IDM na Jihočeské univerzitě

Ing. Jan Marek
jmarek@jcu.cz

Prehistorie

- Shell skripty
- Pouze k zakládání studentů
- Zaměstnanci ad-hoc
- Rušení účtů když je čas (skoro nikdy)
- Hledání autentizační platformy – OpenLDAP
- Hledání řešení pro správu účtů

Novell IDM

- **Zdál se být vhodný technologicky**
  - Základ NDS (LDAP)
  - Nad ním Java, konektory pomocí XSL-T transformací
- **Původní cenová politika – licence na server**
  - Z toho vyplynulo rozhodnutí ponechávat v IDM neaktivní identity
    - Co kdyby se vrátili (u zaměstnanců běžné – letní semestr učí, zimní ne, u studentů zřídka)
    - Možnost marketingového využití kontaktů?

Novell IDM 2.

- **Změna licenčního modelu**
  - Po roce a částečném nasazení nová verze
  - Licencování na uživatele
  - První licence na 20000 uživatelů, cca 1 mil. Kč
- **Po 8 letech pokus o nasazení nové verze a rozšíření funkcionality**
  - 15500 aktivních uživatelů – cca 980 tis. Kč
  - 40000 neaktivních uživatelů – cca 1,2mil. Kč
  - Přitom 99% sleva!!!
  - A to ještě nepočítáme implementaci nové funkcionality

Hledání OSS alternativy

- **Nalezeny 3 alternativy – forky IDM fy Sun:**
  - OpenIDM

    https://www.forgerock.com/products/identity-management/

    Orchitech Solutions http://www.orchitech.cz/cs/home
  - MidPoint

    https://evolveum.com/midpoint/

    AMI http://www.ami.cz/
  - CzechIDM

    http://www.czechidm.com/cs/

    BCV Solutions http://www.bcvsolutions.cz/

Výběrové řízení

Rozhodli jsme se pro toto zadání:

- Implementace a 5 let podpora
- V ceně veškeré licence na celých 5 let
- Otevřený zdrojový kód veškerých úprav a konfigurací
- Jako hodnotící kritérium součet ceny za implementaci a ceny za 5 let podpory požadovaného popsaného řešení
- Maximální cena za implementaci a licence cca 1.6 mil. Kč

Struktura IDM

- **Jeden člověk, jedna identita**
  - Párování dle RČ – problém s cizinci – až 4 RČ
    - Dočasné
    - Z matriky
    - Číslo soc. pojištění
    - Po získání občanství trvalé RČ
- **Původně 2, pak 3 zdroje identit**
  - STAG, ASEI/Odysea, pak CŽV od DERS-u
- **Řízené systémy**
  - AD, LDAP, LDAP pro FreeRADIUS, PostgreSQL, idkarty, údaje do STAG-u

Přechod na nové řešení

Novell:

- + Po letech používání stabilizované a funkční řešení
- + Pevná definice rozhraní zdrojů identit
- - Cena
- - Problematická a vcelku drahá rozšiřitelnost

OpenIDM:

- + Cena, hlavně s ohledem na počet spravovaných identit
- + Řešení postavené na OSS (PostgreSQL, jetty)
- - nelze postupně připojovat jeden systém za druhým
- - práce na analýze a implementaci jsou navíc nad rutinou

Dotazy?