Red Hat Decision Manager 7.4

Red Hat Decision Manager と Red Hat Single Sign-On の統合

ガイド

Last Updated: 2023-03-08

Red Hat Decision Manager 7.4 Red Hat Decision Manager と Red Hat Single Sign-On の統合

ガイド

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

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 Decision Manager を統合して、セキュアな認証メソッドを一元化して提供する方法を説明します。

目次

はじめに

システム管理者は、Red Hat シングルサインオンを Red Hat Decision Manager に統合し、単一の認証メソッドを使用することで Red Hat Decision 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 JBoss EAP 7.2 に Red Hat Decision Manager がインストールされていること。詳細は、**Red Hat JBoss EAP 7.2 への Red Hat Decision 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 Decision Manager と RH-SSO を統合する際に、Red Hat Decision 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 Decision Manager 環境を使用できます。

以下の章では、 Red Hat Decision 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 Decision Manager を認証するには、Red Hat Decision 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 Decision Manager に接続できます。

- ***5章RH-SSO を使用した Decision Server の認証***
  RH-SSO サーバーを使用して Decision Server を認証するには、Decision Server が提供するリモートサービスを保護する必要があります。これを行うことで、リモートの Red Hat Decision Manager サービスコンシューマー (ユーザーまたはサービス) を有効にし、RH-SSO を経由して認証します。Decision Server には Web インターフェイスがありません。

- ***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 Decision Server が RH-SSO を使用している場合、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 Decision 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 Decision Manager との LDAP 統合を容易にするには、LDAP での RH-SSO を使用することを検討してください。詳細は **Red Hat Single Sign-On Server 管理ガイド**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

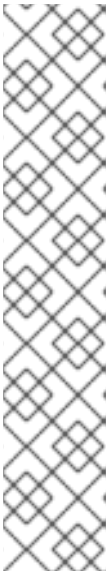
レルムは、Web またはアプリケーションサーバーに定義するセキュリティーポリシードメインです。セキュリティーレルムは、異なるアプリケーションリソースのアクセスを制限するのに使用します。RH-SSO インスタンスが非公開か他の製品と共有されているかにかかわらず、新規レルムを作成する必要があります。マスターレルムを、スーパー管理者がシステムのレルムを作成して管理する場所として維持できます。他の製品システムと共有している RH-SSO インスタンスと統合して、これらのアプリケーションでシングルサインオンを行うためには、これらのアプリケーションですべて同じレルムが使用される必要があります。RH-SSO 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 Decision 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
   - **Version:** 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 スタートガイド** のインストールおよび起動の章に記載される手順に従ってください。実稼働環境の高度な設定については、**Red Hat Single Sign On サーバー管理ガイド**を参照してください。



注記

同じシステムで RH-SSO と Red Hat Decision Manager サーバーの両方を実行する場合には、以下の手段のいずれかによりポートの競合を避けてください。

- **RHSSO_HOME/standalone/configuration/standalone.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。以下に例を示します。

```
<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
```

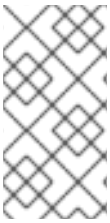
第3章 RED HAT DECISION MANAGER ロールおよびユーザー

Business Central または Decision 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。

Business Central と Decision Server は、JAVA 認証承認サービス (JAAS) ログインモジュールを使用してユーザーを認証します。Business Central と Decision Server の両方が単一のインスタンスで実行されている場合は、同じ JAAS サブジェクトとセキュリティードメインを共有します。したがって、Business Central に対して認証されたユーザーは、Decision Server にもアクセスできます。

ただし、Business Central と Decision Server が異なるインスタンスで実行されている場合、JAAS ログインモジュールは両方に対して個別にトリガーされます。したがって、Business Central で認証されたユーザーは、Decision Server にアクセス (Business Central でプロセス定義を表示または管理など) するための個別認証が必要となります。ユーザーが Decision Server で認証されていない場合は、ログファイルに 401 エラーが記録され、Business Central に **Invalid credentials to load data from remote server.Contact your system administrator.** メッセージが表示されます。

本セクションでは、利用可能な Red Hat Decision Manager のユーザーロールを説明します。



注記

admin、**analyst**、および **rest-all** のロールは Business Central 用に予約されています。**kie-server** ロールは Decision Server 用に予約されています。このため、Business Central または Decision Server のいずれか、またはそれら両方がインストールされているかどうかによって、利用可能なロールは異なります。

- **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をすべて利用できます。**admin** ロールを持つユーザーは、Red Hat Decision 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ます。プロジェクトのモデル化が可能です。ただし、このユーザーは、**Design → Projects** ビューでスペースに貢献者を追加したり、スペースを削除したりできません。**analyst** ロールを持つユーザーは、管理者向けの **Deploy → Execution Servers** ビューにアクセスできません。ただし、これらのユーザーは、ライブラリーパースペクティブにアクセスするときに **Deploy** ボタンを使用できます。

- **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 Decision Server (KIE サーバー) 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必要になります。

3.1. RED HAT DECISION MANAGER ユーザーの追加

Business Central または Decision 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 Decision 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. Red Hat Decision Manager へのアクセスを許可するロールの新規ユーザーを割り当てます。たとえば、Business Central にアクセスするには **admin** ロールを割り当てるか、Decision Server にアクセスするには **kie-server** ロールを割り当てます。

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 リモートサービスのセキュリティー」
- 「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」
- 「RH-SSO のユーザーおよびグループの管理の有効化」

前提条件

- **Red Hat JBoss EAP 7.2 への Red Hat Decision 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 Decision 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

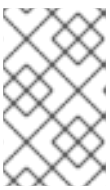
このセクションは、「RH-SSO への Business Central クライアントの作成」 を除き、スタンドアロンのインストールが対象です。Red Hat OpenShift Container Platform で RH-SSO と Red Hat Decision Manager を統合する場合には、「RH-SSO への Business Central クライアントの作成」 の手順のみを実行して、Red Hat OpenShift Container Platform に Red Hat Decision Manager 環境をデプロイしてください。Red Hat OpenShift Container Platform に Red Hat Decision Manager をデプロイする手順は、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。

初回のログイン時に、新規ユーザー登録フォームで初期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。

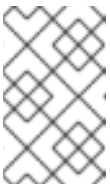
3. **Realm Settings** ページで **Add Realm** をクリックします。
Add realm ページが表示されます。

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、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。以下に例を示します。

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

   注記

   Red Hat OpenShift Container Platform で RH-SSO を設定している場合には、Decision 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 Decision 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 Decision 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

- **Version:** 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 アプリケーションおよびサービスのセキュリティー保護ガイド** 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.xml** ファイルおよび **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、**standalone.xml** ファイルおよび **standalone-full.xml** ファイルを編集して、RH-SSO サブシステムの設定を追加します。以下に例を示します。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
 <secure-deployment name="decision-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 認証の両方のアプローチ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、アプリケーションに、ユーザー名ではなくユーザー ID が表示されます。

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、Red Hat Decision Manager ではユーザー名が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。

7. **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 リモートサービスのセキュリティー

Business Central は、リモート API を使用してサードパーティークライアントが使用可能なリモートサービスエンドポイントを各種提供します。

手順

1. Business Central アプリケーションデプロイメント記述子ファイル (**WEB-INF/web.xml**) を開き、以下の変更を適用します。
   - 以下の行を追加して、url-patterns の **security-constraint** パラメーターを追加します。

```
<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>
    <role-name>rest-project</role-name>
    <role-name>rest-deployment</role-name>
    <role-name>rest-process</role-name>
    <role-name>rest-process-read-only</role-name>
    <role-name>rest-task</role-name>
    <role-name>rest-task-read-only</role-name>
    <role-name>rest-query</role-name>
    <role-name>rest-client</role-name>
  </auth-constraint>
</security-constraint>
```

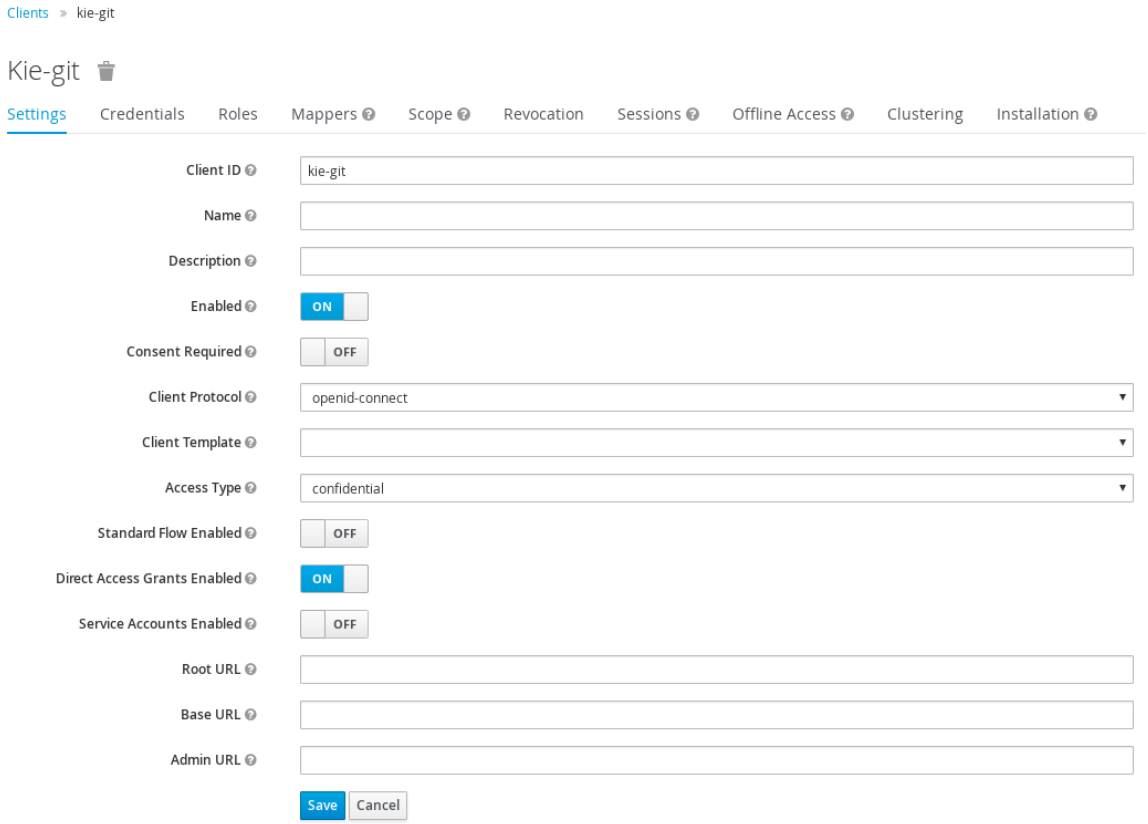
2. 変更を保存します。

4.4. 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. **RH-SSO 管理コンソール** (http://localhost:8180/auth/admin) 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. **Save** 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.xml** ファイルおよび **standalone-full.xml** ファイルに、正しい RH-SSO ログインを指定します。デフォルトでは、Red Hat Decision 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
```

4.5. RH-SSO のユーザーおよびグループの管理の有効化

本セクションでは、Business Central を設定して、RH-SSO に保存されたユーザーおよびグループを管理する方法を説明します。

手順

1. 以下のライブラリーが **WEB-INF/lib** ディレクトリーにあることを確認します。

```
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. サードパーティーセキュリティーの JAR ファイルを削除します。以下は例になります。

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

3. **WEB-INF/classes/security-management.properties** ファイルの内容を、以下の内容に置き換えます。

```
org.uberfire.ext.security.management.api.userManagementServices=KCAdapterUserManagem
entService
org.uberfire.ext.security.management.keycloak.authServer=http://localhost:8180/auth
```

注記

WEB-INF/classes/security-management.properties ファイルが存在しない場合は、そのファイルを作成します。

4. **/META-INF/jboss-deployment-structure.xml** ファイルで、以下の依存関係および除外を編集します。

```
<dependencies>
    <module name="org.jboss.resteasy.resteasy-jackson-provider" services="import"/>
</dependencies>
<exclusions>
    <module name="org.jboss.resteasy.resteasy-jackson2-provider"/>
    <module name="com.fasterxml.jackson.datatype.jackson-datatype-jsr310"/>
</exclusions>
```

第5章 RH-SSO を使用した DECISION SERVER の認証

Decision 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。Decision 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 Decision 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、Decision 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 Decision 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ているユーザーが 1 人以上 RH-SSO に追加されている。
- **Red Hat JBoss EAP 7.2 への Red Hat Decision Manager のインストールおよび設定**の記載通りに、Decision 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設定されます。

- 「RH-SSO で Decision 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 Decision Server のインストールおよび設定」
- 「Decision 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 Decision 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 Decision Manager を統合する場合には、「RH-SSO で Decision Server クライアントの作成」 の手順を実行して、Red Hat OpenShift Container Platform に Red Hat Decision Manager 環境をデプロイしてください。Red Hat OpenShift Container Platform に Red Hat Decision Manager をデプロイする手順は、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 DECISION 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 Decision 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 Decision Manager のインストールおよび設定**の記載通りに、Decision 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 Decision 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ているユーザーが 1 人以上 RH-SSO に追加されている。

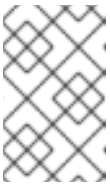
手順

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 Decision 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。以下に例を示します。

   - **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、Decision 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 DECISION 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、Decision 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 Decision Manager のインストールおよび設定**の記載通りに、Decision 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 Decision 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ているユーザーが 1 人以上 RH-SSO に追加されている。

注記

Decision 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
   - **Version:** 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 アプリケーションおよびサービスのセキュリティー保護ガイド 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.xml** ファイルおよび **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.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。

7. Red Hat JBoss EAP システムの **EAP_HOME/standalone/configuration** に移動し、**standalone.xml** ファイルおよび **standalone-full.xml** ファイルを編集して、RH-SSO サブシステムの設定を追加します。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 認証の両方のアプローチ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、アプリケーションに、ユーザー名ではなくユーザー ID が表示されます。

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 Decision Server を実行します。

```
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>
```

以下に例を示します。

```
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. Decision 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. DECISION SERVER のトークンベースの認証

Red Hat Decision Manager と Decision 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 Decision 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 Decision 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

Decision Server はトークンを更新できないので、寿命が長いトークンを使用してください。トークンの有効期限は、2038 年 1 月 19 日以降には設定しないでください。セキュリティーのベストプラクティスで、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 Decision 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**: Decision 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 Decision 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/decision-central/rest/repositories
```

- Decision 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 Decision 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、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。以下に例を示します。
   - **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。
   これにより、有効期限が切れる前にトークンを取得してサービスを呼び出すための十分な時間が得られます。

   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 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 Decision 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 Decision 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/decision-central/rest/repositories
```

付録A バージョン情報

本書の最終更新日: 2021 年 11 月 15 日 (月)