15. Windows server 2008 / 2012, DNS princip, AD

Windows 2008

Vychází ze stejného kódu jako Windows Vista (Windows NT 6.0 kernel), se kterou sdílí mnoho ze své funkcionality a architektury. Automaticky tak těží z výhod nových technologií spojených s vývojem Windows Vista, jako je přebudovaný síťový modul (IPv6, nativní podpora bezdrátových sítí nebo zvýšení rychlosti a bezpečnosti), lepší podpora instalačních obrazů, spouštění a zálohování, širší možnosti diagnostiky, monitoringu a záznamu událostí serveru, lepší bezpečností prvky (Bitlocker, ASLR, RODC, vylepšený Windows Firewall), .NET Framework 3.0, vylepšení jádra a správy paměti a procesů.

Server Core

Snad nejvýraznější novinkou Windows Server 2008 je nová verze instalace označená jako Server Core. Je to zjednodušená instalace, ve které chybí Windows Explorer a veškerá nastavení se provádějí pomocí příkazového řádku nebo vzdáleně pomocí Microsoft Management Console (MMC). Server Core dále postrádá .NET Framework a další prvky. Server Core stroj může být konfigurován pro několik základních rolí: Doménový řadič/Active Directory doména, ADLDS (ADAM), DNS server, DHCP server, souborový server, tiskový server, Windows Media Server, Terminal Services Easy Print, TS Remote Programs a TS Gateway, IIS 7 web server a Windows Server Virtualization virtual server.

Windows 2012

Byly přidány různé funkce (s velkým důrazem na cloud), jako aktualizovaná verze Hyper-V, která se používá na správu IP adres, nová verze Správce úloh systému Windows a nový souborový systém.

DNS; Domain Name System

Systém, který překládá doménové názvy na IP adresy. Počítače mezi sebou komunikují pomocí IP adres. Ty jsou však pro člověka špatně zapamatovatelné a tak se vymyslely domény a vznikl systém DNS. Běžnému uživateli pak stačí zapamatovat si doménové jméno a DNS zařídí, že se prohlížeč spojí se správným serverem a zobrazí Vám požadované stránky.

Struktura

DNS systém tvoří hierarchickou stromovou strukturu. Každý uzel tohoto stromu obsahuje informace o části jména (doméně), které je mu přiděleno a odkazy na své podřízené domény. Kořen tohoto stromu, nultou úroveň, tvoří tečka. Na první úrovni se nacházejí Top Level Domains (TLD), které lze rozdělit do dvou základních tříd:

- **gTLD**
  - Generické TLD domény
    - .com, .net…
- **ccTLD**
  - Country-code TLD
    - .cz
  - Národní domény států
    - …

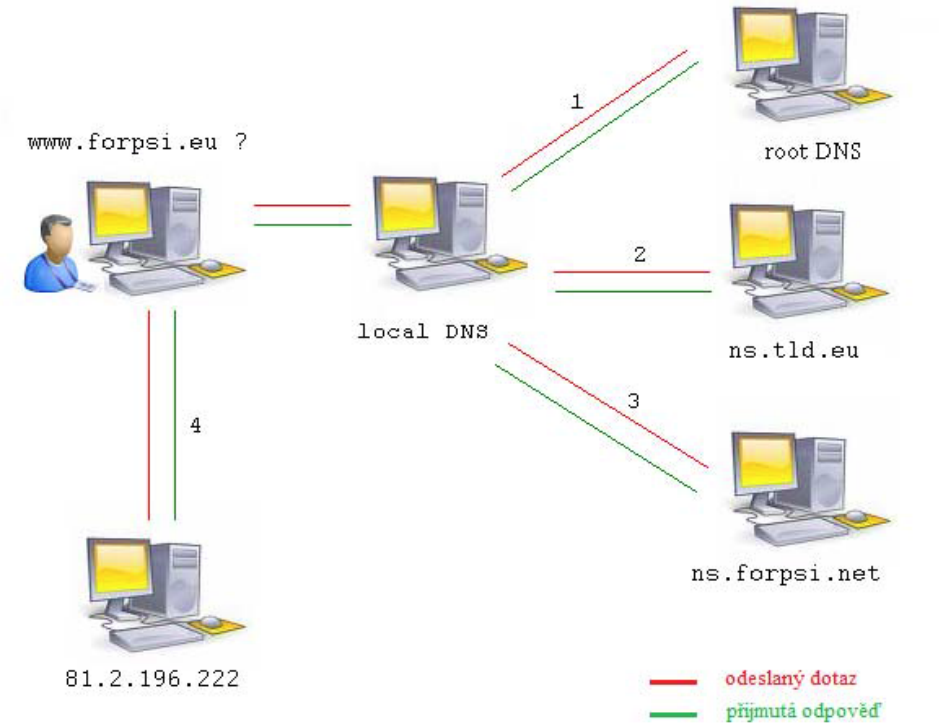
Každá doména může mít maximálně 127 úrovní. Jednotlivé subdomény mohou mít až 63 znaků (v praxi bývají zavedeny tvrdší limity) a celé doménové jméno z nich složené, může mít maximálně 255 ASCII znaků.

Typy DNS serverů

- **Primární**
  - Stará se o záznamy ve své zóně
  - Každá doména musí mít primární server
- **Sekundární**
  - Automatická kopie primární serveru pro případ jeho poruchy
  - Sám si průběžně kopíruje data z primárního serveru
- **Cachovací**
  - Slouží jako vyrovnávací paměť systému pro snížení zátěže a zrychlení odezvy
  - Uchovává výsledky a mezivýsledky dotazů dokud nevyprší jejich platnost
- **Root**
  - Kořenový server, který zná adresy autoritativních serverů všech domén TLD

Princip DNS

Každá doména má uvedeny autoritativní DNS servery, na kterých jsou uloženy konkrétní DNS záznamy ukazující na nějakou IP adresu. Autoritativní DNS servery jsou uvedeny také ve Whois databázi.



Každý má od poskytovatele internetu přiděleny lokální DNS servery (Cachovací). Prohlížeč se jich zeptá, zda znají IP adresu pro hledanou doménu (www.forpsi.eu). Server prohledá svou cache paměť, kde si data o IP adresách vždy na určitou dobu uchovává a pokud ji nenajde, ptá se dále.

- Zeptá se kořenových DNS serverů, zda znají IP adresu pro doménu www.forpsi.eu
  - Kořenový DNS server odpoví, že doménu nezná, ale ví, kdo spravuje DNS záznamy pro doménu EU
  - Pošle tento údaj
- Server informaci použije a zeptá se jednoho ze serverů pro doménu EU. Zda nezná IP adresu domény
  - Tento server pak odpoví, že doménu nezná, ale ví, které servery jsou autoritativní pro doménu forpsi.eu. a ty serveru pošle
- Server opět použije získanou informaci a zeptá se jednoho z autoritativních DNS serverů na doménu
  - Tento server již zná konkrétní IP adresu a tu lokálnímu serveru vrátí
  - Ten pak předá tuto IP adresu zpět prohlížeči → splnil svůj úkol.
- Prohlížeč pak kontaktuje přímo server pod danou IP adresou s požadavkem na zaslání webové stránky a ty zobrazí v počítači.

AD; Active Directory

Adresářové služby LDAP implementované firmou Microsoft pro řadu systémů Windows NT. Umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.

- Vyžaduje instalaci služby DNS
- Založena na standardních internetových protokolech
- Jednoznačně definuje strukturu sítě
- Organizuje skupiny počítačů a domén

Výhody

- Redukce celkových nákladů na vlastnictví
- Úspora času
- Zjednodušená administrace
  - Sdružení dat do jednoho místa (informace o uživatelích, různých zdrojích, aplikacích…)
- Flexibilita
- Škálovatelnost
  - Navrženo tak, že spolehlivě pracuje v jakékoliv velikosti
- Managment Console
  - Jednoduše lze vytvořit administrativní konzolu s takovými nástroji, které jsou potřeba, což umožní pracovat na jednom místě přehledně a efektivně
- Computer Managnemt
  - Nástroj, kterým se konfigurují počítače uživatelů z vlastního počítače

Vnější struktura Active Directory

- Služba Active Directory obsahuje logické i fyzické struktury součástí sítě
- Logická struktura Active Directory je tvořena doménami (domain), organizačními jednotkami (organizational unit), stromem (tree) a lesem (forest).

Doména

Skupina počítačů sdílejících společnou adresářovou databázi.

- Základní jednotka AD, tvoří ji min. 1 DC
- Bezpečnostní hranice ve struktuře Active Directory
- Reprezentuje replikační hranici
- Má jednoznačné označení
- Má vlastní zásady zabezpečení
- Vytváří vztahy důvěry s ostatními doménami

Lesy a stromy domén

- Každá doména služby Active Directory má název DNS (vsps.cz)
- V případě, kdy jedna nebo více domén sdílejí stejná adresářová data, nazývají se LES

Group Policy

Skupiny zásad (Group Policy) je nástroj pro hromadnou správu oprávnění a nastavení, aplikovaných jak na celý počítač, tak na přihlášeného uživatele. Ve skupinách zásad je možné vytvářet kolekce nastavení, kterým se říká Object GPO, které dokáží měnit konkrétní parametry chování počítače nebo uživatele. Samotné nastavení GPO se pak "linkuje" na jednotlivé organizační jednotku OU v AD, čímž se zajistí aplikování nastavení jen na vybrané počítače nebo uživatele. Tímto způsobem tedy můžeme spravovat potenciálně tisíce počítačů nebo uživatelů změnou jednoho GPO.

Použití

- Aplikování firemních standardů (skrytí ovládacích panelů, síťové tiskárny, spuštění scriptů…)
- Aplikování zabezpečení (změna oprávnění na určitých složkách, složitost hesla, skupiny s možností se lokálně přihlásit…)
- Hromadná instalace aplikací (Office, Adobe Reader, atd.)

Policy "Politiky"

- Politiky se dělí na Lokální a Doménové
- **Lokální**
  - Každý počítač od Windows 2000 má lokální politiky (local Group Policy), které ovlivňují lokální počítač a přihlášené uživatele
  - Pokud počítač není připojen do domény, tak právě lokální politiky jsou jako jediné použity