



Single Sign On (SSO) verwenden

StorageGRID

NetApp
March 12, 2025

Inhalt

Single Sign On (SSO) verwenden	1
Konfigurieren Sie Single Sign-On	1
Funktionsweise von Single Sign-On	1
Voraussetzungen und Überlegungen für Single Sign-On	4
Anforderungen an Identitätsanbieter	4
Serverzertifikate-Anforderungen	5
Port-Anforderungen	5
Bestätigen Sie, dass verbundene Benutzer sich anmelden können	6
Verwenden Sie den Sandbox-Modus	7
Zugriff auf den Sandbox-Modus	8
Geben Sie die Daten des Identitätsanbieters ein	9
Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen	13
Testen Sie SSO-Verbindungen	14
Aktivieren Sie Single Sign On	17
Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS	17
Erstellen Sie mit Windows PowerShell ein Vertrauensverhältnis, das sich auf die Kunden stützt	18
Erstellen Sie durch den Import von Federationmetadaten ein Vertrauen von Kunden	19
Erstellen Sie manuell ein Vertrauen der Vertrauensbasis	20
Erstellen von Enterprise-Applikationen in Azure AD	22
Zugriff auf Azure AD	23
Erstellen von Enterprise-Applikationen und Speichern von StorageGRID SSO-Konfiguration	23
Laden Sie für jeden Admin-Node SAML-Metadaten herunter	24
Hochladen von SAML-Metadaten in jede Enterprise-Applikation	24
Erstellen von SP-Verbindungen (Service Provider) in PingFederate	24
Alle Voraussetzungen in PingFederate	25
Erstellen Sie eine SP-Verbindung in PingFederate	26
Deaktivieren Sie Single Sign-On	29
Deaktivieren Sie die einmalige Anmeldung für einen Admin-Knoten vorübergehend und aktivieren Sie sie erneut	30

Single Sign On (SSO) verwenden

Konfigurieren Sie Single Sign-On

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

Funktionsweise von Single Sign-On

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

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

Melden Sie sich an, wenn SSO aktiviert ist

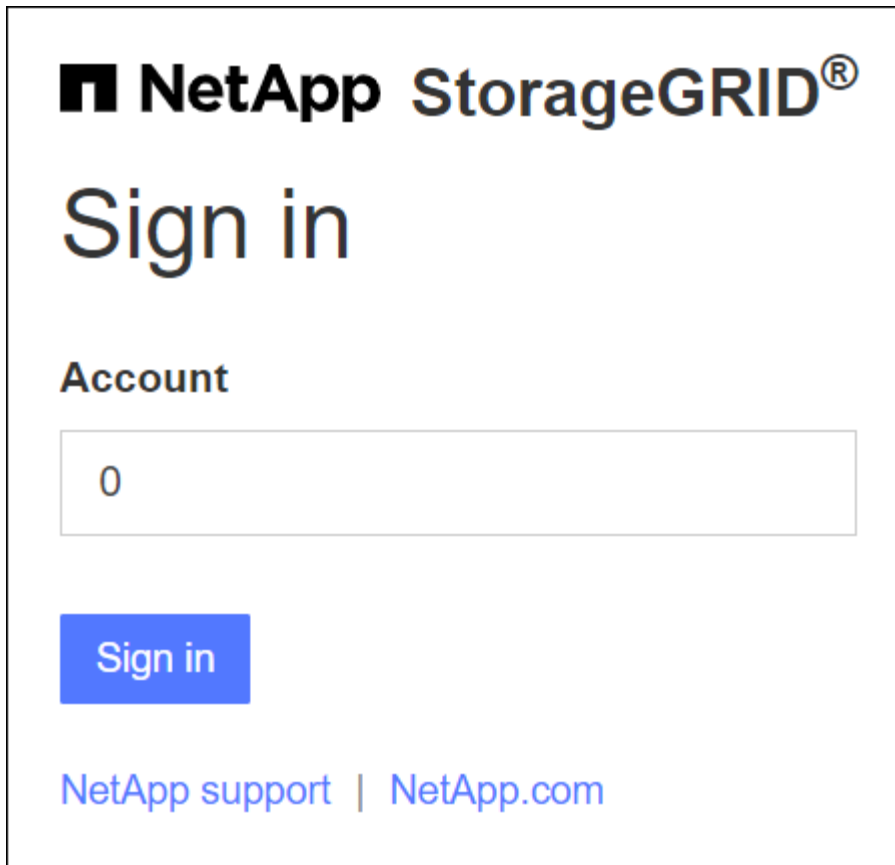
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur SSO-Seite Ihres Unternehmens weitergeleitet, um Ihre Anmeldedaten zu validieren.

Schritte

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

Die Seite StorageGRID-Anmeldung wird angezeigt.

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



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



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

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

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

Sign in with your organizational account

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

Falls Ihre SSO-Anmeldedaten korrekt sind:

- a. Der Identitäts-Provider (IdP) stellt eine Authentifizierungsantwort für StorageGRID bereit.
- b. StorageGRID validiert die Authentifizierungsantwort.
- c. Wenn die Antwort gültig ist und Sie zu einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen gehören, werden Sie je nach ausgewähltem Konto beim Grid Manager oder dem Mandanten-Manager angemeldet.



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

5. Wenn Sie über ausreichende Berechtigungen verfügen, können Sie optional auf andere Admin-Nodes zugreifen oder auf den Grid Manager oder den Tenant Manager zugreifen.

Sie müssen Ihre SSO-Anmeldedaten nicht erneut eingeben.

Abmelden, wenn SSO aktiviert ist

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

Schritte

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

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

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



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

Voraussetzungen und Überlegungen für Single Sign-On

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

Anforderungen an Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

- Active Directory Federation Service (AD FS)
- 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-Service, den Sie für die Identitätsföderation verwenden, steuert, welcher SSO-Typ Sie implementieren können.

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

AD-FS-Anforderungen

Sie können eine der folgenden Versionen von AD FS verwenden:

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



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

Zusätzlichen Anforderungen

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

Überlegungen zu Azure

Wenn Sie Azure als SSO-Typ verwenden und Benutzer über Hauptbenutzernamen verfügen, die den sAMAccountName nicht als Präfix verwenden, können Anmeldeprobleme auftreten, wenn StorageGRID seine Verbindung mit dem LDAP-Server verliert. Damit Benutzer sich anmelden können, müssen Sie die Verbindung zum LDAP-Server wiederherstellen.

Serverzertifikate-Anforderungen

Standardmäßig verwendet StorageGRID auf jedem Admin-Node ein Zertifikat der Managementoberfläche, um den Zugriff auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandanten-Management-API zu sichern. Wenn Sie Trusts (AD FS), Enterprise-Anwendungen (Azure) oder Service Provider Connections (PingFederate) für StorageGRID konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID-Anfragen.

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



Es wird nicht empfohlen, das Standardserverzertifikat eines Admin Node in einer Vertrauensstelle, einer Unternehmensanwendungen oder einer SP-Verbindung zu verwenden. Wenn der Knoten ausfällt und Sie ihn wiederherstellen, wird ein neues Standard-Serverzertifikat generiert. Bevor Sie sich beim wiederhergestellten Knoten anmelden können, müssen Sie das Vertrauensverhältnis der zu bestellenden Partei, die Enterprise-Anwendung oder die SP-Verbindung mit dem neuen Zertifikat aktualisieren.

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

Port-Anforderungen

Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten. Siehe "[Kontrolle des Zugriffs über externe Firewall](#)".

Bestätigen Sie, dass verbundene Benutzer sich anmelden können

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

Bevor Sie beginnen

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

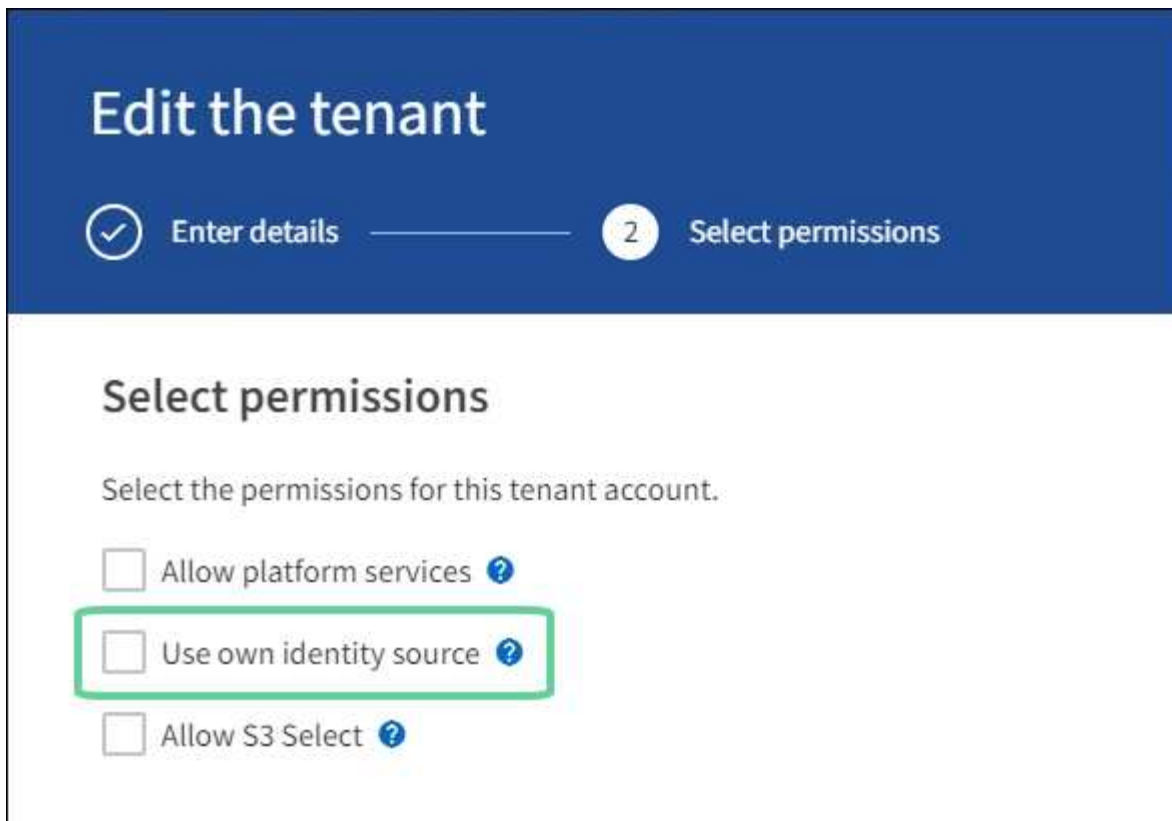
Schritte

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



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

- a. Melden Sie sich für jedes Mandantenkonto bei Tenant Manager an.
 - b. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
 - c. Bestätigen Sie, dass das Kontrollkästchen **Enable Identity Federation** nicht aktiviert ist.
 - d. Wenn dies der Fall ist, bestätigen Sie, dass keine föderierten Gruppen mehr für dieses Mandantenkonto benötigt werden, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.
2. Bestätigen Sie, dass ein verbundener Benutzer auf den Grid Manager zugreifen kann:
 - a. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Zugriffskontrolle** > **Admin-Gruppen** aus.
 - b. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
 - c. Abmelden.
 - d. Bestätigen Sie, dass Sie sich wieder bei Grid Manager als Benutzer in der föderierten Gruppe anmelden können.
 3. Wenn es bereits bestehende Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root-Zugriffsberechtigung anmelden kann:
 - a. Wählen Sie im Grid Manager die Option **MITERS** aus.
 - b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen** > **Bearbeiten**.
 - c. Wählen Sie auf der Registerkarte Details eingeben die Option **Weiter**.
 - d. Wenn das Kontrollkästchen **eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern** aus.



Die Seite Mandant wird angezeigt.

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

Verwandte Informationen

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

Verwenden Sie den Sandbox-Modus

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 wieder in den Sandbox-Modus wechseln, wenn Sie die Konfiguration ändern oder erneut testen müssen.

Bevor Sie beginnen

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

- Sie haben die "[Root-Zugriffsberechtigung](#)".
- Sie haben eine Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für die Identitätsföderation **LDAP-Diensttyp** haben Sie entweder Active Directory oder Azure ausgewählt, basierend auf dem SSO-Identitäts-Provider, den Sie verwenden möchten.

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

Über diese Aufgabe

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

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

Damit StorageGRID (der Service-Provider) und der SSO-Identitäts-Provider 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-Node ein Vertrauensverhältnis (AD FS), eine Enterprise-Applikation (Azure) oder einen Serviceprovider (PingFederate) zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, um SSO zu aktivieren.

Im Sandbox-Modus ist es einfach, diese Rückkehrkonfiguration durchzuführen und alle Einstellungen zu testen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht mit SSO anmelden.

Zugriff auf den Sandbox-Modus

Schritte

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

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

Single Sign-on

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

SSO status  Disabled Sandbox Mode Enabled

Save



Wenn die SSO-Statusoptionen nicht angezeigt werden, vergewissern Sie sich, dass Sie den Identitätsanbieter als föderierte Identitätsquelle konfiguriert haben. Siehe "[Voraussetzungen und Überlegungen für Single Sign-On](#)".

2. Wählen Sie **Sandbox-Modus**.

Der Abschnitt „Identitätsanbieter“ wird angezeigt.

Geben Sie die Daten des Identitätsanbieters ein

Schritte

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

Active Directory

- a. Geben Sie den **Federationsdienstnamen** für den Identitätsanbieter ein, genau wie er im Active Directory Federation Service (AD FS) angezeigt wird.



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

- b. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.

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

Wenn Sie diese Einstellung auswählen, kopieren Sie den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

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



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

- c. Geben Sie im Abschnitt „Einvertrauende Partei“ die **bezeichner der bevertrauenden Partei** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jedes Vertrauen der betreffenden Partei in AD FS verwenden.

- Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder ``StorageGRID`` ein.
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge `[HOSTNAME]` in die Kennung ein. ``SG-[HOSTNAME]`` Beispiel: . Dadurch wird eine Tabelle erstellt, die die ID der betreffenden Partei für jeden Admin-Knoten in Ihrem System anhand des Hostnamen des Knotens anzeigt.



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

- d. Wählen Sie **Speichern**.

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



Azure

a. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.

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

Wenn Sie diese Einstellung auswählen, kopieren Sie den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

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



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

b. Geben Sie im Abschnitt Enterprise-Anwendung den **Enterprise-Anwendungsnamen** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für die einzelnen Enterprise-Applikationen in Azure AD verwenden.

- Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder ``StorageGRID`` ein.
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge `[HOSTNAME]` in die Kennung ein. ``SG-[HOSTNAME]`` Beispiel: `.`` Dadurch wird eine Tabelle mit dem Namen einer Enterprise-Anwendung für jeden Admin-Knoten in Ihrem System generiert, basierend auf dem Hostnamen des Knotens.



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

c. Führen Sie die Schritte unter "[Erstellen von Enterprise-Applikationen in Azure AD](#)" aus, um für jeden in der Tabelle aufgeführten Admin-Node eine Unternehmensanwendungen zu erstellen.

d. Kopieren Sie in Azure AD die Federations-Metadaten-URL für jede Enterprise-Applikation. Fügen Sie dann diese URL in das entsprechende Feld **Federation Metadaten URL** in StorageGRID ein.

e. Nachdem Sie eine URL für die Federation Metadaten für alle Administratorknoten kopiert und eingefügt haben, wählen Sie **Speichern**.

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



PingFederate

a. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen

sendet.

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

Wenn Sie diese Einstellung auswählen, kopieren Sie den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

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



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

b. Geben Sie im Abschnitt Dienstanbieter (SP) die **SP-Verbindungs-ID** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede SP-Verbindung in PingFederate verwenden.

- Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder ``StorageGRID`` ein.
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge `[HOSTNAME]` in die Kennung ein. ``SG-[HOSTNAME]`` Beispiel: `.``. Dadurch wird basierend auf dem Hostnamen des Node eine Tabelle mit der SP-Verbindungs-ID für jeden Admin-Node im System generiert.



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


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

Verwenden Sie das folgende Format:

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

d. Wählen Sie **Speichern**.

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

Save 

Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen

Wenn die Konfiguration gespeichert ist, wird die Bestätigungsmeldung des Sandbox-Modus angezeigt. Dieser Hinweis bestätigt, dass der Sandbox-Modus jetzt aktiviert ist und eine Übersicht enthält.

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

Führen Sie diese Schritte aus, um Trusts (Active Directory) von Vertrauensstellen (Vertrauensstellen), vollständige Enterprise-Applikationen (Azure) zu konfigurieren oder SP-Verbindungen (PingFederate) zu konfigurieren.

Active Directory

Schritte

1. Wechseln Sie zu Active Directory Federation Services (AD FS).
2. Erstellen Sie eine oder mehrere Treuhänder für StorageGRID, die sich auf der StorageGRID Single Sign-On-Seite in der Tabelle befinden.

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

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

Azure

Schritte

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

PingFederate

Schritte

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

Für jeden in der Tabelle aufgeführten Admin-Node müssen Sie 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 korrekt konfiguriert sind.

Active Directory

Schritte

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

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

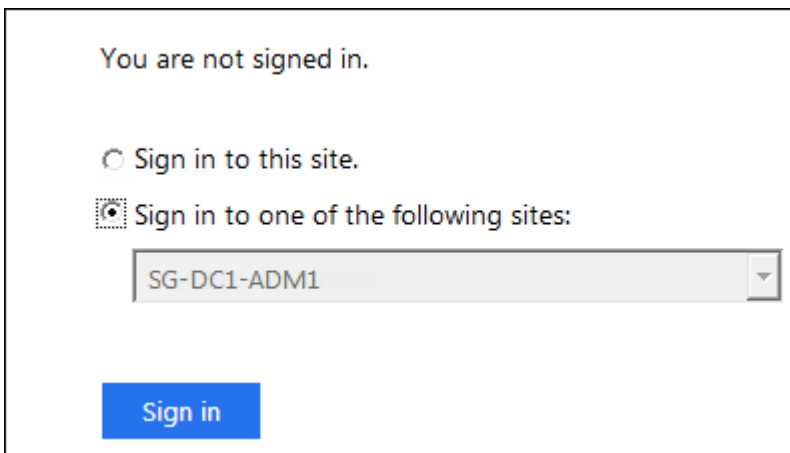
Sandbox mode

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

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



You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

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

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

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

überprüfen.

Azure

Schritte

1. Wechseln Sie im Azure-Portal zur Seite Single Sign On.
2. Wählen Sie **Diese Anwendung testen**.
3. Geben Sie die Anmeldeinformationen eines föderierten Benutzers ein.
 - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

✓ 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-Node in Ihrem Raster zu überprüfen.

PingFederate

Schritte

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

Wählen Sie jeweils einen Link aus, und testen Sie ihn.

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 föderierten Benutzers ein.
 - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

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

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

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

Aktivieren Sie Single Sign On

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



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

Schritte

1. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Single Sign-On**.
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 über denselben Computer auf StorageGRID zugreifen, mit dem Sie auf Azure zugreifen, stellen Sie sicher, dass der Azure-Portal-Benutzer auch ein autorisierter StorageGRID-Benutzer ist (ein Benutzer in einer föderierten Gruppe, die in StorageGRID importiert wurde). Oder melden Sie sich vom Azure-Portal ab, bevor Sie sich bei StorageGRID anmelden.

Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS

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

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ **AD FS** ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe "[Verwenden Sie den Sandbox-Modus](#)".
- Sie kennen den vollständig qualifizierten Domännennamen (oder die IP-Adresse) und die vertrauenden Partei-ID für jeden Admin-Knoten in Ihrem System. Diese Werte finden Sie in der Detailtabelle Admin Nodes auf der StorageGRID Single Sign-On-Seite.



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

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

Über diese Aufgabe

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

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

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

Schritte

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

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

- Geben Sie für *Admin_Node_Identifier* die ID der aussetzenden Partei für den Admin-Knoten genau so ein, wie sie auf der Seite Single Sign-On angezeigt wird. `SG-DC1-ADM1` Beispiel: .
 - Geben Sie für *Admin_Node_FQDN* den vollständig qualifizierten Domännennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)
3. Wählen Sie im Windows Server Manager **Tools > AD FS Management** aus.

Das AD FS Management Tool wird angezeigt.

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

Die Liste der Vertrauensstellen wird angezeigt.

5. Fügen Sie eine Zugriffskontrollrichtlinie zum neu erstellten Vertrauen der Vertrauensstellenden Partei hinzu:
 - a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
 - b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
 - c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
 - d. Wählen Sie **Anwenden**, und wählen Sie **OK**
6. Fügen Sie dem neu erstellten Treuhandgesellschaft eine Richtlinie zur Ausstellung von Forderungen hinzu:

- a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
- b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
- c. Wählen Sie **Regel hinzufügen**.
- d. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
- e. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

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

- f. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
 - g. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
 - h. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
 - i. Wählen Sie **Fertig**, und wählen Sie **OK**.
7. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.
- a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
 - b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifizier** und **Signatur** ausgefüllt sind.

Wenn die Metadaten fehlen, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie die Werte manuell ein.

8. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
9. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Anweisungen finden Sie unter ["Verwenden Sie den Sandbox-Modus"](#).

Erstellen Sie durch den Import von Federationmetadaten ein Vertrauen von Kunden

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

Schritte

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

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

Geben Sie für `Admin_Node_FQDN` den vollständig qualifizierten Domännennamen für denselben Admin-

Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

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



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

- Fügen Sie eine Antragsregel hinzu:

- Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
- Wählen Sie **Regel hinzufügen**:
- Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
- Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

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

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

- Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.

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

Wenn die Metadaten fehlen, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie die Werte manuell ein.

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

- Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Anweisungen finden Sie unter ["Verwenden Sie den Sandbox-Modus"](#) .

Erstellen Sie manuell ein Vertrauen der Vertrauensbasis

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

Schritte

- Wählen Sie im Windows Server Manager **Tools** aus, und wählen Sie dann **AD FS Management** aus.

2. Wählen Sie unter Aktionen **Vertrauensstellung hinzufügen** aus.
3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus, und wählen Sie **Start**.
4. Wählen Sie **Geben Sie Daten über den Besteller manuell** ein, und wählen Sie **Weiter**.
5. Schließen Sie den Assistenten für Vertrauen in die vertrauende Partei ab:

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

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

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

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

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

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

Admin_Node_Identifizier

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

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

Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.



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

6. Um den Assistenten für die Antragsregel zu starten, wählen Sie **Regel hinzufügen**:
 - a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
 - b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID zu Name ID** oder **UPN zu Name ID**.
 - c. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
 - d. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
 - e. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.

- f. Wählen Sie **Fertig**, und wählen Sie **OK**.
7. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
8. Konfigurieren Sie auf der Registerkarte **Endpunkte** den Endpunkt für einzelne Abmeldung (SLO):
 - a. Wählen Sie **SAML hinzufügen**.
 - b. Wählen Sie **Endpunkttyp > SAML Logout**.
 - c. Wählen Sie **Bindung > Umleiten**.
 - d. Geben Sie im Feld **Trusted URL** die URL ein, die für Single Logout (SLO) von diesem Admin-Node verwendet wird:

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

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

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



Die Verwendung des Standardzertifikats des Admin-Knotens (`server.crt`) wird nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat neu generiert, wenn Sie den Knoten wiederherstellen, und Sie müssen das Vertrauen der Vertrauensstelle aktualisieren.

- b. Wählen Sie **Anwenden**, und wählen Sie **OK**.

Die Eigenschaften der zu vertrauenden Partei werden gespeichert und geschlossen.

10. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
11. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Anweisungen finden Sie unter ["Verwenden Sie den Sandbox-Modus"](#).

Erstellen von Enterprise-Applikationen in Azure AD

Mit Azure AD erstellen Sie für jeden Admin-Node in Ihrem System eine Enterprise-Applikation.

Bevor Sie beginnen

- Sie haben mit der Konfiguration der Single Sign-On-Funktion für StorageGRID begonnen und als SSO-Typ **Azure** ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe "[Verwenden Sie den Sandbox-Modus](#)".
- Sie haben den **Enterprise-Anwendungsnamen** für jeden Admin-Knoten in Ihrem System. Sie können diese Werte aus der Detailtabelle „Admin-Knoten“ auf der Seite „StorageGRID Single Sign-On“ kopieren.



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

- Sie haben Erfahrung beim Erstellen von Enterprise-Applikationen in Azure Active Directory.
- Sie verfügen über ein Azure Konto mit einem aktiven Abonnement.
- Im Azure-Konto verfügen Sie über eine der folgenden Rollen: Global Administrator, Cloud Application Administrator, Application Administrator oder Eigentümer des Service-Principal.

Zugriff auf Azure AD

Schritte

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

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

Um die SSO-Konfiguration für Azure in StorageGRID zu speichern, müssen Sie Azure verwenden, um für jeden Admin-Node eine Unternehmensanwendung zu erstellen. Sie kopieren die Federation Metadaten-URLs aus Azure und fügen sie in die entsprechenden Felder **Federation Metadaten-URL** auf der StorageGRID Single Sign-on-Seite ein.

Schritte

1. Wiederholen Sie die folgenden Schritte für jeden Admin-Node.
 - a. Wählen Sie im Fensterbereich Azure Enterprise-Anwendungen **Neue Anwendung** aus.
 - b. Wählen Sie **Erstellen Sie Ihre eigene Anwendung**.
 - c. Geben Sie für den Namen den **Enterprise-Anwendungsnamen** ein, den Sie aus der Tabelle Admin-Knoten Details auf der StorageGRID-Seite Single Sign-On kopiert haben.
 - d. Lassen Sie das * eine andere Anwendung integrieren, die Sie nicht in der Galerie finden (nicht-Galerie)* Optionsfeld ausgewählt.
 - e. Wählen Sie **Erstellen**.
 - f. Wählen Sie im **2 den Link *Get Started** aus. Aktivieren Sie das Feld Single Sign On*, oder wählen Sie den Link **Single Sign-On** im linken Rand.
 - g. Wählen Sie das Feld **SAML** aus.
 - h. Kopieren Sie die **App Federation Metadaten-URL**, die Sie unter **Step 3 SAML-Signierungszertifikat** finden können.

- i. Gehen Sie auf die Seite StorageGRID Single Sign-On und fügen Sie die URL in das Feld **Federation Metadaten-URL** ein, das dem von Ihnen verwendeten **Enterprise-Anwendungsnamen** entspricht.
2. Nachdem Sie für jeden Admin-Knoten eine Metadaten-URL für den Verbund eingefügt haben und alle weiteren erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, wählen Sie auf der Seite StorageGRID Single Sign-On die Option **Speichern** aus.

Laden Sie für jeden Admin-Node SAML-Metadaten herunter

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

Schritte

1. Wiederholen Sie diese Schritte für jeden Admin-Node.
 - a. Melden Sie sich über den Admin-Node bei StorageGRID an.
 - b. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Single Sign-On**.
 - c. Wählen Sie die Schaltfläche, um die SAML-Metadaten für diesen Admin-Node herunterzuladen.
 - d. Speichern Sie die Datei, die Sie in Azure AD hochladen möchten.

Hochladen von SAML-Metadaten in jede Enterprise-Applikation

Nach dem Herunterladen einer SAML-Metadatendatei für jeden StorageGRID-Admin-Node führen Sie die folgenden Schritte in Azure AD aus:

Schritte

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



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

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

Erstellen von SP-Verbindungen (Service Provider) in PingFederate

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

importieren Sie die SAML-Metadaten aus StorageGRID.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ * Ping föderate* ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe "[Verwenden Sie den Sandbox-Modus](#)".
- Sie haben die **SP-Verbindungs-ID** für jeden Admin-Knoten in Ihrem System. Diese Werte finden Sie in der Detailtabelle Admin Nodes auf der StorageGRID Single Sign-On-Seite.
- Sie haben die **SAML-Metadaten** für jeden Admin-Knoten in Ihrem System heruntergeladen.
- Sie haben Erfahrung beim Erstellen von SP-Verbindungen in PingFederate Server.
- Sie haben den "[Administrator's Reference Guide](#)" für PingFederate Server. Die PingFederate-Dokumentation bietet detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben den "[Administratorberechtigung](#)" für PingFederate Server.

Über diese Aufgabe

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

Alle Voraussetzungen in PingFederate

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

Datenspeicher erstellen

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

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

Passwortvalididator[[Password-Validator] erstellen

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

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

IdP-Adapterinstanz erstellen

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

Schritte

1. Gehen Sie zu **Authentifizierung > Integration > IdP-Adapter**.
2. Wählen Sie **Neue Instanz Erstellen**.
3. Wählen Sie auf der Registerkarte Typ die Option **HTML-Formular-IdP-Adapter** aus.
4. Wählen Sie auf der Registerkarte IdP-Adapter **Neue Zeile zu 'Credential Validators'** hinzufügen.
5. Wählen Sie die [Gültigkeitsprüfung für Kennwortausweise](#) erstellte aus.
6. Wählen Sie auf der Registerkarte Adapterattribute das Attribut **Benutzername** für **Pseudonym** aus.
7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

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

Schritte

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

Erstellen Sie eine SP-Verbindung in PingFederate

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



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

Wählen Sie den SP-Verbindungstyp

Schritte

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

Importieren der SP-Metadaten

Schritte

1. Wählen Sie auf der Registerkarte Metadaten importieren die Option **Datei**.
2. Wählen Sie die SAML-Metadatenfile, die Sie für den Admin-Node von der StorageGRID-Seite für Single Sign-On heruntergeladen haben.
3. Überprüfen Sie die Metadatenübersicht und die Informationen auf der Registerkarte Allgemeine

Informationen.

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

4. Wählen Sie **Weiter**.

Konfigurieren Sie SSO für den IdP-Browser

Schritte

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

Adapterinstanz zuordnen

Schritte

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

10. Überprüfen und speichern Sie dann die Attributquelle.
11. Wählen Sie auf der Registerkarte Attributquelle failsave die Option **SSO-Transaktion abbrechen** aus.
12. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**.
13. Wählen Sie * Fertig*.

Konfigurieren von Protokolleinstellungen

Schritte

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

Anmeldedaten konfigurieren

Schritte

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

Erstellen Sie zusätzliche SP-Verbindungen

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



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

Schritte

1. Wählen Sie **Aktion > Kopieren** aus, um für jeden zusätzlichen Admin-Node eine Kopie der anfänglichen SP-Verbindung zu erstellen.
2. Geben Sie die Verbindungs-ID und den Verbindungsnamen für die Kopie ein, und wählen Sie **Speichern**.
3. Wählen Sie die dem Admin-Node entsprechende Metadatendatei:
 - a. Wählen Sie **Aktion > Aktualisieren mit Metadaten**.
 - b. Wählen Sie **Datei auswählen** und laden Sie die Metadaten hoch.
 - c. Wählen Sie **Weiter**.
 - d. Wählen Sie **Speichern**.
4. Beheben Sie den Fehler aufgrund des nicht verwendeten Attributs:
 - a. Wählen Sie die neue Verbindung aus.
 - b. Wählen Sie **Browser-SSO konfigurieren > Assertion-Erstellung konfigurieren > Attributvertrag** aus.
 - c. Löschen Sie den Eintrag für **Urne:oid**.
 - d. Wählen Sie **Speichern**.

Deaktivieren Sie Single Sign-On

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

Bevor Sie beginnen

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

Schritte

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

Die Seite Single Sign-On wird angezeigt.

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

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

4. Wählen Sie **OK**.

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

Deaktivieren Sie die einmalige Anmeldung für einen Admin-Knoten vorübergehend und aktivieren Sie sie erneut

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

Bevor Sie beginnen

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

Über diese Aufgabe

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



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

Schritte

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

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

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

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

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

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

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

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

5. Melden Sie sich mit dem Benutzernamen root und dem Passwort des lokalen Root-Benutzers an.
6. Wenn Sie SSO vorübergehend deaktiviert haben, da Sie die SSO-Konfiguration korrigieren mussten:
 - a. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Single Sign-On**.

- b. Ändern Sie die falschen oder veralteten SSO-Einstellungen.
- c. Wählen Sie **Speichern**.

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

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

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

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

Bestätigen Sie, dass Sie SSO aktivieren möchten.

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

- Grid-Node neu booten: `reboot`

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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