New setup from pre-configured Simplesamlphp

1.)Pre-configure server w/ pre-req’s from <http://simplesamlphp.org>, then copy the provided /simplesamlphp folder to “/var/” “Installed packages were php, php-mcrypt (requires EPEL repo), php-xml” Any authsource not enabled in this package can be turned on by browsing to the appropriate folder under /simplesamlphp/modules/… and typing “touch enable”. You can see which modules are enabled from the default portal.

2.)First we configure apache with a certificate and alias like below in /etc/httpd/conf.d/ssl.conf

<VirtualHost \*>

ServerName service.example.com

DocumentRoot /var/www/service.example.com

Alias /simplesaml /var/simplesamlphp/www

</VirtualHost>

Above is the default but we set an alias for each social provider like so.

Alias /glwmulti /var/simplesamlphp/www

Alias /ficam1 /var/simplesamlphp/www

Alias /google /var/simplesamlphp/www

Alias /linkedin /var/simplesamlphp/www

Alias /windowslive /var/simplesamlphp/www

Alias /facebook /var/simplesamlphp/www

Alias /twitter /var/simplesamlphp/www

Alias /paypal /var/simplesamlphp/www

Alias /yahoo /var/simplesamlphp/www

Alias /verisign /var/simplesamlphp/www

Alias /Incommon /util

3.)”Config.php edits going from top to bottom” Open /simplesamlphp/config/config.php First set baseurlpath default below. I will leave the config w/ our config but wanted to show you the 2 different methods.

$config = array (

[...]

'baseurlpath' => 'simplesaml/',

Or..

We have it set like this for each individual social provider.

'baseurlpath' => $pathComponents[1] . '/',

4.)Next set admin password

'auth.adminpassword' => '\*\*\*',

5.)set secret salt for simple saml to generate secure hash values. Command in config file to generate random value. Run the command and paste in the value in the config.

\* A possible way to generate a random salt is by running the following command from a unix shell:

\* tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo

\*/

'secretsalt' => 'defaultsecretsalt',

6.)Set a Technicalcontact\_name & email

7.)Configure ‘metadata.sources’ => array( “depending on which metadata sources you will use this may change I’ll leave what we have in there as an example might need to chat to see which is needed here.” A cron job can be setup to automate metadata updates.

8.)Next file “config/authsources.php” this file will be configured based on which social providers you want to use. Each source has a link to setup an api key w/ the provider except for the opened sources. Generally you would login to say facebook w/ your login and configure your site to get an api key and secret which you would put into the authsources file. I’ll leave all the sources we had configured in the file with the api key and secret scrubbed so just fill in the blank on which ones you want to use..

9.) Next file “config/config-metarefresh.php” this configures the cron job to refresh metadata sources might need to talk on this one w/ Paul.

10.) Next file “metadata/saml20-idp-hosted.php” need to create a self signed cert I did mine with openssl to sign metadata and enter it here. Stick the certs in simplesamlphp/certs.

$metadata['\_\_DYNAMIC:1\_\_'] = array(

/\*

\* The hostname of the server (VHOST) that will use this SAML entity.

\*

\* Can be '\_\_DEFAULT\_\_', to use this entry by default.

\*/

'host' => '\_\_DEFAULT\_\_',

/\* X.509 key and certificate. Relative to the cert directory. \*/

'privatekey' => 'samlgwtest-saml.key',

'certificate' => 'samlgwtest-saml.crt',