Authentifizierung mit SAML einrichten

Dieser Artikel setzt Kenntnisse zu den folgenden Themen voraus:

- Single Sign-on (SSO)
- Security Assertion Markup Language (SAML)
- SimpleSAMLphp

Ab Version 5.2 nutzt der UCware Server **SimpleSAMLphp** als Service Provider, um sich bei Bedarf in eine bestehende SSO-Infrastruktur zu integrieren. In diesem Fall müssen sich Benutzer abhängig von den Richtlinien ihrer Institution nicht erneut bei UCware authentifizieren, wenn sie bereits bei einem anderen teilnehmenden Dienst angemeldet sind (und umgekehrt).

Voraussetzungen

SimpleSAMLphp wird automatisch mit Version 5.2 des UCware Servers ausgeliefert bzw. beim Update aus den Paketquellen installiert.

Die Integration von SimpleSAMLphp als **Service Provider (SP)** innerhalb einer SSO-Infrastruktur erfordert den gegenseitiger Austausch von Metadaten nach SAML-Standard mit dem jeweiligen **Identity Provider (IdP)**. Kontaktieren Sie dazu vorab den Administrator des IdPs und stellen Sie sicher, dass die Daten zum Zeitpunkt der Einrichtung übergeben bzw. entgegengenommen werden können.

Darüber hinaus müssen die beim IdP registrierten **Externen IDs** der zu authentifizierenden Benutzer und das Attribut bekannt sein, mit dem der IdP erstere abgleichen soll. Dieses Attribut muss für Authentifizierungsanfragen des SPs freigegeben sein.

Schritt für Schritt

Hinweis:
Bei der Installation legt SimpleSAMLphp automatisch den Benutzer `admin` an und speichert das zugehörige Passwort für den Zugang zur Weboberfläche in der Datei `/var/lib/simplesamlphp/secrets.inc.php` auf dem UCware Server.

SimpleSAMLphp vorbereiten

Führen Sie die folgenden Schritte aus:

1. Um per HTTPS auf SimpleSAMLphp zugreifen zu können, stellen Sie die erforderlichen Locations für den Webserver bereit und laden diesen neu:

   ```
   ln -s /etc/nginx/locations.d/03-saml.conf /etc/nginx/https.d/
   ln -s /etc/nginx/locations.d/90-simplesamlphp.conf /etc/nginx/https.d/
   systemctl reload nginx
   ```

2. Stellen Sie ein Zertifikat und den zugehörigen Schlüssel für die Kommunikation mit dem IdP bereit.

   Hinweis:
   Dafür eignen sich sowohl selbst- als auch CA-signierte Zertifikate. Legen das Zertifikat und den Schlüssel standardmäßig unter `/etc/simplesamlphp/ssl` ab.

   Ein selbstsigniertes Zertifikat können Sie wie folgt im Standardverzeichnis bereitstellen:

   ```
   cd /etc/simplesamlphp/ssl/
   openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -text -out ucware.crt -keyout ucware.key
   ```

3. Erteilen Sie SimpleSAMLphp Zugriff auf das Zertifikat.
   Ergänzen Sie dazu in `/etc/simplesamlphp/config.php` die folgende Zeile:

   ```
   'certdir' => '/etc/simplesamlphp/ssl/',
   ```

Metadaten austauschen

Um Authentifizierungsanfragen senden und entsprechende Antworten erhalten zu können, muss der SP mit den Metadaten des IdPs konfiguriert werden und umgekehrt.

Führen Sie dazu die folgenden Schritte aus:

1. Legen Sie das Ziel für Authentifizierungsanfragen des SPs fest.
   Ergänzen Sie den dazu erforderlichen Eintrag in `/etc/simplesamlphp/authsources.php`.

   ```
   'shibboleth' => array(
   'saml:SP',
   'privatekey' => 'ucware.key',
   'certificate' => 'ucware.crt',
   'idp' => 'https://shibboleth.local/idp/shibboleth',
   ),
   ```

   Hinweis:
   Aufbau und Inhalt des Eintrags hängen vom konkreten Anwendungsszenario und insbesondere vom IdP ab. Detaillierte Informationen dazu finden Sie in der SimpleSAMLphp-Doku. Die folgenden Beispiele beziehen sich auf den Austausch mit einem Shibboleth-Server. `shibboleth.local` und `ucware.local` sind dabei als Platzhalter zu verstehen.

2. Speichern Sie die vom Administrator des **IdPs** bereitgestellten Metadaten in der Datei `/etc/simplesamlphp/metadata/saml20-idp-remote.php`.
   Metadaten im XML-Format lassen sich unter der folgenden Adresse direkt in SimpleSAMLphp konvertieren:

   ```
   https://ucware.local/simplesamlphp/admin/metadata-converter.php
   ```

3. Rufen Sie die Metadaten des **SPs** unter der folgenden Adresse ab:

   ```
   https://ucware.local/simplesamlphp/module.php/core/frontpage_federation.php
   ```

4. Stellen Sie diese Metadaten dem Administrator des IdPs zur Verfügung.

SimpleSAMLphp konfigurieren (optional)

Unter **/etc/simplesamlphp/config.php** können Sie die Konfiguration von SimpleSAMLphp bei Bedarf anpassen. Erläuterungen zu den einzelnen Optionen finden Sie direkt in der Datei.

Um beispielsweise die Gültigkeitsdauer von Einmalanmeldungen anzupassen, ändern Sie den Wert für die Option **session.duration**:

```
'session.duration' => 8 * (60 * 60),
```

Der eingetragene Wert entspricht der Gültigkeitsdauer pro Einmalanmeldung in Sekunden. Im Beispiel beträgt diese 28800 Sekunden bzw. 8 Stunden.

Hinweis:
Stellen Sie sicher, dass der Wert für `session.duration` kleiner ist als für die Option `session.cookie.lifetime`. Letzterer bestimmt die Gültigkeitsdauer des Sitzungs-Cookies im Browser bzw. im nativen UCC-Client.

SimpleSAMLphp testen

Nach dem erfolgreichen Austausch der Metadaten sollten Sie sich testweise beim IdP authentifizieren.

Gehen Sie wie folgt vor:

1. Rufen Sie im Webbrowser die folgende Seite auf:

   ```
   https://ucware.local/simplesamlphp/module.php/core/authenticate.php
   ```

2. Wählen Sie hier den gewünschten IdP aus.
3. Melden Sie sich mit Ihren Benutzerdaten beim IdP an.

Wenn Sie erfolgreich authentifiziert werden, wird die Statusseite von SimpleSAMLphp angezeigt. Das Attribut zur Authentifizierung von Benutzern wird hier unter **Ihre Attribute** angezeigt.

Hinweis:
Übernehmen Sie das Attribut exakt in der hier angezeigten Form zur Einrichtung eines SAML-Backends auf dem UCware Server.

Authentifizierungs-Backend im Admin-Client einrichten

Hinweis:
Sobald Sie ein Authentifizierungs-Backend vom Typ **SAML** eingerichtet haben, blendet der UCware Server die Eingabemaske für lokale Anmeldungen am UCC- und Admin-Clients standardmäßig aus. Dies gilt auch für Benutzer, die ihre lokalen Zugangsdaten behalten. In diesem Fall lässt sich die Eingabemaske über die URL des Clients mit angehängtem Suffix `#local` aufrufen.

Wenn Sie SimpleSAMLphp konfiguriert und getestet haben, können Sie im Admin-Client ein Backend zur Authentifizierung via SAML einrichten.

Gehen Sie dazu wie folgt vor:

1. Rufen Sie die Seite **System > Authentifizierungs-Backend** auf.
2. Erstellen Sie mit ein neues Backend.
3. Wählen als **Backend-Typ** den Eintrag **SAML**.
4. Geben Sie einen **Namen** für das Backend ein.
5. Wählen Sie den gewünschten **Service Provider** aus.
   Die verfügbaren Optionen entsprechen den Einträgen in der **authsources.php**.
6. Geben Sie das **Attribut** ein, mit dem der IdP die **Externen IDs** der Benutzers abgleichen soll.
   Zur korrekten Form das Attributs beachten Sie den Abschnitt SimpleSAMLphp testen.
7. Setzen Sie **Erneut validieren** bei Bedarf auf .
   Dadurch werden die eingegebenen Benutzerdaten bei **jeder** Anmeldung über die API (bzw. im UCC-Client) zur Prüfung an den Service Provider weitergereicht. Dies gilt auch, wenn der Benutzer bereits angemeldet ist.
8. Übernehmen Sie die Einstellungen mit Erstellen.

Benutzer-Authentifizierung via SAML aktivieren

Wenn Sie ein Backend für die Authentifizierung via SAML eingerichtet haben, können Sie es den Benutzern des UCware Servers zuweisen. Dabei handelt es sich um eine individuelle Einstellung, sodass Anmeldungen mit lokalen Zugangsdaten bei Bedarf weiterhin möglich sind – beispielsweise für Administratoren.

Um die Authentifizierung via SAML für einen Benutzer zu aktivieren, gehen Sie wie folgt vor:

1. Rufen Sie die Seite **Benutzer & Gruppen > Benutzer** auf.
2. Erstellen oder bearbeiten Sie einen Benutzer.
3. Wählen Sie dabei das gewünschte SAML-**Backend** aus.

Hinweis:
Dadurch wird das lokale Benutzerpasswort aus der Datenbank des UCware Servers gelöscht.

4. Geben Sie die beim IdP registrierte **Externe Benutzer ID** ein.
5. Übernehmen Sie die Einstellungen mit Erstellen bzw. Speichern.

From:
https://wiki.ucware.com/ - **UCware-Dokumentation**

Permanent link:
https://wiki.ucware.com/adhandbuch/system/authbackends/saml?rev=1685611245

Last update: **01.06.2023 09:20**