IdM v prostředí ZČU v Plzni

Pavel Jindra, František Dvořák
Západočeská univerzita v Plzni

26.11.2015, Seminář IdM CESNET

Obsah

Západočeská univerzita - z pohledu IT

Identity Management Sun IdM - resource adaptéry

Správa identit na ZČU - toky dat , autoritativní zdroje, správa skupin

Uživatelská správa konta - dočasná a hostovská konta

Statistiky a postřehy z provozu

Západočeská univerzita

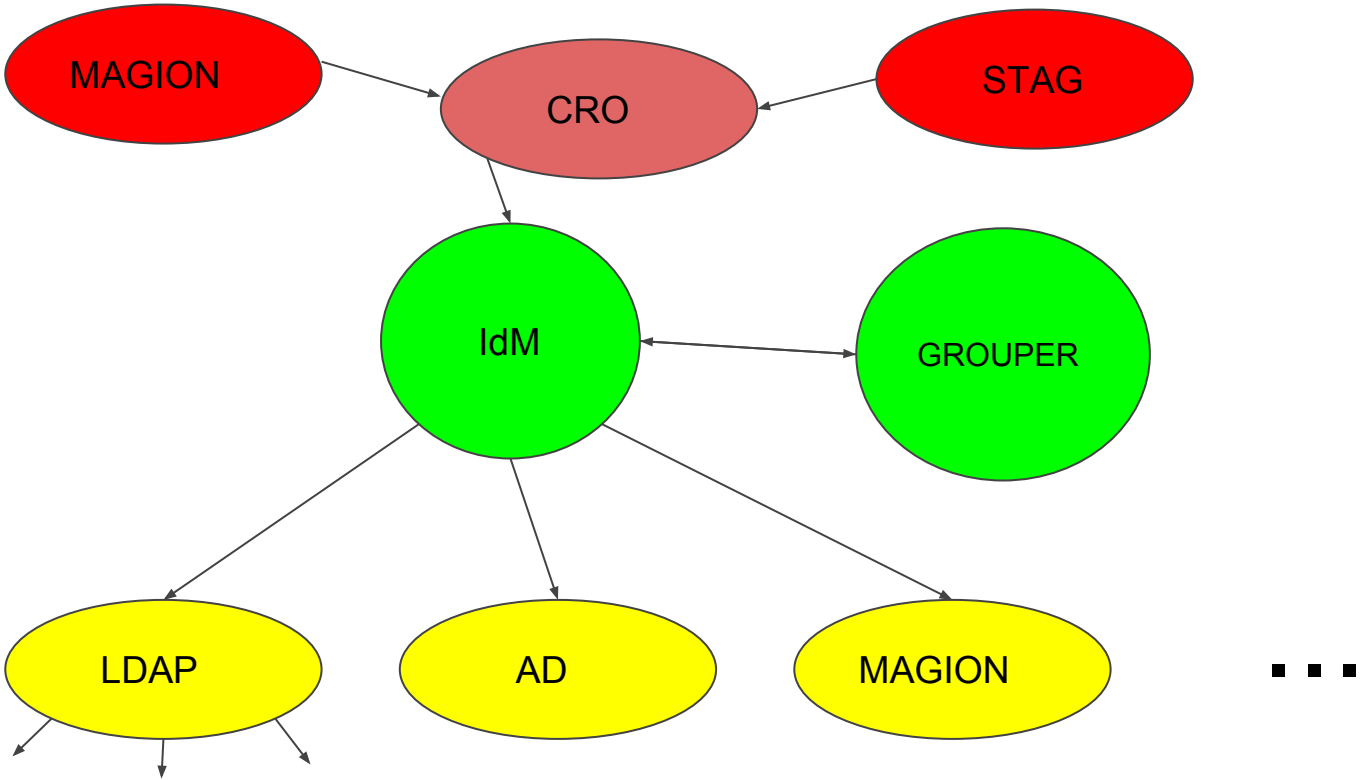
- 8 fakult ve 2 lokalitách (Plzeň, Cheb)
- cca. 15 tis. uživatelů z toho 2500 zaměstnanců
- Autentizační služba - Kerberos
- Úložiště - AFS
- SSO - WebAuth, Shibboleth
- Finanční systém - Magion, Studijní systém - STAG
- Windows - AD doména
- Celouniverzitní správa výpočetního prostředí (CIV) - cca. 50 zam.

Sun Identity Management

- Nasazen od roku 2007 za velmi výhodných licenčních podmínek
- Modulární systém psaný v JAVA
- Vše v XML uložených v Oracle (konfigurace i data)
- RA - DB, AD, LDAP, JDBC script, Shell script, vlastní, ...
- Výhody
  - hodně resource adaptérů
  - bez-agentové připojení resourců
  - modulární
  - silné skriptování
- Nevýhody
  - složitost - vše v XML
  - rychlost - zdlouhavá práce
  - XPRESS skriptovací jazyk

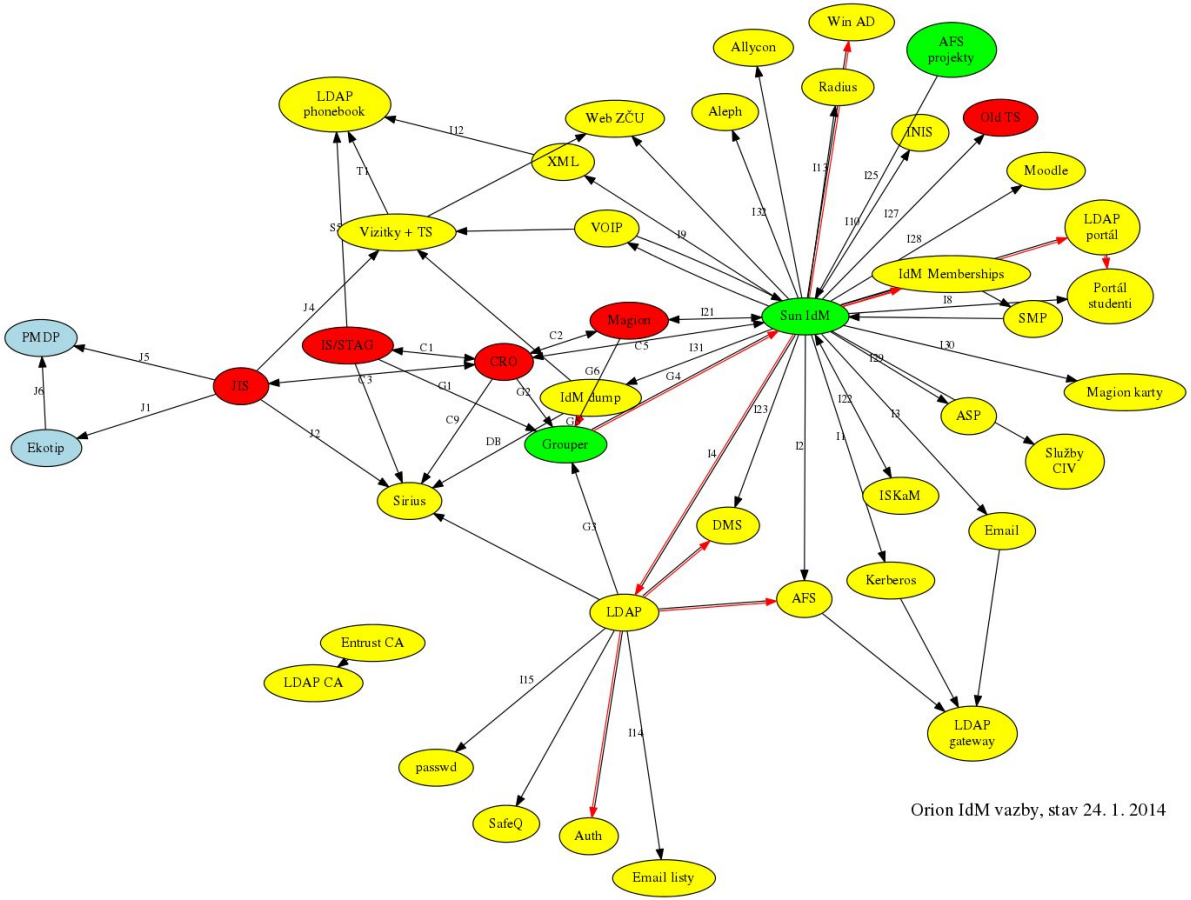
Správa identit na ZČU

Implementační model:



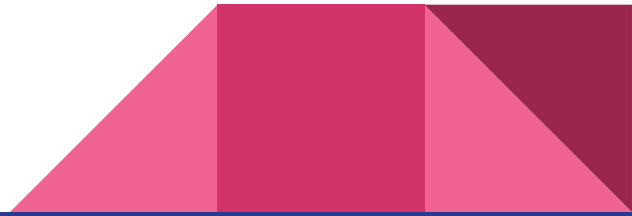
Správa identit

Výsledné schema:



Správa identit - v číslech

- IdM spravuje nejen uživ. konta, ale i další entity
  - nezaregistrované identity: 2050
  - admins: 22
  - skupiny: 1191 (156720 členství)
  - telefony: 2899
  - projekty: 799
  - externí JIS: 1366
  - externí wifi: 45
  - pracoviště (mimo IdM): 407

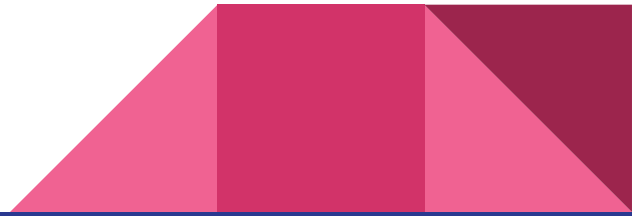


Správa identit - úlohy

- Připojení nového resource
  - IdM se podřizuje stávajícímu systému - problémy primárních klíčů
- Změna rodného čísla
  - nutno zadat do autoritativního systému správně
  - jinak potřeba “deduplikace” identit (sloučit peníze v menze, apod.)
- Asymetricky připojené resource - volná vazba, email interface
- Mazání uživatelů
  - Velká úloha
  - Vždy se najde zapomenutý systém
- Povolování existujících kont (přidání garanta, převod garanta)
- Změna katedry - podle MAGIONu, ručně singularity (určení primární?)
- Hlídací pes, hlídání procesu registrace kont na začátku roku

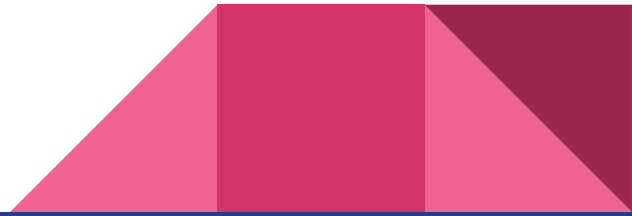
Správa skupin

- Samostatný systém Grouper od Internet 2
- Skupiny slouží jako autorizační data
- Propagují se do dalších systémů - přes LDAP
- Druhy
  - automatické skupiny - generují podle agendy IS
  - ruční - ručně udržované lokálními správci
  - self admin - uživatel se do skupiny může zařadit sám
- Skupinová aritmetika
- Grouper se špatně ovládá a je lehce nespolehlivý



Uživatelská správa konta

- Registraci provádí uživatel - zvolí login (max. 8 znaků)
- Změna hesla po telefonu
  - Nutno nahlásit předem své tel. číslo
- E-mail - forwardovací a třídící pravidla
- Správa členství ve skupinách
- Vizitka
- Správa dodatečných úložišť - projekty



Hostovská konta

- Každý zaměstnanec může zřídit hostovská konta
  - Wifi - dočasný přístup jen do WiFi - krátkodobý
  - Host - plnohodnotné konto
    - host
    - externí spolupracovník
    - sdílená konta (konference apod.)
- Platnost konta 1 rok - nutná obnova, posílá upozornění před koncem
- Garant přebírá za konto odpovědnost
- Aktuálně cca 450 kont (z toho 130 zároveň plnohodnotných)
- Při ukončení garanta se blokují i jeho host konta
- Host konta s RČ se propojí při nástupu

Sun IdM - charakteristika

- Plochá struktura uživatelů - nenašli jsme vhodné kritérium členění
- Atributy nejsou uloženy v IdM - vždy se tahají z resource
- Každá manipulace s uživ. daty vyžaduje spolupráci všech jeho resource
  - 1 identita cca 10s
- Jsou vyžadovány pravidelné rekoncilace
  - hlavní resource CRO trvá cca 12 h
  - běžný resource 1-2 h
- Nepoužíváme atributovou rekoncilaci
- Update jednotlivých uživ. probíhají asynchronně
- Máme externího “hlídacího psa” na IdM
- Implementace rolí se nezdařila uspokojivě

Závěr

- Ačkoliv je IdM “strašlivý cukrovar” rozhodně se vyplatí
- Pečlivě definovat autoritativní zdroje dat
- Integrovat vše do jednoho systému
- Self management šetří práci a zlepšuje uživ. komfort
- Jednotný primární klíč ve všech systémech
- Připojit pokud možno všechny zdroje