JWT-SERVERインストールマニュアル

内容

[環境 3](#_Toc139267603)

[tomcat のインストール 4](#_Toc139267604)

[JDKのインストール 4](#_Toc139267605)

[javaのファイルにパスを通す 4](#_Toc139267606)

[tomcatを起動するユーザーを作成 4](#_Toc139267607)

[tomcatのダウンロード＆展開 4](#_Toc139267608)

[tomcatのサービス登録 4](#_Toc139267609)

[tomcatサービスに権限を与えて起動できるようにし、起動 5](#_Toc139267610)

[apache のインストール 5](#_Toc139267611)

[tomact と apache の連携 5](#_Toc139267612)

[proxyの設定 5](#_Toc139267613)

[ポートの設定 5](#_Toc139267614)

[apache&tomcatの再起動と自動起動設定 6](#_Toc139267615)

[Maven （3.2以上）のインストール 6](#_Toc139267616)

[パスの設定 6](#_Toc139267617)

[jwt-server のインストール 6](#_Toc139267618)

[環境設定 7](#_Toc139267619)

[ビルド＆デプロイ 8](#_Toc139267620)

[mysql (mariadb) のインストール 8](#_Toc139267621)

[mysqlの起動と自動起動設定 8](#_Toc139267622)

[初期設定 8](#_Toc139267623)

[環境設定 9](#_Toc139267624)

[ユーザ作成 9](#_Toc139267625)

[データベース作成 9](#_Toc139267626)

[Keycloakの設定 9](#_Toc139267627)

[realmnの作成 9](#_Toc139267628)

[clientの作成 10](#_Toc139267629)

[ユーザの作成 12](#_Toc139267630)

# 環境

本ドキュメントの手順はCentOS Stream 9環境にて検証している。その他のRHEL Linux環境でも動作は可能であるが一部手順に違いがでる可能性がある。

# tomcat のインストール

## JDKのインストール

# yum -y install java-1.8.0-openjdk-devel

## javaのファイルにパスを通す

# echo "export JAVA\_HOME=$(readlink -e $(which java)|sed 's:/bin/java::')" > /etc/profile.d/java.sh

# echo "PATH=\$PATH:\$JAVA\_HOME/bin" >> /etc/profile.d/java.sh

# source /etc/profile.d/java.sh

## tomcatを起動するユーザーを作成

# useradd -s /sbin/nologin tomcat

## tomcatのダウンロード＆展開

# mkdir -p /usr/local/src/tomcat

# cd /usr/local/src/tomcat

# curl -OL https://dlcdn.apache.org/tomcat/tomcat-8/v8.5.76/bin/apache-tomcat-8.5.76.tar.gz

# tar zxvf apache-tomcat-8.5.76.tar.gz

# mv apache-tomcat-8.5.76 /opt/

# chown -R tomcat. /opt/apache-tomcat-8.5.76

# ln -s /opt/apache-tomcat-8.5.76 /opt/tomcat

# echo 'export CATALINA\_HOME=/opt/tomcat' > /etc/profile.d/tomcat.sh

# source /etc/profile.d/tomcat.sh

## tomcatのサービス登録

# vi /etc/systemd/system/tomcat.service

（sample）

[Unit]

Description=Apache Tomcat 8

After=syslog.target network.target

[Service]

User=tomcat

Group=tomcat

Type=oneshot

PIDFile=/opt/tomcat/tomcat.pid

RemainAfterExit=yes

ExecStart=/opt/tomcat/bin/startup.sh

ExecStop=/opt/tomcat/bin/shutdown.sh

ExecReStart=/opt/tomcat/bin/shutdown.sh;/opt/tomcat/bin/startup.sh

[Install]

WantedBy=multi-user.target

## tomcatサービスに権限を与えて起動できるようにし、起動

# chmod 755 /etc/systemd/system/tomcat.service

# systemctl start tomcat

# apache のインストール

# yum -y install httpd mod\_ssl

# systemctl start httpd

# tomact と apache の連携

## proxyの設定

# vi /etc/httpd/conf.d/proxy-ajp.conf

（追加）

ProxyPass /jwt-server ajp://localhost:8009/jwt-server secret=password

ProxyPassReverse /jwt-server ajp://localhost:8009/jwt-server secret=password

(\*) secretの文字列はserver.xmlファイルで指定したものと同じにする。

## ポートの設定

# vi /opt/tomcat/conf/server.xml

※8080ポートアクセスの不許可

<!--

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />

-->

※8009ポートからのアクセス許可

<Connector protocol="AJP/1.3"

address="localhost"

port="8009"

redirectPort="8443"

secret="password" />

(\*)secretの文字列はproxy-ajp.confで設定した文字列と同じものにする。

## apache&tomcatの再起動と自動起動設定

# systemctl restart tomcat

# systemctl restart httpd

# systemctl enable tomcat

# systemctl enable httpd

# Maven （3.2以上）のインストール

# curl -OL https://archive.apache.org/dist/maven/maven-3/3.8.4/binaries/apache-maven-3.8.4-bin.tar.gz

# tar -xzvf apache-maven-3.8.4-bin.tar.gz

# mv apache-maven-3.8.4 /opt/

# cd /opt

# ln -s /opt/apache-maven-3.8.4 apache-maven

## パスの設定

% vi ~/.bash\_profile

（追加）

JAVA\_HOME=/usr/java/default/

PATH=$PATH:/opt/apache-maven/bin

% source ~/.bash\_profile

# jwt-server のインストール

% git clone https://github.com/oss-tsukuba/jwt-server.git

% cd jwt-server

## 環境設定

% vi src/main/resources/application.properties

（設定例)

# change keycloak settings

keycloak.enabled=true

keycloak.auth-server-url=https://can3.canaly.co.jp:8443/auth

keycloak.realm=hpci

keycloak.resource=jwt-server

keycloak.public-client=false

keycloak.credentials.secret=8a5a0480-1d7a-420c-b3d9-93b65439d321

user-claim=hpci.id

#change MySQL settings

spring.datasource.url=jdbc:mysql://${MYSQL\_HOST:localhost}:3306/gfarmdb

spring.datasource.username=dbuser

spring.datasource.password=passworD12@

spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver

spring.jpa.database=MYSQL

spring.jpa.hibernate.ddl-auto=update

各設定値の内容は以下の通りである。

* keycloak.enabled

Keycloak Spring Boot アダプターの有効/無効を設定する。

* keycloak.auth-server-url

KeycloakサーバのURLを設定する。

* keycloak.realm

レルムを設定する。

* keycloak.resource

クライアントIDを設定する。

* keycloak.public-client

クライアントがpublicか否かを設定する。

* keycloak.credentials.secret

クライアントのシークレットを設定する。クライアントがpublicの場合は不要である。

* user-claim

ユーザIDとして利用するトークンのクレームを設定する。

* spring.datasource.url

データベースのURLを設定する。MySQLを利用する想定である。

* spring.datasource.username

データベースにアクセスするユーザ名を設定する。

* spring.datasource.password

データベースにアクセスするユーザを設定する。

(\*)ユーザのパスワード設定についてはmysql(mariadb)のインストールの章で述べる。

* spring.datasource.driver-class-name

ユーザのパスワードを設定する。

* spring.jpa.database

データベース（DBMS）の種類を設定する。

* spring.jpa.hivernate.ddl-auto

データベースのスキーマの生成方法を設定する。

## ビルド＆デプロイ

% mvn package spring-boot:repackage

% sudo cp target/jwt-server.war /opt/tomcat/webapps/

# mysql (mariadb) のインストール

# yum install -y mariadb mariadb-server

## mysqlの起動と自動起動設定

# systemctl start mariadb

# systemctl enable mariadb

## 初期設定

# mysql\_secure\_installation

# １つ目: 今のrootパスワードを入力(初めはパスワードが無いのでEnterでOK)

Enter current password for root (enter for none): # Enter

…2つ目: unix\_socket 認証に切り替えるか

Switch to unix\_socket authentication [Y/n] **n** #「n」の入力

# 3つ目: rootパスワードを設定するか

Set root password? [Y/n] # Enter

# 4つ目: 新しいrootパスワードを設定

New password: # 新しいパスワードの入力

# 5つ目: 新しいパスワードの確認

Re-enter new password: # 新しいパスワードを再入力

# 6つ目: 匿名ユーザ(初期設定などのために誰でもログインできるユーザ)を削除するか

Remove anonymous users? [Y/n] # Enter

# 7つ目: rootのリモートログインを禁止するか

Disallow root login remotely? [Y/n] # Enter

# 8つ目: testデータベース(テスト用の誰でもアクセス可能なデータベース)を削除するか

Remove test database and access to it? [Y/n] # Enter

# 9つ目: 権限を管理するテーブルをリロードして、設定をすぐに反映するか

Reload privilege tables now? [Y/n] # Enter

## 環境設定

# vi /etc/my.cnf

（[mysqld] セクションに追記）

character\_set\_server=utf8mb4

skip-character-set-client-handshake

# systemctl restart mariadb

## ユーザ作成

% mysql -u root -p

mysql> CREATE USER 'dbuser'@'localhost' IDENTIFIED BY 'passworD12@';

mysql> GRANT ALL PRIVILEGES ON \* . \* TO 'dbuser'@'localhost';

mysql> CREATE DATABASE gfarmdb;

mysql> FLUSH PRIVILEGES;

mysql> quit

(\*)パスワードはapplication.propertiesで指定したパスワードと同じものにする。

## データベース作成

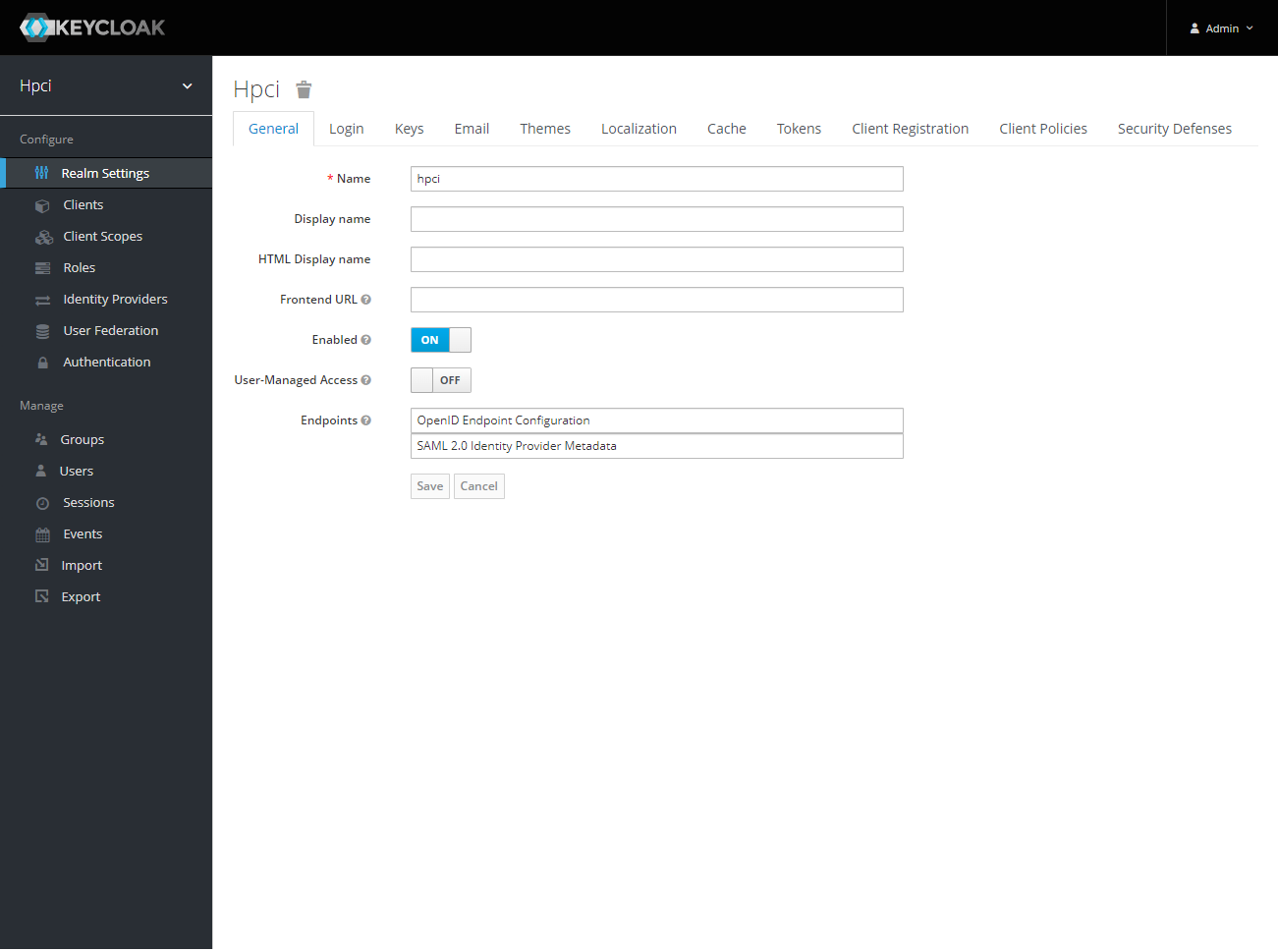
% mysql -u dbuser -p

% mysql -u dbuser -p gfarmdb < jwt-server/ddl/jwt-server.ddl

# Keycloakの設定

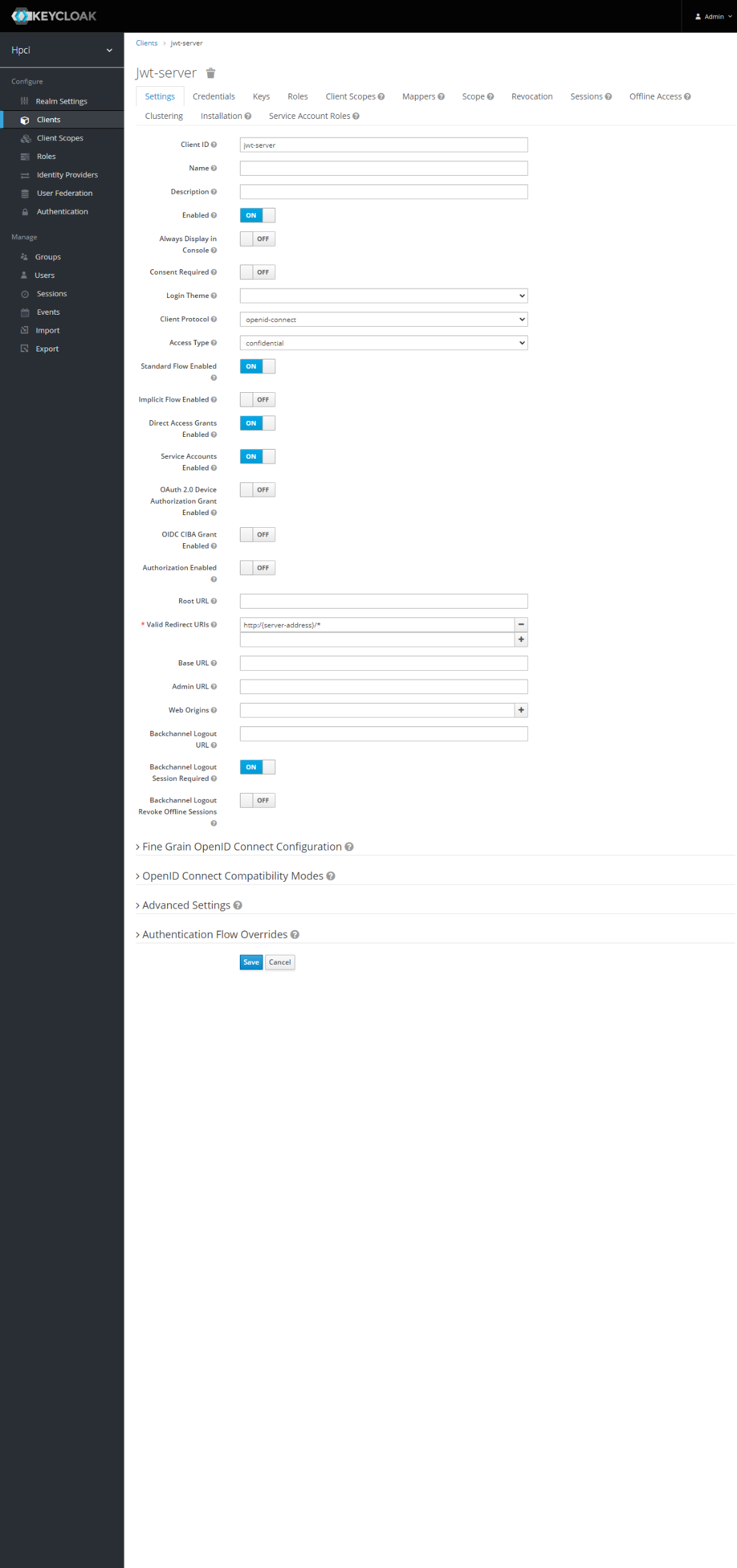
## realmnの作成

レルム「hpci」を作成する。



## clientの作成

hcpi配下にクライアント「jwt-server」を作成する。トークンの認証を行うため、「Access Type」はconfidentialにする必要がある。



## ユーザの作成

必要に応じてユーザを作成する。

