PV176 Správa systémů MS Windows II

Výuka správy rozsáhlých prostředí
založených na platformě Windows

Organizační informace

Organizační informace

- 11 cvičení spojených s přednáškou
- Práce ve dvojicích
- 2 cvičící na každém cvičení
- Windows Server 2008 R2 / Windows 7
  - Vzdálené připojení ze sítě FI nebo z VPN MUNI

Hodnocení

- Písemný teoretický test a následná praktická zkouška na počítačích
- 4 termíny, jeden z nich může být předtermín
- Obsah slidů nemusí stačit k úspěšnému složení zkoušky

Hodnocení

- A: >= 90
- B: 89 – 84
- C: 83 – 78
- D: 77 – 72
- E: 71 – 65
- F/N: =< 64

- 3 domácí úkoly
  - 1 špatně: -5 bodů
  - 2 nebo 3 špatně: -33 bodů

Literatura

- Knihy:
  - Šetka, Petr. ***Mistrovství v Microsoft Windows Server 2003: Ze začínajícího správce expertem***. 2. vydání. Brno : Computer Press, 2008. 704 s. ISBN: 978-80-251-1871-9.
  - Simmons, Curt. ***Active Directory Bible***. Foster City : IDG BooksWorldwide, Inc., 2001. 565 s. ISBN: 0-7645-4762-3.
  - Allen, Robbie. ***Active Directory Cookbook***. Sebastopol: O'Reilly& Associates, Inc., 2003. 622 s. ISBN : 0-596-00464-8.

- Web:
  - Microsoft Technet <http://www.technet.com/>

Dotazy a konzultace

- Partner ve dvojici
- Diskusní fórum
- Email
  - bukac@ics.muni.cz
  - tucek@ics.muni.cz
- Konzultace
  - Po předchozí domluvě na cvičení nebo emailem

Motivace

- Co se můžete naučit?
  - Jak efektivně spravovat stovky počítačů
  - Jak centrálně spravovat a vzdáleně instalovat software na stanicích
  - Jak zpřístupnit a zabezpečit dokumenty jednotlivých uživatelů či skupin
  - Jak navrhnout fyzickou a logickou infrastrukturu organizace
  - Best practices!

Motivace

- Proč byste měli chtít absolvovat tento předmět?
  - Čistě praktické informace přímo z praxe
  - Zkušenosti lidí, kteří denně spravují více jak 1100 počítačů a 40000 uživatelských účtů
  - Práce v týmu
- Proč byste neměli chtít absolvovat tento předmět?

Microsoft MTA

- Microsoft Technology Associate Certification
- Probíhají jednání se společností Microsoft o poskytnutí voucherů na certifikace zdarma
- Nejlepší zhruba třetina studentů

Úvod do teorie

Pracovní skupina

- 2 – 10: Pracovní skupina
  - Počítače rovnocenné
  - Účty ukládané lokálně na každém počítači zvlášť
    - Např. změna hesla na jednom z nich pro ostatní počítače nic neznamená
  - Neexistující centrální management nastavení
  - Uživatelské profily na každém počítači zvlášť
  - Správa vyžaduje postupné provádění nastavení na všech počítačích

Doména Active Directory

- 10+: Doména Active Directory
  - Některé počítače mají výjimečné postavení (doménové řadiče)
  - Každý uživatel má jediný účet, uložený právě na doménovém řadiči
  - Doménoví správci mohou vynucovat nastavení zapojeným počítačům jednorázově a centrálně

Active Directory

- Active Directory
  - Implementace adresářových služeb založená na protokolu LDAP, vytvořená společností Microsoft pro použití v systémech Windows
  - Jedná se o databázi s množstvím navázaných služeb
  - Data jsou ukládána ve formě objektů (~záznamů) zařazených do stromové struktury
  - Každý objekt je zástupcem třídy, každá třída má množinu atributů, atribut každého objektu má jméno a může mít žádnou, jednu nebo i více hodnot
    - Např. záznam třídy „uživatel“ může mít atributy (jméno, příjmení, login, telefon, heslo,…); objektem je například (Jan, Novak, jnovak,,SuperHeslo1,…)

Active Directory

- AD schéma
  - Definice tříd a atributů v databázi a míst, kde se v databázi ukládají objekty
  - Každý atribut je v databázi definován jen jednou, k třídám je jen přidáván
- LDAP (Lightweight Directory Access Protocol)
  - Standardizovaný protokol pro ukládání a přístup k datům na adresářovém serveru
  - Pracuje na portech 389/TCP+UDP (LDAP) a 636/TCP+UDP (LDAPs)

Logická struktura AD

- Doména (Domain)
  - je základní jednotka AD, kterou tvoří minimálně 1 doménový řadič
  - reprezentuje replikační hranici v AD
  - má jednoznačné označení (musí mít!)
  - má vlastní zásady zabezpečení
  - vytváří vztahy důvěry s ostatními doménami
  - Pojmenování domén je úzce spjaté s protokolem DNS, viz další přednáška
  - Proč mít doménu? Protože bez ní to nejde!

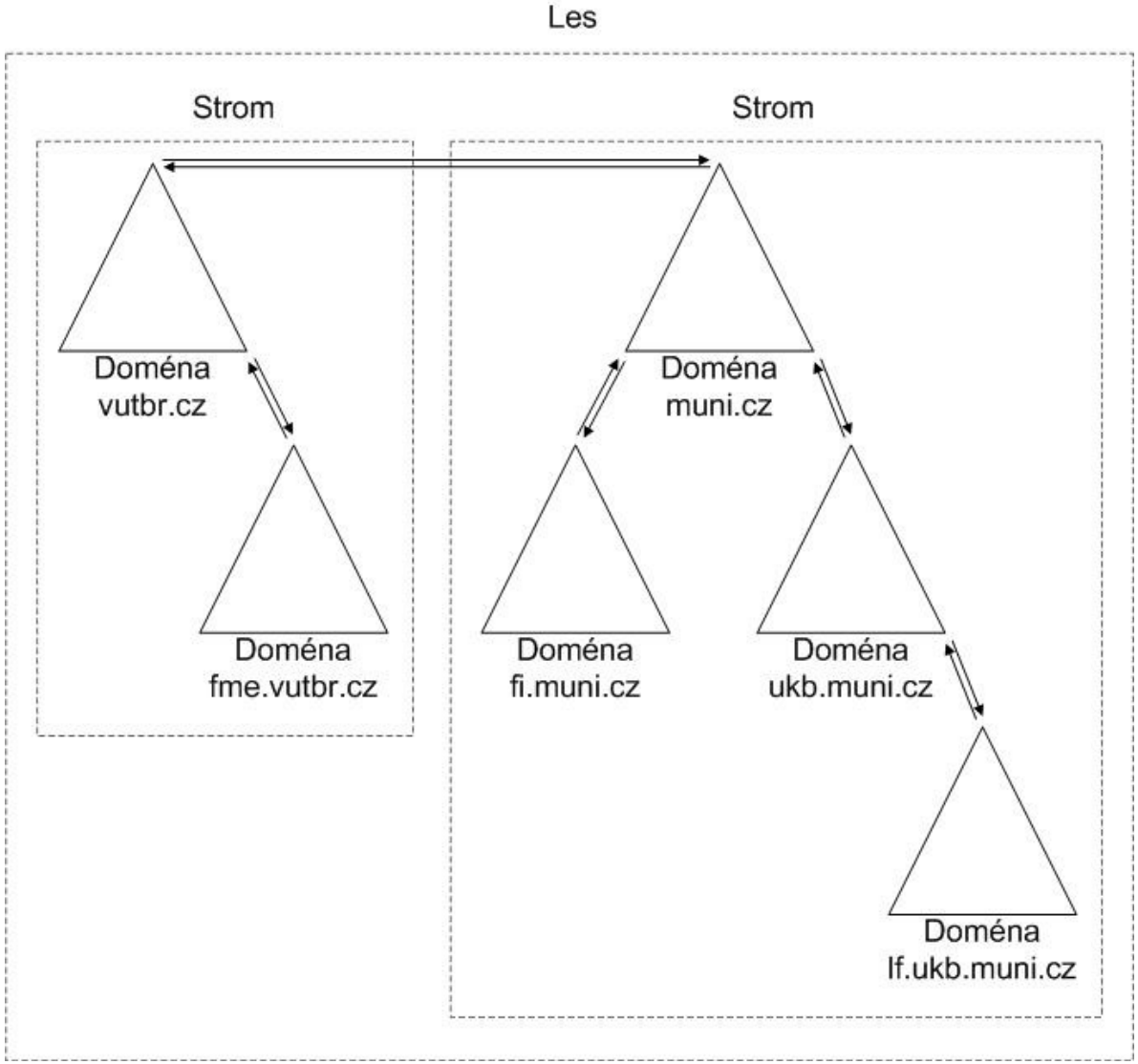
Logická struktura AD

- Strom (Domain tree)
  - je hierarchické spojení domén vytvořené vztahem rodič-potomek.
  - Uživatelé mohou prohledávat informace v rámci doménového stromu
  - Proč mít doménový strom a ne jen jednu doménu?
    - Administrativní a bezpečnostní rozdělení jednotlivých domén

Logická struktura AD

- Les (Forest)
  - je spojená skupina doménových stromů
  - V celém lese je shodné schéma AD databáze
  - Proč mít les s více stromy?
    - užitečný pro pobočky firem, které vyžadují autonomii v administrativních úlohách
    - poskytuje prostor pro více internetových jmen (microsoft.com, microsoft.cz, atd.)
    - dovoluje jednoduché spojování a akvizice firem
    - umožňuje jednoduše společnostem spolupracovat bez nutnosti změny jmen

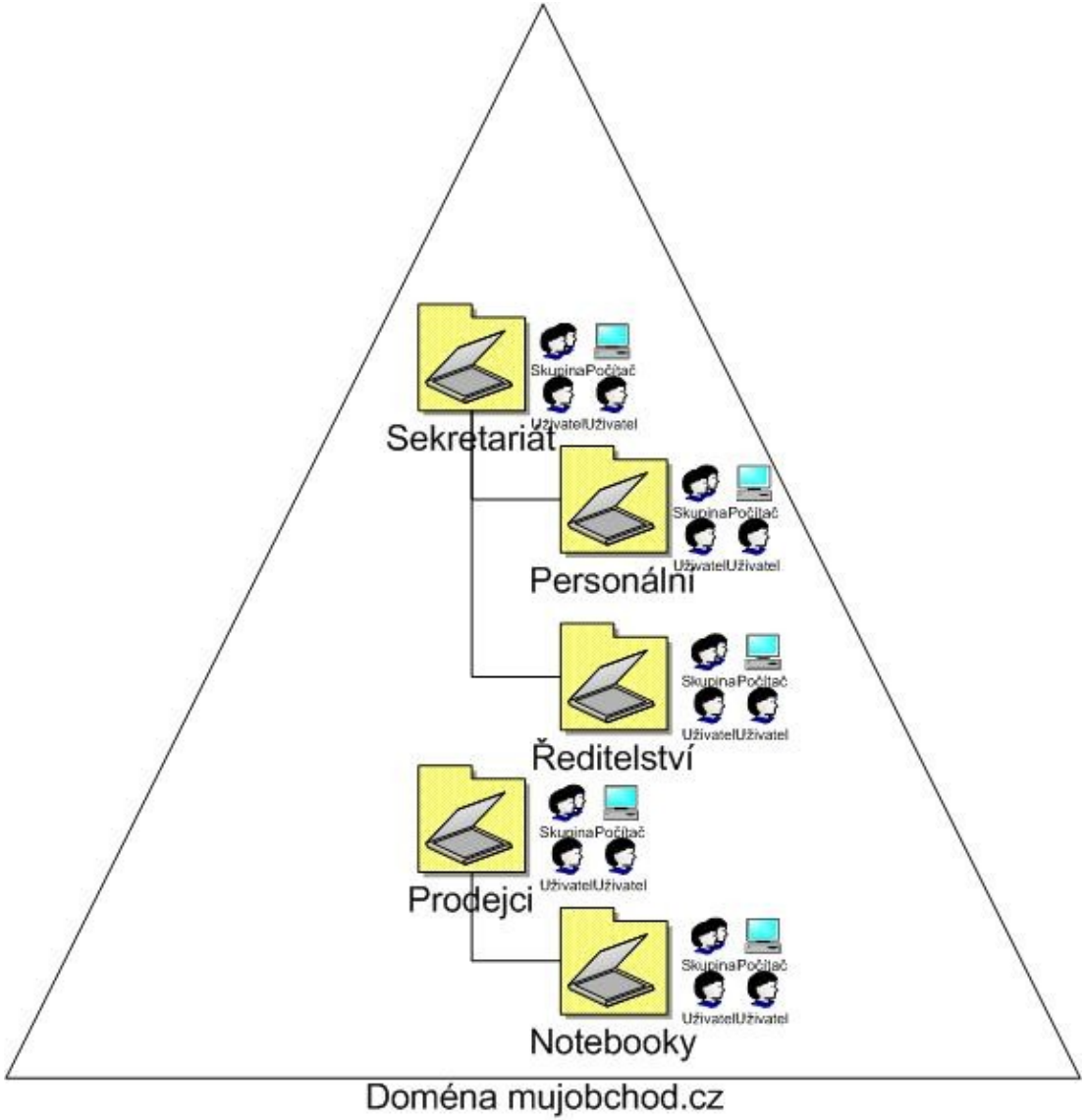
Logická struktura AD – příklad



Organizační jednotka

- Organizační jednotka (OU)
  - je prvkem dalšího členění v rámci domény
  - si také lze představit jako logický kontejner, do kterého můžeme umístit objekty jako uživatelské účty, sdílené prostředky, další OU...
    - Každý objekt se nachází pouze v jedné OU (tato OU však může být sama vložena v jiné OU)
  - obvykle odráží správní nebo fyzickou strukturu organizace

Struktura organizačních jednotek



Adresace objektů v AD

- Distinguished name (DN)
  - Vyjadřuje plnou cestu k objektu v AD
  - Jedná se o hierarchické seřazení organizačních jednotek zevnitř ven a doménových komponent zespodu nahoru
    - OU – organizační jednotka
    - DC – doména
    - CN – kontejner/účet počítače/uživatelský účet/účet skupiny
  - Př.:
    CN=Jan Sup,OU=Studenti,OU=Ucty,DC=fi,DC=muni,DC=CZ

Adresace objektů v AD

- Relative distinguished name (RDN)
  - Vyjadřuje lokální označení objektu
  - RDN je hodnota nejlevější části DN (př. Jan Sup)
- Globally Unique Identifier (GUID)
  - 128 bit číslo přiřazené objektu při vytvoření
  - Jednoznačně vždy za všech okolností identifikuje objekt
- Security identifier (SID)
  - Identifikátor používaný při řízení přístupu
  - Pouze některé objekty (účty, skupiny)
- DN i RDN se mohou v čase měnit, GUID a SID jsou fixní

Fyzická struktura AD

- Základem každé domény je jeden nebo více doménových řadičů (DC, domain controller)
- Doménový řadič
  - je server, na který jsme nainstalovali doménu a ten ji nyní provozuje
  - je vždy součástí právě jedné domény
  - Multimaster mód – doménové řadiče jsou si (víceméně) rovnocenné, doménové služby fungují, pokud funguje aspoň jeden doménový řadič

Fyzická struktura AD

- Síť
- Fyzická struktura AD nijak nemusí souviset s logickou strukturou AD!

Virtuální stroje

Příští seminář

- Šimon Suchomel – CVT FI MU
- Překlad jmen – DNS, NetBIOS,…
- Instalace Active Directory