KEYCLOAK

Core Keycloak features developed in past 12 months

Marek Posolda

Keyconf 2024

OpenID CERTIFIED

OAUTH 2

saml xml.org

QUARKUS

CLOUD NATIVE COMPUTING FOUNDATION

About myself

- Marek Posolda, Red Hat employee
- Brno, Czech republic
- Software engineer in Keycloak since 2013
- Working especially on the core parts (authentication, protocols, clients)

Keycloak 23 - 26 releases

Core features

- Supported User Profile and progressive profiling
  - Supported since Keycloak 24
  - Details & demo later

- Organizations (B2B support)
  - Preview since 25. Supported by default probably since 26
  - Details & demo later

OIDC & OAuth

- Lightweight access tokens support
- OAuth 2.1, FAPI 2 drafts support
- Supporting EdDSA as signature algorithm
- DPoP preview support
- OAuth Grant Type SPI
- OID4VCI - experimental support

Most of Java adapters removed

- All Java OIDC adapters removed in Keycloak 25. The javascript and node.js adapter are the only OIDC adapters still supported (Node.js adapter deprecated)

- Most of SAML adapters removed (Jakarta, Jetty, Servlet filter). The exception are adapters for the new Jakarta based Wildfly server and for EAP 8

UI updates

- New WelcomePage and Account console V3, Account console V2 removed
- New Login theme (Login V2). Login V1 theme deprecated since Keycloak 26
- Admin, Account and Welcome page upgraded to Patternfly 5

Authentication improvements

- Argon2 default algorithm for hashing of user passwords (except for FIPS env)
  - Better security than PBKDF2 with less CPU
- Passkeys preview support
- Configurable required actions

Distribution updates

- Java 21 support in Keycloak 26 (Java 17 deprecated)
- Versioned features
  - New features will support versioning. Existing features like `account3` are marked as version 1 for compatibility reasons
- Hostname v2 (Hostname v1 deprecated and removed in Keycloak 26)
- OpenTelemetry tracing
  - Tracking performance bottlenecks or application failures

High availability improvements

- High availability guide with blueprints for cloud setups (especially AWS)
- Support for multi-site active-passive deployments
  - essential for some environments to provide high availability and a speedy recovery from failures.
  - Since Keycloak 24
- Active-active setup possibly supported since Keycloak 26

Storage updates

- Persistent user sessions
  - User session backed in the DB and able to survive cluster restarts
  - Preview in 25. Enabled by default since 26

- Persistent revoked access tokens (Ability to survive cluster restarts)

- Offline-session & server startup
  - By default, offline sessions loaded on demand instead of at startup

User profile

User profile

- Supported since Keycloak 24, was preview before
- Allows to restrict which user attributes are available for users and format of the user attributes (User attributes are attributes like email, first name etc).
- Dynamic forms with rendered attributes based on the user profile configuration
- Grouping of attributes on the page
- Specify which attributes are read-only or visible (for regular users or for admins)

User profile - advanced

- Validators for attributes
- Annotations: how are attributes rendered in the UI
- Progressive profiling
  - Specific attribute required/available just for some client applications
  - Implemented by client scopes. Attribute can be required/available just for specific ‘scope’

User profile - demo

- Demo

Organizations

What are our main use cases today?

- Identity and Access Management
  - Business to Employee (B2E)
  - Business to Consumer (B2C)

Keycloak organizations

- Aims to improve on B2B use-cases (Business to business)
- Basic multitenancy approach
- Ability to have client applications and Keycloak available for users managed by the 3rd party organization

Organizations

- Preview since Keycloak 25. Supported probably since Keycloak 26

- Dedicated SPI for CRUD of organizations. CRUD of organizations available by admin REST API

- Keycloak users can be linked to some organization by admin (not by user himself)
  - Managed membership: User removed when link (or organization itself) removed
  - Unmanaged membership: User manually added or invited to organization by admin

Keycloak organizations - authentication

- Authentication flows automatically updated when ‘organization’ feature is enabled
  - Browser flow updated for “identity-first” login
  - First broker login flow updated to link user to the organization as “managed user” as long as user was registered by IDP login

- Organization can be linked to the IDP

- The browser flow can redirect automatically to the IDP of the organization as long as the email domain provided on first screen corresponds to the organization domain

Keycloak organizations - token claims

- Attributes can be added to the organizations
- Attributes added to the tokens as long as authenticated user is member of the organization AND the scope ‘organization’ is available (optional client scope, which can be added to clients)
- The claim ‘organizations’ available automatically by the protocol mapper attached to the client scope above

Keycloak organizations - demo

Q & A