SAML and oVirt 3.5

Same way as kerberos is supported for oVirt 3.5 there is also support for SAML via apache module.

There are few SAML apache modules, but I chose mod_auth_mellon, as it has very nice documentation.

First of all we need to setup some identity provider. I chose OpenAM. Please follow steps to quick install of OpenAM with embedded OpenDJ ldap.

OK I presume, that you have up and running OpenAM on tomcat with embedded OpenDJ ldap. Next step is to setup ourt OpenAM as Identity Provider. Go to 'common-tasks' tab and hit the button 'Created Hosted Identity Provider'. Set name of your metadata(your URL). Signing key, if you want. Then create new CoT and named it as you like, not important for us. Now very important thing. You need to add attribute mapping, so we are able to map the uid of user in ldap to REMOTE_USER env of apache. Please set 'Name in assertion' to 'common-name' and 'Local attribute name' to 'cn'. And we are done.

Now we need to setup oVirt apache as service provider(I am using RHEL 6.6):

- Install mod_auth_mellon apache module.

```
$ yum install -y mod_auth_mellon
```

- Obtain IdP metadata.

```
$ wget $YOUR_IDP_URL/saml2/jsp/exportmetadata.jsp -O
/etc/httpd/mellon/idp.xml
```

- Create SP metadata.

```
$/usr/libexec/mod_auth_mellon/mellon_create_metadata.sh
WHAT_EVER_SP_ENTITY_NAME_ID ENTITY-ID https://ovirt/mellon
```

- Step 3 will create for you three files:

```
WHAT_EVER_SP_ENTITY_NAME_ID.xml
WHAT_EVER_SP_ENTITY_NAME_ID.key
WHAT_EVER_SP_ENTITY_NAME_ID.cert
```

- copy them to the */etc/httpd/mellon* and assure that all files and folder can be read by apache.
- Create mod_auth_mellon configuration

```
$ cd /etc/httpd/conf.d && cat >> auth_mellon.conf << EOF
LoadModule auth_mellon_module modules/mod_auth_mellon.so

<Location />
 MellonSPCertFile
/etc/httpd/mellon/WHAT_EVER_SP_ENTITY_NAME_ID.cert
 MellonSPPrivateKeyFile
/etc/httpd/mellon/WHAT_EVER_SP_ENTITY_NAME_ID.key
 MellonSPMetadataFile
/etc/httpd/mellon/WHAT_EVER_SP_ENTITY_NAME_ID.xml
 MellonUser "common-name"
 MellonEndpointPath /mellon
 RewriteEngine on
 RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
 RewriteRule ^(.*)$ - [L,P,E=REMOTE_USER:%1]
 RequestHeader set X-Remote-User %{REMOTE_USER}s
</Location>
<Location /ovirt-engine/api>
 MellonEnable "auth"
 Require valid-user
 AuthType "Mellon"
</Location>
EOF
```

- In OpenAM go to 'common-tasks' , hit 'register remote service provider'. Upload your SP metadata *WHAT_EVER_SP_ENTITY_NAME_ID.xml*. Choose already created CoT. That's all, click 'configure'.

We had setup both mod_auth_mellon as SP and OpenAM as IdP. Last thing is to setup oVirt to respect this setup.

- *$ yum install -y ovirt-engine-extension-aaa-misc ovirt-engine-extension-aaa-ldap*
- *cd /etc/ovirt-engine/extensions.d/*
- *$ cat >> http-authn.properties << EOF*
  ovirt.engine.extension.name = http-authn
  ovirt.engine.extension.bindings.method = jbossmodule
  ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine-extensions.aaa.misc
  ovirt.engine.extension.binding.jbossmodule.class = org.ovirt.engineextensions.aaa.misc.http.AuthnExtension
  ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
  ovirt.engine.aaa.authn.profile.name = http
  ovirt.engine.aaa.authn.authz.plugin = ldap-authz-simple_opendj
  config.artifact.name = HEADER
  config.artifact.arg = X-Remote-User
  EOF
- *$ cat >> ldap-authz-simple_opendj.properties << EOF*
  ovirt.engine.extension.enabled = true
  ovirt.engine.extension.name = ldap-authz-simple_opendj
  ovirt.engine.extension.bindings.method = jbossmodule
  ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine-extensions.aaa.ldap
  ovirt.engine.extension.binding.jbossmodule.class = org.ovirt.engineextensions.aaa.ldap.AuthzExtension
  ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
  config.profile.file.1 = /etc/ovirt-engine/aaa/ldap-authz-simple_opendj.properties
  EOF
- *cat >> /etc/ovirt-engine/aaa/ldap-authz-simple_opendj.properties << EOF*
  include = <opendj.properties>

  pool.default.serverset.type = single
  pool.default.serverset.single.server = YOUR_OPEN_AM_URL

```
pool.default.serverset.single.port = YOUR_EMBEEDED_OPENDJ_PORT
# default 50389

pool.default.auth.type = simple
pool.default.auth.simple.bindDN = cn=Directory Manager
pool.default.auth.simple.password = XXXXXXX
EOF
```

- `cat >> /usr/share/ovirt-engine-extension-aaa-ldap/profiles/opendj.properties  << EOF`

```
include = <simple.properties>

attrmap.map-principal-record.attr.PrincipalRecord_DN.map = _dn
attrmap.map-principal-record.attr.PrincipalRecord_ID.map =
entryUUID
attrmap.map-principal-record.attr.PrincipalRecord_NAME.map =
uid
attrmap.map-principal-record.attr.PrincipalRecord_PRINCIPAL.map
= uid
attrmap.map-principal-
record.attr.PrincipalRecord_DISPLAY_NAME.map = displayName
attrmap.map-principal-
record.attr.PrincipalRecord_DEPARTMENT.map = department
attrmap.map-principal-
record.attr.PrincipalRecord_FIRST_NAME.map = givenName
attrmap.map-principal-record.attr.PrincipalRecord_LAST_NAME.map
= sn
attrmap.map-principal-record.attr.PrincipalRecord_TITLE.map =
title
attrmap.map-principal-record.attr.PrincipalRecord_EMAIL.map =
mail

attrmap.map-group-record.attr.GroupRecord_DN.map = _dn
attrmap.map-group-record.attr.GroupRecord_ID.map = entryUUID
attrmap.map-group-record.attr.GroupRecord_NAME.map = cn
attrmap.map-group-record.attr.GroupRecord_DISPLAY_NAME.map =
description

sequence-init.init.600-opendj-init-vars = opendj-init-vars
sequence.opendj-init-vars.010.description = set base dn
```

```
sequence.opendj-init-vars.010.type = var-set
sequence.opendj-init-vars.010.var-set.variable =
simple_attrsBaseDN
sequence.opendj-init-vars.010.var-set.value = namingContexts
sequence.opendj-init-vars.020.description = set user attribute
sequence.opendj-init-vars.020.type = var-set
sequence.opendj-init-vars.020.var-set.variable =
simple_attrsUserName
sequence.opendj-init-vars.020.var-set.value = uid
sequence.opendj-init-vars.030.description = set principal
record attributes
sequence.opendj-init-vars.030.type = var-set
sequence.opendj-init-vars.030.var-set.variable =
simple_attrsPrincipalRecord
sequence.opendj-init-vars.030.var-set.value = entryUUID, uid,
displayName, department, givenName, sn, title, mail
sequence.opendj-init-vars.040.type = var-set
sequence.opendj-init-vars.040.var-set.variable =
simple_filterUserObject
sequence.opendj-init-vars.040.var-set.value =
(objectClass=person)(uid=*)
sequence.opendj-init-vars.050.description = set group record
attributes
sequence.opendj-init-vars.050.type = var-set
sequence.opendj-init-vars.050.var-set.variable =
simple_attrsGroupRecord
sequence.opendj-init-vars.050.var-set.value = entryUUID, cn,
description
sequence.opendj-init-vars.060.description = set group object
filter
sequence.opendj-init-vars.060.type = var-set
sequence.opendj-init-vars.060.var-set.variable =
simple_filterGroupObject
sequence.opendj-init-vars.060.var-set.value =
(objectClass=groupOfUniqueNames)
sequence.opendj-init-vars.070.description = set group member
filter
sequence.opendj-init-vars.070.type = var-set
sequence.opendj-init-vars.070.var-set.variable =
```

```
simple_attrGroupMemberDN
sequence.opendj-init-vars.070.var-set.value = uniqueMember
EOF
```

- Check correct permissions of all *properties file, it has to be readable by oVirt*

Now we will create test user in OpenDJ.

```
Go to OpenAM -> 'Access Control' tab -> select your realm
(default /). Click 'Subjects' tab -> Add new user -> Fill
appropriate values. (ie user1.)
```

Now go to oVirt webadmin and search within '*http*' profile for *user1* and assign him permissions. Now go to ovirt-engine/api URL and you will be forwarded to OpenAM login screen, fill your credentials and you are now able to access rest-api.