1. SimpleSAMLphp installation

1. SimpleSAMLphp installation

This guide is an exempel on how to do a base installation of SimpleSAMLphp.

- SimpleSAMLphp 1.16.1
- Operating System Ubuntu server 16.04 LTS

Preparations

Upgrade Ubuntu

Upgrade installed packages.
sudo apt-get update && sudo apt-get -y upgrade
sudo reboot

Install Apache and PHP

Any webserver software that supports PHP should work.
sudo apt-get -y install apache2 php libapache2-mod-php php-mcrypt php-dom php-curl

Disable Magic Quotes

Edit /etc/php/7.0/apache2/php.ini and add the following.
; Magic quotes
;
; Magic quotes for incoming GET/POST/Cookie data.
magic_quotes_gpc = Off
; Magic quotes for runtime-generated data, e.g. data from SQL, from exec(), etc.
magic_quotes_runtime = Off
; Use Sybase-style magic quotes (escape ' with '' instead of \').
magic_quotes_sybase = Off

Enabeling HTTPS

Redirect requests to HTTPS. Edit /etc/apache2/sites-enabled/000-default.conf in <VirtualHost *:80> add the following, change myhost.example.com to the FQDN of the server
Redirect permanent / https://myhost.example.com/blocked URL
NOTE: The self-signed (snakeoil) certificate from the ssl-cert package will be used. In production the certificate MUST be obtained from a CA
sudo a2enmod ssl && sudo a2ensite default-ssl

Apache alias

Add an alias for the SimplesSAMLphp location. Edit /etc/apache2/sites-available/default-ssl.conf in <VirtualHost *default*:443> add the folowing.
SetEnv SIMPLESAMLPHP_CONFIG_DIR /var/simplesamlphp/config
Alias /simplesaml /var/simplesamlphp/www
<Directory /var/simplesamlphp/www>
<IfModule mod_authz_core.c>
Require all granted
</IfModule>
</Directory>
Restart Apache.
sudo service apache2 restart

Install SimpleSAMLphp

Download and Extract SimpleSAMLphp

cd /tmp
wget 'https://github.com/simplesamlphp/simplesamlphp/releases/download/v1.16.1/simplesamlphp-1.16.1.tar.gz'
Create the directory and extract SimpleSAMLphp. The directory must be the directory configured in the Apache Virtual Host Alias directive.
sudo mkdir -p /var/simplesamlphp
sudo tar xvzfC simplesamlphp-1.16.1.tar.gz /var/simplesamlphp --strip 1

Generate a Self Signed Certificate

Messages sent between an IdP and a SP can be both encrypted and signed. In order to be able to perform this there need to be a private key and a certificate containing the public key. The SAML profile SAML 2.0 Interoperability Deployment Profile refer to the profie SAML V2.0 Metadata Interoperability Profile Version 1.0. According to the profile, no verification of the certificates MUST occur. The only requirement is that the certificate contains a public key. Therefore, it is recommended to generate your own self-signed certificate.
cd /var/simplesamlphp
sudo openssl req -x509 -sha256 -nodes -days 3652 -newkey rsa:2048 -keyout cert/server.key -out cert/server.crt

Configure SimpleSAMLphp

Generate cryptographic salt to be used in the next step.
tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo
Edit config/config.php change the following. For the secretsalt value use the salt that was generated in the previous step. Change the auth.adminpassword value.
'auth.adminpassword' => 'set new password here',
'admin.protectindexpage' => true,
'secretsalt' => 'random bytes inserted here',
'session.cookie.secure' => true,
'language.default' => 'sv',
'timezone' => 'Europe/Stockholm',
'metadata.sign.enable' => true,
'metadata.sign.privatekey' => 'server.key',
'metadata.sign.privatekey_pass' => null,
'metadata.sign.certificate' => 'server.crt',
'metadata.sign.algorithm' => 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha256',