



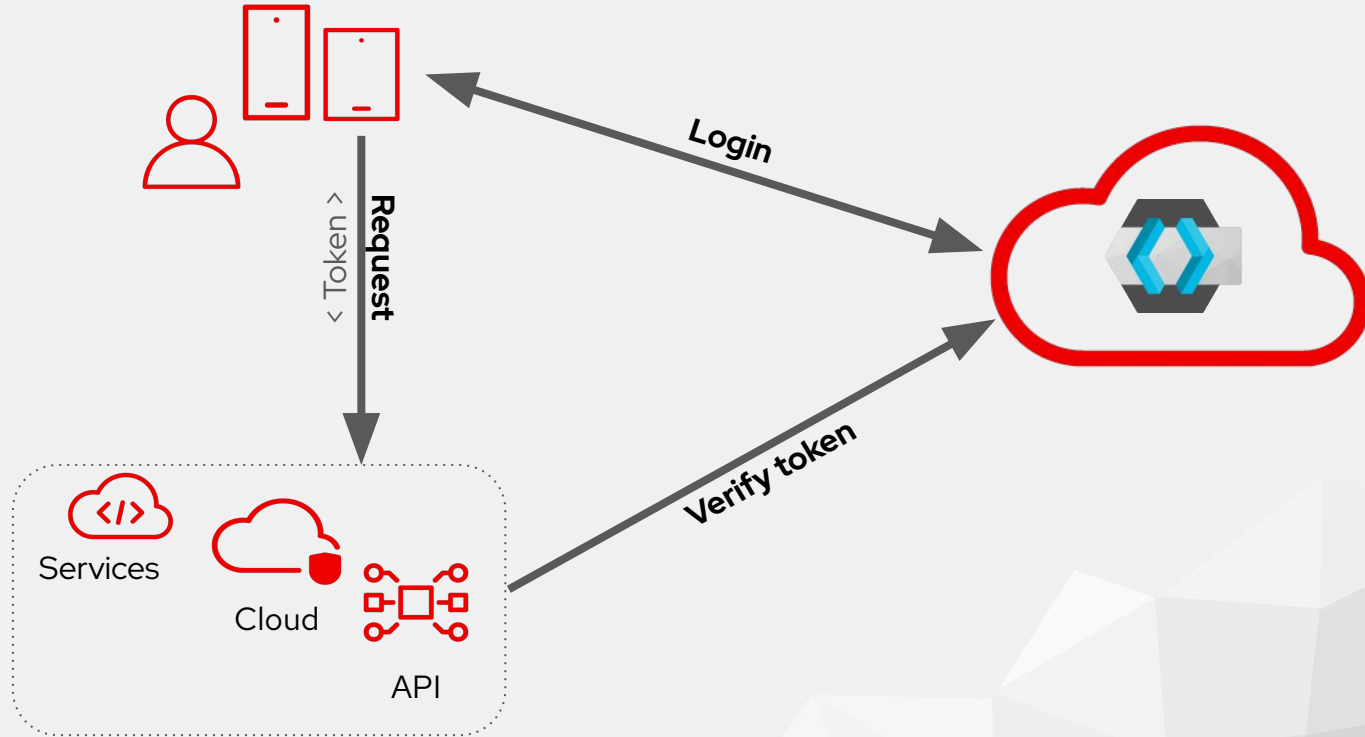
Keycloak: the Open Source Identity and Access Management for Modern Applications

Alexander Schwartz | Principal Software Engineer | Red Hat
Kubecon EU Amsterdam | 2023-04-19

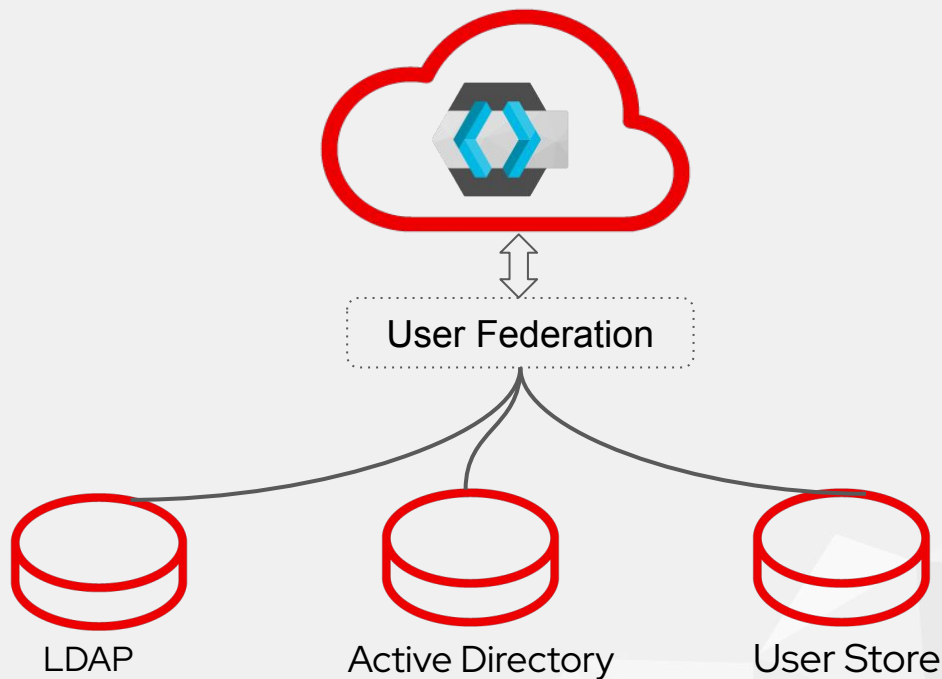
Keycloak is an Open Source Identity and Access Management Solution

- Authenticate and authorize users for applications
- Configure interactively or fully automated
- Bridge to existing security infrastructures
- Extend and customize as needed
- Run and scale in cloud and non-cloud environments

Let Keycloak handle AuthZ and AuthN for your apps



Optional: Use existing user directories via federation



Let's do a demo of Keycloak!

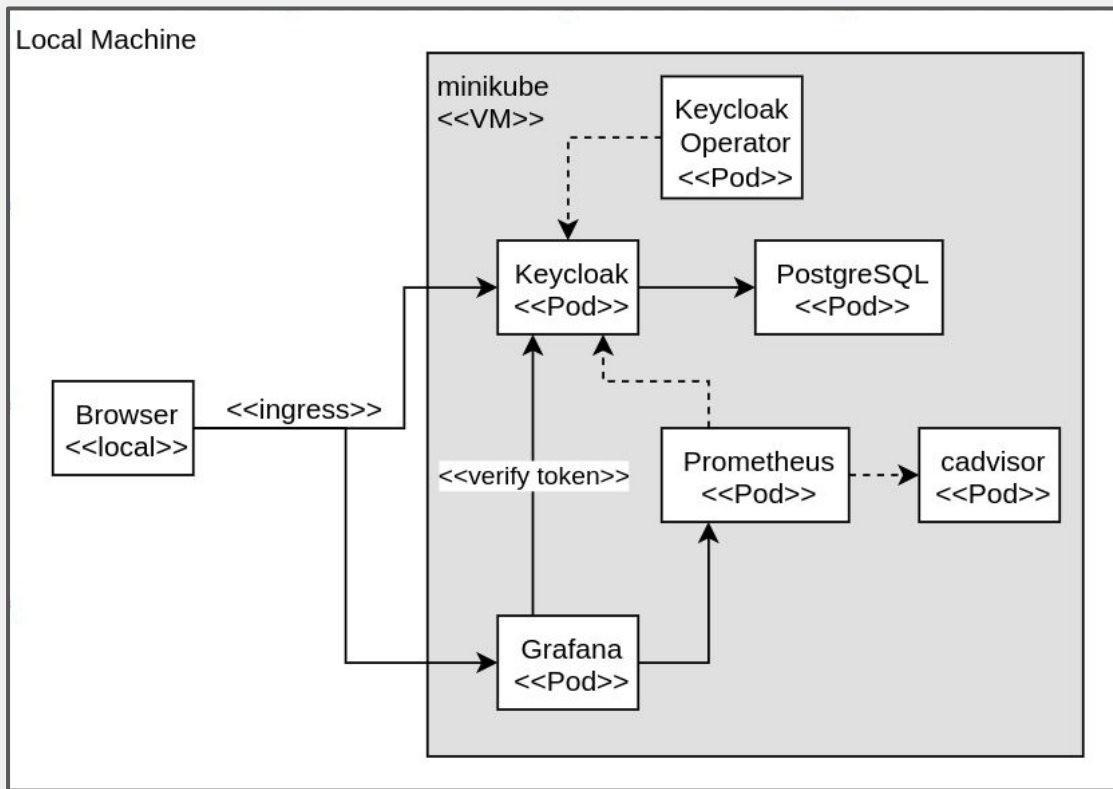
Sign in to your account

Username or email

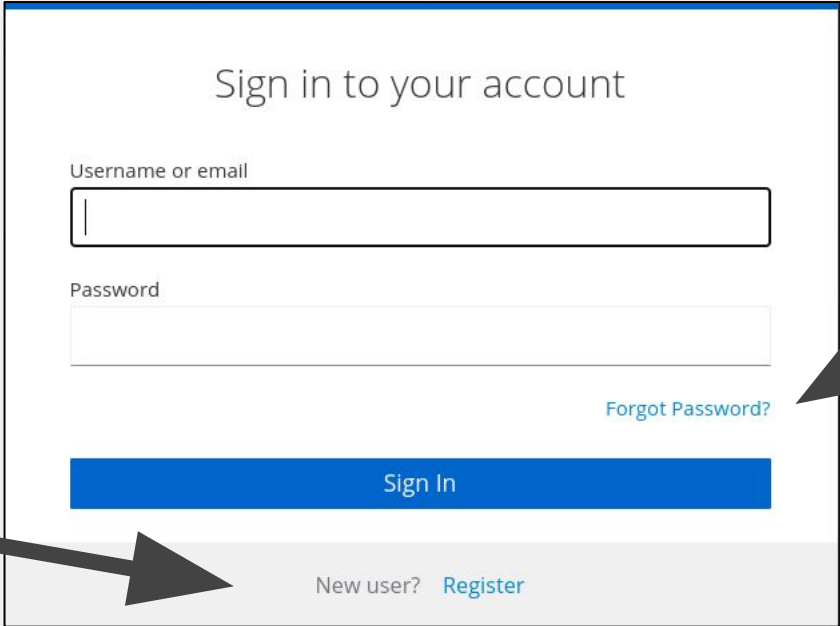
Password

Sign In

Let's do a demo of Keycloak!



... it can do a lot more ...



Sign in to your account

Username or email

Password

[Forgot Password?](#)

[Sign In](#)

New user? [Register](#)

... and use other providers ...





Sign in to your account


Username or email

Password

Sign In

Or sign in with

 GitHub	 OpenShift v4
 StackOverflow	 Google

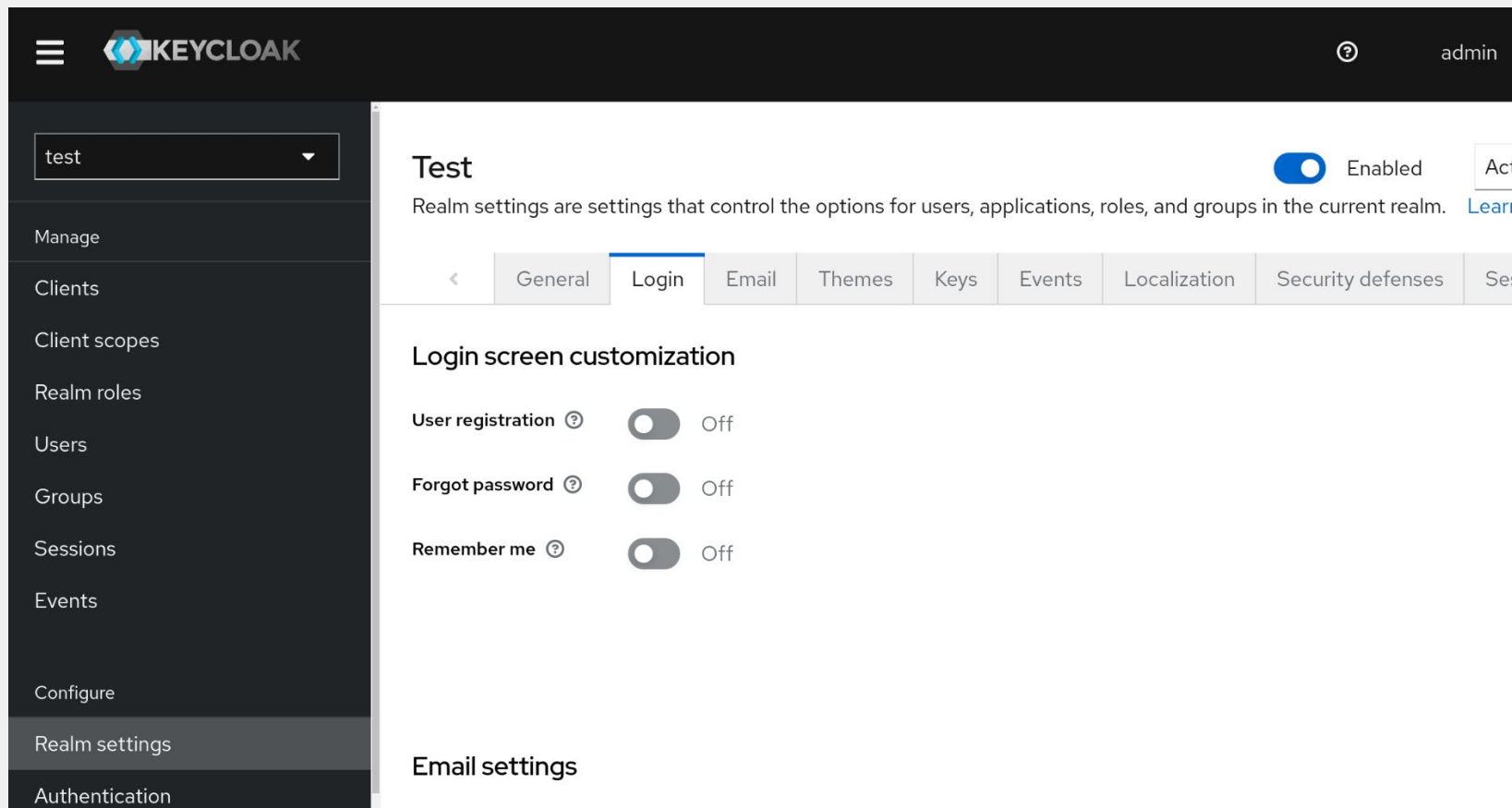


... or skip the form with Kerberos/SNPEGO!

This page intentionally left blank.

Enable Admins

Manage Keycloak via web UI,
REST and CLI



The screenshot displays the Keycloak administration console. On the left is a dark sidebar with a menu. The top of the sidebar features the Keycloak logo and a hamburger menu icon. Below this is a search bar containing the text 'test'. The menu items include 'Manage', 'Clients', 'Client scopes', 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings' (which is highlighted), and 'Authentication'. The main content area on the right has a top navigation bar with a help icon and the text 'admin'. Below this, the 'Test' realm settings page is shown. It includes a toggle switch for 'Enabled' which is turned on. A description states: 'Realm settings are settings that control the options for users, applications, roles, and groups in the current realm.' A horizontal tab bar contains 'General', 'Login' (selected), 'Email', 'Themes', 'Keys', 'Events', 'Localization', 'Security defenses', and 'Sessions'. Under the 'Login' tab, the 'Login screen customization' section contains three settings: 'User registration' (Off), 'Forgot password' (Off), and 'Remember me' (Off), each with a toggle switch and a help icon. The 'Email settings' section is partially visible at the bottom.

KEYCLOAK

test

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

KEYCLOAK

Test

Enabled

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm.

General Login Email Themes Keys Events Localization Security defenses Sessions

Login screen customization

User registration ? Off

Forgot password ? Off

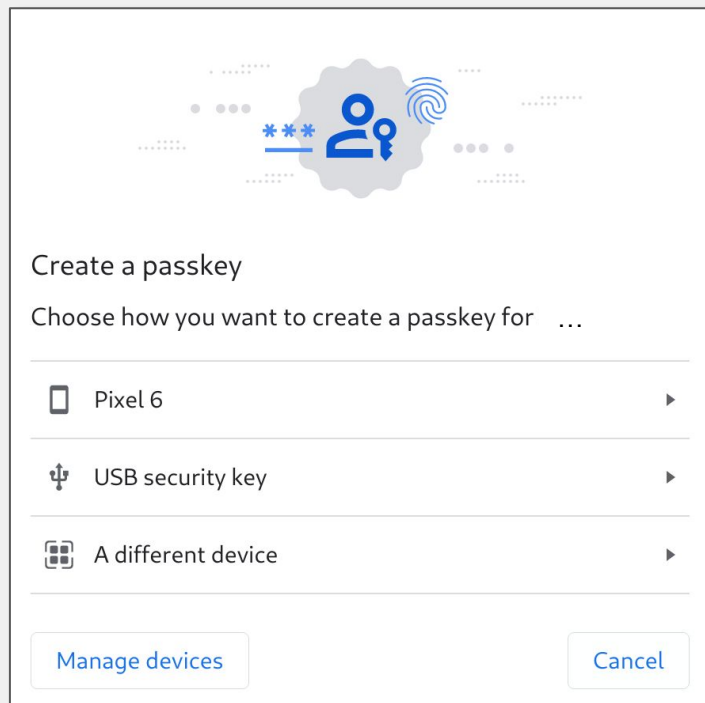
Remember me ? Off

Email settings

Powerful required actions in the login flow

- Configure One Time Passwords
- WebAuthn Register
- Terms and Conditions
- Update Password
- Update Profile
- Verify Email
- ...

... or build your own!



The screenshot shows a 'Create a passkey' dialog box. At the top is a decorative graphic with a person icon, a fingerprint icon, and a key icon. Below the graphic, the text 'Create a passkey' is followed by 'Choose how you want to create a passkey for ...'. There are three options listed: 'Pixel 6' with a smartphone icon, 'USB security key' with a USB key icon, and 'A different device' with a generic device icon. At the bottom, there are two buttons: 'Manage devices' and 'Cancel'.

Create a passkey



Choose how you want to create a passkey for ...

- Pixel 6
- USB security key
- A different device

Manage devices Cancel

Enable Users

Manage account details,
password and second factor.

  KEYCLOAK

[Back to security admin console](#) [Sign out](#)

Personal info

Account security ▾

Signing in

Device activity

Applications

Signing in

Configure ways to sign in.

Basic authentication

Password

Sign in by entering your password.

My password	Created March 31, 2023 at 6:29 PM	Update
-------------	--	------------------------

Two-factor authentication

Authenticator application

Enter a verification code from authenticator application

[Set up authenticator application](#)

Enable continuous everything

- Export/import of realms
- REST API and CLI
- Configuration files and CRDs

```
apiVersion: k8s.keycloak.org/v2alpha1
kind: Keycloak
metadata:
  labels:
    app: keycloak
  name: keycloak
  namespace: ...
spec:
  hostname:
    hostname: keycloak...
  additionalOptions:
    - name: db
      value: postgres
    - name: db-url
      value: jdbc:postgresql://...
    - name: db-pool-min-size
      value: ...
    - name: db-pool-max-size
```

Customize to your needs

From the *Server developer guide*:

- Customize the theme
- Configure login flows
- Add new required actions
- Create event listener
- Supply mappers for federations
- Connect any custom user storage

Extending the server

The Keycloak SPI framework offers the possibility to implement or override existing functionality. However Keycloak also provides capabilities to extend its core functionality in several possibilities to:

- Add custom REST endpoints to the Keycloak server
- Add your own custom SPI
- Add custom JPA entities to the Keycloak data model

Add custom REST endpoints

This is a very powerful extension, which allows you to deploy your own REST endpoints. There are several kinds of extensions, for example the possibility to trigger functionality on specific events or to extend the default set of built-in Keycloak REST endpoints.

To add a custom REST endpoint, you need to implement the `RealmResourceProvider` interfaces. `RealmResourceProvider` has on

Engaging with the community

- All issues and pull requests on GitHub
- Discussions on mailing lists and GitHub discussions
- Contributing guidelines guide new contributors
- List of community contributions
- FAPI-SIG (Financial-grade API Security Special Interest Group)
<https://github.com/keycloak/kc-sig-fapi>

More information: <https://www.keycloak.org/community>

Recent changes in Keycloak

- Change from Wildfly to Quarkus 2
(less memory consumption and faster startup times)
- New Operator
- New Admin Console
- Step-up authentication
- Session Limits
- Client Secret Rotation
- Recovery Codes
- WebAuthN
- OIDC Logout Improvements

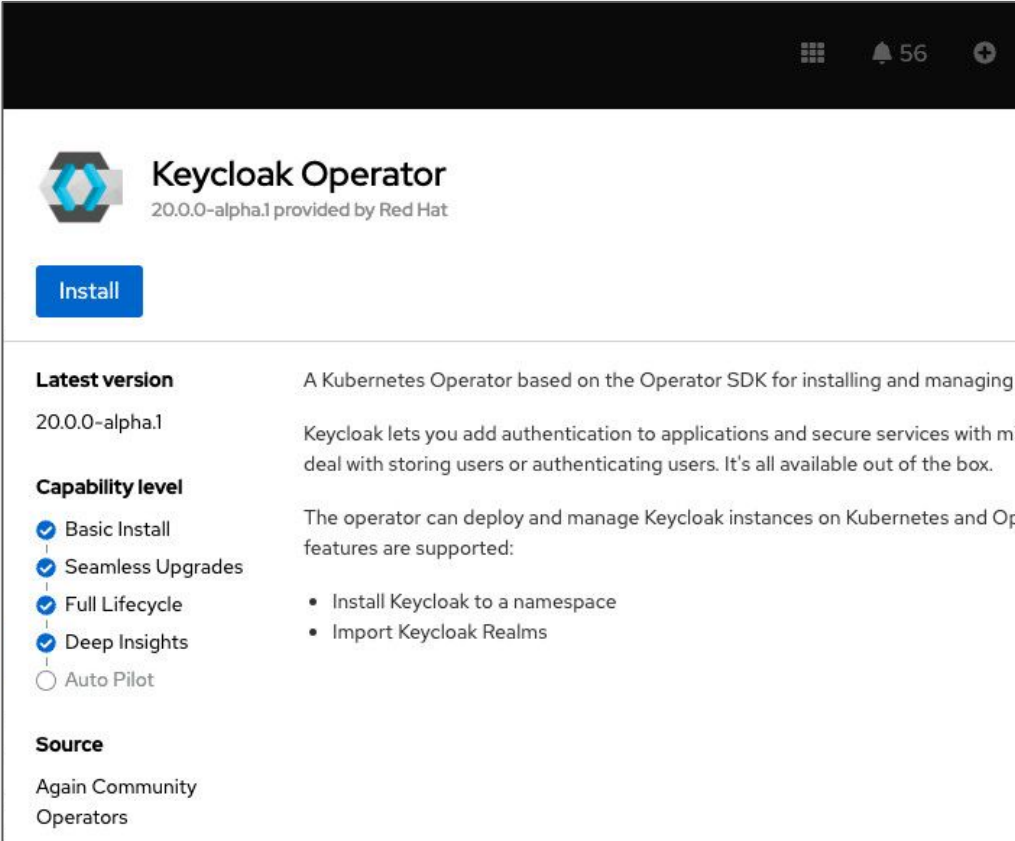
Looking at the future roadmap*

- Upgrade Quarkus 2 → 3
- FIPS 140-2 support
- Cross-DC and multi-region support
- Zero-downtime upgrades
- OpenJDK 17 support
- New Account Console

* Roadmap details (features & timelines) do NOT represent any commitments and are ALWAYS subject to change.

Run in cloud and non-cloud environments

- Extract archive and run
- Use pre-built containers
- Customize the Keycloak container with your providers
- Use the Keycloak Operator



The screenshot shows the GitHub repository page for the Keycloak Operator. At the top, there's a navigation bar with a grid icon, a notification bell showing 56 alerts, and a plus icon. Below this, the repository name "Keycloak Operator" is displayed in a large font, with the version "20.0.0-alpha.1 provided by Red Hat" underneath. A blue "Install" button is prominently featured. The main content area is divided into two columns. The left column contains the "Latest version" (20.0.0-alpha.1) and a "Capability level" section with a list of features: "Basic Install", "Seamless Upgrades", "Full Lifecycle", "Deep Insights", and "Auto Pilot". The right column provides a description of the operator as a Kubernetes Operator based on the Operator SDK, and lists supported features: "Install Keycloak to a namespace" and "Import Keycloak Realms". At the bottom, the "Source" is listed as "Again Community Operators".

Keycloak Operator
20.0.0-alpha.1 provided by Red Hat

[Install](#)

Latest version
20.0.0-alpha.1

Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☒ Full Lifecycle
- ☒ Deep Insights
- ☐ Auto Pilot

Source
Again Community Operators

A Kubernetes Operator based on the Operator SDK for installing and managing Keycloak instances on Kubernetes and OpenShift.

Keycloak lets you add authentication to applications and secure services with m... deal with storing users or authenticating users. It's all available out of the box.

The operator can deploy and manage Keycloak instances on Kubernetes and Op... features are supported:

- Install Keycloak to a namespace
- Import Keycloak Realms

Keycloak is an Open Source Identity and Access Management Solution

- Authenticate and authorize users for applications
- Configure interactively or fully automated
- Bridge to existing security infrastructures
- Extend and customize as needed
- Run and scale in cloud and non-cloud environments

Links

- Keycloak
<https://www.keycloak.org>
- Demo
<https://github.com/ahus1/keycloak-cloud-native-demo>
- Getting started on bare metal
<https://www.keycloak.org/getting-started/getting-started-zip>
- Getting started on OpenShift
<https://www.keycloak.org/getting-started/getting-started-openshift>
- Keycloak Operator Guides
<https://www.keycloak.org/guides#operator>
- Server Developer Guide
https://www.keycloak.org/docs/latest/server_development