Approval System for Keycloak

Keycloak is a highly configurable open-source single sign-on server. In complex deployment environments, Keycloak can be managed by a team of administrators with hierarchical organizational structure and different access levels. Each of them then can be responsible for different parts of the server's configuration. E.g. one can be responsible for creating new users (like employees), other for managing user roles and groups and assigning access rights to them and the third could be a master supervising admin which can do all of it. Some of the changes to the server's configuration could be even done by the end-users., e.g. a user can self-register to the system and create an account on their own.

- Study Keycloak and its codebase.
- Research the possibilities for Keycloak Approval System.
    - This system would be able to intercept selected server's configuration-changing events, such as creating/registering a new user, user self-requests adding to a group and other settings changes in general.
    - Such events/changes won't be propagated at once but instead an approval request would be created.
    - Changes go into effect after the approval request is approved.
    - This behavior should be configurable – what action performed by who should require an approval and who will approve it?
- Design and implement a highly extensible SPI to Keycloak for such Approval System as well as example implementation of this SPI (e.g. approvals for user creation/registration).

In mentioned complex systems, Keycloak could be deployed alongside JBoss BPM Suite which is a powerful platform for business process management.

In the second part of the thesis:

- Study JBoss BPM Suite (BPMS).
- Research the possibilities for integrating the Keycloak Approval System to BPMS processes.
    - It would make sense to handle (to some extent) an approval request from within a business process, so the final approve/reject decision could be made based on a (complex) process logic. This would make the Approval System much more agile.

Cílem práce je vytvoření systému pro schvalování změn v konfiguraci serveru Keycloak. Keycloak je open source projekt vyvíjený společností Red Hat, který zprostředkovává single sign-on autentizaci a autorizaci uživatelů.

Server Keycloak při nasazení v komplexních prostředích umožňuje spolupráci více administrátorů uspořádaných do hierarchie, což je umožněno díky detailnímu nastavení rolí a přístupových práv pro každého z nich. Tito administrátoři typicky potom mohou mít na starosti různé oblasti konfigurace serveru Keycloak. Jeden z nich tak např. může mít na starosti vytváření nových uživatelů (běžně např. zaměstnanců), další správu uživatelských rolí a jejich oprávnění a další potom figurovat jako jejich „nadřízený“ a mít tak přístup ke všem zmíněným položkám.

Kromě daných správců mohou do jisté míry konfiguraci serveru Keycloak měnit a ovlivnit i samotní uživatelé. Uživatel se např. může sám registrovat nebo si změnit email apod.

Dosavadní implementace serveru Keycloak umožňuje pouze autorizaci přístupu pro provádění takovýchto změn v konfiguraci, tzn. pouze úplnému povolení či zakázaní jejich provedení. Úkolem studenta bude návrh a implementace systému, který by umožňoval schvalování konfiguračních změn v serveru Keycloak. Tento systém by měl fungovat následujícím způsobem:

- Server Keycloak při provádění (vybraných) změn v konfiguraci – jako třeba registrace nebo vytvoření uživatele – tuto operaci přeruší a vytvoří požadavek na její schválení.
- Tato operace nepřejde v platnost (např. uživatel nebude vytvořen), dokud nebude odpovídající požadavek na schválení potvrzen oprávněným správcem.

Tento systém by měl být vysoce konfigurovatelný (kdo a pro jakou operaci potřebuje schválení a kdo může toto schválení provést) s důrazem na rozšiřitelnost a univerzálnost – jinými slovy, aby jej bylo možné použít v jakémkoliv místě serveru Keycloak. Práce by pak měla obsahovat i ukázkové nasazení tohoto systému – měla by se tedy spíše zaměřit na systém schvalování jako takový, než na jeho konkrétní nasazení napříč všemi částmi serveru Keycloak.

Student zároveň prozkoumá možnosti integrace jeho řešení s produktem JBoss BPM Suite (BPMS), což je platforma pro zprávu podnikových procesů vyvíjená společností Red Hat. Jakmile server Keycloak vytvoří požadavek na schválení nějaké operace, mělo by být možné na tento požadavek reagovat (schválit, popř. zamítnout) z nějakého procesu v platformě BPMS, což by umožnilo vysokou pružnost tohoto schvalovacího systému.