Contrail Identity Provider

Installation

Contrail package installation

First, you will need to install the database with initial data.

```
# aptitude install contrail-federation-id-prov
```

Test the installation. The Identity Provider Database should be up-and-running.

```
$ curl -X GET --header "Content-Type: application/json" http://
localhost:8080/federation-id-prov/users/1
```

You should obtain output similar to this:

```
{"lastName":"","ids":"/users/1/
ids","password":"$2a$06$DCq7YPn5Rq63x1Lad4cll.kD3zZ845LsvMekyowTQk
2VNmbDdQsWO","ovfs":"/users/1/ovfs","slas":"/users/1/
slas","username":"coordinator","providers":"/users/1/
providers","email":"coordinator@contrail.eu","slats":"/users/1/
slats","roles":"/users/1/roles","applications":"/users/1/
applications","uuid":"5a947f8c-83d3-4da0-a52c-d9436ae77bb5","attributes":"/
users/1/attributes","firstName":"Coordinator","groups":"/users/1/groups"}
```

Password is hashed with bCrypt and in plaintext it should read as “password” :)

SimpleSAMLphp installation

Installation

If one wishes that `contrail-federation-id-prov` acts as Identity Provider supporting SAML2 and OpenID authentication, SimpleSAMLphp needs to be installed after Contrail package installation. SimpleSAMLphp-depended files are packaged with `contrail-federation-id-prov` package and are installed on local filesystem under `/usr/share/contrail/federation-`

`id-prov/simplesamlphp-1.9` after installation of the package.

First, you will need to install the latest SimpleSAMLphp. This has been tested with version 1.9. (currently the latest version). Grab the sources like this:
`$ wget` http://simplesamlphp.googlecode.com/files/simplesamlphp-1.9.0.tar.gz

Extract the package and copy the whole directory simplesamlphp-1.9.0 under `/usr/share/`
Lets name `/usr/share/simplesamlphp-1.9.0` directory as `${S_ROOT}`.

Set-up SimpleSAMLphp

Files needed

These files are packed together with `contrail-federation-id-prov` package under `/usr/share/contrail/federation-id-prov/simplesamlphp-1.9`:

```
./usr
./usr/share
./usr/share/simplesamlphp-1.9.0
./usr/share/simplesamlphp-1.9.0/metadata
./usr/share/simplesamlphp-1.9.0/metadata/saml20-sp-remote.php
./usr/share/simplesamlphp-1.9.0/modules
./usr/share/simplesamlphp-1.9.0/modules/saml2debug
./usr/share/simplesamlphp-1.9.0/modules/saml2debug/enable
./usr/share/simplesamlphp-1.9.0/modules/openid
./usr/share/simplesamlphp-1.9.0/modules/openid/enable
./usr/share/simplesamlphp-1.9.0/modules/contrailmodule
./usr/share/simplesamlphp-1.9.0/modules/contrailmodule/lib
./usr/share/simplesamlphp-1.9.0/modules/contrailmodule/lib/Auth
./usr/share/simplesamlphp-1.9.0/modules/contrailmodule/lib/Auth/Source
./usr/share/simplesamlphp-1.9.0/modules/contrailmodule/lib/Auth/Source/CAuth.php
./usr/share/simplesamlphp-1.9.0/modules/contrailmodule/default-enable
./usr/share/simplesamlphp-1.9.0/modules/openidProvider
./usr/share/simplesamlphp-1.9.0/modules/openidProvider/enable
./usr/share/simplesamlphp-1.9.0/log
./usr/share/simplesamlphp-1.9.0/config
./usr/share/simplesamlphp-1.9.0/config/authsources.php
./usr/share/simplesamlphp-1.9.0/config/module_openidProvider.php
./usr/share/simplesamlphp-1.9.0/config/config.php
./openssl-gen-cert
./contrail-openssl.cnf
./var
./var/lib
./var/lib/simplesamlphp-openid-provider
./etc
./etc/apache2
./etc/apache2/sites-available
./etc/apache2/sites-available/simplesaml-ssl
./etc/apache2/sites-available/simplesaml
```

Manual set-up

Overwrite `${S_ROOT}/config/authsources.php`. Edit the file (`${S_ROOT}/config/authsources.php`) and change `'contrailauth'` section so that username and password will be correct (mysql database user accessing to the contrail data).

Copy `config/config.php to ${S_ROOT}/config/config.php` and modify:

- optionally debug to TRUE
- 'auth.adminpassword' to something you remember
- 'secretsalt' to new value (read comment)

- 'technicalcontact_email'
- 'timezone' to e.g. 'Europe/Berlin'
- optionally 'logging.level' to SimpleSAML_Logger::DEBUG,
- optionally 'logging.handler' to 'file',

If you have modified logging variables, make sure you created `${S_ROOT} and chown-ed it to www-data:`

```
# mkdir -p ${S_ROOT}/log
# chown -R www-data:www-data ${S_ROOT}/log
```

This way logs are stored under `${S_ROOT}/log/simplesamlphp.log`

Copy `config/module_openidProvider.php` to `${S_ROOT}/config.`

Create directory `/var/lib/simplesamlphp-openid-provider` and change permissions:

```
# mkdir -p /var/lib/simplesamlphp-openid-provider
# chown -R www-data:www-data /var/lib/simplesamlphp-openid-provider
```

Copy `metadata/saml20-sp-remote.php` under `${S_ROOT}.` You will need to change metadata of 'http://localhost:8001/saml2/metadata/' according to the SP (e.g. contrail-federation-web).

Copy `modules/contrailmodule` to `${S_ROOT}/modules`

```
# cp -r modules/contrailmodule /usr/share/simplesamlphp-1.9.0/modules/
```

Enable `OpenID`, `OpenIDProvider`, optionally `saml2debug`:

```
# touch ${S_ROOT}/modules/openid/enable
# touch ${S_ROOT}/modules/openidProvider/enable
# touch ${S_ROOT}/modules/saml2debug/enable
```

These files are not included in the package, so you will need to edit these manually:

- Edit `/etc/php5/apache2/php.ini` and change `allow_call_time_pass_reference` variable from Off to On. This is due this issue https://groups.google.com/forum/?fromgroups#!topic/simplesamlphp/qgl_O6BFU9A topic `Enabling simpleSAMLphp as an OpenID Provider`: enabling openidProvider module, AS (contrailauth) is working as it should, I am getting these errors in /var/log/apache2:[Mon May 28 10:26:37 2012] [error] [client xx.xxx.xxx.xxx] PHP Fatal error: Class 'SimpleSAML_Logger_LoggingHandlerFile' not found in /usr/share/simplesamlphp-1.9.0-rc2/lib/Auth/OpenID/Server.php on line 1709, referer: https://ec2-xx-xx-xxx-xxx.compute-1.amazonaws.com/simplesaml/module.php/core/frontpage_auth.php
- Under `/etc/php5/conf.d/suhosin.ini` change the value of this variable from 512 to 2048:
    - `suhosin.get.max_value_length = 2048`

Create server certificates

Navigate to `/usr/share/contrail/federation-id-prov/simplesamlphp-1.9` and optionally edit `contrail-openssl.cnf`.

Run `openssl-gen-cert`.

Under `/usr/share/contrail/federation-id-prov/simplesamlphp-1.9/cert/` new private key and certificate will be generated to be used by apache and SimpleSAMLphp installation.

Copy `contrail-federation-idp.cert` and .key under `${S_ROOT}/cert.`

Dependecies

dep: apache2
- Apache HTTP Server metapackage

dep: libapache2-mod-php5
- server-side, HTML-embedded scripting language (Apache 2 module)

dep: openssl (>= 0.9.8g)
- Secure Socket Layer (SSL) binary and related cryptographic tools

dep: php-openid
- PHP OpenID library

dep: php-xml-parser (>= 1.2.8)
- PHP PEAR module for parsing XML

dep: php5
- server-side, HTML-embedded scripting language (metapackage)

dep: php5-mcrypt
- MCrypt module for php5

dep: php5-mhash
- MHASH module for php5

dep: zlib1g
- compression library - runtime

dep: php5-mysql
- MySQL module for php5

dep: php5-radius
- PECL radius module for PHP 5

Easiest way to install all these:

```
# apt-get install apache2 libapache2-mod-php5 openssl php-openid php-xml-parser php5 php5-mcrypt php5-mhash zlib1g php5-mysql php5-radius php5-curl
```

Apache2 set-up

Navigate to `/etc/apache2/sites-available/`. Copy the content of packaged under `/usr/share/contrail/federation-id-prov/simplesamlphp-1.9/etc/apache2/sites-available/simplesaml*` under `/etc/apache2/sites-available/`.

Edit `/etc/apache2/sites-available/simplesaml-ssl` to add paths of SSL cert and the key:

```
SSLCertificateFile      /usr/share/simplesamlphp-1.9.0/cert/contrail-federation-idp.cert
SSLCertificateKeyFile /usr/share/simplesamlphp-1.9.0/cert/contrail-federation-idp.key
```

Enable new sites pointing to SimpleSAMLphp:

```
/etc/apache2/sites-available# a2dissite default
/etc/apache2/sites-available# a2ensite simplesaml-ssl
/etc/apache2/sites-available# a2ensite simplesaml
```

Enable SSL module:

```
# a2enmod ssl
```
Restart apache2
```
# service apache2 restart
```

If you wish to navigate your browser via HTTPS to newly set-up contrail-federation-id-prov, you will need to import the certificate (`/usr/share/simplesamlphp-1.9.0/cert/contrail-federation-idp.cert`) of the server to your browser. Now, you should be able to see the Federation Identity Provider web interface and be able to log into the Contrail Federation Id Provider via console provided by the SimpleSAMLphp.