Správa MS Windows II

Vladimír Pečený

Osnova

- Pracovní skupina vs doména
- Active Directory
  - Historie
  - Technologie
  - Pojmy
- DNS
  - V AD?
- Instalace AD

Pracovní skupina vs. doména

- Pracovní skupina
  - Do 10 počítačů
  - n uživatelů x m strojů = počet účtů :-(
  - Toť vše.
- Doména
  - Centrální prostor s
    - Množinou účtů uživatelů
    - Sadou nastavení aplikovatelná na stroje i uživatele

Když doménu…

- …tak v Active Directory
- Poprvé ve Windows 2000 Server edition
- Adresářová služba založena na protokolu LDAP
- Centralizace zdrojů, služeb, uživatelů
- Možnost hierarchického uspořádání

LDAP

- Lightweight Directory Access Protocol
  - Protokol pro síťový přístup k adresářové službě
  - Adresář
    - Množina informací s podobnými atributy organizována do logické, hierarchické jednotky
    - Telefonní seznam
  - Z potřeb telefonních společností vznikla vyčerpávající specifikace X.500
  - Její implementace DAP a voilá …
  - …nutná redukce a přidání podpory TCP/IP a máme LDAP.

Struktura LDAP

- Adresář je tvořen záznamy ve stromové struktuře
- Záznam tvořen množinou atributů
  - Atribut má své jméno, hodnoty
- Každý záznam má v rámci stromu jedinečné jméno
  - Distinguished Name (DN, RDN?)

Záznam v LDAP

dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1234
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top

Logická struktura AD

- Kopíruje administrativní požadavky
- Doména
  - Známe…
  - Sada účtů, pravidel, nastavení
  - Poddoména, child-parent vztah a vzniká ..
- Strom
  - Strom ke stromu, máme ..
- Les

Logická struktura v AD

- Doména? Moc velké …
- Organizační jednotky
  - Kontejner pro vlastní objekty
  - Nejjemnější aplikace Group Policy
  - Decentralizace správy
- Vlastní objekty
  - Množina jedinečných atributů určena ve *schematu*
- Samotné atributy
  - Lze přidávat nové, editovat staré, …

Globální katalog

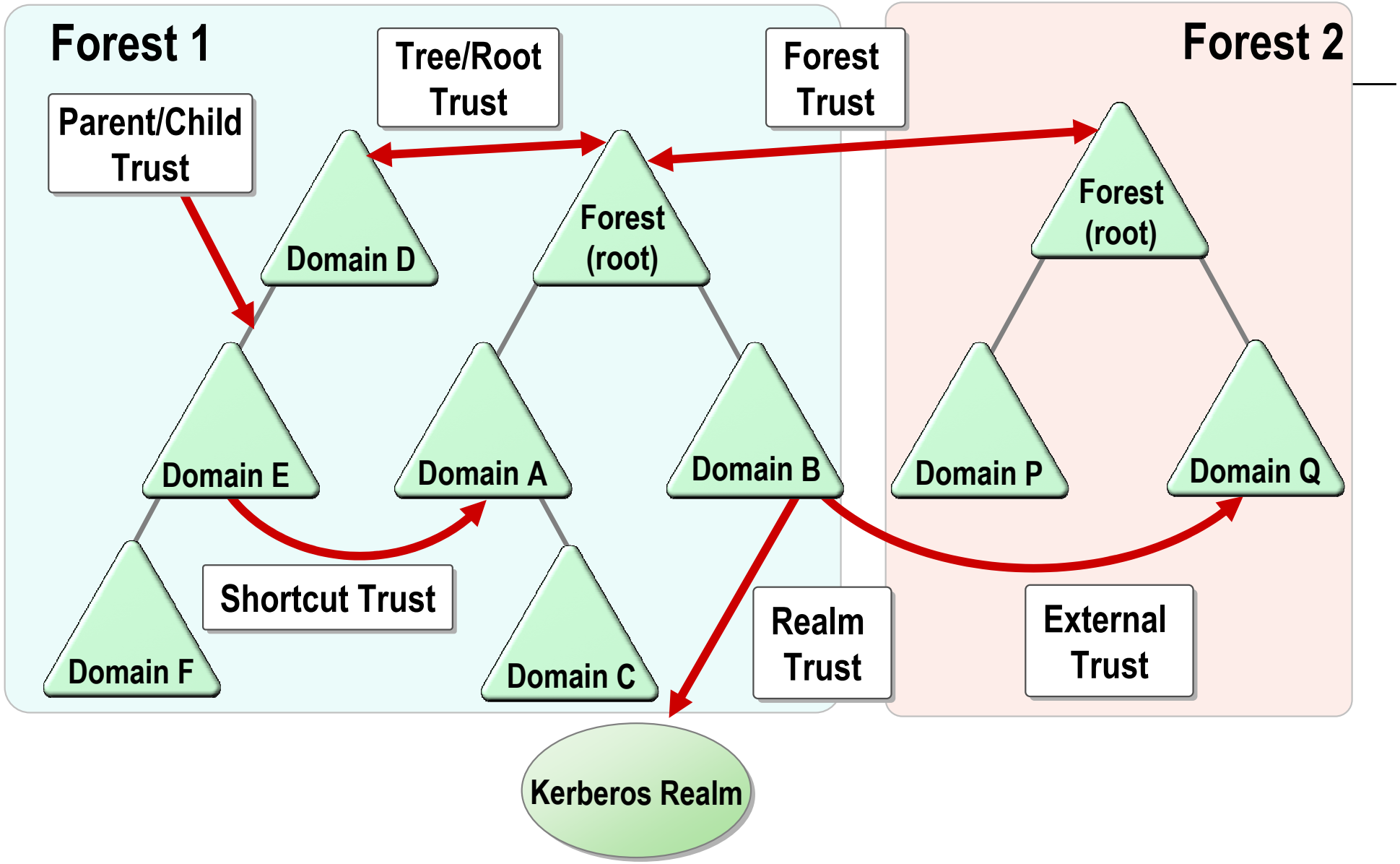
- Použit při prohledávání *Lesa*
  - Množina objektů s podmnožinou atributů (vyhledávacích klíčů?)
  - Read only

Vztah důvěry, Trust

- Umožňují uživatelům z jedné domény přistupovat ke zdrojům v druhé doméně.
- Základní hranicí důvěry je Les, nikoliv doména
  - S každou vytvořenou doménou se vytváří i vztah two-way transitive důvěry
  - Tedy každá s každou a nelze to zrušit

Typy důvěry

- Jedno- dvoucestná, tranzitivní
- Implicitní
- Shortcut
  - Domény z různých stromů, T, 1- 2
- External
  - Domény z různých lesů, T, 1- 2
- Forest
  - Mezi lesy, T, 1- 2
- Realm
  - Připojení do non-AD domén, N- T, 1- 2


Forest 1
Forest 2
Parent/Child Trust
Tree/Root Trust
Forest Trust
Domain D
Forest (root)
Forest (root)
Domain E
Domain A
Domain B
Domain P
Domain Q
Shortcut Trust
Domain F
Domain C
Realm Trust
External Trust
Kerberos Realm

Fyzická struktura AD

- Sleduje a optimalizuje síťový provoz
  - Kdy a jak bude probíhat replikace mezi servery
- Domain Controllers
  - Počítač s Windows Server 2000/2003 a službou Active Directory
  - Každý z řadičů domény poskytuje úložné a replikační funkce
  - Pouze jedna doména na jednom řadiči
  - Porovnání s Windows NT?
  - Všechny DC jsou si rovny, ale …

Operations Masters

- Multimaster replikace
- Existují operace, které musí být prováděny výhradně na jednom DC, ze kterého se později replikují
  - Single master replication
  - Přidání domény, změna schématu
- Tyto operace sjednoceny do operations master roles
  - Stroje jež je provádějí
    - Operations Masters

Flexible Single Master Operations

- Forest-Wide
  - Schema Master
    - Změny schématu
  - Domain Naming Master
    - Přidání či rušení domény
- Domain-Wide
  - PDC emulator
    - Kvůli zpětné kompatibilitě s BDC s Windows NT 4.
  - Relative Identifier Master
    - Každý objekt dostane po vytvoření jedinečné SID
      - Skládá se ze SIDu domény a jedinečného RIDu
      - Každž DC ma svůj pool přidělený RID masterem
      - Pří nedostatkyu žádá nový

Flexible Single Master Operations

- Infrastructure Master
  - Aktualizuje záznamy při přesunu objektu mezi doménami
- Máme 12 domén v 1 lesu…
  - Kolik máme Operations Masters?

Fyzická struktura AD

- Active Directory Sites
  - Logická jednotka řadičů s rychlým připojením
    - Mezi těmito stroji probíhá komunikace velmi často za účelem replikace údajů
- Active Directory Partitions
  - Domain partition
    - Doménové objekty
    - Určeno k replikaci
  - Configuration partition
    - Záznamy o topologii Lesu

Fyzická struktura AD

- Schema partition
  - Definice forest-wide schématu
  - Každý les má pouze jedno schéma kvůli konzistenci
  - Replikováno na každý z DC
- Application partition
  - Volitelné
  - Nevztahují se k bezpečnosti, ale aplikacím
  - Lze replikovat na vybrané DC

Schéma

- Definuje všechny druhy objektů v AD
- Object classes
  - User, Printer, computer
- Attributes
  - Jediněčně definovány
  - Skládáním tvoříme objekty

Instalace AD

- Minimální požadavky
  - Windows 2003 Server
  - NTFS oddíl s min. 250 MBM
  - Administrátorská práva
  - Protokol TCP/IP
  - DNS Server s podporou SRV záznamů

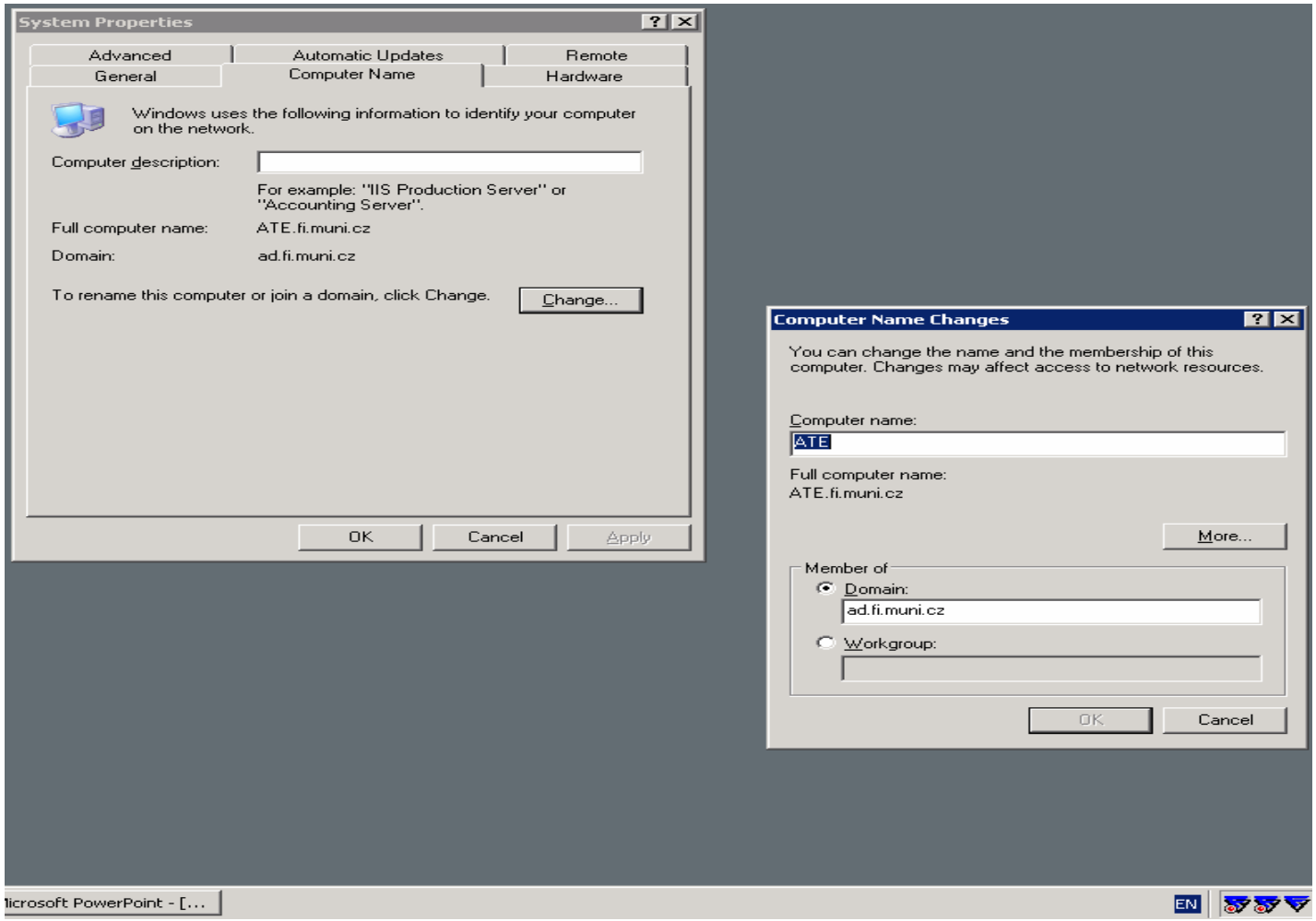
Instalace AD

- Dcpromo
- DC
  - pro novou doménu
  - Existující doménu
- Doména
  - v novém lese
  - Child doména
  - Nový doménový strom v lese

Instalace AD

- DNS název domény
  - Pro zpětnou kompatibilitu i NetBios jméno
- Dále určíme úložiště důležitých souborů
  - Databáze AD & Logy
- Vytvoření SYSVOL složky
  - Slouží k potřebám replikace
  - Uložení politik, přihlašovacích skriptů (NETLOGON)

Přidání počítače do domény



Nástroje pro správu AD

- Vizuální MMC Snap-in
  - Active Directory Users and Computers
  - Active Directory Domains and Trusts
  - Active Directory Sites and Services
  - Active Directory Schema
  - *Group Policy Management*
- Příkazová řádka
  - Dsadd
  - Dsmod
  - Dsquery
  - Dsmove

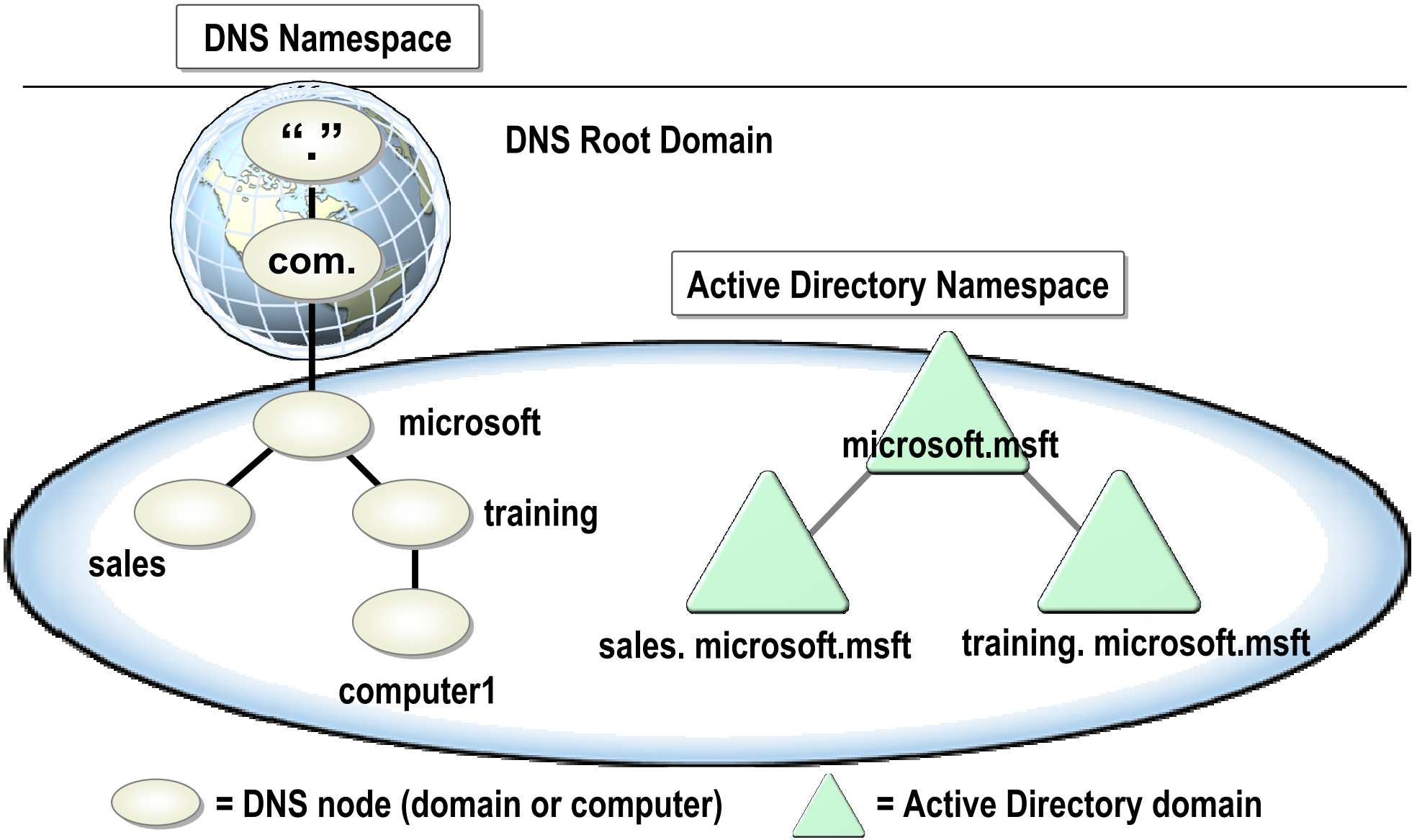
DNS

- Jmenná služba
- Obsahuje důležité informace o zdrojích a službách v AD
- Stroje v síti tak mohou jednoduše lokalizovat AD služby
- Jméno stroje v DNS = jméno stroje v AD
- Název Primary zone odpovídá názvu domény
- Dynamická aktualizace záznamů?

DNS

- DNS domain name (Primary DNS suffix) = jméno domény v AD
- Integrace AD s DNS umožňuje lokalizaci DC v síti tak, že se klient může přihlásit …
- …a to díky SRV záznamům

DNS and Active Directory Namespaces



SRV záznamy

- Identifikují stroj a služby, které nabízí.
- Autentizace, prohledávání, …
- Formát

Service.Protocol.Name Ttl Class SRV Priority Weight Port Target

_ldap._tcp.contoso.msft 600 IN SRV 0 100 389 london.contoso.msft