



Red Hat build of Keycloak 24.0

スタートガイド

法律上の通知

Copyright © 2024 Red Hat, Inc.

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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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

このガイドは、実稼働環境で使用する前に Red Hat build of Keycloak 24.0 を使用して評価するのに役立ちます。これには、Red Hat build of Keycloak をインストールして開発モードで実行する手順、ユーザーとアプリケーションを管理するためのレルムとアカウントを作成する手順、およびシングルページアプリケーション (SPA) のセキュリティーを保護する手順が含まれています。

目次

多様性を受け入れるオープンソースの強化	3
第1章 スタートガイド	4
1.1. 作業を開始する前の注意事項	4
1.2. RED HAT BUILD OF KEYCLOAK のダウンロード	4
1.3. RED HAT BUILD OF KEYCLOAK の起動	4
1.4. 管理者ユーザーの作成	4
1.5. 管理コンソールへのログイン	4
1.6. レルムを作成します。	4
1.7. ユーザーを作成します。	5
1.8. アカウントコンソールにログインします。	7
1.9. 最初のアプリケーションのセキュリティー保護	7
1.10. 次のステップ	9

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[Red Hat CTO である Chris Wright のメッセージ](#) をご覧ください。

第1章 スタートガイド

1.1. 作業を開始する前の注意事項

[OpenJDK 17](#) がインストールされていることを確認してください。

1.2. RED HAT BUILD OF KEYCLOAK のダウンロード

Red Hat build of Keycloak を [Red Hat の Web サイト](#) からダウンロードして展開します。

このファイルを展開すると、**rhbk-24.0.5** という名前のディレクトリーが作成されます。

1.3. RED HAT BUILD OF KEYCLOAK の起動

1. 端末から、**rhbk-24.0.5** ディレクトリーを開きます。
2. 以下のコマンドを入力します。

- Linux では、次を実行します。

```
bin/kc.sh start-dev
```

- Windows では、次を実行します。

```
bin\kc.bat start-dev
```

start-dev オプションを使用すると、開発モードで Red Hat build of Keycloak が起動します。このモードでは、Red Hat build of Keycloak を初めて試して、すぐに起動して実行することができます。このモードは、Red Hat build of Keycloak の開発など、開発者にとって便利なデフォルト設定を提供します。

1.4. 管理者ユーザーの作成

Red Hat build of Keycloak にはデフォルトの管理者ユーザーがありません。Keycloak を起動する前に、管理者ユーザーを作成する必要があります。

1. <http://localhost:8080/> を開きます。
2. ユーザー名とパスワードをフォームに入力します。

1.5. 管理コンソールへのログイン

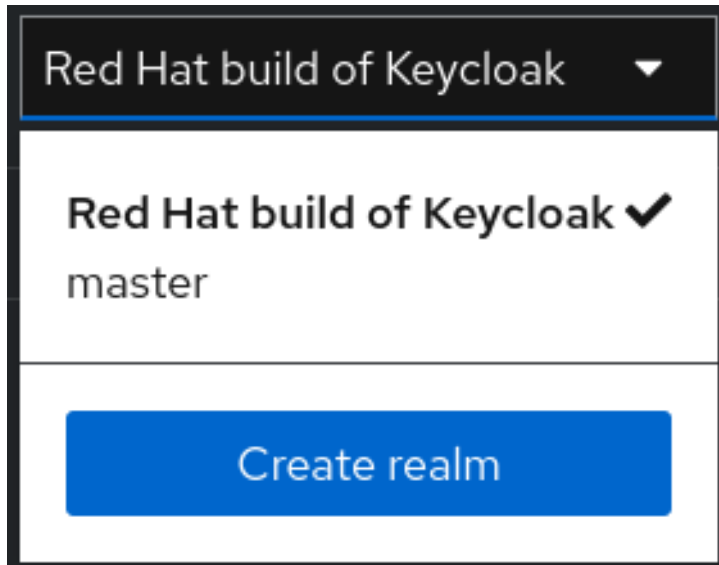
1. [Red Hat build of Keycloak 管理コンソール](#) に移動します。
2. 前の手順で作成したユーザー名とパスワードでログインします。

1.6. レルムを作成します。

Red Hat build of Keycloak のレルムはテナントに相当します。各レルムにより、管理者はアプリケーションとユーザーの分離グループを作成できます。Red Hat build of Keycloak には、最初は **master** と呼ばれる単一のレルムが含まれています。このレルムは、Red Hat build of Keycloak の管理にのみ使用し、アプリケーションの管理には使用しません。

次の手順を使用して、最初のレルムを作成します。

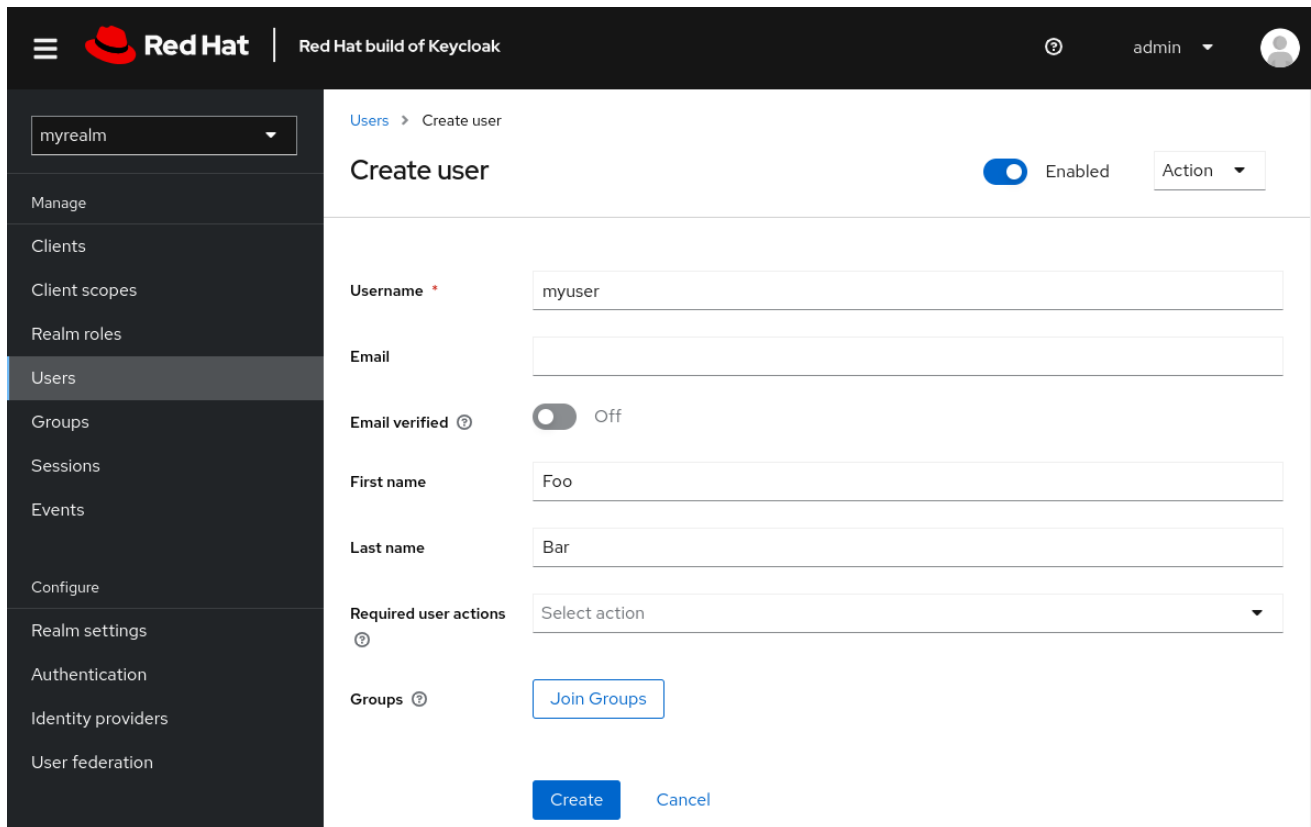
1. Red Hat build of Keycloak [管理コンソール](#) を開きます。
2. master realm の横にある Red Hat build of Keycloak をクリックし、Create Realm をクリックします。
3. Realm name フィールドに **myrealm** と入力します。
4. Create をクリックします。



1.7. ユーザーを作成します。

最初、レルムにはユーザーがいません。ユーザーを作成するには、以下を実行します。

1. 現在のレルムがまだ **myrealm** であることを確認します。これは **Manage** の上に表示されています。
2. 左側のメニューで **Users** をクリックします。
3. **Add user** をクリックします。
4. フォームに次の値を入力します。
 - Username: **myuser**
 - First name: 任意の名
 - Last name: 任意の姓
5. **Create** をクリックします。



Red Hat build of Keycloak

admin

myrealm

Users > Create user

Create user Enabled Action

Username * myuser

Email

Email verified Off

First name Foo

Last name Bar

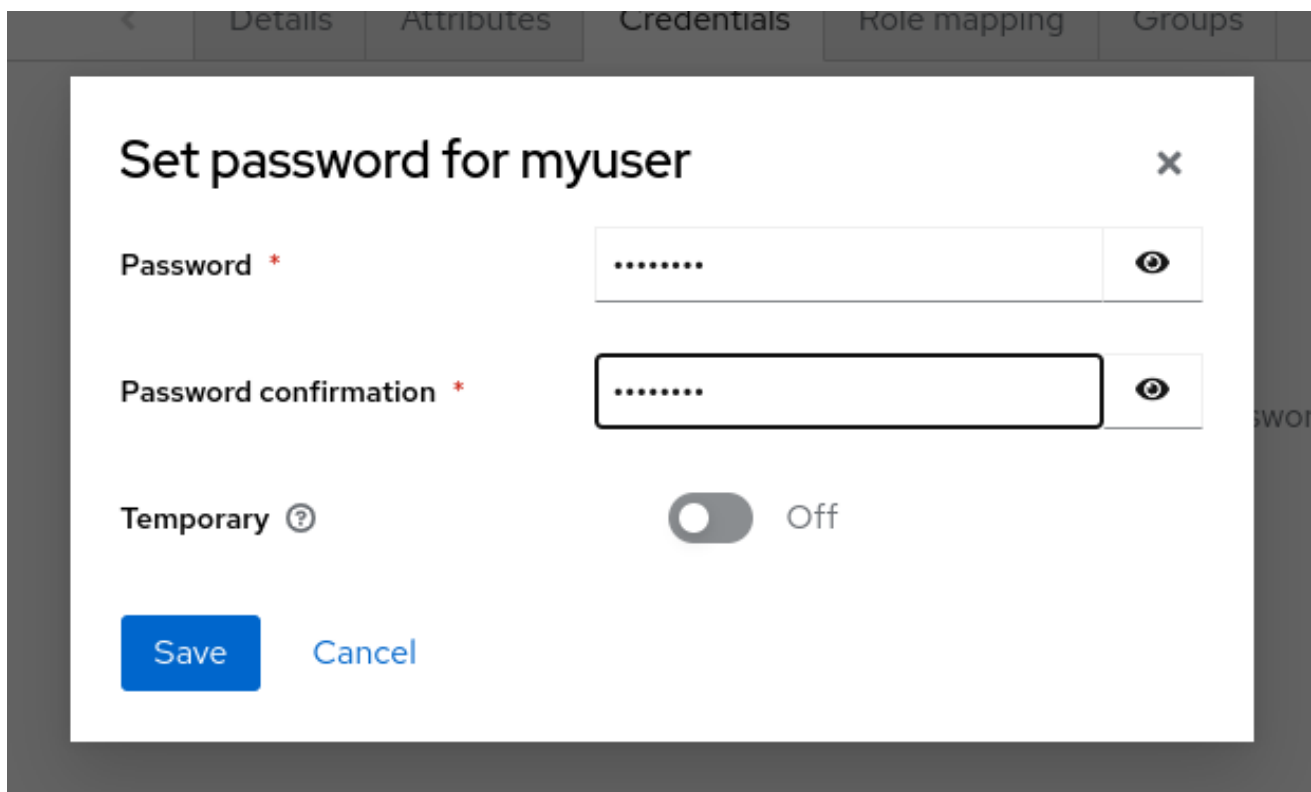
Required user actions Select action

Groups Join Groups

Create Cancel

このユーザーがログインするにはパスワードが必要です。初期パスワードを設定するには、以下を実行します。

1. ページの上部にある **Credentials** をクリックします。
2. **Set password** フォームにパスワードを入力します。
3. ユーザーが最初のログイン時にこのパスワードを更新する必要がないように、**Temporary** を **Off** に切り替えます。



Details Attributes Credentials Role mapping Groups

Set password for myuser ×

Password * 👁

Password confirmation * 👁

Temporary Off

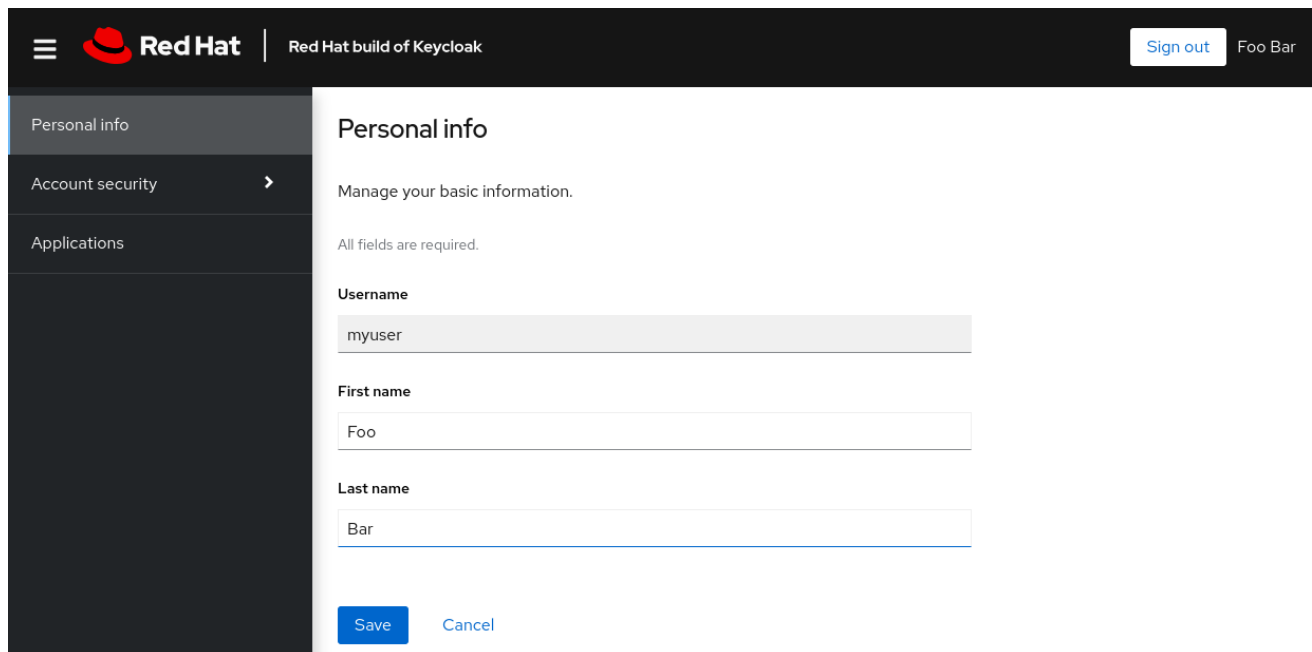
Save Cancel

1.8. アカウントコンソールにログインします。

これで、アカウントコンソールにログインし、このユーザーが正しく設定されていることを確認できます。

1. [Red Hat build of Keycloak アカウントコンソール](#) を開きます。
2. 前の手順で作成した **myuser** とパスワードでログインします。

アカウントコンソールのユーザーとして、プロフィールの変更、2 要素認証の追加、ID プロバイダーアカウントの追加などを実行してアカウントを管理できます。



The screenshot shows the 'Personal info' page in the Red Hat build of Keycloak account console. The page has a dark header with the Red Hat logo and 'Red Hat build of Keycloak' text. On the right of the header, there is a 'Sign out' button and the text 'Foo Bar'. A left sidebar contains navigation links for 'Personal info', 'Account security', and 'Applications'. The main content area is titled 'Personal info' and contains the text 'Manage your basic information.' and 'All fields are required.' Below this are three input fields: 'Username' (containing 'myuser'), 'First name' (containing 'Foo'), and 'Last name' (containing 'Bar'). At the bottom of the form are 'Save' and 'Cancel' buttons.

1.9. 最初のアプリケーションのセキュリティー保護

最初のアプリケーションに対してセキュリティー保護を行うには、まずアプリケーションを Red Hat build of Keycloak インスタンスに登録します。

1. [Red Hat build of Keycloak 管理コンソール](#) を開きます。
2. 左上隅にある **master** という単語をクリックし、**myrealm** をクリックします。
3. **Clients** をクリックします。
4. **Create client** をクリックします
5. フォームに次の値を入力します。
 - **Client type: OpenID Connect**
 - **Client ID: myclient**

The screenshot shows the 'Create client' page in the Red Hat build of Keycloak. The left sidebar contains a navigation menu with options like 'Manage', 'Clients', 'Client scopes', 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings', 'Authentication', 'Identity providers', and 'User federation'. The main content area is titled 'Create client' and includes a sub-header 'Clients > Create client'. Below this, there's a 'General Settings' tab. The form fields are: 'Client type' (OpenID Connect), 'Client ID' (myclient), 'Name' (empty), 'Description' (empty), and 'Always display in console' (Off). At the bottom, there are 'Next', 'Back', and 'Cancel' buttons.

6. **Next** をクリックします。

7. **Standard flow** が有効になっていることを確認します。

8. **Next** をクリックします。

9. **Login settings** で以下の変更を行います。

- **Valid redirect URIs** を **https://www.keycloak.org/app/*** に設定します。
- **Web origins** を **https://www.keycloak.org** に設定します。

10. **Save** をクリックします。

Red Hat | Red Hat build of Keycloak

admin

myrealm

Clients > Create client

Create client

Clients are applications and services that can request authentication of a user.

- 1 General Settings
- 2 Capability config
- 3 Login settings

Root URL

Home URL

Valid redirect URIs + Add valid redirect URIs

Valid post logout redirect URIs + Add valid post logout redirect URIs

Web origins + Add web origins

Save Back Cancel

クライアントが正常に作成されたことを確認するために、[Keycloak Web サイト](#) の SPA テストアプリケーションを使用できます。

1. <https://www.keycloak.org/app/> を開きます。
2. **Save** をクリックして、デフォルト設定を使用します。
3. **Sign in** をクリックし、前に起動した Red Hat build of Keycloak サーバーを使用してこのアプリケーションを認証します。

1.10. 次のステップ

実稼働環境で Red Hat build of Keycloak を実行する前に、以下の操作を行うことを検討してください。

- PostgreSQL などの実稼働対応データベースへの切り替え。
- 独自の証明書を使用した SSL の設定。
- よりセキュアな管理者パスワードへの切り替え。

詳細は、[サーバーガイド](#) を参照してください。