Portal Tirol Authentifizierung mittels SAML

Inhalt dieser Seite veraltet

Durch die Übersiedelung der Drupal-CMS und Moodle/Mahara auf die WEBCC/WEBLB Infrastruktur, werden die Konfigurationen (Apache, Shibboleth Native-SP) automatische generiert und die SP-Metadaten automatisch auf die neuen IDPs verteilt.

Weiter führende Informationen siehe Kochbuch - DevOps-Rezepte

Voraussetzung

Bei der SAML Authentifizierung werden sensible Authentifizierungs- und Authorisierungsinformationen übermittelt. Aus diesem Grund ist es zwingend erforderlich, dass am Webauftritt **S**ecure **S**ocket **L**ayer (**SSL**) aktiviert ist und die Kommunikation über https erfolgt.

Anleitung zur Absicherung eines Webservers mittels SSL.

Allgemein

Für die SAML-Authentifizierung wird Shibboleth verwendet.

Dafür gibt es zwei Teile:

- **I**dentity **P**rovider (**IdP**): Das ist jener Teil, der die Authentifizierung auf der Seite des Portals durchführt.
- **S**ervice **P**rovider (**SP**): Das ist jener Teil, der bei der Anwendung liegt, die im Portal integriert ist.

Klarerweise kommunizieren beide Teile miteinander. Da wir die Authentifizierung auf der Anwendungsseite realisieren, konzentrieren wir uns auf den Service Provider (SP). Der Identity Provider (IdP) ist bereits vorhanden und wird von der DVT bereitgestellt.

Offizielle Dokumentation von Shibboleth: https://wiki.shibboleth.net/confluence/display/SHIB2/Home

Installation des SP

Die Installation des SP wird vom RZ-Server mittels Templates (per 2016/11 RHEL7_2) durchgeführt.

Notwendige Rechte für den Konfigurations-User am Linux

siehe 4.4.3.1 Installation

Basiskonfiguration des Servers

Die Konfiguration kann grob in drei Teile eingeteilt werden:

- Konfiguration von Shibboleth SP
- Konfiguration von Apache
- Konfiguration der Anwendung Moodle, Drupal, etc.

Konfiguration von Shibboleth SP

Alle Konfigurationsdateien liegen unter /etc/dvt/shibboleth (vor RHEL7_2: /etc/shibboleth)

Die zentrale Datei für die Konfiguration, unabhängig vom verwendeten Apache-Server, lautet **shibboleth2.xml** .

shibboleth2.xml

Die Erstellung der **shibboleth2.xml** erfolgt ab RHEL7_2 automatisch mit dem Skript **shibconf.sh**

Die ab hier folgende Beschreibung ist nur für ältere Installationen (TiBS Drupal) relevant.

In dieser Datei können die entityId des SP, der zu verwendete IdP, dessen Metadaten und einige andere Einstellungsmöglichkeiten vorgenommen werden.

Hier ein Auszug, wo die meisten Einstellungen getroffen werden, wertvolle Infos liefert auch folgende Seite: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPGettingStarted

```
<!--
    The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined.
    Resource requests are mapped by the RequestMapper to an applicationId that
    points into to this section (or to the defaults here).
    -->
    <ApplicationDefaults entityID="https://<Hostname>/sp/<Anwendungsname>"
             signing="true" encryption="true"
             REMOTE_USER="eppn persistent-id targeted-id">

        <!--
        Controls session lifetimes, address checks, cookie handling, and the protocol handlers.
        You MUST supply an effectively unique handlerURL value for each of your applications.
        The value defaults to /Shibboleth.sso, and should be a relative path, with the SP computing
        a relative value based on the virtual host. Using handlerSSL="true", the default, will force
        the protocol to be https. You should also set cookieProps to "https" for SSL-only sites.
        Note that while we default checkAddress to "false", this has a negative impact on the
        security of your site. Stealing sessions via cookie theft is much easier with this disabled.
        -->
        <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
                  checkAddress="false" handlerSSL="true" cookieProps="; path=<Pfad>; secure; HttpOnly">

            <!--
            Configures SSO for a default IdP. To allow for >1 IdP, remove
            entityID property and adjust discoveryURL to point to discovery service.
            (Set discoveryProtocol to "WAYF" for legacy Shibboleth WAYF support.)
            You can also override entityID on /Login query string, or in RequestMap/htaccess.
            -->
            <SSO entityID="https://portal.tirol.gv.at/IdPWeb/shibboleth">
              SAML2 SAML1
            </SSO>
```

```
        <!-- SAML and local-only logout. -->
        <Logout>SAML2 Local</Logout>

        <!-- Extension service that generates "approximate" metadata based on SP configuration. -->
        <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>

        <!-- Status reporting service. -->
        <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>

        <!-- Session diagnostic service. -->
        <Handler type="Session" Location="/Session" showAttributeValues="false"/>

        <!-- JSON feed of discovery information. -->
        <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
    </Sessions>

    <!--
    Allows overriding of error template information/filenames. You can
    also add attributes with values that can be plugged into the templates.
    -->
    <Errors supportContact="<Support-Mailadresse>"
        helpLocation="/about.html"
        styleSheet="/shibboleth-sp/main.css"/>

    <!-- Example of remotely supplied batch of signed metadata. -->
    <!--
    <MetadataProvider type="XML" uri="http://federation.org/federation-metadata.xml"
          backingFilePath="federation-metadata.xml" reloadInterval="7200">
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
        <MetadataFilter type="Signature" certificate="fedsigner.pem"/>
    </MetadataProvider>
    -->

    <MetadataProvider type="XML" file="IdPWeb-metadata_portal.xml" />


    <!-- Map to extract attributes from SAML assertions. -->
    <AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>

    <!-- Use a SAML query if no attributes are supplied during SSO. -->
    <AttributeResolver type="Query" subjectMatch="true"/>

    <!-- Default filtering policy for recognized attributes, lets other data pass. -->
    <AttributeFilter type="XML" validate="true" path="attribute-policy.xml"/>

    <!-- Simple file-based resolver for using a single keypair. -->
    <CredentialResolver type="File" key="sp-key.pem" certificate="sp-cert.pem"/>

    <!--
    The default settings can be overridden by creating ApplicationOverride elements (see
    the https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplicationOverride topic).
    Resource requests are mapped by web server commands, or the RequestMapper, to an
    applicationId setting.

    Example of a second application (for a second vhost) that has a different entityID.
    Resources on the vhost would map to an applicationId of "admin":
    -->
    <!--
    <ApplicationOverride id="admin" entityID="https://admin.example.org/shibboleth"/>
    -->
  </ApplicationDefaults>
```

Es sind ein paar Merkmale mit <> umschlossen, jene sind zu ersetzen:

- **<hostname>** ersetzen mit Ihrem Hostnamen
- **<Anwendungsname>** ersetzen mit dem Namen der Anwendung, über die Benutzer authentifiziert werden sollen
- **<Pfad>** ersetzen mit dem Pfad, auf den das Cookie eingegrenzt werden soll. (z.B. /moodle)

- **<Support-Mailadresse>** ersetzen mit einer Mailadresse, die zu Ihrem Support führt

Und jetzt noch eine kurze Erläuterung zu folgenden Tags:

- <SSO entityID="https://portal.tirol.gv.at/IdPWeb/shibboleth">: Hierbei handelt es sich um die entityId des zu verwendeten IdP, gegen jenen eine Authentifizierung durchgeführt wird. Wenn Benutzer zwischen mehreren IdPs wählen sollen, muss hier ein DiscoveryService konfiguriert werden.
    - V-Portal Tirol (Testumgebung): <SSO entityID="https://v-portal.tirol.gv.at/IdPWeb/shibboleth">
    - Portal Tirol: <SSO entityID="https://portal.tirol.gv.at/IdPWeb/shibboleth">
- <MetadataProvider type="XML" file="IdPWeb-metadata_portal.xml" />: Diese XML-Datei erhalten Sie von der DVT und muss im o.a. Konfigurationsordner abgelegt werden.
    - V-Portal Tirol (Testumgebung): v-idp-metadata.xml
    - Portal Tirol: p-idp-metadata.xml
- <AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>: Bei erfolgreicher Authentifizierung überträgt der IdP dem SP per XML Daten über den Benutzer in Feldern. Die attribute-map.xml verbindet den URN-Feldnamen mit einem sprechenden Namen, mit dem die Anwendung dann weiter arbeiten kann.

Dokumentation: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPShibbolethXML

attribute-map.xml

Wie bereits darüber im letzten Punkt beschrieben, findet in der Datei attribute-map.xml ein Mapping der Felder statt.

Hier wiederum ein Auszug mit einem möglichen Mapping der Felder:

```
    <Attribute name="urn:oid:2.5.4.42"                 id="X-PVP-GIVEN-NAME" />
    <Attribute name="urn:oid:2.5.4.4"                  id="X-PVP-PRINCIPAL-NAME" />
    <Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="X-PVP-MAIL" />
    <Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="X-PVP-USERID" />
        <!-- optionale Attribute fuer die Organisationseinheit und Rolle -->
        <Attribute name="urn:oid:2.5.4.11"                  id="X-PVP-OU" />
        <Attribute name="urn:oid:1.2.40.0.10.2.1.1.3"       id="X-PVP-OU-GV-OU-ID" />
        <Attribute name="urn:oid:1.2.40.0.10.2.1.1.261.30"  id="X-PVP-ROLES" />
    <Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"  id="affiliation" />
```

Mit dem Attribute id kann dann die Anwendung in den Serverumgebungsvariablen den entsprechenden Wert finden.

Dokumentation: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeExtractor

Konfiguration von Apache

Unter Linux wird normalerweise schon bei der Installation eine Datei namens shib.conf angelegt mit den grundlegenden Einstellungen für Apache. Diese Konfiguration sollte im httpd.conf durch ein Include eingebunden sein.

Unter Windows ist diese Datei noch nicht eingebunden bzw. angelegt. Als Vorlage dienen hier die Dateien apache.config, apache2.config, apache22.config oder apache24.config, je nach Apache-Version, die im Ordner /etc/shibboleth liegen.

Hier wiederum ein Auszug aus einer **shib.conf**. Wichtig ist, dass das Apache-Modul mod_shib geladen und nach jeder Änderung der Apache-Server durchgestartet wird:

```
# https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig

# RPM installations on platforms with a conf.d directory will
# result in this file being copied into that directory for you
# and preserved across upgrades.

# For non-RPM installs, you should copy the relevant contents of
# this file to a configuration location you control.

#
# Load the Shibboleth module.
#
LoadModule mod_shib /your/path/to/lib/shibboleth/mod_shib_24.so

#
# Turn this on to support "require valid-user" rules from other
# mod_authn_* modules, and use "require shib-session" for anonymous
# session-based authorization in mod_shib.
#
ShibCompatValidUser Off

#
# Ensures handler will be accessible.
#
<Location /Shibboleth.sso>
  AuthType None
  Require all granted
</Location>

#
# Used for example style sheet in error templates.
#
<IfModule mod_alias.c>
  <Location /shibboleth-sp>
    AuthType None
    Require all granted
  </Location>
  Alias /shibboleth-sp/main.css /your/path/to/doc/shibboleth/main.css
</IfModule>

#
# Configure the module for content.
#
# You MUST enable AuthType shibboleth for the module to process
# any requests, and there MUST be a require command as well. To
# enable Shibboleth but not specify any session/access requirements
# use "require shibboleth".
#
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require shib-session
</Location>
```

Wie man am letzten Location-Eintrag sieht, kann so jedes beliebige Verzeichnis oder auch eine Datei mit Shibboleth geschützt werden. Wenn der Ordner /secure nicht existiert und im produktiven Betrieb nicht benötigt wird, muss der Location-Eintrag /secure entfernt werden.

Dokumentation: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig

⚠ Nach Abschluß der Konfiguration müssen beide Daemons neu gestartet werden. Der Shibboleth Daemon muss vor dem Apache neu gestartet werden.

```
/etc/init.d/shibd restart
/etc/init.d/httpd restart
```

Metadaten des SP an die DVT übermitteln

Die Metadaten des SP müssen bei den IdPs der Federation Teilnehmern (Portal Tirol) hinterlegt werden. Zu diesem Zweck senden Sie bitte die XML Datei mit den Metadaten ihres frisch konfigurierten Serviceproviders an die DVT. Die Datei kann bei einer Standardkonfiguration wie oben beschrieben unter folgender URL abgerufen werden: https://<hostname>/Shibboleth.sso/Metadata.

Senden Sie diese Datei unter dem Betreff: Registrierung Serviceprovider und unter Angabe des Namens und einer kurzen Beschreibung des Dienstes an support@tsn.at.

Hier ein Beispiel der Metadaten XML Datei:

```
<md:EntityDescriptor ID="_bc5caf5f4e3e3ffc537132ef23a05610f076a0ab" entityID="https://<hostname>/sp
/<Anwendungsname>">
        <md:Extensions>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512"/>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384"/>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha224"/>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha384"/>
                <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        </md:Extensions>
        <md:SPSSODescriptor AuthnRequestsSigned="1" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:
protocol urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:1.0:protocol">
                <md:Extensions>
                        <init:RequestInitiator Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-init"
Location="https://<hostname>/Shibboleth.sso/Login"/>
                </md:Extensions>
                <md:KeyDescriptor>
                        <ds:KeyInfo>
                                <ds:KeyName><hostname></ds:KeyName>
                                <ds:X509Data>
                                        <ds:X509SubjectName>CN=<hostname></ds:X509SubjectName>
                                        <ds:X509Certificate>
MIIDGDCCAgCgAwIBAgIJAIoRtErqju9rMA0GCSqGSIb3DQEBBQUAMCYxJDAiBgNV
BAMTG2R2dC1kdnQwMDgyLWdpcy50aXJvbC5sb2NhbDAeFw0xNDAyMTkwODQwMTla
Fw0yNDAyMTcwODQwMTlaMCYxJDAiBgNVBAMTG2R2dC1kdnQwMDgyLWdpcy50aXJv
bC5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANWIM8wp6k1K
sI1i5SAgmHsvEeIikeev1Jl40rjGZvWdQvr6JGhY5Roh19MWGiO/eZkVaRsjR5nv
yosReaIpeAdZxZZmenPxD2Pb7HrgJHIpj10evRy15JYXP4rMK7TIIpT07eS64B6h
VnfEb9IDRwmStiqno5j94Fbfrx6S9DuIi4BEQdDllCMKyqLLkV334TD2nXUnoTi0
EVf9Q5qtSVcHdxlZGYsMoLlOEBq9Pyj1T7I3DY7xBDGUDykGRIpbc1pwVeAteldr
Nsl6EGaZ+I5XKwynZBdkrMtrvtFO61bqx8DmTuKGHMeHITrjcn/BZDvhpFDGvquI
v91cxl5fJ+UCAwEAAaNJMEcwJgYDVR0RBB8wHYIbZHZ0LWR2dDAwODItZ2lzLnRp cm9sLmxvY2FsMB0GA1UdDgQWBBSjGEaVEvd/xtdWTBJMu
/upkGOrZjANBgkqhkiG 9w0BAQUFAAOCAQEAqzrYY1Ht995FDyVYOVwK6AOqvL1yGmp0TtH6VS15HvJw5l2A Ce6N
/6lwyArj2L7YjbjO7hIN3fej8iZ9oyYM3p8kulDiEfRtkqia2Kl4UMowwA4c mWgYtMkGfjnEnz9j8E3ItEyUmm0jk0Z0
/UBM5YeJxEzS0A+bD+eb671lVrktxLbT ZV/Eg9ol62U2CknswJi8En7ugrny9KOfjK91n60YEnYxGHniw/IR8a+j3E3BHg8i
GQKgmiKGvDBTFNBNb95yKgx13O8K384/covj6N+tlXxGbsB2rBRvjORE6b/zNNKP OPWhTFAbOYaqBLcOdzGUM+BM8UVbwEYnpukZfA==
                                        </ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                        <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
                        <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes192-cbc"/>
                        <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                        <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
                        <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
                </md:KeyDescriptor>
                <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://<hostname>/Shibboleth.sso/SAML2/POST" index="1"/>
                <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-
SimpleSign" Location="https://<hostname>/Shibboleth.sso/SAML2/POST-SimpleSign" index="2"/>
                <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Location="
https://<hostname>/Shibboleth.sso/SAML2/ECP" index="4"/>
        </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Bevor Sie keine Rückmeldung vom DVT Support Team über die erfolgreiche Eintragung der Metadaten erhalten haben, kann die nachfolgende Konfiguration nicht durchgeführt werden.

Konfiguration der Anwendung

Als abschliessender Schritt muss die Anwendung konfiguriert werden sodass die Anmeldeinformationen vom Shibboleth SP Modul übernommen werden.

Eine Anleitung für Drupal und Moodle findet sich anbei:

- SAML Authentifizierung für Drupal konfigurieren
- SAML Authentifizierung in MOODLE konfigurieren