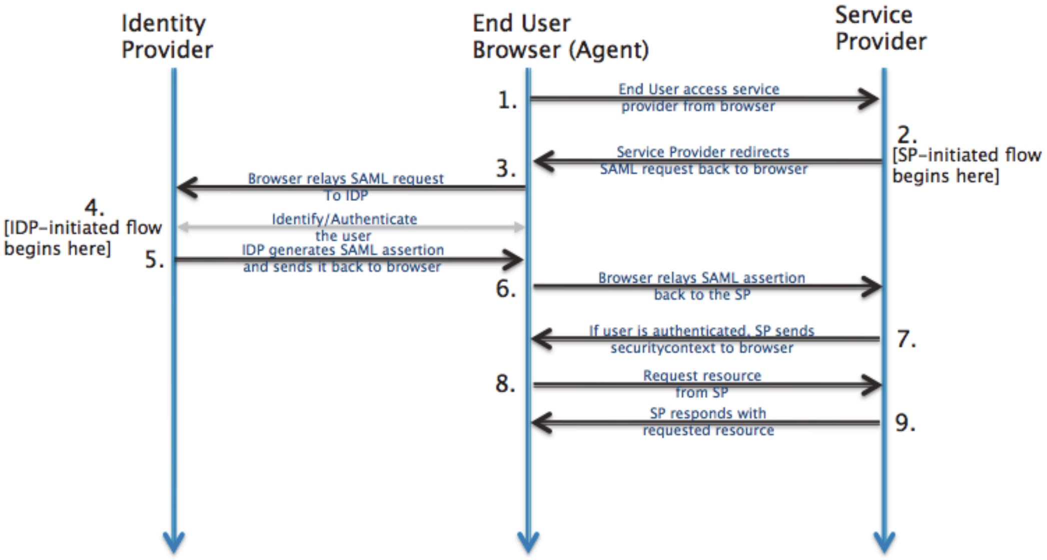
Registering in PingIdentity IdP

SAML: Overview

[1] SAML is mostly used as a web-based authentication mechanism as it relies on the browser being used as an agent that brokers the authentication flow. At high-level, the authentication flow of SAML looks like this:


Identity Provider
End User Browser (Agent)
Service Provider
1.
End User access service provider from browser
2.
[SP–initiated flow begins here]
3.
Service Provider redirects SAML request back to browser
Browser relays SAML request To IDP
4.
[IDP–initiated flow begins here]
Identify/Authenticate the user
5.
IDP generates SAML assertion and sends it back to browser
6.
Browser relays SAML assertion back to the SP
7.
If user is authenticated, SP sends securitycontext to browser
8.
Request resource from SP
9.
SP responds with requested resource

Identity Provider	pingidentity.com	The 3rd-party entity that takes care of the user's authentication; There are multiple such entities with SAML protocol support, such as SSOCircle.com, OneLogin.com, Salesforce.com… For this example, we'll be using pingidentity.com
End-user browser agent	Pentaho User	User that accesses BA-server via browser
Service Provider	BA-server	Pentaho BA Server

[1] http://developer.okta.com/docs/guides/saml_guidance.html

Registering in PingIdentity Identification Provider (IdP)

Note: Each user that intends to use BA-server needs to register itself first in PingIdentity

Prerequisites

1. **Have your chosen Service Provider (i.e. Ba-Server) metadata xml file at hand**

   Developer/QA only: if none is created yet, you can leverage on the already existing SP metadata file for Pentaho BA-Server. For this:
   a. Next to this document, you should have a "`resources`" folder
   b. Download "pentaho-sp.xml" and rename it to something more identifiable with this IdP (e.g. "pentaho-pingidentity-sp.xml");

Registering yourself in PingIdentity

1. Go to https://admin.pingone.com
2. Click "Sign up now"
3. Fill in all fields
   a. Be sure to provide a real email, as a confirmation email will be sent to you (where you will afterwards set your PingIdentity password).
4. Once registration is done, once again go to https://admin.pingone.com and login using your newly defined credentials.
5. Click on the "Add Applications" section
6. Click on the "Add Application" button, as it will open a drop-down; select "New SAML Application"

Field Name	**Field value**
Application Name	Pentaho BA-server
Application Description	SAML integration test for Pentaho BA-server
Application Logo	(optional)
Application Icon	(optional)

7. Click "Continue to Next Step"
8. On the "Protocol Version" field, select "SAML v 2.0"
9. On the Upload Metadata field, upload **your SP metadata xml file**
   a. Recall "Prerequisites" section, step 1: "pentaho-pingidentity-sp.xml"
   b. **Important**: if you get a message stating "`The Entity ID 'xyz' is already in use. You must select a unique entity ID value`", then you cannot upload your metadata file holding that entity ID.

    You can search for the intended application in the "Application Catalog" (top most tab). If none exists there, contact the Services team.

10. Once the metadata file is uploaded, you should get some fields automatically populated (with the information provided by the metadata xml file):

Field Name	**Field value**
Assertion Consumer Serv.	http://localhost:8080/pentaho/saml/SSO
Entity ID	SAML integration test for Pentaho BA-server
Application URL	(empty)
Single Logout Endpoint	http://localhost:8080/pentaho/saml/SingleLogout
Single Logout Response	(empty)
Logout Binding Type	Post
Verification Certificate	(a "saml20metadata.cer" appeared in green)
Signing Algorithm	RSA_SHA256
Force Re-authentication	(unchecked)

11. Click "Continue to next step"
12. Click "Save & Publish"
    a. **Note**: we will be returning to this specific "Attribute Mapping" page later on, once we have configured Roles and have assigned those to our user.
13. On the "Recap configuration" page, click "Finish"

Creating Pentaho Roles and assigning them to Users

1. Go to the "Users" tab (top most bar, 3rd option)
2. On the Users page, click the "Groups" tab
3. Click the "Add Group" button
4. Add a group that can be later used as a Pentaho Role
    a. The best way to do this is to add a prefix to the group name itself (for example, "Pentaho:")
    b. So, for example, if the role would be "Administrator", the group name would be "Pentaho:Administrator"
    c. **Important: you are free to choose the prefix you desire; please memorize the prefix you have chosen, as you will need to reference it afterwards in pentaho.saml.cfg, in the "saml.role.related.user.attribute.prefix" property**
5. On the Users page, click the "Users" tab
6. Select your user (i.e. click its name)
7. Click "Edit" (top right corner)
8. On the "Groups Memberships" section, click "Add"
9. In the "Add Group Membership" pop-up, select the new "Pentaho:Administrator" role and click "Add"
10. Back to the Users edition page, click "Save"
    a. (**optional**) Want to add more roles? You can safely redo the steps in this "Creating Pentaho Roles and assigning them to Users" section.

Sending Pentaho Roles alongside the Authentication Credentials

1. Go to the "Applications" tab (top most bar, 2rd option)

2. Click on your application row
3. Click the “Edit” button
4. Click the “Continue to the Next Step” button in this page and the next one
    a. Stop at the “SSO Attribute Mapping” configuration page
5. Click the “Add new attribute” button
6. On the Application Attribute, type the name of the attribute that will carry the role list (Example: “Pentaho Role”)
    a. **Important: you are free to choose the name you desire; please memorize the name you have chosen, as you will need to reference it afterwards in pentaho.saml.cfg, in the “saml.role.related.user.attribute.name” property**
7. Click on the “Name or literal” field: a drop-down will appear: select “memberOf”
8. Click the “Advanced” button
9. In the “Function” drop-down, select “GetLocalPartFromEmail”
10. Click “Save”
11. Click “Save & Publish”

Getting PingIdentity metadata xml file

1. Go to the “Applications” tab (top most bar, 2rd option)
2. Click on your application row
3. Locate the “SAML Metadata” field and click the “Download” link next to it
    a. **Save this xml metadata file in your local machine**.
    b. **This is PingIdentify providing us a auto-generated “PingIdentity IdP Metadata” xml.**
    c. Rename it to something that will help you identify it (example: “pingidentity-metadata-idp.xml”)
    d. **Important: you will need to place the path to this file afterwards in pentaho.saml.cfg, in the “saml.idp.metadata.filesystem” property**
    e. Open “pingidentity-metadata-idp.xml” with a text editor of your choice
    f. Locate the “entityID” attribute
        i. It should be something like “https://pingone.com/idp/<some-id>”
        ii. **Important: copy-paste this value into pentaho.saml.cfg, in the “saml.idp.url” property**

Ensuring Pentaho Application is enabled in PingIdentity

1. Go to the “Applications” tab (top most bar, 2rd option)
2. Ensure the “Enabled” tab is set to “Yes”

Setting pentaho-solutions/system/karaf/etc/pentaho.saml.cfg properties

1. Edit pentaho-solutions/system/karaf/etc/pentaho.saml.cfg
2. Locate property **saml.idp.metadata.filesystem**
   a. Set the path to the PingIdentity metadata xml file you downloaded in previous steps
3. Locate property **saml.idp.url**
   a. Open your PingIdentity metadata xml file with a text editor of your choice
   b. Locate the "entityID" attribute
      i. It should be something like "https://pingone.com/idp/<some-id>"
      ii. Copy-paste that value into the saml.idp.url property
4. Locate property **saml.role.related.user.attribute.name**
   a. Set the name of the attribute that carries the Roles we've created in previous steps
5. Locate property **saml.role.related.user.attribute.prefix**
   a. Set the prefix (if one was defined) that each of the Pentaho Roles will hold
6. Locate property **ensure.outgoing.logout.request.signed** and set it to 'false'

Recap

We have:

1. Registered onto PingIdentity

2. Added an application called "pentaho", uploaded our metadata xml file to it which automatically populated that application's information

3. Created PingIdentity "groups" that start with a "Pentaho:" prefix and assigned those to our user (and only those)

4. Configured the SAML response so that the authenticated response (from PingIdentity to Pentaho) also carries a list of attributes, namely those "Pentaho:*" groups

5. Got the idp and sp metadata xml files

6. Got the PingIdentity url to use from the "entityID" value

Q&A

Q1 | Do I need a certificate to sign the authentication requests?

Yes.

For this sample, we are using a certificate provided by spring-security-saml, stored in a .jks (keystore file).

It's already bundled in the saml-authentication-provider sample (jar:/security/keystore.jks).

You can get the original here: https://github.com/spring-projects/spring-security-saml/blob/1.0.1.RELEASE/core/src/test/resources/org/springframework/security/saml/key/keystore.jks

If you plan to connect to some other IdPs, then you must ensure you update the keystore file to include the certificate provided by that Identification Provider.