Documentação de conhecimento do Keycloak

Joyce Gregório da Silva

Novembro de 2025
Esperança-PB

1. **O que é o Keycloak?**

O keycloak é uma ferramenta open source utilizada para gestão de identidade e controle de acesso, possuindo código aberto oferecendo autenticação e autorização para sistemas. Seus recursos englobam:

- **Autenticação centralizada:** Permitindo a autenticação dos usuários em diversos sistemas a partir de um único login;
- **Autorização e controle de acesso:** Oferece mecanismos para definição de acesso com suporte a funções e mecanismos de segurança;
- **Integração com provedores de identidade externos:** Pode ser integrado com provedores como google, facebook dentre outros permitindo a autenticação a partir das contas criadas nessas fontes;
- **Suporte a protocolos de segurança:** A ferramenta é compatível com protocolos de autenticação mais utilizados, facilitando a integração com diversas plataformas.

Vamos utilizar no produto de atendimento da APAE a versão mais atual, sendo ela a 26.4.2. Nesta versão, a autenticação pode acontecer sem a utilização de senhas, apenas com as validações das contas contidas em ferramentas como o google sendo essa a pretensão inicial.

2. **Alguns conceitos básicos e essenciais para a utilização do keycloak**

O keycloak utiliza alguns conceitos e nomeações para seus recursos, como:

- Realm: É o domínio onde os usuários, credenciais, funções e clientes são gerenciados.
- Client: O termo client refere-se às “aplicações” ou “clientes” configurados dentro do realm, os quais interagem com os recursos e permissões associadas. Como por exemplo os fronts e backs das aplicações
- Role: A role é um conjunto de permissões que podem ser atribuídas de forma específica a um client ou ao realm.
- Group: Um group é uma estrutura organizacional que permite a criação de conjuntos de configurações, as quais podem ser aplicadas

de maneira centralizada, evitando a necessidade de repetição para cada usuário individual. Exemplo: Grupo “Departamento Pessoal”.

- User: O conceito de user refere-se ao cadastro de usuários que acessam os clients
- Identity Providers: Os Identity Providers referem-se a provedores de identidade externos à organização, permitindo que os usuários realizem seu próprio cadastro por meio de métodos como login via Google, Facebook, LinkedIn, entre outros.
- User Federation: A User Federation consiste em uma integração com bases de dados externas, possibilitando a vinculação dessas fontes ao Keycloak.

3. Funcionamento do keycloak

1. Usuário entra na URL da aplicação
2. A aplicação faz o redirecionamento para a página de login do Keycloak
3. Usuário insere as credenciais
4. Keycloak valida o usuário
5. Caso válido, redireciona para a aplicação, caso inválido é retornado a página de login

4. Utilizando o keycloak no docker

A utilização do keycloak no docker é realizada a partir de alguns comandos.

A iniciação começa com a inserção do comando:

```
docker run -p 127.0.0.1:8080:8080 -e KC_BOOTSTRAP_ADMIN_USERNAME=admin -e KC_BOOTSTRAP_ADMIN_PASSWORD=admin quay.io/keycloak/keycloak:26.4.2 start-dev
```

Esse comando inicia de fato o keycloak criando um usuário uma senha tendo como padrão o `admin` para ambos os parâmetros. Após essa configuração, é necessário entrar na porta local direcionada pelo keycloak, geralmente a porta 8080.

A partir disso, fazer login no console de administração do keycloak e seguir todos os comandos elencados na documentação do keycloak para a criação do realm que seria utilizado para gerenciar o keycloak no nosso produto: https://www.keycloak.org/getting-started/getting-started-docker.

5. Vídeos que vão auxiliar no entendimento do keycloak e seu funcionamento:

Os vídeos foram selecionados a partir das datas de publicação buscando ser o mais atual possível e compatível com o nível de lançamento da versão do keycloak.

- Utilização do keycloak a partir do doker compose: https://youtu.be/MSBeLYadqt8?si=5A06Y_Kq7rELx_7M; https://youtu.be/LJarozXEblg?si=v6qAWQ5zhFVZ1GTb
- Componentes de arquitetura do keycloak: https://youtu.be/JNDVEp3m_rs
- OAuth Client Credentials com Java, Spring Boot e Keycloak: https://youtu.be/BoPLhhIN9ks?si=xh_zsYPccgbrAxS2

6. Integrações com back-end Spring Boot e front-end React

A integração do Keycloak em uma arquitetura com back-end em Spring Boot e front-end em React divide claramente as responsabilidades de segurança. O front-end atua na interação com o usuário para a autenticação, enquanto o back-end se concentra em proteger os dados e a lógica de negócio.

Para a integração com o spring boot o fluxo irá funcionar em 3 pontos:

1. O spring boot assume o papel de servidor de recursos, tendo como responsabilidade proteger os endpoints estabelecidos na API, delegando as tarefas ao front-end. Sendo assim, primeiro ocorre a validação do token que irá acontecer a cada nova requisição dos endpoints, a aplicação irá aguardar a geração do token de acesso respectivo.
2. Buscar a segurança do emissor do token: neste ponto vai ser utilizado o módulo Spring Security OAuth2 Resource Server, a aplicação é configurada para confiar apenas nos tokens emitidos pelo seu realm específico no Keycloak. Ela faz isso validando a assinatura criptográfica do token com as chaves públicas que o Keycloak disponibiliza.
3. Por fim, após a validação do token e obter a confirmação de confiança do mesmo, o Spring Security inspeciona as informações contidas nele, como os papéis do usuário, podendo ser o padrão que é o admin ou user. Com base nessas roles, a aplicação pode conceder ou negar o acesso a determinados endpoints, permitindo um controle de acesso. Em resumo, o spring boot vai atuar exigindo credenciais que confirmem a validação do token.

A integração com o front-end tem o papel de orquestrar a autenticação do usuário no sistema, sendo feita em 4 passos:

1. Início do Fluxo de Login: Quando um usuário tenta acessar uma área protegida da aplicação, a biblioteca do Keycloak detecta que ele não está autenticado e o redireciona automaticamente para a página de login do Keycloak. A aplicação React em si não constrói ou exibe formulários de login; ela delega 100% dessa interface ao Keycloak, o que centraliza e padroniza a experiência de login.
2. Gerenciamento de Tokens: Após o usuário se autenticar com sucesso no Keycloak, ele é redirecionado de volta para a aplicação React. O Keycloak inclui um código especial na URL de retorno, que a biblioteca `keycloak-js` utiliza para obter os tokens de acesso.
3. Comunicação com o Back-end: Com os tokens em mãos, a aplicação React pode agora fazer chamadas para a API protegida do Spring Boot. A cada chamada, ela anexa o acesso do token no cabeçalho `Authorization` no formato `Bearer <token>`. É este token que o back-end irá validar.
4. Gerenciamento da Sessão: A biblioteca também gerencia o ciclo de vida da sessão do usuário no front-end, como renovar o *access token* silenciosamente usando o *refresh token* antes que ele expire, garantindo uma experiência de uso fluida e sem interrupções.

7. Considerações finais

A adoção do Keycloak representa uma decisão estratégica para a modernização e segurança do produto de atendimento da APAE, buscando centralizar a gestão de identidades e o controle de acesso a ferramenta, removendo a complexidade da autenticação e autorização das mãos da equipe de desenvolvimento, delegando essa responsabilidade a uma solução robusta, especializada e em conformidade com os principais protocolos de mercado. Conforme detalhado, a arquitetura com React no front-end e Spring Boot no back-end exemplifica essa separação de papéis, onde cada componente possui uma responsabilidade clara e bem definida. O resultado é um sistema mais seguro, escalável e de manutenção simplificada, permitindo que os desenvolvedores foquem na entrega de valor para o negócio em vez de se preocuparem com os pormenores da segurança. Em suma, o Keycloak não é apenas uma ferramenta, mas um pilar fundamental para a construção de uma aplicação moderna, segura e preparada para o futuro.

8. Referências

Autores do keycloak.Keycloak.Documentation. Acesso em 02 de novembro de 2025. Disponível em https://www.keycloak.org/documentation.

Autores do keycloak. Keycloak. Docker. Acesso em outubro de 2025. Disponível em https://www.keycloak.org/getting-started/getting-started-docker.

VALIM, Júlia. Vantico. Um guia para o keycloak e suas vulnerabilidades de segurança. Acesso em 03 de novembro de 2025. Disponível em https://vantico.com.br/guia-para-keycloak-e-vulnerabilidades/.

ARAVINDA, Isura. Medium. Integrando a autenticação Keycloak com o Spring Boot: um guia completo. Acesso em 03 de novembro de 2025. Disponível em https://medium.com/@iaravinda33/integrating-keycloak-authentication-with-spring-boot-a-complete-guide-98df2c8d244a.

TORRUBIA, Salva. DEV. Integração do React com o Keycloak: Autenticação segura para o backend existente. Acesso em 03 de novembro de 2025. Disponível em https://dev.to/saltorgil/react-keycloak-integration-secure-auth-for-existing-backend-182b.