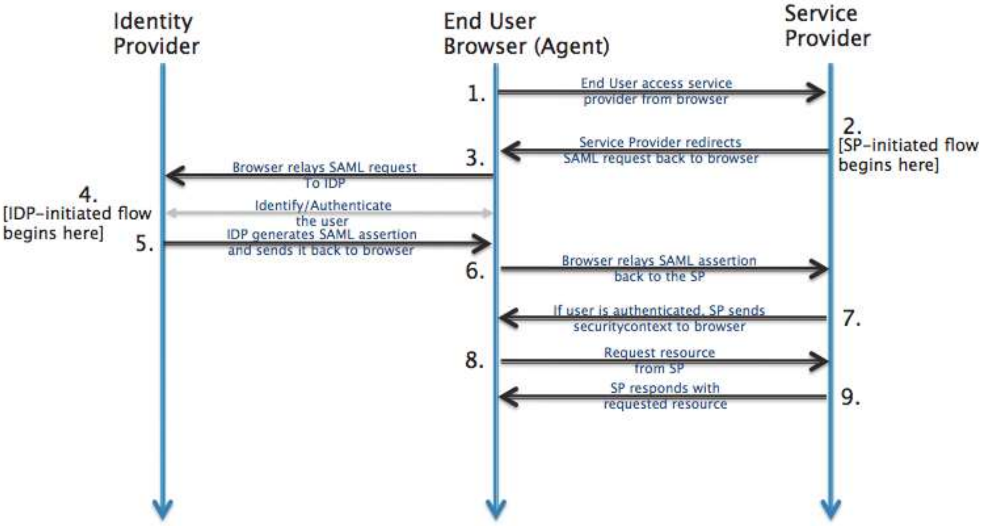
Registering in Active Directory Federation Services 3.0 (AD FS) IdP

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		The 3rd-party entity that takes care of the user's authentication; There are multiple such entities with SAML protocol support, such as OpenSSO, SSOCircle.com, OneLogin.com, Salesforce.com… For this example, we'll be using an AD FS server
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

Pre-requisites for Microsoft AD FS IdP SAML authentication

AD FS requires SSL (HTTPS) connection endpoints so please setup Pentaho BA-server to use SSL connection

1. Access https://help.pentaho.com/Documentation/6.0/0P0/150/030/000

and follow the instructions

MS AD FS SSL Certificate generation

1. For following the next steps, you should have *keystool* available. *keytool* is part of the standard java distribution.
2. Creating SSL certificate for ADFS server
   a. In the following line replace {your domain} by the domain you will use for this tutorial (e.g., idpcompany.org), you can leave everything as it is.

keytool -genkey -keyalg RSA -keysize 2048 -dname "cn=**{your domain},** ou=Organizational Unit, o=Organization, c=US" -alias ADFS -keypass password -keystore IDP_keystore.jks -storepass password -validity 9999

   b. Execute the following command in order to convert the private and public keys to pfx format, to be import later at ADFS.

keytool -importkeystore -srckeystore IDP_keystore.jks -srcstoretype JKS -destkeystore IDP_keys.pfx -deststoretype PKCS12 -deststorepass password -srckeypass password -srcalias ADFS -srcstorepass password

Prepare Service Provider metadata

3. Next to this document, you should have a “resources” folder:
   a. Download “pentaho-sp.xml” file to your local machine
   b. Rename it to a better suited AD FS/BA-server connection name, such as “pentaho-ADFS-sp.xml”
4. Edit “pentaho-ADFS-sp.xml”
   a. Replace “localhost” by the real ip address or name of the machine hosting BA-server
   b. Change the port of the endpoints from “8080” to “8443” or other port that you have defined in your ba-server
   c. Change the endpoints location urls from “http” to “https”
5. Save the file “pentaho-ADFS-sp.xml”, this will be your SP metadata that should be made available in Windows Server 2012 hosting AD FS
6. Use also this metadata in you BA-server

Setup MS AD FS

Prerequisites

1. **Windows Server 2012 R2**
2. **Private and public keys of a SSL Certificate with the common name set to the desired domain name (e.g., "idpcompany.org") or a common name that comprehends the idp domain name (e.g., certificate common name set to "*.idpcompany.org" and the idp domain name is "adfs.idpcompany.org")**
   a. **If you don't have a SSL Certificate, please refer to section: "MS AD FS SSL Certificate generation"**
3. **Service Provider Metadata**

Installing AD DS (Domain Services) and AD FS (Federation Services)

4. Login into Windows Server 2012 R2 with an administrator account
5. Open "Server Manager" application
6. Click on "Manage" (top menu, right side option) and select "Add Roles and Features"
7. Click "Next >"on the first page "Before you Begin"
8. In the next page, "Installation Type", you have two options
   a. Select "Role-based or feature-based installation"
   b. Click "Next >"
9. In the next page, "Server Selection",
   a. Choose "Select a server from the server pool"
   b. Verify that in the Server Pool exists one server and it is selected
   c. Click "Next >"
10. In the following screen,
    a. Select the Roles:
       i. "Active Directory Domain Services",
       ii. "Active Directory Federation Services".
    b. If a popup window appears asking to add features, click on "Add Features".
11. Next page, "Features", do not make changes
    a. Click "Next >"
12. Now you should have a page called "Active Directory Domain Services"
    a. Click "Next >"
13. The following page, should be "Active Directory Federation Services"
    a. Click also "Next >"
14. Finally, on the "Confirmation" page
    a. Click "Install"
    b. Wait for the Installation to finish.
    c. When it finishes click "Close"

Configure AD DS (Domain Services)

1. On the left menu of Server Manager click on "AD DS"
2. Below "SERVERS" there should be a warning with yellow background with the text: "Configuration required for Active Directory Domain Services at WIN-…. ".
   a. After the text, click on "More…".
   b. A new window should open.
   c. In the top box, you should have a row with the following "Message" column: "Configuration required for Active Directory Domain Services at WIN-..",

d. On the same row click on the “Action” column “Promote this server to a domain controller”.

e. The Active Directory Domain Services Configuration Wizard should now appear.

3. On the first page:
   a. Select “Add a new forest”
   b. After “Root domain Name:” type your domain that should be the same as the SSL certificate’s common name (e.g., idpcompany.org)
   c. Click “Next >”
4. Next page, “Domain Controller Options”
   a. “Forest functional level:” Windows Server 2012 R2
   b. “Domain functional level:” Windows Server 2012 R2
   c. Check “Domain Name System (DNS) server”
   d. Type a “Password” and type the same for “Confirm password”
   e. Click “Next >”
5. Next page, “DNS Options” there is nothing you will do
   a. Click “Next >”
6. Next page, “Additional Options”,
   a. Keep the suggestion for “The NetBIOS domain name:” field or just type your domain name uppercased (e.g., IDPCOMPANY)
   b. Click “Next >”
7. In page,“Paths”
   a. Leave every field as it is, there should something like:
      i. DataBase Folder: C:\Windows\NTDS
      ii. Log files folder: C:\Windows\NTDS
      iii. SYSVOL folder: C:\Windows\SYSVOL
   b. Click “Next >”
8. In page, “Review Options”, here you can review your selection and go to previous steps to correct any mistake
   a. If everything is correct, Click “Next >”
9. In page “Prerequisites Check”, the configuration wizard will search for prerequisites, if it passes with warnings, do not worry
   a. Click “Install”
10. Finally, in “Results”
    a. Click “Close“
    b. And the windows server should restart

Configure AD FS (Federation Services)

1. Open “Server Manager” application
2. On the left menu of “Server Manager” click on “AD FS”
3. Below “SERVERS” there should be a warning with yellow background with the following text: “Configuration required for Active Directory Federation Services at WIN-…. ”.
   a. After the text, click on “More…”.
   b. A new window should open.
   c. In the top box, you should have a row with the following “Message” column: “Configuration required for Active Directory Federation Services at WIN-..”,

d. On the same row click on the Action “Configure the federation service on this server.”.

e. The Active Directory Federation Services Configuration Wizard should now appear.

4. In “Welcome” page:

   a. Select “Create the first federation server in a federation server farm”

   b. Click “Next >”

5. In “Connect to AD DS” page

   a. The account that appears should be the same which you used to setup “AD DS” in last section, the default should be right (e.g., IDPCOMPANY\Administrator)

   b. Click “Next >”

6. In “Specify Service Properties” page

   a. Click “Import”

   b. Select the public and private key contained in a pfk file extension that contains the SSL Certificate (e.g., IDP_keys.pfk)

      i. You may have created it previously and the common name should be the same of your server domain.

      ii. If you don’t have such Certificate or file, please refer back to section: “MS AD FS SSL Certificate generation”

   c. When asked for a password, if you are using the SSL Certificate generated in “MS AD FS SSL Certificate generation” type “password”, otherwise type the password of your key.

   d. The SSL Certificate and Federation Service Name fields should now have the domain you selected.

   e. Type a name for the “Federation Service Display Name” field (e.g., IDP Company)

   f. Click “Next >”

7. Next page, “Specify Service Account”

   a. The option “Use an existing domain user account or group Managed Service Account” should be already selected. Click “Select…”

   b. In the text box below “Enter the object name to select (examples):” type your account name (e.g., Administrator).

   c. Click “OK”

   d. In the field “Account Password:“ type your account password

   e. Click “Next >”

8. In “Specify Database” page

   a. Should be selected the option “Create a database on this server using Windows Internal Database”

   b. Click “Next >”

9. In “Review Options” page, you can review your selection and go to previous steps to correct any mistake

   a. If everything is correct, Click “Next >”

10. At “Prerequisites Check” page, the configuration wizard will search for prerequisites, it should pass all checks

    a. Click “Configure”

11. Wait for the Installation to finish

12. Finally, in “Results” page

    a. Click “Close”

Configure SP in AD FS

1. Open “AD FS Management” application
2. Left click on “AD FS” to select it
3. Right click on “Action” on the top menu and select “Add Relying Party Trust Wizard”
4. A new window should open in the “Welcome” page
    a. Click “Start”
5. In “Select Data Source” page, you should have three options
    a. Choose “Import data about the relying party from a file”
    b. Click “Browse…” and select the SP metadata file (e.g., that you have modified in section “Prepare Service Provider metadata”
    c. Click “Next >”
6. Next page, “Specify Display Name”
    a. Type “pentaho” in the text box below “Display name:”
    b. Click “Next >”
7. In “Configure Multi-factor Authentication Now?” page
    a. Select the option “I do not want to configure multi-factor authentication settings for this relying party trust at this time”
    b. Click “Next >”
8. Next page, “Choose Issuance Authorization Rules”
    a. Select “Permit all users to access this relying party”
    b. Click “Next >”
9. In “Ready to Add Trust” page, you have the information that will be added about the SP. If the SP metadata was correct, everything should be correct and you can proceed
    a. Click “Next >”
10. In “Finish” page
    a. Enable the check followed by the text: “Open the Edit Claim Rules dialog for this relying party trust when the wizard closes”
    b. Click “Close”
11. A new window called “Edit Claim Rules for pentaho” should open
    a. Select the “Issuance Transform Rules” tab
    b. Click on “Add Rule…”
12. The window “Add Transform Claim Rule Wizard” should open
    a. Select “Send LDAP Attributes as Claims” below “Claim rule template:”
    b. Click “Next >”
13. In “Configure Claim Rule” page
    a. Type “pentaho claim rules” below “Claim rule name:” or you can type other name if you like
    b. Below “Attribute Store:”, select “Active Directory”
    c. Below “Mapping of LDAP attributes to outgoing claim types:” there is a table of two columns and a row. Each time you fill a row, a new empty one will be added to the end of the table. Please fill the table to look according to the following table:

LDAP Attribute (Select or type to add more)	**Outgoing Claim Type (Select or type to add more)**
E-Mail-Addresses	E-Mail Address
User-Principal-Name	Name ID
Token-Groups - Qualified by Long Domain	Pentaho Role

d. Click “Finish”
e. In the remaining window click “OK”.

14. Back to “AD FS Management” main window, you will now export the signing certificate of AD FS
    a. Go To “Services” on the left menu and expand it
    b. Click on “Certificates”
    c. On the middle section, right click on the row below “Token-signing”, select “View Certificate…”
    d. A new window appears, select “Details” tab
    e. Click “Copy to File…”
    f. The “Certificate Export Wizard” should appear
        i. Click “Next”
        ii. Select “Base-64 encoded X.509 (.CER)”
        iii. Click “Next”
        iv. Click “Browse..” and save the file (e.g., C:\ADFS_Signing.cer). **This is the public key of ADFS signing. Later, you will have to add it to ba-server keystore**.
        v. Click “Next”
        vi. The next page is just a summary, so click “Finish”
        vii. A window should appear with the text “The export was successful.”
            1. Click “OK”
    g. Click “OK” to close the certificate window
15. Again back to “AD FS Management” main window, you still need to make modifications into our “Party Trust”
    a. Got to “Trust Relationships” on the left menu and expand it
    b. Click on “Relying Party Trusts”
    c. On the middle section, double click on the row with the “Display Name” “pentaho”.
    d. Select the “Advanced” tab
    e. Change the “Secure hash algorithm” to “SHA-256”
    f. Click “OK”
16. In this step, you will create a new group called “Pentaho_Administrator” that will be assigned to the users that you want to have administrator’s rights in BA-server
    a. Open “Active Directory Users and Computers” application
    b. On the left menu, expand your domain (e.g., idpcompany.com)
    c. Select and Right click on “Users” and go to “New” -> “Group”
    d. A window called “New Object – Group” will open
        i. Type “Pentaho_Administrator” below “Group name:”
        ii. The same name should appear in “Group name (pre-windows 2000):”
        iii. “Group scope” should be “Global”
        iv. “Group type” should be “Security”
        v. Click “OK”
    e. With “Users” selected, the new group should appear on the list
    f. Right click on the user that you want to grant Pentaho Administrator rights. (e.g., Administrator) and select “Properties”
        i. The user Properties window will open
        ii. Select the tab “Member Of”
        iii. Click on “Add…”
        iv. Above “Enter the object names to select (examples):”, type “Pentaho_Administrator”

v. Click “OK” to close the window

g. Click “OK” again to close the user properties window

17. Now the AD FS server is configured, please restart your windows server (alternatively you can just restart AD FS service on “Server Manager”)
18. The idp login and logout webpage is:
    a. Replace {AD FS host name} by AD FS machine’s name (e.g., idpcompany.org)

    https://{AD FS host name}/adfs/ls/idpinitiatedsignon.htm (You can start a Global logout from the IdP from this url)

Recap

We have:

1. Setup AD FS in windows server 2012 R2

2. Added a “Relying Party Trusts” called “pentaho”, and configured the endpoints by passing the SP metadata

3. Configured the claims to send user properties to the SP in the authenticated response (from AD FS to Pentaho). This response carries:
    a. User’s Name ID
    b. User’s e-mail-addresses
    c. User’s list of groups

4. Changed the “Secure hash algorithm” of “pentaho” to “SHA-256”

5. Got the AD FS signing certificate to be trusted by BA-server

Setup AD FS in BA-server

Add AD FS Signing Certificate to BA-server keystore

1. Have AD FS signing certificate at hand that you created in step 14 of "Configure SP in AD FS"
2. Download the keystore holding the keys of SP to the same location of AD FS signing certificate
    a. **Important: Don't have a keystore yet? Only for Dev/QA/Services teams, and for testing proposes you can grab the keystore at either:**
        i. **Inside of the kar file "pentaho-saml-sample-6.0-SNAPSHOT.kar" at repository/pentaho/pentaho-saml/6.0-SNAPSHOT/, there is a jar file named "pentaho-saml-6.0-SNAPSHOT.jar" inside of this jar at security/ folder is the keystore.jks file**
        ii. **Or at:**

https://github.com/spring-projects/spring-security-saml/blob/1.0.1.RELEASE/core/src/test/resources/org/springframework/security/saml/key/keystore.jks

3. Add signing certificate to the keystore
    a. Execute the following command
        i. Replace {AD FS signing certificate} by AD FS singing certificate file name
        ii. Replace {keystore path} to the path of the keystore used in BA-server (e.g., keystore.jks*)*
        iii. Replace {keystore password} by the password of the keystore
            1. Important: Using the Dev/QA/Services keystore? the password is *nalle123*

keytool -import -alias ADFS -file {AD FS signing certificate} *-keystore keystore.jks -storepass* {keystore password}

    b. When asked to "Trust this certificate? [no]:" type "yes" and press enter
4. Later on BA-server set {keystore path} to be the keystore property.

Getting AD FS metadata xml file

1. Go to page:
    a. replace {AD FS host name} by AD FS machine's name

https://{AD FS host name}/federationmetadata/2007-06/federationmetadata.xml

    a. **Save this xml metadata file in your local machine**.
    b. **This is AD FS providing us a auto-generated "AD FS IdP Metadata" xml.**
    c. Rename it to something that will help you identify it (example: "adfs-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 "adfs-metadata-idp.xml" with a text editor of your choice
    f. Locate the "entityID" attribute
        i. It should be something like:

"https://{AD FS host name}/federationmetadata/2007-06/federationmetadata.xml"

        ii. where, {AD FS host name} is the AD FS machine's name

iii. **Important**: **copy-paste this value into pentaho.saml.cfg, in the "saml.idp.url" property**

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

1. Edit pentaho-solutions/system/karaf/etc/pentaho.saml.cfg
2. Locate property **saml.sp.metadata.filesystem**
    a. Set the path to the same "pentaho-ADFS-sp.xml" file that you created in section "Prepare Service Provider metadata"
3. Locate property **saml.idp.metadata.filesystem**
    a. Set the path to the AD FS metadata xml file you downloaded in previous steps
4. Locate property **saml.idp.url**
    a. Open your AD FS metadata xml file with a text editor of your choice
    b. Locate the "entityID" attribute
        i. It should be something like:

"https://{AD FS host name}/federationmetadata/2007-06/federationmetadata.xml"

        ii. where, {AD FS host name} is the AD FS machine's name
        iii. Copy-paste that value into the saml.idp.url property
5. Locate property **saml.signature.algorithm** and set the value to **SHA256**, or match the algorithm specified on the Advanced tab of the pentaho Relying Party Trust
6. 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 (e.g., Pentaho Role)
7. Locate property **saml.role.related.user.attribute.prefix**
    a. Set the prefix that each of the Pentaho Roles will hold to:
    { AD FS host name }\\{group prefix for pentaho}
    b. where { AD FS host name } is the name that resolves to your AD FS machine address (e.g., idpcompany.org in this tutorial)
    c. and {group prefix for pentaho} is the manual defined prefix for Pentaho groups (e.g., Pentaho_ in this tutorial).
8. Locate property **ensure.outgoing.logout.request.signed**
    a. Set it to 'true'

Troubleshooting

Install JCE Unlimited Strength in your jre or jdk

If you are getting this error:
ERROR [Decrypter] Error decrypting the encrypted data element
org.apache.xml.security.encryption.XMLEncryptionException: Illegal key size
Original Exception was java.security.InvalidKeyException: Illegal key size

The solution is to install the JCE Unlimited Strength, which are stronger security libraries that oracle can not ship with the jre and jdk due to export policies.

1. Download at http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html
2. Follow the instructions in the "README.txt" inside of the downloaded archive

Add AD FS host name to your hosts

If you are building a test environment and the idp name (e.g., idpcompany.org) is not recognized in your network (if you followed the tutorial and have AD FS and BA-server in different machines or VMs), then you have to add the name, to the hosts file of your operative system:

1. Find the ip address of idp hosting server (execute "ipconfig" in windows server's PowerShell)
2. Depending on your operative system, open the host file (you can find more information at https://en.wikipedia.org/wiki/Hosts_%28file%29)
3. Add a new line replacing {idp ip address} by the real ip address of the idp and { AD FS host name } by the idp name that is not recognized in your network.
   {idp ip address}   { AD FS host name }
   e.g.,
   192.168.1.1   idpcompany.org