Red Hat Process Automation Manager 7.7

Red Hat Process Automation Manager と Red Hat シングルサインオンの統合

Last Updated: 2020-03-31

Red Hat Process Automation Manager 7.7 Red Hat Process Automation Manager と Red Hat シングルサインオンの統合

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

法律上の通知

概要

本書では、Red Hat シングルサインオン (RH-SSO) と Red Hat Process Automation Manager を統合して、単一のセキュアな認証メソッドを提供する方法を説明します。

目次

前書き

システム管理者は、Red Hat シングルサインオンを Red Hat Process Automation Manager に統合し、単一の認証メソッドを使用することで Red Hat Process Automation Manager ブラウザーアプリケーションを保護できます。

前提条件

- Red Hat Process Automation Manager が Red Hat JBoss EAP 7.2 にインストールされている。詳細は、『**Red Hat JBoss EAP 7.2 への Red Hat Process Automation Manager のインストールおよび設定**』を参照してください。

第1章 統合オプション

Red Hat シングルサインオン (RH-SSO) は、ブラウザーアプリケーションと REST Web サービス、および Git へのアクセスのセキュリティーを確保するために使用できるシングルサインオンソリューションです。

Red Hat Process Automation Manager と RH-SSO を統合する際に、Red Hat Process Automation Manager 向けに SSO と IDM (アイデンティティ管理) を作成します。RH-SSO のセッション管理機能により、一度認証するだけで、Web 上でさまざまな Red Hat Process Automation Manager 環境を使用できます。

以下の章では、 Red Hat Process Automation Manager と RH-SSO を統合する方法を説明します。

- *4章RH-SSO を使用した Business Central の認証*
  RH-SSO サーバーを使用して Red Hat Process Automation Manager を認証するには、Red Hat Process Automation Manager Web クライアント (Business Central) とリモートサービスの両方を RH-SSO で保護する必要があります。この統合により、Business Central またはリモートサービスコンシューマーのいずれかから RH-SSO を介して Red Hat Process Automation Manager に接続できます。

- *5章RH-SSO を使用した KIE Server の認証*
  RH-SSO サーバーを使用して KIE Server を認証するには、KIE Server が提供するリモートサービスのセキュリティーを確保する必要があります。これにより、リモートの Red Hat Process Automation Manager サービスコンシューマー (ユーザーまたはサービス) が RH-SSO 経由で認証できるようになります。KIE Server には Web インターフェースがありません。

- *6章RH-SSO を使用したサードパーティークライアントの認証*
  Business Central または KIE Server が RH-SSO を使用している場合には、サードパーティークライアントは RH-SSO を使用して自己認証する必要があります。認証後は、Business Central および KIE Server が提供するリモートサービスのエンドポイント (REST API、リモートファイルシステムサービスなど) を使用できます。

Red Hat Process Automation Manager を使用して、LDAP の統合をスムーズに行うには、LDAP が含まれる RH-SSO の使用を検討してください。詳細は『Red Hat Single Sign-On Server Administration Guide』の「LDAP and Active Directory」の章を参照してください。

第2章 RH-SSO のインストールおよび設定

レルムは、Web またはアプリケーションサーバーに定義するセキュリティーポリシードメインです。セキュリティーレルムは、異なるアプリケーションリソースのアクセスを制限するのに使用します。レルムは、RH-SSO インスタンスが非公開か、他の製品と共有されているかにかかわらず、新たに作成する必要があります。マスターレルムは、スーパー管理者がお使いのシステム内でレルムを作成して管理する場所として確保できます。他の製品システムと共有している RH-SSO インスタンスと統合して、このようなアプリケーションでシングルサインオンを行うには、全アプリケーションで同じレルムを使用する必要があります。RH-SSO レルムを作成するには、RH-SSO 7.3 をダウンロードしてインストールし、設定します。

注記

Business Central および KIE Server が異なるサーバーにインストールされている場合は、両サーバーでこの手順を行ってください。

手順

1. Red Hat カスタマーポータルの Software Downloads ページに移動し (ログインが必要)、ドロップダウンオプションから製品およびバージョンを選択します。
   - **製品:** Red Hat Single Sign-On
   - **バージョン:** 7.3
2. **Red Hat Single Sign-on 7.3.0 Server**(**rh-sso-7.3.0.zip**) をダウンロードします。
3. 基本的な RH-SSO スタンドアロンサーバーをインストールして設定するには、『Red Hat Single Sign On Getting Started Guide』の「Installing and Booting」の章に記載の手順に従ってください。実稼働環境への高度な設定は『Red Hat Single Sign On Server Administration Guide』を参照してください。

注記

RH-SSO サーバーと Red Hat Process Automation Manager サーバーの両方を同じシステムで実行する場合は、以下のいずれかを行って、ポートが競合しないようにする必要があります。

- 以下のように、**RHSSO_HOME/standalone/configuration/standalone-full.xml** ファイルを更新して、ポートのオフセットを 100 に設定してください。

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

- 環境変数を使用してサーバーを実行する。

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

第3章 RED HAT PROCESS AUTOMATION MANAGER ロールおよびユーザー

Business Central または KIE Server にアクセスするには、サーバーを起動する前にユーザーを作成して適切なロールを割り当てます。本セクションは、利用可能な Red Hat Process Automation Manager ユーザーロールを説明します。

注記

admin、**analyst**、**developer**、**manager**、**process-admin**、**user**、および **rest-all** のロールは Business Central に予約されており、**kie-server** ロールは KIE Server に予約されています。このため、利用可能なロールは、インストールされているシステムが、Business Central、KIE Server、またはその両方かによって異なります。

- **admin**: **admin** ロールを持つユーザーは Business Central 管理者です。管理者は、ユーザーの管理や、リポジトリーの作成、クローン作成、および管理ができます。アプリケーションで必要な変更にすべてアクセスできます。**admin** ロールを持つユーザーは、Red Hat Process Automation Manager の全領域にアクセスできます。

- **analyst**: **analyst** ロールを持つユーザーには、すべてのハイレベル機能へのアクセスがあり、プロジェクトのモデル化および実行が可能です。ただし、このユーザーは、**Design → Projects** ビューでスペースにコントリビューターを追加したり、スペースを削除したりできません。**Deploy → Execution Servers** ビューへのアクセスは管理者を対象にしており、**analyst** ロールを持つユーザーは利用できません。ただし、**Deploy** ボタンは、このユーザーが Library パースペクティブにアクセスする時に利用できます。

- **developer**: **developer** ロールを持つユーザーは、ほぼすべての機能にアクセスができ、ルール、モデル、プロセスフロー、フォーム、およびダッシュボードを管理できます。アセットリポジトリーを管理し、プロジェクトを作成、ビルド、およびデプロイでき、Red Hat CodeReady Studio を使用してプロセスを表示できます。**developer** ロールが割り当てられているユーザーには、新規リポジトリーの作成やクローン作成などの、特定の管理機能は表示されません。

- **manager**: **manager** ロールを持つユーザーはレポートを表示できます。このユーザーは通常、ビジネスプロセス、そのパフォーマンス、ビジネスインジケーター、その他のビジネス関連のレポートに関する統計に関心があります。このルールを持つユーザーがアクセスできるのはプロセスおよびタスクのレポートに限られます。

- **process-admin**: **process-admin** ロールを持つユーザーは、ビジネスプロセス管理者です。ビジネスプロセス、ビジネスタスク、および実行エラーへの完全アクセスがあります。このユーザーは、ビジネスレポートを表示でき、タスク受信箱リストにアクセスできます。

- **user**: **user** ロールが割り当てられたユーザーは、タスクインボックスリストで作業できます。このリストには、現在実行中のプロセスの一部であるビジネスタスクなどが含まれます。このロールが割り当てられたユーザーは、タスクレポートやプロセスの表示、プロセスの管理ができます。

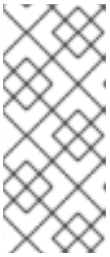
- **rest-all**: **rest-all** ロールを持つユーザーは、Business Central REST 機能にアクセスできます。

- **kie-server**: **kie-server** ロールを持つユーザーは、KIE Server REST 機能へのアクセスがあります。このロールは、Business Central で **Manage** ビューおよび **Track** ビューにアクセスするユーザーにとって必須となります。

3.1. RED HAT PROCESS AUTOMATION MANAGER ユーザーの追加

Business Central または KIE Server の認証に RH-SSO を使用する前に、作成したレルムにユーザーを追加する必要があります。新しいユーザーを追加して、Red Hat Process Automation Manager にアクセスするためのロールを追加するには、以下の手順を行います。

1. RH-SSO 管理コンソールにログインして、ユーザーを追加するレルムを開きます。
2. **Manage** セクションで **Users** メニューアイテムをクリックします。
   Users ページに空のユーザー一覧が表示されます。
3. 空のユーザー一覧で **Add User** ボタンをクリックして、新規ユーザーの作成を開始します。
   Add User ページが開きます。
4. **Add User** ページで、ユーザー情報を入力して **Save** をクリックします。
5. **Credentials** タブをクリックして、パスワードを作成します。
6. 新規ユーザーに、Red Hat Process Automation Manager へのアクセスが可能なロール (Business Central にアクセスできる **admin** ロールや、KIE Server にアクセスできる **kie-server** ロールなど) を 1 つ割り当てます。



注記

Business Central から OpenShift にデプロイするプロジェクトの場合は、ロールを割り当てずに **mavenuser** という RH-SSO ユーザーを作成し、OpenShift テンプレートの **BUSINESS_CENTRAL_MAVEN_USERNAME** および **BUSINESS_CENTRAL_MAVEN_PASSWORD** に、このユーザーを追加します。

7. **Roles** セクションの **Realm Roles** タブで、このロールをレルムロールとして定義します。
8. **Users** ページの **Role Mappings** タブをクリックして、ロールを割り当てます。

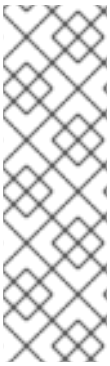
第4章 RH-SSO を使用した BUSINESS CENTRAL の認証

本章では、RH-SSO を介して Business Central を認証する方法を説明します。この章には以下のセクションが含まれます。

- 「RH-SSO への Business Central クライアントの作成」
- 「Business Central への RH-SSO クライアントアダプターのインストール」
- 「RH-SSO を使用した Business Central ファイルシステムサービスのセキュリティー」

前提条件

- 『**Red Hat JBoss EAP 7.2 への Red Hat Process Automation Manager のインストールおよび設定**』の記載通りに、Business Central が Red Hat JBoss EAP 7.2 サーバーにインストールされている。
- 「*2章RH-SSO のインストールおよび設定*」の記載通りに、RH-SSO がインストールされている。
- 「「Red Hat Process Automation Manager ユーザーの追加」 」の記載通りに、Business Central ユーザーが RH-SSO に追加されている。



注記

このセクションは、「RH-SSO への Business Central クライアントの作成」 を除き、スタンドアロンのインストールが対象です。Red Hat OpenShift Container Platform で RH-SSO と Red Hat Process Automation Manager を統合する場合には、「RH-SSO への Business Central クライアントの作成」 の手順のみを実行して、Red Hat OpenShift Container Platform に Red Hat Process Automation Manager 環境をデプロイしてください。Red Hat OpenShift Container Platform への Red Hat Process Automation Manager のデプロイの手順は、Red Hat カスタマーポータル の適切なドキュメントを参照してください。

4.1. RH-SSO への BUSINESS CENTRAL クライアントの作成

RH-SSO サーバーの起動後、RH-SSO 管理コンソールを使用して RH-SSO 向けに Business Central クライアントを作成します。

手順

1. Web ブラウザーに **http://localhost:8180/auth/admin** と入力して、RH-SSO 管理コンソールを開き、RH-SSO のインストール時に作成した管理者の認証情報を使用してログインします。

注記

Red Hat OpenShift Container Platform で RH-SSO を設定している場合には、RH-SSO ルートに公開されている URL を入力します。OpenShift 管理者は、必要に応じてこの URL を提供してください。

初回ログイン時に、新規ユーザー登録で最初のユーザーを設定できます。

2. RH-SSO 管理コンソールで、**Realm Settings** メニューアイテムをクリックします。

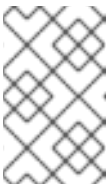
3. **Realm Settings** ページで **Add Realm** をクリックします。
Add realm ページが表示されます。

4. **Add realm** ページで、レルムの名前を指定して **Create** をクリックします。

5. **Clients** メニューアイテムをクリックし、**Create** をクリックします。
Add Client ページが表示されます。

6. **Add Client** ページで、以下のようにレルムにクライアントを新規作成するのに必要な情報を指定します。

   - **Client ID**: kie
   - **Client protocol**: openid-connect
   - Root URL: **http://localhost:8080/business-central**

   注記

   Red Hat OpenShift Container Platform で RH-SSO を設定している場合には、KIE Server ルートに公開されている URL を入力します。OpenShift 管理者は、必要に応じてこの URL を提供してください。

7. **Save** をクリックして変更を保存します。
作成した新規クライアントの **Access Type** は、デフォルトでは **public** に設定されています。この設定を **confidential** に変更します。

   これで、Business Central アプリケーションのクライアントが含まれるレルムに RH-SSO サーバーが設定され、**localhost:8180** で HTTP 接続をリッスンした状態で実行しています。このレルムは、Business Central アプリケーションに異なるユーザー、ロール、セッションを提供します。

4.2. BUSINESS CENTRAL への RH-SSO クライアントアダプターのインストール

RH-SSO をインストールしたら、Red Hat JBoss EAP に RH-SSO クライアントアダプターをインストールして、Business Central に対して設定する必要があります。

前提条件

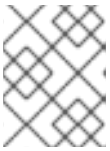
- 『Red Hat JBoss EAP 7.2 への Red Hat Process Automation Manager のインストールおよび設定』の記載通りに、Business Central が Red Hat JBoss EAP 7.2 インスタンスにインストールされている。
- 「*2章RH-SSO のインストールおよび設定*」の記載通りに、RH-SSO がインストールされている。
- 「「Red Hat Process Automation Manager ユーザーの追加」」の記載通りに、**admin** ロールが割り当てられたユーザーが RH-SSO に追加されている。

手順

1. Red Hat カスタマーポータルの Software Downloads ページに移動し (ログインが必要)、ドロップダウンオプションから製品およびバージョンを選択します。

- **製品:** Red Hat Single Sign-On
- **バージョン:** 7.3

2. **Red Hat Single Sign-on 7.3. Client Adaptor for JBoss EAP 7**(**rh-sso-7.3-eap7-adapter.zip**) をダウンロードします。
3. **rh-sso-7.3-eap7-adapter.zip** を展開してインストールします。インストール手順は『Red Hat Single Sign On Securing Applications and Services Guide』の「JBoss EAP Adapter」セクションを参照してください。



注記

-Dserver.config=standalone-full.xml プロパティーでアダプターをインストールします。

4. **EAP_HOME/standalone/configuration** に移動して、**standalone-full.xml** ファイルを開きます。
5. 両方のファイルから、**<single-sign-on/>** 要素を削除します。
6. Red Hat JBoss EAP インストールの **EAP_HOME/standalone/configuration** ディレクトリーに移動し、テキストエディターで **standalone-full.xml** ファイルを開きます。
7. 以下の例に表示されているシステムプロパティーを **<system-properties>;** に追加します。

```
<system-properties>
  <property name="org.jbpm.workbench.kie_server.keycloak" value="true"/>
  <property name="org.uberfire.ext.security.management.api.userManagementServices"
value="KCAdapterUserManagementService"/>
  <property name="org.uberfire.ext.security.management.keycloak.authServer"
value="http://localhost:8180/auth"/>
</system-properties>
```

8. 以下のように、RH-SSO サブシステム設定を追加します。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
 <secure-deployment name="business-central.war">
   <realm>demo</realm>
   <realm-public-
key>MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrVrCuTtArbgaZzL1hvh0xtL5mc
7o0NqPVnYXkLvgcwiC3BjLGw1tGEGoJaXDuSaRllobm53JBhjx33UNv+5z/UMG4kytBWxheNV
KnL6GgqlNabMaFfPLPCF8kAgKnsi79NMo+n6KnSY8YeUmec/p2vjO2NjsSAVcWEQMVhJ31L
wIDAQAB</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>
```

この例で、

- **secure-deployment name** は、アプリケーションの WAR ファイルの名前です。
- **realm** は、使用するアプリケーション用に作成したレルムの名前です。
- **realm-public-key** は、作成したレルムの公開鍵です。この鍵は、RH-SSO 管理コンソールで作成したレルムの **Realm settings** ページの **Keys** タブで確認できます。**realm-public-key** の値を指定しない場合は、サーバーが自動的に取得します。
- **auth-server-url** は、RH-SSO 認証サーバーの URL です。
- **enable-basic-auth** は、クライアントがトークンベースと Basic 認証アプローチの両方を使用して要求を実行できるように、Basic 認証メカニズムを有効にする設定です。
- **resource** は、作成したクライアントの名前です。
- **credential name** は、作成したクライアントの秘密鍵です。この鍵は、RH-SSO 管理コンソールの **Clients** ページの **Credentials** タブで確認できます。
- **principal-attribute** は、ユーザーのログイン名です。この値を指定しないと、ユーザー名ではなくユーザー ID がアプリケーションに表示されます。

注記

RH-SSO サーバーは、ユーザー名を小文字に変換します。したがって、RH-SSO と統合すると、ユーザー名が Red Hat Process Automation Manager では小文字で表示されます。ユーザー名が、ビジネスプロセスに大文字でハードコードされている場合は、アプリケーションが大文字のユーザー名を識別できない場合があります。

9. Elytron サブシステムには、JACC 仕様に基づいた組み込みポリシープロバイダーがあります。**standalone.xml** または、Elytron がインストールされているファイルで手動で JACC を有効にするには、以下のタスクのいずれかを実行します。

   - ポリシープロバイダーを作成するには、 Red Hat JBoss EAP の管理コマンドラインインターフェース (CLI) で以下のコマンドを入力します。

     ```
     /subsystem=elytron/policy=jacc:add(jacc-policy={})
     /subsystem=undertow/application-security-domain=other:remove
     /subsystem=undertow/application-security-domain=other:add(http-authentication-factory=keycloak-http-authentication,enable-jacc=true)
     ```

     Red Hat JBoss EAP の管理 CLI に関する詳細は、『管理 CLI ガイド』を参照してください。

   - Red Hat JBoss EAP インストールの **EAP_HOME/standalone/configuration** ディレクトリーに移動し、**standalone.xml** ファイルおよび **standalone-full.xml** ファイルで Elytron と undertow サブシステム設定の場所を特定して JACC を有効化します。以下に例を示します。

     ```
     <subsystem xmlns="urn:wildfly:elytron:4.0" ...>
     ......
      <policy name="jacc"><jacc-policy/></policy>
     </subsystem>
     ```

     ```
     <subsystem xmlns="urn:jboss:domain:undertow:7.0" ...>
     ```

```
.....
 <application-security-domains>
   <application-security-domain name="other" http-authentication-factory="keycloak-http-
authentication" enable-jacc="true"/>
 </application-security-domains>
</subsystem>
```

10. **EAP_HOME/bin/** に移動し、以下のコマンドを実行して Red Hat JBoss EAP サーバーを起動します。

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

注記

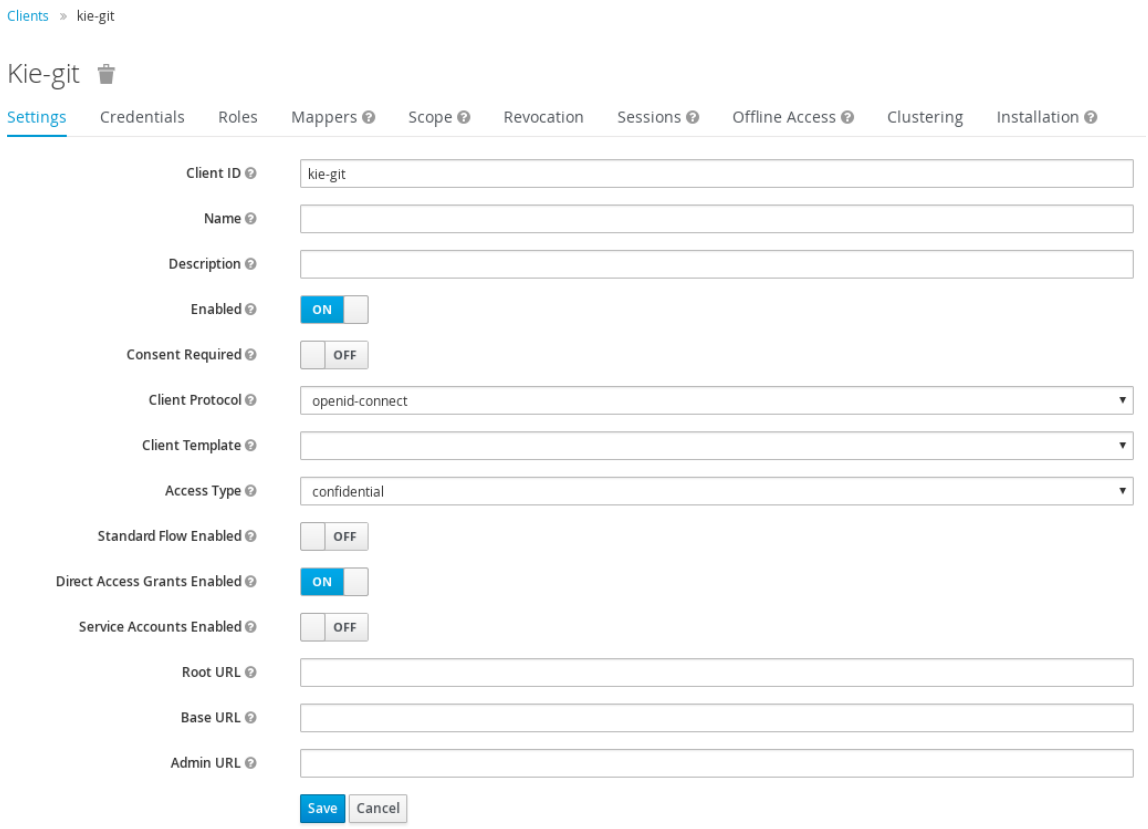
RH-SSO セキュリティーサブシステムを使用するようにアプリケーションの WAR ファイルを更新して、Business Central の RH-SSO アダプターを設定することもできます。ただし Red Hat では、RH-SSO サブシステムからアダプターを設定することを推奨します。つまり、設定を各 WAR ファイルに適用するのではなく、Red Hat JBoss EAP の設定を更新します。

4.3. RH-SSO を使用した BUSINESS CENTRAL ファイルシステムサービスのセキュリティー

ファイルシステムなど、他のリモートサービス (例: リモート GIT サービス) を使用するには、正しい RH-SSO ログインモジュールを指定する必要があります。

手順

1. JSON 設定ファイルを生成します。
   a. http://localhost:8180/auth/admin から **RH-SSO 管理コンソール** に移動します。
   b. **Clients** をクリックします。
   c. 以下の設定で新規クライアントを作成します。
      - **Client ID** は **kie-git** に設定します。
      - **Access Type** は **confidential** に設定します。
      - **Standard Flow Enabled** オプションを無効にします。
      - **Direct Access Grants Enabled** オプションを有効にします。



d. **保存** をクリックします。

e. クライアント設定画面の上部にある **Installation** タブをクリックして、**Format Option** に **Keycloak OIDC JSON** を選択します。

f. **Download** をクリックします。

2. ダウンロードした JSON ファイルを、サーバーのファイルシステム内でアクセス可能なディレクトリーに移動するか、アプリケーションクラスパスに追加します。

3. **EAP_HOME/standalone/configuration/standalone-full.xml** ファイルに、正しい RH-SSO ログインモジュールを指定します。デフォルトでは、Red Hat Process Automation Manager のセキュリティードメインは **other** に設定されます。このセキュリティードメインの **login-module** のデフォルト値を、以下の例で示す値に置き換えます。

```
<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. **module-option** 要素で指定した JSON ファイルには、リモートサービスのセキュリティーを確保するために使用するクライアントが含まれます。**module-option** 要素の **$EAP_HOME/kie-git.json** の値を、この JSON 設定ファイルの絶対パスまたはクラスパス (**classpath:/EXAMPLE_PATH/kie-git.json**) に置き換えます。
これで、RH-SSO サーバーで認証されたすべてのユーザーは、内部 GIT リポジトリーのクローンを作成できます。以下のコマンドで、**USER_NAME** を RH-SSO ユーザー (**admin** など) に変更します。

■

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

第5章 RH-SSO を使用した KIE SERVER の認証

KIE Server は、サードパーティークライアントの REST API を提供します。KIE Server と RH-SSO を統合した場合は、サードパーティークライアントのアイデンティティー管理を RH-SSO サーバーに委譲できます。

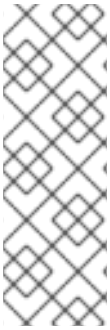
Red Hat Process Automation Manager のレルムクライアントを作成して、Red Hat JBoss EAP に RH-SSO クライアントアダプターを設定したら、KIE Server に RH-SSO 認証を設定できます。

前提条件

- 「2章*RH-SSO のインストールおよび設定*」の記載通りに、RH-SSO がインストールされている。
- 「Red Hat Process Automation Manager ユーザーの追加」 の記載通りに、**kie-server** ロールが割り当てられたユーザーが 1 つ以上 RH-SSO に追加されている。
- 『**Red Hat JBoss EAP 7.2 への Red Hat Process Automation Manager のインストールおよび設定**』の記載通りに、KIE Server が Red Hat JBoss EAP 7.2 インスタンスにインストールされている。

本章は以下のセクションで構成されます。

- 「RH-SSO で KIE Server クライアントの作成」
- 「クライアントアダプターを使用する KIE Server のインストールおよび設定」
- 「KIE Server のトークンベースの認証」



注記

このセクションは、「RH-SSO で KIE Server クライアントの作成」 を除き、スタンドアロンのインストールが対象です。Red Hat OpenShift Container Platform で RH-SSO と Red Hat Process Automation Manager を統合する場合には、「RH-SSO で KIE Server クライアントの作成」 の手順のみを実行して、Red Hat OpenShift Container Platform に Red Hat Process Automation Manager 環境をデプロイしてください。Red Hat OpenShift Container Platform への Red Hat Process Automation Manager のデプロイの手順は、Red Hat カスタマーポータル の適切なドキュメントを参照してください。

5.1. RH-SSO で KIE SERVER クライアントの作成

RH-SSO 管理コンソールを使用して、既存のレルムに KIE Server クライアントを作成します。

前提条件

- 『**Red Hat JBoss EAP 7.2 への Red Hat Process Automation Manager のインストールおよび設定**』の記載通りに、KIE Server が Red Hat JBoss EAP 7.2 サーバーにインストールされている。
- 「2章*RH-SSO のインストールおよび設定*」の記載通りに、RH-SSO がインストールされている。
- 「Red Hat Process Automation Manager ユーザーの追加」 の記載通りに、**kie-server** ロールが割り当てられたユーザーが 1 つ以上 RH-SSO に追加されている。

手順

1. RH-SSO 管理コンソールで、「2章*RH-SSO のインストールおよび設定*」で作成したセキュリティーレルムを開きます。
2. **Clients** をクリックし、**Create** をクリックします。
   Add Client ページが表示されます。
3. **Add Client** ページで、レルムに KIE Server クライアントを作成するのに必要な情報を入力し、**Save** をクリックします。以下は例になります。
   - **クライアント ID**: **kie-execution-server**
   - Root URL: **http://localhost:8080/kie-server**
   - **クライアントのプロトコル**: **openid-connect**

注記

Red Hat OpenShift Container Platform で RH-SSO を設定している場合には、KIE Server ルートに公開されている URL を入力します。OpenShift 管理者は、必要に応じてこの URL を提供してください。

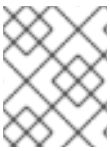
4. 新規クライアントの **Access Type** は、デフォルトでは **public** に設定されています。この設定を **confidential** に変更して、もう一度 **Save** をクリックします。
5. **Credentials** タブに移動して秘密鍵をコピーします。秘密鍵は、**kie-execution-server** クライアントを設定するのに必要になります。

5.2. クライアントアダプターを使用する KIE SERVER のインストールおよび設定

RH-SSO をインストールしたら、Red Hat JBoss EAP に RH-SSO クライアントアダプターをインストールして、KIE Server に対して設定する必要があります。

前提条件

- 『**Red Hat JBoss EAP 7.2 への Red Hat Process Automation Manager のインストールおよび設定**』の記載通りに、KIE Server が Red Hat JBoss EAP 7.2 サーバーにインストールされている。
- 「2章*RH-SSO のインストールおよび設定*」の記載通りに、RH-SSO がインストールされている。
- 「Red Hat Process Automation Manager ユーザーの追加」 の記載通りに、**kie-server** ロールが割り当てられたユーザーが 1 つ以上 RH-SSO に追加されている。



注記

KIE Server を Business Central 以外のアプリケーションにデプロイする場合には、2 番目のサーバーに RH-SSO をインストールして設定します。

手順

1. Red Hat カスタマーポータルの Software Downloads ページに移動し (ログインが必要)、ドロップダウンオプションから製品およびバージョンを選択します。
   - **製品:** Red Hat Single Sign-On
   - **バージョン:** 7.3
2. **Red Hat Single Sign-on 7.3.0 Client Adaptor for JBoss EAP 7**(**rh-sso-7.3.0-eap7-adapter.zip**) をダウンロードします。
3. **rh-sso-7.3.0-eap7-adapter.zip** を展開してインストールします。インストール手順は『Red Hat Single Sign On Securing Applications and Services Guide』の「JBoss EAP Adapter」セクションを参照してください。
4. **EAP_HOME/standalone/configuration** に移動して、**standalone-full.xml** ファイルを開きます。
5. 両方のファイルから、**<single-sign-on/>** 要素を削除します。
6. Red Hat JBoss EAP システムの **EAP_HOME/standalone/configuration** ディレクトリーに移動し、**standalone-full.xml** ファイルを編集して RH-SSO サブシステム設定を追加します。以下は例になります。
7. Red Hat JBoss EAP システムの **EAP_HOME/standalone/configuration** に移動し、**standalone-full.xml** ファイルを編集して RH-SSO サブシステム設定を追加します。以下に例を示します。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="kie-execution-server.war">
    <realm>demo</realm>
    <realm-public-
key>MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrVrCuTtArbgaZzL1hvh0xtL5mc
7o0NqPVnYXkLvgcwiC3BjLGw1tGEGoJaXDuSaRllobm53JBhjx33UNv+5z/UMG4kytBWxheNV
KnL6GgqlNabMaFfPLPCF8kAgKnsi79NMo+n6KnSY8YeUmec/p2vjO2NjsSAVcWEQMVhJ31L
wIDAQAB</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>
```

この例で、

- **secure-deployment name** は、アプリケーションの WAR ファイルの名前です。
- **realm** は、使用するアプリケーション用に作成したレルムの名前です。
- **realm-public-key** は、作成したレルムの公開鍵です。この鍵は、RH-SSO 管理コンソールで作成したレルムの **Realm settings** ページの **Keys** タブで確認できます。この公開鍵の値を指定しない場合は、サーバーが自動的に取得します。

- **auth-server-url** は、RH-SSO 認証サーバーの URL です。
- **resource** は、作成したサーバークライアントの名前です。
- **enable-basic-auth** は、クライアントがトークンベースと Basic 認証アプローチの両方を使用して要求を実行できるように、Basic 認証メカニズムを有効にする設定です。
- **credential name** は、作成したサーバークライアントの秘密鍵です。この鍵は、RH-SSO 管理コンソールの **Clients** ページの **Credentials** タブで確認できます。
- **principal-attribute** は、ユーザーのログイン名です。この値を指定しないと、ユーザー名ではなくユーザー ID がアプリケーションに表示されます。

8. 設定変更を保存します。
9. 以下のコマンドを使用し、Red Hat JBoss EAP サーバーを再起動して KIE Server を実行します。

```
EXEC_SERVER_HOME/bin/standalone.sh -c standalone-full.xml -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>
```

以下は例になります。

```
EXEC_SERVER_HOME/bin/standalone.sh -c standalone-full.xml -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/business-central/rest/controller -Dorg.kie.server.controller.user=kiecontroller -Dorg.kie.server.controller.pwd=password
```

10. KIE Server の実行中に、以下のコマンドを実行してサーバーの状態を確認します。**<KIE_SERVER_USER>** は **kie-server** ロールが割り当てられているユーザー名で、そのパスワードは **<PASSWORD>** です。

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

5.3. KIE SERVER のトークンベースの認証

Red Hat Process Automation Manager と KIE Server 間の通信に、トークンベースの認証を使用することもできます。アプリケーションにおいて、ユーザー名とパスワードの代わりに、完全なトークンをアプリケーションサーバーのシステムプロパティーとして使用できます。ただし、トークンは自動的に更新されないため、アプリケーションの通信が行われている間にトークンが失効しないようにする必要があります。トークンを取得する方法は「トークンベースの認証」を参照してください。

手順

1. トークンを使用して KIE Server を管理するように Business Central を設定するには、以下を実行します。
   a. **org.kie.server.token** プロパティーを設定します。

b. **org.kie.server.user** プロパティーと **org.kie.server.pwd** プロパティーは設定しないでください。
これで、Red Hat Process Automation Manager は **Authorization: Bearer $TOKEN** 認証メソッドを使用します。

2. トークンベースの認証を使用して REST API を使用する場合は、以下を行います。

a. **org.kie.server.controller.token** プロパティーを設定します。

b. **org.kie.server.controller.user** プロパティーおよび **org.kie.server.controller.pwd** プロパティーは設定しないでください。

注記

KIE Server はトークンを更新できないので、有効期限の長いトークンを使用してください。また、トークンの有効期限は、2038 年 1 月 19 日以降にならないようにしてください。セキュリティーのベストプラクティスをチェックし、お使いの環境に適したソリューションかどうかを確認してください。

第6章 RH-SSO を使用したサードパーティークライアントの認証

Business Central または KIE Server が提供するさまざまなリモートサービスを使用するには、curl、wget、Web ブラウザー、カスタムの REST クライアントなどのクライアントが、RH-SSO サーバー経由で認証を受け、要求を実行するために有効なトークンを取得する必要があります。リモートのサービスを使用するには、認証済みのユーザーに以下のロールを割り当てる必要があります。

- **rest-all** Business Central リモートサービスを使用する場合
- **kie-server**: KIE Server のリモートサービスを使用する場合

RH-SSO 管理コンソールを使用してこれらのロールを作成し、リモートサービスを使用するユーザーに割り当てます。

クライアントは、以下のオプションのいずれかを使用して RH-SSO 経由で認証できます。

- クライアントでサポートされている場合は Basic 認証
- トークンベースの認証

6.1. BASIC 認証

Business Central および KIE Server の両方に対して RH-SSO クライアントアダプターの設定で Basic 認証を有効にした場合には、以下の例のようにトークンの付与/更新の呼び出しをせずにサービスを呼び出すことができます。

- Web ベースのリモートリポジトリーエンドポイントの場合:

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

- KIE Server の場合

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

6.2. トークンベースの認証

よりセキュアな認証オプションを希望される場合には、RH-SSO から付与されたトークンを使用すると、Business Central および KIE Server の両方からリモートサービスを使用できます。

手順

1. RH-SSO 管理コンソールで **Clients** メニューアイテムをクリックし、**Create** をクリックして新規クライアントを作成します。
   Add Client ページが表示されます。
2. **Add Client** ページで、以下のようにレルムにクライアントを新規作成するのに必要な情報を指定します。
   - **Client ID**: kie-remote
   - **Client protocol**: openid-connect
3. **Save** をクリックして変更を保存します。

4. **Realm Settings** でトークンの設定を変更します。
   a. RH-SSO 管理コンソールで、**Realm Settings** メニューアイテムをクリックします。
   b. **Tokens** タブをクリックします。
   c. **Access Token Lifespan** の値を **15** 分に変更します。
   このように設定すると、トークンを取得してから失効するまでに余裕をもってサービスを呼び出すことができます。
   d. **Save** をクリックして変更を保存します。
5. リモートクライアントの公開クライアントを作成したら、以下のコマンドを使用して、RH-SSO サーバーのトークンエンドポイントに対して HTTP 要求を行ってトークンを取得できます。

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

   このコマンドのユーザーは Business Central RH-SSO ユーザーです。詳細は「Red Hat Process Automation Manager ユーザーの追加」を参照してください。

6. RH-SSO サーバーから取得したトークンを表示するには、以下のコマンドを使用します。

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

このトークンを使用してリモートの呼び出しを認証できるようになります。たとえば、Red Hat Process Automation Manager の内部リポジトリーを確認するには、以下のようにトークンを使用します。

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

付録A バージョン情報

本ドキュメントの最終更新日: 2020 年 3 月 18 日 (水)