Windows Server™ 2003 Active Directory®

Active Directory ukládá informace o počítačích, uživatelích a ostatních objektech v síti. Zpřístupňuje tyto zdroje uživatelům. Poskytuje komplexní informace o organizaci, pojmenovávání, správě, přístupu a zabezpečení těchto objektů.

Active Directory zajišťuje:

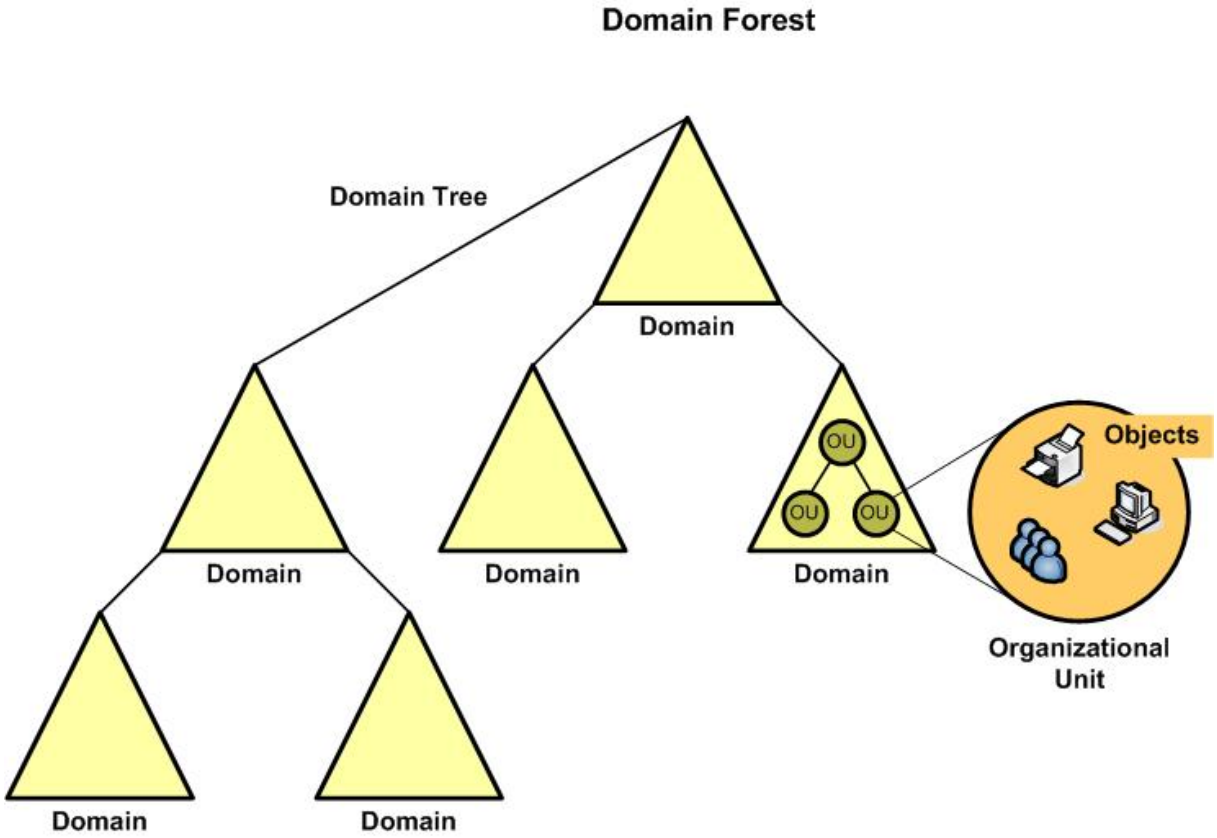
- Centrální řízení přístupu k síťovým prostředkům
- Centralizovaná a decentralizovaná správa síťových prostředků
- Ukládá objekty bezpečně v logické struktuře
- Optimalizuje síťový provoz

Centrální řízení přístupu k síťovým zdrojům zajistí, že pouze autorizovaní uživatelé získají přístup k síťovým prostředkům.

Centralizovaná správa síťových prostředků umožní administrátorovi spravovat prostředky z jednoho místa pomocí jednotného rozhraní. Struktura Active Directory nicméně umožní delegovat určité úkoly dalším administrátorům.

Veškeré objekty jsou v Active Directory uloženy bezpečně v hierarchické logické struktuře.

Fyzické struktura Active Directory umožňuje efektivně využívat kapacitu sítě. Uživatelé se vždy přihlašují k nejbližšímu serveru apod.



Logická struktura Active Directory

Logická struktura Active Directory se skládá z následujících komponent

- **Objekty (Objects)** – jsou základním prvkem logické struktury Active Directory. Každý objekt je definován skupinou atributů. Tyto atributy mohou nabývat různých hodnot. Každý objekt je sestaven z jedinečné kombinace těchto hodnot.

- **Organizační jednotky (Organizational Units)** – jsou to v podstatě kontejnery, které mohou sdružovat objekty podle typu, účelu apod. K jednotlivým organizačním jednotkám můžeme delegovat administrátora, který je bude spravovat.

- **Domény (Domains)** – jsou jádrem logické struktury Active Directory. Doména sdružuje definované objekty, které sdílí stejnou databázi AD, bezpečnostní politiku a vztahy důvěryhodnosti s ostatními doménami.

- **Doménové stromy (Domain Trees)** – domény sdružené dohromady v hierarchickém stromu. Přidáním další domény do stromu vznikne tzv. **Child Domain**. Je to doména, která má svou mateřskou doménu **Parent Domain** a její DNS název je kombinací mateřské domény a nového názvu (test.mojedomena.com). Říkáme, že strom má spojitý jmenný prostor.

- **Lesy (Forests)** – představují kompletní instanci Active Directory. Sestávají se z jednoho nebo více stromů. První doména lesa se nazývá **Forest Root Domain**. Les je hranicí pro schéma Active Directory.

Fyzická struktura Active Directory je tvořena

- **Doménovými řadiči (Domain Controllers) –** jsou to počítače s operačním systémem Windows Server 2000 nebo Windows Server 2003 a nainstalovanou službou Active Directory. Řadičů domény může (mělo by) být více.

- **Lokality (Sites)** – skupiny počítačů s bezpečným spojením, typicky LAN – 10 Mbps a více. Doménové řadiče uvnitř v rámci těchto lokalit komunikují často a přenáší mnoho dat. Lokality je důležité rozvrhnout podle možností propojení.

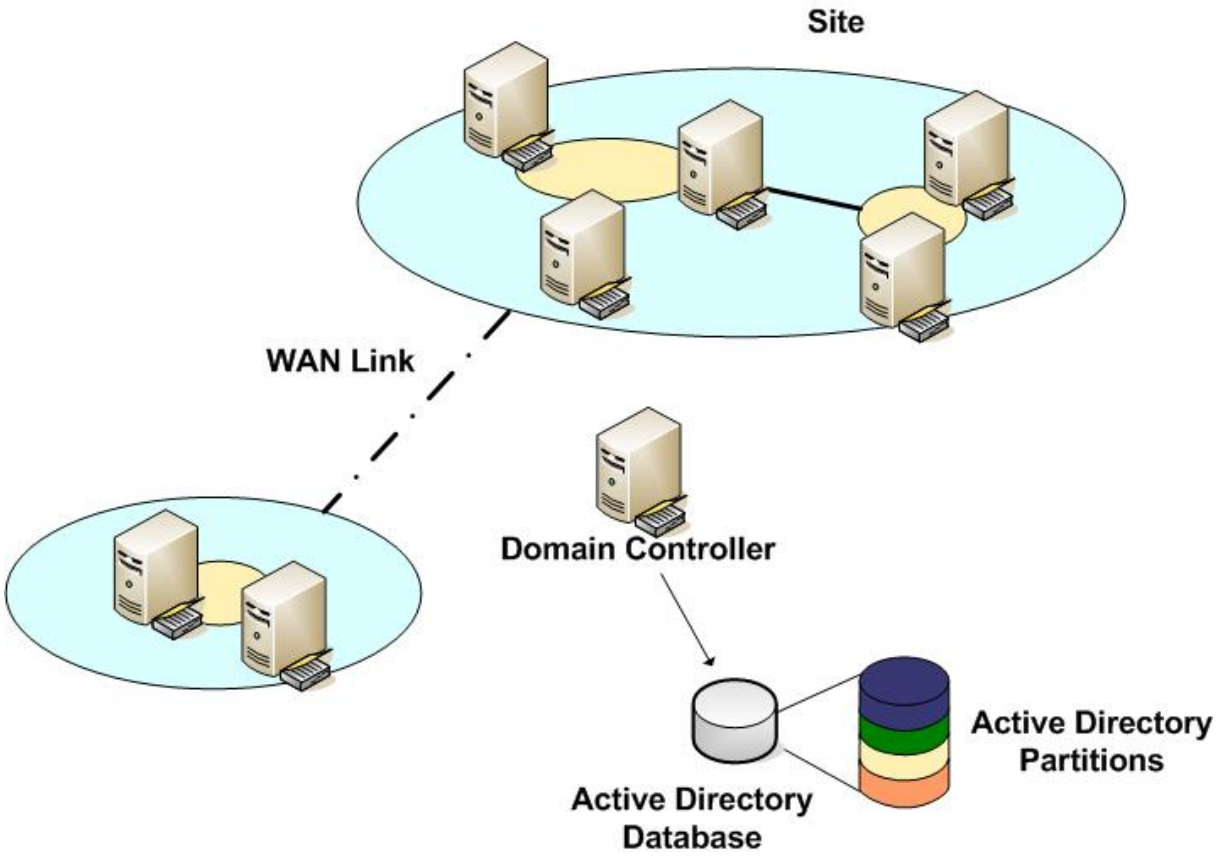
- **Oddíly Active Directory (Active Directory Partitions) –** v nich jsou umístěny vlastní data.

    - **Domain partition –** obsahuje repliky všech objektů v dané doméně, je replikován pouze v dané doméně.

    - **Configuration partition –** obsahuje topologii lesa tedy záznamy o všech řadičích a spojení mezi nimi. Je replikován v rámci celého lesa.

    - **Schema partition –** obsahuje informace o schématu Active Directory v daném lese. Je replikován v rámci celého lesa.

- **Application partition –** volitelný oddíl, je používán aplikacemi. Je replikován na zvolené doménové řadiče.



Fyzická struktura Active Directory

Druhy doménových řadičů

V doméně typu Windows Server 2000 nebo Windows Server 2003 nejsou doménové řadiče primární a záložní jako v doméně Windows NT 4.0. Přesto nejsou všechny řadiče domény stejné. Nazývají se **hlavní operační servery (Operations masters)**. Jednotlivé role serverů se označují jako **FSMO** role (Flexible Single Master Operations). Rozlišujeme následující typy:

- **Emulátor primárního řadiče domény (PDC Emulator) –** je důležitý pro zpětnou kompatibilitu s doménami Windows NT. Zajišťuje změny hesel pro počítače s operačním systémem Windows NT, Windows 98 nebo Windows 95. Minimalizuje prodlevy při změně hesel. Synchronizuje čas na všech doménových řadičích což je důležité pro přihlašování pomocí Kerberos v5. Řeší potenciální problémy v replikaci GPO.

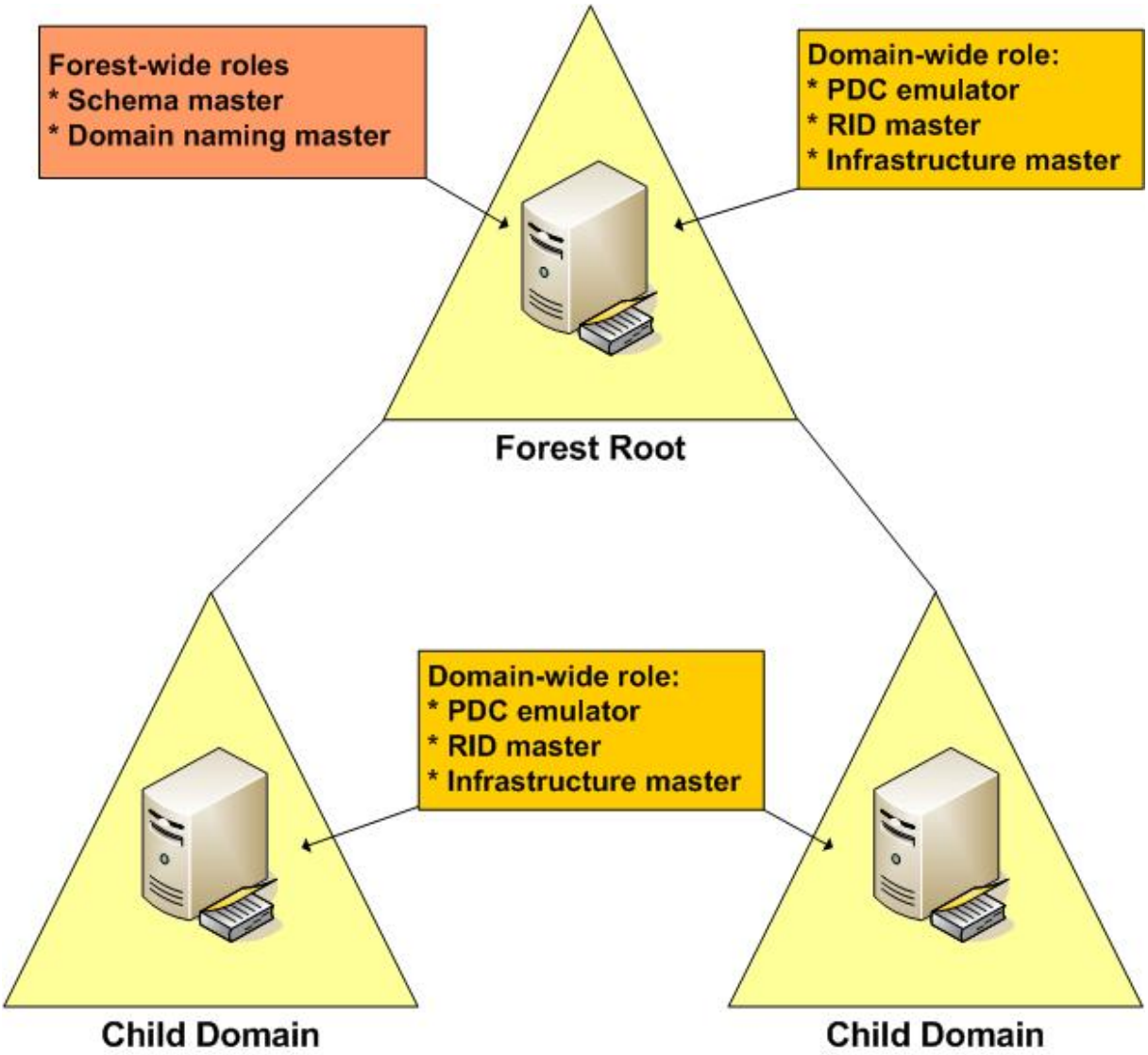
- **Správce relativních identifikátorů (RID Master) –** je důležitý při přesouvání objektů mezi doménami. Má na starosti smazání objektu po jeho přesunu do jiné domény, takže se nemůže stát, aby se objekt objevil při přesouvání ve více doménách.

$$ObjectSID = DomainSID + RID$$

- **Hlavní server infrastruktury (Infrastructure Master) –** má na starosti aktualizace referencí objektů, které ukazují do jiných domén. Jedná se zejména o univerzální skupiny. Tento řadič nemá význam pokud Active Directory obsahují pouze jedinou doménu.

- **Hlavní server schématu (Schema Master) –** řídí veškeré aktualizace schématu. Je tedy nezbytný při přidávání atributů k objektům. V lese je pouze jediný Schema Master.

- **Hlavní operační server pro pojmenovávání domén (Domain Namig Master)** – zajišťuje, že v lese nebudou dvě domény se stejným názvem. Je důležitý pouze při přidávání domén pomocí dcpromo. V lese je pouze jediný Domain Namig Master.



FSMO role řadičů domén

Globální katalog

Jedná se o speciální typ doménového řadič, který obsahuje výběr informací o všech objektech v Active Directory. Díky němu nemusí dotaz do Active Directory prohledávat všechny domény v lese. Efektivně zpracovává veškeré dotazy napříč celou strukturou Active Directory.

Globální katalog je nezbytný pro správnou funkci aplikací jako Microsoft Exchange apod. Dále umožňuje přihlašování do sítě na základě členství v univerzálních skupinách.

Platí pravidlo, že pokud je v dané lokalitě více uživatelů (>50) je vhodné tam umístit globální katalog.

Jednoznačná jména – Distinguished Names

Veškeré dotazy do Active Directory probíhají pomocí **protokolu LDAP** - Lightweight Directory Access Protocol. LDAP je podmnožinou standardu X.500.

LDAP používá k identifikaci objektu jednoznačné jméno, které se skládá z několika částí. Jméno musí být unikátní v celé struktuře Active Directory. Musí být také zajištěno, že žádné dva objekty v jednom kontejneru nebudou mít stejné jméno. Jméno, které identifikuje objekty v rámci jednoho kontejneru se nazývá relativní jednoznačné jméno – Relative Distinguished Name.

Jednoznačné jméno se skládá těchto částí:

- CN – Common Name, jméno objektu v kontejneru
- OU – Organizational Unit, jméno organizační jednotky, která obsahuje objekt. Organizačních jednotek může být v názvu více.
- DC – Domain Component, jméno obsahuje vždy alespoň 2 části typu DC jedná se o název domény jako vscht nebo cz

Celé jméno pak vypadá takto:

CN=Jan Novák, OU=UPRT, DC=vscht, DC=cz