Installing OpenAM

Guide for deploying OpenAM, and initial configuration.

Table of Contents

Prerequisites

- OpenAM Server Setup
- Acquiring OpenAM Packages

Initial OpenAM installation

1. After having acquired the war (see Acquiring OpenAM Packages), copy it to Tomcat

   ```
   > sudo cp OpenAM-12.0.0.war /var/lib/tomcat8/webapps/openam.war
   ```

   Note that we copied to "openam.war" so that it'll show up in your URL as **/openam**
2. If you've properly set up Apache, you should now be able to access the deployed OpenAM instance by navigating to the URL in a browser, e.g., https://identity.yourhost.com/openam. You should see the OpenAM configuration page asking if you want the default or the custom configuration. Click the link "Create New Configuration" under Custom Configuration.
3. Read and accept the license agreement by checking "I accept the license agreement" then click Continue.
4. Enter the password you would like to use for the 'amadmin' user
5. Make the following changes to the Server Settings:
   - Ensure the Server URL matches your FQDN (which you should have set up prior to deploying the openam.war).
   - Change the protocol and port from http:80 to https:443 if you're using SSL (Recommended).
   - Cookie Domain should be auto-filled with ".yourdomain.tld", e.g., ".yourdomain.com"
   - The configuration directory can be left as the default: **/usr/share/tomcat8/openam**, tomcat's home directory on Ubuntu running Tomcat8.
   - Click Next
6. Make the following selections in the Configuration Data Store Settings:
   - Leave the default "First Instance" radio button selected
   - Leave the "OpenAM" radio button selected for Configuration Data Store, unless you're using some other external instance.
   - Copy/Write down the encryption key in case you want to use it for accessing settings with OpenAM admin tools. This can be used to encrypt/decrypt configuration exports, etc.
   - Usually you'd alter the root suffix to match your FQDN, but since this is just an internal configuration store, you can leave it as the default. If you were creating a new external store, or making use of a pre-existing one, you'd need to enter the information for that datastore instead.
   - Click Next.
7. Make the following selections in the User Data Store Settings:
   - It's not recommended to use the embedded OpenDJ user store in production environments, but currently that is what DCDS has been using. Once a fully set up external LDAP/OpenDJ store is tested, this documentation will be updated to reflect that.
   - Select the "OpenAM User Data Store" radio button
     - You'll see the warning: **The OpenAM user data store is not recommended for large scale production environments or deployments with a complex topology.**
   - Click Next.
8. Make the following selections in the Site Configuration Settings:
   - Currently DCDS does not set up load balancing within OpenAM. Leave the default of "No" selected, and click Next.
9. Make the following selections in the Default Policy Agent User Settings:
   - Choose and enter a password for the Policy Agent. This will be used when setting up the Web Agent for Policy enforcement later.
   - Click Next.
10. Review your configuration choices, and if satisfied, click Create Configuration.
11. If configuration completed successfully, you should see a dialog saying "Configuration Complete".
12. Click the link to "Proceed to login". You should be brought to the OpenAM login page.
    - If the login page does not appear, review the set up of your system's FQDN.
13. Login with the 'amadmin' user, which you specified the password for in step 4. This should bring you to the OpenAM Administration Console.