PV176 Správa systémů MS Windows II

Výuka správy rozsáhlých prostředí
založených na platformě Windows

Organizační informace

- 12 povinných cvičení spojených s přednáškou
  - Víc jak dvě neomluvené -> neabsolvování předmětu
- 3 povinné úkoly
- Práce ve dvojicích
- 2 cvičící na každém cvičení
- Windows Server 2008 R2 / Windows 7 (3/1)
  - Vzdálené připojení ze sítě FI nebo z VPN MUNI

Hodnocení

- Vnitrosemestrální test v podobě odpovědníku v ISu (10b)
- Závěrečný test v podobě teoretické a praktické části na počítačích (30b + 30b)
- 3 úkoly (10b + 10b + 10b)
- Pro úspěšné ukončení je třeba alespoň 60b, alespoň 20b musí být z teoretických částí (vnitro + závěrečný test)
- Obsah slidů nemusí stačit k úspěšnému složení zkoušky

Domácí úkoly

- 3 povinné úkoly každý za max. 10b
- Na vypracování každého je 14 dnů
- Za neodevzdání je penalizace -5b (a ztráta 10b za samotný úkol)
- Bez možnosti opravy
- Rozsah
  - 1. úkol 2-3 kapitola
  - 2. úkol 4-6 kapitola
  - 3. úkol 7-11 kapitola

Hodnocení

- A: >= 93
- B: 85 – 92
- C: 77 – 84
- D: 69 – 76
- E: 60 – 68
- F/N: < 60

- Vnitro 10b
- Úkoly 30b
- Závěrečný test 60b

Literatura

- Knihy:
  - Mistrovství v Microsoft Windows Server 2003: Ze začínajícího správce expertem. 2. vydání
  - MCTS Self-Paced Training Kit (Exam 70-640) Configuring Windows Server 2008 Active Directory, 2nd Edition
  - MCTS Self-Paced Training Kit (Exam 70-642): Configuring Windows Server® 2008 Network Infrastructure, 2nd Edition
  - Windows® Group Policy Resource Kit: Windows Server® 2008 and Windows Vista®
  - Windows Server® 2008 Active Directory® Resource Kit

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

Motivace

- Co se můžete naučit?
  - Jak efektivně centrálně spravovat stovky počítačů
  - Jak centrálně spravovat a vzdáleně instalovat software na stanicích
  - Jak navrhnout fyzickou a logickou infrastrukturu organizace
  - Výhody použití AD
  - Best practices!

Osnova přednášek

1. Úvod
2. Networking (DHCP, firewall, adresace)
3. Překlad jmen, instalace AD (NetBIOS, DNS)
4. Základy AD (skupiny, SID, GUID)
5. Group Policy (OU, ADMX store)
6. Instalace SW (MSI)
7. Pohled uživatele (profily,offline files, úprava prostředí)
8. FSMO role + AD Functional levels
9. Topologie (fyzická, logická)
10. Zabezpečení (backup, oprávnění,WSUS)
11. Další role Windows Serveru 2008 R2 (Hyper-V)
12. Další role Windows Serveru 2008 R2 (WSUS, DFS, RDS, IIS, WDS)

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 centrálně vynucovat nastavení všech zapojených počítačů

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, povinný/nepovinný (zadefinováno ve schématu)
    - Např. záznam třídy „uživatel“ může mít atributy (jméno, příjmení, login, telefon, heslo,…); objektem je například (Jan, Novak, jnovak,,SuperHeslo1,…)
    - Třídy: user, group, computer, printer, OU
  - %SystemRoot%\ntds\NTDS.DIT (tmp.edb,edb.log,edb.chk,..)

LDAP

- LDAP (Lightweight Directory Access Protocol)
- Pro snadnou organizaci různých typů záznamů bylo zvoleno použití protokolu LDAP
- Standardizovaný protokol pro ukládání a přístup k datům na adresářovém serveru
  - Pracuje na portech 389/TCP+UDP (LDAP) a 636/TCP+UDP (LDAPs)

Schéma

- Definuje všechny druhy objektů v AD (atributy,objekty)
- Každý atribut je v databázi definován jen jednou, k třídám je jen přidáván
- Každý objekt je definován seznamem atributů
- Definuje které atributy jsou povinné a které ne (pro konkrétní objekt) a jejich možné hodnoty
- Změnou schématu můžeme vytvořit nové třídy objektů, přidávat atributy
- Adsiedit.msc

Logická struktura AD

- Tvořena pomocí lesa, stromů, domén, organizačních jednotek
- Doména (Domain/Root 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
  - Proč mít doménu? Protože bez ní to nejde!

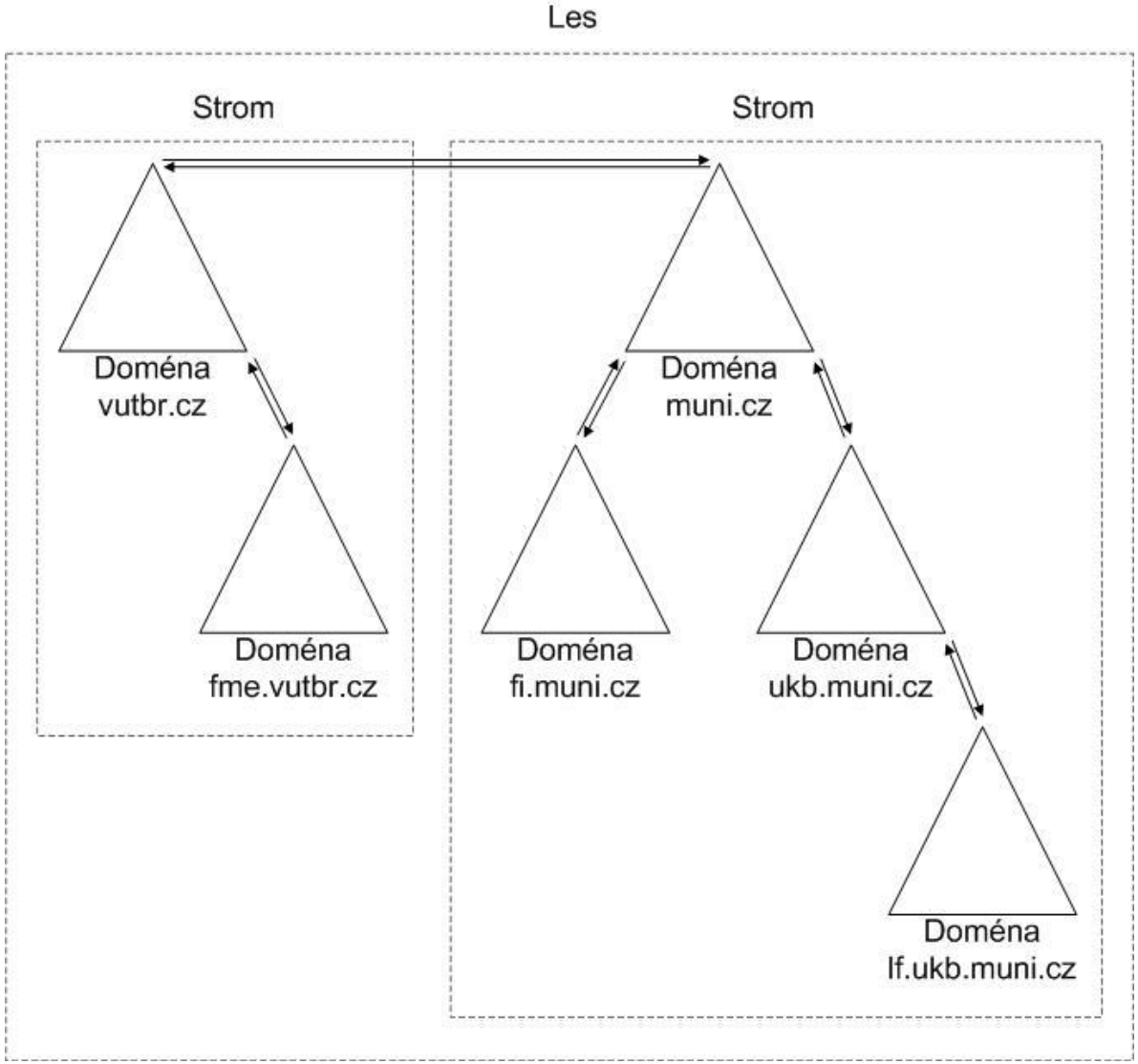
Logická struktura AD

- 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

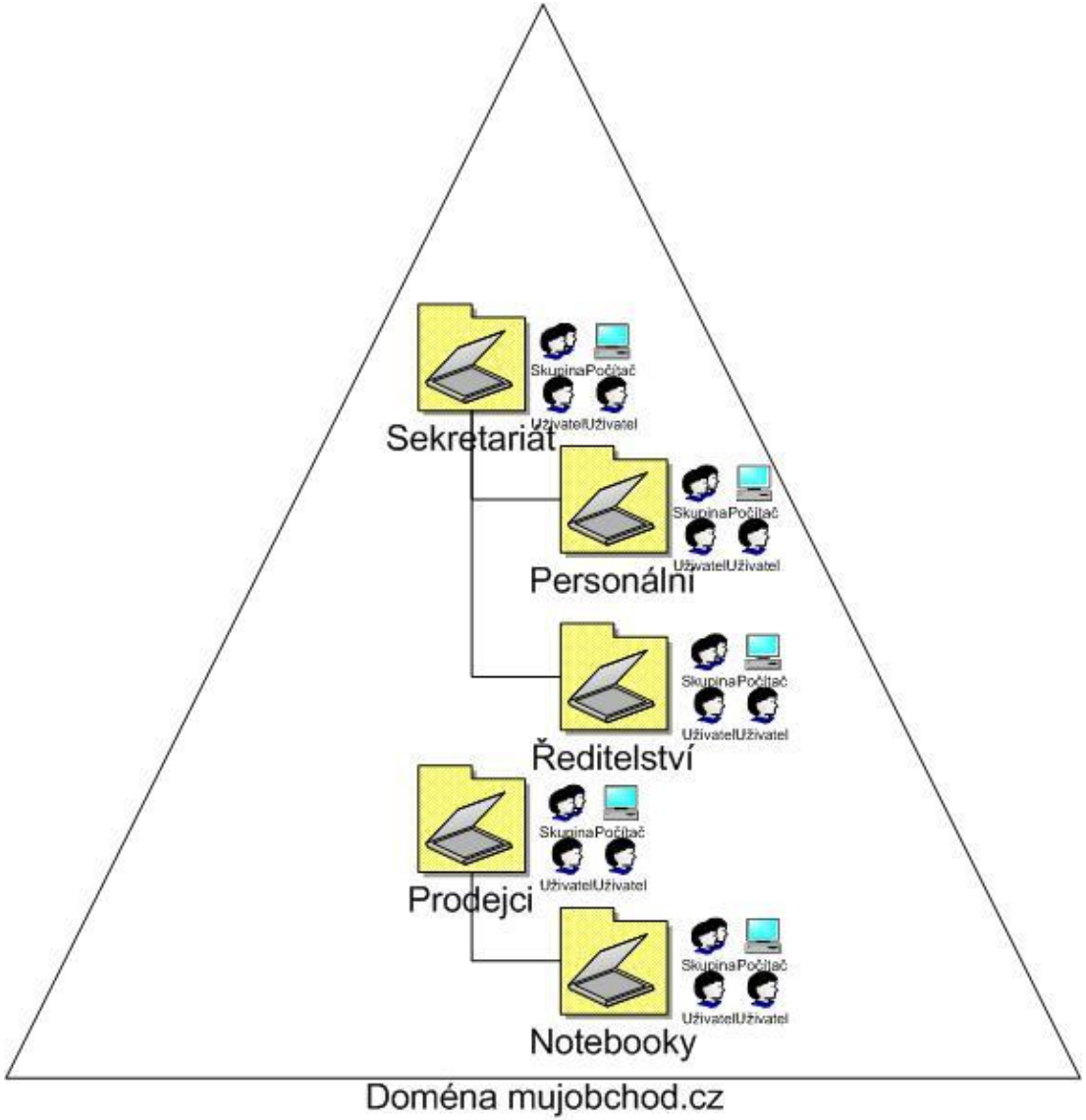
Logická struktura AD – příklad



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 (domain component)
    - CN – kontejner/účet počítače/uživatelský účet/účet skupiny (common name)
  - 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 (CN)
  - RDN je hodnota nejlevější části DN (př. Jan Sup)
  - Musí být unikátní v rámci OU
- 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 je fixní (SID se mění při migraci účtů)

Adresace objektů v AD

- Fully qualified domain name (FQDN)
  - Název přesně určující stroj v DNS struktuře
  - Hostname + domain name
    - nereis05.ad.fi.muni.cz
- User principal name (UPN)
  - Je alternativní přihlašovací jméno pro uživatele
  - Ve tvaru LogonName@DNSDomain (domain name/alternative name)
    - xnovak@fi.muni.cz
    - xnovak@ntfi

Globální katalog

- Slouží k vyhledávání informací o objektech
- Umístěn na vybraném DC (výchozí je první DC)
- Částečná replika (pro čtení) všech domén v lese, obsahuje jen vybrané atributy každého objektu z celého lesa
- Komunikace skrze TCP port 3268 (3269 u zabezpečené verze)

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
  - Poskytuje úložné a replikační funkce
  - Multimaster mód – doménové řadiče jsou si (víceméně) rovnocenné, doménové služby fungují, pokud funguje aspoň jeden doménový řadič
  - Singlemaster mód – některé typy akcí vyžadují provádění na jednom serveru (Operation masters role = FSMO role)
  - Read-only DC

Fyzická struktura AD

- AD Sites (sajta)
  - Kombinace jednoho i více subnetů
  - Logická jednotka dom. řadičů s rychlým a spolehlivým síťovým připojením
  - Různý interval replikace v rámci jedné sajty a mezi více sajtami
  - Zvětšení kontroly nad replikací (schedule, RPC/SMTP)
  - Default site (Default-First-Site-Name)
  - Jedna site může obs. víc domén
- Fyzická struktura AD nijak nemusí souviset s logickou strukturou AD!

AD služby (role)

- Directory Services (AD DS)
  - Správa komunikace uživatel-doména, uchovává informace o objektech
- Certificate Services (AD CS)
  - Vytváření a správa veřejných certifikátů
- Federation Services (AD FS)
  - Web single sign-on (SSO) při přístupu k webovým aplikacím organizace
- Lightweight Directory Services (AD LDS)
  - Poskytuje možnosti LDAP bez potřeby AD directory-enabled aplikacím
- Rights Management (AD RM)
  - Ochrana podnikových informací (word processor, email client)

Virtuální stroje

Virtuální stroje

- Rozdělení do dvojic
- Přidělení strojů
- RD (RD tabs, Mremote)