Osnova dnešní přednášky

Pracovní skupina x doména

Active Directory

- Něco z historie
- Použité technologie
- Pojmy

Instalace Active Directory

DNS

- DNS v Active Directory

Pracovní skupina x doména

Pracovní skupina

- Malé skupiny PC
- Omezené možnosti migrace uživatelů
- Žádné služby navíc

Doména

- Větší množství uživatelů,
- počítačů
- a nastavení aplikovatelných na ně

Historie

- 1993 … Windows NT 3.1 (Advanced Server)
- 1994 … Windows NT 3.5
- 1995 … Windows NT 3.51
- 1996 … Windows NT 4.0
- 2000 … Windows Server 2000 (NT 5.0)
- 2003 … Windows Server 2003 (NT 5.2)
- 2008 … Windows Server 2008 (NT 6.0)

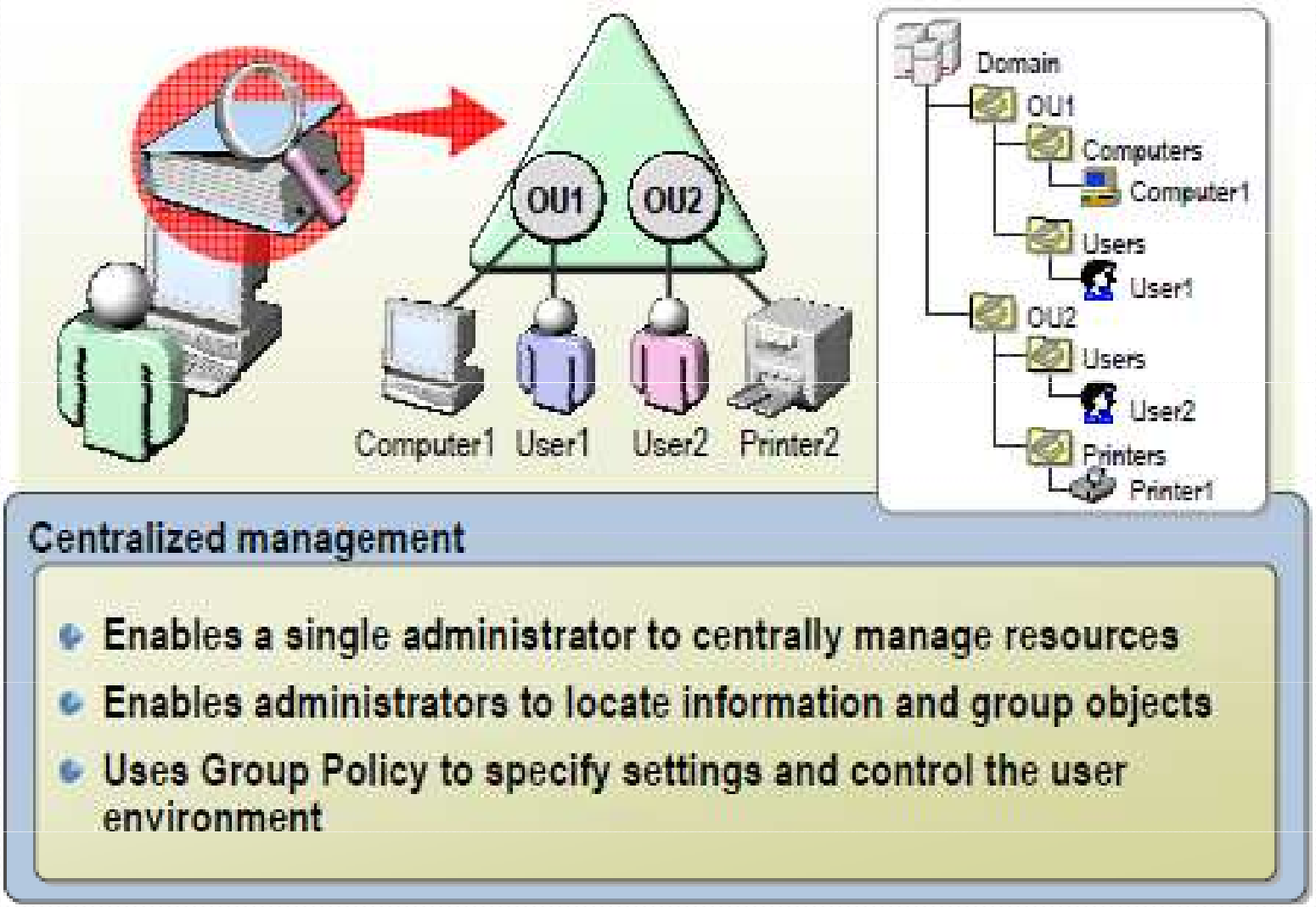
Active Directory (AD)

Proč?

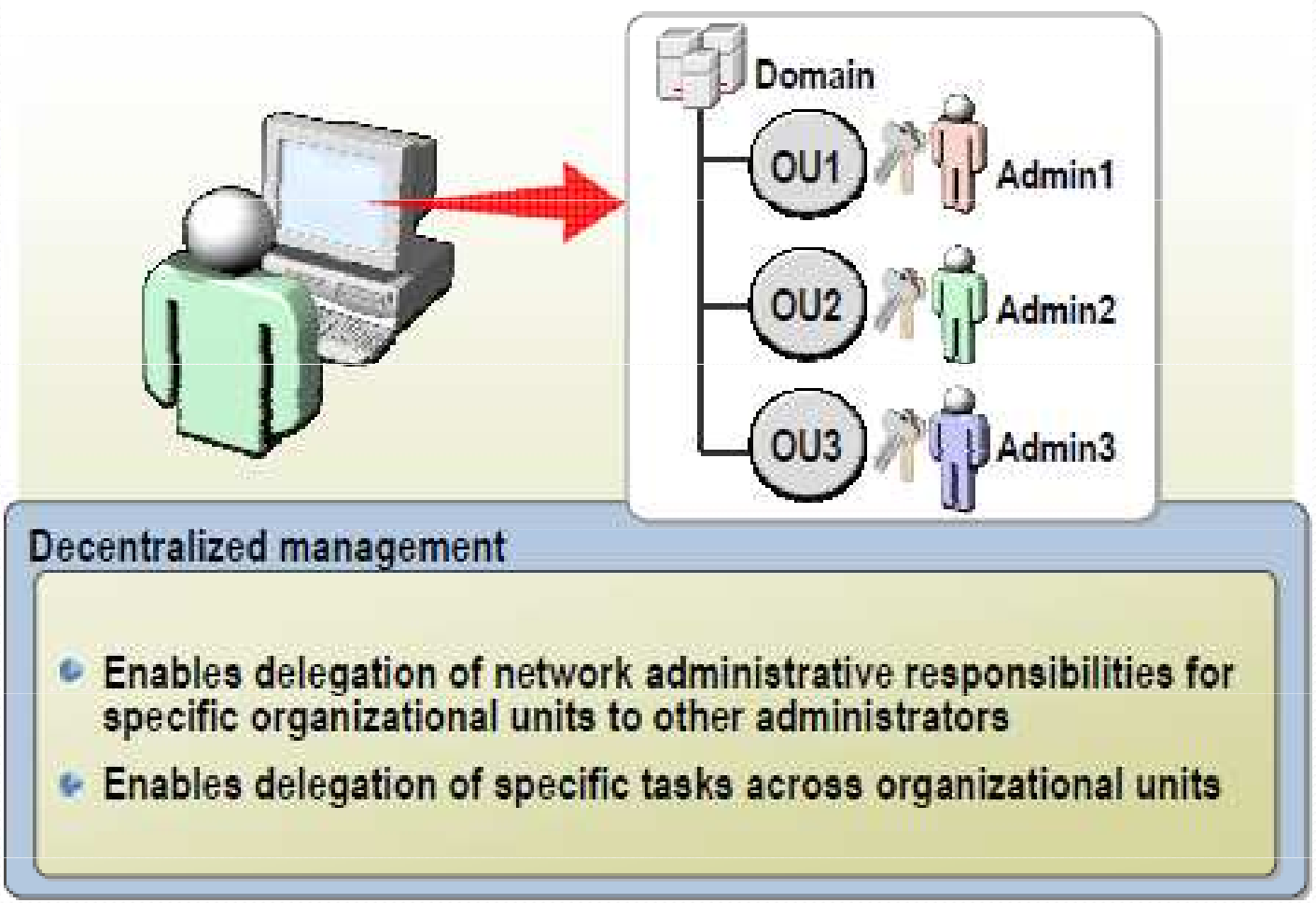
- Centralizuje správu síťových zdrojů
- Centralizuje a decentralizuje management zdrojů
- Je bezpečným skladištěm objektů s logickou hierarchickou strukturou
- Optimalizuje síťový provoz

Adresářová služba je založena na protokolu LDAP

Centralizovaný management AD



Decentralizovaný management AD



LDAP

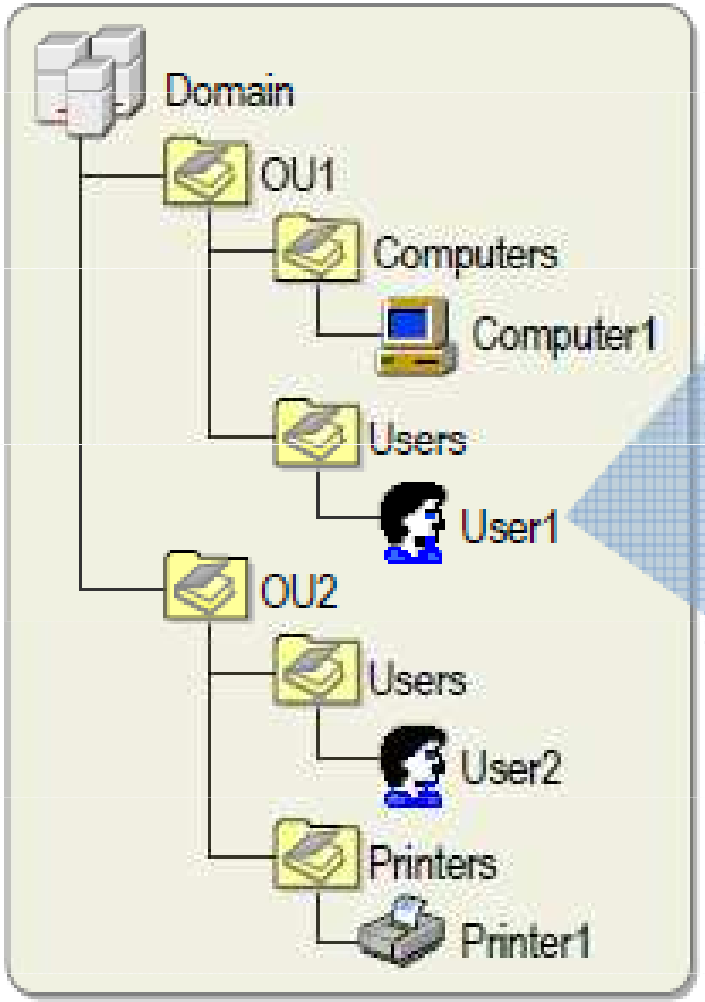
Lightweight Directory Access Protocol

- Protokol pro síťový přístup k adresářové službě
- Co je adresář?
  - Množina informací s podobnými atributy organizovaná do logické hierarchické struktury
- Potřeby telefonních služeb vedly ke vzniku specifikace X.500 a její implementace DAP
- DAP nebyl zcela nejvhodnější, chyběla podpora TCP/IP, vznik LDAP

Struktura LDAP

- Adresář je tvořen záznamy ve stromové struktuře
- Záznamy jsou tvořeny množinou atributů
- Každý záznam má v rámci stromu jedinečné jméno – Distinguished Name

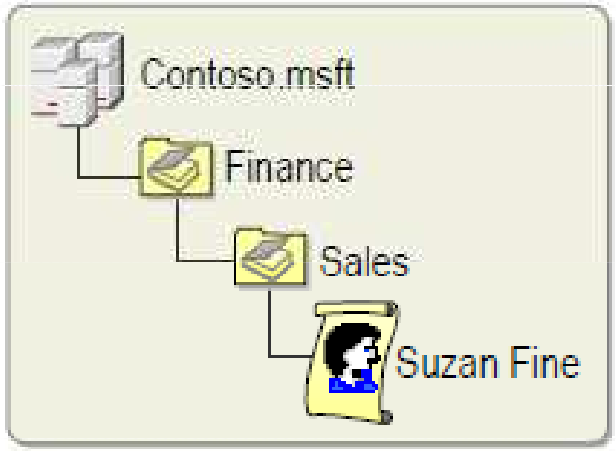
Adresářová služba (Directory Service)



Ferda Šiška	
Attributes	**Values**
Name	Ferda Šiška
Building	FI
Floor	2

Distinguished Name (DN)

Distinguished Name určuje doménu objektu a cestu, jak se k danému objektu dostat.



Relative distinguished name

CN=Suzan Fine,OU=Sales,OU=Finance,DC=contoso,DC=msft

Logická struktura AD

Kopíruje administrativní požadavky, geografickou polohu, …

Doména

- Sada účtů, počítačů, pravidel, …
- Poddoména – vztah child-parent

Strom (tree)

- Dvě a více domén se vztahem child-parent

Les (forest)

- Dva a více stromů

Logická struktura AD

Je možné zjemňovat členění v doméně:

Organizační jednotka (Object Unit, OU)

- Kontejner pro vlastní objekty
- Nejjemnější aplikace Group Policy
- Decentralizace správy

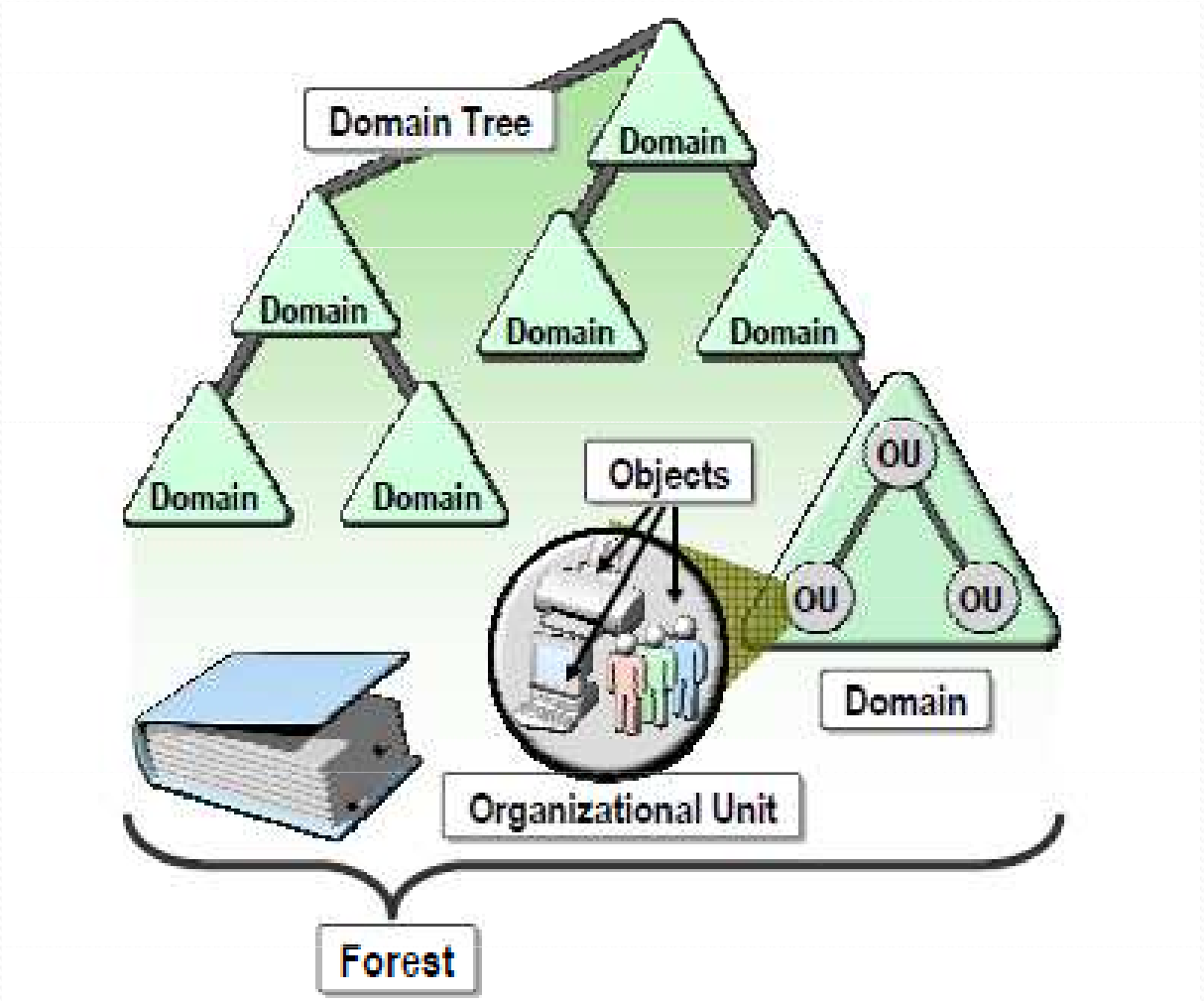
Vlastní objekty

- Množina jedinečných atributů určena ve Schematu

Atributy

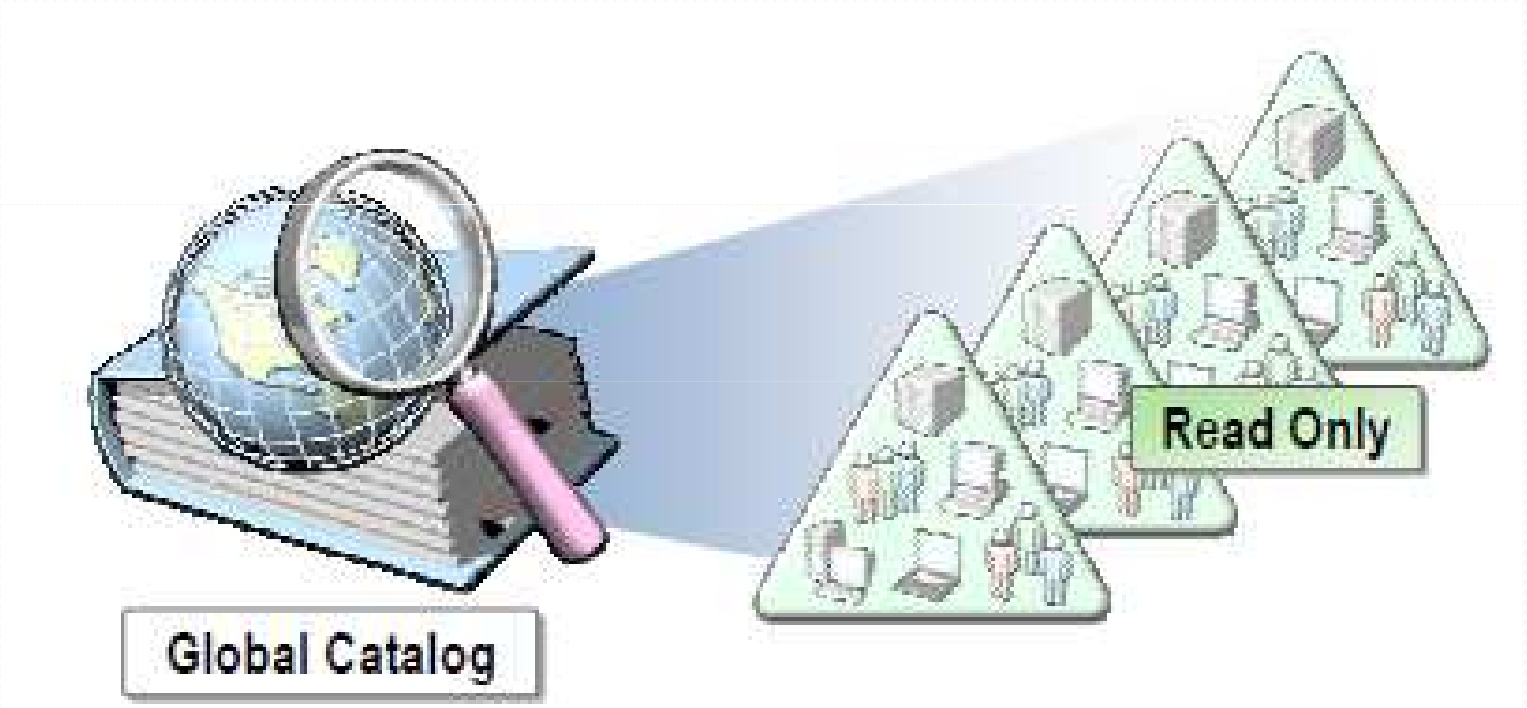
- Lze přidávat nové
- Editovat staré

Logická struktura AD



Global Catalog (GC)

- K prohledávání forestu
- Množina objektů s podmnožinou atributů



Trusts

Trusty umožňují uživatelům z jedné domény přistupovat ke zdrojům v doméně druhé.

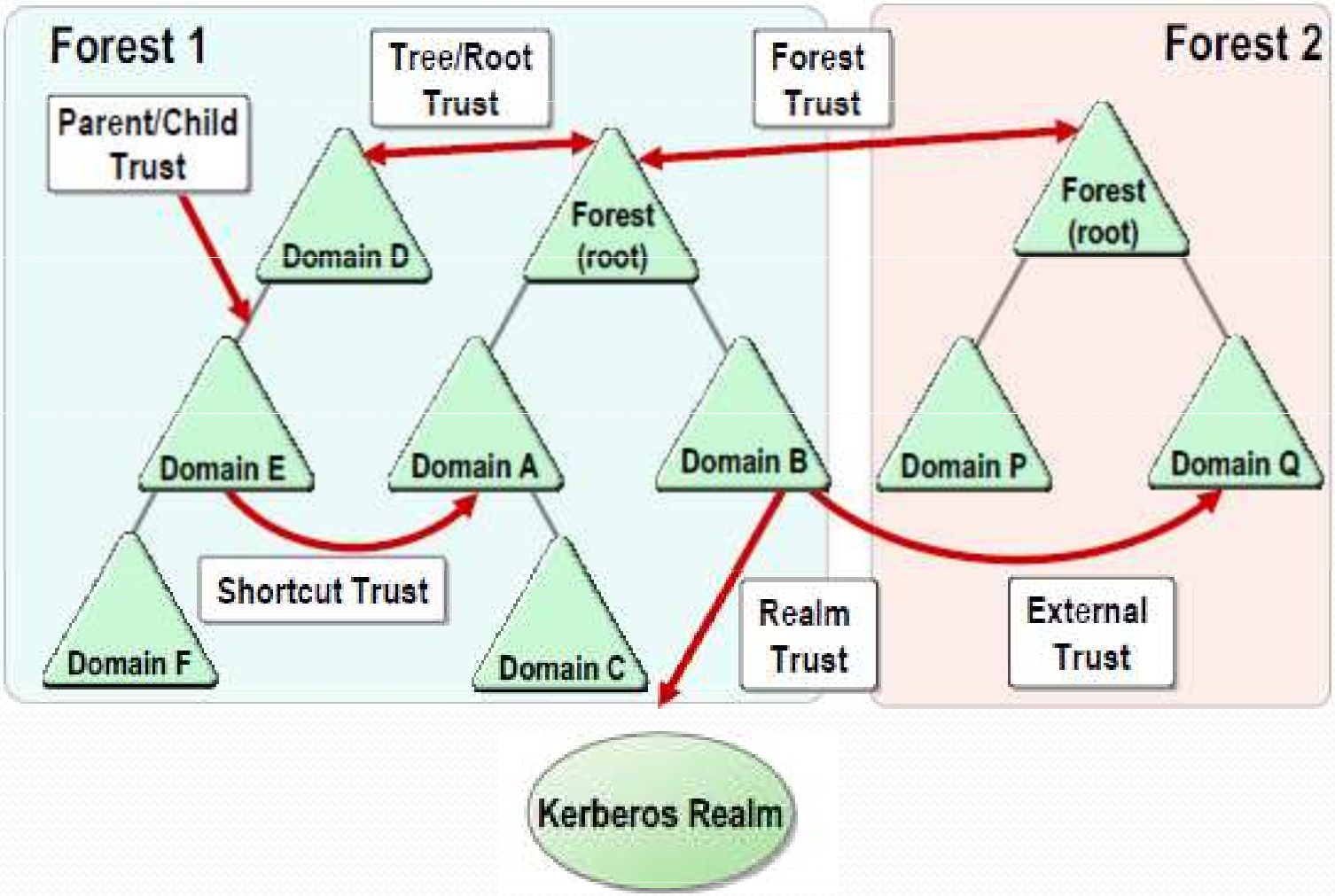
Základní hranicí důvěry je forest, nikoliv doména!

- S každou vytvořenou doménou se vytváří i vztah two-way transitive důvěry

Typy

- Jednocestný x dvoucestný
- Tranzitivní
- Implicitní
- Shortcut
- External
- Forest
- Realm

Trusts


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

Fyzická struktura AD

Sleduje a optimalizuje síťový provoz

- Kdy a jak bude probíhat replikace mezi servery

Domain Controller (DC)

- Počítač s Windows Server 2000/2003/2008 a službou AD
- Každý z řadičů domény poskytuje úložné a replikační funkce
- Na jednom řadiči pouze jedna doména

Active Directory Sites

- Logická jednotka řadičů s rychlým připojením
- Mezi těmito stroji probíhá komunikace velmi často za účelem replikace údajů

Fyzická struktura AD

AD partitions

- Domain partition
  - Doménové objekty
  - Určeno k replikaci
- Configuration Partition
  - Záznamy o topologii forestu
- Schema partition
  - Definice forest-wide schématu
  - Každý les má pouze jedno schéma kvůli konzistenci
  - Replikováno na každý z DC

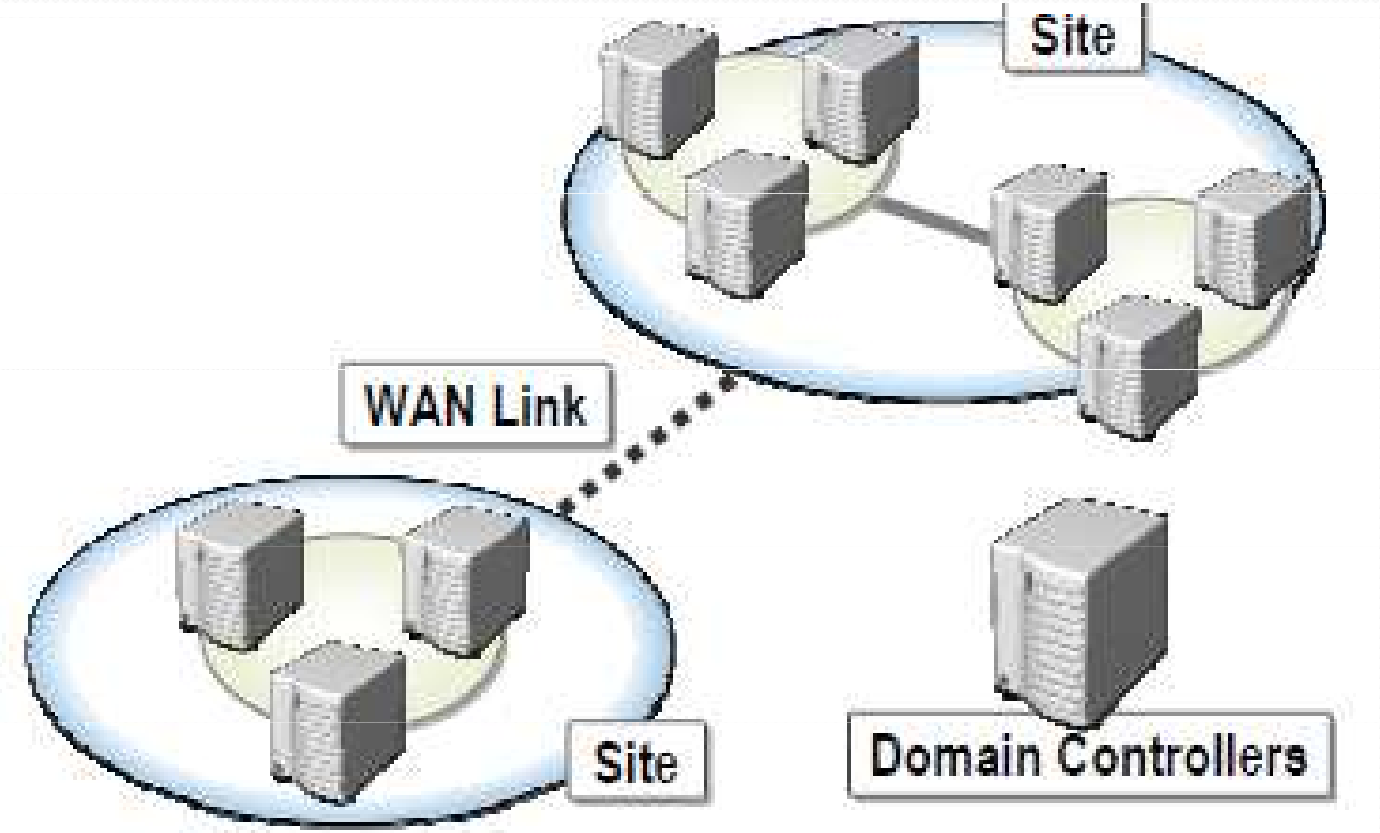
Fyzická struktura AD

Application partition

- Volitelné
- Nevztahují se k bezpečnosti, ale k aplikacím
- Lze replikovat na vybrané DC

- Domain Controllers
- Sites
- WAN Links

Fyzická struktura AD



Schema

Definuje všechny druhy objektů v AD

Object classes

- User, Printer, Computer

Attributes

- Jediněčně definovány
- Skládáním tvoříme objekty

Operation Masters

Multi-master replikace

- Více masterů – při výpadku jednoho nahrazení jiným
- Snižuje síťový provoz

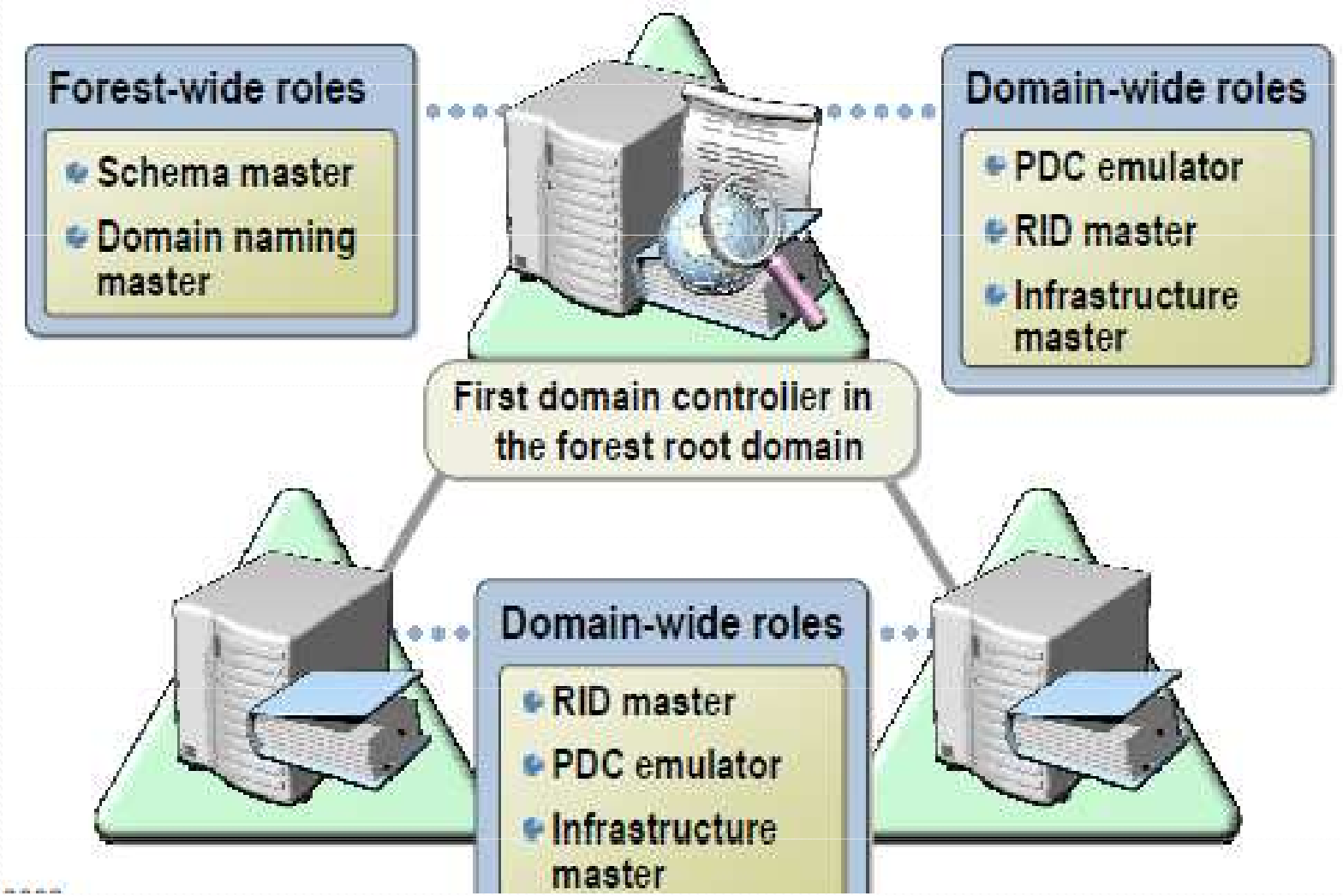
Flexible single master operation (FSMO)

- Přidání domény, změna schématu

Tyto operace sjednoceny do operations master roles

- Stroje jež je provádějí – Operation Masters

Operation Masters



Flexible Single Master Operations

Forest-wide

- Schema Master
  - Udržuje veškeré modifikace schematu forestu
- Domain Name Master
  - Sleduje jména všech domén ve forestu a je potřeba při přidávání nové nebo rušení existující domény z forestu

Flexible Single Master Operations

Domain-wide

- Relative ID Master
  - Každý objekt dostane po vytvoření jedinečné SID
  - Skládá se ze SIDu domény a jedinečného RIDu
  - Každé DC má svůj pool přidělený RID masterem
  - Při nedostatku žádá nový
- Infrastructure Master
  - Uchovává SIDy, GUIDy a DNs pro možnost odkazování objektů přes domény
  - Aktualizuje záznamy při přesunu objektu mezi doménami

Flexible Single Master Operations

- PDC Emulator
  - Zajišťuje zpětnou kompatibilitu s BDC v NT 4.0
  - Autoritativní zdroj času v doméně
  - Je upřednostňovaný ostatními DC pro replikaci a ověřování hesel

Instalace AD

Minimální požadavky

- Operační systém Windows Server
- NTFS oddíl s min. 250 MB
- Administrátorská práva
- Protokol TCP/IP
- DNS Server s podporou SRV záznamů

Spuštění pomocí

- Příkazu dcpromo
- Manage Your Server (v Administrative Tools)

Instalace AD

DNS název domény

- Pro zpětnou kompatibilitu i NetBios jméno

Dále určíme úložiště důležitých souborů

- Databáze AD a logy

Vytvoření SYSVOL složky

- Slouží k potřebám replikace
- Uložení politik, přihlašovacích skriptů (NETLOGON)

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

Nástroje pro správu AD

Příkazová řádka

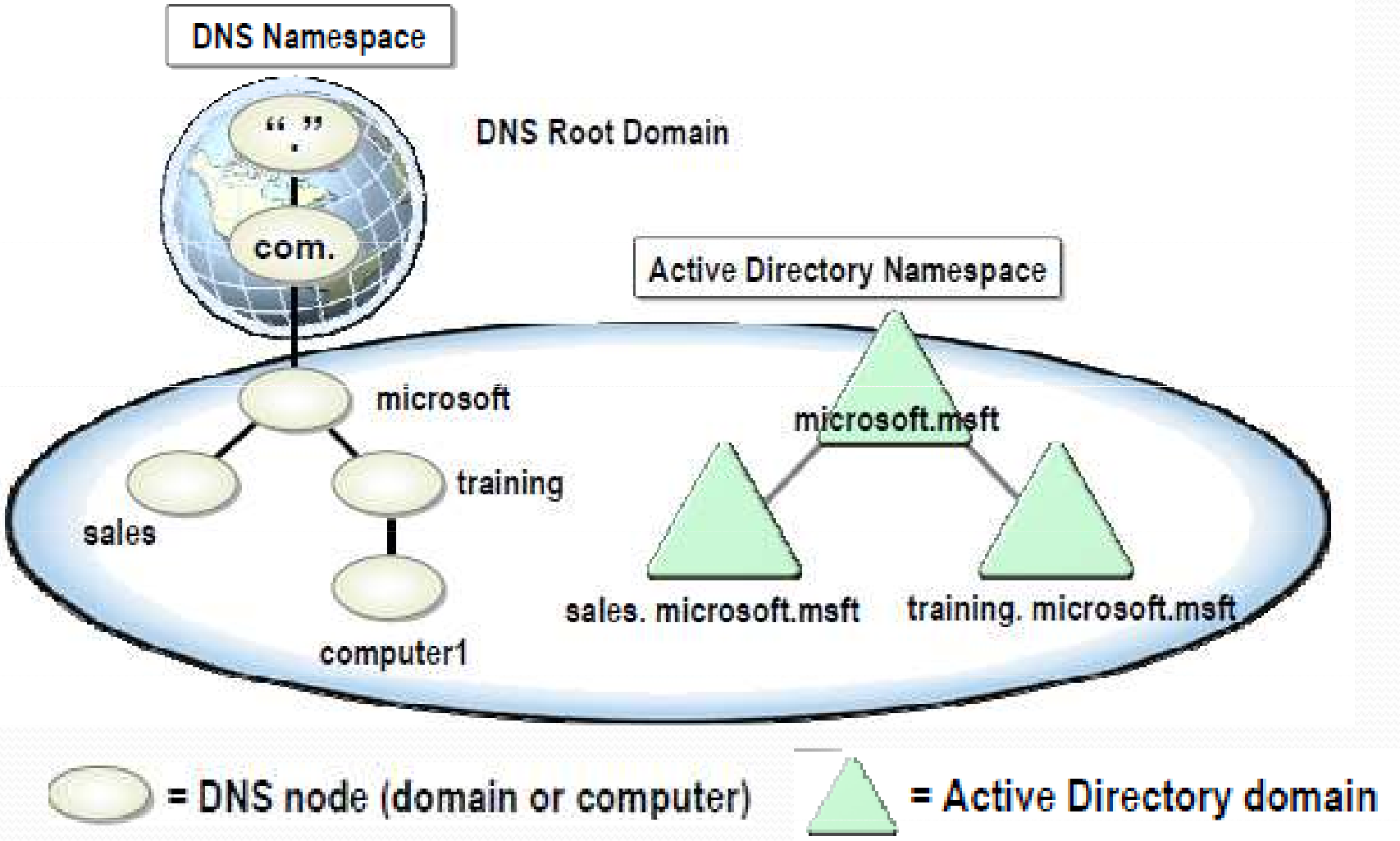
- Dsadd
- Dsmod
- Dsquery
- Dsmove

Windows Script Host

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.
- 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


DNS Namespace
" "
.
DNS Root Domain
com.
Active Directory Namespace
microsoft
training
sales
computer1
microsoft.msft
sales. microsoft.msft
training. microsoft.msft
= DNS node (domain or computer)
= Active Directory domain

SRV záznamy

- SRV záznamy jsou DNS záznamy, které mapují službu na počítač, který ji poskytuje.

- Formát SRV záznamu

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

- Příklad

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

Konec

Děkuji za pozornost ☺