Verwenden Sie Single Sign-On (SSO).

StorageGRID software

NetApp
October 21, 2025

Inhalt

Verwenden Sie Single Sign-On (SSO). . . . 1
- Konfigurieren der einmaligen Anmeldung . . . 1
  - So funktioniert Single Sign-On . . . 1
- Anforderungen und Überlegungen zur einmaligen Anmeldung . . . 4
  - Anforderungen an den Identitätsanbieter . . . 4
  - Serverzertifikatanforderungen . . . 5
  - Portanforderungen . . . 6
- Bestätigen, dass sich Verbundbenutzer anmelden können . . . 6
- Sandbox-Modus verwenden . . . 7
  - Zugriff auf den Sandbox-Modus . . . 8
  - Geben Sie die Details des Identitätsanbieters ein . . . 9
  - Konfigurieren von Vertrauensstellungen der vertrauenden Seite, Unternehmensanwendungen oder SP Verbindungen . . . 13
  - Testen Sie SSO-Verbindungen . . . 14
  - Aktivieren der einmaligen Anmeldung . . . 17
- Erstellen von Vertrauensstellungen der vertrauenden Seite in AD FS . . . 17
  - Erstellen einer Vertrauensstellung der vertrauenden Seite mithilfe von Windows PowerShell . . . 18
  - Erstellen einer Vertrauensstellung der vertrauenden Seite durch Importieren von Verbundmetadaten . . . 19
  - Manuelles Erstellen einer Vertrauensstellung der vertrauenden Seite . . . 20
- Erstellen von Unternehmensanwendungen in Azure AD . . . 22
  - Zugriff auf Azure AD . . . 23
  - Erstellen Sie Unternehmensanwendungen und speichern Sie die StorageGRID SSO-Konfiguration . . . 23
  - Laden Sie SAML-Metadaten für jeden Admin-Knoten herunter . . . 24
  - Laden Sie SAML-Metadaten in jede Unternehmensanwendung hoch . . . 24
- Erstellen Sie Service Provider (SP)-Verbindungen in PingFederate . . . 25
  - Erfüllen Sie die Voraussetzungen in PingFederate . . . 25
  - Erstellen einer SP Verbindung in PingFederate . . . 26
- Deaktivieren der einmaligen Anmeldung . . . 29
- Deaktivieren und aktivieren Sie Single Sign-On für einen Admin-Knoten vorübergehend. . . . 30

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

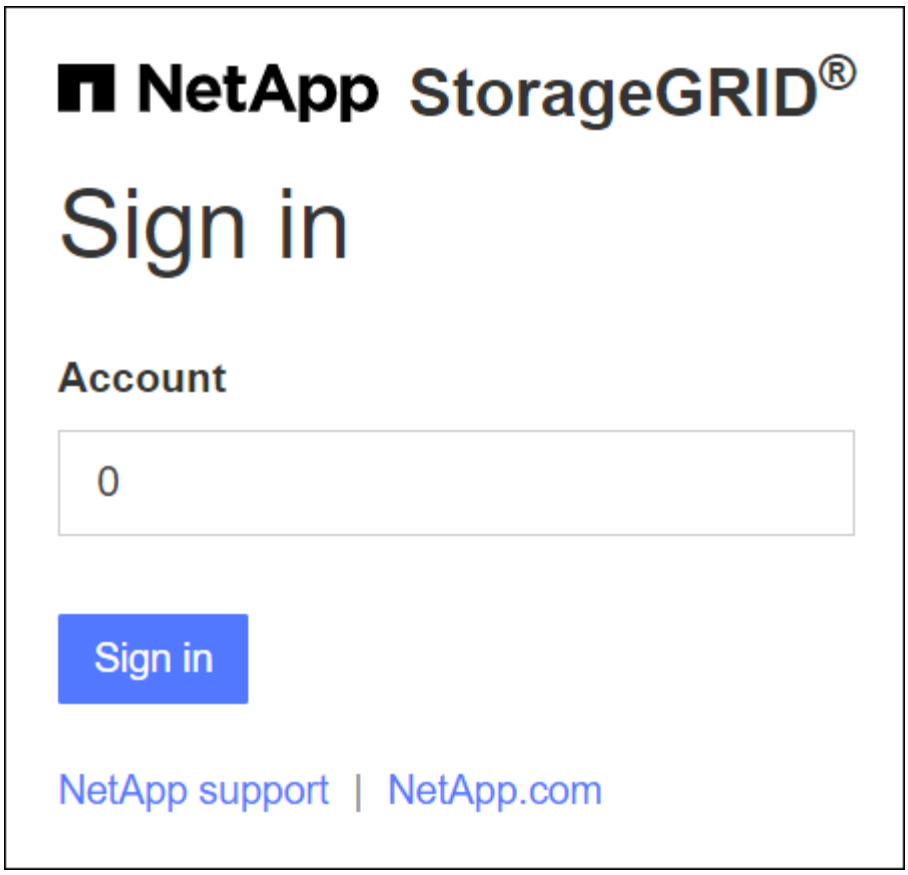
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur Validierung Ihrer Anmeldeinformationen auf die SSO-Seite Ihrer Organisation weitergeleitet.

Schritte

1. Geben Sie den vollqualifizierten Domänennamen 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:

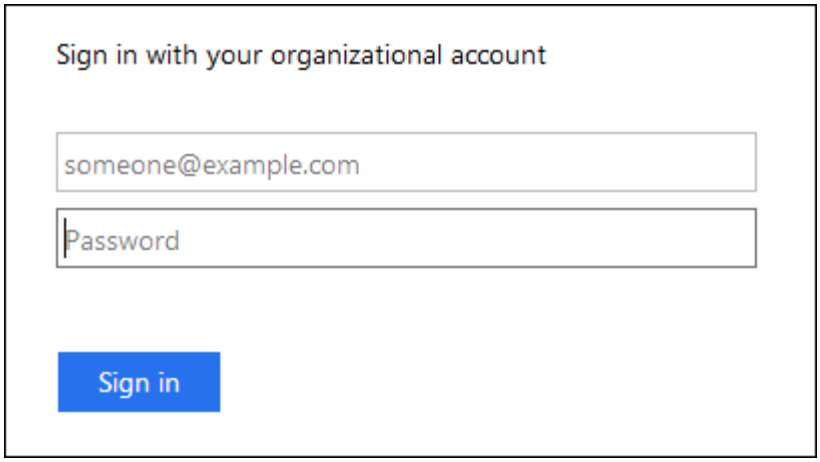


- Wenn Sie zuvor entweder auf den Grid Manager oder den Tenant Manager zugegriffen haben, werden Sie aufgefordert, ein aktuelles Konto auszuwählen oder eine Konto-ID einzugeben:

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

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



4. Sign in .

   Wenn Ihre SSO-Anmeldeinformationen korrekt sind:

   a. Der Identitätsanbieter (IdP) stellt StorageGRID eine Authentifizierungsantwort bereit.
   b. StorageGRID validiert die Authentifizierungsantwort.
   c. 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

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

Konfigurierter LDAP-Diensttyp	Optionen für SSO-Identitätsanbieter
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.

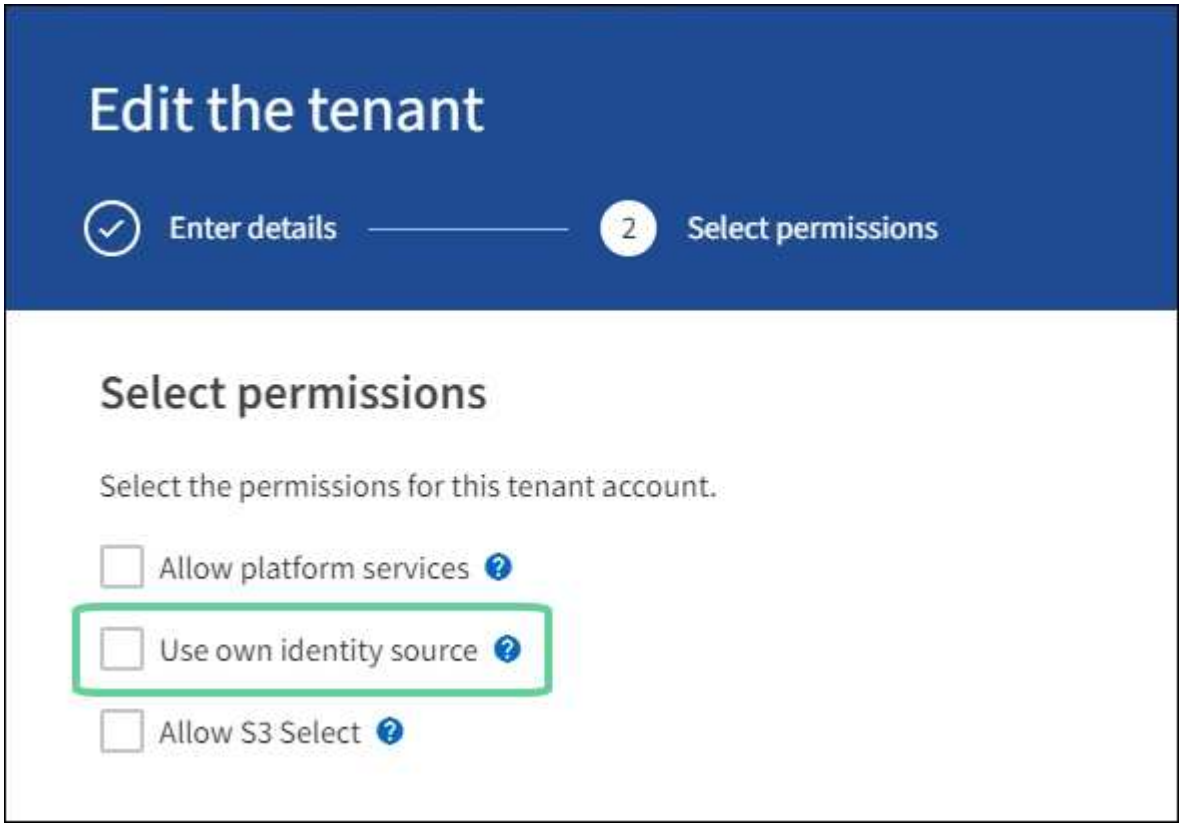
   Wenn Sie SSO aktivieren, wird eine im Tenant Manager konfigurierte Identitätsquelle durch die im Grid Manager konfigurierte Identitätsquelle überschrieben. Benutzer, die zur Identitätsquelle des Mandanten gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Identitätsquelle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



Die Mandantenseite wird angezeigt.

a. Wählen Sie das Mandantenkonto aus, wählen Sie * Sign in* und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.

b. Wählen Sie im Mandanten-Manager **ZUGRIFFSVERWALTUNG** > **Gruppen**.

c. Stellen Sie sicher, dass mindestens einer föderierten Gruppe aus dem Grid Manager die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.

d. Abmelden.

e. 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.

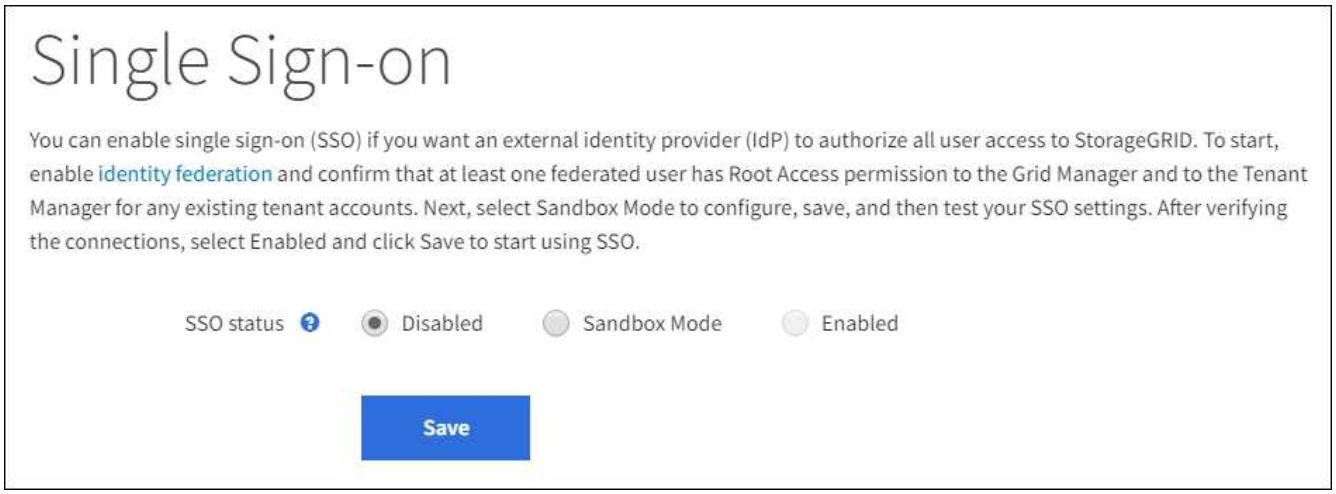
Der Sandbox-Modus erleichtert die Durchführung dieser Hin- und Her-Konfiguration und das Testen aller Ihrer Einstellungen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht per SSO anmelden.

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.



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.

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-Verbunddienste (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-Metadatendatei 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

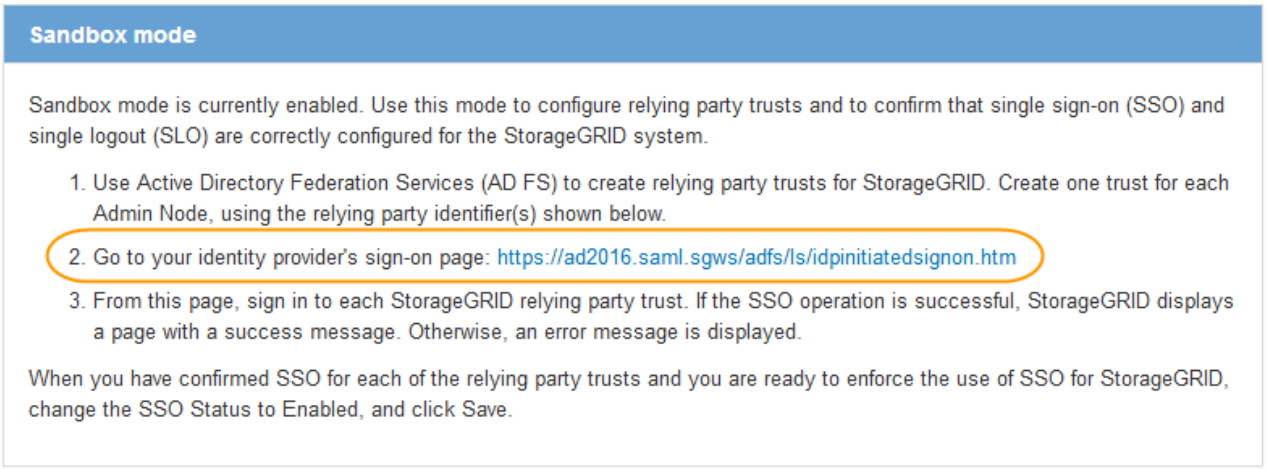
Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID System erzwingen, sollten Sie bestätigen, dass Single Sign-On und Single Logout für jeden Admin-Knoten richtig konfiguriert sind.

Active Directory

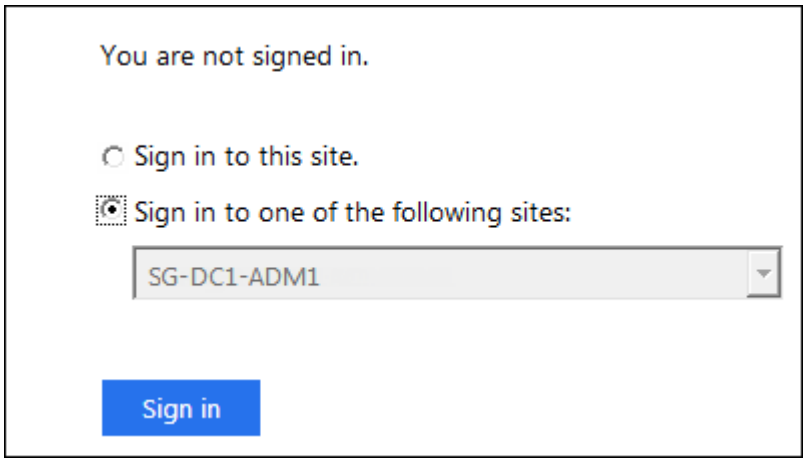
Schritte

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

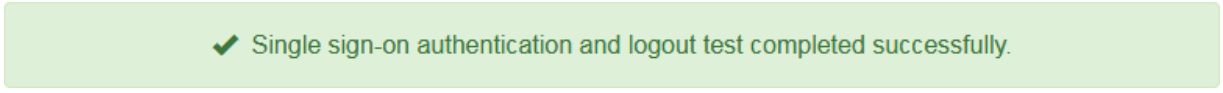
   Die URL wird aus dem Wert abgeleitet, den Sie in das Feld **Name des Verbunddienstes** eingegeben haben.

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.

   - 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.

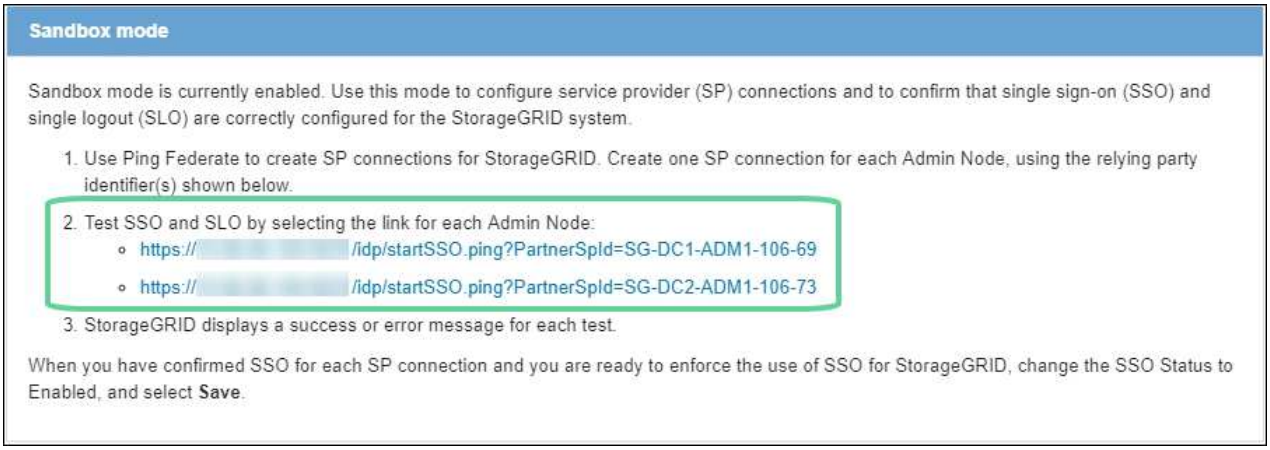
   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers und versuchen Sie es erneut.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Knoten in Ihrem Raster zu überprüfen.

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.

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 Domänennamen (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 Domänennamen 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 Domänennamen 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 Domänennamen 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 Domänennamen 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 Dienstprinzipals.

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 diehttps://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 dieKennwort-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 zuErstellen 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-Profile“ 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 OptionAdapterinstanz 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 dieDatenspeicher 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 dieSignaturzertifikat 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 Metadatendatei 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.