simpleSAMLphp Service Provider

Overview

These are instructions for installing the simpleSAMLphp framework and configuring it to work with MyAccess. If your application is written in PHP, you may prefer to use simpleSAMLphp rather than Shibboleth.

These instructions assume you are using the Apache web server on a UNIX-like operating system. simpleSAMLphp will also work on Windows, but you will need to adjust the instructions. They were written for simpleSAMLphp 1.10.0, but will probably work on other versions.

For simpleSAMLphp to work, your PHP install needs to have the mcrypt module loaded. If you intend to use simpleSAMLphp with Drupal, you will also need the sqlite PHP module.

Install simpleSAMLphp

Download the latest version of simpleSAMLphp:

http://code.google.com/p/simplesamlphp/downloads/

Unpack the archive into /opt and make a symbolic link without the version number:

```
cd /opt
sudo tar -xvzf ~/simplsamlphp-x.x.x.tar.gz
sudo ln -s simplesamlphp-x.x.x simplesamlphp
```

Configure Apache

The www directory in the simpleSAMLphp distribution needs to be accessible through the web server. To do that, add the following line to your Apache configuration:

```
Alias /simplesaml /opt/simplesamlphp/www
```

Then reload your Apache configuration:

```
sudo apachectl graceful
```

On certain operating systems (Ubuntu, Debian) you may need to use "apache2ctl" instead of "apachectl".

Create SSL certificate

Generate an SSL certificate and key that simpleSAMLphp will use to secure communication with the UCSF MyAccess IdP. Run the following commands:

```
cd /opt/simplesamlphp/cert
sudo openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pem
```

Answer the questions, but don't worry too much about the answers. This information won't be visible to your users.

Configure simpleSAMLphp

Edit the file /opt/simplesamlphp/config/authsources.php and make the following changes.

Configure SSL cert

Let simpleSAMLphp know about the SSL certificate and key you just created. Find the "default-sp" section, and add these lines:

```
'privatekey' => 'saml.pem',
'certificate' => 'saml.crt',
```

Set entityID

Still in the "default-sp" section, find the "entityID" line and set the value to the domain name of your app followed by "/simplesaml". For example:

```
'entityID' => 'https://YOUR-DOMAIN-HERE.ucsf.edu/simplesaml',
```

Specify an Identity Provider

Still in the "default-sp" section, find the "idp" line and set the value to match the MyAccess IdP you want to use. Unless you've been told otherwise, use the staging IdP.

- **Production**: urn:mace:incommon:ucsf.edu (https://dp.ucsf.edu/idp/shibboleth is deprecated and should no longer be used)
- **Staging**: https://idp-stage.ucsf.edu/idp/shibboleth
- **Development**: https://idp-dev.ucsf.edu/idp/shibboleth

For example:

```
'idp' => 'https://idp-stage.ucsf.edu/idp/shibboleth',
```

Set Admin Password

Close authconfig.php and open config.php. Find the auth.adminpassword line, and set it to a value of your choice. Please do not use the same password you use elsewhere at UCSF. For example:

```
'auth.adminpassword' => 'not a good password',
```

Set Contact Information

Find the lines for technicalcontact_name and technicalcontact_email and set them to your name and email address, or those of the person who will be maintaining the application. For example:

```
'technicalcontact_name'     => 'Joe Schmo',
'technicalcontact_email'    => 'joe.schmo@ucsf.edu',
```

Convert Attribute Names

You'd probably rather deal with attribute names like "givenName" and "email" than "urn:oid:2.5.4.42" and "urn:oid:1.2.840.113549.1.9.1", wouldn't you? simpleSAMLphp will convert them for you, but you have to tell it to. Find the "authproc.sp" section, and add this line:

```
51 => array('class' => 'core:AttributeMap', 'oid2name'),
```

Drupal Only: Change Session Store

If you are going to use simpleSAMLphp with Drupal, you need to change the way that simpleSAMLphp stores its session data. Find the store.type and store.sql.dsn lines and change them to this:

```
'store.type' => 'sql'
'store.sql.dsn' => 'sqlite:/tmp/simplesamlsessiondb.sq3'
```

For this to work, you will also need to have the SQLite PHP module installed.

Load Metadata

Download the attached saml20-idp-remote.php and shib13-idp-remote.php files and save them into /opt/simplesamlphp/metadata/.

Save SP Metadata

To integrate with MyAccess, you will need to send us a copy of your SP's metadata. You can get that by visiting this URL, replacing "hostname.ucsf.edu" with your site's domain name:

https://hostname.ucsf.edu/simplesaml/module.php/saml/sp/metadata.php/default-sp