



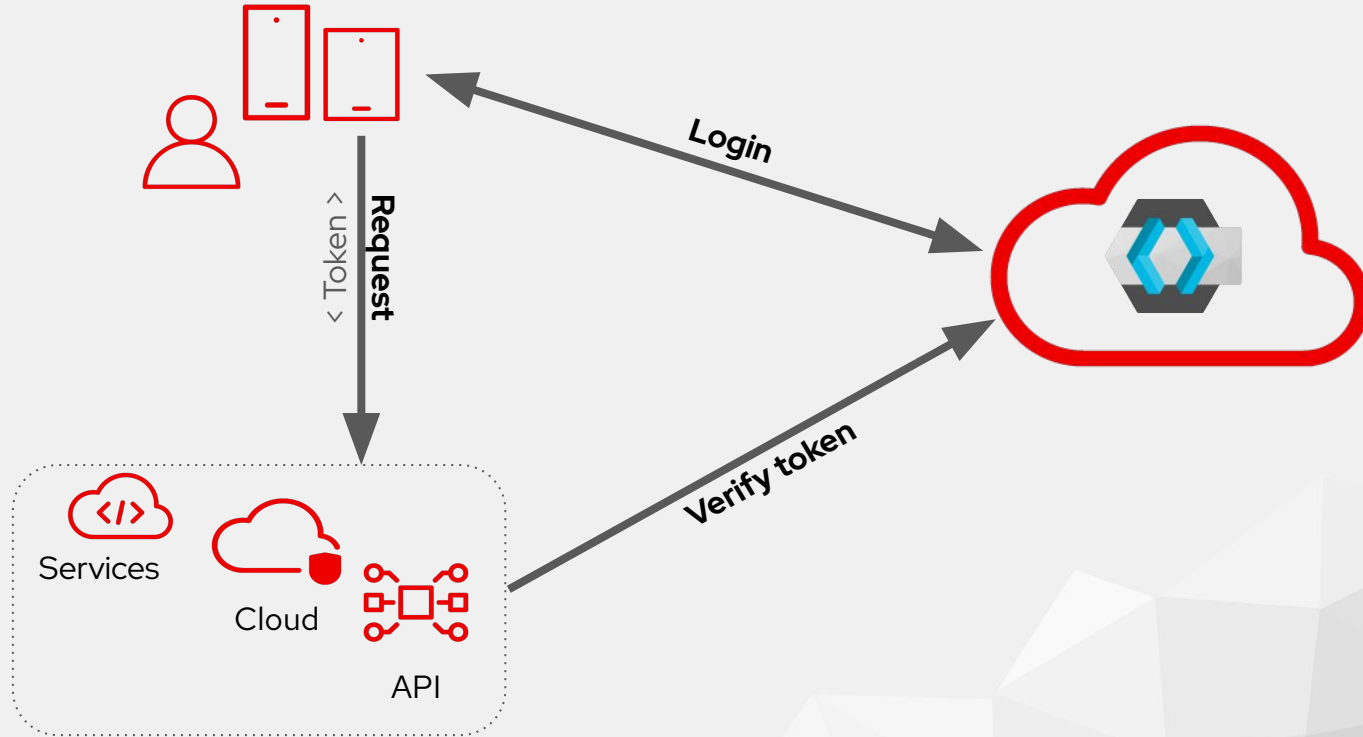
What's new in Keycloak, the open source IAM?

Alexander Schwartz | Principal Software Engineer | Red Hat

What's new in Keycloak, the open source IAM? | 2024-08-18

What is Identity and Access Management (IAM), and do I need one?

Authenticate and authorize users for services



Keycloak is an Open Source Identity and Access Management Solution



Initial commit 2013-07-02



Cloud Native Computing Foundation
incubating project April 2023



Apache License, Version 2.0

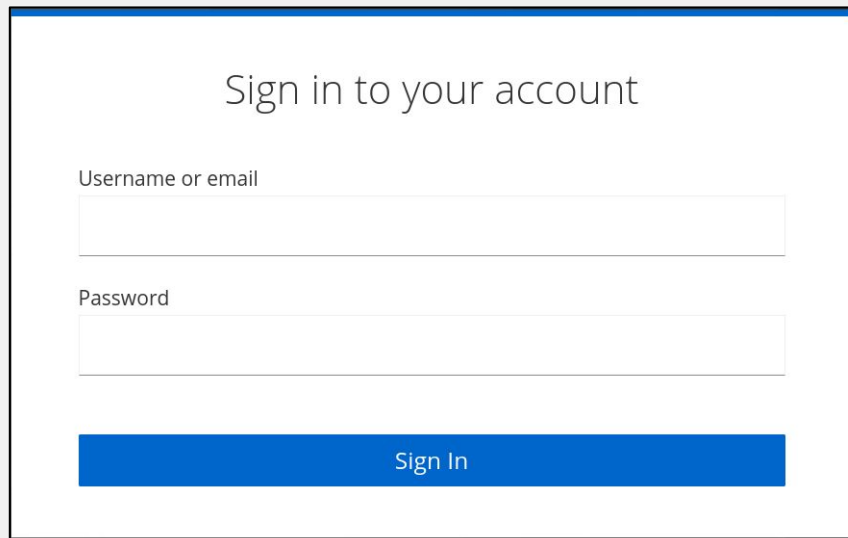
21k GitHub stars

Keycloak at the Beginning

- OpenID Connect Protocol Implementation for the server
- Services and database to store information about clients and identities
- From Developers for Developers

Soon after that:

- Multi Factor authentication
- Client libraries
- SAML, LDAP, ...

A mockup of a Keycloak login form. It features a white background with a blue border. At the top, the text "Sign in to your account" is centered. Below this, there are two input fields: "Username or email" and "Password". Each field has a light gray border and a small blue icon on the left. At the bottom, there is a blue button with the text "Sign In" in white.

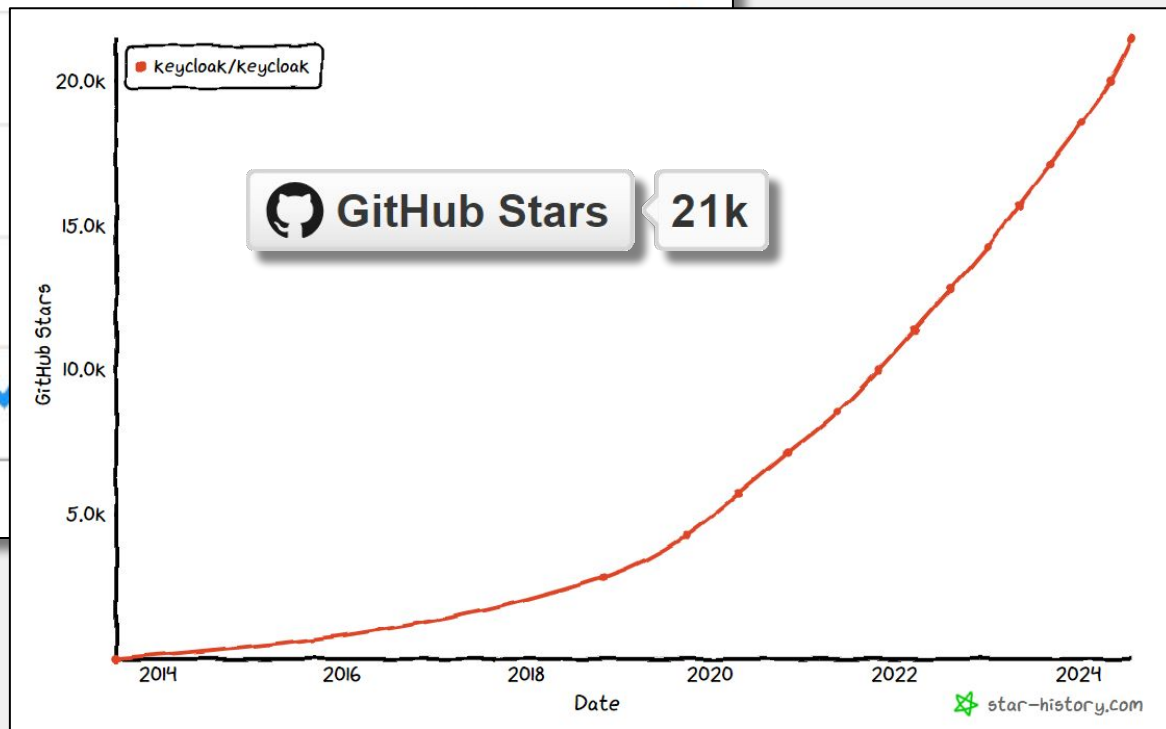
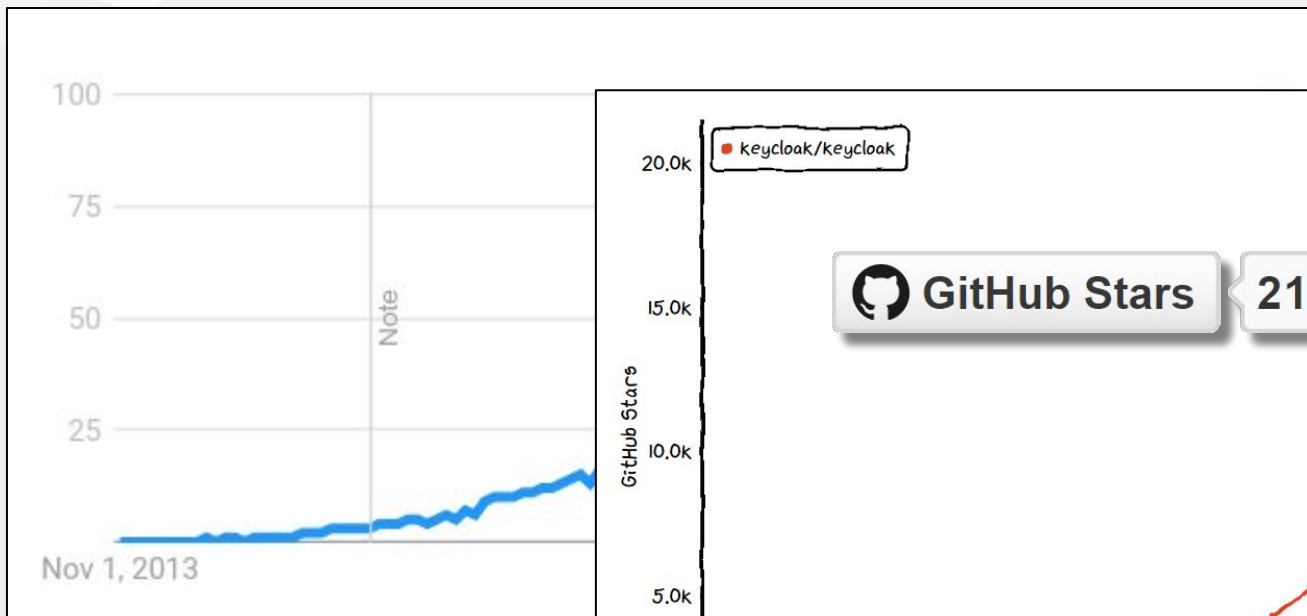
Sign in to your account

Username or email

Password

Sign In

How it grew



A Keycloak Journey

Day 0: Getting started as a developer

Day 1: Single-Sign-On is cool!

Day 2: Become flexible in your setup

Day 3: Eliminate daily churn

Day 0: Getting started as a developer

- Run a single container (inside or outside Kubernetes) or extract an archive
 - Works with Testcontainers
 - Configure using CLI, API, Web UI or export/import a realm using JSON for identical environments
- ➔ Makes sense already for a single application!

Running Keycloak as a developer

```
docker run --name keycloak -p 8080:8080 \  
  -e KEYCLOAK_ADMIN=admin \  
  -e KEYCLOAK_ADMIN_PASSWORD=change_me \  
  quay.io/keycloak/keycloak:latest \  
  start-dev
```

```
docker run --name keycloak_w_import -p 8080:8080 \  
  -e KEYCLOAK_ADMIN=admin \  
  -e KEYCLOAK_ADMIN_PASSWORD=change_me \  
  -v /path/to/realm/data:/opt/keycloak/data/import \  
  quay.io/keycloak/keycloak:latest \  
  start-dev --import-realm
```

Starting Keycloak, Quarkus Edition

start-dev	start	build	start --optimized
Development	Simple Deployment	Prepare Deployment	Performant Deployment
<ul style="list-style-type: none">• Medium Performance• Not secure/no TLS	<ul style="list-style-type: none">• TLS Certificates required• Slow start• Good run-time performance	<ul style="list-style-type: none">• Build configuration known (database, features, ...)	<ul style="list-style-type: none">• TLS Certificates required• Fast start• Good run-time performance

Day 1: Single-Sign-On is cool!

- Users need to remember only one password
- Authenticate only once per day
- Add second factor for authentication for security
- Theme the frontend to match your needs

➡ Makes sense already for a single application!

Make first contact with Keycloak

Sign in to your account

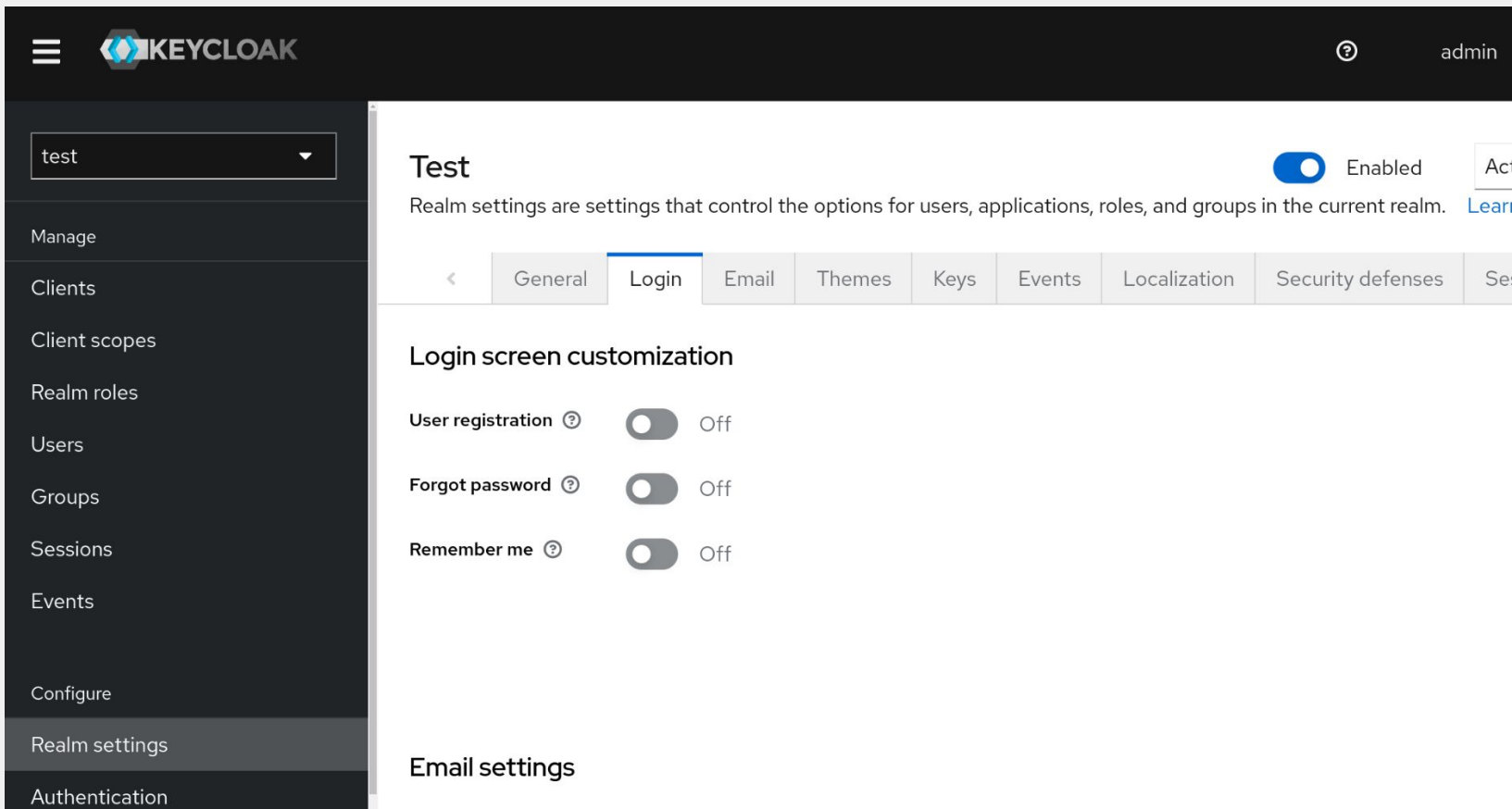
Username or email

Password

Sign In

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.' Below the description is a horizontal tab bar with options: 'General', 'Login' (selected), 'Email', 'Themes', 'Keys', 'Events', 'Localization', 'Security defenses', and 'Sessions'. The 'Login' tab contains a section titled 'Login screen customization' with three settings: 'User registration' (Off), 'Forgot password' (Off), and 'Remember me' (Off). Each setting has a toggle switch and a help icon. At the bottom of the main content area, the 'Email settings' section is partially visible.

test

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

KEYCLOAK

admin

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

Login screen customization

User registration ? Off


Forgot password ? Off

Remember me ? Off

Email settings

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

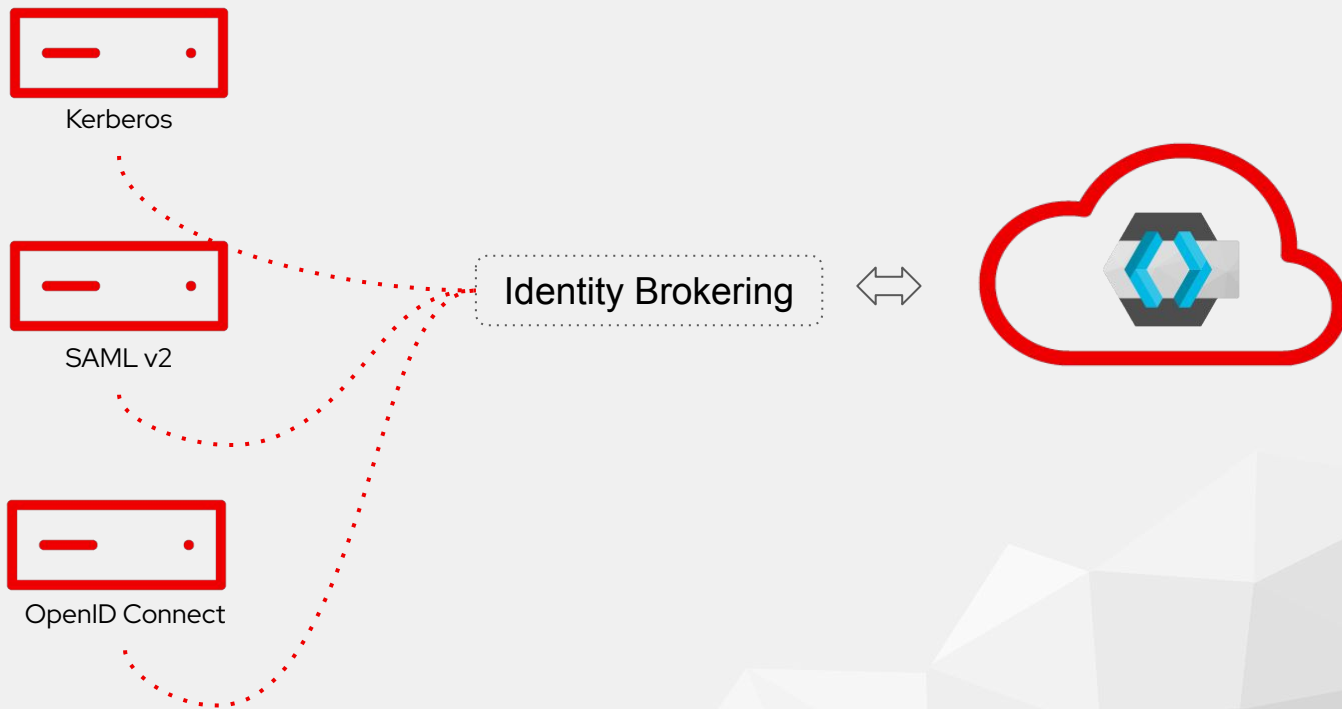
```
apiVersion: k8s.keycloak.org/v2alpha1
kind: Keycloak
metadata:
  labels:
    app: keycloak
  name: keycloak
  namespace: ...
spec:
  hostname:
    hostname: keycloak...
  additionalOptions:
    - name: db
      value: postgres
    - name: db-url
      value: jdbc:postgresql://...
    - name: db-pool-min-size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

Day 2: Become flexible in your setup

- Integrate LDAP and Kerberos
- Brokerage to existing SAML services
- Brokerage to existing OIDC services
- Integrate existing custom stores
- SCIM integration

➔ Reuse the existing user infrastructure!

Brokerage to existing services



Skip the form with Kerberos/SNPEGO!

This page intentionally left blank.

... and use other providers ...





Sign in to your account


Username or email

Password

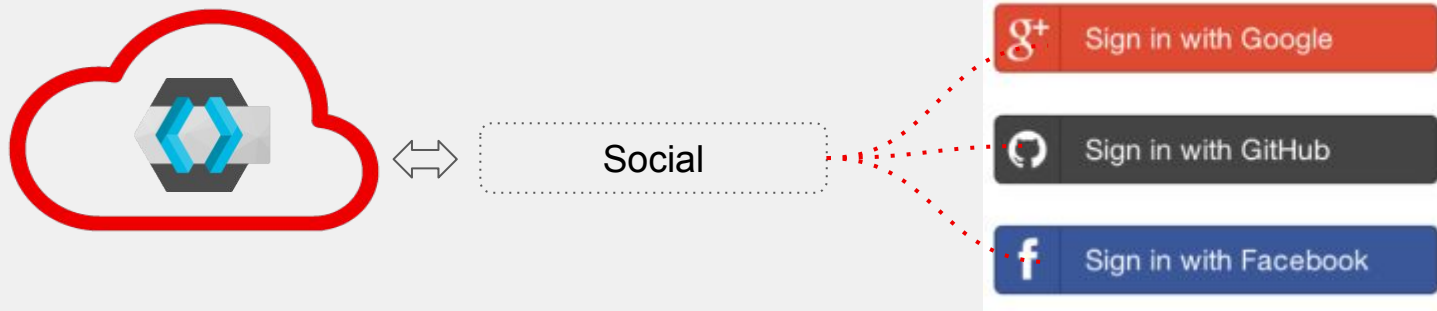
Sign In

Or sign in with

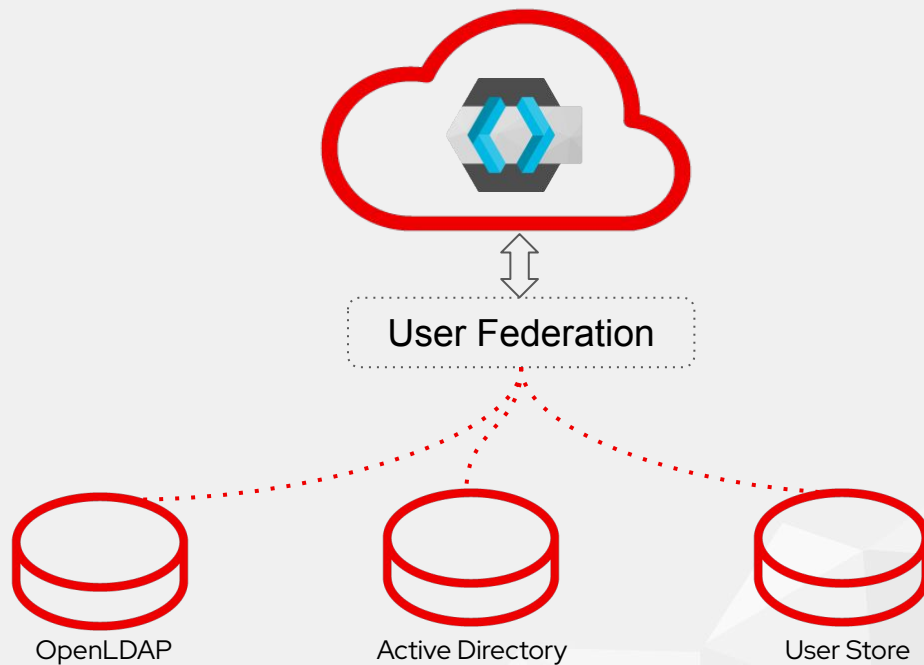
 GitHub	 OpenShift v4
 StackOverflow	 Google



Use social logins to authenticate



Use existing user directories via federation



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.

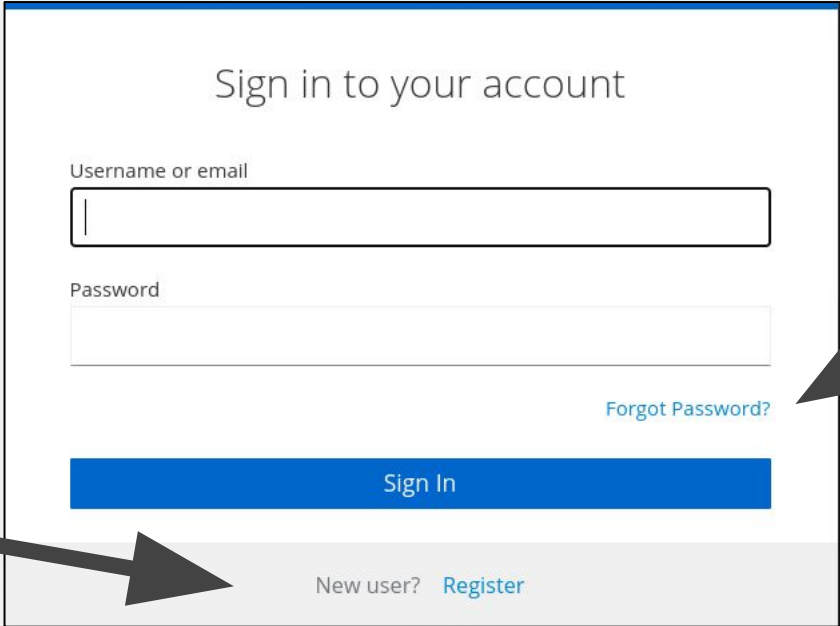
To add a custom REST endpoint, you need to implement the `RealmResourceProvider` interfaces. `RealmResourceProvider` has on

Day 3: Eliminate daily churn

- User required actions
- User password recovery (even when using LDAP)
- Self-registration for users
- User data self-management

➔ Resolve the need for calls and tickets!

The login screen can do a lot more!



Sign in to your account

Username or email

Password

[Forgot Password?](#)

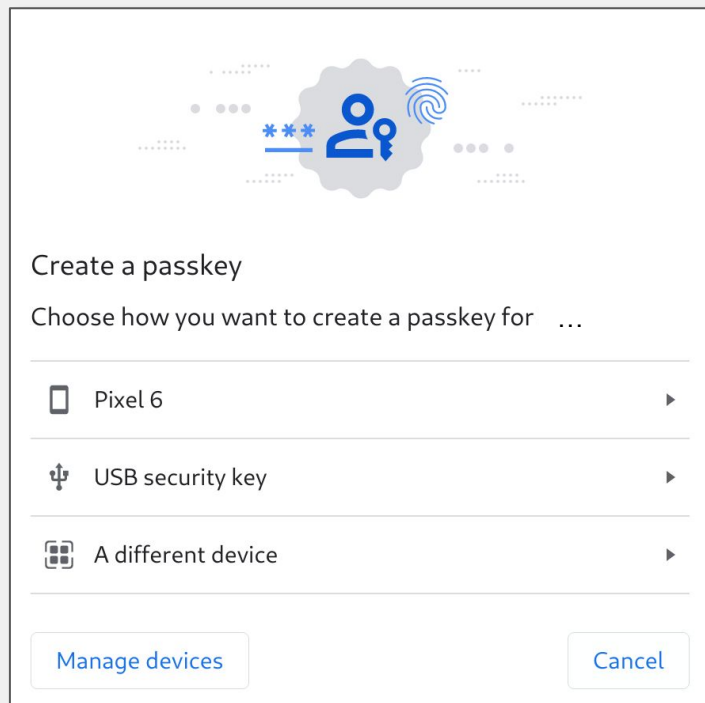
[Sign In](#)

New user? [Register](#)

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 icon, and 'A different device' with a 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

A Keycloak Journey

Day 0: Getting started as a developer

Day 1: Single-Sign-On is cool!

Day 2: Become flexible in your setup

Day 3: Eliminate daily churn

Keycloak is an Open Source Identity and Access Management Solution

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

Keycloak Book: 2nd Edition!

Based on Keycloak 22 and Quarkus: new and improved user experience and a new admin console with a higher focus on usability. You will see how to leverage Spring Security, instead of the Keycloak Spring adapter while using Keycloak 22.



EXPERT INSIGHT

Keycloak – Identity and Access Management for Modern Applications

Harness the power of Keycloak, OpenID Connect, and OAuth 2.0 to secure applications

Second Edition



Stian Thorgersen
Pedro Igor Silva

<packt>

Highlights Keycloak 24

- Passkey support evolving
- **Load Shedding and Non-Blocking Probes**
- **Multi-site support with blueprints**
- Sizing Guide
- Quarkus 3.8
- **User Profile**
- Simplified truststore handling
- Extending the Admin UI via SPI (experimental)

Loadshedding

Well-behaving even when the system receives more requests than it can handle.

Loadshedding

Well-behaving even when the system receives more requests than it can handle.

Action	Behavior before	Behavior after
Incoming requests	Requests queue up, delayed response, client times out.	Limit the queue, fail fast for excessive requests*

* needs to be configured via `http-max-queued-requests`

Loadshedding

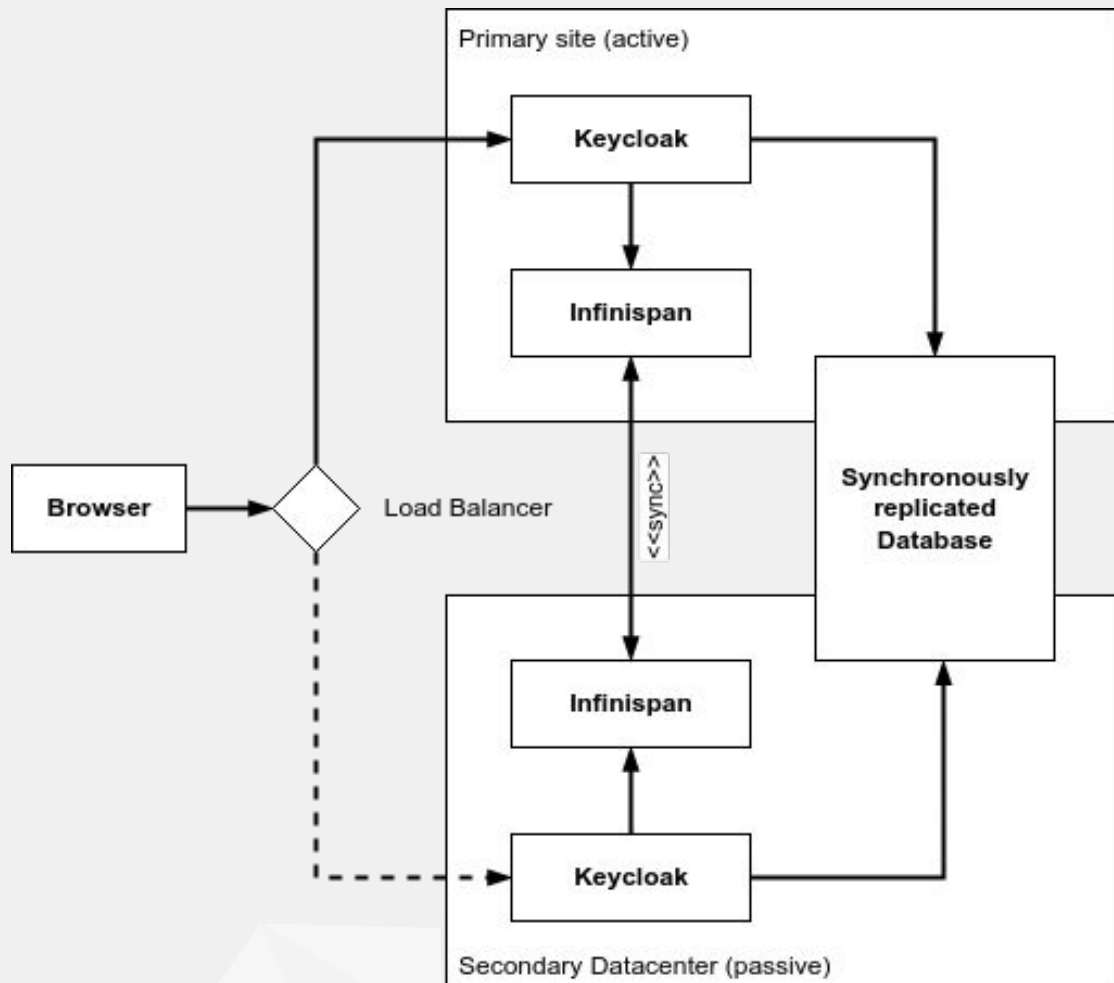
Well-behaving even when the system receives more requests than it can handle.

Action	Behavior before	Behavior after
Incoming requests	Requests queue up, delayed response, client times out.	Limit the queue, fail fast for excessive requests*
Liveness probe	Timeout, Pod restarted by Kubernetes	Non-Blocking, Pod survives

* needs to be configured via `http-max-queued-requests`

Multi-Site support

- Synchronous database and Infinispan to avoid data loss
- Low-latency network between sites to avoid long response times
- Active-passive to avoid potential deadlocks in Infinispan



Multi-Site support

Improvements not only for multi-site setups:

- Sizing Guide (memory, CPU, threads)
- Simplified configuration for a typical external Infinispan setup
- Automated load and failure tests
- Protection against cache stampedes
- AWS Aurora PostgreSQL Multi AZ support (in progress)
- Infinispan and JGroups hardening

Declarative User Profile configuration

<

General

Login

Email

Themes

Keys

Events

Lo

AttributesAttributes GroupJSON editor

▼ All groups

Create attribute

Attribute [Name]	Display name
<div>⋮</div> username	\${username}
<div>⋮</div> email	\${email}
<div>⋮</div> firstName	\${firstName}
<div>⋮</div> lastName	\${lastName}

Permission

Who can edit? ⓘ

✓

User

✓

Admin

Who can view? ⓘ

✓

User

✓

Admin

Validations

Validator name	Config
length	{ "min":3, "max":255 }
username-prohibited-characters	{ }
up-username-not-idn-homograph	{ }

User Profile for admins, registration, and users

General

Username *


Email


First name

Last name

Register * Required fields

Username *

Password * 

Confirm password * 

Email *

First name *

Last name *

[« Back to Login](#)

Personal info
Manage your basic information

General

Username *

Email *

First name *

Last name *

Highlights Keycloak 25

- Argon2 password hashing
- Simplified hostname configuration
- Persistent user sessions (preview)
- Passkeys improvements (preview)
- Separate management port for health and metrics
- **Organizations (preview)**
- OpenJDK 21

Organisations

[Organizations](#) > Organization details

myorg ☒ Enabled Action ▾

[Settings](#) [Attributes](#) [Members](#) [Identity providers](#)

Name *

Alias ?

Domain ? ⊖

[+ Add domain](#)

Description

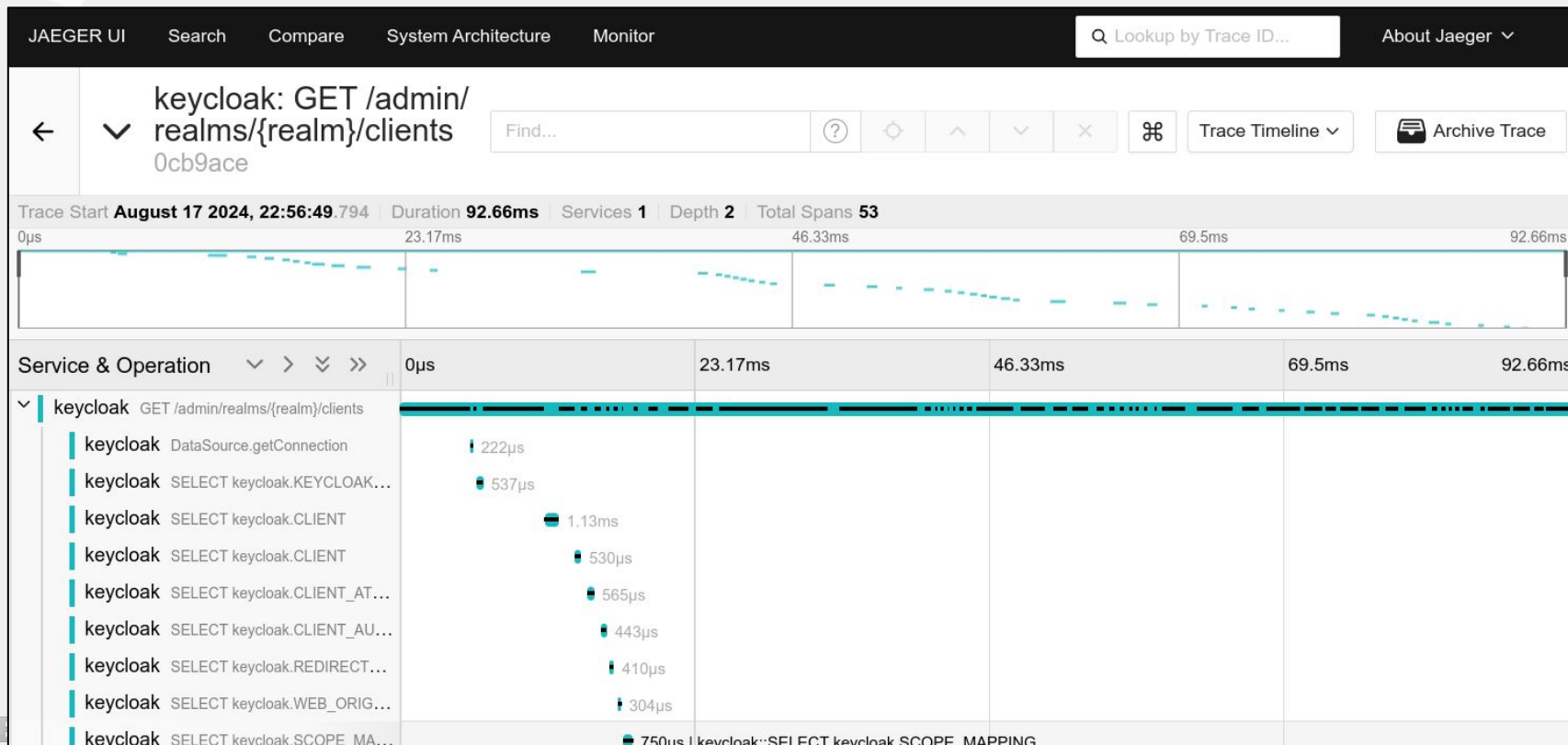
[Save](#) [Reset](#)

Highlights Keycloak 26*

- Infinispan marshalling changed to ProtoStream
- Quarkus 3.15.x
- Persistent User sessions (by default)
- Keycloak multi-site setup in Active/Active mode
- Keycloak Admin user recovery
- **OpenTelemetry tracing support (preview)**
- Removal of legacy cookies
- Organizations continued

* Subject to change

OpenTelemetry Tracing



Conferences & Events



KeyConf24



Vienna (AT) & Online



2024-09-19

<https://keyconf.dev/>

KubeCon North America



Salt Lake City (US)



2024-11-12...15

<https://events.linuxfoundation.org/>



Keycloak DevDay



Darmstadt (DE)



2025-03-06

<https://keycloak-day.dev/>

Meetup Keycloak Hour of Code



Online



Every 1-2 months

[https://www.meetup.com/
keycloak-hour-of-code/](https://www.meetup.com/keycloak-hour-of-code/)



Community Links



Keycloak

<https://keycloak.org/>

CNCF Slack

#keycloak

#keycloak-dev

<https://slack.cncf.io/>



Keycloak Community

Discourse Forum

GitHub Discussion

Mailing Lists

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

Keycloak OAuth SIG

#keycloak-oauth-sig

<https://github.com/keycloak/kc-sig-fapi>



Links

- **Keycloak**
<https://www.keycloak.org/>
- **Keycloak Nightly Release**
<https://github.com/keycloak/keycloak/releases/tag/nightly>
- **Keycloak Book 2nd Edition**
<https://www.packtpub.com/product/kc/9781804616444>
- **Keycloak High Availability**
<https://www.keycloak.org/high-availability/introduction>
- **Keycloak Benchmark**
<https://www.keycloak.org/keycloak-benchmark/>
- **Extend Admin UI via SPI**
<https://github.com/keycloak/keycloak-quickstarts/tree/main/extension/extend-admin-console-spi>
- **Keycloak Hour of Code**
<https://www.meetup.com/keycloak-hour-of-code/>


Contact



Alexander Schwartz
Principal Software Engineer

aschwart@redhat.com

<https://www.ahus1.de>

 @ahus1de

 @ahus1@fosstodon.org