Strategický rozvoj Univerzity Hradec Králové
CZ.02.2.69/0.0/0.0/16_015/0002427

Úvod do Active Directory

Mgr. Josef Horálek, Ph.D.

Co je to AD a k čemu slouží

Active Directory je adresářová služba. Pod pojmem adresářová služba si můžeme představit skupinu aplikací, které organizují informace o počítačích, uživatelích, skupinách a dalších zdrojích v počítačové síti. Tyto získané informace jsou zprostředkovávány správcům AD, uživatelům, aplikacím apod. a jsou uloženy v *„centrální organizované databázi (databáze informací o objektech a jejich vzájemných vztazích)“* (1). AD je založena na principu fungování síťového protokolu LDAP, kde je jeho funkčnost jednou z nezbytných součástí.

> *LDAP (Lightweight Directory Access Protocol) je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře)*

„AD je adresářová služba od společnosti Microsoft založená na LDAP. V současné době je nejpoužívanější adresářovou službou. Hlavní cíl AD je ověřovat uživatele a počítače vůči doméně a spravovat politiky členských počítačů, …“ (1)

V roce 1999 byla služba Active Directory, od společnosti Microsoft, poprvé představena a její první implementace byla uvedena v operačním systému Windows 2000 Server.
V následujících verzích Windows serverů byla postupně vylepšována funkčnost a správa služby Active Directory.

Od verze Microsoft Windows Server 2008 je pro Active Directory používán název Active Directory Domain Services (ADDS). Od této verze systému je oproti předchozím verzím poskytována minimalistická instalace serveru tzv. Server Core, která představuje minimální nutnou konfiguraci pro samotný běh OS. Windows Server umožňuje doinstalování rolí, ve kterých bude server vystupovat pro okolní svět. Když se řekne Active Directory, je obecně myšlena role Microsoft Windows Server – Active Direcory Domain Services (ADDS). Každá taková role serveru se skládá ze služeb, které obsahují funkce. Je potřeba zmínit, že pod název AD patří i další služby, kterými jsou:

- ADDS – Služby domén Active Directory (Active Directory Domain Services)
- ADCS – Služby certifikátů Active Directory (Active Directory Certificate Services)
- ADFS – Služby federace Active Directory (Active Directory Federation Services)
- ADLDS – Active Directory Lightweight Directory Services
- ADRMS – Active Directory Rights Management Services

Hlavním úkolem AD je ověřování uživatelů a počítačů v doméně a správa politik na ně aplikovaných. AD je tvořena objekty, které představují počítače, uživatelské účty, skupiny apod. V současné době patří AD mezi nejpoužívanější adresářovou službu. (1)

Možnosti využití AD

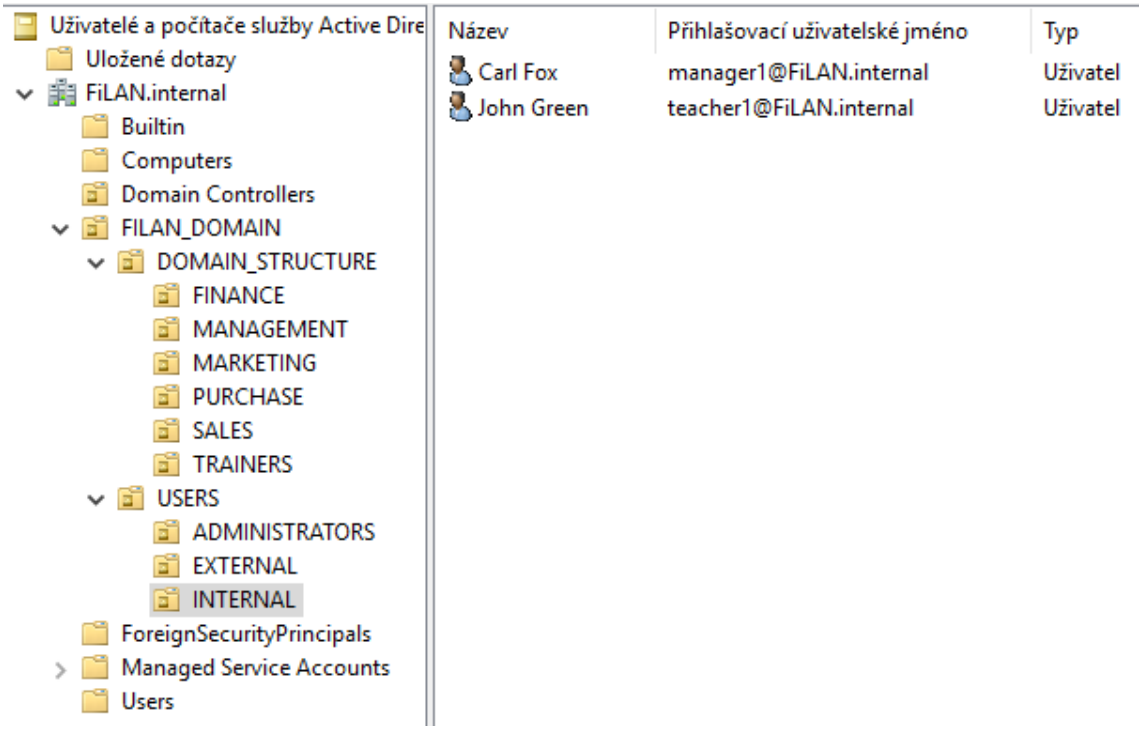
AD můžeme využít v každém prostředí, ve kterém je zajištěn správný síťový provoz a je vyžadován přístup 24/7 (provoz 24hodin, 7 dní v týdnu). Taková prostředí mohou představovat firemní organizace, nemocnice, správní instituce apod., ve kterých často dochází ke změnám uživatelů a používaných zařízení. AD dokáže zajistit jejich efektivní správu při vysoké úrovni zabezpečení. Další z hlavních výhod je, že nemá žádné omezení na velikost lokality, kterou má pokrýt.

Komponenty AD

Active Directory je dělena dle dvou základních kritérií – logická struktura a fyzická struktura.

Logická struktura je používána, aby byla správně chápána organizace domény a doménových zdrojů. Na logické úrovni je vytvořeno hierarchické uskupení. Správně vytvořená logická struktura by měla odrážet skutečnou situaci prostředí, ve kterém je aplikována. Její nejmenší jednotkou je objektový list (Leaf Object), což je objekt, který nemá žádné další „potomky“. Jako Leaf Object je možné si představit např. konkrétního uživatele, počítač nebo tiskárnu.

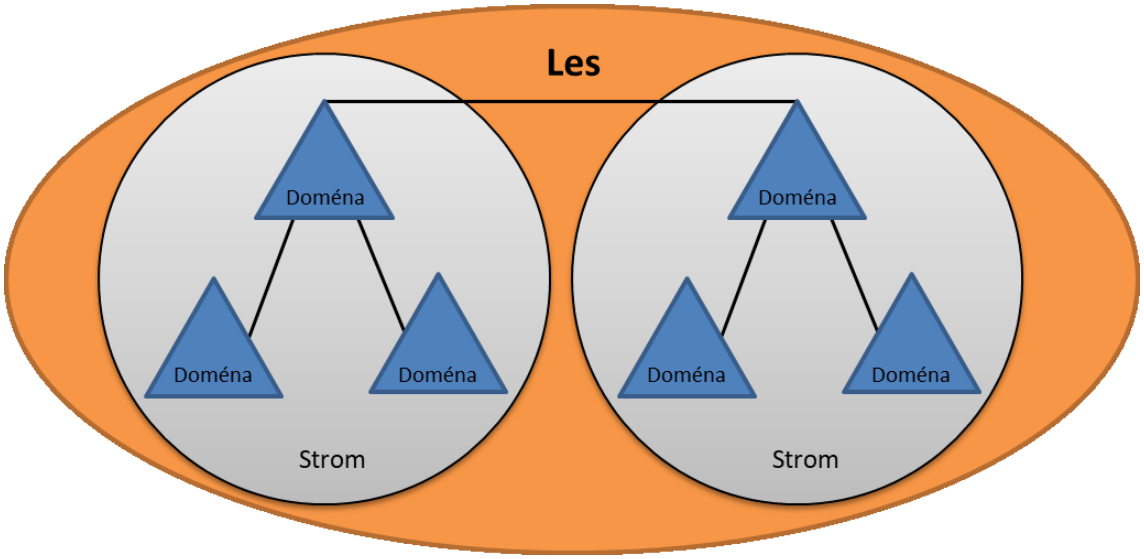
Fyzickou strukturu představují fyzická zařízení, kterými jsou např. doménové kontroléry (DC), sítě a podsítě (site) (2)



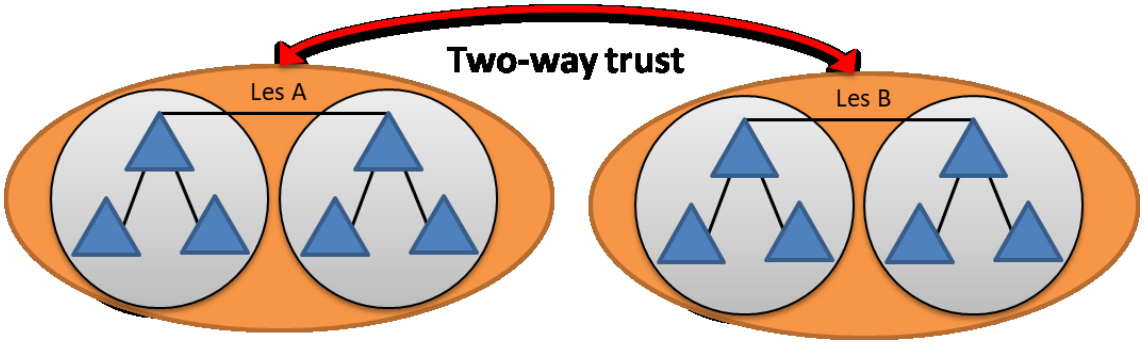
Obr. 1 Ukázková reprezentace logické struktury

Les

Les je objektový kontejner na nejvyšší úrovni v logické struktuře. Les představuje společný prostor pro jeho podřazené prvky. Pro existenci lesa je potřeba alespoň jednoho stromu. Zahrnuje v sobě domény, schémata, konfigurace a další informace. V lese je nejdůležitějším prvkem tzv. **Root Domain**, která představuje nejvyšší úroveň jmenného prostoru (**Namespace**) v rámci jednoho celého lesa. Každá doména v lese pracuje nezávisle, ale díky lesu je umožněna jejich vzájemná komunikace. V případě požadavků na vytvoření větší sítě je možné propojit více lesů vzájemně pomocí implicitního dvoucestného vztahu důvěry (**Forest Trust**). (3)



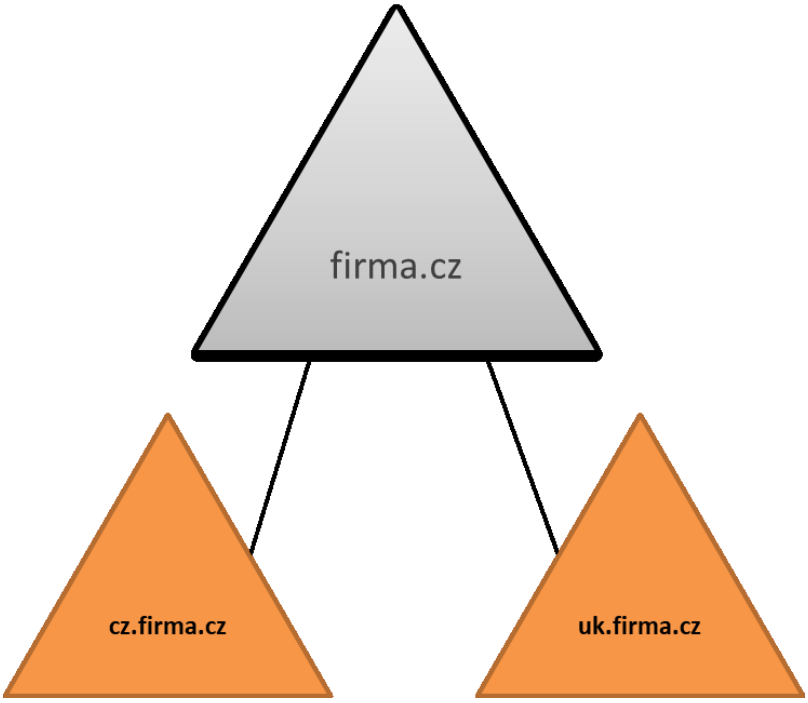
Obr. 2 Les



Obr. 3 Forest trust – propojení více lesů

Strom

Strom je objektový kontejner podřízený objektovému kontejneru les a nadřazený doméně. Každý strom patří do nějakého lesa. Strom může obsahovat libovolný počet domén nižšího řádu. Obrázek č. 4 vyobrazuje propojení rodičovské domény (Parent Domain) **firma.cz** s podřízenými doménami (Child Domain) **cz.firma.cz** a **uk.firma.cz**. Doména **firma.cz** je považována za kořenovou doménu (Root Domain). Domény v jednom stromě sdílí vlastní jmenný prostor. (3)

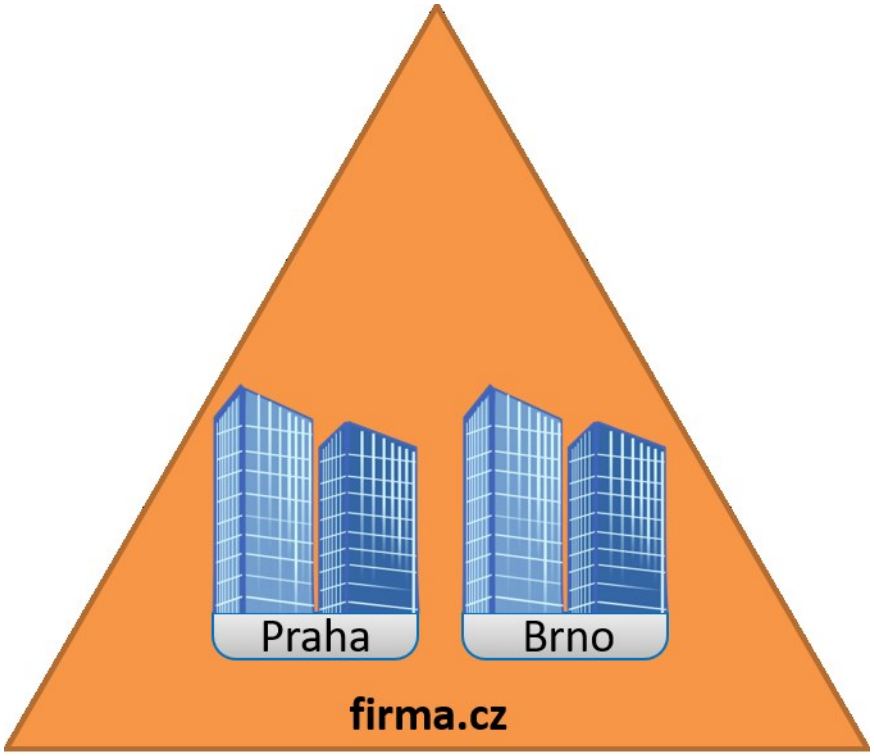


Obr. 4 Stromy domény

Doména

Doména je základní komponentou logické struktury AD. Je považována za administrativní a bezpečnostní hranici. V doméně jsou přímo uloženy objekty (může se jednat o milióny), které do ní patří. Každá doména má svou skupinu správců a ti mají plná práva nad každým jejím objektem. Oprávnění těchto správců se nevztahují na objekty mimo doménu. AD může být tvořena jednou nebo více doménami. V praxi se nejčastěji setkáváme s použitím pouze jedné domény. Doména není omezena na fyzickou lokaci a může tedy být geologicky nezávisle velká. Přístup k doménovým objektům je řízen pomocí ACL (Access Control List), které upravuje oprávnění přístupu k objektům. (3)

Demonstrace na Obr. 5 představuje doménu **firma.cz**, která má pobočky v Praze a v Brně. I přes to, že jsou tyto budovy od sebe velmi vzdálené, je možné, aby takovouto doménu spravovala jedna skupina administrátorů s kanceláří např. v Praze. Podobný příklad platí i pro uživatele z Brna, kteří mohou komunikovat s uživateli v Praze, protože jsou všichni členy jedné domény.



Obr. 5 Doména

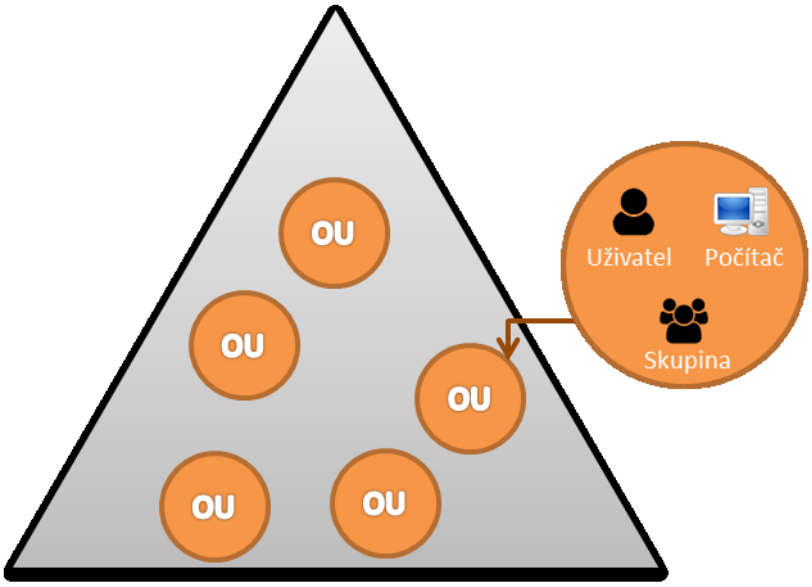
Organizační jednotka (OU)

Organizační jednotka je kontejner, který se uvnitř domény používá k seskupování/organizování objektů do logických administračních skupin. Důvodem k tomuto seskupování může být aplikace rozdílných politik přístupu, jelikož OU je nejmenší jednotka, na kterou můžeme delegovat administrační oprávnění. OU nemusí být vždy jen skupina objektů, ale i pouze jeden objekt (uživatel). (2)

„OU můžeme zanořovat do sebe a vytvářet libovolnou hierarchickou strukturu. Hierarchie OU je lokální uvnitř domény a neovlivňuje jiné domény.“ (3)

V praxi může organizační jednotka představovat jednotlivá oddělení v rámci dané společnosti. Pokud bychom jako příklad uvedli obchodní firmu, tak by sem určitě patřily OU pro vedení společnosti, oddělení financí, oddělení marketingu, nákupu, prodeje apod. Do těchto skupin by byli zahrnuti jednotliví zaměstnanci. V případě, že by některý ze zaměstnanců měl více funkcí, spadal by do více OU.

Příklad: Oblastní vedoucí, který vede skupinu obchodních zástupců, by byl v OU vedení společnosti a v OU svěřené skupiny obchodních zástupců.

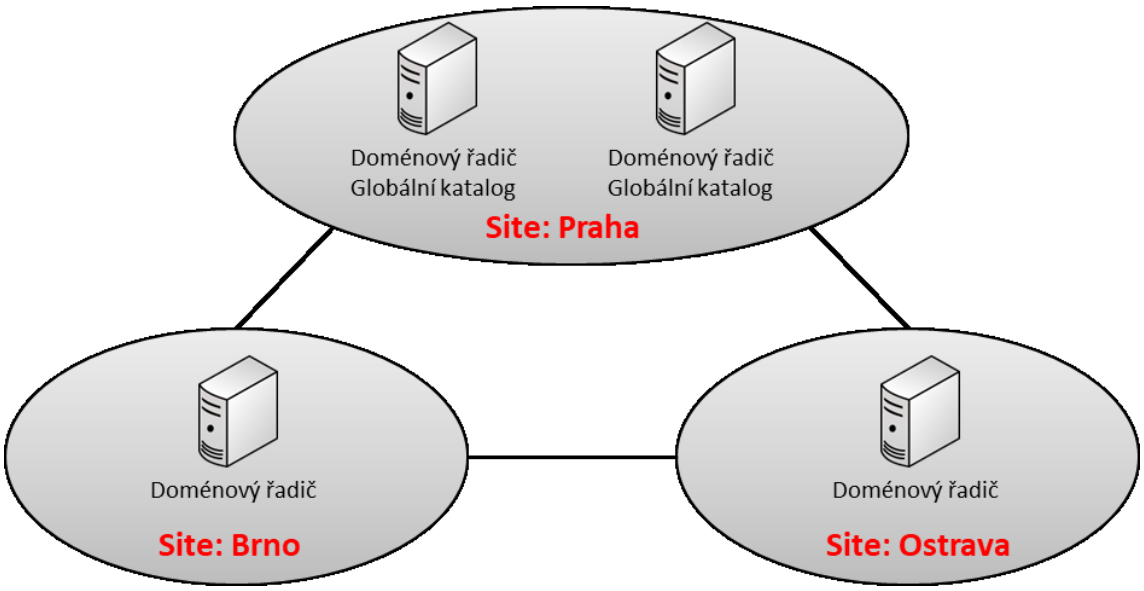


Obr. 6 Organizační jednotka

Site

Site = pobočka/lokalita. Sites představují fyzickou síťovou topologii, do které patří alespoň jedna podsíť (Subnet). Nová site je použita vždy, když zavádíme do domény novou lokalitu. V podstatě je vytvořena nová podsíť. Site zajišťuje replikaci dat mezi jednotlivými doménovými kontroléry/řadiči (Domain Controller). Replikace dat musí probíhat jak v rámci jedné site, tak i mezi ostatními, aby byl zajištěn konzistentní stav doménových řadičů.

„Site je kombinace jednoho nebo více IP subnetů, které jsou spojeny spolehlivými a rychlými linkami. Pokud máme více lokálních sítí (lokalit, poboček) spojených pomocí WAN sítě, tak se většinou vytváří site pro každou LAN.“ (3)



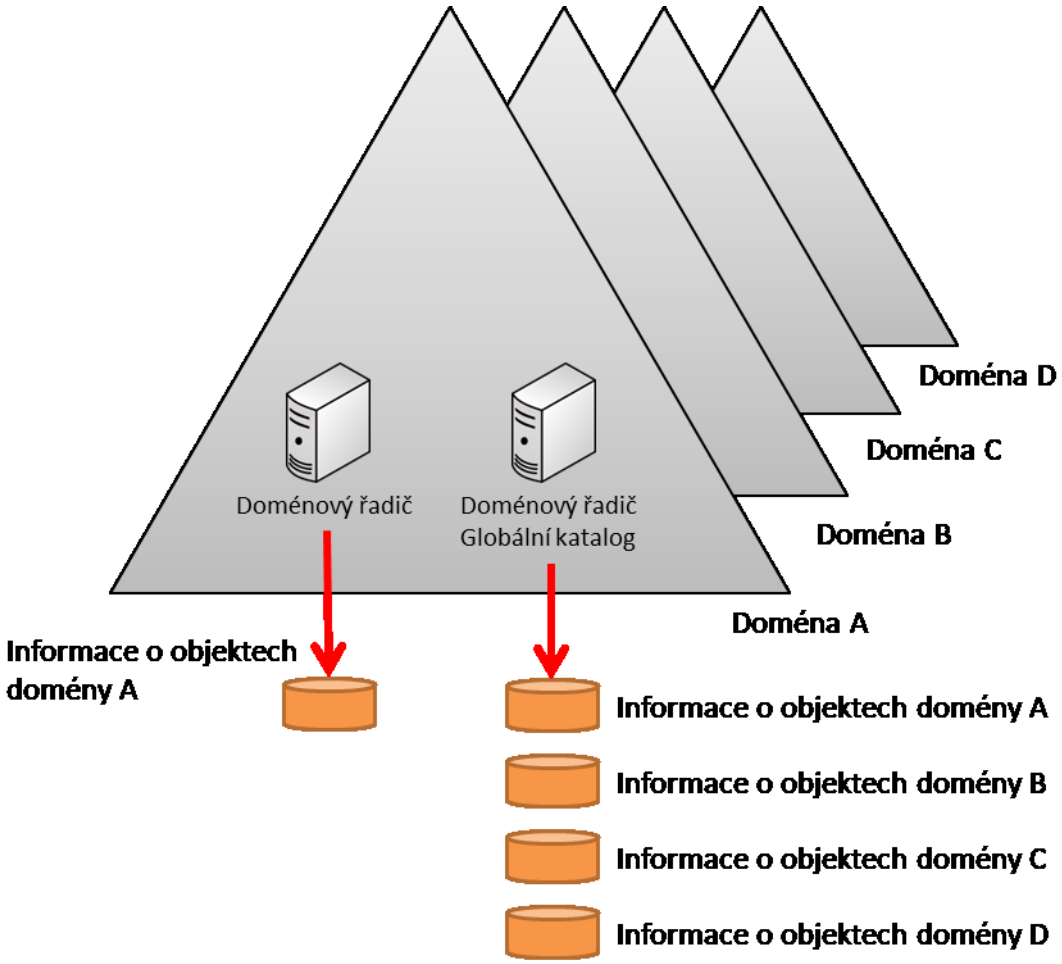
Obr. 7 Site – propojení více site/poboček

Globální katalog (GC)

Globální katalog je komponenta AD, která není součástí fyzické ani logické struktury. Hlavní funkcí GC je vlastnit základní informace o všech objektech v rámci celého lesa. (4)

Základními informacemi je myšleno uživatelské jméno (má tvar e-mailové adresy), lokace, telefon, e-mail, členství v univerzálních skupinách apod. V každé doméně musí být minimální jeden GC server, který je zároveň i doménovým řadičem. Jako GC server je automaticky vybrán prvně instalovaný DC v lese.

Představme si situaci, kdy máme les dvou a více domén, a chceme přistoupit k objektu z jiné domény. Všechny DC v doméně, ze které je přistupováno, mají informace pouze o objektech naší domény, uložené ve svém GC. Aby získaly informace o objektech z jiné domény, dotazují se právě globálního katalogu nadřazené domény nebo přímo lesa, který jim poskytne požadované základní informace.



Obr. 8 Globální katalog – schéma

Group Policy Objects (GPO)

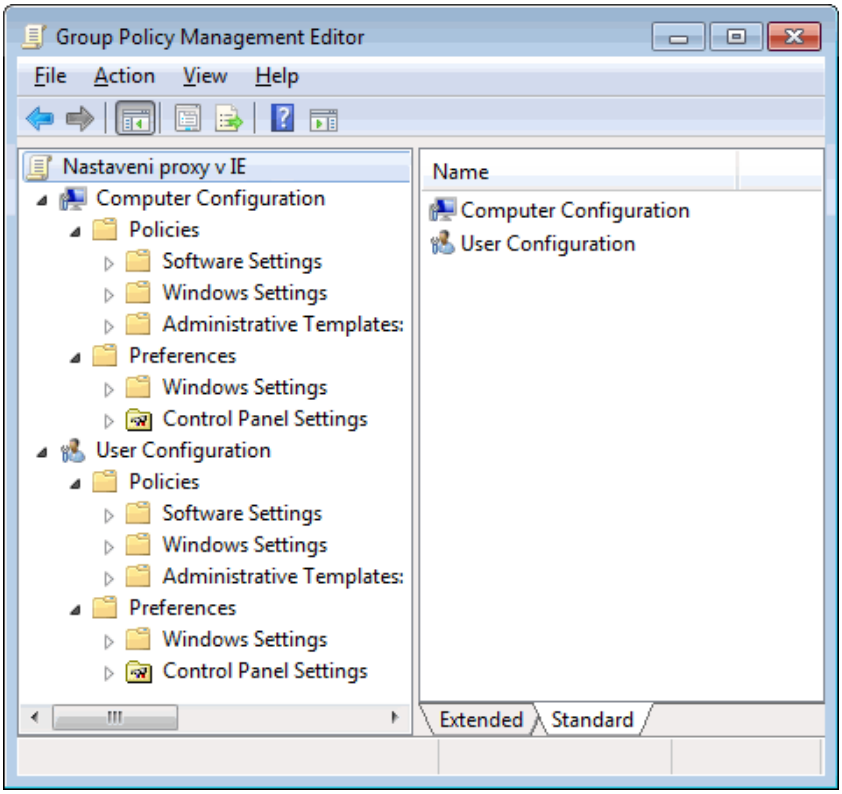
Se službou Active Directory souvisí také Group Policy Object. Jak píše autor webu SAMURAJ-cz.com Petr Bouška, definice GPO je: *„Group Policy (skupinové politiky) slouží k centrální správě počítačů s pomocí Active Directory. Hlavně se tedy využijí pro počítače zařazené do domény.“* (5) Jedná se o nástroj, kterým je řízeno chování objektů v doméně (počítače, skupiny, uživatelé apod.).

Oproti GPO je možné využít i lokální politiky (Local Group Policy), ale od těchto bude tato práce oproštěna.

Za pomoci editoru globálních politik (Group Policy Management Console) je administrátor domény schopen určovat širokou škálu nastavení objektů jako jsou např.:

- Politiky zabezpečení – pravidla hesel, uzamykání účtů apod.
- Politiky chování systémů – úprava plochy, zpřístupnění SW, nastavení zvuku
- Instalace SW
- Mapování síťových disků

GPO mají dvě hlavní části – konfigurace politik uživatelů a konfigurace politik počítače. Obě tyto části zapisují změny do registrů. Rozdíl je pouze ve větvi, kterou používají, a to buď HKEY_LOCAL_MACHINE (HKLM) anebo HKEY_CURRENT_USER (HKCU). Při použití konfigurace pro objekt počítače, jsou politiky aplikovány při jeho startu. Při aplikaci konfigurace pro uživatele jsou až při přihlášení uživatele. (5)



Obr. 9 Editor správy Group Policy

Aplikace GPO je provedena propojením (Link to) na některý z doménových kontejnerů (les, strom, doména…). Při použití politik platí pravidla dědění – podřízený kontejner dědí ze všech nadřazených – aplikována dle hierarchie v AD.

Závěrem

Hlavním cílem AD je autentizace a autorizace objektů v doméně. Tuto činnost zajišťují tzv. doménové kontroléry (DC). Jsou to servery běžící na OS Windows Server. Každý DC může patřit vždy jen do jedné domény.

Doménové kontroléry bývají zpravidla minimálně dva v každé doméně. Důvodem je replikace doménového adresáře. Díky replikaci je zajištěna záloha domény v případě, že by některý ze serverů přestal fungovat.

AD je velmi úzce spjata se službou DNS a GPO. Služba DNS zajišťuje její funkčnost a GPO slouží k řízení přístupů.

„Aby AD správně fungovaly, je nutné mít funkční DNS server, pomocí kterého si pracovní stanice a servery zjišťují umístění nezbytných služeb v síti (řadič domény, LDAP, KERBEROS, …)“ (1)

„K doméně AD se mohou připojit klientské systémy Windows pouze ve vyšších edicích (Enterprise, Professional, …)“ (1)

Seznam použité literatury

1. Miroslav, Pokorný. TNPW1. O Active Directory. [Online] [Citace: 7. 7 2018.] http://lide.uhk.cz/fim/student/pokormi2/tnpw1/.

2. Corporation, Microsoft. What are domains and forests? [Online] 22. 7 2018. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10).

3. Bouška, Petr. SAMURAJ-cz.com. [Online] [Citace: 12. 7 2018.] https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/.

4. Corporation, Microsoft. Active Directory Domain Services. [Online] 21. 7 2018. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services.

5. Bouška, Petr. Group Policy - řízení aplikace a politik. SAMURAJ-cz.com. [Online] 12. 12 2010. [Citace: 25. 7 2018.] https://www.samuraj-cz.com/clanek/group-policy-rizeni-aplikace-politik/.

6. Alena Kabelová, Libor Dostálek. Velký průvodce protokoly TCP/IP a systémem DNS 5. aktualizované vydání. Brno : Computer Press, 2012. ISBN 978-80-251-2236-5.

7. Adaptic, s. r. o. – tvorba webu, webdesign. Co je DNS. adaptic.cz. [Online] [Citace: 19. 7 2018.] http://www.adaptic.cz/znalosti/slovnicek/dns/.

8. CZ.NIC. O doménách a DNS. [Online] [Citace: 19. 7 2018.] https://www.nic.cz/page/312/o-domenach-a-dns/.

9. Corporation, Microsoft. Planning Global Catalog Server Placement. Microsoft Docs. [Online] 31. 5 2017. [Citace: 12. 08 2018.] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/planning-global-catalog-server-placement.

10. Allen, Robert. Group Policy Best Practices. activedirectorypro.com. [Online] 24. 12 2016. [Citace: 22. 8 2018.] https://activedirectorypro.com/group-policy-best-practices/.