Add user self-management, brokerage and federation to your infrastructure with Keycloak

Alexander Schwartz | Principal Software Engineer | Red Hat
Identity and Access Management devroom | FOSDEM | 2024-02-04
Day 1: Single-Sign-On is cool!
Day 2: Become flexible in your setup
Day 3: Eliminate daily churn
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!
Let Keycloak handle AuthZ and AuthN for your apps
Let’s do a demo of Keycloak!
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 existing user stores!
Brokerage to existing services

Kerberos

SAML v2

OpenID Connect

Identity Brokering
Skip the form with Kerberos/SNPEGO!

This page intentionally left blank.
Use social logins to authenticate
Use existing user directories via federation

- OpenLDAP
- Active Directory
- User Store
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!
Required actions (there’s a lot to choose from!)

<table>
<thead>
<tr>
<th>Required actions</th>
<th>Enabled</th>
<th>Set as default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure OTP</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Terms and Conditions</td>
<td>Off</td>
<td>Disabled off</td>
</tr>
<tr>
<td>Update Password</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Update Profile</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Verify Email</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Delete Account</td>
<td>Off</td>
<td>Disabled off</td>
</tr>
<tr>
<td>Webauthn Register</td>
<td>On</td>
<td>Off</td>
</tr>
</tbody>
</table>
Password recovery and self-registration
User Profile configuration

- **Attributes**
  - Name: username
    - Display name: ${username}
  - Name: email
    - Display name: ${email}
  - Name: firstName
    - Display name: ${firstName}
  - Name: lastName
    - Display name: ${lastName}

- **Permission**
  - Who can edit: User, Admin
  - Who can view: User, Admin

- **Validations**
  - **Validator name**: length
    - Config: {"min":3,"max":255}
  - **Validator name**: username-prohibited-characters
    - Config: {}
  - **Validator name**: up-username-not-idn-homograph
    - Config: {"min":3,"max":255}
User Profile for admins, registration, and users
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 Benchmark
  https://github.com/keycloak/keycloak-benchmark
- 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