DEPLOY CAS CLIENT MODULE ON OBM SYSTEMS

April, 2014

System Requirements (Recommended)

- OBM 2.5.3

- LAMP Stack:
    - Apache 2.2.15
    - MySQL 5.5.34
    - PHP 5.4.21

- Roundcube Webmail 0.8.7

- Roundcube CAS Plugin
  https://github.com/dfwarden/Roundcube-CAS-Authn

- phpCAS 1.2.2
  https://wiki.jasig.org/display/CASC/phpCAS

- Pam_cas-2.0.11-esup-2.0.5

Preparation

1. Backup Roundcube configuration file

```
# cd /usr/share/obm/php/webmail/config/
# cp main.inc.php main.inc.php.bak
```

2. Make a new directory named “cas_authn” in Roundcube's plugin directory

```
# mkdir -p /usr/share/obm/php/webmail/plugins/cas_authn
# chown -R apache.apache /usr/share/obm/php/webmail/plugins/cas_authn
# ls -l  /usr/share/obm/php/webmail/plugins | grep cas
```

Deploy CAS Client Module

1. Download CAS client module to your client box

```
# git clone git@github.com:dfwarden/Roundcube-CAS-Authn.git
```

2. Upload the downloaded CAS client module to your OBM Systems

```
# rsync -avz -e <your-ssh-port> cas_authn/* root@<your-server-hostname>:/usr/share/obm/php/webmail/plugins/cas_authn/
```

3. Download phpCAS 1.2.2 to your OBM Systems

```
# cd /usr/share/obm/php/webmail/plugins/cas_authn/
# wget http://downloads.jasig.org/cas-clients/php/1.2.2/CAS-1.2.2.tgz
# tar zxvf CAS-1.2.2.tgz
# mv -v CAS-1.2.2/* .
# rm -Rf CAS-1.2.2
```

4. Chown “apache” user and group to directory containing the CAS client module

```
# chown -R apache.apache /usr/share/obm/php/webmail/plugins/cas_authn
```

5. Config your roundcube configuration to use new installed plugin

```
# cd /usr/share/obm/php/webmail/config/
# vim main.inc.php +383
// ----------------------------------
// PLUGINS
// ----------------------------------
// List of active plugins (in plugins/ directory)
//$rcmail_config['plugins'] = array('obm_cas_client');
$rcmail_config['plugins'] = array('cas_authn');
```

Save the config file and exit.

6. Rename the config.inc.php.dist file

```
# cd /usr/share/obm/php/webmail/plugins/cas_authn/
# cp config.inc.php.dist config.inc.php
```

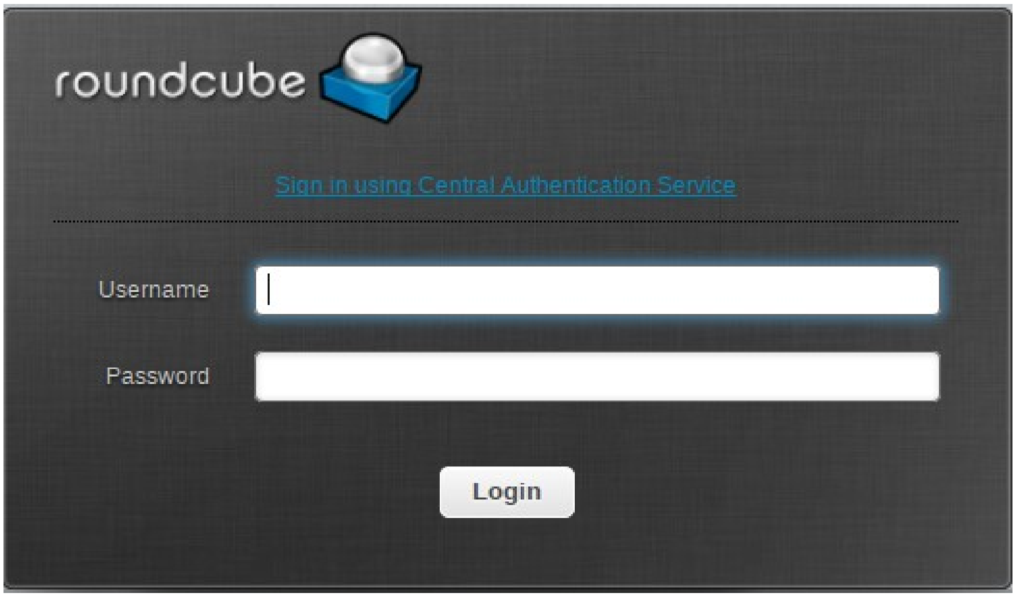
7. Reload your Apache Web Server

```
# service httpd reload
```

8. Access your Roundcube Webmail

https://<your-server-hostname>/webmail/

Your web client will be displayed as below:



9. Click the button “Sign in using Central Authentication Service” if you want to authenticate users with SSO

Deploy pam_cas module

Preparation

- openssl (1.0.0)
- development tools (gcc, cvs, libgcc...)

1. Download the module “pam_cas”

```
# cd /usr/share/obm/php/webmail/plugins/cas_authn/
# wget https://sourcesup.renater.fr/frs/download.php/2418/Pam_cas-2.0.11-esup-2.0.5.tar.gz
# tar zxvf Pam_cas-2.0.11-esup-2.0.5.tar.gz
```

2. Verify that openssl is installed on system

```
# rpm -qa | grep openssl
# yum insall openssl
```

3. Verify that the development tools are installed on system

```
# rpm -qa | grep gcc
# yum groupinstall "Development Tools"
```

4. Compile the module “pam_cas”

```
# cd Pam_cas-2.0.11-esup-2.0.5/sources/
# mv Makefile.redhat Makefile
# vim Makefile +8
```

Edit the content of Makefile as below:

```
CPFLAGS =       -O2 -fPIC
```

Save the file and exit.

```
# make
# make test
# ldd pam_cas.so
```

5. Review the configuration file of the module

```
# cd /usr/share/obm/php/webmail/plugins/cas_authn/Pam_cas-2.0.11-esup-2.0.5/
```

```
# less pam_cas.conf
```

6. Using the module “pam_cas” (Integration for the IMAP Server)

```
# cd /usr/share/obm/php/webmail/plugins/cas_authn/Pam_cas-2.0.11-esup-2.0.5/sources
```

```
# cp pam_cas.so /lib/security/
```

```
# cp ../pam_cas.conf /etc/
```

```
# ls -l /lib/security/
```

```
# cp /etc/pam.d/imap /etc/pam.d/imap.bak
```

```
# vim /etc/pam.d/imap
```

```
auth    sufficient /lib/security/pam_cas.so -simap://<your-server-hostname> -f/etc/pam_cas.conf
```

Save the file and exit.

```
# service saslauthd restart
```

```
# service cyrus-imapd restart
```

7. Configure the module “pam_cas”

Following steps mentioned in the link below:

http://www.esup-portail.org/consortium/espace/SSO_1B/tech/cas/cas_pam.html

8. Convert OBM’s SSL Certificate from PEM format to DER format

```
# openssl x509 -in <your-obm-certificate-path>/obm_certs.pem -out <your-obm-certificate-path>/obm_certs.der -outform DER
```

9. Import OBM’s SSL Certificate into Java keystore

```
# keytool -import -storepass changeit -keystore /usr/lib/jvm/java-1.6.0-openjdk.x86_64/jre/lib/security/cacerts -file <your-obm-certificate-path>/obm_certs.der -alias <your-obm-server-hostname>
```

10. Verify that OBM’s SSL Certificate is installed in Java keystore

```
# keytool -v -list -storepass changeit -keystore /usr/lib/jvm/java-1.6.0-openjdk.x86_64/jre/lib/security/cacerts
```

11. Edit the “cas.properties” file of CAS Server

```
# cd <your CATALINA_HOME>/webapps/cas/WEB-INF/
# vim cas.properties
```

Add contents to the configuration file as below:

```
...
server.name=https://<your-cas-server-hostname>:8443
cas.securityContext.ticketValidator.casServerUrlPrefix=${server.prefix}/proxyValidate
host.name=<your-cas-server-hostname>
...
```

Save the file and exit

12. Restart Apache Tomcat Server

```
# cd /opt/openroad/bin/
# ./shutdown.sh
# ./startup.sh
# lsof -i :8443
```

13. Verify that module “pam_ldap” is installed on your systems

```
# rpm -qa | grep pam_ldap
```

```
# yum install pam_ldap
```

14. Edit the configuration file “/etc/pam.d/imap”

```
# vim /etc/pam.d/imap
```

Edit contents as below:

```
auth    sufficient /lib/security/pam_cas.so -simap://<your-obm-server-hostname> -f/etc/pam_cas.conf

account    required     pam_ldap.so

#auth       required     pam_nologin.so

#auth       include      password-auth

#account    include      password-auth

#session    include      password-auth
```

Save the file and exit..

15. Edit the configuration file “/etc/pam_cas.conf”

```
# vim /etc/pam_cas.conf
```

Edit contents as below:

```
host <your-cas-server-hostname>

port <your-cas-server-ssl-port>

uriValidate /cas/proxyValidate

ssl on

debug on

trusted_ca <path-to-cas-server-certs>/cas_server_certs.pem
```

16. Edit the configuration file “/etc/sysconfig/saslauthd”

```
# vim /etc/sysconfig/saslauthd
```

Edit contents as below:

```
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/var/run/saslauthd
# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam
# Options sent to the saslauthd. If the MECH is other than "pam" uncomment the next line.
# DAEMONOPTS=--user saslauth
# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS="-c"
```

17. Backup and edit the configuration file “/etc/pam_ldap.conf”

```
# cp /etc/pam_ldap.conf /etc/pam_ldap.conf.bak
# vim /etc/pam_ldap.conf
```

Edit contents as below:

```
...
base dc=local
...
```

18. Restart the service saslauthd on your systems

```
# /etc/init.d/saslauthd restart
# ps -ef | grep saslauthd
```

19. Edit the file “cas_authn.php” of the CAS client module

```
# vim cas_authn.php +106
...
// If control reaches this point, user is authenticated to CAS.
            $user = phpCAS::getUser();
            $user .= '@<your-mail-domain>';
            $pass = '';
...
```

20 (Optional). Configure OBM Systems to authenticate users via SSO

```
# cp /etc/obm/obm_conf.inc /etc/obm/obm_conf.inc.bak
# vim /etc/obm/obm_conf.inc
Edit contents as below:
// authentification : 'CAS' (SSO AliaSuite), 'ldap' (LDAP authentication) or 'standalone' (default)
$auth_kind = 'CAS';
$cas_server = '<your-cas-server-hostname>';
$cas_server_port = <your-cas-server-port>;
$cas_server_uri = '/cas';
// CAS server SSL validation: 'ca' for
//      certificate from a CA, empty for no SSL validation.
$cas_validation = "ca";
// CAS server certificate in PEM format, used when CAS validation is set to
//      'self' or 'ca'.
$cas_cert = '<path-to-cas-server-certs>/cas_server_certs.pem';
```