OpenAM Setup v0.1

Tomcat

Standard stuff.

Initial Wizard

Default User Password

User = amadmin
Pass = Adam's password+

Server Settings

Server URL = openam.tin-pham.com:8080
Cookie Domain = .tin-pham.com
Platform Local = en_US
Configuration Director = /opt/openam-config

> Serious bug here, you MUST use the fully quantified domain name, openam.tin-pham.com and not tin-pham.com in your browser url.

Configuration Data Store Settings

First Instance = selected

Data Store = OpenDS or Sun Java System Directory Server
SSL/TLS Enabled = no
Host Name = localhost
Port = 50389
Admin Port = 5444
JMX Port = 1689
Root Suffix = dc=openam,dc=tin-pham,dc=com
Login ID = cn=Directory Manager
Password = Adam's password+

Originally I wanted to use OpenDJ but there's some issues all over the place so instead I will use their internal data store for the Configuration Data Store settings. Also,

> ForgeRock also **recommends** using the embedded LDAP server as the **configuration** store when you have **four or fewer instances of OpenAM** in production.

> Due to a bug, hostname with a single . will not work. For example, kyrypton.com will not work but www.krypton.com or opendj.krypton.com will work.

> Regarding the Root Suffix, I wonder if we need to use a different one for the config data versus user data.

If you really want to use an external data store for the Configuration read https://wikis.forgerock.org/confluence/display/openam/Configure+an+external+OpenDJ+or+OpenDS+as+the+configuration+store

User Data Store Settings

The OpenAM data store is not supported in the production environment per the wizard.

Other User Data Store = selected

User Data Store Type = OpenDS

SSL/TLS Enabled = no
Host Name = opendj.tin-pham.com
Port = 1389
Root Suffix = dc=tin-pham,dc=com
Login ID = cn=Directory Manager

Site Configuration

Select No

Default Policy Agent User

Set password for policy agent must be different so using 2Keys.

Summary Details

Configuration Store Details

SSL/TLS Enabled	No
Host Name	tin-pham.com
Listening Port	1389
Root Suffix	dc=opendj.tin-pham,dc=com
User Name	cn=Directory Manager
Directory Name	/opt/openam-config

User Store Details

SSL/TLS Enabled	No
Host Name	tin-pham.com
Listening Port	1389
Root Suffix	dc=opendj.tin-pham,dc=com
User Name	cn=Directory Manager
User Data Store Type	OpenDS

Site Configuration Details

This instance is not setup behind a load balancer

Run

The LDAP operation failed., refer to install.log under /opt/openam-config for more information.

Another bug in a sense. Carefully reading the manual,

If you decide to use an existing installation of OpenDJ for configuration data, then you **must** first relax the restriction on objects with multiple structural object classes, by using the OpenDJ *dsconfig* command before completing OpenAM configuration.

Enter this into the command line

```
cd /opt/opends.0
./dsconfig -h opendj.tin-pham.com -p 4444 -D "cn=Directory Manager" -w
****** set-global-configuration-prop --set
single-structural-objectclass-behavior:warn -X -n
```

When the configuration completes, click Proceed to Login, and then login as OpenAM administrator.

There is a note from the online manual,

> Restrict permissions to the configuration directory (by default $HOME/openam, where $HOME corresponds to the user who runs the web container).

But no instructions on how to do this or even why we need to do this.

Ah, I figured it out. By default OpenAM selects the user running the web container's home directory as the location for the OpenAM configuration files. It is saying to set permissions up so other users can not modify it. In our case, we are using serveradmin as the user running the web container, but then we choose a more explicit directory /opt/openam-config and is already configured to only allow staff and svradm.