Překlad jmen, úvod do Active Directory

Autoři: Šimon Suchomel,
David Leška

Překlad jmen

- motivace:

  jméno (např. služby sítě, stroje)

  www.muni.cz

  ⇔

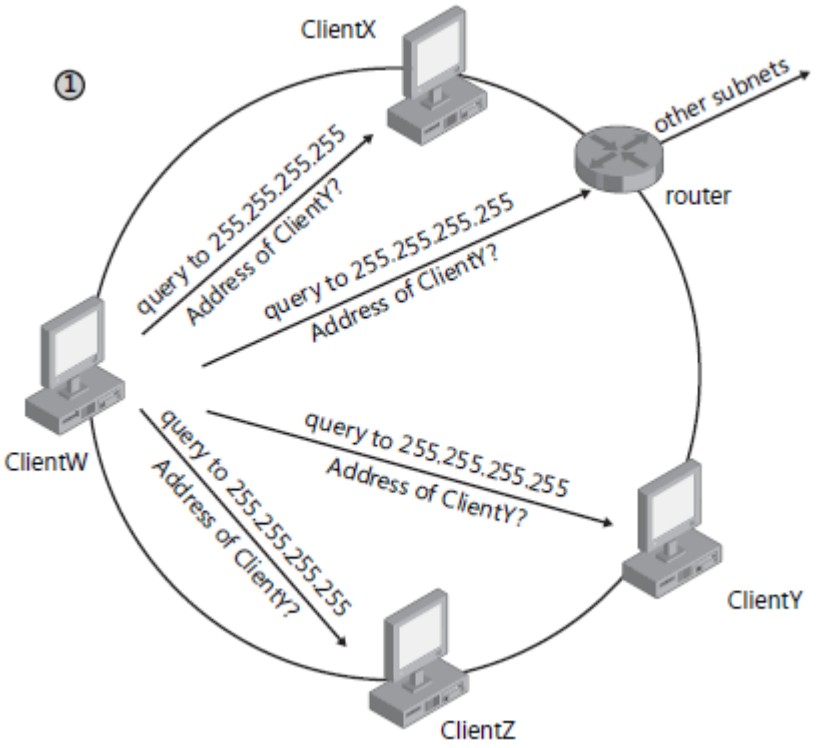
  umístění (adresa IP kam se stroj připojí)

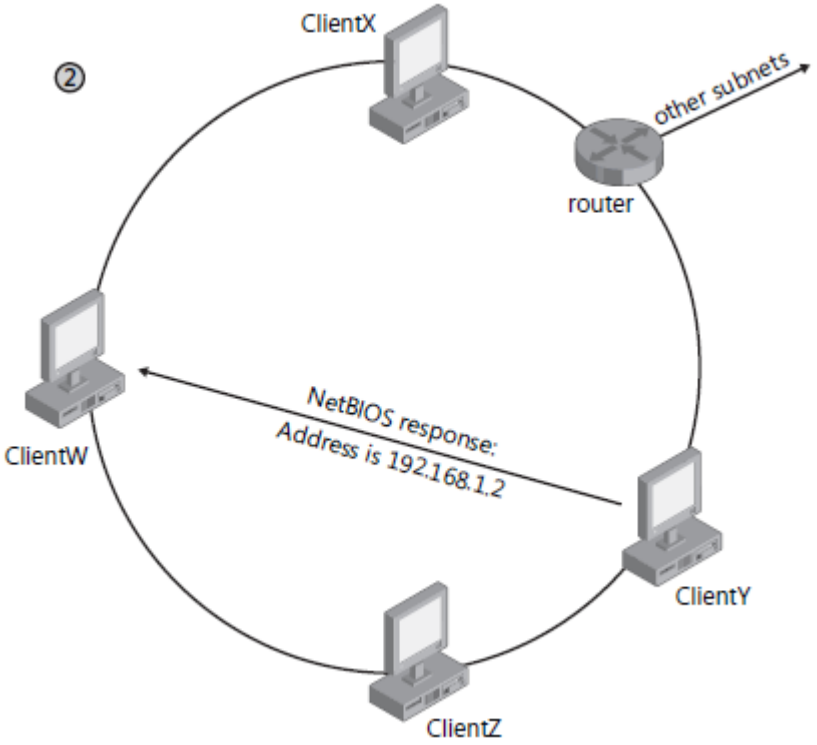
  147.251.5.237
- bez něj nefunguje nic

Překladové služby

- DNS, hierarchický, klient – server, bude probrán dále
- NetBIOS
- LLMNR (Link Local Multicast Name Resolution) Microsoft The Cable Guy Article

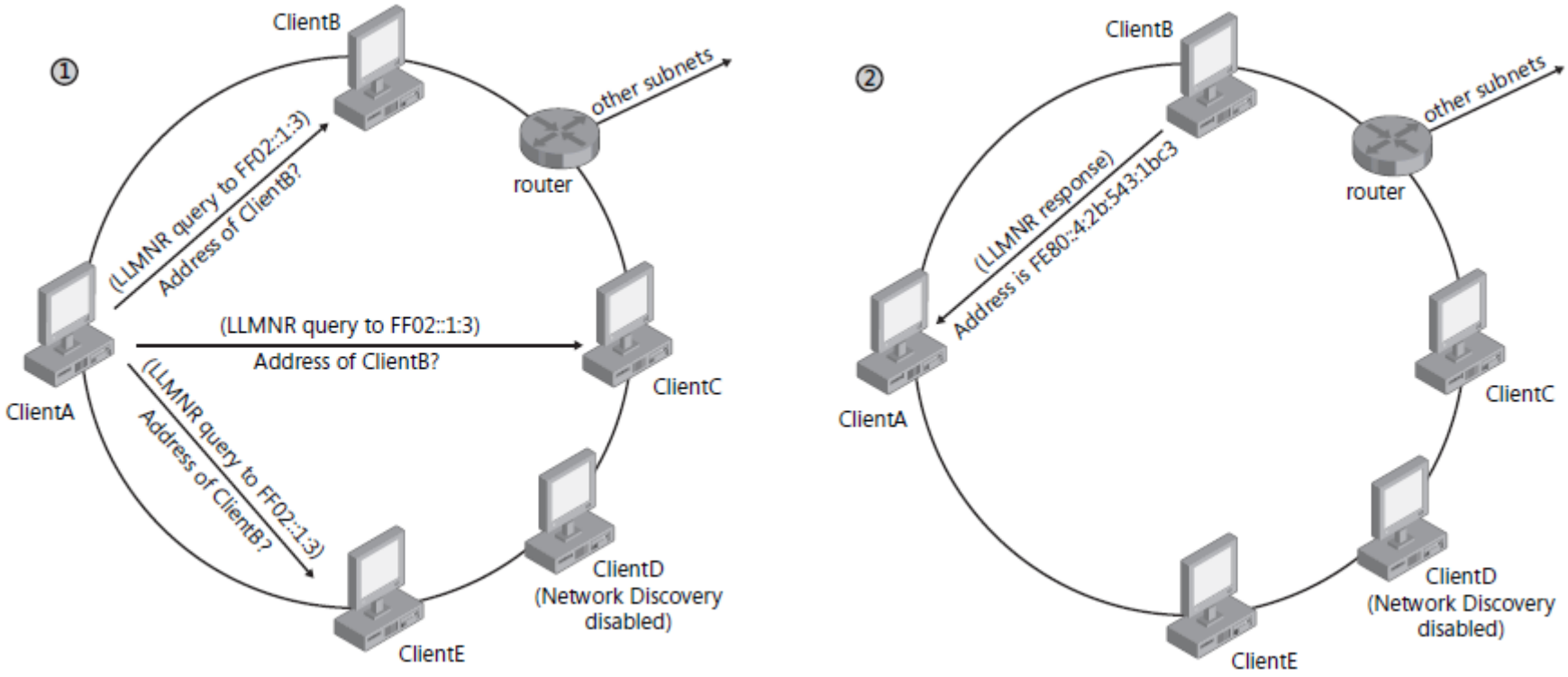
NetBIOS broadcast





Převzato z MCTS Self Paced Training Kit Exam 70-642.Configuring Windows Server 2008 Network

LLMNR multicast



Převzato z MCTS Self Paced Training Kit Exam 70-642.Configuring Windows Server 2008 Network

Statický překlad jmen

- NetBIOS – soubor LMHOSTS pro WINS

  147.251.53.156 nereis01 #PRE

- Host name – soubor HOSTS pro DNS

  147.251.48.66 atys

  147.251.48.17 artemis instalace

%SYSTEMROOT%\system32\drivers\etc\

Name Resolution Order

- Mnoho systémů překladu jména, jak Windows přesně jméno překládají?
- Default Name Resolution Order (lze měnit), jméno se hledá v tomto pořadí:
  1. Je to mé vlastní jméno?
  2. Hosts soubor.
  3. Dotaz na DNS servery.
  4. NetBIOS.

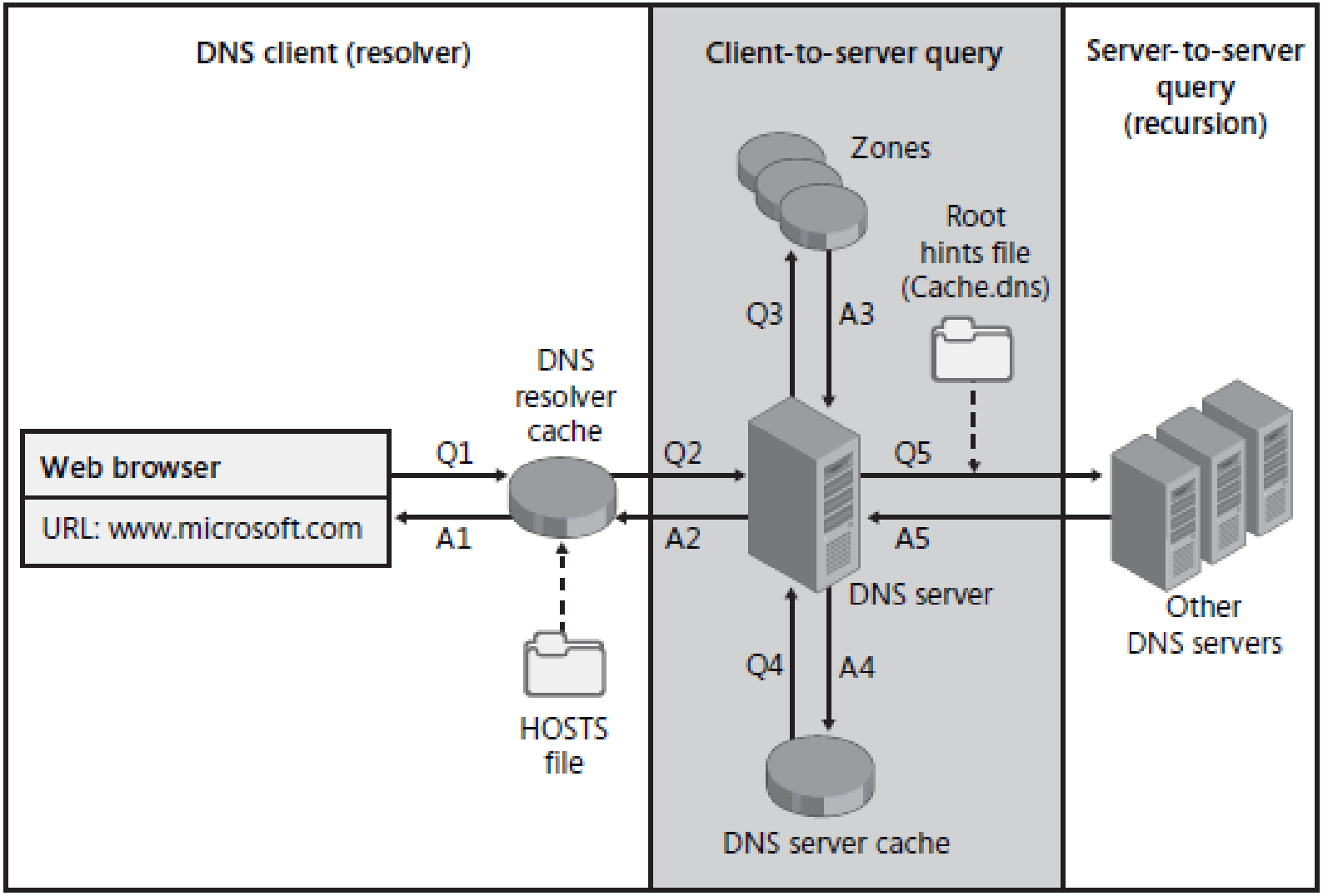
DNS

- Hierarchický systém doménových jmen
  - Root –> top level –> … př. www.muni.cz.
  - Private Domain Namespace př. jezek.local
- Protokol používá porty TCP/53 i UDP/53
- Architektura klient - server.
- Překlad jmen pro DNS klienty (typu host < – > IP) a dále zajišťuje informace o distribuci služeb v síti (SRV záznamy, služba < – > IP)
- Drží data: DNS server (autoritativní), DNS zóna

hostname

- Každý počítač má hostname
- na rozdíl od NetBIOSu použitelný v Internetu – hierarchický obor názvů
- Je částí FQDN, Fully Qualified Domain Name
  - atlantis.fi.muni.cz
- jediný hostitel může být v síti znám pod více hostitelskými jmény
- Pozn. UNC konvence
  - \\atlantis

DNS překlad



Převzato z MCTS Self Paced Training Kit Exam 70-642.Configuring Windows Server 2008 Network

Instalace DNS serveru

- Server manager – přidání role
- PowerShell Install-WindowsFeature –Name DNS –IncludeManagementTools
- Ověřit otevření TCP + UDP / 53 na FW
- DNS servery ať poslouchají jen na interní síťovce. Na obou serverech nastavit první server jako DNS, odebrat DNS server 4.33 ze druhé síťovky, nastavit primární DNS suffix

DNS zóny

- **primární** zóna: obsahuje informace o zóně v textovém souboru s možností zápisu; je vždy jen jedna. Soubory jsou v adresáři <System32>\DNS
- **sekundární** zóna: obsahuje informace o zóně v textovém souboru, ale pouze pro čtení
- zóna **integrovaná** do Active Directory: jedná se o primární zónu, která nemá záznamy v textovém souboru, ale ukládá je přímo do databáze AD
- **stub** zóna: tato zóna se použije, pokud potřebujeme spojit jmenné prostory více zón; obsahuje pouze SOA, NS a A záznamy jmenných serverů ostatních zón; je určena pouze pro čtení; může být integrovaná do AD

Zone transfer

- Replikace primární zóny na sekundární.
- AXFR IXFR.
- V plánovaných intervalech dle hodnot v SOA.
- Pokud se na primáru změnil serial number.
- Mimo plán lze nastavit change notification.
- AD integrovaná zóna má všechny servery primární, využívá se replikací AD.

Vytvoření zóny

- Z GUI DNS managera ‘dnsmgmt.msc’
- PowerShell:
- Primární: AddDnsServerPrimaryZone –Name ‘kredenc.moje’ –ZoneFile ‘kredenc.moje.dns’ –DynamicUpdate NonSecureAndSecure
- Sekundární: Add-DnsServerSecondaryZone -Name ‘kredenc.moje’ -ZoneFile ‘kredenc.moje.dns’ -MasterServers 10.10.10.1

DNS nejčastější typy záznamů

- host – address (A, AAAA) – běžný záznam, překlad jména na IP adresu počítače
- alias – canonical name (CNAME) – další jméno (alias) pro existující záznam v doméně
- mail exchanger (MX) – adresa poštovního serveru
- service location (SRV) – adresa konkrétní TCP/IP služby, jako ldap, kerberos, kms a další
- name server (NS) – seznam serverů, které zajišťují DNS služby pro doménu, záznam se nachází v nadřazené doméně a v aktuální doméně
- pointer (PTR) – užívá se pro reverzní překlad IP -> host, leží v reverzní zóně (1.10.10.10.in-addr.arpa, IP adresa v opačném pořadí plus speciální zóna)
- start of authority (SOA) – odkazuje na server, kde jsou primární údaje (primární NS), definuje základní vlastnosti zóny

Vytvoření DNS záznamu

- Z GUI DNS managera
- Powershell commandlety, např.
- Add-DnsServerResourceRecordA -Name “www" -ZoneName “kredenc.moje" -AllowUpdateAny -IPv4Address “10.10.10.5" -TimeToLive 01:00:00
- Univerzální commandlet pro zbytek záznamů: Add-DnsServerResourceRecord -ZoneName “kredenc.moje„ -A -Name “www”-IPv4Address 10.10.10.5
- Dynamicky, sám počítač nebo prostřednictvím DHCP serveru. Existuje úklid starých záznamu pomocí aging a scavenging.

Úkol k zónám

- Nainstalovat uvedenou infrastrukturu:
- Na prvním serveru primární DNS
- Druhý je jen DNS klientem prvního
- Na třetím serveru nainstalovat DNS server, nastavit DNS sufix, nastavit interní 10.X.X.X adresu jako DNS server, nastavit stub zónu pro kredenc.moje.
- Vyzkoušet resolvaci, nslookup….
- Volitelně nebo conditional forwarders.
- Add-DnsServerStubZone –Name ‘kredenc.moje’ –MasterServers 10.10.10.1,10.10.10.2 –ZoneFile ‘kredenc.moje.dns’

DNS Cache

- Snížení zátěže, uchovává odpověď po určitou dobu.
- Pozitivní: hodnota záznamu, negativní: nepodařilo se záznam najít, doporučena malá hodnota života negativního záznamu.
- Na klientu i serveru.
- Klientská: ipconfig /displaydns, ipconfig /flushdns, Clear-DnsClientCache, Get-DnsClientCache
- Serverová: z GUI (po zaškrtnutí View-Advanced) nebo powershell Show-DNSServerChache, Get-DNSServerChache, Set-DNSServerChache, Clear-DNSServerChache

Vybrané možnosti DNS

- Forwarders – DNS servery, na které se přeposílají dotazy
- Root Hints – předdefinované kořenové servery Internetu
- Dynamické záznamy v DNS – klienti se můžou registrovat, záznamy pak mohou stárnout (aging) a lze je uklízet (scavenging)
- DNS sufix list – umožňuje používat krátká jména

Kontrolní otázka

- Forwarders, root hints, conditional forwarders

- Jaký je rozdíl mezi forwarders a conditional forwarders?
  - Forwarders přeposílají vše
  - Conditional na vybranou zónu
  - Root hints se použijí v případě, že není forwarder

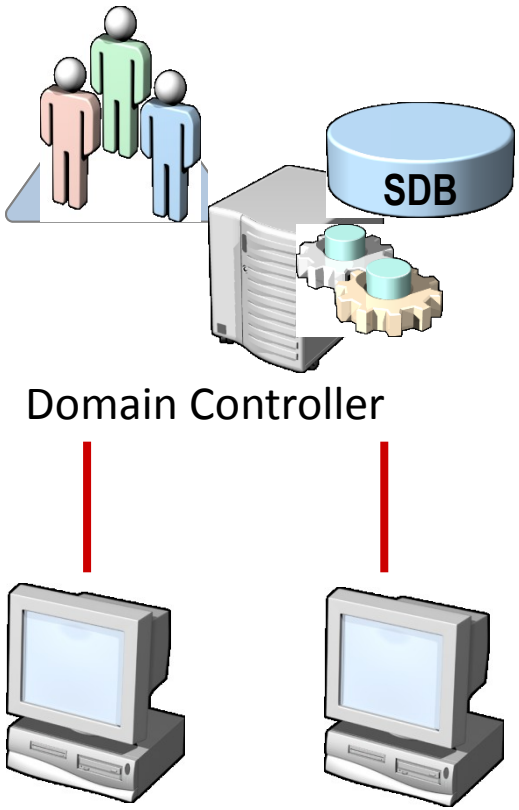
DNSSEC

- rozšiřuje DNS protokol o nové typy RR a příznaky v DNS zprávě, pro ověření pravosti DNS odpovědi
- DNSKEY klíč zóny
- RRSIG podpis společný pro RRset (skupina RR se stejnou hodnotou před typem)
- Kvůli kompatibilitě s klienty provádí validaci resolver na základě příznaku DO (DNSSEC OK) v doatzu. Úspěšná validace – je nastaven AD (Authenticated Data) příznak. Neúspěch, vrácena chyba SERVFAIL.

DNS Politiky

- Nastavení DNS serveru, neplést si s Windows Policy/GPO.
- Novinka ve Windows 2016 server.
- Dodatečná konfigurace ovlivňující chování DNS serveru.
- Mnoho možností, například odlišné odpovědi na dotazy podle adresy, času, geolokace serveru i klienta. Ochrana před útoky na DNS server. Aplikační load balancing.
- Více ve článku na MS Technet.

Úvod do Active Directory



- Centralizovaná správa
- Objekty bezpečně uloženy v jedné logické struktuře
- Optimalizuje síťový provoz
- Rozšiřitelnost
- Uživatel se přihlásí jedním účtem a má přístup ke všem prostředkům, na které má oprávnění v celé struktuře
- Oddělení logické struktury (domény, OU, objekty) od fyzické struktury sítě samotné

Struktura AD

- Logická struktura
  - Oddělení od fyzické reprezentace (sítě), pro zpřehlednění správy
  - Nezávisí na fyzickém umístění serverů, konektivitě mezi lokacemi
- Fyzická struktura
  - Popisuje servery a jejich propojení pomocí sítě

Základní terminologie

- Doména
  - Základní jednotka logické struktury AD, tvoří ji minimálně 1 DC
  - Umožňuje definovat administrativní hranice
  - Má vlastní zásady zabezpečení
  - Reprezentuje replikační hranici v AD
- Řadič domény (Domain Controller)
  - Server, který provozuje AD DS roli
  - Obsahuje kopii doménového adresáře – databázi
  - Na jednom DC může být v jeden okamžik pouze jedna doména
  - DC si mezi sebou vzájemně replikují informace o všech objektech v rámci domény
- Databáze Active Directory

Logická struktura databáze AD

- **Objekt**
  - Pojmenovaná množina atributů
  - Například uživatelský účet, může mít atributy: jméno, příjmení, email, tel. číslo, heslo,…
  - Objekty jsou ukládány v hierarchické struktuře pomocí kontejnerů (podobně jako soubory v adresářích)
- **Schéma**
  - Množina pravidel definující třídy objektů a atributů, které se mohou vyskytovat v adresáři
  - AD má objekt „uživatelský účet“ proto, že schéma definuje třídu objektu „uživatelský účet“ , atributy (jméno, příjmení, email, tel. číslo, heslo..) a asociaci mezi třídou objektu a atributy

Rozdělení AD služeb

- Active Directory Domain Services (AD DS)
- LDAP - Lightweight Directory Access Protocol
- Certificate Services
- Active Directory Rights Management Services (AD RMS)
- Active Directory Federation Services (AD FS)