# 16. AD DS a DNS

## Teoretická část

**Popište a vysvětlete, k čemu slouží doména** **a jak pracuje v rámci serveru. Popište role AD DS a** **DNS, vysvětlete, jak se nastavují a jak pracují.**

## Praktická část

1. **Na serveru ukažte nastavení domény a DNS (Otevřít roli DNS a popsat)**
2. **Na serveru vytvořte doménový profil** **(V AD DS vytvořit uživatele)**

## Doplňující otázky

1. **Předveďte nastavení sítě a server manager.**

# Doména

Internetová doména (doménové jméno) je v [informatice](https://cs.wikipedia.org/wiki/Informatika) označení jednoznačného jména (identifikátoru) [počítače](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D) nebo [počítačové sítě](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5), které jsou připojené do [Internetu](https://cs.wikipedia.org/wiki/Internet).

Doména je přepis IP adresy na jméno. Přepis zajišťují DNS servery.

Doména je tvořena jednotlivými doménovými úrovněmi.

Doména na serveru pracuje jako svazek Koncových objektů (PC, Tisk, Server).

**Active Directory (AD)**

**AD je rozsáhlou adresářovou službou organizovaných do domén**. Tyto mohou být

organizovány do doménových stromů podle struktury DNS a mohou tak zasahovat I celosvětovou strukturu v Internetu. **Struktura je tvořena objekty**, z nichž některé jsou typu **uzlového** (mohou obsahovat další objekty) anebo typu **koncového** (samy o sobě představují nějaký prostředek sítě).

**Uzlové objekty:**

* **Domény** - jsou to nejvýše hierarchicky umístěné organizační útvary tvořící logickou strukturu
* **Organizační útvar** - slouží k seskupování objektů a složek uvnitř domén za účelem nastavení různých „skupinových politik“ (GPO)
* **Sítě a služby** - slouží k popisu fyzické struktury sítě v rámci domény; obsahuje umístění služeb, tiskáren a pracovních stanic do jednotlivých sítí (podsítí)
* **Složka** - slouží ke zpřehlednění struktury domény pro seskupování prostředků sítě stejného typu (např. skupiny, uživatelé, počítače apod.)

**Koncové objekty:**

* **Tiskárna**
* **Počítač** - pracovní stanice v rámci domény,
* **Doménový řadič** - server v doméně nesoucí DB s AD,
* **Uživatel** - uživatelský účet oprávněného uživatele domény,
* **Skupina** - jsou to buď předinstalované bezpečnostní skupiny (např. users, administrators apod.) nebo uživatelsky definované skupiny pro zjednodušení nastavení práv,
* **GPO** - bezpečnostní nastavení tzv. bezpečnostní politikou.

**Podmínky pro provoz AD**

* **Protokol TCP/IP**
* Jmenný server **DNS**
* Souborový systém **NTFS**
* **sdílený prostor** pro replikaci záznamů DB
* **administrátorská práva**
* **DHCP**

**Typy logických struktur:**

**1. doména**

Je to nejjednodušší struktura, která je tvořena objekty představujícími prostředky sítě, které mohou být seskupovány do organizačních útvarů (organizačních jednotek a složek). Pravidla bezpečnosti jsou pak definována jak pro doménu, tak pro organizační jednotky nebo fyzickou strukturu jako celek (sítě a služby).

**2. doménový strom**

Je to logický útvar, který je tvořen více doménami, které mohou být ve vzájemném hierarchickém vztahu s vazbami důvěry mezi nimi (trustees). Typickým příkladem takového stromu by mohl být Internet a struktura definována v DNS.

**3. doménový les**

Je to logický útvar, který může být tvořen více doménovými stromy, které také mohou být ve vzájemném hierarchickém vztahu s vazbami důvěry mezi nimi (trustees). Je to logický útvar pro korporativní vazby mezi velkými nadnárodními společnostmi.

Vztahy důvěry mezi doménami mohou být jednosměrné nebo obousměrné (vzájemné symetrické nebo nesymetrické) a tranzitivní nebo netranzitivní (nepřenáší se na nižší složky struktury). Standardní jsou vztahy obousměrné tranzitivní.

**Vytváření vazeb mezi doménami (trusty).**

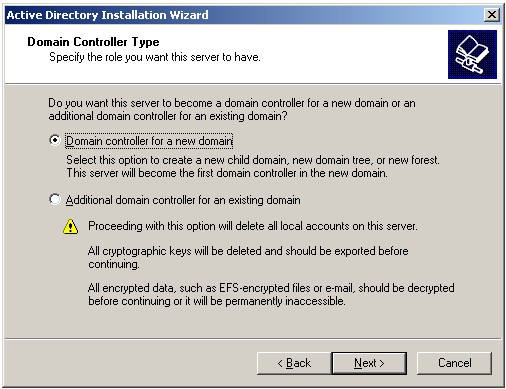
Tyto vazby se nastavují pouze uživatelem s plnými právy administratora, a to na

doménovém řadiči v doméně. Nastavuje se pomocí konzoly Domény a vztahy

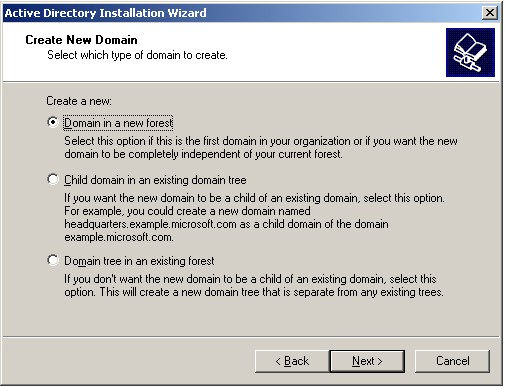
důvěrnosti>důvěry , kde je možné kontrolovat a nastavit důvěry pro danou domény (kterým doména důvěřuje a které domény důvěřují této doméně).

**Domain Controller**

*Doménový řadič* (Domain Controller je *počítač* (server), na kterém běží operační systém Windows Server a databáze Active Directory. V doméně může být více doménových řadičů a každý obsahuje úplnou repliku adresáře pro danou doménu. Na jednom řadiči může být pouze jedna doména. Doménový řadič také slouží k autentizaci uživatelů.

Pokud máme více DC a provedeme nějakou změnu v AD, tak ji provedeme na jednom z DC. Následně se provádí automatická *replikace* (periodicky plánovaná nebo v případě důležitých údajů okamžitá), aby ostatní DC měli stejný stav. Běžné replikace jsou typu *multimaster*, všechny DC jsou si rovny a mají zapisovatelnou kopii adresáře.

Instalace:



Dále určíte zda-li chcete založit nový les, novou doménu v existujícím stromu nebo založíte nový strom.

**DC** = server, který v doméně zajišťuje bezpečnost - přihlašování uživatelů, přístupová práva,

# DNS

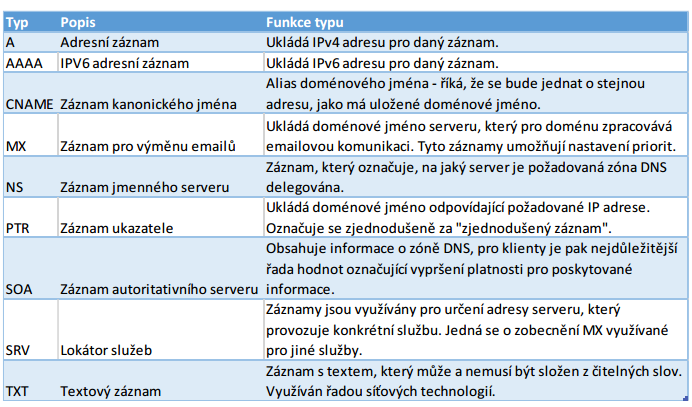
**DNS (Domain Name System) je hierarchický systém**[**doménových jmen**](https://cs.wikipedia.org/wiki/Dom%C3%A9nov%C3%A9_jm%C3%A9no), který je **realizován servery DNS** a **protokolem stejného jména**, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou **vzájemné převody doménových jmen a**[**IP adres**](https://cs.wikipedia.org/wiki/IP_adresa) [uzlů sítě](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_uzel). Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de fakto jako **distribuovaná databáze síťových informací**.

Protokol používá **porty**[**TCP**](https://cs.wikipedia.org/wiki/Transmission_Control_Protocol)**/53 i**[**UDP**](https://cs.wikipedia.org/wiki/User_Datagram_Protocol)**/53**, je definován v [RFC1035](http://www.faqs.org/rfcs/rfc1035.html). Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny [názvy domén](https://cs.wikipedia.org/wiki/Internetov%C3%A1_dom%C3%A9na). Jména domén umožňují lepší orientaci lidem, **adresy pro stroje jsou však vyjádřeny pomocí adres 32bitových (**[**IPv4**](https://cs.wikipedia.org/wiki/TCP/IP#IPv4)**) A záznam nebo 128bitových** ([IPv6](https://cs.wikipedia.org/wiki/TCP/IP#IPv6)) - AAAA záznam. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno - PTR záznam.

# Historie DNS

Protože je používání názvů pro člověka daleko příjemnější než používání číselných adres, vznikla už v dobách [ARPANETu](https://cs.wikipedia.org/wiki/ARPANET" \o "ARPANET) potřeba takový převod realizovat. Původně byl na všechny počítače distribuován jediný soubor (v Unixu /etc/**hosts**). Tato koncepce přestala velmi rychle vyhovovat potřebám a především nárokům na rychlou aktualizaci. Přesto se tento soubor dodnes používá, v závislosti na konfiguraci systému je možné jej použít buď prioritně před dotazem na DNS nebo v případě, že DNS neodpovídá. Je možné jej také použít k uložení vlastních přezdívek pro často navštěvované servery, případně také pro blokování reklam a podobně.

# DNS Záznamy

Pro přenos DNS dat po síti se využívá formátu záznamů, který je označován jako Resource Record. Jednotlivé záznamy v sobě, kromě jiného, obsahují typ záznamu (Qtype) a každý z typů v sobě nese odlišné informace, jejichž přehled je v Tabulce.

## Lookup Zone

Pro správu Microsoft DNS služby slouží snap-in do MMC konzole. V této konzoli se připojíme k určitému DNS serveru a ve stromu pod ním se nachází několik položek.

* *Cached Lookups* – každý DNS server standardně uchovává po určitou dobu záznamy, které v poslední době hledal, aby opakovaný dotaz mohl rychleji zodpovědět (pro zobrazení těchto záznamů musíme mít zapnuto Advanced View)
* *Forward Lookup Zones* – teprve zde jsou jednotlivé zóny (může jich být na serveru více), obsahuje mapování jmen na IP
* *Revers Lookup Zones* – obsahuje obrácené mapování IP adres na jména (PTR záznamy)

# Server Manager a nastavení Sítě

V server Manageru můžeme nastavovat náš Server.

* Jméno serveru
* Doména
* Firewall
* Remote Desktop
* IP Adresa
* Windows Update
* Time Zone
* Instalace Rolí
* Nastavení Rolí

# Nastavení sítě

Na kartě, sledování Performance monitor