte

1. Wählen Sie auf der Registerkarte „Zuordnung der Authentifizierungsquelle“ die Option „Neue Adapterinstanz zuordnen“ aus.
2. Wählen Sie auf der Registerkarte Adapterinstanz die Option **Adapterinstanz** Sie erstellt haben.
3. Wählen Sie auf der Registerkarte „Zuordnungsmethode“ die Option „Zusätzliche 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 **Datenspeicher** Sie haben hinzugefügt.
6. Gehen Sie auf der Registerkarte „LDAP-Verzeichnissuche“ wie folgt vor:
 - Geben Sie den **Basis-DN** ein, der genau mit dem Wert übereinstimmen sollte, den Sie in StorageGRID für den LDAP-Server eingegeben haben.
 - Wählen Sie als Suchbereich **Unterbaum** aus.
 - Suchen Sie für die Stammobjektklasse nach einem der folgenden Attribute und fügen Sie es hinzu: **objectGUID** oder **userPrincipalName**.
7. Wählen Sie auf der Registerkarte „LDAP-Binärattribut-Kodierungstypen“ **Base64** für das Attribut **objectGUID** aus.
8. Geben Sie auf der Registerkarte „LDAP-Filter“ **sAMAccountName=\${username}** ein.
9. Wählen Sie auf der Registerkarte „Attribute Contract Fulfillment“ aus der Dropdown-Liste „Quelle“ die Option „LDAP (Attribut)“ und wählen Sie aus der Dropdown-Liste „Wert“ entweder **objectGUID** oder **userPrincipalName** aus.
10. Überprüfen und speichern Sie die Attributquelle.
11. Wählen Sie auf der Registerkarte „Failsave-Attributquelle“ die Option „SSO-Transaktion abbrechen“ aus.
12. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**.

13. Wählen Sie **Fertig**.

Konfigurieren der Protokolleinstellungen

Schritte

1. Wählen Sie auf der Registerkarte * SP -Verbindung* > **Browser-SSO** > **Protokolleinstellungen** die Option **Protokolleinstellungen konfigurieren**.
2. Akzeptieren Sie auf der Registerkarte Assertion Consumer Service URL die Standardwerte, die aus den StorageGRID SAML-Metadaten importiert wurden (**POST** für Binding und `/api/saml-response` für Endpunkt-URL).
3. Akzeptieren Sie auf der Registerkarte SLO-Service-URLs die Standardwerte, die aus den StorageGRID SAML-Metadaten importiert wurden (**REDIRECT** für Binding und `/api/saml-logout` für die Endpunkt-URL).
4. Deaktivieren Sie auf der Registerkarte „Zulässige SAML-Bindungen“ die Optionen „**ARTIFACT**“ und „**SOAP**“. Nur **POST** und **REDIRECT** sind erforderlich.
5. Lassen Sie auf der Registerkarte „Signaturrichtlinie“ die Kontrollkästchen **Signatur von Authentifizierungsanforderungen erforderlich** und **Assertion immer signieren** aktiviert.
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 Browser-SSO-Einstellungen zu speichern.

Konfigurieren der Anmeldeinformationen

Schritte

1. Wählen Sie auf der Registerkarte „SP -Verbindung“ die Option „Anmeldeinformationen“ aus.
2. Wählen Sie auf der Registerkarte „Anmeldeinformationen“ die Option „Anmeldeinformationen konfigurieren“ aus.
3. Wählen Sie die [Signaturzertifikat](#) Sie haben erstellt oder importiert.
4. Wählen Sie **Weiter**, um zu **Einstellungen für die Signaturüberprüfung verwalten** zu gelangen.
 - a. Wählen Sie auf der Registerkarte „Vertrauensmodell“ die Option „Unverankert“ aus.
 - b. Überprüfen Sie auf der Registerkarte „Signaturüberprüfungszertifikat“ die Informationen zum Signaturzertifikat, die aus den StorageGRID SAML-Metadaten importiert wurden.
5. Überprüfen 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 SP Verbindungen zu erstellen, die Sie für jeden Admin-Knoten in Ihrem Raster benötigen. Sie laden für jede Kopie neue Metadaten hoch.



Die SP Verbindungen für verschiedene Admin-Knoten verwenden identische Einstellungen, mit Ausnahme der Entitäts-ID, der Basis-URL, der Verbindungs-ID, des Verbindungsnamens, der Signaturüberprüfung und der SLO-Antwort-URL des Partners.

Schritte

1. Wählen Sie **Aktion** > **Kopieren**, um für jeden zusätzlichen Admin-Knoten eine Kopie der ursprünglichen 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 Metadatenfile aus, die dem Admin-Knoten entspricht:
 - a. Wählen Sie **Aktion > Mit Metadaten aktualisieren**.
 - 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 > Assertionserstellung konfigurieren > Attributvertrag**.
 - c. Löschen Sie den Eintrag für **urn:oid**.
 - d. Wählen Sie **Speichern**.

Deaktivieren der einmaligen Anmeldung

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .

Schritte

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

Die Single Sign-On-Seite wird angezeigt.

2. Wählen Sie die Option **Deaktiviert**.
3. Wählen Sie **Speichern**.

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

4. Wählen Sie **OK**.

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

Deaktivieren und aktivieren Sie Single Sign-On für einen Admin-Knoten vorübergehend.

Wenn das Single Sign-On-System (SSO) ausfällt, können Sie sich möglicherweise nicht beim Grid Manager anmelden. In diesem Fall können Sie SSO für einen Admin-Knoten vorübergehend deaktivieren und wieder aktivieren. Um SSO zu deaktivieren und anschließend wieder zu aktivieren, müssen Sie auf die Befehlsshell des Knotens

zugreifen.

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen" .
- Sie haben die `Passwords.txt` Datei.
- Sie kennen das Passwort für den lokalen Root-Benutzer.

Informationen zu diesem Vorgang

Nachdem Sie SSO für einen Admin-Knoten deaktiviert haben, können Sie sich als lokaler Root-Benutzer beim Grid Manager anmelden. Um Ihr StorageGRID -System zu sichern, müssen Sie die Befehlsshell des Knotens verwenden, um SSO auf dem Admin-Knoten wieder zu aktivieren, sobald Sie sich abmelden.



Das Deaktivieren von SSO für einen Admin-Knoten hat keine Auswirkungen auf die SSO-Einstellungen für andere Admin-Knoten im Raster. Das Kontrollkästchen **SSO aktivieren** auf der Single Sign-On-Seite im Grid Manager bleibt aktiviert und alle vorhandenen SSO-Einstellungen bleiben erhalten, sofern Sie sie nicht aktualisieren.

Schritte

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

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#` .

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

Eine Meldung weist darauf hin, dass der Befehl nur für diesen Admin-Knoten gilt.

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

Eine Meldung weist darauf hin, dass die einmalige Anmeldung auf dem Knoten deaktiviert ist.

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

Die Anmeldeseite des Grid Managers wird jetzt angezeigt, da SSO deaktiviert wurde.

5. Sign in .
6. Wenn Sie SSO vorübergehend deaktiviert haben, weil Sie die SSO-Konfiguration korrigieren mussten:
 - a. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Einmaliges Anmelden**.
 - b. Ändern Sie die falschen oder veralteten SSO-Einstellungen.
 - c. Wählen Sie **Speichern**.

Wenn Sie auf der Single Sign-On-Seite „Speichern“ auswählen, wird SSO für das gesamte Raster automatisch wieder aktiviert.

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

Manager zugreifen mussten:

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

Eine Meldung weist darauf hin, dass der Befehl nur für diesen Admin-Knoten gilt.

Bestätigen Sie, dass Sie SSO aktivieren möchten.

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

- Starten Sie den Grid-Knoten neu: `reboot`

8. Greifen Sie über einen Webbrowser vom selben Admin-Knoten aus auf den Grid Manager zu.
9. Vergewissern Sie sich, dass die StorageGRID Sign in angezeigt wird und dass Sie Ihre SSO-Anmeldeinformationen eingeben müssen, um auf den Grid Manager zuzugreifen.

Copyright-Informationen

Copyright © 2025 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.