**Integrating WSO2 Identity Server with Pentaho CE version using SAML2**

**System Environment**: Ubuntu 16.04 OS

Setup Apache Maven for generating a .kar file for Pentaho Community Edition

**Apache Maven Setup for Ubuntu**:

Follow the below list of commands and actions to setup Apache Maven

Open a terminal window on Ubuntu machine using keys **CTRL+ALT+T** keys

Run the command: **sudo apt-get upgrade -y**

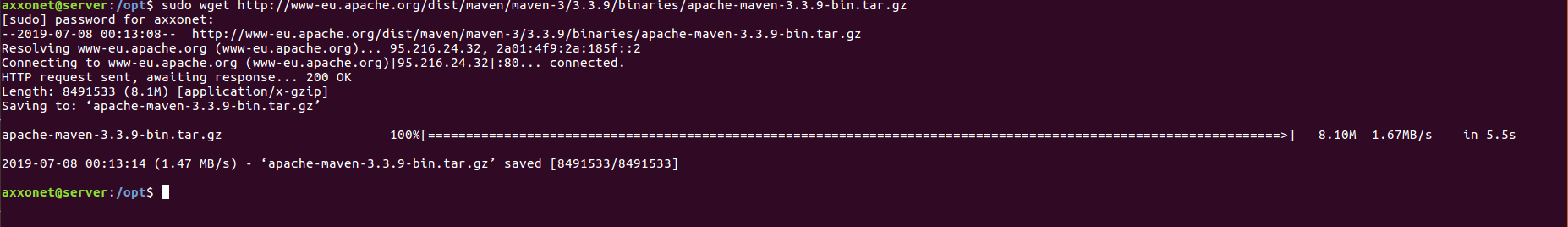
As **JAVA** setup is already complete when setting up **Pentaho 8.2.0.0-342 Community edition** version. Before setting up apache maven, make sure **JAVA** is setup in the Ubuntu machine.

Run the below commands, to install **Apache Maven**

1. **cd /opt/**
2. **sudo wget http://www-eu.apache.org/dist/maven/maven-3/3.3.9/binaries/apache-maven-3.3.9-bin.tar.gz**

**Apache Maven** file will be downloaded in the **/opt** folder

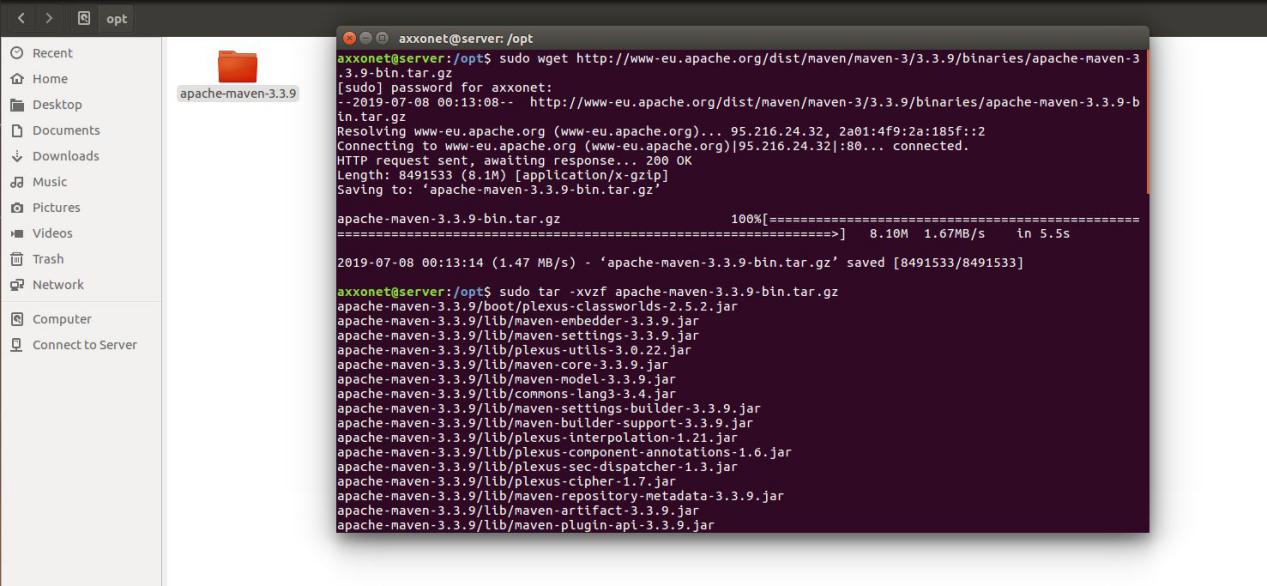
Refer the screenshot



Run the command to extract the downloaded Apache Maven archive

**sudo tar -xvzf apache-maven-3.3.9-bin.tar.gz**

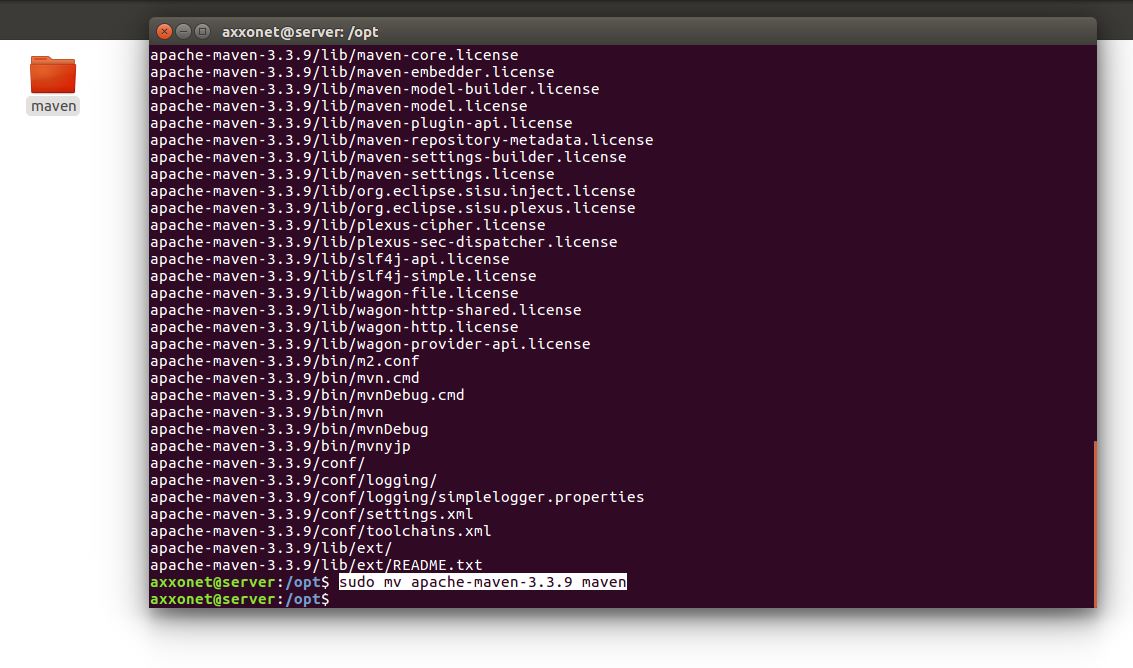
**apache-maven-3.3.9** has now been extracted and is available in **/opt** folder on Ubuntu machine. Refer screenshot



Rename a**pache-maven-3.3.9** as **maven** using the below command

**sudo mv apache-maven-3.3.9 maven**

Refer screenshot folder has been renamed as **maven**

****

Now setup Apache Maven related **environment variables** such as **M2\_HOME**,**M2**,,**MAVEN\_OPTS** and **PATH**. This can be done by creating a **maven.sh** file inside of the **/etc/profile.d/** directory. To do these actions run the below set of commands

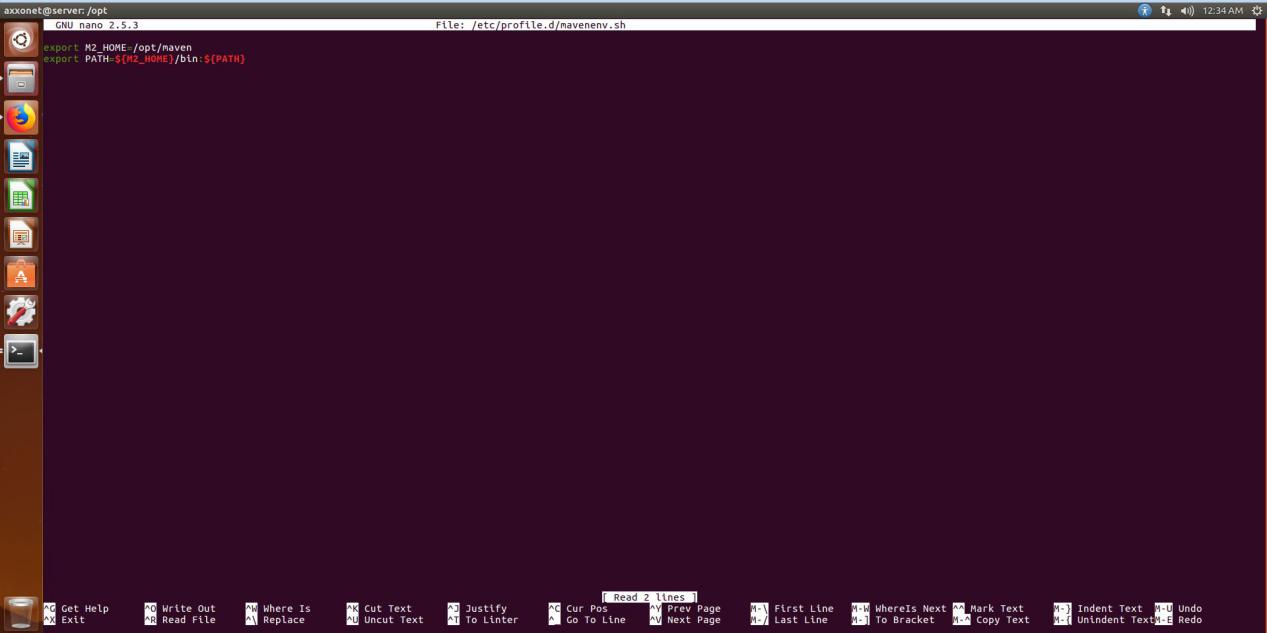
**sudo nano /etc/profile.d/mavenenv.sh**

Copy and paste the below mentioned lines

**export M2\_HOME=/opt/maven**

**export PATH=${M2\_HOME}/bin:${PATH}**

Once pasted, do **CTRL+X** to save enter **Y** and select **Enter** to exit. Refer screenshot



Update the permissions of the environment variables by using the below command

**sudo chmod +x /etc/profile.d/mavenenv.sh**

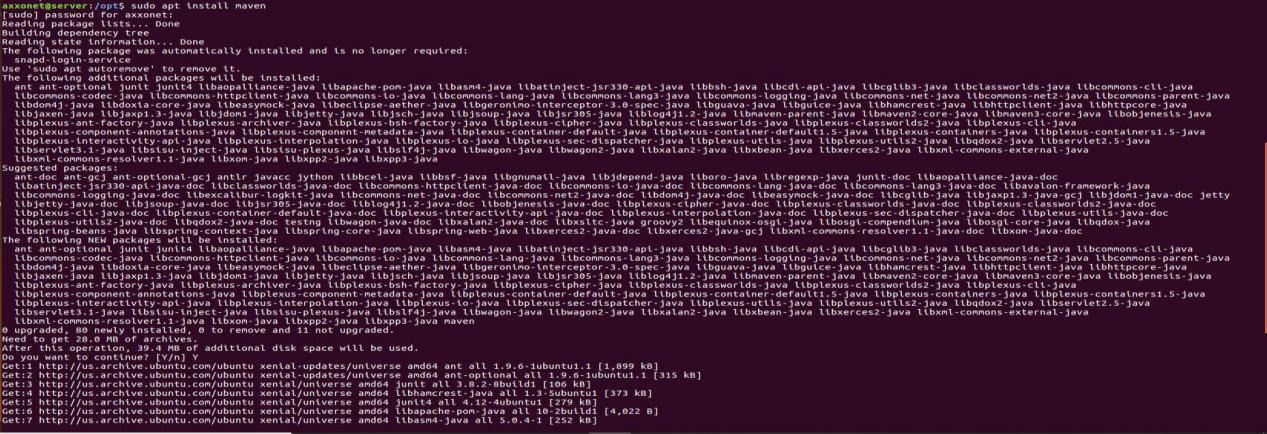
Now load the Environment variables using the following command

**sudo source /etc/profile.d/mavenenv.sh**

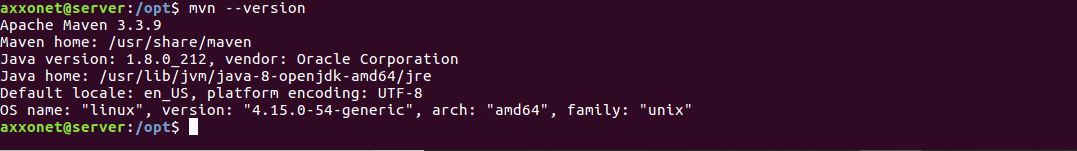
If **sudo** doesn’t work, then remove sudo from command and type the command from source **source /etc/profile.d/mavenenv.sh**

Once restart the Ubuntu machine and open a terminal window and run the command **sudo apt install maven** and install the apache maven and run the command

**mvn -version** after installing apache maven.

****

After installation process completes, on the terminal window type in the command **mvn --version**  and select Enter. The command should show the version of **apache maven** setup in the Ubuntu machine. Refer the screenshot



This Concludes the **Apache Maven** setup on the Ubuntu machine

-------------------------------------------------------------------------------------------------------

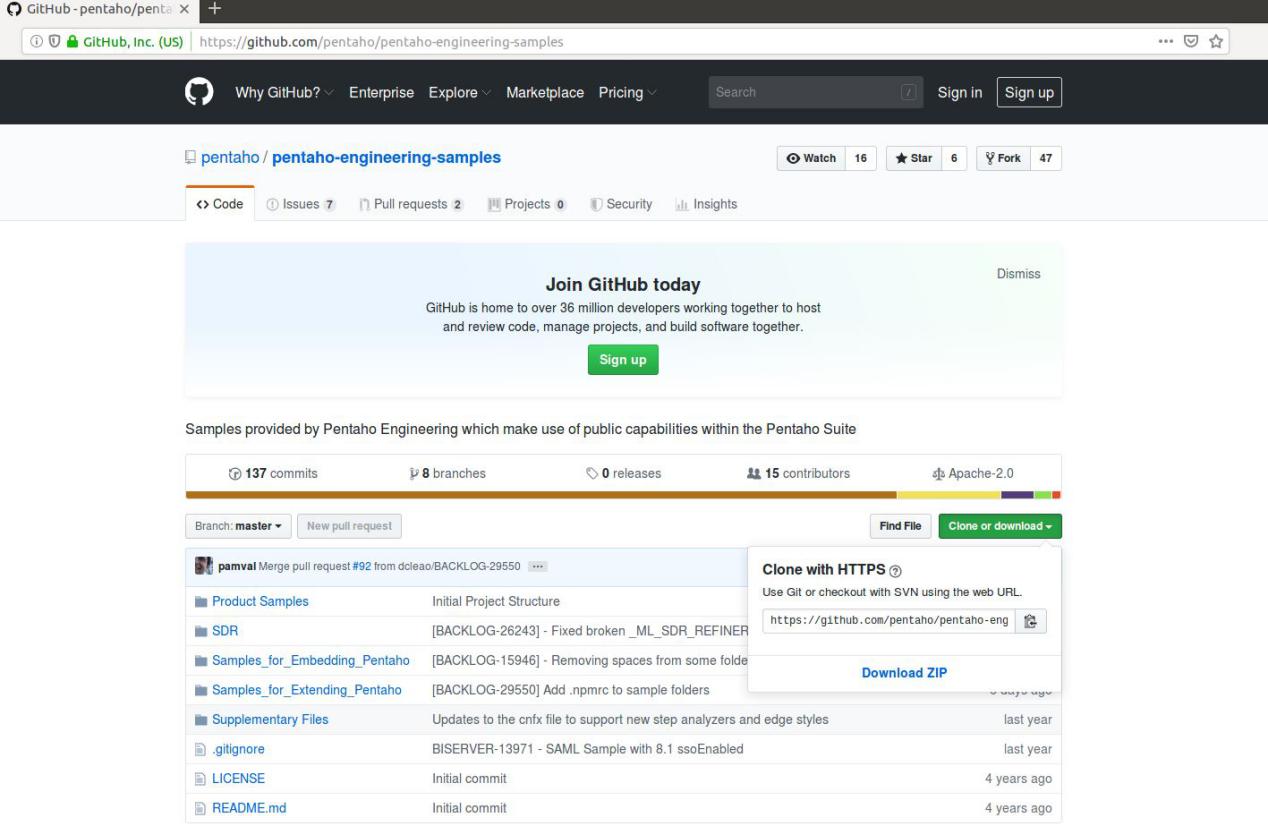
**Creating SAML2 Plugin for Pentaho:**

Open the **github** link mentioned below on a browser of your choice

<https://github.com/pentaho/pentaho-engineering-samples>

Download the zip folder and place it in a folder of your choice. Here in this documentation it is placed in **Downloads** folder

Refer screenshot



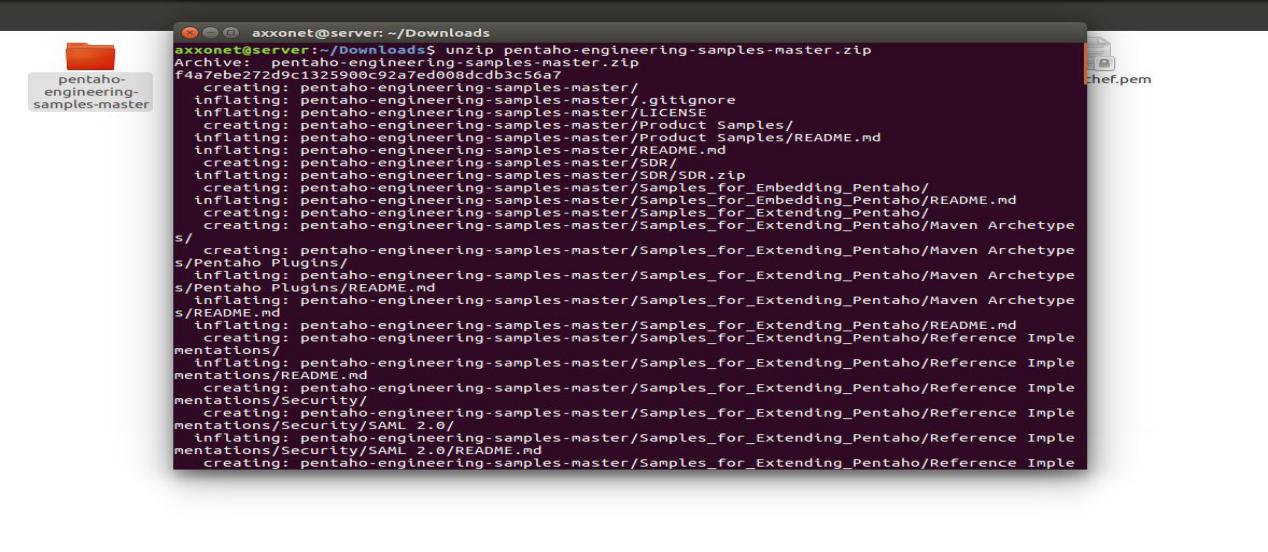
The zip file is placed in downloads folder, refer screenshot



Now extract the contents of the zipped folder using the command

**unzip pentaho-engineering-samples-master.zip**

A folder with the name **pentaho-engineering-samples-master.zip** should be created. Refer screenshot



Now by opening a terminal window run the following command

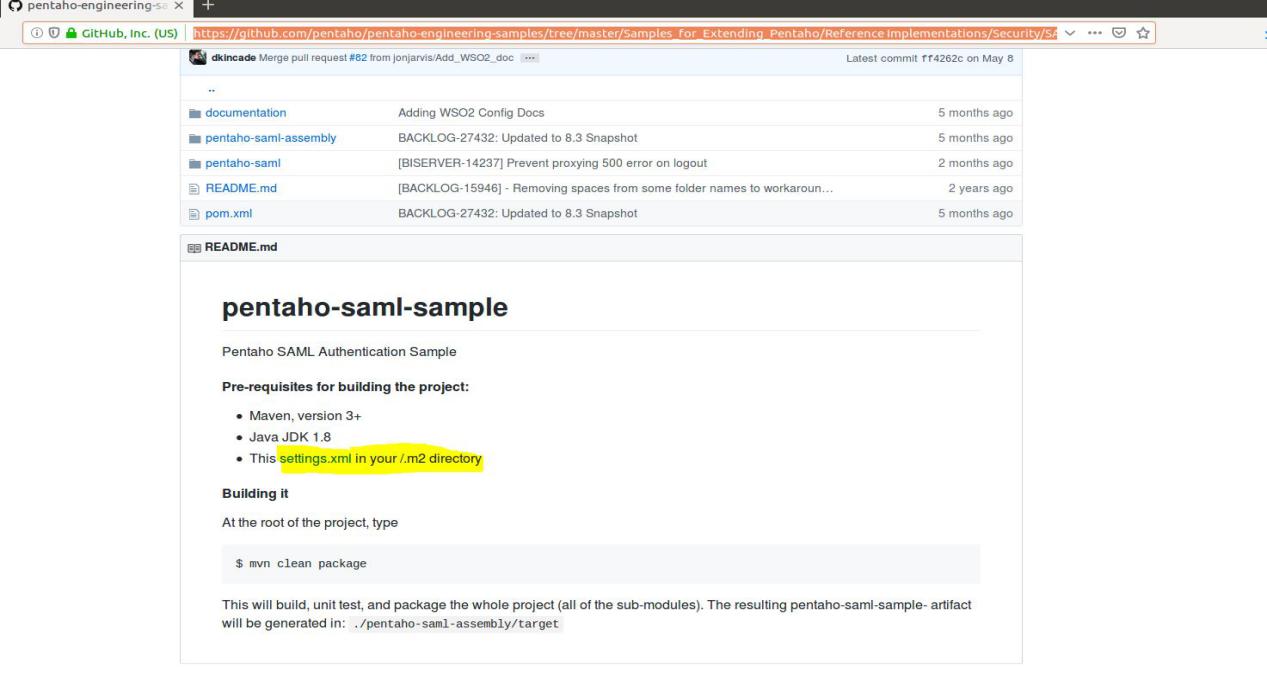
**cd /home/axxonet/Downloads/pentaho-engineering-samples-master/Samples\_for\_Extending\_Pentaho/Reference\ Implementations/Security/SAML\ 2.0**

Refer screenshot



Now before creating SAML plugin for Pentaho, go to the below link and download the settings.xml file. Refer screenshot

<https://github.com/pentaho/pentaho-engineering-samples/tree/master/Samples_for_Extending_Pentaho/Reference%20Implementations/Security/SAML%202.0>



The Settings.xml file will be available in Downloads directory, copy the file to /etc/maven folder by using the below command

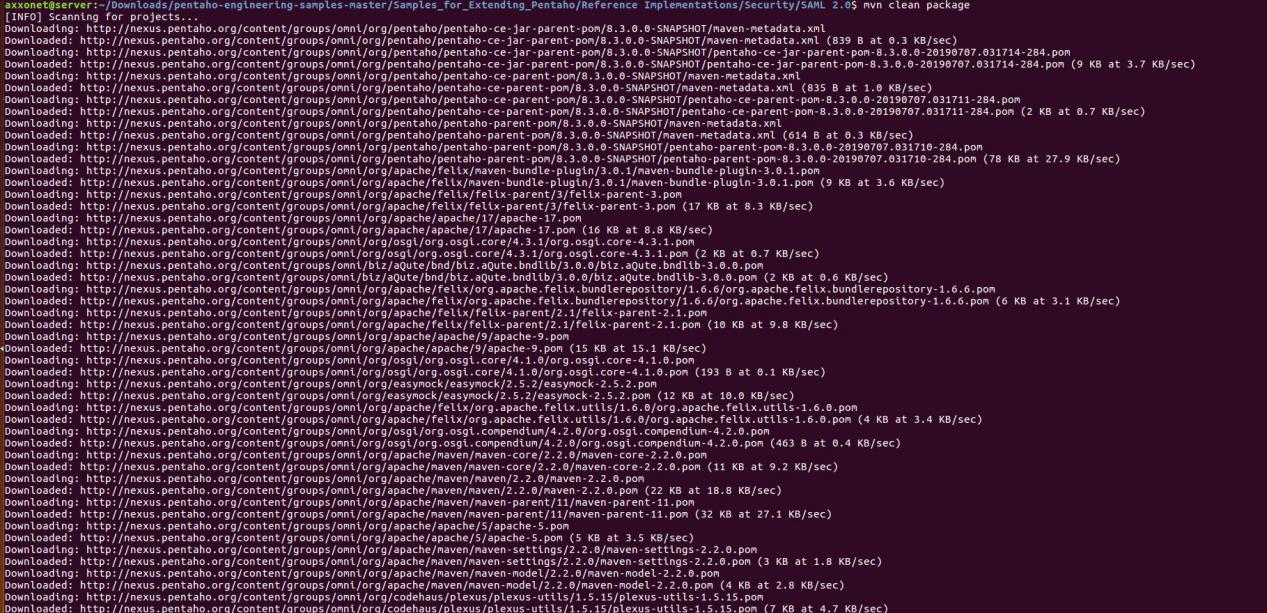
**sudo cp /home/axxonet/Downloads/settings.xml /etc/maven**

Now go to the path using the command

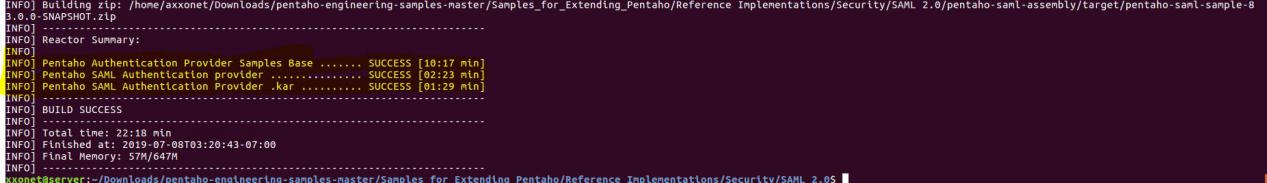
**cd /home/axxonet/Downloads/pentaho-engineering-samples-master/Samples\_for\_Extending\_Pentaho/Reference\ Implementations/Security/SAML\ 2.0**

After going to the path run the command **sudo mvn clean package -X.**

This command creates the SAML plugin for Pentaho 8.2 community version. Refer screenshot



If the package executes successfully, the message as shown in screenshot will come on the terminal window. Refer screenshot



The SAML package that has been created will be available in **/SAML 2.0/pentaho-saml-assembly/target** folder

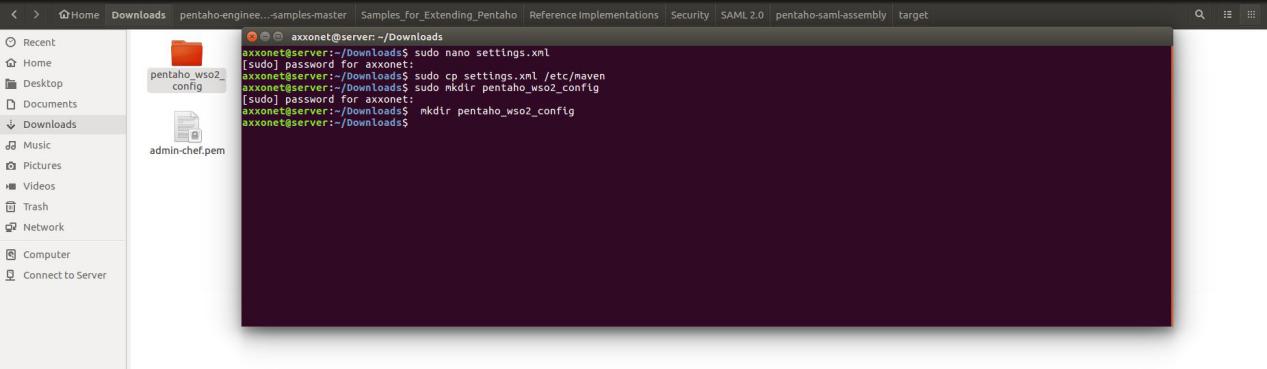
The SAML plugin package for pentaho community version has been created

-------------------------------------------------------------------------------------------------------

**SAML files to pentaho\_wso2\_config folder**

Now create a folder by name **pentaho\_wso2\_config** in Downloads or any folder of your choice on Ubuntu machine. Refer the below command

**mkdir pentaho\_wso2\_config,** a folder by the mentioned name will be created in Downloads folder. Refer screenshot



Next few steps refer to extracting and copying some files from **SAML 2.0** sub folders to **pentaho\_wso2\_config** folder

Follow the below list of commands

Go to the **SAML 2.0/pentaho-saml-assembly/target** folder and unzip the file **pentaho-saml-sample-8.3.0.0-SNAPSHOT.zip** using the following command

**unzip pentaho-saml-sample-8.3.0.0-SNAPSHOT.zip**

Folder by **pentaho-saml-sample-8.3.0.0-SNAPSHOT** will be created , now open a terminal window and copy the **pentaho-saml-sample-8.3.0.0-SNAPSHOT.kar** to folder **pentaho\_wso2\_config** using the command

**cp pentaho-saml-sample-8.3.0.0-SNAPSHOT.kar ~/Downloads/pentaho\_wso2\_config**

Similarly copy the file logout.jsp to pentaho\_wso2\_config folder using the command

**cp logout.jsp ~/Downloads/pentaho\_wso2\_config**

Now go to **/SAML 2.0/pentaho-saml/target/classes/cfg** path and copy the **pentaho-saml.cfg** file to **pentaho\_wso2\_config** use the below mentioned command

**cp pentaho-saml.cfg ~/Downloads/pentaho\_wso2\_config**

Go to **SAML 2.0/documentation/resources** folder and copy the file **pentaho-sp.xml** to **pentaho\_wso2\_config** folder. Use the below mentioned command

**cp pentaho-sp.xml ~/Downloads/pentaho\_wso2\_config/**

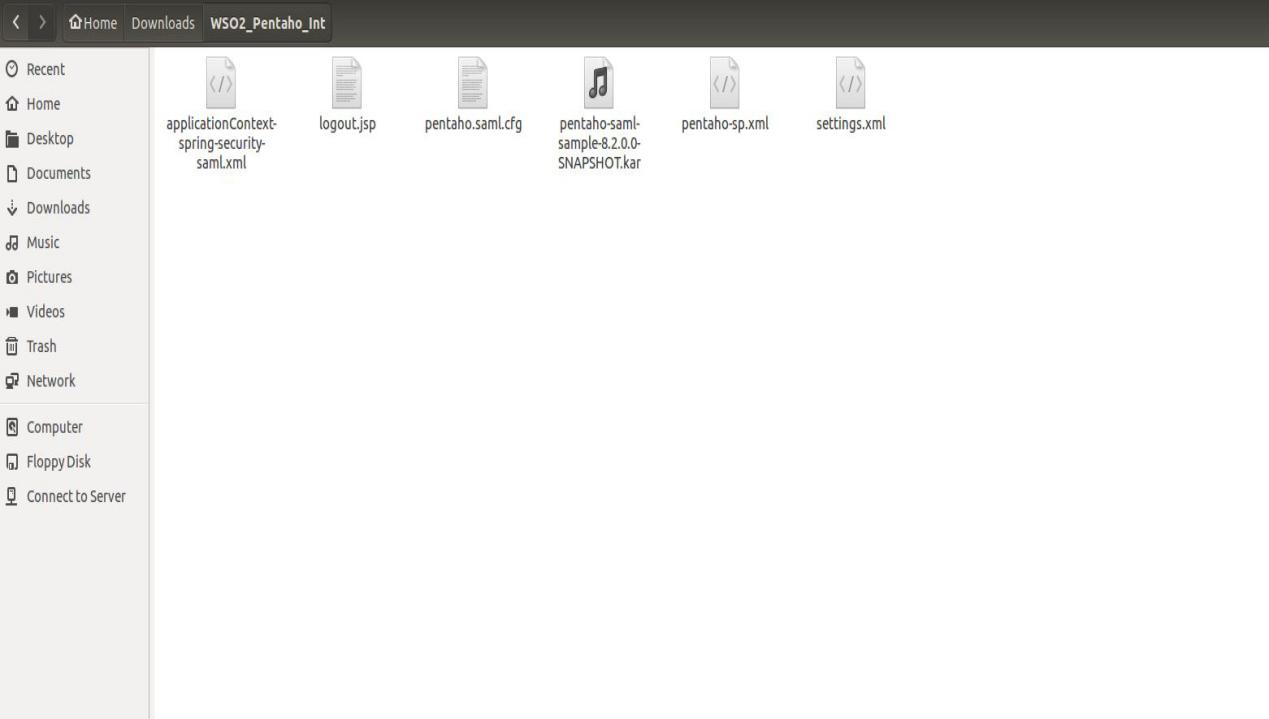
Open the below mentioned link and select the file **applicationContext-spring-security-saml-ce.xml**

<https://github.com/kleysonr/pentaho-security-samples/tree/master/wso2is-ldap/pentaho-server/pentaho-solutions/system>

Selecting the **applicationContext-spring-security-saml-ce.xml,** will open the code of the **.xml** file. Select and copy the entire content of the **.xml** file on to a empty document in your Ubuntu machine and name the document as **applicationContext-spring-security-saml.xml** and save the file in **WSO2\_Pentaho\_Int** folder.

If the above steps are followed ,the **WSO2\_Pentaho\_Int** folder should have following 5 files. Refer the screenshot and the list below

1. **applicationContext-spring-security-saml.xml**
2. **logout.jsp**
3. **pentaho-saml.cfg**
4. **pentaho-sp.xml**
5. **pentaho-saml-sample-8.2.0.0-SNAPSHOT.kar**

****

**Copy the below list of files to Pentaho Community Version folder:**

Copy the file **logout.jsp** to “**\pentaho-server\tomcat\webapps\pentaho**” folder

Copy the file **pentaho-saml-sample-8.2.0.0-SNAPSHOT.kar** to “**\pentaho-server\pentaho-solutions\system\karaf\deploy**” folder

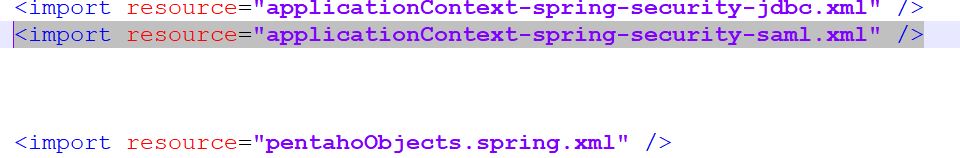
Copy the file **pentaho.saml.cfg** to “**\pentaho-server\pentaho-solutions\system\karaf\etc**” folder

Copy the **applicationContext-spring-security-saml.xml** file to “**\pentaho-server\pentaho-solutions\system”** folder

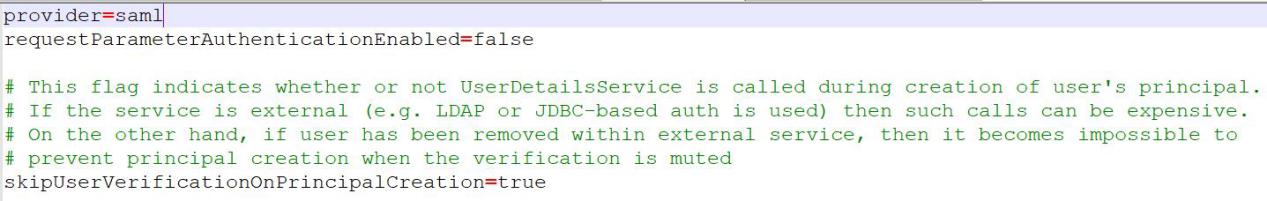
Now edit the **pentaho-spring-beans.xml** file available in **\pentaho-server\pentaho-solutions\system** folder; with a text editor and write the following line

**<import resource="applicationContext-spring-security-saml.xml" />**

Refer screenshot below



Edit the “**security.properties**” file available in the **\pentaho-server\pentaho-solutions\system** folder using a text editor and change the value of provider value to **saml** from **jackrabbit** and save it. Refer screenshot below



**Checks before starting Pentaho Community Edition BA Server:**

Files that we have placed in Pentaho Community Edition BA Server and the files that have been edited are as follows:

**applicationContext-spring-security-saml.xml**

**pentaho.saml.cfg**

**pentaho-saml-sample-8.2.0.0-SNAPSHOT.kar**

**logout.jsp**

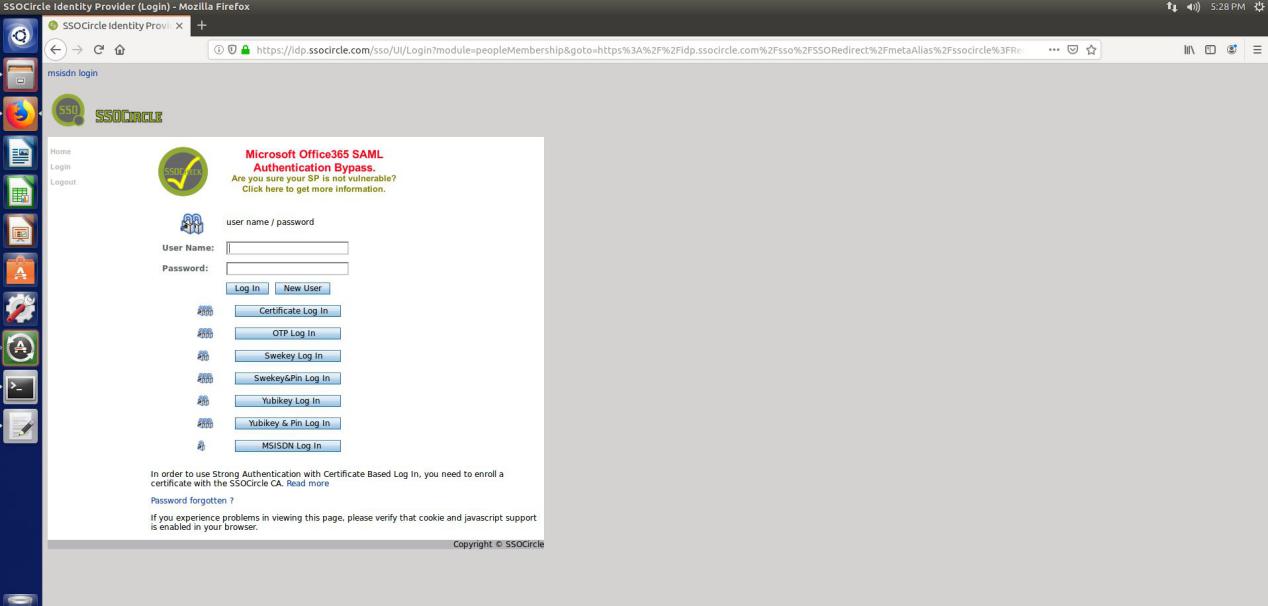
**Edited files:**

**pentaho-spring-beans.xml**

**Security.properties**

Now go to **~/Downloads/pentaho-server/** folder, open a terminal window and run the command **./start-pentaho.sh**

Once the server starts successfully and you type <http://localhost:8080> on a Browser of your choice , the URL should lead you **Login Page of SSO Circle.** Refer screenshot



We will not be able to login to Pentaho Home page with the default pentaho user credentials.

If this is achieved , the **SAML2 plugin** for Pentaho Community Edition is working.

Stop the **Pentaho BA Server**.

SAML plugin has been activated

**Configuration of Pentaho with WSO2 Identity Server**

Open a browser of your choice and enter the following URL “<https://localhost:9443/carbon/admin/login.jsp>”

Enter the default user credentials mentioned below

**Username**: admin, **Password**: admin

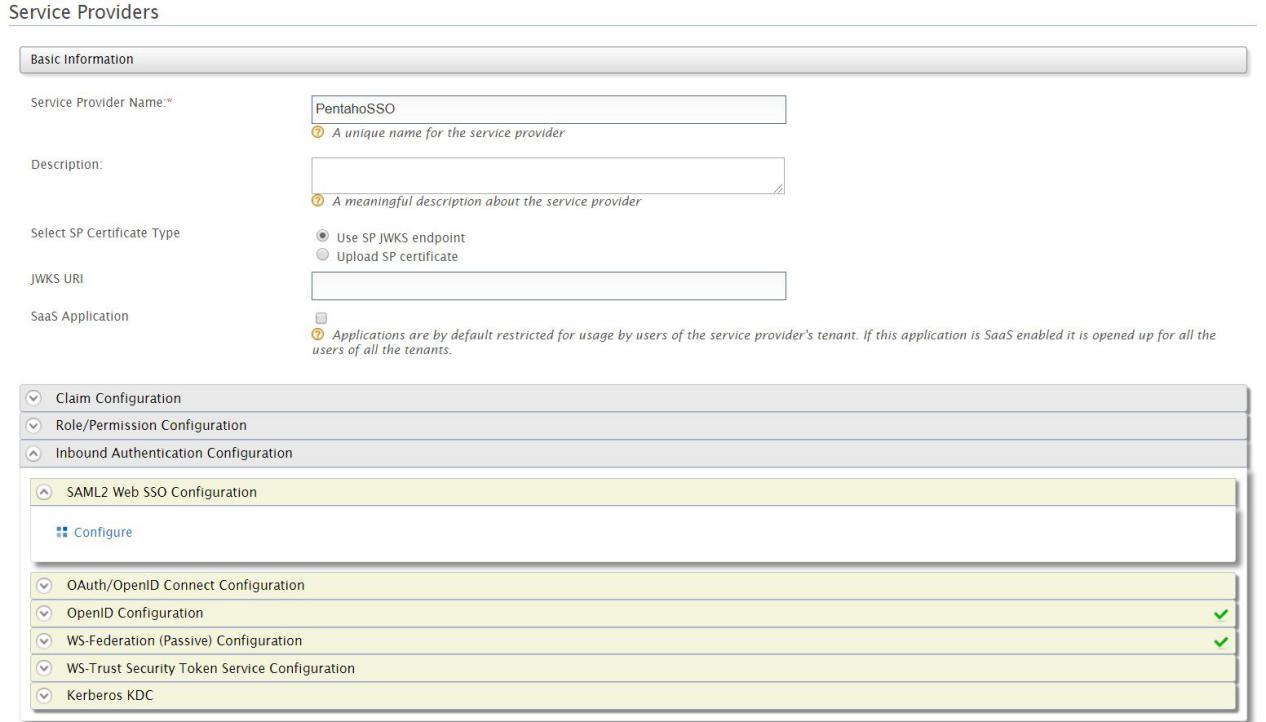
After logging into WSO2 Carbon Server; On the left side under **Service Providers**,Select the “**Add**”button. It will take you to the following page. Refer the screenshot below



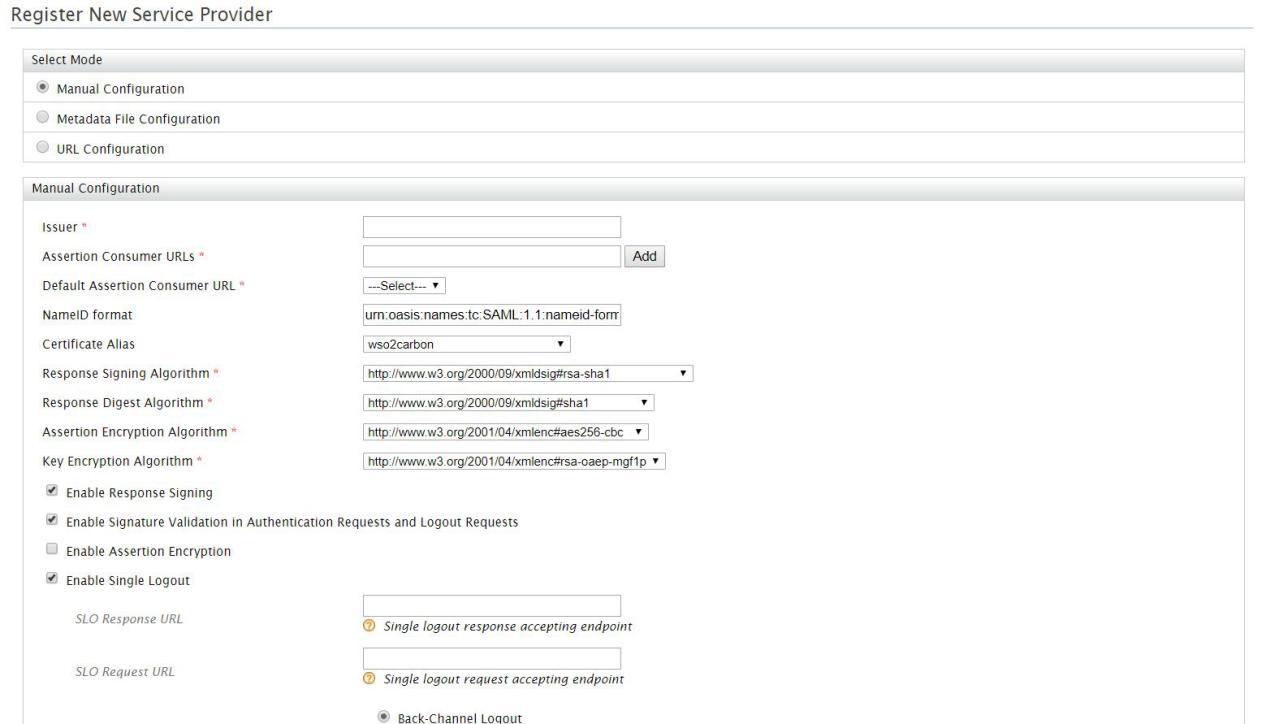
Select “M**anual configuration**” radio button, then under **Service Provider Name** enter a name of your choice and description if required and select the “**Register**” option.

**Note**: For documentation purpose service provider name is given as **PentahoSSO**

Now Expand the **Inbound Authentication Configuration** and select the **Configure** option by expanding **SAML2 Web SSO Configuration**. Refer Screenshot below



After you select the Configure option, it should take you to the following page,Refer screenshot below



Select the **Metadata File Configuration** radio button, it will ask you to **Choose File**, Refer screenshot below

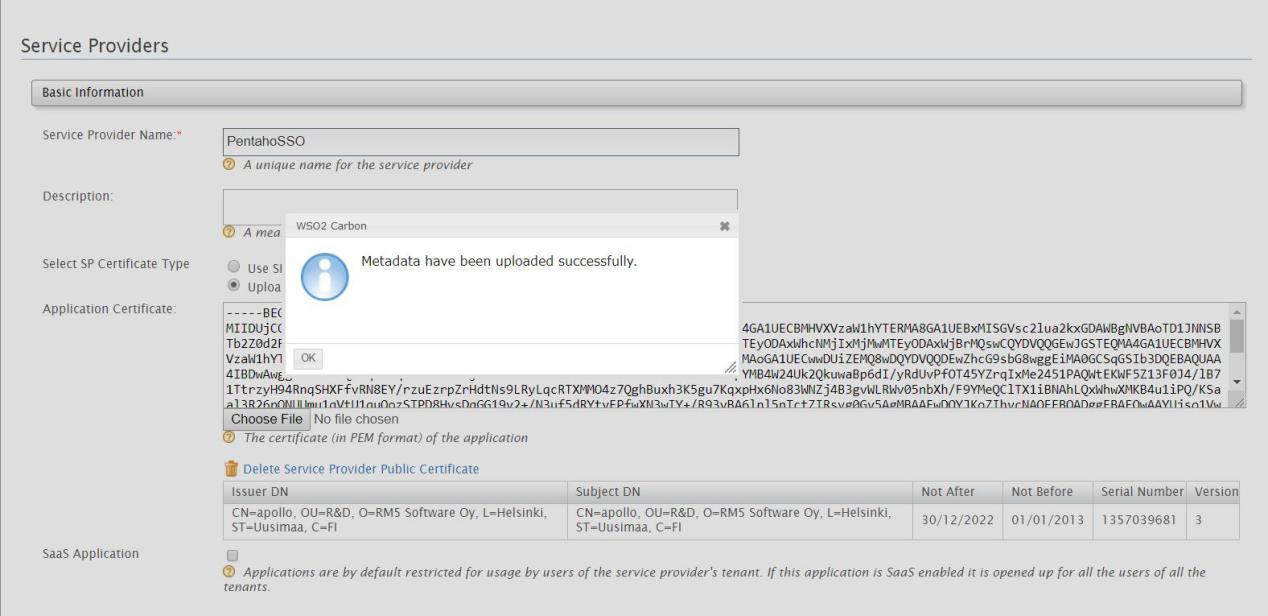


In Choose File, go to the path **WSO2\_Pentaho\_Int** which has been created in earlier steps and select the **pentaho-sp.xml** file and then select the **Upload** button.

**Note:** Before uploading the file, the **pentaho-sp.xml** file will be having “**http://localhost:8080**”,always use the **port number** and **hostname** or **ip number** which has been defined in **server.xml** file located in “**pentaho-server\tomcat\conf**” and do the respective changes to the **pentaho-sp.xml** file using a text editor.

And also **comment** the entire “**<md:KeyDescriptor use="encryption">**” section in the **pentaho-sp.xml** file.

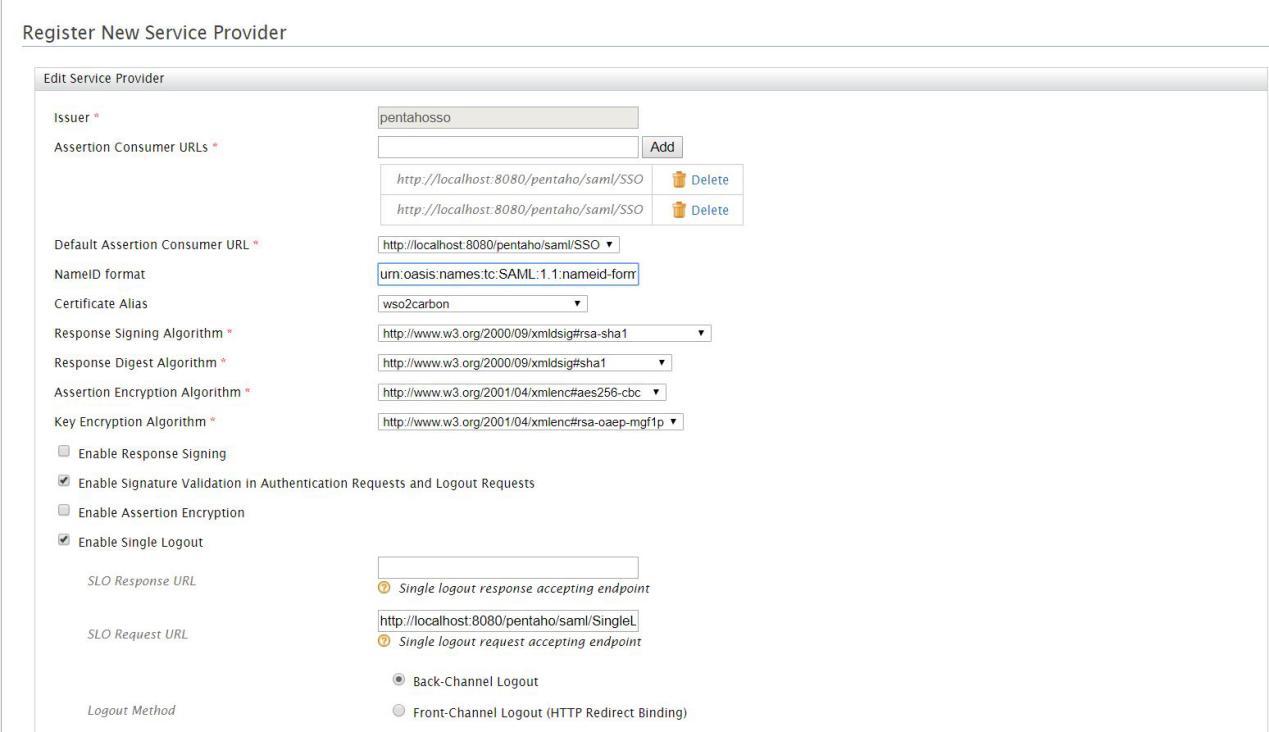
If the **pentaho-sp.xml** file has been successfully uploaded,refer the screenshot message



Select “**OK**”, On Observing the **Application Certificate** should be available.

Now select the **edit** option in **SAML2 Web SSO Configuration**

After selecting the edit option, all the details will be filled in the page. Refer the screenshot below

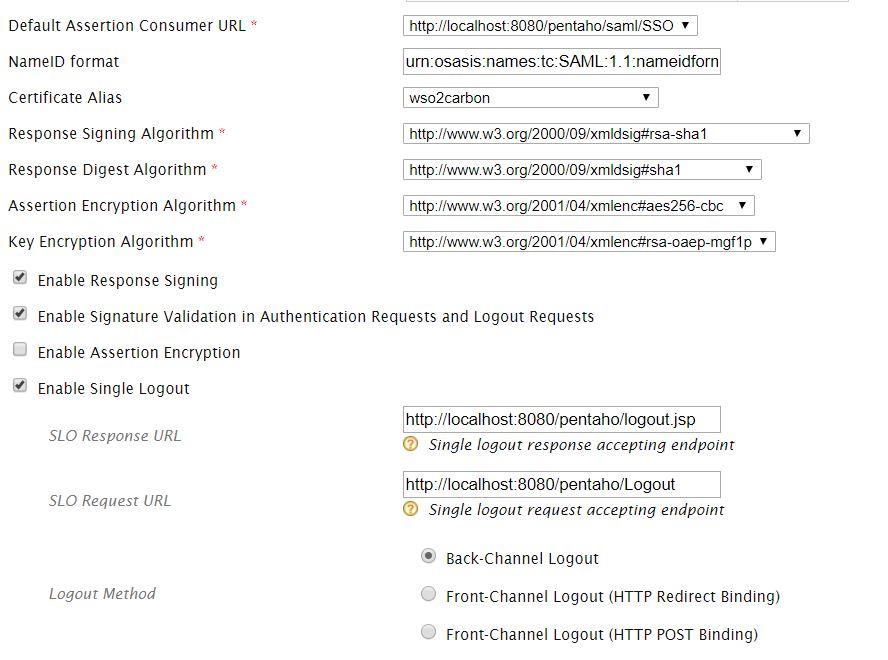


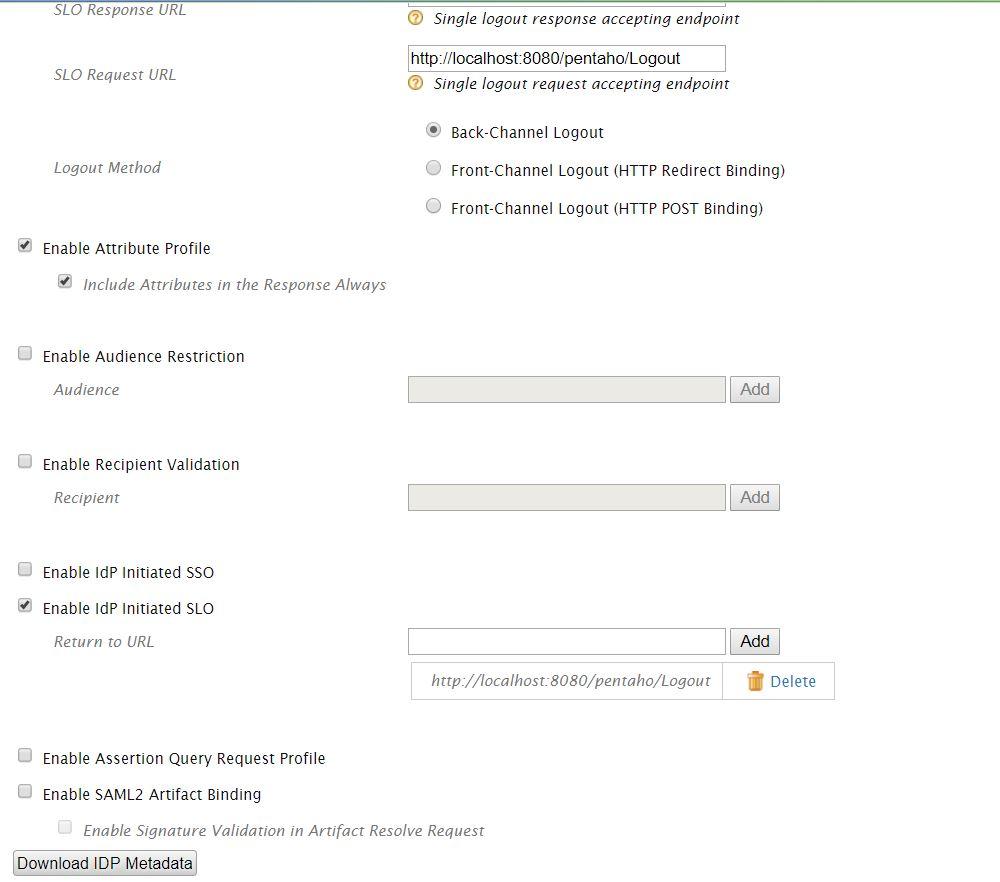
Change the **NameID format** to “**urn:osasis:names:tc:SAML:1.1:nameidformat-unspecified**”

Change the SLO Response URL to “**http://localhost:8080/pentaho/logout.jsp**”

Change the SLO Request URL to “**http://localhost:8080/pentaho/Logout**”

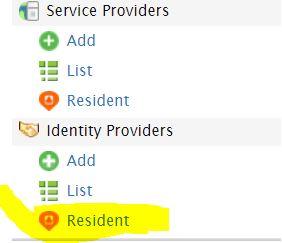
Do the following checks based on the below screenshots



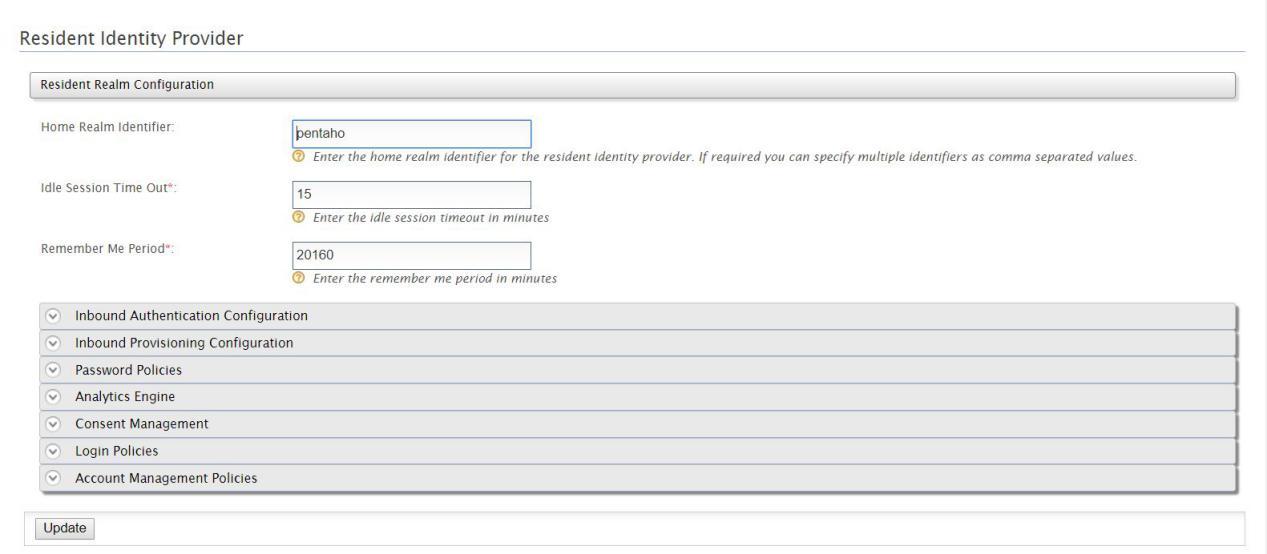


After doing all the Checks, select the “**Update**”option available at the bottom of the page.

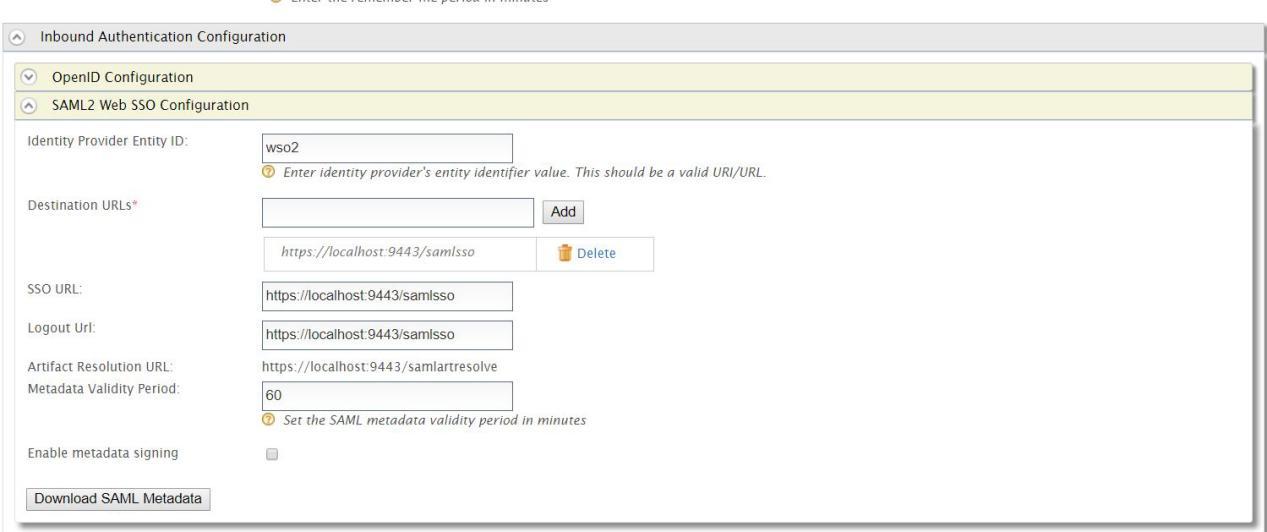
Now select the “**Resident**”option under **Identity Providers** which is available on the left side of the page. Refer the screenshot



The page will now look as follows

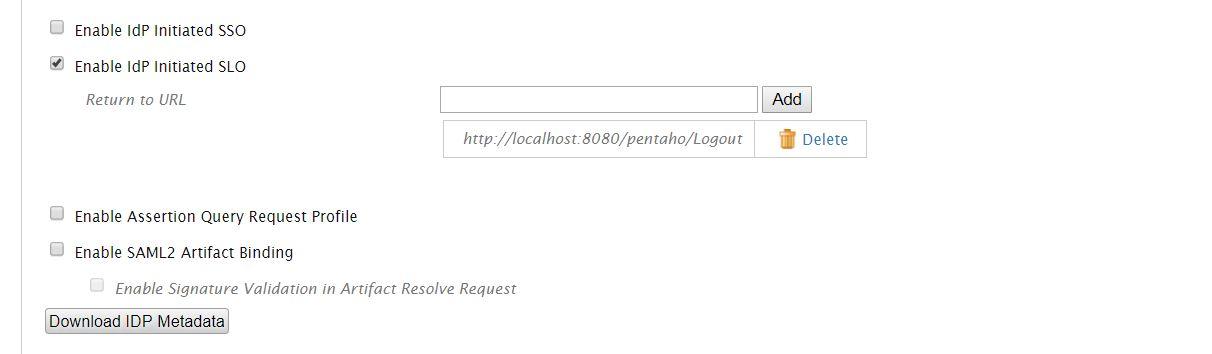


Now edit the **SAML2 WEB SSO Configuration** by expanding the **Inbound Authentication Configuration** and change the Identity Provider Entity ID: value to “**wso2**”. Refer screenshot



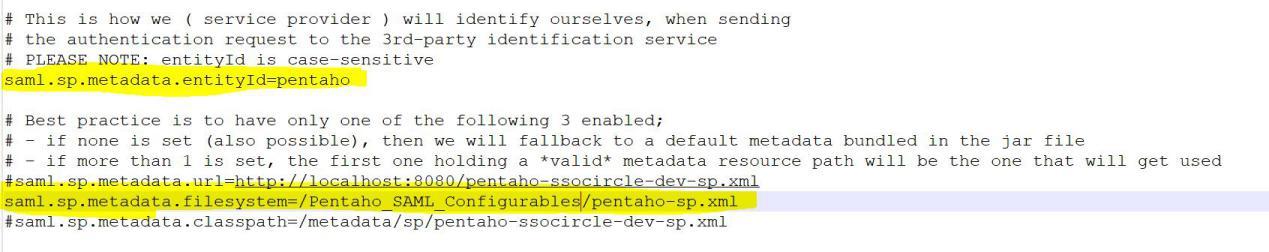
And then Select the **Update** option available at bottom.

After updating, go to “**List**” option in Service Providers and Edit the **Pentaho SSO (**which we have created earlier**)**and edit the **SAML2 Web SSO Configuration** by expanding the **Inbound Authentication Configuration.** Select the **Download IDP Metadata** option and save the **metadata.xml** file in **WSO2\_Pentaho\_Int** folder. Refer the below screenshot



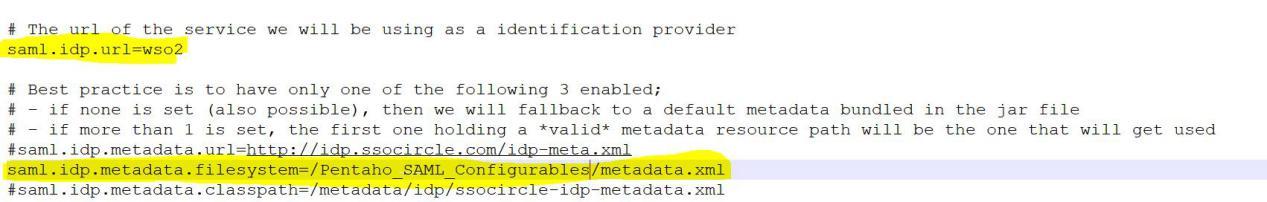
Now edit the **pentaho.saml.cfg** file using a text editor, locate the “**saml.sp.metadata.entityId**” and give its value as “**pentaho**”

In the same file enable “**saml.sp.metadata.filesystem**”by removing **#** and give its value as /**WSO2\_Pentaho\_Int/pentaho-sp.xml** and disable the line below by adding **#** . Refer screenshot below



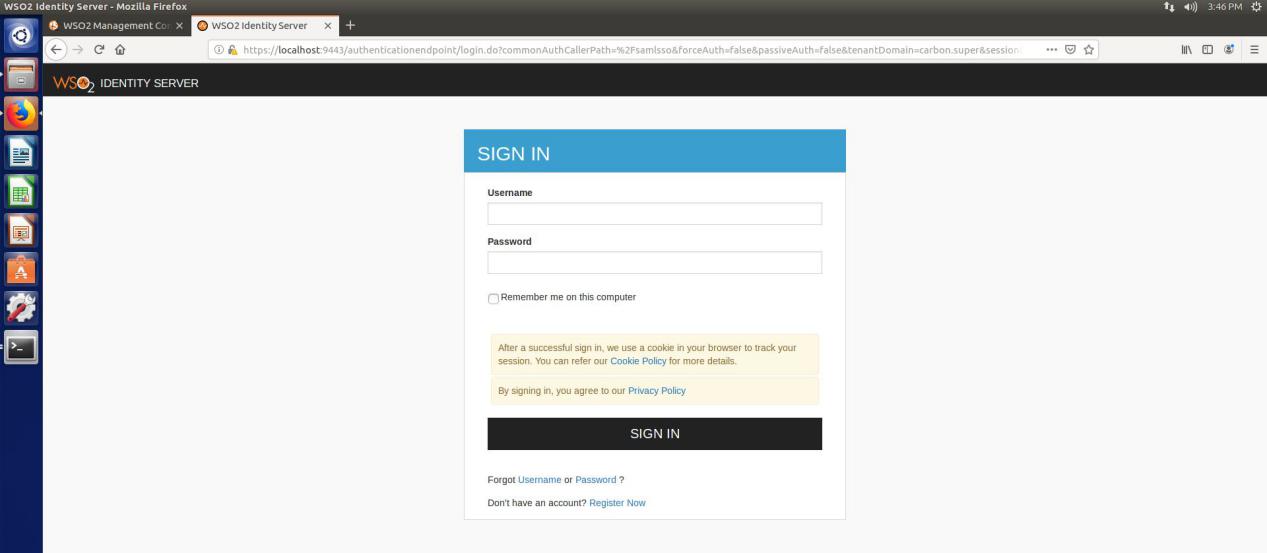
In the same file locate **“saml.idp.url**” and give its value as “**wso2**”

In the same file enable saml.idp.metadata.filesystem by removing # and give its value as /**WSO2\_Pentaho\_Int/metadata.xml** and disable the below line by adding #. Refer screenshot below



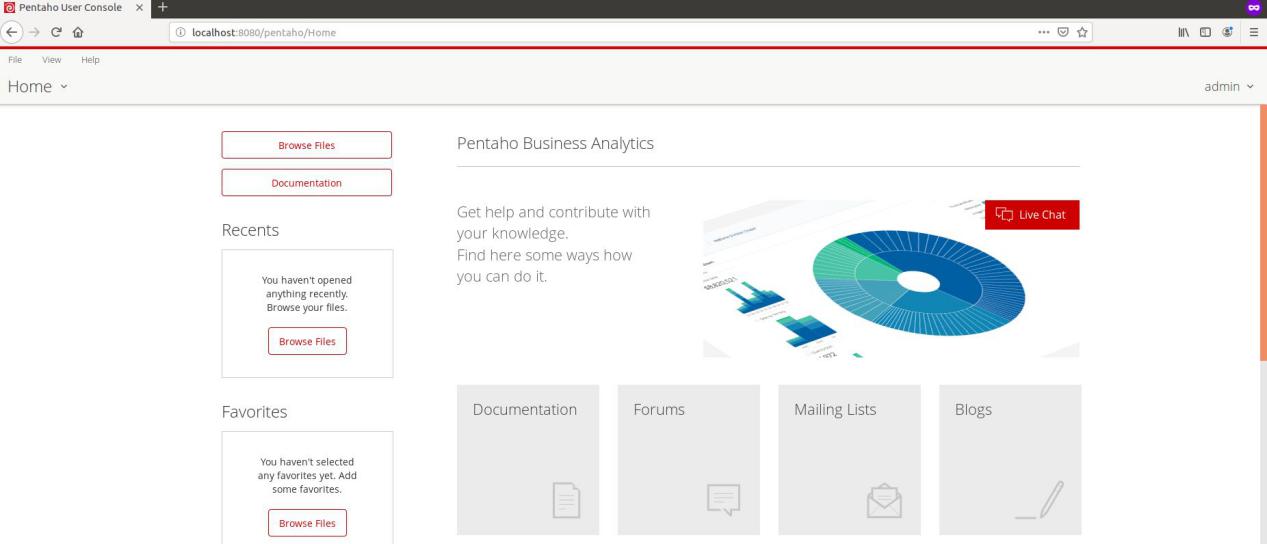
Save the file.

Now Start the **Pentaho BA server**, and enter “**http://localhost:8080/**” on a browser of your choice, if everything is configured with reference to WSO2, the Pentaho URL should redirect the page to the following URL and refer the screenshot



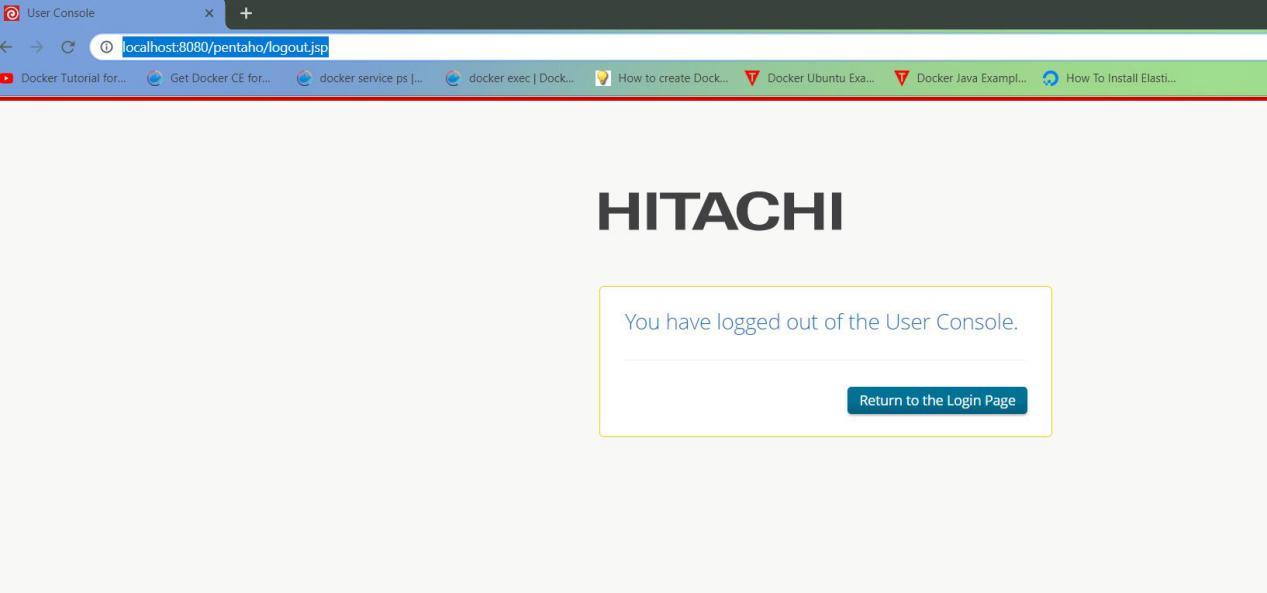
Give the Username and Password as “**admin**”,its the default credentials when you are using WSO2 Carbon Server. Once the credentials are authenticated and authorized , the page will be redirecting to “**http://localhost:8080/pentaho/Home**”.

Refer the screenshot



**Note:** As WSO2 Identity Server is now the authentication provider, the user logging in by default will only get “**Read**” Privileges. The **User Creation**, **Roles Creation**,**Role mapping** ,**Permissions** or **Privileges** will be explained clearly in later part of documentation.

When the user wants to Logout of Pentaho, after Logging out the URL will be redirected to “**http://localhost:8080/pentaho/logout.jsp**” page. Refer screenshot below



**User Creation, Role Mapping and Permissions in WSO2**

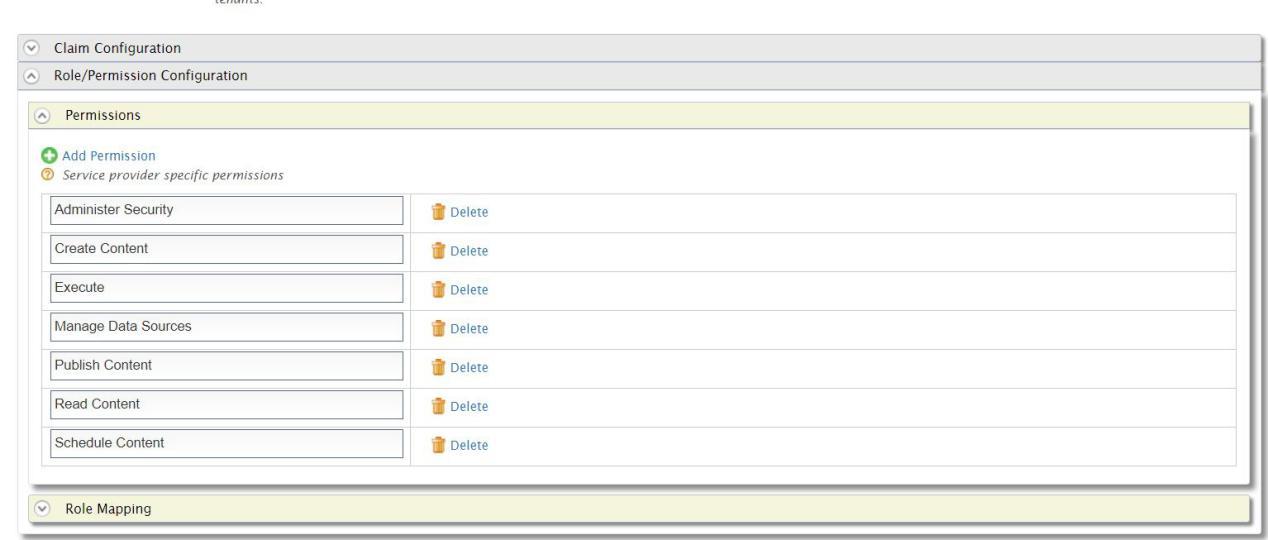
**Permissions:** By default Pentaho will be having the 7 following privileges or Permissions to end users

1. **Administer Security**
2. **Create Content**
3. **Execute**
4. **Manage Data Sources**
5. **Publish Content**
6. **Read Content**
7. **Schedule Content**

The above mentioned Permissions or Privileges should be defined. In WSO2 select **“List”**  option in Service Provider and edit the Entity Id “**PentahoSSO**”

Expand the **Roles/Permission Configuration** and Select the **+Add Permission** option and add the above mentioned 7 permissions and then select the **Update** option.

 Once it updates, the service provider will be having the mentioned permissions. Refer screenshot



The permissions we have created for Service Provider Entity ID **PentahoSSO** can be viewed in **User and Roles** section available in top left corner of the Carbon Server page. Select the **“List”** option in Users and Roles, select **Roles**, it will provide the list of roles available , there select “**Permissions**” option for **Application/PentahoSSO** and scroll down to bottom and check all the boxes Refer the screenshot.



**Role Mapping:**

 By default Pentaho has 4 Roles, their default permissions in Pentaho are defined as follows:

**Super User or Administrator** role has all the **7** permissions.

**Business Analyst** role has only **Publish Content** Permission.

**Power User** role has **Read Content,Create Content,Publish Content,Execute, Schedule Content** permissions.

**Report Author** role has **Schedule Content** and **Manage Data Sources** permissions.

Now create or add 4 roles with the above mentioned names in WSO2 Identity Server Users and Roles section.

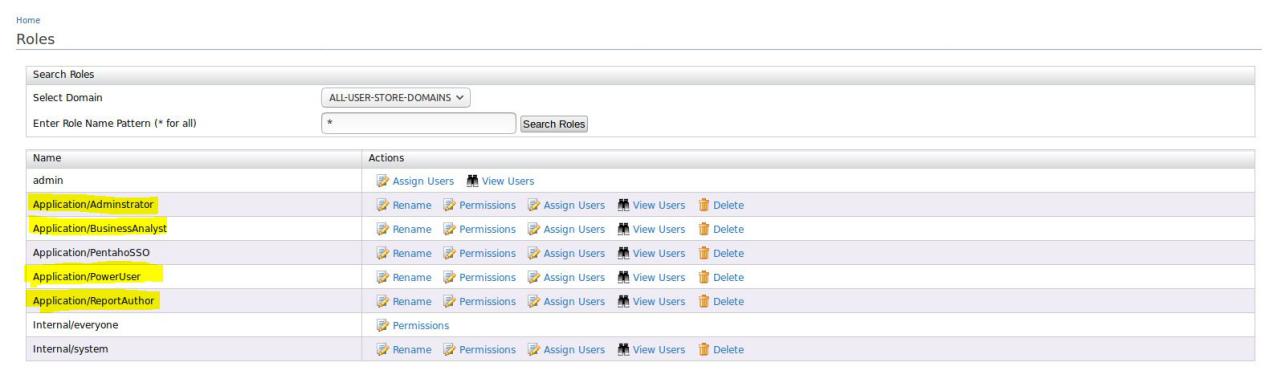
Select the **+Add** option, then Select **Add New** **Role** option, the select the **Application** option from **Domain** drop down, enter the name “**BusinessAnalyst**” and select **next** button. Refer screenshot below

**Note:** **WSO2 doesn’t allow Blank Spaces while entering role names.**

****

After selecting next button, WSO2 will take you to Permissions Page, scroll down to the Application Section at the bottom and select the permission **Publish Content** and select the **finish** option.

Follow the same procedure for the remaining 3 roles **Administrator or Super User,Report Author** and **Power User** and give respective permissions mentioned above in the document. After all roles are created, the roles section when you select List option will look like this



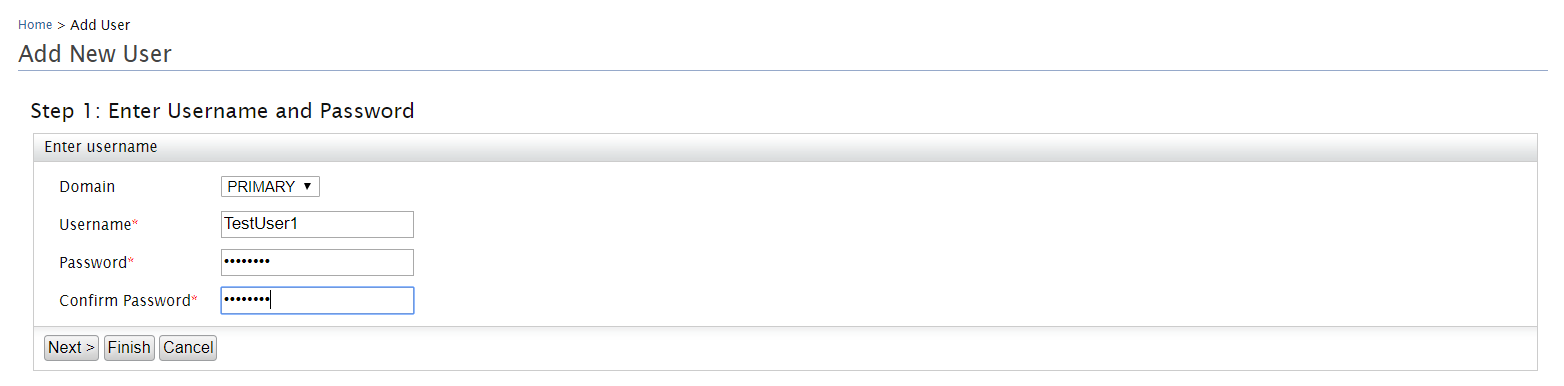
Highlighted in yellow are the roles that have been created.

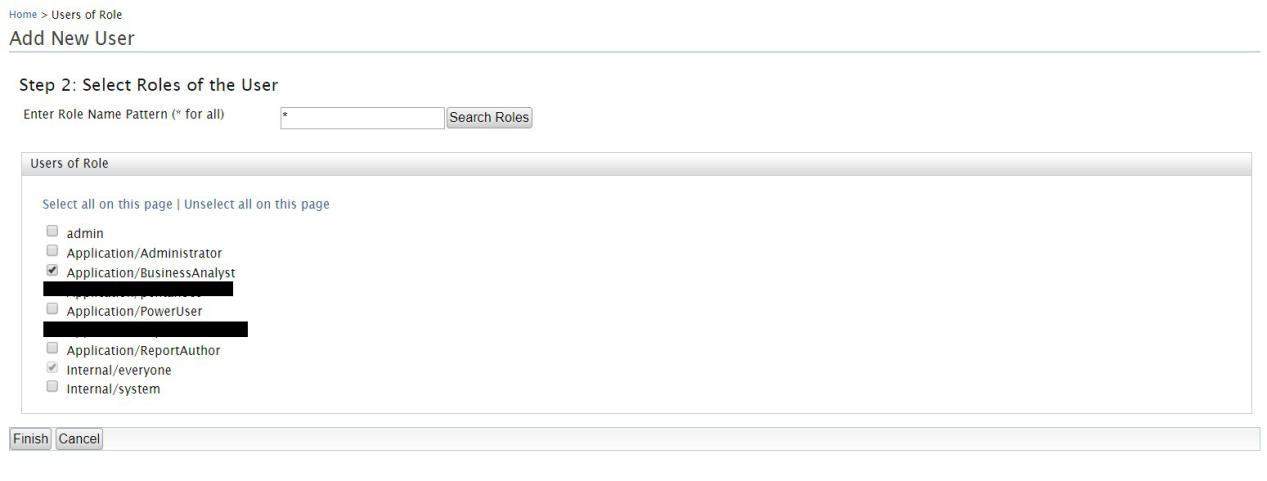
**Roles Admin,Internal/everyone,Internal/system** are default Carbon Server roles.

**Application/PentahoSSO** is created when Service provider is being created.

**Note**: When creating roles,don’t map any role to **admin** user.

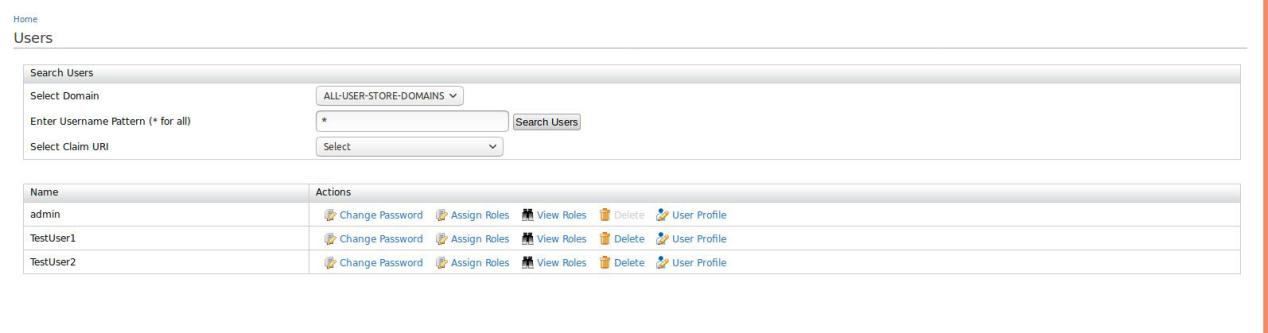
Create some test users by selecting **+Add** under **Users and Roles** section, and the select **Add New User** option and create users and map them to the roles that have been created. Refer the screenshots below





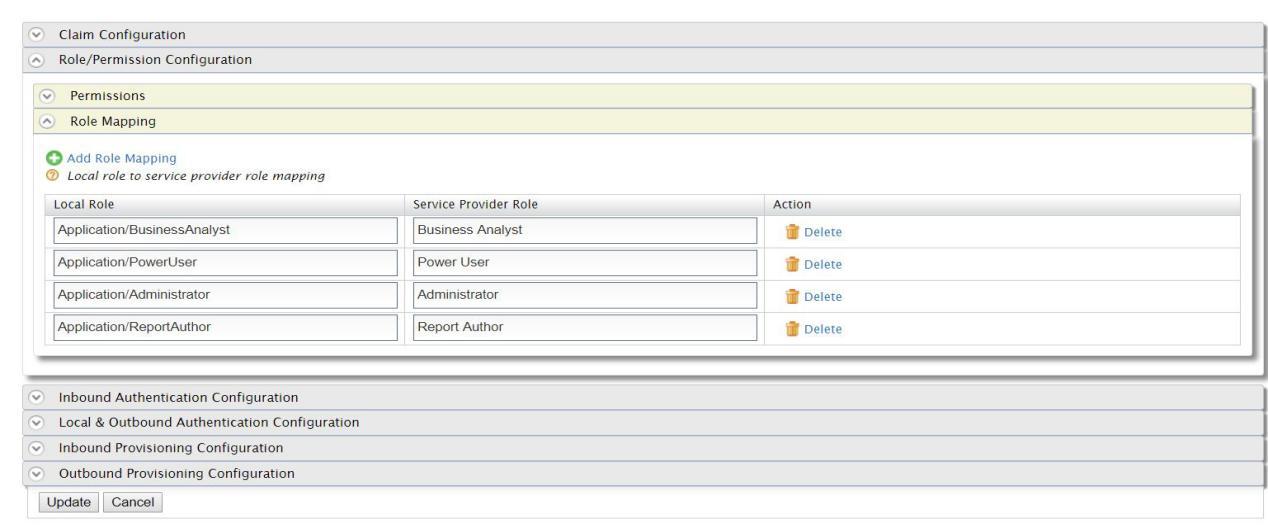
Select Finish option, similarly create another **TestUser2** and map it to **Application/Administrator** role.

Refer the users screenshot below



Users and Roles have been created and users have been mapped to roles.

Now select “List” from Service Providers and **Edit** the PentaoSSO Service Provider Entity ID, Expand Roles and Permissions Configuration. Select the + **Add Role Mapping** option and map the created roles in WSO2 with that of Pentaho. Refer the screenshot below



Select **Update** Option.

After Updating Expand the Claim Configuration. In that select the option “**Define Custom Claim Dialect**”

Select **+Add Claim URI**

Under Service Provider Claim

Enter **Pentaho Role**

Under Local Claim, Select the URL **<http://wso2.org/claims/role>**

Check the **Requested Claim** and **Mandatory Claim** boxes

The select **Update** option available at the bottom.

The below step is optional

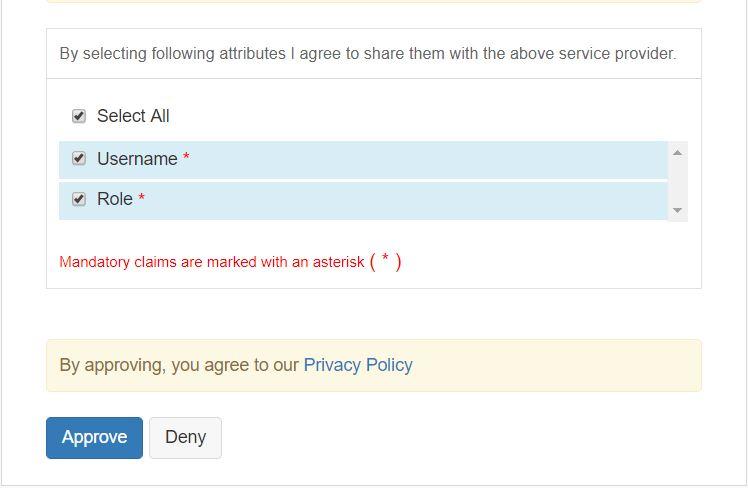
Now with a text editor edit the **pentaho-saml.cfg** file, locate and change the value of **saml.role.related.user.attribute.name** = **Pentaho Roles** from **Pentaho Role** and save the file.

**Role Mapping** process is now complete.

Before proceeding with logging into Pentaho BA server with created users, Stop and Start the Pentaho BA Server

**TestUser2** has **Admin** privileges and **TestUser1** has **Business Analyst** privileges.

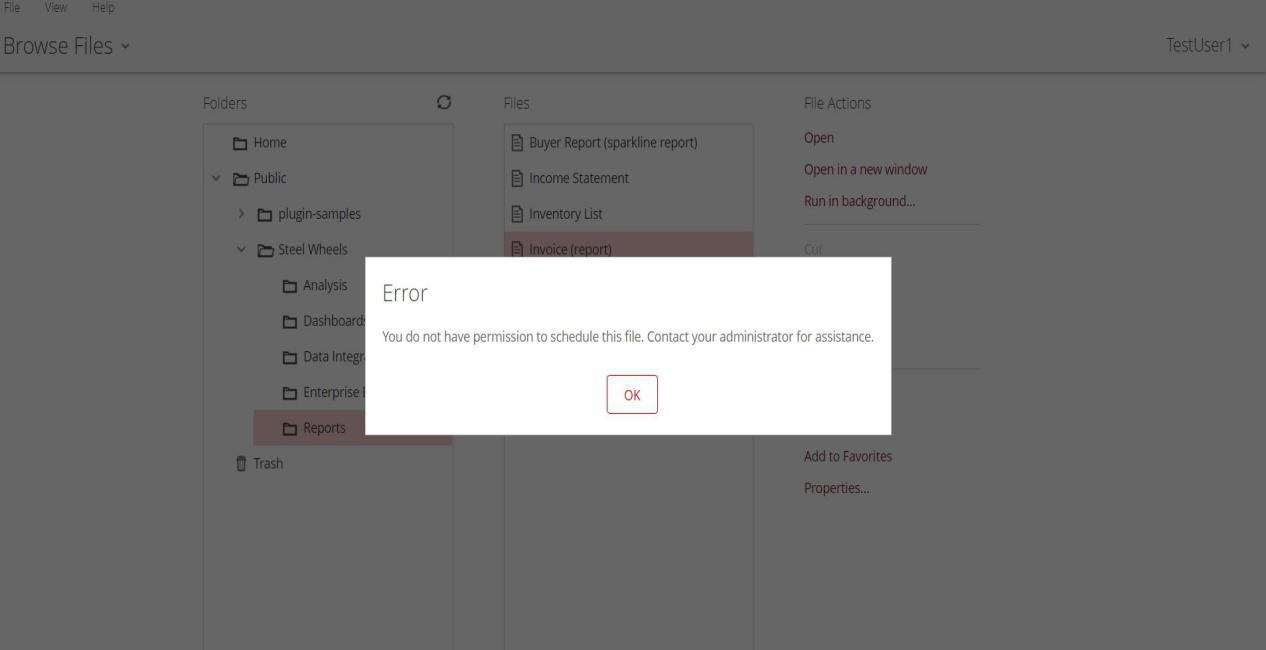
While logging in as **TestUser1** for the first time, **Username** and **Role** check boxes will come, select both the check boxes and select Approve option. Refer screenshot



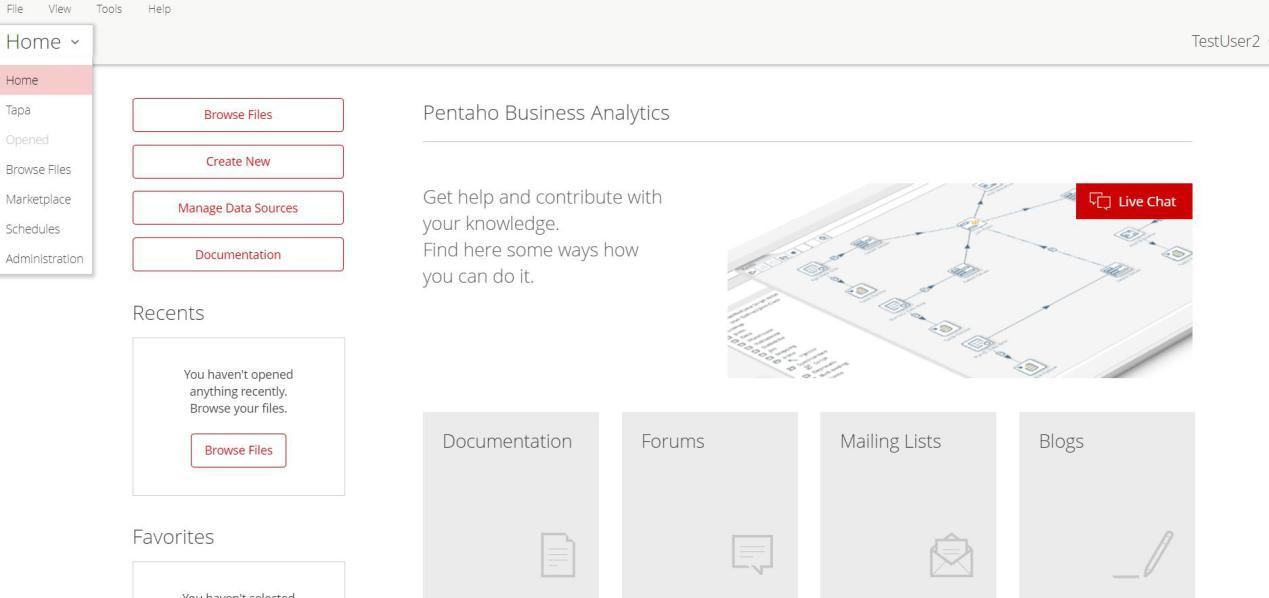
**Note**:Any created user in WSO2 Identity server when logging in for first time should select the **Username** and **Role** check boxes.

**Note**: **Read Content** permission is provided to all **Authenticated** users

As defined earlier in the document, **Business Analyst** role has only **Publish Content** permission, so when TestUser1 tries to schedule a Report, permission has to be denied. Refer the screenshot



Now logout as **TestUser1** and try Logging in as **TestUser2** who has **admin** privileges. Even for **TestUser2** when he is logging in for first time he has to select the **Username** and **Role** check boxes



**TestUser2** has complete **admin** privileges.

This is how Pentaho Community Edition is integrated with WSO2

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_