



# Red Hat Decision Manager 7.2

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

ガイド



# Red Hat Decision Manager 7.2 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

Copyright © 2023 | You need to change the HOLDER entity in the en-US/Integrating\_Red\_Hat\_Decision\_Manager\_with\_Red\_Hat\_Single\_Sign-On.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 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 .....	3
第1章 統合オプション .....	4
第2章 RH-SSO のインストールおよび設定 .....	5
第3章 RED HAT DECISION MANAGER ユーザーの追加 .....	6
第4章 RH-SSO を使用した DECISION CENTRAL の認証 .....	7
4.1. RH-SSO 用の DECISION CENTRAL クライアントの作成 .....	7
4.2. DECISION CENTRAL 用の RH-SSO クライアントアダプターのインストール .....	8
4.3. RH-SSO を使用した DECISION CENTRAL リモートサービスのセキュリティー保護 .....	9
4.4. RH-SSO を使用した DECISION CENTRAL ファイルシステムサービスのセキュリティー保護 .....	11
4.5. RH-SSO のユーザーおよびグループの管理の有効化 .....	12
第5章 RH-SSO を使用した DECISION SERVER の認証 .....	14
5.1. RH-SSO で DECISION SERVER クライアントの作成 .....	14
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 .....	15
5.3. DECISION SERVER のトークンベースの認証 .....	17
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 .....	18
6.1. BASIC 認証 .....	18
6.2. トークンベースの認証 .....	18
付録A バージョン情報 .....	20



## 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 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 Decision 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 (Decision 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、Decision 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**

Decision 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、Decision 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 スタートガイド](#)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ポリシードメインです。セキュリティレルムは、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 7.2 をダウンロードしてインストールし、設定します。

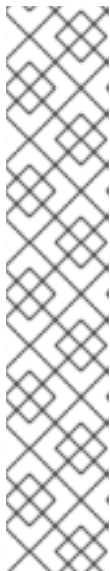


### 注記

Decision 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
  - **バージョン:** 7.2
2. **Red Hat Single Sign-on 7.2.0 Server(rh-ssso-7.2.0.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 ユーザーの追加

Decision 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** ページに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、Decision 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。
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 DECISION CENTRAL の認証

この章では、RH-SSO を介して Decision 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 用の Decision Central クライアントの作成」
- 「Decision Central 用の 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 Decision Central リモートサービスのセキュリティー保護」
- 「RH-SSO を使用した Decision Central ファイルシステムサービスのセキュリティー保護」
- 「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 への Red Hat Decision Manager のインストールおよび設定](#)の記載どおりに、Decision 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。
- [3章Red Hat Decision Manager ユーザーの追加](#)の記載どおりに、Decision Central ユーザーが RH-SSO に追加されている。

### 4.1. RH-SSO 用の DECISION CENTRAL クライアントの作成

RH-SSO サーバーが起動したら、Web ブラウザーで <http://localhost:8180/auth/admin> にアクセスし、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。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。

1. 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。
2. **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。
3. **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。
4. **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。
5. **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>
6. **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、Decision 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 接続をリッスンするように実行されます。このレル

ムは、Decision 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. DECISION CENTRAL 用の 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、Decision Central に対して設定する必要があります。

### 前提条件

- [Red Hat JBoss EAP への Red Hat Decision Manager のインストールおよび設定](#)の記載どおりに、Decision 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。
- [3章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
  - **バージョン:** 7.2
2. Red Hat Single Sign-on 7.2.0 Client Adaptor for JBoss EAP ([rh-ssso-7.2.0-eap7-adapter.zip](#)) をダウンロードします。
3. [rh-ssso-7.2.0-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 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
KnL6GgqINabMaFfPLPCF8kAgKnsi79NMo+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、Decision 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 DECISION CENTRAL リモートサービスのセキュリティー保護

Decision 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。RH-SSO でこれらのサービスを認証するには **BasicAuthSecurityFilter** パラメーターを無効にする必要があります。

## 手順

1. Decision Central アプリケーション記述子ファイル (**WEB-INF/web.xml**) を開き、以下の変更を加えます。

- 以下の行を削除して、**org.uberfire.ext.security.server.BasicAuthSecurityFilter** クラスのサーブレットフィルターとマッピングを削除します。

```
<filter>
  <filter-name>HTTP Basic Auth Filter</filter-name>
  <filter-class>org.uberfire.ext.security.server.BasicAuthSecurityFilter</filter-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>
```

- 以下の行を追加して、フィルターマッピングから削除した 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 DECISION CENTRAL ファイルシステムサービスのセキュリティ保護

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。

[Clients](#) > kie-git

Kie-git 

[Settings](#) [Credentials](#) [Roles](#) [Mappers](#) [Scope](#) [Revocation](#) [Sessions](#) [Offline Access](#) [Clustering](#) [Installation](#)

Client ID	<input type="text" value="kie-git"/>
Name	<input type="text"/>
Description	<input type="text"/>
Enabled	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Consent Required	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Client Protocol	<input type="text" value="openid-connect"/>
Client Template	<input type="text"/>
Access Type	<input type="text" value="confidential"/>
Standard Flow Enabled	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Direct Access Grants Enabled	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Service Accounts Enabled	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Root URL	<input type="text"/>
Base URL	<input type="text"/>
Admin URL	<input type="text"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

- 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。

- 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。
- 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>
```

- 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

このセクションでは、Decision 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について説明します。

### 手順

- 以下のライブラリーが **WEB-INF/lib** ディレクトリ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
```

- 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
```

- 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=KCAdapterUserManagementService
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"/>
</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。
- [3章Red Hat Decision Manager ユーザーの追加](#) の記載どおりに、**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 への Red Hat Decision Manager のインストールおよび設定](#) の記載どおりに、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」](#)

### 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 への Red Hat Decision Manager のインストールおよび設定](#) の記載どおりに、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。
- [3章Red Hat Decision Manager ユーザーの追加](#) の記載どおりに、**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。
  - **Client ID:** kie-execution-server
  - **Root URL:** \http://localhost:8080/kie-server

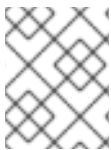
- **Client protocol:** openid-connect
4. 新規クライアントの **Access Type** は、デフォルトでは **public** に設定されています。この設定を **confidential** に変更して、もう一度 **Save** をクリックします。
  5. **Credentials** タブに移動して秘密鍵をコピーします。秘密鍵は、**kie-execution-server** クライアントを設定するのに必要になります。

## 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 への Red Hat Decision Manager のインストールおよび設定](#)の記載どおりに、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。
- [3章Red Hat Decision Manager ユーザーの追加](#)の記載どおりに、**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 Decision 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での [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:** 7.2
2. **Red Hat Single Sign-on 7.2.0 Client Adaptor for JBoss EAP (rh-sso-7.2.0-eap7-adapter.zip)** をダウンロードします。
3. **rh-sso-7.2.0-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
KnL6GgqINabMaFiPLPCF8kAgKnsi79NMo+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=<CONTROLLER_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
```

- 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

- トークンを使用して Decision Server を管理するように Decision Central を設定するには、以下を実行します。
  - org.kie.server.token** プロパティを設定します。
  - org.kie.server.user** プロパティと **org.kie.server.pwd** プロパティ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。
- 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。
  - org.kie.server.controller.token** プロパティを設定します。
  - org.kie.server.controller.user** プロパティおよび **org.kie.server.controller.pwd** プロパティ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

Decision 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**: Decision 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

Decision 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 ベースのリモトリポジトリ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、Decision 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لم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 Decision Central RH-SSO ユーザーです。詳細は、[3章 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)