WebLogic Integration Kit

Contents

WebLogic Integration Kit

The PingFederate WebLogic Integration Kit adds a new service provider (SP) integration option to PingFederate.

Features

The Weblogic Integration Kit consists of two parts:

- The adapter, which runs within the PingFederate server.
- The 'PingFederate Identity Asserter for Weblogic', which resides with the application server.

The kit uses a proprietary, secure token format (PFTOKEN) to transfer the attributes between the PingFederate server and the Weblogic server.

ⓘ **Note:** The Standard Adapter is bundled with the PingFederate installation. For details, see the "Standard Adapter Configuration" appendix in the PingFederate *Administrator's Manual*.

The integration kit leverages the Standard Adapter, which is packaged with the PingFederate 4.x server. It uses BEA's Security Service Provider Interface (SSPI) to implement an identity asserter that is used for perimeter authentication by Weblogic domain.

Intended audience

This document is intended for PingFederate administrators.

If you need help during the setup process, see the following resources:

- The following sections of the PingFederate documentation:
  - *Identity provider SSO configuration*
  - *Managing IdP adapters*
  - *Authentication Policies*
  - *SP connection management*

System requirements

- PingFederate 4 server
- The J2SE Java Runtime Environment 1.4.2 or later for the agent side
- Weblogic Server 9.X

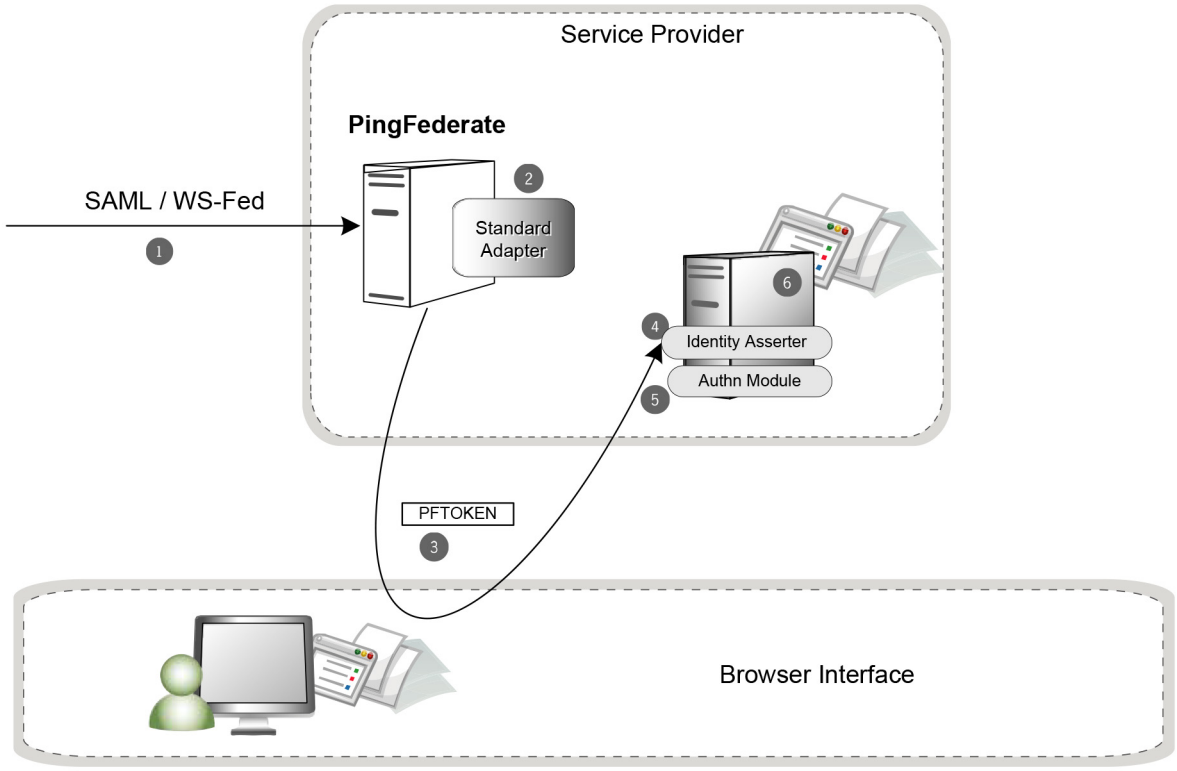
ⓘ **Note:** WebLogic Server 9.1 was tested and several issues were discovered. Version 9.2 is recommended for use with PingFederate 4.

Overview of the SSO flow

A Weblogic Identity Assertion provider is a specific form of Authentication provider that allows users or system processes to assert their identity using tokens (in other words, perimeter authentication). Identity Assertion providers enable perimeter authentication and support single sign-on. For more information, see the *Weblogic server documentation*.

To integrate with Weblogic on the IdP side, use the Java Integration Kit. It is available from the *PingFederate server add-ons page*.

The following figure shows the basic scenario in which PingFederate server leverages the Standard Adapter and the Identity Asserter to allow SSO to a Weblogic domain.



Processing steps:

1. PingFederate 4 server receives a SAML / WS-Federation assertion..
2. The PingFederate SP server parses the SAML assertion and passes the user attributes to the Standard SP Adapter. The Adapter encrypts the data internally and generates a PFTOKEN.

> ⓘ **Note:** Optionally, the PingFederate server can be configured to look up additional attributes from data stores and add them to the attributes received in the IdP's assertion. In many cases, the SP may want to persist an account and pass internal attributes for profiling or other reasons. (See the *Administrator's Manual* for more information.)

3. A request containing the PFTOKEN is redirected to the SP application. Additional attributes can be configured to transfer as part of the 'Request Header" or as "Cookies".
4. PingFed Identity Asserter for Weblogic is invoked that retrieves the username from PFTOKEN.
5. The configured Authn Module with Weblogic is invoked and validates the username extracted in the previous step thereby creating a valid Principal.
6. A local security context is created and the user has access to the protected resource.

Setup

Setup PingFederate and QuickStart sample application

About this task

In this section we setup PingFederate and the Quickstart sample application that is shipped with the product. Setting up Quickstart isn't necessary for this integration but it ensures that the basic issues around PingFederate configuration are sorted out.

Steps

1. Download PingFederate and follow the Quick Start Guide to set up the IdP/SP SSO scenario.
2. Verify that the SSO is working for the PingFederate IdP/SP Quick Start Sample Application.
3. Once the basic SSO is working with the Quick Start Sample application, make the following changes to update the Quick Start setup to test the Weblogic integration.
   a. From the main menu of the PingFederate Admin Console, click 'Local Settings' and update 'SSO Success URL' under 'SP Events' to `http://hostname:7001/wlssample/secure.jsp`, where hostname is the name of the machine where the Weblogic server is running.
   b. From the main menu of PingFederate Admin Console, click "SP Adapters".
   c. Select the adapter configured while configuring the QuickStart.
   d. In the Adapter configuration screen, change the value of "PFTOKEN holder name" to "PFTOKEN_WLSIDENTITY'.
   e. Change the value of "Transfer method" to "Cookie".
   f. Change the Password. We will be entering the same password in Weblogic console while configuring the identity asserter.

WebLogic initial setup

About this task

In this section, we setup a Weblogic Server instance and configure a user /group in the embedded LDAP server. Once the basic setup (as mentioned in this document) is up and running, you can change the users/groups/roles as required by your environment. Instead of using the embedded LDAP Server, you can also use any external directory server that is supported by Weblogic. The user/group as specified in this section is used by the web application (wlssample) that is part of this distribution.

Steps

1. Download Weblogic 9.x Server. For instructions, see *Downloading and installing WebLogic Server* in the WebLogic documentation.
2. Create a Weblogic Domain. Use Domain Configuration Wizard to create one as shown in *Starting the Configuration Wizard* in the WebLogic documentation. For this guide, we'll assume that the Weblogic Server is running at `http://localhost:7001` and the domain name is "mydomain".
3. Start the Weblogic Server and access the console at `http://localhost:7001/console`.
4. Use the navigation menu and select mydomain -> Security Realms ->myrealm -> Users and Groups -> Groups.
5. Click "New" and enter 'PingIdentity' as the group name and hit 'OK'. Leave the "Provider" as "DefaultAuthenticator'.

6. Use the navigation menu and selectmydomain -> Security Realms -> myrealm -> Users and Groups -> Users.
7. Click “New” and enter name=”joe”, password=”password” and hit “OK”. Leave the “Provider” as “DefaultAuthenticator’.
8. Select the user “joe” again and add it to the group “PingIdentity” by clicking the tab “Group” and moving “PingIdentity” from “Available” to “Chosen”. [The group ‘PingIdentity’ is specified in the bundled web application as the group that is allowed to access protected resources.]
9. Shutdown the Weblogic application server.

WebLogic Identity Asserter installation

In this section, we install the Identity Asserter (part of this distribution) to the Weblogic Server. This can be done using with either of the following approaches.

Option One:

Copy the following files to the DOMAIN_DIR/lib, where DOMAIN_DIR represents the root directory of your domain e.g. mydomain.

- pf4-identityasserter-1.1.jar
- commons-codec-1.3.jar
- pf4-pftoken-agent-1.1.jar

This will allow for PingFederate Identity Asserter to be available for configuration through the Weblogic console.

Option Two:

You can also install the identity asserter with the following steps:

1. Copy the file `pf4-identityasserter-1.1.jar` to the following directory: `<BEA_HOME>\weblogic91\server\lib\mbeantypes`, where<BEA_HOME>is the directory where BEA software is installed.
2. Copy the following jar files to your startup classpath of the Weblogic Server instance.
   - pf4-pftoken-agent-1.1.jar
   - commons-codec-1.3.jar

WebLogic Identity Asserter configuration

About this task

This section discusses how to configure the Ping Federate Identity Asserter using the WebLogic Console. Once configured, the WebLogic server with invoke it for every new request. The order of various security providers can be configured through the WebLogic console. Sort the order and ensure that this identity asserter is the first one in the providers list.

Steps

1. Start the weblogic server using startWebLogic.cmd. Access the console at `http://localhost:7001/console`.
2. Through the navigation menu, Select **mydomain**# **Security-Realms**# **myrealm**# **Providers**# **Authentication**.
3. Click the ‘ ***Lock & Edit’*** button in the Change Center to activate the buttons on this page.
4. Click “**New**”. It will show the “*Create a new Authentication Provider*” screen.
5. Enter *Name=”PingFed Identity Asserter”*. Choose *Type=”PingFedIdentityAsserter”* and click OK.

6. Select ‘PingFed Identity Asserter’ again from the list and click on the tab ‘Provider Specific’. Enter the same password you entered while configuring the Standard Adapter in PingFederate console.
7. Click “Activate Changes’ in the ‘Change Center’.
8. Shutdown the Weblogic Server.

> ⓘ **Note:**
>
> There is a known bug in the WebLogic Server 9.2. The ‘`Base64CodingRequired`’ Flag as set in the WebLogic Console isn’t effective. Make the following change manually in the `config.xml` to get around the issue.
>
> Look for the following line (under element `authentication-provider`):
> `<sec:name>PingFedIdentityAsserter</sec:name>`
>
> And add the following line under it:
>
> `<sec:base64-decoding-required>false</sec:base64-decoding-required>`
>
> `CR257702`
>
> Contact BEA support with this CR number to get more details or patch.

WebLogic SP application setup

About this task

In this step, we deploy the web application that is shipped as part of this distribution. The security settings in the web.xml have been set to use “CLIENT-CERT” and the page “secure.jsp” is secured to only allow access to the selected group/role. The steps here are only for guidance. If you have other preferred steps for deploying web applications to Weblogic Server, you can use them as well.

Steps

1. Copy the directory ‘wlssample from the attached zip to the following directory `<DOMAIN_DIR>/autodeploy`, where <DOMAIN_DIR> represents the root directory of the Weblogic domain e.g. mydomain.
2. Start the weblogic server.
3. Access the web application by pointing the browser to the following location: `http://locahost:7001/wlssample/secure.jsp`. You should get a 401 (Unauthorized Access). This will validate the resource is protected.

Testing

About this task

In this section, we test the application. We use the Quickstart IdP Application for the IdP side and use the application shipped with this distribution for the SP side.

Steps

1. Access the IdP web application by pointing the browser to IdP URL as configured in Section A.
2. Login using joe/test.
3. Initiate SSO by clicking ‘IdP-initiated SSO to Sample_SP’. The request will be redirected to the SP Application *secure.jsp* page and the principal/subject information will be displayed on the screen.

Release notes

Qualification statement

Version Tested:

- pf4-weblogic-integration-kit-1.1.zip

Operating Systems Tested:

- Windows Server 2003

Weblogic version used:

- Weblogic Server 9.1

PingFederate Configuration Items:

- Standard IdP Adapter
  - Authentication Service – For SSO
  - PFTOKEN Holder Name – Name of Cookie or query parameter – Must be Unique
  - Domain Name – For Cookie validation
  - Cookie Path – For PFToken Cookie
  - Password – For encryption
  - Transfer Method – For sending PFToken
  - PFToken Cookie Max Age – Lifetime the token can be used – Integer > 0
  - Encryption algorithm – AES
  - Cipher Mode – CBC,
  - Key Size – 128
  - Iteration Count – Number of iterations for generating the client key
- Standard SP Adapter
  - PFTOKEN Holder Name – Name of Cookie or query parameter – Must be PFTOKEN_WLSIDENTITY
  - Domain Name – For Cookie validation
  - Cookie Path – For PFToken Cookie
  - Password – For encryption
  - Transfer Method – For sending PFToken – Must be Cookie
  - PFToken Cookie Max Age – Lifetime the token can be used – Integer > 0. It's best to set this value to 0 so the Cookie is treated as a session cookie.
  - Encryption algorithm – AES
  - Cipher Mode – CBC,
  - Key Size – 128
  - Iteration Count – Number of iterations for generating the client key
  - Send extended attributes – sending extended attributes.

Purpose:

The PingFederate 4 Weblogic Integration kit adds a new Service Provider (SP) integration option to PingFederate. The kit uses a proprietary, secure token format (PFTOKEN) to transfer the attributes between the PingFederate server and the Weblogic server.

The Weblogic Integration Kit consists of two parts. The first part is the Standard Adapter, which runs on the PingFederate server. The second part is the "PingFederate Identity Asserter for Weblogic", which resides with the application server.

Known issues/problems/limitations:

- The “PingFederate Identity Asserter for Weblogic” doesn’t have access to the cookies and therefore it can not delete them. It’s recommended to set up PFToken Cookie Max Age value as 0 so the Cookie is treated as a session cookie.
- pf4-weblogic-integration-kit-1.1 is dependent on standard integration kit v1.1.
- The current version of the adapter doesn’t support Single Logout (SLO) for WebLogic domain.
- A persistent cookie (PFTOKEN_WLSIDENTITY) is used to transfer user information between the PingFederate server and the Weblogic domain. The default maxAge for the cookie as specified through the PingFederate console is ‘300 seconds’. If the user closes the browser/application, opens a new browser within the maxAge interval and navigates to the WebLogic hosted application, the browser will find the cookie again. It will then present the cookie to the WebLogic app server, and that server will then assert the identity and therefore log in the user again. To mitigate this behavior, you can set the maxAge value to a lower value through PingFederate Admin console.

Exclusions:

- The Weblogic Integration Kit has not been stress or performance tested.
- The Weblogic Integration Kit has not been tested in a clustered environment.
- The Weblogic Integration Kit is not FIPS 140 compliant. The encryption information contained in and used by the Integration Kit is not stored in the Hardware Security Module (HSM) when PingFederate is used with an HSM.

Download manifest

The distribution `.zip` archive for the Weblogic Integration Kit contains the following:

- /docs – contains additional documentation:
  - legal.pdf – copyrights and license information
  - Weblogic_Integration_Kit_Qualification_Statement.doc – testing and platform information
  - Weblogic_Integration_Kit_User_Guide.pdf – this document
- /dist – contains libraries needed to run the adapter:
  - pf4-pftoken-adapter-1.1.jar – the Standard Adapter JAR file

    ⓘ **Note:**

    The Standard Adapter is bundled with the PingFederate 4 installation. Verify that you have the latest version of the jar file in:

    ```
    <pf_install_dir>\pingfederate\server\default\deploy.
    ```

  - commons-codec-1.3.jar – from apache for common encoding/decoding operations
  - pf4-pftoken-agent-1.1.jar – the Agent Toolkit for Java (supports JDK 1.4.x and JDK 1.5.x)
  - pf4-identityasserter-1.1.jar – PingFederate Identity Asserter for Weblogic
- /test – contains test setup
  - webapps/wlsapp – Sample web application