Single Sign-On (SSO) nutzen

StorageGRID software

NetApp
July 23, 2026

Inhalt

Single Sign-On (SSO) nutzen

Erfahren Sie mehr über StorageGRID SSO

Wenn Single Sign-On (SSO) aktiviert ist, ist der Zugriff auf Grid Manager, Tenant Manager, die Grid Management API oder die Tenant Management API für Benutzer nur möglich, wenn ihre Anmeldeinformationen über den von Ihrer Organisation implementierten SSO-Anmeldeprozess autorisiert werden. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

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

${post_edited_translations.segment}

Anmelden, wenn SSO aktiviert ist

Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur SSO-Seite Ihrer Organisation weitergeleitet, um Ihre Anmeldeinformationen zu bestätigen.

Schritte

1. Geben Sie den vollqualifizierten Domainnamen oder die IP-Adresse eines beliebigen StorageGRID Admin Node in einem Webbrowser ein.

   Die StorageGRID Anmeldeseite wird angezeigt.

   - Wenn Sie die URL zum ersten Mal mit 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 kürzlich verwendetes Konto auszuwählen oder eine Konto-ID einzugeben.

   > Die StorageGRID Sign-in-Seite wird nicht angezeigt, wenn die vollständige URL für ein Mandantenkonto eingegeben wird (das heißt, eine vollqualifizierte Domain oder IP-Adresse gefolgt von `/?accountId=20-digit-account-id`). Stattdessen erfolgt eine sofortige Weiterleitung zur SSO Sign-in-Seite Ihrer Organisation, wo Mit Ihren SSO-Anmeldeinformationen anmelden möglich ist.

2. Geben Sie an, ob Sie auf den Grid Manager oder den Tenant Manager zugreifen möchten:
   - Um auf den Grid Manager zuzugreifen, das Feld **Konto-ID** leer lassen, **0** als Konto-ID eingeben oder **Grid Manager** auswählen, falls dieser in der Liste der zuletzt verwendeten Konten erscheint.
   - ${post_edited_translations.segment}
3. **Anmelden** auswählen

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

4. Mit Ihren SSO-Anmeldeinformationen anmelden.

   Wenn Ihre SSO-Anmeldeinformationen korrekt sind:

a. Der Identitätsanbieter (IdP) stellt eine Authentifizierungsantwort für StorageGRID bereit.

b. StorageGRID validiert die Authentifizierungsantwort.

c. Wenn die Antwort gültig ist und Sie einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen angehören, sind Sie beim Grid Manager oder beim Tenant Manager angemeldet, abhängig davon, welches Konto Sie ausgewählt haben.

> Wenn das Dienstkonto nicht erreichbar ist, können Sie sich trotzdem anmelden, sofern Sie ein bestehender Benutzer sind, der einer Verbundgruppe mit StorageGRID Zugriffsberechtigungen angehört.

5. Optional ist auch der Zugriff auf andere Admin-Knoten, den Grid Manager oder den Tenant Manager möglich, sofern die entsprechenden Berechtigungen vorliegen.

   Sie müssen Ihre SSO-Anmeldeinformationen nicht erneut eingeben.

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   Die StorageGRID Sign in-Seite wird angezeigt. Das Dropdown-Menü **Recent Accounts** wurde aktualisiert und enthält nun **Grid Manager** oder den Namen des Mandanten, sodass zukünftig schneller auf diese Benutzeroberflächen zugegriffen werden kann.

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

${post_edited_translations.segment}	**Und Sie melden sich ab von…**	**Sie sind abgemeldet…**
Grid Manager auf einem oder mehreren Admin Nodes	Grid Manager auf einem beliebigen Admin-Node	Grid Manager auf allen Admin Nodes **Hinweis:** Wenn Sie Entra ID für SSO verwenden, kann es einige Minuten dauern, bis Sie von allen Admin Nodes abgemeldet sind.
Mandantenmanager auf einem oder mehreren Admin-Nodes	Mandantenmanager auf einem beliebigen Admin-Node	Mandantenmanager auf allen Admin-Nodes
Sowohl Grid Manager als auch Tenant Manager	Grid Manager	Nur der Grid Manager. Um sich von SSO abzumelden, ist auch eine Abmeldung vom Tenant Manager erforderlich.

Anforderungen und Überlegungen für StorageGRID SSO

Vor der Aktivierung von Single Sign-On (SSO) für ein StorageGRID System sind die Anforderungen und Überlegungen zu prüfen.

Anforderungen an Identitätsanbieter

${post_edited_translations.segment}

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

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

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

AD FS Anforderungen

Es können beliebige der folgenden Versionen von AD FS verwendet werden:

- ${post_edited_translations.segment}
- Windows Server 2019 AD FS
- ${post_edited_translations.segment}

> Windows Server 2016 sollte "${post_edited_translations.segment}" oder höher verwenden.

Zusätzliche Anforderungen

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Überlegungen zu Entra ID

Wenn Sie Entra ID als SSO-Typ verwenden und Benutzer über Benutzerprinzipalnamen verfügen, die nicht sAMAccountName als Präfix verwenden, können Anmeldeprobleme auftreten, wenn StorageGRID die Verbindung zum LDAP-Server verliert. Damit sich Benutzer anmelden können, muss die Verbindung zum LDAP-Server wiederhergestellt werden.

Anforderungen an Serverzertifikate

Standardmäßig verwendet StorageGRID auf jedem Admin-Knoten ein Managementoberflächenzertifikat, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern. Bei der Konfiguration von Vertrauensstellungen zwischen vertrauenden Parteien (AD FS), Unternehmensanwendungen (Entra ID) oder Dienstanbieterverbindungen (PingFederate) für StorageGRID wird das Serverzertifikat als Signaturzertifikat für StorageGRID-Anfragen verwendet.

Falls Sie dies noch nicht "Ein benutzerdefiniertes Zertifikat für die Managementoberfläche konfiguriert" haben, sollte es jetzt erfolgen. Wenn ein benutzerdefiniertes Serverzertifikat installiert wird, wird es für alle Admin Nodes verwendet und kann in allen StorageGRID relying party trusts, enterprise applications oder SP connections genutzt werden.

> ⓘ Die Verwendung des Standardserverzertifikats eines Administratorknotens in einer Vertrauensstellung der vertrauenden Seite, einer Unternehmensanwendung oder SP Verbindung wird nicht empfohlen. Wenn der Knoten ausfällt und wiederhergestellt wird, wird ein neues Standardserverzertifikat generiert. Vor der Anmeldung am wiederhergestellten Knoten ist die Vertrauensstellung der vertrauenden Seite, die Unternehmensanwendung oder die SP Verbindung mit dem neuen Zertifikat zu aktualisieren.

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich an der Befehlsshell des Knotens anmelden und zum `/var/local/mgmt-api` Verzeichnis wechseln. Ein benutzerdefiniertes Serverzertifikat trägt den Namen `custom-server.crt`. Das Standard-Serverzertifikat des Knotens trägt den Namen `server.crt`.

Port-Anforderungen

Single Sign-On (SSO) ist auf den eingeschränkten Ports des Grid Manager oder Tenant Manager nicht verfügbar. Der Standard-HTTPS-Port (443) muss verwendet werden, wenn Benutzer sich mit Single Sign-On authentifizieren sollen. Siehe "Zugriffskontrolle an der externen Firewall".

Bestätigen Sie, dass sich Verbundbenutzer bei StorageGRID anmelden können

Bevor Sie Single Sign-On (SSO) aktivieren, muss bestätigt werden, dass sich mindestens ein Verbundbenutzer beim Grid Manager und beim Tenant Manager für alle bestehenden Mandantenkonten anmelden kann.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die Identitätsföderation bereits konfiguriert.

Schritte

1. Falls bereits Mandantenkonten vorhanden sind, ist zu bestätigen, dass keiner der Mandanten seine 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 Tenants gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Grid Manager Identitätsquelle.

a. Bei jedem Mieterkonto im Tenant Manager anmelden.
b. **Zugriffsverwaltung** > **Identitätsföderation** auswählen.
c. Bestätigen Sie, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht ausgewählt ist.
d. ${post_edited_translations.segment}

2. Bestätigen, dass ein Verbundbenutzer auf den Grid Manager zugreifen kann:
   a. ${post_edited_translations.segment}
   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 eine erneute Anmeldung beim Grid Manager als Benutzer der Verbundgruppe möglich ist.
3. ${post_edited_translations.segment}
   a. Im Grid Manager **Mandanten** auswählen.
   b. ${post_edited_translations.segment}
   c. Auf der Registerkarte „Details eingeben“ **Weiter** auswählen.
   d. Wenn das Kontrollkästchen **Eigene Identitätsquelle verwenden** ausgewählt ist, das Kontrollkästchen deaktivieren und **Speichern** auswählen.

      Die Mieterseite wird angezeigt.

   e. Wählen Sie das Mandantenkonto aus, wählen Sie **Anmelden** und melden Sie sich beim Mandantenkonto als lokaler Root-Benutzer an.
   f. Im Mandantenmanager **Zugriffsverwaltung** > **Gruppen** auswählen.
   g. Stellen Sie sicher, dass mindestens einer föderierten Gruppe des Grid Managers die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.
   h. Abmelden.
   i. ${post_edited_translations.segment}

Verwandte Informationen

- "Anforderungen und Überlegungen zum Single Sign-On"
- "${post_edited_translations.segment}"
- "Ein Mandantenkonto verwenden"_

SSO in StorageGRID konfigurieren

Sie können dem Konfigurationsassistenten für Single Sign-On (SSO) folgen und den Sandbox-Modus aktivieren, um SSO zu konfigurieren und zu testen, bevor es für alle StorageGRID Benutzer aktiviert wird. Nachdem SSO aktiviert wurde, besteht die

Möglichkeit, bei Bedarf in den Sandbox-Modus zurückzukehren, um die Konfiguration zu ändern oder erneut zu testen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für den Identitätsverbund-Diensttyp **LDAP** wurde entweder Active Directory oder Entra ID ausgewählt, abhängig vom SSO-Identitätsanbieter, der verwendet werden soll.

Konfigurierter LDAP-Diensttyp	Optionen für SSO Identitätsanbieter
Active Directory Federation Service (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Über diese Aufgabe

Wenn SSO aktiviert ist und ein Benutzer versucht, sich an einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanfrage an den SSO-Identitätsanbieter. Der SSO-Identitätsanbieter sendet daraufhin eine Authentifizierungsantwort an StorageGRID, die angibt, ob die Authentifizierungsanfrage erfolgreich war. Für erfolgreiche Anfragen:

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

Damit StorageGRID (dem Dienstanbieter) und der SSO-Identitätsanbieter sicher über Benutzerauthentifizierungsanfragen kommunizieren können, sind diese Aufgaben zu erledigen:

1. Einstellungen in StorageGRID konfigurieren.
2. Mit der Software des SSO-Identitätsanbieters wird für jeden Admin-Node eine Vertrauensstellung der vertrauenden Seite (AD FS), eine Enterprise Application (Entra ID) oder ein Service Provider (PingFederate) erstellt.
3. Zu StorageGRID zurückkehren, um SSO zu aktivieren.

Der Sandbox-Modus vereinfacht diese Hin- und Her-Konfiguration und ermöglicht es, alle Einstellungen zu testen, bevor SSO aktiviert wird. Im Sandbox-Modus können sich Benutzer nicht mit SSO anmelden.

Assistenten aufrufen

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Single sign-on**. Die Single sign-on-Seite wird angezeigt.

Wenn die Schaltfläche „SSO-Einstellungen konfigurieren“ deaktiviert ist, sollte überprüft werden, ob der Identitätsanbieter als föderierte Identitätsquelle konfiguriert wurde. Siehe "Anforderungen und Überlegungen zum Single Sign-On".

2. **SSO-Einstellungen konfigurieren** auswählen. Die Seite „Details zum Identitätsanbieter angeben“ erscheint.

Angaben zum Identitätsanbieter bereitstellen

Schritte

1. Den **SSO-Typ** aus der Dropdown-Liste auswählen.
2. Wenn Sie Active Directory als SSO-Typ ausgewählt haben, ist der **Verbunddienstname** für den Identitätsanbieter genau so einzugeben, wie er im Active Directory Federation Service (AD FS) erscheint.

   Um den Namen des Verbunddienstes zu finden, gehen Sie zum Windows Server-Manager. **Tools** > **AD FS Management** auswählen. Im Menü „Action“ die Option **Edit Federation Service Properties** auswählen. Der Federation Service Name wird im zweiten Feld angezeigt.

3. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitätsanbieter SSO-Konfigurationsinformationen als Antwort auf StorageGRID Anfragen sendet.
   - **CA-Zertifikat des Betriebssystems verwenden**: Das standardmäßig auf dem Betriebssystem installierte CA-Zertifikat wird zur Absicherung der Verbindung verwendet.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Ein benutzerdefiniertes CA-Zertifikat wird verwendet, um die Verbindung zu sichern.

     Wenn Sie diese Einstellung auswählen, den Text des benutzerdefinierten Zertifikats kopieren und in das Textfeld **CA Certificate** einfügen.

   - **Kein TLS verwenden**: Es wird kein TLS-Zertifikat verwendet, um die Verbindung zu sichern.

     Wenn Sie das CA-Zertifikat ändern, "Den mgmt-api Service auf den Admin-Knoten neu starten" und testen Sie sofort, ob ein SSO-Zugriff auf den Grid Manager erfolgreich ist.

4. **Weiter** auswählen. Die Seite „Identifikator der vertrauenden Partei angeben“ wird angezeigt.

Relying-Party-Kennung angeben

1. Füllen Sie die Felder auf der Seite „Vertrauende Parteikennung angeben“ entsprechend dem ausgewählten SSO-Typ aus.

Active Directory

a. Geben Sie die **Relying party identifier** für StorageGRID an. Dieser Wert steuert den Namen, der für jede Relying party trust in AD FS verwendet wird.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und nicht damit zu rechnen ist, dass in Zukunft weitere Admin-Knoten hinzugefügt werden, geben Sie `SG` oder `StorageGRID` ein.
   - Wenn Ihr Grid mehr als einen Admin Node enthält, muss die Zeichenfolge `[HOSTNAME]` in die Kennung eingefügt werden. Beispielsweise `SG-[HOSTNAME]`. Das Einfügen dieser Zeichenfolge führt zu einer Tabelle, die die Relying-Party-Kennung für jeden Admin Node im Grid basierend auf dem Hostnamen des Nodes anzeigt.

   > Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Vertrauensstellung einrichten. Eine Vertrauensstellung für jeden Admin-Knoten gewährleistet, dass sich Benutzer sicher an jedem Admin-Knoten an- und ausloggen können.

b. **Speichern und Sandbox-Modus aktivieren** auswählen.

Entra ID

a. Im Abschnitt „Enterprise Application“ ist der **Enterprise application name** für StorageGRID anzugeben. Dieser Wert legt den Namen fest, der für jede Enterprise Application in Entra ID verwendet wird.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und nicht damit zu rechnen ist, dass in Zukunft weitere Admin-Knoten hinzugefügt werden, geben Sie `SG` oder `StorageGRID` ein.
   - Wenn Ihr Grid mehr als einen Admin Node enthält, sollte die Zeichenfolge `[HOSTNAME]` im Bezeichner enthalten sein. Zum Beispiel `SG-[HOSTNAME]`. Das Einfügen dieser Zeichenfolge führt zu einer Tabelle, die für jeden Admin Node in Ihrem System einen Enterprise Application Name basierend auf dem Hostnamen des Knotens anzeigt.

   > Sie müssen für jeden Admin Node in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Eine eigene Unternehmensanwendung für jeden Admin Node stellt sicher, dass sich Benutzer sicher bei jedem Admin Node anmelden und wieder ausloggen können.

b. Die Schritte in "Unternehmensanwendungen in Entra ID erstellen" führen zur Erstellung einer Unternehmensanwendung für jeden in der Tabelle aufgeführten Admin Node.

c. Kopieren Sie aus Entra ID die Föderationsmetadaten-URL für jede Unternehmensanwendung. Anschließend diese URL in das entsprechende Feld **Federation metadata URL** in StorageGRID einfügen.

d. Nachdem Sie eine Federation-Metadaten-URL für alle Admin-Knoten kopiert und eingefügt haben, **Speichern und Sandbox-Modus aktivieren** auswählen.

PingFederate

a. Im Abschnitt „Service Provider (SP)“ ist die **SP-Verbindungs-ID** für StorageGRID anzugeben. Dieser Wert bestimmt den Namen, den Sie für jede SP-Verbindung in PingFederate verwenden.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und nicht damit zu rechnen ist, dass in Zukunft weitere Admin-Knoten hinzugefügt werden, geben Sie `SG` oder `StorageGRID`

ein.

- Wenn Ihr Grid mehr als einen Admin-Node enthält, ist die Zeichenfolge `[HOSTNAME]` in die Kennung aufzunehmen. Zum Beispiel `SG-[HOSTNAME]`. Die Einbindung dieser Zeichenfolge führt zu einer Tabelle, die die SP-Verbindungs-ID für jeden Admin-Node in Ihrem System basierend auf dem Hostnamen des Nodes anzeigt.

> Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System eine SP-Verbindung erstellen. Eine SP-Verbindung für jeden Admin-Knoten stellt sicher, dass sich Benutzer sicher an jedem Admin-Knoten an- und ausloggen können.

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

Folgendes Format wird verwendet:

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

c. **Speichern und Sandbox-Modus aktivieren** auswählen.

Vertrauensstellungen der vertrauenden Seite, Unternehmensanwendungen oder SP Verbindungen konfigurieren

Nachdem Sie die Konfiguration gespeichert und den Sandbox-Modus aktiviert haben, kann die Konfiguration für den von Ihnen ausgewählten SSO-Typ abgeschlossen und getestet werden.

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

Active Directory

Schritte

1. Zu Active Directory Federation Services (AD FS) wechseln.
2. Eine oder mehrere Vertrauensstellungen für StorageGRID werden erstellt, wobei jeweils die in der Tabelle auf der Seite „SSO konfigurieren“ aufgeführten Relying-Party-Bezeichner verwendet werden.

   Für jeden in der Tabelle aufgeführten Admin-Knoten muss eine Vertrauensstellung erstellt werden.

   Anweisungen sind unter "Erstellen von Vertrauensstellungen für vertrauende Parteien in AD FS" zu finden.

Entra ID

Schritte

1. Auf der Single sign-on-Seite des Admin-Knotens, bei dem Sie aktuell angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten auswählen.
2. Anschließend sind diese Schritte für alle anderen Admin-Knoten in Ihrem Grid zu wiederholen:
   a. Melden Sie sich am Node an.
   b. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   c. Die SAML-Metadaten für diesen Knoten herunterladen und speichern.
3. Wechseln Sie zum Azure Portal.
4. Führen Sie die Schritte in "Unternehmensanwendungen in Entra ID erstellen" aus, um die SAML-Metadatendatei für jeden Admin-Node in die entsprechende Entra ID Enterprise Application hochzuladen.

PingFederate

Schritte

1. Auf der Single sign-on-Seite des Admin-Knotens, bei dem Sie aktuell angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten auswählen.
2. Anschließend sind diese Schritte für alle anderen Admin-Knoten in Ihrem Grid zu wiederholen:
   a. Melden Sie sich am Node an.
   b. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   c. Die SAML-Metadaten für diesen Knoten herunterladen und speichern.
3. Zu PingFederate wechseln.
4. "Eine oder mehrere Service Provider (SP) Verbindungen für StorageGRID erstellen". Die SP-Verbindungs-ID für jeden Admin-Knoten (angezeigt in der Tabelle auf der Seite „SSO konfigurieren“) und die SAML-Metadaten, die für diesen Admin-Knoten heruntergeladen wurden, sind zu verwenden.

   Für jeden in der Tabelle aufgeführten Admin-Knoten muss eine SP-Verbindung erstellt werden.

Testkonfiguration

Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID System erzwingen, vergewissern Sie sich, dass Single Sign-On und Single Logout für jeden Admin Node korrekt konfiguriert sind.

Active Directory

Schritte

1. Auf der Seite „SSO konfigurieren“ befindet sich der Link im Schritt „Konfiguration testen“ des Assistenten.

   ${post_edited_translations.segment}

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. ${post_edited_translations.segment}
4. Geben Sie Ihren Verbundbenutzernamen und Ihr Passwort ein.
   - ${post_edited_translations.segment}
   - 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. ${post_edited_translations.segment}

Entra ID

Schritte

1. ${post_edited_translations.segment}
2. **Diese Anwendung testen** auswählen.
3. Die Anmeldeinformationen eines Verbundbenutzers eingeben.
   - ${post_edited_translations.segment}
   - 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. ${post_edited_translations.segment}

PingFederate

Schritte

1. Auf der Seite „SSO konfigurieren“ ist der erste Link in der Meldung zum Sandbox-Modus auszuwählen.

   Jeweils ein Link kann ausgewählt und getestet werden.

2. Die Anmeldeinformationen eines Verbundbenutzers eingeben.
   - ${post_edited_translations.segment}
   - 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. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

Single Sign-On aktivieren

Sobald bestätigt wurde, dass Sie sich per SSO an jedem Admin-Knoten anmelden können, lässt sich SSO für das gesamte 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. Im Schritt „Testkonfiguration“ des Assistenten zur SSO-Konfiguration **SSO aktivieren** auswählen.
2. Die Warnmeldung prüfen und **SSO aktivieren** auswählen.

   Single Sign-on ist jetzt aktiviert. Die Single Sign-on Seite wird angezeigt und enthält nun die Details für das soeben konfigurierte SSO.

3. Zum Bearbeiten der Konfiguration **Bearbeiten** auswählen.
4. Zum Deaktivieren von Single Sign-On **SSO deaktivieren** auswählen.

Wenn das Azure-Portal verwendet wird und von demselben Computer aus auf StorageGRID zugegriffen wird, von dem auch auf Entra ID zugegriffen wird, ist sicherzustellen, dass der Azure-Portal-Benutzer ebenfalls ein autorisierter StorageGRID Benutzer ist (ein Benutzer in einer Verbundgruppe, die in StorageGRID importiert wurde), oder es erfolgt ein Ausloggen vom Azure-Portal, bevor versucht wird, sich bei StorageGRID anzumelden.

Erstellen von Relying-Party-Vertrauensstellungen in AD FS für StorageGRID

Sie müssen Active Directory Federation Services (AD FS) verwenden, um für jeden Admin Node in Ihrem System eine Vertrauensstellung der vertrauenden Seite zu erstellen. Vertrauensstellungen der vertrauenden Seite können mithilfe von PowerShell-Befehlen, durch Importieren von SAML-Metadaten aus StorageGRID oder durch manuelle Eingabe der Daten erstellt werden.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **AD FS** als SSO-Typ ausgewählt.
- Sie haben "Sandbox-Modus wurde aktiviert" im Grid Manager.
- Sie kennen den vollqualifizierten Domainnamen (oder die IP-Adresse) und die Kennung der vertrauenden Partei für jeden Admin Node in Ihrem System. Diese Werte sind in der Detailtabelle der Admin Nodes auf der StorageGRID Configure SSO-Seite zu finden.

  Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Vertrauensstellung einrichten. Eine Vertrauensstellung für jeden Admin-Knoten gewährleistet, dass sich Benutzer sicher an jedem Admin-Knoten an- und ausloggen können.

- Sie haben Erfahrung mit der Erstellung von Vertrauensstellungen für vertrauende Parteien in AD FS oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- ${post_edited_translations.segment}
- Wenn Sie die Vertrauensstellung der vertrauenden Seite manuell erstellen, verfügen Sie über das benutzerdefinierte Zertifikat, das für die StorageGRID Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich über die Befehlsshell bei einem Admin Node anmelden.

Über diese Aufgabe

Diese Anleitung gilt für Windows Server 2016 AD FS. Wenn Sie eine andere Version von AD FS verwenden, werden Sie geringfügige Unterschiede im Ablauf feststellen. In der Microsoft AD FS-Dokumentation finden sich weitere Informationen bei Fragen.

Erstellen einer Vertrauensstellung der vertrauenden Seite mithilfe von Windows PowerShell

Mit Windows PowerShell lassen sich schnell eine oder mehrere Vertrauensstellungen für vertrauende Parteien erstellen.

Schritte

1. Im Windows-Startmenü mit der rechten Maustaste auf das PowerShell-Symbol klicken und **Als Administrator ausführen** auswählen.
2. An der PowerShell-Eingabeaufforderung den folgenden Befehl eingeben:

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

   - Für *`Admin_Node_Identifier`* den Admin-Knoten ist der Relying Party Identifier exakt so einzugeben, wie er auf der Single Sign-on-Seite angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.
   - Für *`Admin_Node_FQDN`* den gleichen Admin-Knoten den vollqualifizierten Domänennamen eingeben. (Falls erforderlich, kann stattdessen die IP-Adresse des Knotens verwendet werden. Wenn jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese Relying-Party-Vertrauensstellung aktualisiert oder neu erstellt werden muss, falls sich diese IP-Adresse jemals ändert.)
3. Wählen Sie im Windows Server-Manager **Tools** > **AD FS Management** aus.

   ${post_edited_translations.segment}

4. **AD FS** > **Vertrauensstellungen der vertrauenden Seite** auswählen.

   Die Liste der vertrauenden Partei-Vertrauensstellungen wird angezeigt.

5. Eine Zugriffssteuerungsrichtlinie zur neu erstellten Vertrauensstellung der vertrauenden Seite hinzufügen:
   a. Die soeben erstellte Vertrauensstellung der vertrauenden Partei befindet sich an folgender Stelle.
   b. Mit der rechten Maustaste auf die Vertrauensstellung klicken und **Zugriffssteuerungsrichtlinie bearbeiten** auswählen.
   c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
   d. **Anwenden** und anschließend **OK** auswählen
6. Eine Claim Issuance Policy zum neu erstellten Relying Party Trust hinzufügen:
   a. Die soeben erstellte Vertrauensstellung der vertrauenden Partei befindet sich an folgender Stelle.
   b. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Claim-Issuance-Richtlinie bearbeiten**.
   c. **Regel hinzufügen** auswählen.
   d. Auf der Seite „Regelvorlage auswählen“ in der Liste **LDAP-Attribute als Ansprüche senden** auswählen und **Weiter** wählen.
   e. Auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel eingeben.

Beispielsweise **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

f. Für den Attributspeicher wird **Active Directory** ausgewählt.

g. ${post_edited_translations.segment}

h. In der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle wird **Name ID** aus der Dropdown-Liste ausgewählt.

i. **Fertigstellen** und anschließend **OK** auswählen.

7. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

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

      Falls die Metadaten fehlen, sollte überprüft werden, ob die Federation-Metadatenadresse korrekt ist, oder die Werte können manuell eingegeben werden.

8. ${post_edited_translations.segment}

9. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und "${post_edited_translations.segment}", um zu bestätigen, dass sie korrekt konfiguriert sind.

${post_edited_translations.segment}

Sie können die Werte für jede Relying-Party-Trust-Beziehung importieren, indem Sie auf die SAML-Metadaten für jeden Admin-Node zugreifen.

Schritte

1. ${post_edited_translations.segment}

2. Unter Aktionen die Option **Vertrauensstellung der vertrauenden Partei hinzufügen** auswählen.

3. Auf der Willkommensseite **Claims aware** auswählen und **Start** wählen.

4. **Daten über die vertrauende Partei importieren, die online oder in einem lokalen Netzwerk veröffentlicht wurden** auswählen.

5. ${post_edited_translations.segment}

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

   Für *`Admin_Node_FQDN`* den gleichen Admin-Knoten den vollqualifizierten Domänennamen eingeben. (Falls erforderlich, kann stattdessen die IP-Adresse des Knotens verwendet werden. Wenn jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese Relying-Party-Vertrauensstellung aktualisiert oder neu erstellt werden muss, falls sich diese IP-Adresse jemals ändert.)

6. Den Assistenten für die Vertrauensstellung der vertrauenden Partei abschließen, die Vertrauensstellung der vertrauenden Partei speichern und den Assistenten schließen.

   Beim Eingeben des Anzeigenamens ist der Relying Party Identifier für den Admin Node zu verwenden, genau wie er auf der Single Sign-on-Seite im Grid Manager angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.

7. Fügen Sie eine Anspruchsregel hinzu:

   a. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Claim-Issuance-Richtlinie**

bearbeiten.

b. **Regel hinzufügen** auswählen:

c. Auf der Seite „Regelvorlage auswählen“ in der Liste **LDAP-Attribute als Ansprüche senden** auswählen und **Weiter** wählen.

d. Auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel eingeben.

   Beispielsweise **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

e. Für den Attributspeicher wird **Active Directory** ausgewählt.

f. ${post_edited_translations.segment}

g. In der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle wird **Name ID** aus der Dropdown-Liste ausgewählt.

h. **Fertigstellen** und anschließend **OK** auswählen.

8. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

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

      Falls die Metadaten fehlen, sollte überprüft werden, ob die Federation-Metadatenadresse korrekt ist, oder die Werte können manuell eingegeben werden.

9. ${post_edited_translations.segment}

10. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und "${post_edited_translations.segment}" um zu bestätigen, dass sie korrekt konfiguriert sind.

Eine Vertrauensstellung der vertrauenden Seite manuell erstellen

Wenn Sie die Daten für die vertrauenden Teilvertrauensstellungen nicht importieren, können Sie die Werte manuell eingeben.

Schritte

1. ${post_edited_translations.segment}
2. Unter Aktionen die Option **Vertrauensstellung der vertrauenden Partei hinzufügen** auswählen.
3. Auf der Willkommensseite **Claims aware** auswählen und **Start** wählen.
4. **Daten über die vertrauende Partei manuell eingeben** auswählen und **Weiter** auswählen.
5. Den Assistenten für die Vertrauensstellung der vertrauenden Partei abschließen:

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

      Für Konsistenz ist der Relying Party Identifier für den Admin Node genau so zu verwenden, wie er auf der Single Sign-on-Seite im Grid Manager angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.

   b. Der Schritt zur Konfiguration eines optionalen Token-Verschlüsselungszertifikats kann übersprungen werden.

   c. Auf der Seite „URL konfigurieren“ das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll aktivieren** auswählen.

   d. Geben Sie die SAML-Service-Endpunkt-URL für den Admin-Node ein:

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

Für *Admin_Node_FQDN* geben Sie den vollqualifizierten Domainnamen für den Admin Node ein. (Falls erforderlich, kann stattdessen die IP-Adresse des Knotens verwendet werden. Wenn hier jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese relying party trust aktualisiert oder neu erstellt werden muss, falls sich die IP-Adresse jemals ändert.)

e. Auf der Seite „Kennungen konfigurieren“ ist die Kennung der vertrauenden Partei für denselben Admin-Knoten anzugeben:

Admin_Node_Identifier

Für *Admin_Node_Identifier* den Admin-Knoten ist der Relying Party Identifier exakt so einzugeben, wie er auf der Single Sign-on-Seite angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.

f. Die Einstellungen werden überprüft, die Vertrauensstellung der vertrauenden Seite gespeichert und der Assistent geschlossen.

Das Dialogfeld „Richtlinie zur Schadensmeldung bearbeiten“ wird angezeigt.

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

6. Um den Assistenten für Anspruchsregeln zu starten, **Regel hinzufügen** auswählen:
   a. Auf der Seite „Regelvorlage auswählen“ in der Liste **LDAP-Attribute als Ansprüche senden** auswählen und **Weiter** wählen.
   b. Auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel eingeben.

      Beispielsweise **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

   c. Für den Attributspeicher wird **Active Directory** ausgewählt.
   d. ${post_edited_translations.segment}
   e. In der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle wird **Name ID** aus der Dropdown-Liste ausgewählt.
   f. **Fertigstellen** und anschließend **OK** auswählen.
7. ${post_edited_translations.segment}
8. Auf der Registerkarte **Endpunkte** wird der Endpunkt für Single Logout (SLO) konfiguriert:
   a. **SAML hinzufügen** auswählen.
   b. Wählen Sie **Endpunkttyp** > **SAML Logout**.
   c. **Bindung** > **Umleitung** auswählen.
   d. Im Feld **Vertrauenswürdige URL** ist die URL anzugeben, die für das Single Logout (SLO) von diesem Admin-Node verwendet wird:

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

Für *Admin_Node_FQDN* geben Sie den vollqualifizierten Domainnamen des Admin Node ein. (Falls erforderlich, kann stattdessen die IP-Adresse des Node verwendet werden. Wenn jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese relying party trust aktualisiert oder neu erstellt werden muss,

falls sich die IP-Adresse jemals ändert.)

   a. Wählen Sie **OK**.

9. Auf der Registerkarte **Signatur** wird das Signaturzertifikat für diese Relying-Party-Vertrauensstellung angegeben:

   a. Das benutzerdefinierte Zertifikat hinzufügen:

      - Wenn Sie über das benutzerdefinierte Verwaltungszertifikat verfügen, das Sie in StorageGRID hochgeladen haben, wählen Sie dieses Zertifikat aus.
      - Falls das benutzerdefinierte Zertifikat nicht vorhanden ist, am Admin Node anmelden, in das `/var/local/mgmt-api` Verzeichnis des Admin Node wechseln und die `custom-server.crt` Zertifikatsdatei hinzufügen.

      > Die Verwendung des Standardzertifikats des Admin-Knotens (`server.crt` ist nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat bei der Wiederherstellung des Knotens neu generiert und die Vertrauensstellung der vertrauenden Seite muss aktualisiert werden.

   b. **Anwenden** und anschließend **OK** auswählen.

      Die Eigenschaften der Relying Party werden gespeichert und geschlossen.

10. ${post_edited_translations.segment}
11. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und "${post_edited_translations.segment}" um zu bestätigen, dass sie korrekt konfiguriert sind.

Erstellen Sie Unternehmensanwendungen in Entra ID für StorageGRID

Entra ID wird verwendet, um eine Unternehmensanwendung für jeden Admin-Knoten in Ihrem System zu erstellen.

Bevor Sie beginnen

- Sie haben mit der Konfiguration von Single Sign-On für StorageGRID begonnen und **Entra ID** als SSO-Typ ausgewählt.
- Sie haben "Sandbox-Modus wurde aktiviert" im Grid Manager.
- Sie haben den **Enterprise application name** für jeden Admin-Node in Ihrem System. Diese Werte können aus der Admin-Node-Detailtabelle auf der Seite „SSO konfigurieren“ kopiert werden.

> Sie müssen für jeden Admin Node in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Eine eigene Unternehmensanwendung für jeden Admin Node stellt sicher, dass sich Benutzer sicher bei jedem Admin Node anmelden und wieder ausloggen können.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Entra ID aufrufen

Schritte

1. Melden Sie sich bei der "Azure Portal"an.
2. Navigieren Sie zu "Entra ID".
3. Wählen Sie "Unternehmensanwendungen".

Unternehmensanwendungen erstellen und StorageGRID SSO-Konfiguration speichern

Um die SSO-Konfiguration für Entra ID in StorageGRID zu speichern, ist es erforderlich, mit Entra ID für jeden Admin-Knoten eine Unternehmensanwendung zu erstellen. Die Föderationsmetadaten-URLs werden aus Entra ID kopiert und in die entsprechenden Felder für **Federation metadata URL** auf der Seite „SSO konfigurieren“ eingefügt.

Schritte

1. ${post_edited_translations.segment}
   a. Im Bereich Entra ID Enterprise-Anwendungen die Option **Neue Anwendung** auswählen.
   b. **Eigene Anwendung erstellen** auswählen.
   c. Für den Namen ist der **Enterprise application name** einzugeben, der aus der Tabelle „Admin-Knotendetails“ auf der Seite „SSO konfigurieren“ kopiert wurde.
   d. Die Option **Integrate any other application you don’t find in the gallery (Non-gallery)** bleibt ausgewählt.
   e. Wählen Sie **Create**.
   f. Wählen Sie den Link **Los geht’s** im Feld **2. Einmalanmeldung einrichten** oder den Link **Einmalanmeldung** in der linken Marge.
   g. Das Kontrollkästchen **SAML** auswählen.
   h. ${post_edited_translations.segment}
   i. ${post_edited_translations.segment}
2. Nachdem Sie für jeden Admin-Knoten eine Metadaten-URL für die Föderation eingefügt und alle anderen erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, auf der Seite „SSO konfigurieren“ **Speichern** auswählen.

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. Diese Schritte sind für jeden Admin Node zu wiederholen.
   a. Bei StorageGRID vom Admin-Knoten aus anmelden.
   b. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   c. Die Schaltfläche auswählen, um die SAML-Metadaten für diesen Admin-Knoten herunterzuladen.
   d. Die Datei speichern, die anschließend in Entra ID hochgeladen wird.

SAML-Metadaten in jede Unternehmensanwendung hochladen

Nach dem Herunterladen einer SAML-Metadatendatei für jeden StorageGRID Admin Node sind in Entra ID die folgenden Schritte durchzuführen:

Schritte

1. Zurück zum Azure Portal.
2. ${post_edited_translations.segment}

> Möglicherweise ist es erforderlich, die Seite „Unternehmensanwendungen“ zu aktualisieren, damit zuvor hinzugefügte Anwendungen in der Liste angezeigt werden.

   a. Zur Eigenschaftenseite der Unternehmensanwendung wechseln.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. Die SAML-Konfiguration abschließen.
   e. Die Schaltfläche **Metadatendatei hochladen** auswählen und die SAML-Metadatendatei auswählen, die für den entsprechenden Admin Node heruntergeladen wurde.
   f. Nachdem die Datei geladen wurde, **Speichern** auswählen und anschließend **X**, um das Fenster zu schließen. Die Seite „Single Sign-On mit SAML einrichten“ wird wieder angezeigt.
3. "Jede Anwendung testen".

Erstellen Sie Dienstanbieterverbindungen in PingFederate für StorageGRID

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

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **Ping Federate** als SSO-Typ ausgewählt.
- Sie haben "Sandbox-Modus wurde aktiviert" im Grid Manager.
- Sie verfügen über die **SP-Verbindungskennung** für jeden Admin Node in Ihrem System. Sie finden diese Werte in der Detailtabelle der Admin Nodes auf der Seite „Configure SSO“.
- Sie haben die **SAML-Metadaten** für jeden Admin Node in Ihrem System heruntergeladen.
- Sie haben Erfahrung in der Erstellung von SP Verbindungen im PingFederate Server.
- Sie haben die "Administrator-Referenzhandbuch" für den PingFederate Server. Die PingFederate Dokumentation enthält detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben die "Administratorberechtigung" für den PingFederate Server.

Über diese Aufgabe

Diese Anleitung fasst zusammen, wie der PingFederate Server Version 10.3 als SSO-Anbieter für StorageGRID konfiguriert wird. Wenn eine andere Version von PingFederate verwendet wird, müssen diese Anweisungen möglicherweise angepasst werden. In der PingFederate Server-Dokumentation finden Sie ausführliche Anweisungen für Ihre Version.

Voraussetzungen in PingFederate abschließen

Bevor Sie die SP Verbindungen für StorageGRID erstellen können, müssen Sie die erforderlichen Voraufgaben in PingFederate abschließen. Informationen aus diesen Voraufgaben werden bei der Konfiguration der SP Verbindungen verwendet.

Datenspeicher erstellen

Falls noch nicht geschehen, einen Datenspeicher erstellen, um PingFederate mit dem AD FS LDAP-Server zu verbinden. Die Werte verwenden, die beim "Konfiguration der Identitätsföderation" in StorageGRID verwendet wurden.

- **Typ**: Verzeichnis (LDAP)
- **LDAP-Typ**: Active Directory
- **Name des Binärattributs**: **objectGUID** ist auf der Registerkarte LDAP-Binärattribute exakt wie angegeben einzugeben.

Passwort-Anmeldeinformationsvalidator erstellen

Falls noch nicht geschehen, einen Passwort-Anmeldeinformationsprüfer erstellen.

- **Typ**: LDAP-Benutzername Passwort Credential Validator
- **Datenspeicher**: Der von Ihnen erstellte Datenspeicher wird ausgewählt.
- **Suchbasis**: Informationen aus LDAP eingeben (z. B. DC=saml,DC=sgws).
- **Suchfilter**: sAMAccountName=${username}
- **Gültigkeitsbereich**: Teilbaum

IdP Adapterinstanz erstellen

Falls noch nicht geschehen, eine IdP-Adapterinstanz erstellen.

Schritte

1. Wechseln Sie zu **Authentifizierung** > **Integration** > **IdP Adapter**.
2. **Neue Instanz erstellen** auswählen.
3. Auf der Registerkarte „Typ“ ist **HTML Form IdP Adapter** auszuwählen.
4. Auf der Registerkarte „IdP-Adapter“ die Option **Neue Zeile zu 'Credential Validators' hinzufügen** auswählen.
5. Wählen Sie die Passwort-Anmeldeinformationsprüfer aus, die Sie erstellt haben.
6. Auf der Registerkarte Adapterattribute ist das Attribut **username** für **Pseudonym** auszuwählen.
7. **Speichern** auswählen.

Signaturzertifikat erstellen oder importieren

Falls noch nicht geschehen, das Signaturzertifikat erstellen oder importieren.

Schritte

1. Wechseln Sie zu **Sicherheit** > **Signatur- und Entschlüsselungsschlüssel & Zertifikate**.
2. Das Signaturzertifikat wird erstellt oder importiert.

Eine SP Verbindung in PingFederate erstellen

Wenn eine SP-Verbindung in PingFederate erstellt wird, wird die SAML-Metadaten-Datei importiert, die zuvor von StorageGRID für den Admin-Node heruntergeladen wurde. Die Metadatendatei enthält viele der benötigten spezifischen Werte.

Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System eine SP-Verbindung erstellen, damit sich Benutzer sicher an jedem Knoten an- und abmelden können. Diese Anweisungen dienen dazu, die erste SP-Verbindung zu erstellen. Anschließend zu Zusätzliche SP Verbindungen erstellen können alle weiteren benötigten Verbindungen erstellt werden.

SP Verbindungstyp auswählen

Schritte

1. Wechseln Sie zu **Anwendungen** > **Integration** > **SP Connections**.
2. **Verbindung erstellen** auswählen.
3. **Für diese Verbindung keine Vorlage verwenden** auswählen.
4. **Browser SSO Profiles** und **SAML 2.0** als Protokoll auswählen.

SP Metadaten importieren

Schritte

1. Auf der Registerkarte „Metadaten importieren“ wird **Datei** ausgewählt.
2. Wählen Sie die SAML-Metadatendatei aus, die Sie von der Seite „SSO konfigurieren“ für den Admin Node heruntergeladen haben.
3. Die Metadatenübersicht und die Informationen auf der Registerkarte „Allgemeine Informationen“ werden angezeigt.

   Die Partner-Entitäts-ID und der Verbindungsname sind auf die StorageGRID SP Verbindung-ID festgelegt. (zum Beispiel 10.96.105.200-DC1-ADM1-105-200). Die Basis-URL ist die IP des StorageGRID Admin Node.

4. **Weiter** auswählen.

IdP Browser-SSO konfigurieren

Schritte

1. Auf der Registerkarte „Browser SSO“ die Option „Browser SSO konfigurieren“ auswählen.
2. Auf der Registerkarte SAML-Profile die Optionen **SP-initiiertes SSO**, **SP-initiales SLO**, **IdP-initiiertes SSO** und **IdP-initiiertes SLO** auswählen.
3. **Weiter** auswählen.
4. Auf der Registerkarte „Assertion Lifetime“ werden keine Änderungen vorgenommen.
5. Auf der Registerkarte „Assertion Creation“ die Option **Assertion Creation konfigurieren** auswählen.
   a. Auf der Registerkarte „Identitätszuordnung“ wird **Standard** ausgewählt.
   b. Auf der Registerkarte „Attributvertrag“ wird **SAML_SUBJECT** als Attributvertrag und das importierte, nicht spezifizierte Namensformat verwendet.
6. Wählen Sie unter „Vertrag verlängern“ die Option **Löschen**, um das `urn:oid` zu entfernen, das nicht verwendet wird.

Adapterinstanz zuordnen

Schritte

1. Auf der Registerkarte „Zuordnung der Authentifizierungsquelle“ die Option **Neue Adapterinstanz zuordnen** auswählen.
2. Auf der Registerkarte „Adapterinstanz“ die von Ihnen erstellte Adapterinstanz Instanz auswählen.
3. Auf der Registerkarte „Mapping-Methode“ ist **Zusätzliche Attribute aus einem Datenspeicher abrufen** auszuwählen.
4. Auf der Registerkarte „Attributquelle & Benutzersuche“ **Attributquelle hinzufügen** auswählen.
5. Geben Sie auf der Registerkarte „Datenspeicher“ eine Beschreibung an und wählen Sie die Datenspeicher aus, die Sie hinzugefügt haben.
6. Auf der Registerkarte „LDAP-Verzeichnissuche“:
   - Geben Sie den **Basis-DN** ein, der exakt mit dem Wert übereinstimmen muss, den Sie in StorageGRID für den LDAP-Server eingegeben haben.
   - Für den Suchbereich **Unterbaum** auswählen.
   - Für die Root-Objektklasse nach einem der folgenden Attribute suchen und entweder **objectGUID** oder **userPrincipalName** hinzufügen.
7. Auf der Registerkarte LDAP Binary Attribute Encoding Types ist für das Attribut **objectGUID** der Typ **Base64** auszuwählen.
8. Auf der Registerkarte LDAP-Filter **sAMAccountName=${username}** eingeben.
9. Auf der Registerkarte „Attributvertragserfüllung“ im Dropdown-Menü „Quelle“ **LDAP (Attribut)** auswählen und im Dropdown-Menü „Wert“ entweder **objectGUID** oder **userPrincipalName** auswählen.
10. Die Attributquelle wird überprüft und anschließend gespeichert.
11. Auf der Registerkarte „Failsave-Attributquelle“ die Option **SSO-Transaktion abbrechen** auswählen.
12. Die Zusammenfassung kann überprüft und **Fertig** ausgewählt werden.
13. **Fertig** auswählen.

Protokolleinstellungen konfigurieren

Schritte

1. Auf der Registerkarte **SP Connection** > **Browser SSO** > **Protocol Settings** ist **Configure Protocol Settings** auszuwählen.
2. Auf der Registerkarte „Assertion Consumer Service URL“ die Standardwerte übernehmen, die aus den StorageGRID SAML-Metadaten importiert wurden (**POST** für Binding und `/api/saml-response` für Endpoint URL).
3. Auf der Registerkarte SLO Service URLs die Standardwerte übernehmen, die aus den StorageGRID SAML-Metadaten importiert wurden (**REDIRECT** für Binding und `/api/saml-logout` für Endpoint URL).
4. Auf der Registerkarte „Zulässige SAML-Bindungen“ sind **ARTIFACT** und **SOAP** zu deaktivieren. Nur **POST** und **REDIRECT** sind erforderlich.
5. Auf der Registerkarte „Signaturrichtlinie“ bleiben die Kontrollkästchen **Authn-Anfragen müssen signiert werden** und **Assertion immer signieren** ausgewählt.
6. Auf der Registerkarte „Verschlüsselungsrichtlinie“ ist **Keine** auszuwählen.
7. Die Zusammenfassung kann überprüft und mit **Fertig** die Protokolleinstellungen gespeichert werden.

8. Die Zusammenfassung kann überprüft und mit **Fertig** die Browser SSO-Einstellungen gespeichert werden.

Anmeldeinformationen konfigurieren

Schritte

1. Wählen Sie auf der Registerkarte SP Connection die Option **Anmeldeinformationen**.
2. Auf der Registerkarte „Anmeldeinformationen“ die Option **Anmeldeinformationen konfigurieren** auswählen.
3. Wählen Sie die Unterzeichnungszertifikat aus, die Sie erstellt oder importiert haben.
4. **Weiter** auswählen, um zu **Einstellungen für die Signaturprüfung verwalten** zu gelangen.
   a. Auf der Registerkarte „Vertrauensmodell“ die Option „Nicht verankert“ auswählen.
   b. Auf der Registerkarte „Signaturverifizierungszertifikat“ werden die Informationen zum Signaturzertifikat angezeigt, die aus den StorageGRID SAML-Metadaten importiert wurden.
5. Die Zusammenfassungsbildschirme werden überprüft und mit **Speichern** wird die SP Verbindung gespeichert.

Zusätzliche SP Verbindungen erstellen

Sie können die erste SP-Verbindung kopieren, um die SP-Verbindungen zu erstellen, die Sie für jeden Admin-Knoten in Ihrem Grid benötigen. Für jede Kopie werden neue Metadaten hochgeladen.

> ⓘ Die SP Verbindungen für verschiedene Admin-Knoten verwenden identische Einstellungen, mit Ausnahme der Partner Entity ID, der Base URL, der Connection ID, des Connection Name, der Signature Verification und der SLO Response URL.

Schritte

1. Wählen Sie **Aktion** > **Kopieren**, um eine Kopie der ursprünglichen SP-Verbindung für jeden zusätzlichen Admin-Knoten 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-Node entspricht:
   a. **Aktion** > **Mit Metadaten aktualisieren** auswählen.
   b. **Datei auswählen** auswählen und die Metadaten hochladen.
   c. **Weiter** auswählen.
   d. **Speichern** auswählen.
4. Der Fehler aufgrund des ungenutzten Attributs wird behoben:
   a. Die neue Verbindung auswählen.
   b. **Browser SSO konfigurieren > Assertionserstellung konfigurieren > Attributvertrag** auswählen.
   c. Löschen Sie den Eintrag für **urn:oid**.
   d. **Speichern** auswählen.

SSO in StorageGRID deaktivieren

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

Identitätsföderation deaktivieren können.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.

   Die Single Sign-on-Seite wird angezeigt.

2. **SSO deaktivieren** auswählen.
3. **Ja** auswählen.

   Es erscheint eine Warnmeldung, dass sich lokale Benutzer nun anmelden können.

Beim nächsten Anmelden bei StorageGRID erscheint die StorageGRID-Anmeldeseite, und Sie müssen den Benutzernamen und das Passwort für einen lokalen oder föderierten StorageGRID Benutzer eingeben.

SSO für einen StorageGRID Admin-Node vorübergehend deaktivieren und wieder aktivieren

Sie können sich möglicherweise nicht beim Grid Manager anmelden, wenn das Single Sign-On (SSO)-System ausfällt. In diesem Fall kann SSO für einen Admin-Knoten vorübergehend deaktiviert und anschließend wieder aktiviert werden. Zum Deaktivieren und anschließenden erneuten Aktivieren von SSO ist der Zugriff auf die Befehlsshell des Knotens erforderlich.

Bevor Sie beginnen

- Du hast "spezifische 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-Knoten deaktiviert haben, können Sie sich beim Grid Manager als lokaler Root-Benutzer anmelden. Um Ihr StorageGRID System zu schützen, muss die Befehlsshell des Knotens verwendet werden, um SSO auf dem Admin-Knoten unmittelbar nach dem Abmelden wieder zu aktivieren.

> Die Deaktivierung von SSO für einen Admin-Knoten hat keine Auswirkungen auf die SSO-Einstellungen anderer Admin-Knoten im Grid. Das Kontrollkästchen **Enable SSO** auf der Seite Single Sign-on im Grid Manager bleibt ausgewählt, und alle bestehenden SSO-Einstellungen werden beibehalten, sofern sie nicht aktualisiert werden.

Schritte

1. ${post_edited_translations.segment}
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`

d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

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

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

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

3. Bestätigen Sie, dass SSO deaktiviert werden soll.

Eine Meldung weist darauf hin, dass Single Sign-On auf dem Knoten deaktiviert ist.

4. ${post_edited_translations.segment}

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

5. Mit dem Benutzernamen root und dem Passwort des lokalen Root-Benutzers anmelden.
6. Wenn Sie SSO vorübergehend deaktiviert haben, weil die SSO-Konfiguration korrigiert werden musste:
   a. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   b. Die fehlerhaften oder veralteten SSO-Einstellungen können geändert werden.
   c. **Speichern** auswählen.

      Durch Auswahl von **Speichern** auf der Single Sign-on-Seite wird SSO für das gesamte Grid 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 die Aufgabe oder Aufgaben aus, die erforderlich sind.
   b. **Abmelden** auswählen und den Grid Manager schließen.
   c. SSO kann auf dem Admin-Node erneut aktiviert werden. Einer der folgenden Schritte ist möglich:

      - Führen Sie folgenden Befehl aus: `enable-saml`

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

      Bestätigen Sie, dass Sie SSO aktivieren möchten.

   Eine Meldung weist darauf hin, dass Single Sign-On auf dem Knoten aktiviert ist.

      ◦ Grid-Knoten neu starten: `reboot`

8. Über einen Webbrowser kann vom selben Admin-Knoten aus auf den Grid Manager zugegriffen werden.
9. Bestätigt wird, dass die StorageGRID Sign in-Seite angezeigt wird und dass zur Anmeldung beim Grid Manager die SSO-Anmeldedaten eingegeben werden müssen.