Red Hat Process Automation Manager 7.0

Integrating Red Hat Process Automation Manager with Red Hat Single Sign-On

Last Updated: 2018-10-05

Red Hat Process Automation Manager 7.0 Integrating Red Hat Process Automation Manager with Red Hat Single Sign-On

Red Hat Customer Content Services
brms-docs@redhat.com

法律上の通知

概要

This document describes how to integrate Red Hat Single Sign-On with Red Hat Process Automation Manager to provide a single secure authentication method.

目次

PREFACE

As a system administrator, you can integrate Red Hat Single Sign-On with Red Hat Process Automation Manager to secure your Red Hat Process Automation Manager browser applications with a single authentication method.

Prerequisite

Red Hat Process Automation Manager is installed on Red Hat JBoss EAP 7.1. For information, see **Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.1**.

第1章 INTEGRATION OPTIONS

Red Hat Single Sign-On (RH-SSO) is a single sign-on solution that you can use to secure your browser applications with your REST web services and Git access.

When you integrate Red Hat Process Automation Manager with RH-SSO, you create an SSO and identity management (IDM) environment for Red Hat Process Automation Manager. The session management feature of RH-SSO enables you to use a single authentication for different Red Hat Process Automation Manager environments on the internet.

The following chapters describe how you can integrate RH-SSO with Red Hat Process Automation Manager:

- **4章*Authenticating Business Central through RH-SSO***
  To authenticate Red Hat Process Automation Manager through an RH-SSO server, you must secure both the Red Hat Process Automation Manager web client (Business Central) and remote services through RH-SSO.This integration enables you to connect to Red Hat Process Automation Manager through RH-SSO using either Business Central or a remote service consumer.

- **5章*Authenticating Process Server through RH-SSO***
  To authenticate Process Server through an RH-SSO server, you must secure the remote services provided by Process Server. Doing this enables any remote Red Hat Process Automation Manager service consumer (user or a service) to authenticate through RH-SSO. Note that Process Server does not have a web interface.

- **6章*Authenticating third-party clients through RH-SSO***
  If Business Central or Process Server are using RH-SSO, third-party clients must authenticate themselves using RH-SSO. After authentication, they can consume the remote service endpoints provided by Business Central and Process Server, such as the REST API or remote file system services.

For more information about RH-SSO, see the **Red Hat Single Sign-On Getting Started Guide**.

第2章 INSTALLING AND CONFIGURING RH-SSO

A realm is a security policy domain defined for a web or application server. Security realms are used to restrict access for different application resources. You should create a new realm whether your RH-SSO instance is private or shared with other products. You can keep the master realm as a place for super administrators to create and manage the realms in your system. If you are integrating with an RH-SSO instance that is shared with other product installations to achieve single sign-on with those applications, all of those applications must use the same realm. To create an RH-SSO realm, download, install, and configure RH-SSO 7.2.

注記

If Business Central and Process Server are installed on different servers, complete this procedure on both servers.

Procedure

1. Navigate to the Software Downloads page in the Red Hat Customer Portal (login required), and select the product and version from the drop-down options:
   - Product: Red Hat Single Sign-On
   - Version: 7.2
2. Download **Red Hat Single Sign-on 7.2.0 Server** (`rh-sso-7.2.0.GA.zip`).
3. To install and configure a basic RH-SSO standalone server, follow the instructions in the "Installing and Booting" chapter of the **Red Hat Single Sign On Getting Started Guide**. For advanced settings for production environments, see the **Red Hat Single Sign On Server Administration Guide**.

注記

If you want to run both RH-SSO and Red Hat Process Automation Manager servers on the same system, ensure that you avoid port conflicts. by doing one of the following:

- Update the `RHSSO_HOME/standalone/configuration/standalone.xml` file and set a port offset to 100. For example:

```
<socket-binding-group name="standard-sockets" default-
interface="public" port-
offset="${jboss.socket.binding.port-offset:100}">
```

- Use an environment variable to run the server:

```
bin/standalone.sh -Djboss.socket.binding.port-
offset=100
```

第3章 ADDING RED HAT PROCESS AUTOMATION MANAGER USERS

Before you can use RH-SSO to authenticate Business Central or Process Server, you must add users to the realm that you created. To add new users and assign them a role to access Red Hat Process Automation Manager, complete the following steps:

1. Log in to the RH-SSO Admin Console and open the realm to which you want to add a user.
2. Click the **Users** menu item under the **Manage** section.
   An empty user list appears on the **Users** page.
3. Click the **Add User** button on the empty user list to start creating your new user.
   The **Add User** page opens.
4. Provide user information on the **Add User** page and click **Save**.
5. Select the **Credentials** tab and create a password.
6. Assign the new user one of the roles that allow access to Red Hat Process Automation Manager. For example, assign the **`admin`** role to access Business Central or assign the **`kie-server`** role to access Process Server.
7. Define the roles as realm roles in the **Realm Roles** tab under the **Roles** section.
8. Click the **Role Mappings** tab on the **Users** page to assign roles.

第4章 AUTHENTICATING BUSINESS CENTRAL THROUGH RH-SSO

This chapter describes how to authenticate Business Central through RH-SSO. It includes the following sections:

- 「Creating the Business Central client for RH-SSO」
- 「Installing the RH-SSO client adapter for Business Central」
- 「Securing Business Central remote service using RH-SSO」
- 「Securing Business Central file system services using RH-SSO」
- 「Enabling user and group management for RH-SSO」

Prerequisites

- Business Central is installed in a Red Hat JBoss EAP 7.1 server, as described in **Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.1**.
- RH-SSO is installed as described in 2章*Installing and configuring RH-SSO*.
- Business Central users have been added to RH-SSO as described in 3章*Adding Red Hat Process Automation Manager users*.

4.1. CREATING THE BUSINESS CENTRAL CLIENT FOR RH-SSO

After the RH-SSO server starts, open http://localhost:8180/auth/admin in a web browser and log in using the admin credentials that you created while installing RH-SSO. When you login for the first time, you can set up the initial user on the new user registration form.

1. In the RH-SSO Admin Console, click the **Realm Settings** menu item.
2. On the **Realm Settings** page, click **Add Realm**.
   The **Add realm** page opens.
3. On the **Add realm** page, provide a name for the realm and click**Create**.
4. Click the **Clients** menu item and click **Create**.
   The **Add Client** page opens.
5. On the **Add Client** page, provide the required information to create a new client for your realm. For example:
   - **Client ID**: kie
   - **Client protocol**: openid-connect
   - **Root URL**: http://**localhost**:8080/business-central
6. Click **Save** to save your changes.
   After you create a new client, its **Access Type** is set to `public` by default. Change it to `confidential`.

The RH-SSO server is now configured with a realm with a client for Business Central applications and running and listening for HTTP connections at **`localhost:8180`**. This realm provides different users, roles, and sessions for Business Central applications.

4.2. INSTALLING THE RH-SSO CLIENT ADAPTER FOR BUSINESS CENTRAL

After you install RH-SSO, you must install the RH-SSO client adapter for Red Hat JBoss EAP and configure it for Business Central.

Prerequisites

- Business Central is installed in a Red Hat JBoss EAP 7.1 instance, as described in as described in **Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.1**.
- RH-SSO is installed as described in 2章*Installing and configuring RH-SSO*.
- A user with the **`admin`** role has been added to RH-SSO as described in 3章*Adding Red Hat Process Automation Manager users*.

Procedure

1. Navigate to the Software Downloads page in the Red Hat Customer Portal (login required), and select the product and version from the drop-down options:
   - Product: Red Hat Single Sign-On
   - Version: 7.2
2. Download **Red Hat Single Sign-on 7.2.0 Client Adaptor for JBoss EAP 7** (**`rh-sso-7.2.0.GA-eap7-adapter.zip`**).
3. Unzip and install **`rh-sso-7.2.0.GA-eap7-adapter.zip`**. For installation instructions, see the "JBoss EAP Adapter" section of the **Red Hat Single Sign On Securing Applications and Services Guide**.
4. Go to **`EAP_HOME/standalone/configuration`** and open the **`standalone.xml`** and **`standalone-full.xml`** files.
5. Delete the **`<single-sign-on/>`** element from both of the files.
6. Navigate to the **`EAP_HOME/standalone/configuration`** directory in your Red Hat JBoss EAP installation and edit the **`standalone.xml`** and **`standalone-full.xml`** files to add the RH-SSO subsystem configuration. For example:

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
 <secure-deployment name="decision-central.war">
   <realm>demo</realm>
   <realm-public-
key>MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrVrCuTtArbgaZzL1hvh0xtL5m
c7o0NqPVnYXkLvgcwiC3BjLGw1tGEGoJaXDuSaRllobm53JBhjx33UNv+5z/UMG4kytB
WxheNVKnL6GgqlNabMaFfPLPCF8kAgKnsi79NMo+n6KnSY8YeUmec/p2vjO2NjsSAVcW
EQMVhJ31LwIDAQAB</realm-public-key>
   <auth-server-url>http://localhost:8180/auth</auth-server-url>
```

```
    <ssl-required>external</ssl-required>
    <enable-basic-auth>true</enable-basic-auth>
    <resource>kie</resource>
    <credential name="secret">759514d0-dbb1-46ba-b7e7-
ff76e63c6891</credential>
    <principal-attribute>preferred_username</principal-attribute>
 </secure-deployment>
</subsystem>
```

In this example:

- **`secure-deployment name`** is the name of your application's WAR file.
- **`realm`** is the name of the realm that you created for the applications to use.
- **`realm-public-key`** is the public key of the realm you created. You can find the key in the **Keys** tab in the **Realm settings** page of the realm you created in the RH-SSO Admin Console. If you do not provide a value for **`realm-public-key`**, the server retrieves it automatically.
- **`auth-server-url`** is the URL for the RH-SSO authentication server.
- **`enable-basic-auth`** is the setting to enable basic authentication mechanism, so that the clients can use both token-based and basic authentication approaches to perform the requests.
- **`resource`** is the name for the client that you created.
- **`credential name`** is the secret key for the client you created. You can find the key in the **Credentials** tab on the **Clients** page of the RH-SSO Admin Console.
- **`principal-attribute`** is the login name of the user. If you do not provide this value, your User Id is displayed in the application instead of your user name.

注記

The RH-SSO server converts the user names to lower case. Therefore, after integration with RH-SSO, your user name will appear in lower case in Red Hat Process Automation Manager. If you have user names in upper case hard coded in business processes, the application might not be able to identify the upper case user.

7. Navigate to **`EAP_HOME/bin/`** and enter the following command to start the Red Hat JBoss EAP server:

```
./standalone.sh -c standalone-full.xml
```

注記

You can also configure the RH-SSO adapter for Business Central by updating your application's WAR file to use the RH-SSO security subsystem. However, Red Hat recommends that you configure the adapter through the RH-SSO subsystem. Doing this updates the Red Hat JBoss EAP configuration instead of applying the configuration on each WAR file.

4.3. SECURING BUSINESS CENTRAL REMOTE SERVICE USING RH-SSO

Business Central provides different remote service endpoints that can be consumed by third-party clients using a remote API. To authenticate those services through RH-SSO, you must disable the **`BasicAuthSecurityFilter`** parameter.

Procedure

1. Open the Business Central application deployment descriptor file (**`WEB-INF/web.xml`**) and apply the following changes to it:
   - Remove the following lines to remove the servlet filter and its mapping for class **`org.uberfire.ext.security.server.BasicAuthSecurityFilter`**:

```
<filter>
  <filter-name>HTTP Basic Auth Filter</filter-name>
  <filter-
class>org.uberfire.ext.security.server.BasicAuthSecurityFilter</f
ilter-class>
  <init-param>
    <param-name>realmName</param-name>
    <param-value>KIE Workbench Realm</param-value>
  </init-param>
</filter>

<filter-mapping>
  <filter-name>HTTP Basic Auth Filter</filter-name>
  <url-pattern>/rest/*</url-pattern>
  <url-pattern>/maven2/*</url-pattern>
  <url-pattern>/ws/*</url-pattern>
</filter-mapping>
```

   - Add the following lines to add the **`security-constraint`** parameter for the url-patterns that you have removed from the filter mapping:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>remote-services</web-resource-name>
    <url-pattern>/rest/*</url-pattern>
    <url-pattern>/maven2/*</url-pattern>
    <url-pattern>/ws/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>rest-all</role-name>
  </auth-constraint>
</security-constraint>
```

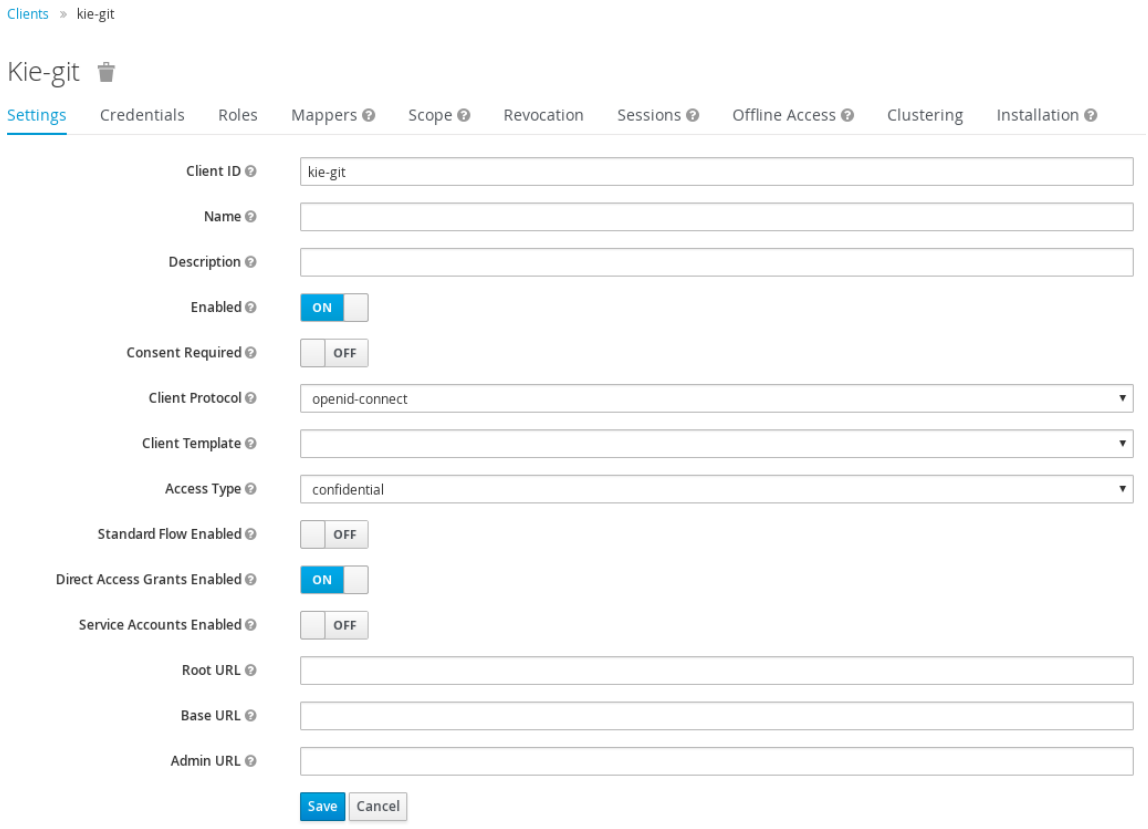
2. Save your changes.

4.4. SECURING BUSINESS CENTRAL FILE SYSTEM SERVICES USING RH-SSO

To consume other remote services such as file systems (for example, a remote GIT service), you must specify the correct RH-SSO login module.

Procedure

1. Generate a JSON configuration file:
   a. Navigate to the **RH-SSO Admin Console** located at http://localhost:8080/auth/admin.
   b. Click **Clients**.
   c. Create a new client with the following settings:
      - Set **Client ID** as **`kie-git`**.
      - Set **Access Type** as **`confidential`**.
      - Disable the **Standard Flow Enabled** option.
      - Enable the **Direct Access Grants Enabled** option.



   d. Click **Save**.
   e. Click the **Installation** tab at the top of the client configuration screen and choose **Keycloak OIDC JSON** as a **Format Option**.
   f. Click **Download**.
2. Move the downloaded JSON file to an accessible directory in the server's file system or add it to the application class path.
3. Specify the correct RH-SSO login module in the **`EAP_HOME/standalone/configuration/standalone.xml`** and **`standalone-full.xml`**

files. By default, the security domain in Red Hat Process Automation Manager is set to **other**. Replace the default values of the **login-module** in this security domain with the values in the following example:

```
<security-domain name="other" cache-type="default">
  <authentication>
    <login-module
code="org.keycloak.adapters.jaas.DirectAccessGrantsLoginModule"
flag="required">
      <module-option name="keycloak-config-file"
value="$EAP_HOME/kie-git.json"/>
    </login-module>
  </authentication>
</security-domain>
```

4. The JSON file specified in the **module-option** element contains a client used for securing the remote services. Replace the **$EAP_HOME/kie-git.json** value of the **module-option** element with the absolute path or the class path (**classpath:/EXAMPLE_PATH/kie-git.json**) to this JSON configuration file.
   At this point, all users authenticated through the RH-SSO server can clone internal GIT repositories. In the following command, change **USER_NAME** to a RH-SSO user, for example **admin**:

```
git clone ssh://USER_NAME@localhost:8001/system
```

4.5. ENABLING USER AND GROUP MANAGEMENT FOR RH-SSO

This section describes how you can configure Business Central to manage users and groups stored in RH-SSO.

Procedure

1. Ensure that the following libraries are in the **WEB-INF/lib** directory:

```
uberfire-security-management-api-<latest_artifact_version>.jar
uberfire-security-management-backend-<latest_artifact_version>.jar
uberfire-security-management-keycloak-<latest_artifact_version>.jar
keycloak-core-<latest_artifact_version>.jar
keycloak-common-<latest_artifact_version>.jar
```

2. Remove third-party security JAR files, for example:

```
uberfire-security-management-wildfly-<latest_artifact_version>.jar
uberfire-security-management-tomcat-<latest_artifact_version>.jar
```

3. Replace the entire contents of the **WEB-INF/classes/security-management.properties** file with the following content:

```
org.uberfire.ext.security.management.api.userManagementServices=KCCr
edentialsUserManagementService
org.uberfire.ext.security.management.keycloak.authServer=http://loca
lhost:8081/auth
org.uberfire.ext.security.management.keycloak.realm=demo
```

```
org.uberfire.ext.security.management.keycloak.user=admin
org.uberfire.ext.security.management.keycloak.password=admin
org.uberfire.ext.security.management.keycloak.clientId=kie
org.uberfire.ext.security.management.keycloak.clientSecret=759514d0-
dbb1-46ba-b7e7-ff76e63c6891
```

注記

If the **WEB-INF/classes/security-management.properties** file does not exist, create it.

4. Edit the following dependencies and exclusions in the **/META-INF/jboss-deployment-structure.xml** file:

```
<dependencies>
    <module name="org.jboss.resteasy.resteasy-jackson-provider"
services="import"/>
</dependencies>
<exclusions>
    <module name="org.jboss.resteasy.resteasy-jackson2-provider"/>
</exclusions>
```

第5章 AUTHENTICATING PROCESS SERVER THROUGH RH-SSO

Process Server provides a REST API for third-party clients. If you integrate Process Server with RH-SSO, you can delegate third-party client identity management to the RH-SSO server.

After you have created a realm client for Red Hat Process Automation Manager and set up the RH-SSO client adapter for Red Hat JBoss EAP, you can set up RH-SSO authentication for Process Server.

Prerequisites

- RH-SSO is installed as described in 2章*Installing and configuring RH-SSO*.
- At lease one user with the **`kie-server`** role has been added to RH-SSO as described in 3章*Adding Red Hat Process Automation Manager users*.
- Process Server is installed in a Red Hat JBoss EAP 7.1 instance, as described in **Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.1**.

This chapter contains the following sections:

- 「Creating the Process Server client on RH-SSO」
- 「Installing and configuring Process Server with the client adapter」
- 「Process Server token-based authentication」

5.1. CREATING THE PROCESS SERVER CLIENT ON RH-SSO

Use the RH-SSO Admin Console to create a Process Server client in an exiting realm.

Prerequisites

- Process Server is installed in a Red Hat JBoss EAP 7.1 server, as described in **Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.1**.
- RH-SSO is installed as described in 2章*Installing and configuring RH-SSO*.
- At lease one user with the **`kie-server`** role has been added to RH-SSO as described in 3章*Adding Red Hat Process Automation Manager users*.

Procedure

1. In the RH-SSO Admin Console, open the security realm that you created in 2章*Installing and configuring RH-SSO*.
2. Click **Clients** and click **Create**.
   The **Add Client** page opens.
3. On the **Add Client** page, provide the required information to create a Process Server client for your realm, then click **Save**. For example:
   - **Client ID**: kie-execution-server
   - **Root URL**: http://**localhost**:8080/kie-server

- **Client protocol**: openid-connect

4. The new client **Access Type** is set to **`public`** by default. Change it to **`confidential`** and click **Save** again.

5. Navigate to the **Credentials** tab and copy the secret key. The secret key is required to configure the **`kie-execution-server`** client.

5.2. INSTALLING AND CONFIGURING PROCESS SERVER WITH THE CLIENT ADAPTER

After you install RH-SSO, you must install the RH-SSO client adapter for Red Hat JBoss EAP and configure it for Process Server.

Prerequisites

- Process Server is installed in a Red Hat JBoss EAP 7.1 server, as described in **Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.1**.
- RH-SSO is installed as described in 2章*Installing and configuring RH-SSO*.
- At lease one user with the **`kie-server`** role has been added to RH-SSO as described in 3章*Adding Red Hat Process Automation Manager users*.

注記

If you deployed Process Server to a different application server than Business Central, install and configure RH-SSO on your second server as well.

Procedure

1. Navigate to the Software Downloads page in the Red Hat Customer Portal (login required), and select the product and version from the drop-down options:
   - Product: Red Hat Single Sign-On
   - Version: 7.2
2. Download **Red Hat Single Sign-on 7.2.0 Client Adaptor for JBoss EAP 7** (**`rh-sso-7.2.0.GA-eap7-adapter.zip`**).
3. Unzip and install **`rh-sso-7.2.0.GA-eap7-adapter.zip`**. For installation instructions, see the "JBoss EAP Adapter" section of the **Red Hat Single Sign On Securing Applications and Services Guide**.
4. Go to **`EAP_HOME/standalone/configuration`** and open the **`standalone.xml`** and **`standalone-full.xml`** files.
5. Delete the **`<single-sign-on/>`** element from both of the files.
6. Navigate to **`EAP_HOME/standalone/configuration`** directory in your Red Hat JBoss EAP installation and edit the **`standalone.xml`** file to add the RH-SSO subsystem configuration. For example:

7. Navigate to **`EAP_HOME/standalone/configuration`** in your Red Hat JBoss EAP installation and edit the **`standalone.xml`** and **`standalone-full.xml`** files to add the RH-SSO subsystem configuration. For example:

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="kie-execution-server.war">
     <realm>demo</realm>
     <realm-public-
key>MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrVrCuTtArbgaZzL1hvh0xtL5m
c7o0NqPVnYXkLvgcwiC3BjLGw1tGEGoJaXDuSaRllobm53JBhjx33UNv+5z/UMG4kytB
WxheNVKnL6GgqlNabMaFfPLPCF8kAgKnsi79NMo+n6KnSY8YeUmec/p2vjO2NjsSAVcW
EQMVhJ31LwIDAQAB</realm-public-key>
     <auth-server-url>http://localhost:8180/auth</auth-server-url>
     <ssl-required>external</ssl-required>
     <resource>kie-execution-server</resource>
     <enable-basic-auth>true</enable-basic-auth>
     <credential name="secret">03c2b267-7f64-4647-8566-
572be673f5fa</credential>
     <principal-attribute>preferred_username</principal-attribute>
  </secure-deployment>
</subsystem>

<system-properties>
  <property name="org.kie.server.sync.deploy" value="false"/>
</system-properties>
```

In this example:

- **`secure-deployment name`** is the name of your application WAR file.
- **`realm`** is the name of the realm that you created for the applications to use.
- **`realm-public-key`** is the public key of the realm you created. You can find the key in the **Keys** tab in the **Realm settings** page of the realm you created in the RH-SSO Admin Console. If you do not provide a value for this public key, the server retrieves it automatically.
- **`auth-server-url`** is the URL for the RH-SSO authentication server.
- **`resource`** is the name for the server client that you created.
- **`enable-basic-auth`** is the setting to enable basic authentication mechanism, so that the clients can use both token-based and basic authentication approaches to perform the requests.
- **`credential name`** is the secret key of the server client you created. You can find the key in the **Credentials** tab on the **Clients** page of the RH-SSO Admin Console.
- **`principal-attribute`** is the login name of the user. If you do not provide this value, your User Id is displayed in the application instead of your user name.

8. Save your configuration changes.
9. Use the following command to restart the Red Hat JBoss EAP server and run Process Server.

```
EXEC_SERVER_HOME/bin/standalone.sh -Dorg.kie.server.id=<ID> -
```

```
Dorg.kie.server.user=<USER> -Dorg.kie.server.pwd=<PWD> -
Dorg.kie.server.location=<LOCATION_URL> -Dorg.kie.server.controller=
<CONTROLLER_URL> -Dorg.kie.server.controller.user=<CONTROLLER_USER>
-Dorg.kie.server.controller.pwd=<CONTOLLER_PASSWORD>
```

For example:

```
EXEC_SERVER_HOME/bin/standalone.sh -Dorg.kie.server.id=kieserver1 -
Dorg.kie.server.user=kieserver -Dorg.kie.server.pwd=password -
Dorg.kie.server.location=http://localhost:8080/kie-execution-
server/services/rest/server -
Dorg.kie.server.controller=http://localhost:8080/decision-
central/rest/controller -
Dorg.kie.server.controller.user=kiecontroller -
Dorg.kie.server.controller.pwd=password
```

10. When Process Server is running, enter the following command to check the server status, where **<KIE_SERVER_USER>** is a user with the **kie-server** role and **<PASSWORD>** is the password for that user:

```
curl http://<KIE_SERVER_USER>:<PASSWORD>@localhost:8080/kie-
execution-server/services/rest/server/
```

5.3. PROCESS SERVER TOKEN-BASED AUTHENTICATION

You can also use token-based authentication for communication between Red Hat Process Automation Manager and Process Server. You can use the complete token as a system property of your application server, instead of the user name and password, for your applications. However, you must ensure that the token will not expire while the applications are interacting because the token is not automatically refreshed. To get the token, see 「Token-based authentication」.

Procedure

1. To configure Business Central to manage Process Server using tokens:
   a. Set the **org.kie.server.token** property.
   b. Make sure that the **org.kie.server.user** and **org.kie.server.pwd** properties are not set.
   Red Hat Process Automation Manager will then use the **Authorization: Bearer $TOKEN** authentication method.
2. To use the REST API using the token-based authentication:
   a. Set the **org.kie.server.controller.token** property.
   b. Make sure that the **org.kie.server.controller.user** and **org.kie.server.controller.pwd** properties are not set.

注記

Because Process Server is unable to refresh the token, use a high-lifespan token. A token's lifespan must not exceed January 19 2038. Check with your security best practices to see whether this is a suitable solution for your environment.

第6章 AUTHENTICATING THIRD-PARTY CLIENTS THROUGH RH-SSO

To use the different remote services provided by Business Central or by Process Server, your client, such as curl, wget, web browser, or a custom REST client, must authenticate through the RH-SSO server and have a valid token to perform the requests. To use the remote services, the authenticated user must have the following roles:

- **`rest-all`** for using Business Central remote services.
- **`kie-server`** for using the Process Server remote services.

Use the RH-SSO Admin Console to create these roles and assign them to the users that will consume the remote services.

Your client can authenticate through RH-SSO using one of these options:

- Basic authentication, if it is supported by the client
- Token-based authentication

6.1. BASIC AUTHENTICATION

If you enabled basic authentication in the RH-SSO client adapter configuration for both Business Central and Process Server, you can avoid the token grant and refresh calls and call the services as shown in the following examples:

- For web based remote repositories endpoint:

```
curl http://admin:password@localhost:8080/decision-
central/rest/repositories
```

- For Process Server:

```
curl http://admin:password@localhost:8080/kie-execution-
server/services/rest/server/
```

6.2. TOKEN-BASED AUTHENTICATION

If you want a more secure option of authentication, you can consume the remote services from both Business Central and Process Server using a granted token provided by RH-SSO.

Procedure

1. In the RH-SSO Admin Console, click the **Clients** menu item and click **Create** to create a new client.
   The **Add Client** page opens.
2. On the **Add Client** page, provide the required information to create a new client for your realm. For example:
   - **Client ID**: kie-remote
   - **Client protocol**: openid-connect

3. Click **Save** to save your changes.
4. Change the token settings in **Realm Settings**:
   a. In the RH-SSO Admin Console, click the **Realm Settings** menu item.
   b. Click the **Tokens** tab.
   c. Change the value for **Access Token Lifespan** to **15** minutes.
      This gives you enough time to get a token and invoke the service before it expires.
   d. Click **Save** to save your changes.
5. After a public client for your remote clients is created, you can now obtain the token by making an HTTP request to the RH-SSO server's token endpoint using:

```
RESULT=`curl --data "grant_type=password&client_id=kie-
remote&username=admin&password=password"
http://localhost:8180/auth/realms/demo/protocol/openid-
connect/token`
```

   The user in this command is an RH-SSO user. For more information, see 3章*Adding Red Hat Process Automation Manager users*.
6. To view the token obtained from the RH-SSO server, use the following command:

```
TOKEN=`echo $RESULT | sed 's/.*access_token":"//g' | sed 's/".*//g'`
```

You can now use this token to authorize the remote calls. For example, if you want to check the internal Red Hat Process Automation Manager repositories, use the token as shown below:

```
curl -H "Authorization: bearer $TOKEN" http://localhost:8080/decision-
central/rest/repositories
```

付録A VERSIONING INFORMATION

Documentation last updated on: Monday, October 1, 2018.