Centralizovaná správa identit a přístupů na služby na MU

Slávek Licehammer

26. 11. 2015

IdM na MU

- Na MU právě vzniká nová koncepce správy identit a řízení přístupu na služby
- Motivací jsou stále náročnější požadavky na autentizační a autorizační infrastrukturu
- Cílem je revize a vylepšení existujících systémů a postupů od základů

Identity

- Existující zdroje identit na MU
  - IS - studijní agenda
  - INET - zaměstnanecká agenda
  - Guest manager - správa externích uživatelů
- Částečně vzájemně synchronizovány
- Překryvy ve funkcionalitě

Skupiny

- Existující zdroje skupin
  - IS
  - INET
  - nástroj ACL
- Active Directory
  - Plněno vybranými existujícími skupinami
- Správa skupin není plně v rukou uživatelů
- Problém: členové skupin jsou omezeni systémem, ve kterém je skupina spravována

Řízení přístupu na služby

- Využívané systémy
  - IS
  - Active directory
  - Account Manager
- Account manager
  - Propojení existujících systému a generování změn v ACL pro služby
  - Změny detekovány 2x denně

Koncepční problémy

- Minimální evidence služeb
  - Oprávnění uživatelé
  - Požadované atributy uživatelů
- Správa externistů
  - externí zaměstnanci, návštěvníci knihoven, účastnící konferencí, komerční partneři…
- Jednotná správa přístupu na služby
- Podpora life-cycle uživatele
  - Autorizace navázána na existenci a typ účtu

Koncept řešení

- Centralizovaná správa identit, skupin a přístupu na služby
- Delegace oprávnění
  - Správce služby ✕ administrativní správce
- Implicitní a explicitní skupiny uživatelů
- Jasně definovaný životní cyklus uživatele
- Využití existujících identit uživatelů
  - eduID.cz, sociální identity, eduGAIN
- Podpora správcům služeb

Návaznost na existující stav

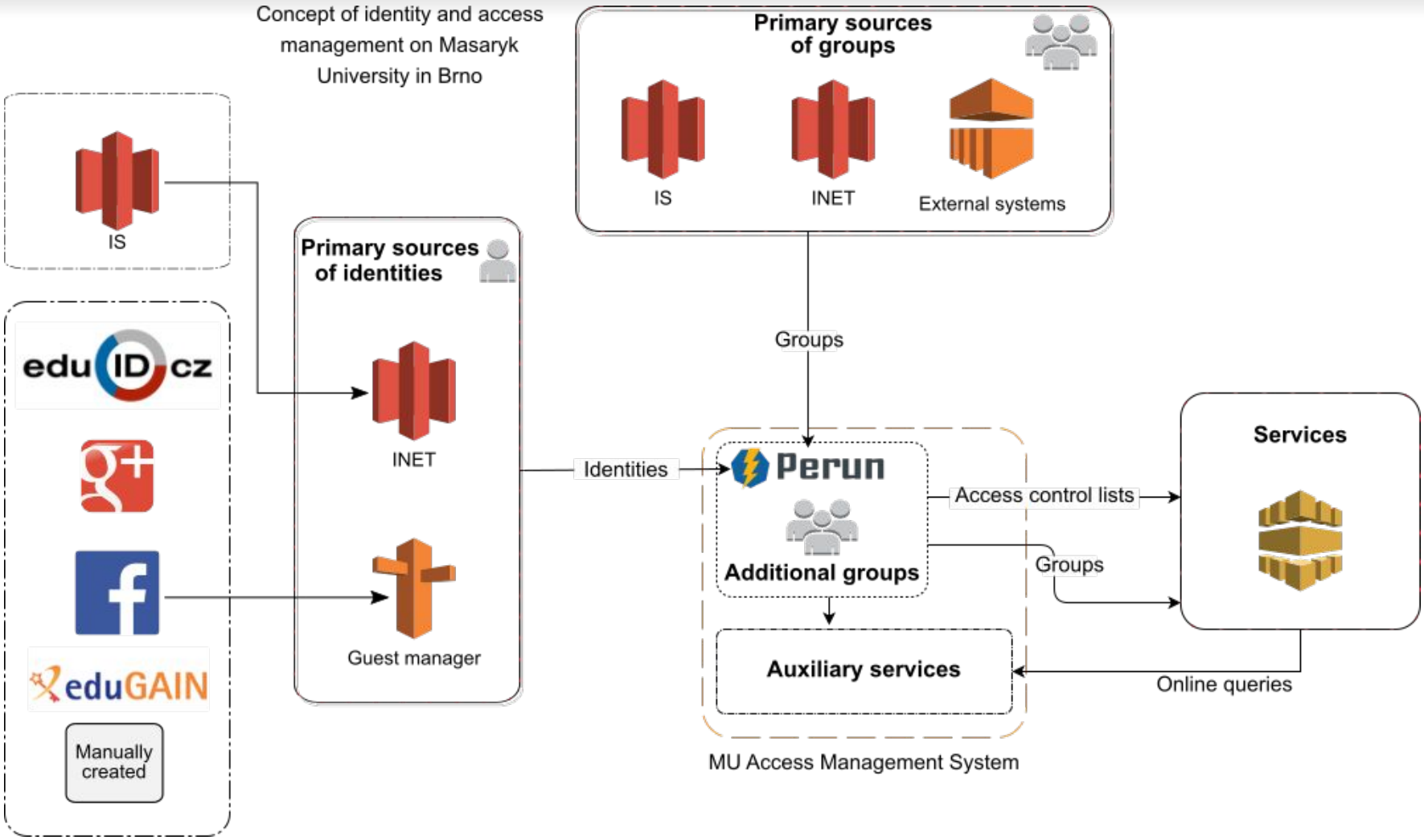
- Nutnost zachovat existující systémy
  - Změna by byla příliš nákladná
  - Import dat do centrálního řešení
    - Umožňuje propojit data za všech systémů
- Mechanismus přechodu na nové řešení
  - Postupná migrace jednotlivých služeb
  - Nejprve služby které nevystačí se současným řešením

Perun

- IAM - Identity and access management system
- Vyvíjen společně MU a CESNETem
- Kompletní řešení
  - správa identit, skupin, registrací
  - správa služeb a přístupů
  - správa atributů
- Navržen pro integraci do existujících prostředí

- Více na odpolední prezentaci

Role Peruna na MU



Podmínky pro realizaci

- Podpora vedení univerzity
- Spolupráce správců současných IdM řešení
- Spolupráce správců služeb
- Čas - na MU nižší jednotky roků
- Personální zajištění

Překážky

- Zmapování aktuálního stavu
- Odstranění výjimek v přístupech na služby
- Úprava služeb aby dokázaly pracovat se všemi typy identit
- Pomalá implementace
  - Potřeba správců služeb mít funkční řešení co nejdříve
- Vzájemné pochopení ze strany některých správců služeb

Co se osvědčilo

- Spolupráce s vedením
- Jasná vize finálního řešení
- Agilní metodiky
  - Inkrementální přístup
  - Začít tam, kde jsou slabiny současného systému
- Poskytování dostatku informací všem zájemcům o tuto problematiku

Shrnutí

- IAM na MU
  - Dlouhodobý plán nasazování nového řešení
- Použití Peruna
  - Konsolidace existujících identit a skupin
    - umožnění jejich kombinací
  - Centrální evidence služeb a přístupů
  - Delegace oprávnění na administrativní správce

Děkuji za pozornost

http://perun.cesnet.cz

Slávek Licehammer
slavek@ics.muni.cz