Installing OpenAM Agent

Guide for setting up an OpenAM Web Agent. See OpenAM's documentation as a reference: https://backstage.forgerock.com/#!/docs/openam-policy-agents/3.3.0/web-install-guide/

Table of Contents

The below guide shows you how to set up the Agent for the API. You can also set one up in front of your Mapserver, if you have one.

> Note: Even though we're using 3.3.4, in many cases the OpenAM documentation wasn't changed since 3.3.0. Just be sure you've downloaded version 3.3.4 of the Web Policy Agent.

> **Prerequisites**
> - Acquiring OpenAM Packages

Setup Web Agent

For the purposes of this guide, we'll assume the you placed the ***Apache-v2.4-Linux-64-Agent-3.3.4.zip*** file in the **/opt** directory on the Data VM.

1. Unzip the archive:

```
> cd /opt
> unzip Apache-v2.4-Linux-64-Agent-3.3.4.zip
Archive:  Apache-v2.4-Linux-64-Agent-3.3.4.zip
   creating: web_agents/
   ...
>
```

   The 'web_agents' directory should not appear at this location.

2. Use the cd to navigate to the apache agent directory:

```
> cd web_agents/apache24_agent
> ls -l
drwxr-xr-x 2 user user 4096 Jan 15  2015 bin
-rw-r--r-- 1 user user 8770 Jan 15  2015 binary-license.txt
drwxr-xr-x 2 user user 4096 Jan 15  2015 config
drwxr-xr-x 2 user user 4096 Jan 15  2015 data
drwxr-xr-x 2 user user 4096 Jan 15  2015 etc
drwxr-xr-x 2 user user 4096 Jan 15  2015 installer-logs
drwxr-xr-x 2 user user 4096 Jan 15  2015 lib
-rw-r--r-- 1 user user 8770 Jan 15  2015 license.txt
drwxr-xr-x 2 user user 4096 Jan 15  2015 locale
-rw-r--r-- 1 user user 5797 Jan 15  2015 README
>
```

> If you've previously installed an agent on this machine, there'a a config file that may point to the installation path: '**/etc/.amAgentLocator**'. Delete or edit this to match your new configuration to allow the setup script to operate properly

3. Before you begin the agentadmin setup, create a file that contains the Agent password you entered when you set up OpenAM:

```
> cd /opt/web_agents
> echo "YourAgentPassword" > agentpass.txt
```

Now when the agentadmin setup asks you for the file containing the password, enter the directory: ex) **/opt/web_agents/agentpass.txt**

4. Depending on your Apache setup, you may not have an ***httpd.conf*** config file. The agentadmin script will warn you that you didn't enter a proper Apache config path, so if it doesn't exist, create it:

```
> touch /etc/apache2/httpd.conf
```

5. Run the agentadmin setup script, which will ask you questions regarding your instance so it can set up the agent

```
# First, stop the apache service if it's running
> service apache2 stop
* Stopping web server apache2
*
> bin/agentadmin --install

Please read the following License Agreement carefully:


[Press <Enter> to continue...] or [Enter n To Finish]

# Press 'n' to finish, and it will ask you if you agree:

Do you completely agree with all the terms and conditions of this License
Agreement (yes/no): [no]: yes # Type yes

...

************************************************************************
Welcome to the OpenAM Policy Agent for Apache Server.
************************************************************************

Enter the complete path to the directory which is used by Apache Server to
store its configuration Files. This directory uniquely identifies the
Apache Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Apache Server Config Directory Path [/opt/apache24/conf]: /etc/apache2
# NOTE this is the path to enter on Ubuntu, it varies on other Linux
distributions


Enter the URL where the OpenAM server is running. Please include the
deployment URI also as shown below:
(http://openam.sample.com:58080/openam)
[ ? : Help, < : Back, ! : Exit ]
OpenAM server URL: https://identity.yourserver.com:443/openam # Type in the
server, including protocol at the end of the domain, where your Identity server
is located, ending with the
                                                              # deployment
endpoint, usually /openam

Enter the Agent URL as shown below: (http://agent1.sample.com:1234)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: https://data.yourserver.com:443 # Enter the base URL for your EM-API
```

```
installation on the Data VM


Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: DataVMAgent # Remember this name, as you'll need it
to set up Policies/Agents in OpenAM's GUI


Enter the path to a file that contains the password to be used for identifying
the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /opt/web_agents/agentpass.txt


WARNING:
Password validation cannot be done as OpenAM server is not running.

-----------------------------------------------
SUMMARY OF YOUR RESPONSES
-----------------------------------------------
Apache Server Config Directory : /etc/apache2
OpenAM server URL :
https://identity.yourserver.com:443/openam
Agent URL : https://data.yourserver.com:443
Agent Profile name : DataVMAgent
Agent Profile Password file name : /opt/web_agents/agentpass.txt
Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]: 1

Creating directory layout and configuring Agent file for Agent_001
instance ...DONE.
Reading data from file /opt/web_agents/pass.txt and
encrypting it ...DONE.
Generating audit log file name ...DONE.
Creating tag swapped OpenSSOAgentBootstrap.properties file for instance
Agent_001 ...DONE.
Creating a backup for file /etc/apache2/httpd.conf ...DONE.
Adding Agent parameters to
/opt/home/dcds/web_agents/apache24_agent/Agent_001/config/dsame.conf
file ...DONE.
Adding Agent parameters to /etc/apache2/httpd.conf file ...DONE.

SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/opt/web_agents/apache24_agent/Agent_001/config/OpenSSOAgentBootstrap.properties
Agent Configuration Tag file location
/opt/web_agents/apache24_agent/Agent_001/config/OpenSSOAgentConfiguration.propert
ies
Agent Audit directory location:
/opt/web_agents/apache24_agent/Agent_001/logs/audit
Agent Debug directory location:
/opt/web_agents/apache24_agent/Agent_001/logs/debug
```

```
Install log file location:
/opt/web_agents/apache24_agent/installer-logs/audit/install.log
```

```
Thank you for using OpenAM Policy Agent

>
```

6. You should see the above successful installation with a Summary of files to take note of.
7. Start the apache service to verify the agent is installed, using the following command:

   ```
   > service apache2 start
    * Starting web server apache2 # Ensure it started without error
    *
   ```

   Depending on your Apache configuration, if you created ***httpd.conf*** without having any other configs refer to it, you'll need to copy the line the setup script added over to your ***apache2.conf*** file

   ```
   > vi /etc/apache2/httpd.conf
   # Look for a line like this:
   include /opt/web_agents/apache24_agent/Agent_001/config/dsame.conf
   ```

   If the line "include /..../dsame.conf exists in ***httpd.conf*** , copy and place it at the bottom of your ***apache2.conf*** file. Once completed, reload apache.
8. Now that apache2 is running again with the Agent properly loaded, open a browser, and enter the data VM URL. You should see a 403 Forbidden or be redirected to an OpenAM login screen.
9. You can now set up the Agent in the OpenAM Administration GUI.

> Be sure to return to OpenAM Configuration and to add the Custom header value to the API application, now that we've added the Agent.

Add Agent to OpenAM

Sign into the OpenAM Administrative GUI to add the Agent.

1. Navigate to Access Control / (Top Level Realm) Agents, and You'll be on the Web tab
2. Under the Agent table, click "New...". You'll be at a form called "New Web", where you'll enter the details for the Web Agent:
   a. Name: Enter the Profile Name you entered when you set up the Agent on the Data VM
   b. Password: Enter the password you set for the Agent when you initially set up the OpenAM Console
   c. Configuration: Leave as default, Centralized
   d. Server URL: Enter the full path, including port and deployment path, to your OpenAM instance, e.g., https://identity.yourserver.com:443/openam
   e. Agent URL: Enter the full path, including port, to your Data VM, e.g., https://data.yourserver.com:443 (the same as the Agent URL in the Agent setup steps)
3. Click "Create". You should now back at the Web tab, with your Agent now listed in the Agents table.

Configure Policies

1. Navigate to Access Control / (Top Level Realm) Policies
2. Click "Add New Application"
3. Provide a Name and description: API
4. Click Next.
5. Define Resource Patterns
   a. There's a list of available patterns. By default, there's usually just one, "*". Click on that to add it to the column on the right.
   b. When the the asterisk (*) is highlighted, and this is where you'll enter the base URL of the API: https://data.yourserver.com:443/* Note the asterisk on the end. Click the + button. It will add it to the Resources column.
   c. For the next one, which it has again highlighted the asterisk, enter the the full URL, including protocol, to your API deployment path, e.g., https://data.yourserver.com:443/api/*, and click the + button.
   d. For this final one, enter the same URL as in the previous step, but also append "?*", so it looks like this: https://data.yourserver.com:443/api/*?*

    e. Click the + button.
    f. Click Next, then click Finish. You should be back at the Applications listing, now with your API entry added.

6. Find your "API" entry in the applications table. Note there's a pencil icon, and a page icon. If you hover over them with your mouse, the pencil says Edit Application, and the page says View Policies. Click on the Page/View Policies icon.
7. Click Add New Policy. You will be brought to a Policy creation form, where you can provide details for the policy.
    a. Name: API Policy
    b. Description: Policy governing API
    c. Click Next.
8. You should see a list of available Patterns, which you entered in the previous steps. Add each of them to the column on the right by clicking on them, then also clicking on the + button on the right to add it to the Resources. Click Next.
9. Check the Actions checkbox, which will select all actions for you, leave the default selection of Allow for each action, and click Next.
10. Click "+ Subject Condition", and in the Type dropdown that is added, select "Authenticated Users". Now you need to click and drag the box with this condition up into the green conditional box above, then click Next.
11. Click "+ Environment Condition", and in the Type dropdown, select "Authentication to a realm". A box will be provided. Enter "/" (without quotes), which is the default top level realm. Click and drag this box up into the green conditional box above, as in the previous step. Click Next.
12. No Response Attributes will be set, so click Next again.
13. Review your selections, and click Finish. You'll now see your Policy listed, with the resources it protects. Click Back.
14. Navigate to your Agent tab
    a. Click on your Agent in the Agent table, and click the OpenAM Services tab
    b. Scroll to the bottom of the page, in the Policy Client Service section. The last field is "Application". Enter the name of the Application you entered in the Policy for the API. In the above example, it was "API".
    c. Click Save.
15. Now to ensure everything has taken effect, restart the apache2 process on the Data VM. Now if you try to access your API via a browser, you should get redirected to an OpenAM login page.

Add Policy for /static

1. Repeat the steps above in the Configure Policies section, except configure it for https://<datavm>:443/static
2. Restart the apache2 process on the Data VM to ensure the agent receives the new policy and application for the static directory.