Keycloak - recently added features

Marek Posolda
Keyconf 2023

Focus on key non-functional requirements

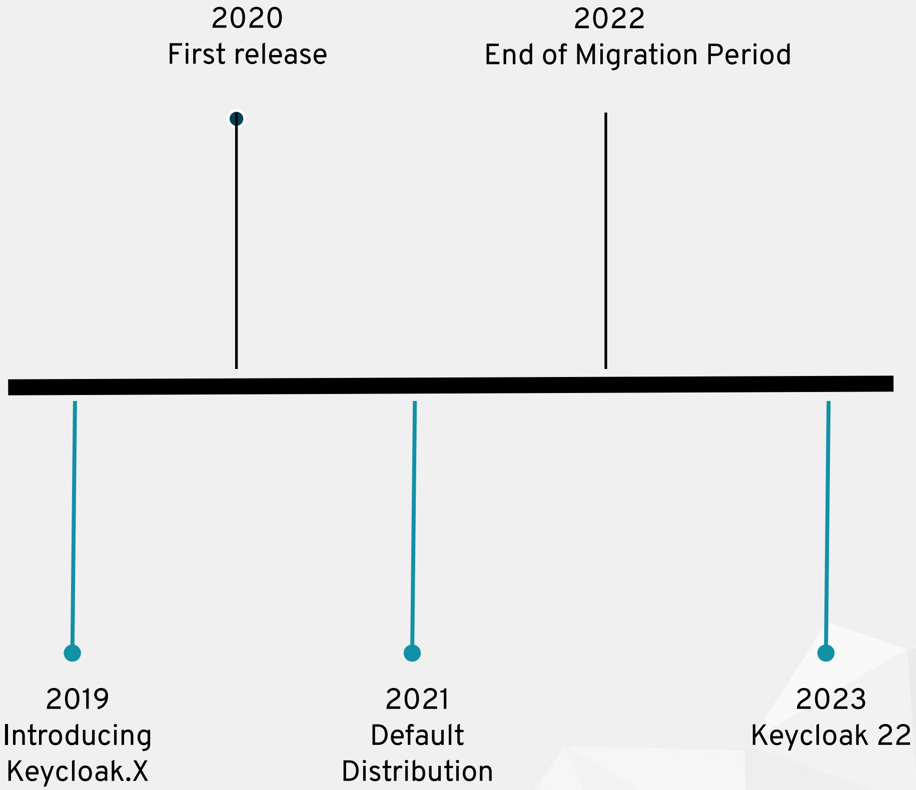
- **Usability**
  - Self-descriptiveness
  - Simplified Configuration

Keycloak on Quarkus

Keycloak on Quarkus

- Keycloak server deployed on Quarkus now
- Previously, main Keycloak distribution was deployed on Wildfly since early Keycloak

A bit of history …



2019
Introducing Keycloak.X

2020
First release

2021
Default Distribution

2022
End of Migration Period

2023
Keycloak 22

Focus on key non-functional requirements

- **Cloud-Friendly**
  - Faster start-up time and low memory footprint
  - Software efficiency ➡ Reduce costs
  - Reduced and constrained container images
  - Immutability

Unified configuration experience

- Well-defined configuration options and documentation
  - https://www.keycloak.org/server/all-config
- Cross-environment configuration format
  - On-premise

    ```
    $ kc.sh start --db=postgres --db-url-host=mypostgres
    ```

  - Container

    ```
    $ podman  run quay.io/keycloak/keycloak start --db=postgres --db-url-host=mypostgres
    ```

  - Kubernetes

    ```
    containers:
            - name: keycloak
              image:
    quay.io/keycloak/keycloak:21.1.1
              args: ["start"]
              env:
                - name: KC_DB
                  value: "postgres"
                - name: KC_DB_URL_HOST
    ```

Support for Multiple Configuration Sources

- Configuration can be set using
  - CLI
    - --http-port
  - Environment Variables
    - KC_HTTP_PORT
  - Configuration File (defaults to conf/keycloak.conf)
    - http-port
  -

Providers/SPI configuration

- Basic configuration parameters are useful for most of the typical use-cases
- More advanced use-cases may need configure specified SPI
- Any SPI previously configurable in standalone.xml can be also configured by CLI, environment variable or configuration file
- Example:
  - ./kc.sh start --spi-password-hashing-pbkdf2-sha256-max-padding-length=14
  - Configuration of option “max-padding-length” of provider “pbkdf2-sha256” of SPI “password-hashing”

New UI

New admin console

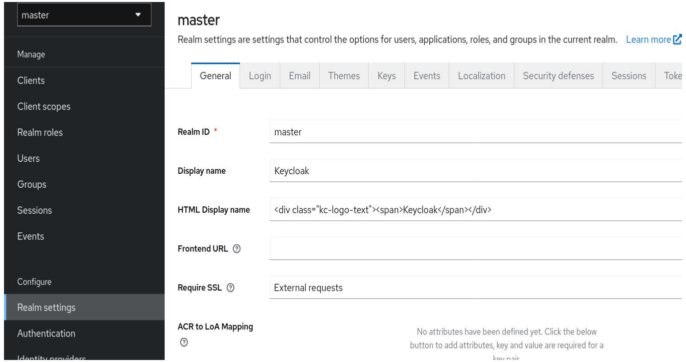
- New admin console based on Patternfly 3
- Improved UI and usability
- Old admin console was deprecated in Keycloak 19 and removed in Keycloak 21

New account console

- Improved UI for logged-in users
- Added in Keycloak 12
- Old account console is going to be removed in Keycloak 22

Main Changes

Admi
n



master ▾

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

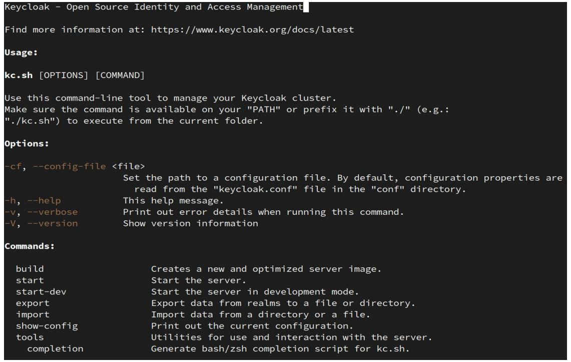
master

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

General | Login | Email | Themes | Keys | Events | Localization | Security defenses | Sessions | Toke

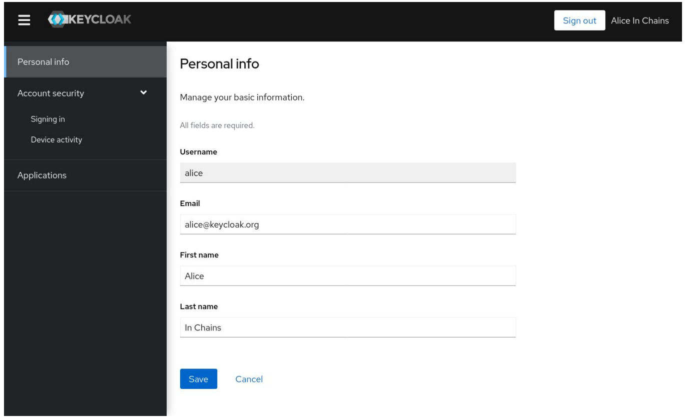
Realm ID *	master
Display name	Keycloak
HTML Display name	<div class="kc-logo-text"><span>Keycloak</span></div>
Frontend URL ⓘ	
Require SSL ⓘ	External requests
ACR to LoA Mapping ⓘ	No attributes have been defined yet. Click the below button to add attributes, key and value are required for a key pair

Operation



```
Keycloak - Open Source Identity and Access Management

Find more information at: https://www.keycloak.org/docs/latest

Usage:

kc.sh [OPTIONS] [COMMAND]

Use this command-line tool to manage your Keycloak cluster.
Make sure the command is available on your "PATH" or prefix it with "./" (e.g.:
"./kc.sh") to execute from the current folder.

Options:

-cf, --config-file <file>
                     Set the path to a configuration file. By default, configuration properties are
                       read from the "keycloak.conf" file in the "conf" directory.
-h, --help           This help message.
-v, --verbose        Print out error details when running this command.
-V, --version        Show version information

Commands:

  build                   Creates a new and optimized server image.
  start                   Start the server.
  start-dev               Start the server in development mode.
  export                  Export data from realms to a file or directory.
  import                  Import data from a directory or a file.
  show-config             Print out the current configuration.
  tools                   Utilities for use and interaction with the server.
    completion            Generate bash/zsh completion script for kc.sh.
```

Users



KEYCLOAK

Sign out Alice In Chains

Personal info

Account security

Signing in

Device activity

Applications

Personal info

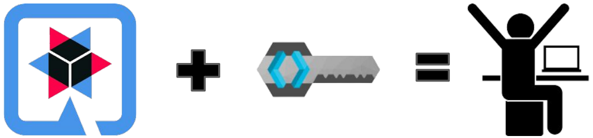
Manage your basic information.

All fields are required.

Username	alice
Email	alice@keycloak.org
First name	Alice
Last name	In Chains

Save Cancel

Dev



FIPS 140-2

What is FIPS 140-2?

- The Federal Information Processing Standard Publication 140-2, (FIPS 140-2)
- U.S. government computer security standard used to approve cryptographic modules
- Keycloak supports to run in FIPS 140-2 compliant mode. In this case, Keycloak will use only FIPS approved cryptography algorithms for it’s functionality

System requirements

- FIPS 140-2 adds restrictions on cryptography algorithms, which can be used internally by Keycloak
- Possibly also restrictions on key sizes etc
- Keycloak should run on FIPS enabled system (RHEL, Fedora), which means that Java itself is set in FIPS enabled way (only FIPS compliant security providers etc)

BouncyCastle FIPS

- Keycloak uses BouncyCastle library for lots of it’s cryptography functionalities
- Default BouncyCastle library needs to be replaced with FIPS flavour (BCFIPS)
- Administrator should do it by himself as Keycloak is not bundled with BCFIPS
- Run Keycloak with –features=fips –fips-mode=enabled|strict
- Strict mode uses “BCFIPS approved mode” - more restrictions on cryptography algorithms

Affected Keycloak functionality?

- Default RSA key sizes requires size 2048 bits or more (by default 1024 bits are allowed)
- JKS keystores/truststores not supported. Strict mode currently supports only BCFKS keystores/truststores (no PKCS12 keystores support)

Other improvements

Feature Update

- **Authentication**
  - Step-up Authentication
  - Client Secret Rotation - preview
  - Recovery Codes - preview
  - Update user’s email upon user confirmation - preview
  - Improvements to WebAuthn Resident Keys, paving the road for *Passkey* support

Other non-functional updates

- Java 17 support for server (Java 11 deprecated and likely removed in Keycloak 22)
- Server uses jakarta instead of JEE (your custom providers might be affected)
- New Operator (written in Java)
- Container image based on ubi9-micro
  - Huge reductions of 3rd party dependencies (and CVEs)

- **Keycloak OpenID Connect Adapters**
- Deprecated, available only for JEE
  - Wildfly/Undertow/Tomcat/Jetty Adapters
  - Spring Adapter
- Focus on leveraging existing OpenID Connect libraries from your language and framework of choice

Q & A