Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Nasazení Active Directory v podnikovém prostředí

Michal Plíva

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Plíva Michal

Informatika

Název práce

Nasazení Active Directory v podnikovém prostředí

Anglický název

Deploying Active Directory in an enterprise environment

Cíle práce

Diplomová práce má dva hlavní cíle. Prvním z nich je představení služby Active Directory jakožto nástroje pro správu počítačové sítě a možností, které tato služba poskytuje administrátorům počítačových sítí. Druhým cílem je vlastní návrh a nasazení Active Directory pro konkrétní podnik. Mezi dílčí body diplomové práce patří představit způsob fungování AD a jeho využití v podniku, charakteristika jednotlivých rolí Domain Controllerů a jejich vlastností. Dále v práci bude rozebrána služba Group Policy, která patří mezi nosné pilíře služby Active Directory. Poté budou v práci rozebrány možnosti replikací serverů a obnovy AD po katastrofě. Na závěr teoretické části bude rozebrán Read Only DC a jeho podmínky nasazení. V druhé části bude návrh AD pro konkrétní podnik a jeho nasazení.

Metodika

Diplomová práce bude rozdělena do dvou částí a každá část do několika kapitol. V první části bude detailně probraná jak fyzická, tak logická architektura Active Directory, budou uvedeny její možnosti, požadavky a výhody. Následně budou rozebrány výhody a možnosti Group Policy a pravidla zpracování jednotlivých politik. V další kapitole budou rozebrány procesy, které zajišťují replikaci mezi servery společně s postupy, jak se zachovat v případě katastrof. Na závěr zde bude porovnání klasického DC s RODC a bude probráno, kdy, kde, jak a proč je vhodnější nasazení RODC a naopak. Všechny teoretické poznatky z první části této práce budou využity pro praktickou část, která bude zahrnovat instalaci DC, vytvoření domény, základní nastavení AD a některé zásady GP pro nastavení politik dle požadavků managementu. Dále bude zahrnovat praktické ukázky z disaster recovery a instalaci RODC.

Harmonogram zpracování

Studium odborných informačních zdrojů, stanovení dílčích cílů a postupu řešení: 06/2012
Zpracování přehledu řešené problematiky: 07/2012 – 08/2012
Vypracování vlastního řešení, diskuse, doporučení a závěry: 09/2012 - 02/2013
Tvorba finálního dokumentu práce: 02/2013 – 03/2013
Odevzdání práce a tezí: 03/2013

Rozsah textové části
50 - 60 stran

Klíčová slova
Active Directory, FMSO role, replikace AD, instalace AD, Group Policy

Doporučené zdroje informací

STANEK, William R. Group Policy: zásady skupiny ve Windows : kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2010. 351 s. ISBN 978-80-251-2920-3 (BROž.).

STANEK, William R. Active Directory: kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2009. 352 s. ISBN 978-80-251-2555-7 (BROž.) :.

ALLEN, Robbie a Alistair G LOWE-NORRIS. Active Directory: implementace a správa Microsoft Active Directory. 1. vyd. Překlad Alois Liška. Praha: Grada, 2005. 644 s. ISBN 80-247-0973-2.

MALINA, Patrik. Jak vyzrát na Windows PowerShell 2.0. Vyd. 1. Brno: Computer Press, 2010. 464 s. ISBN 978-80-251-2732-2.

STANEK, William R. Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]. Vyd. 1. Brno: Computer Press, 2009. 1364 s. ISBN 978-80-251-2158-0.

Vedoucí práce
Vaněk Jiří, Ing., Ph.D.

Termín odevzdání
březen 2014

Elektronicky schváleno dne 11.3.2013

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

Elektronicky schváleno dne 4.3.2014

Ing. Martin Pelikán, Ph.D.
Děkan fakulty

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „**Nasazení Active Directory v podnikovém prostředí**" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28. 3. 2014 _____

Poděkovaní

Chtěl poděkovat Ing. Jiřímu Vaňkovi, PhD., za rady a připomínky při vedení této práce. Zároveň bych chtěl poděkovat Výpočetnímu centru Vysoké školy ekonomické v Praze za poskytnutí virtuálního prostředí pro praktickou část. Na závěr bych chtěl poděkovat také svým rodičům za podporu během studia.

Nasazení Active Directory v podnikovém prostředí

Deploying Active Directory in an enterprise environment

Souhrn

Diplomová práce se zabývá návrhem a implementací služby Active Directory ve firemním prostředí. Hlavními cíli této práce je představení služby Active Directory jako nástroje pro správu počítačové sítě v podniku a dále samotný návrh a nasazení Active Directory. V teoretické části je rozebrána architektura Active Directory, jsou probrány jednotlivé součásti Active Directory, FSMO role doménových řadičů, vysvětleny možnosti a typy replikací, způsoby zálohy a obnovy Active Directory a probrány postupy návrhu Active Directory. Praktická část se zabývá vlastním návrhem a implementací Active Directory dle specifických požadavků pro konkrétní podnik, vytvořením zálohy doménového řadiče a provedením obnovy služby Active Directory ze zálohy pro případ katastrofy.

Summary

This diploma thesis deals with design and implementation of Active Directory service in corporate environment. Main goals of this thesis are to introduce the Active Directory service as a tool for corporate computer network administration together with design and implementation of Active Directory. Theoretical part includes description of Active Directory architecture, its individual components, FSMO roles of Domain Controllers, explanation of options and types of replications, methods of backing up and restoring of Active Directory and methods of design of Active Directory. Practical part deals with the actual design and implementation of Active Directory according to specifics requirements for a particular company, creating backup of Domain Controller and testing restoration of Active Directory from backup in case of disaster.

Klíčová slova: Active Directory, FSMO role, replikace AD, instalace AD, skupinové politiky, návrh AD, záloha AD, obnova AD

Keywords: Active Directory, FSMO roles, AD replication, AD installation, Group Policy, design AD, backup AD, recovery AD

Obsah

1 Úvod

V současné době je práce s počítačem předpoklad pro většinu činností ve firmách. Ať už se jedná o zpracování účetnictví, emailovou komunikace se zákazníky nebo dodavateli, tvorbu marketingové kampaně, zpracování výkazů nebo třeba návrh nového loga. Téměř každá činnost je vykonávána prostřednictvím počítačů. Každý větší podnik má tedy IT oddělení, které se zabývá správou počítačové sítě. Pokud se jedná o malé podniky, je možné spravovat každý počítač individuálně. Ovšem je už těžko představitelné, že například ve společnosti o několika desítkách či stovkách zaměstnanců bude IT oddělení obcházet každý počítač a instalovat na něj novou verzi internetového prohlížeče, důležitou aktualizaci, popřípadě novou síťovou tiskárnu. Další oblastí, kterou je nutnou v podniku řešit centrálně je bezpečnost. Je nutné zabezpečit nejen přístup k počítačové síti a data, ale i síťové zdroje tak, aby k nim měli přístup jen oprávnění zaměstnanci. V tomto případě je vhodné přejít na řešení, které umožní centralizovanou správu podnikových počítačů, uživatelských účtů, síťových zdrojů a bezpečnosti a které umožní správcům efektivně spravovat celé IT prostředí. Jedním z těchto nástrojů může být služba Active Directory od společnosti Microsoft.

2 Cíl práce a metodika

Diplomová práce má dva hlavní cíle. Prvním z nich je představení služby Active Directory jako nástroje pro správu počítačové sítě a možností, které tato služba poskytuje administrátorům počítačových sítí. Druhým cílem je vlastní návrh a nasazení Active Directory pro konkrétní podnik.

Mezi dílčí body diplomové práce patří:

- představení logické a fyzické architektury Active Directory
- charakteristika jednotlivých FSMO rolí doménových řadičů
- možnosti a využití RODC (Doménového řadiče jen pro čtení)
- služba Group Policy (Skupinové politiky)
- typy replikací doménových řadičů
- záloha a obnova Active Directory
- obecný návrh Active Directory
- instalace a konfigurace Active Directory
- instalace RODC

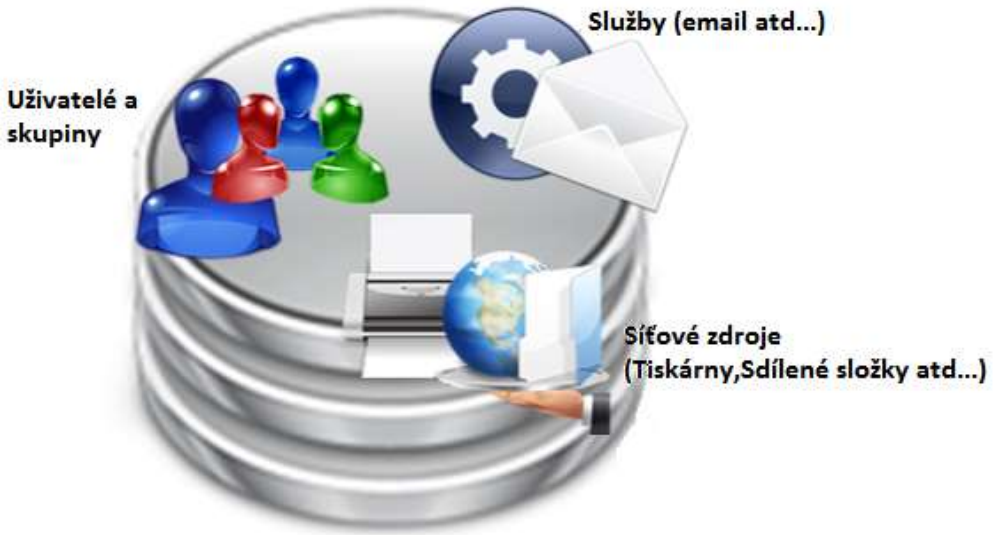
V první části bude detailně probrána jak fyzická, tak logická architektura Active Directory, budou uvedeny její možnosti, požadavky a výhody. Dále bude probrán doménový řadič a FSMO role, které zajišťují správnou funkčnost doménového prostředí. Následně budou rozebrány výhody a podmínky pro nasazení RODC. Poté bude následovat kapitola, kde budou rozebrány výhody a možnosti Group Policy a možnosti jednotlivých politik. V další kapitole budou rozebrány procesy, které zajišťují replikace mezi doménovými řadiči. Na závěr zde bude uveden způsob zálohy a obnovy Active Directory a způsoby návrhu struktury Active Directory. Všechny teoretické poznatky z první části této práce budou využity pro praktickou část, která bude zahrnovat instalaci doménového řadiče, vytvoření domény, základní nastavení Active Directory a vytvoření skupinových politik pro nastavení uživatelských oprávnění dle požadavků managementu. Dále bude práce zahrnovat instalaci doménového řadiče jen pro čtení, praktickou ukázku zálohy doménového řadiče a autoritativní obnovu objektů v Active Directory ze zálohy.

3 Teoretická východiska

3.1 Představení Active Directory

Active Directory je adresářová služba od společnosti Microsoft a poprvé byla představena ve verzi Microsoft Server 2000. Umožňuje centrální správu počítačové sítě v podniku. Samotná služba je zodpovědná za autorizaci a autentifikaci uživatelů, jejich přístup ke sdíleným adresářům, oprávněním, síťovým tiskárnám, dalším multifunkčním zařízením a jejich centrální správu.

Samotné Active Directory si lze představit jako velkou databázi, která uchovává informace o uživatelích a skupinách, o službách (email atd.) a o síťových zdrojích (tiskárny, sdílené složky atd), které jsou v Active Directory k dispozici. Všechny tyto záznamy představují v Active Directory objekty. Každý objekt má své atributy, které určují informace, jež je možné o objektu uchovávat, vyhledat a používat. Například objekt uživatel má, kromě jiného, atributy typu jméno, příjmení a login. Podle všech atributů je možné uživatele vyhledat, roztřídit, zpracovat pro další účely správy. Na obrázku Obrázek 1 je graficky znázorněna databáze Active Directory a 3 primární objekty, o kterých uchovává informace.



Obrázek 1 Active Directory [zdroj: http://www.trainsignal.com/]

Kromě těchto tří primárních objektů, obsahuje AD plno dalších objektů, jako například certifikáty, počítače, skupinové politiky, které mohou být spravovány.

3.1.1 Co vše lze spravovat pomocí AD

Pomocí Active Directory je tedy možné vytvářet, mazat upravovat uživatele, počítače, síťové zdroje a zpracovávat další objekty v Active Directory.

Dále existuje plno dalších oblastí, které je možno řídit pomocí Active Directory a skupinových politik[1]:

- Aplikace - zde je možno instalovat na PC automaticky software, povolit instalaci uživatelům a nastavení předvoleb pro instalaci různých programů
- USB zařízení – možnost ovládat chování systému po připojení různých USB zařízení. Opět je možnost zakázat určitá zařízení a tím znemožnit například uživateli vynesení důležitých dat z firmy na flash disku
- Mapování jednotek – automatické mapování jednotek pro různé skupiny uživatelů
- Prostředí - Nastavení různého systémového prostředí – změna ikon, plochy, skrytí voleb atd.
- Registry – úprava klíčů, podklíčů a hodnot dat v registrech
- Naplánované úlohy – možnost nastavit/spouštět určité úlohy na PC
- Služby – ovládat služby
- Soubory a složky – kopírovat, vytvářet různé sobory a složky na počítačích
- Zástupci – vytvářet zástupce pro programy, aplikace, skripty atd.

Jak je vidět, tak možnosti ovládáni počítačů a uživatelů jsou opravdu obrovské a záleží jen na správcích, jak jich využijí. Rozhodně se jedná o komplexní nástroj pro správu počítačových sítí.

3.2 Architektura Active Directory

Architekturu Active Directory je možné vnímat z dvou pohledů

- Logická architektura – jak vnímáme objekty v Active Directory, jak k ním můžeme přistupovat a využívat je.
- Fyzická architektura - způsob ukládání dat na pevném disku

Znalost logické architektury nám pomůže při její implementaci v podnikovém prostředí a při správě počítačové sítě jako celku v jakémkoliv podniku. Znalost fyzické struktury nám naopak umožní lépe chápat vnitřní fungování Active Directory a jejich procesů.

[1] PLÍVA, M., *Semestrální projekt na předmět Počítačové sítě, s. 12*

3.2.1 Logická struktura Active Directory

Logická struktura Active Directory je nezávislá na fyzické struktuře. Jedná se o zobrazení sítě v objektech a dle určité hierarchie, které nám umožňují její snadné řízení. Mezi základní objekty patří[2]:

- Domain(Doména)
- Forest (Les)
- Tree (Strom)
- Organizational Unit (Organizační jednotka)

S těmito objekty pracujeme při řízení počítačové sítě a snažíme se fyzickou strukturu počítačové sítě převést tak, aby co nejvhodněji odpovídala logické struktuře Active Directory.

3.2.1.1 Doména (Domain)

Doména je základní prvek Active Directory. Při vytváření Active Directory na prvním Windows Serveru se vytváří doména. Doménu si lze představit jako logickou skupinu počítačů, na kterých běží operační systém Windows a které sdílejí centrální databázi Active Directory. Doména slouží jako "virtuální" hranice, která umožnuje řídit a nastavovat jednotlivé objekty, které se nacházejí v doméně.

Doménu si lze představit jako jedinečný „jmenný prostor" a graficky je v odborných publikacích značena jako trojúhelník.

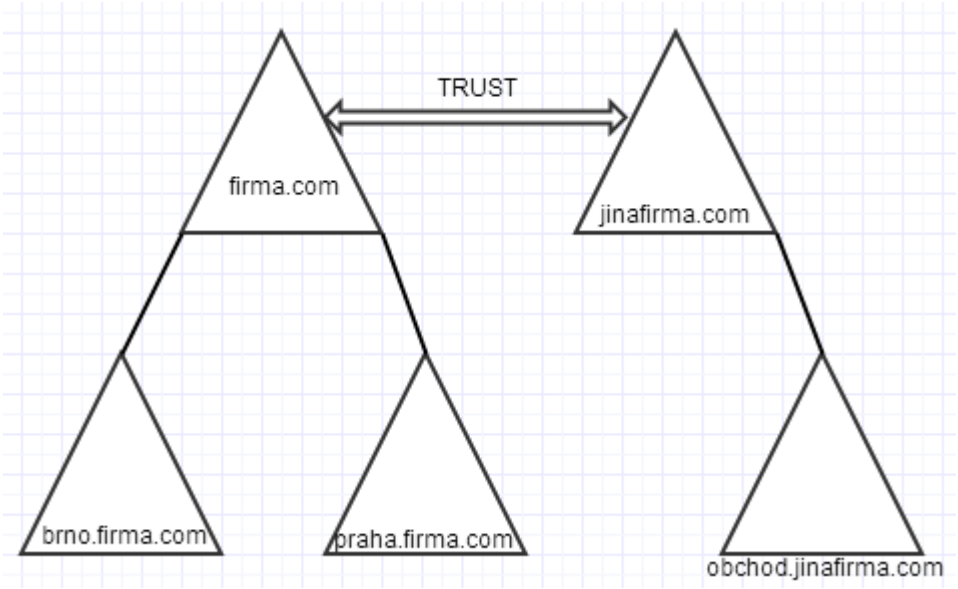
[2] STANEK,WILLIAM R., Mistrovství v Microsoft Windows Server 2008, s. 945

Obrázek 2 Grafické znázornění domény Active Directory [zdroj: autor]

Počítače v doméně jsou pojmenovány částí doménového jména (SUFFIX) a registrovány v databázi Active Directory. Díky tomu mohou být ovládány. Příklad může být jméno doménového řadiče. Představme si, že se v doméně podíváme na název doménového řadiče. Zjistíme, že je ve tvaru „DC1.firma.local“. Z toho je patrné, že název řadiče v sobě obsahuje i název domény (firma.local).

3.2.1.2 Les (Forest)

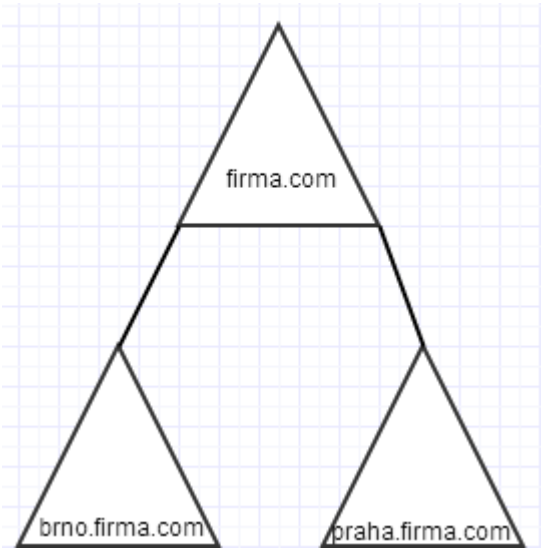
Les je nejvyšší úroveň v logické struktuře Active Directory. Les se skládá ze všech domén, které jsou v rámci jednoho podniku. Samozřejmě může existovat les, který obsahuje pouze jednu doménu. U velké organizace se les skládá z několika stromů, které jsou vzájemně spojeny vztahem důvěry (trust). Díky vztahu důvěry mezi oběma doménami mohou uživatelé z jedné domény využívat síťové zdroje z druhé domény a naopak. Následující obrázek znázorňuje příklad lesa v Active Drectory:



Obrázek 3 Les v Active Directory[zdroj: autor]

3.2.1.3 Strom (Tree)

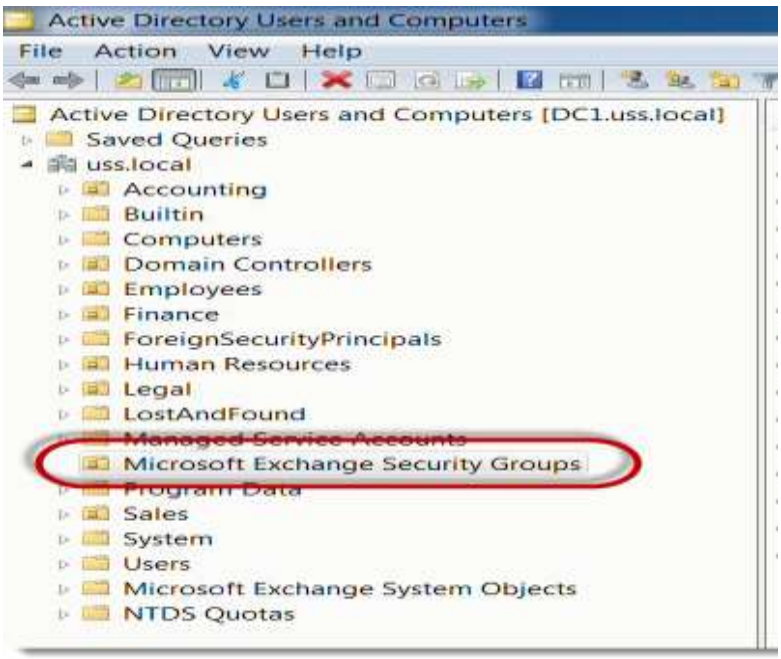
Strom se skládá z několika domén, mezi nimiž je vzájemný vztah rodič-dítě (parent-child). První doména ve stromu je tzv. kořenová doména (root domain, parent) a ostatní domény jsou její pod domény (child). Každá pod doména přebírá zároveň do svého jména také název rodičovské domény. Grafické znázornění stromu zobrazuje následující obrázek:



Obrázek 4 Grafická podoba stromu v Active Directory [zdroj:autor]

3.2.1.4 Organizační jednotka (Organizational Unit)

Jedná se o kontejner, na který je možno aplikovat skupinové politiky. Vnořováním organizačních jednotek můžeme vytvořit logickou strukturu v podniku podle odděleních nebo dle polohy (pokud máme více poboček) a různým organizačním jednotkám tak můžeme nastavovat jiné politiky a snáze tak vše řídit. Do organizačních jednotek se nejčastěji umisťují objekty typu uživatel, počítač, síťové zdroje a tiskárny. Příklad struktury organizačních jednotek v podniku je možné vyčíst z následujícího obrázku:

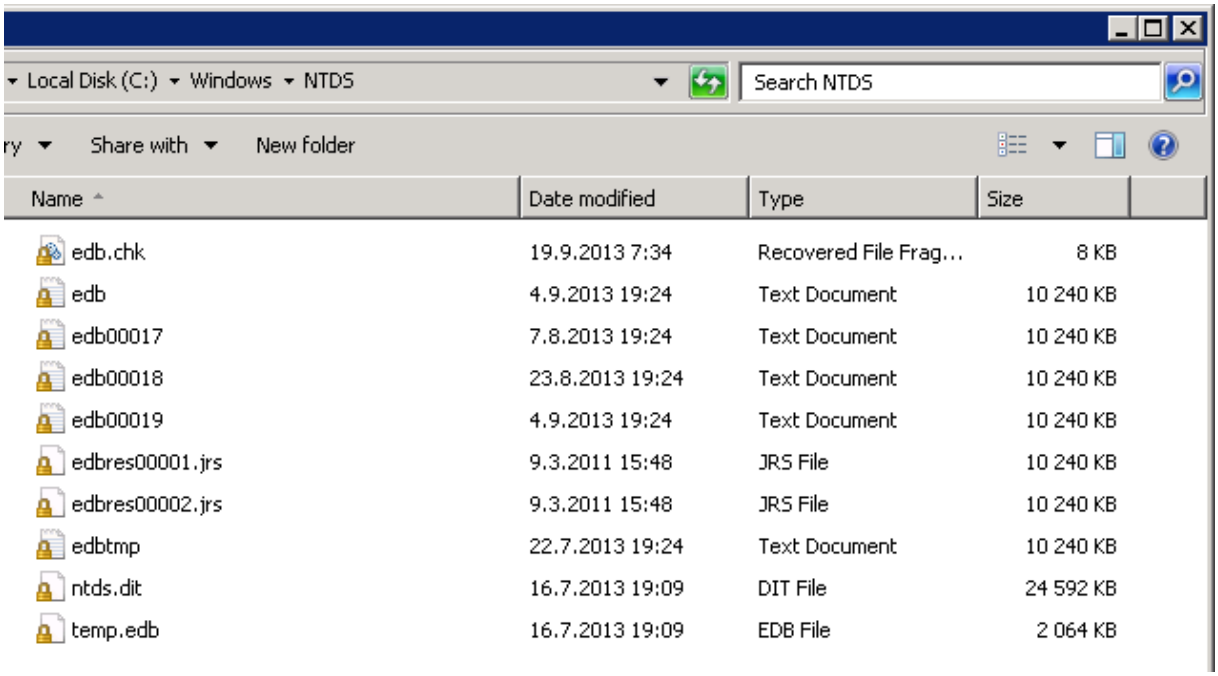


Obrázek 5 Organizační jednotky v AD [zdroj: http://blogs.interfacett.com/]

3.2.2 Fyzická struktura Active Directory – NTDS.DIT

Databáze Active Directory je uložena v souboru NTDS.DIT, který se standardně nachází v %systemroot%\NTDS. Kromě tohoto souboru se v této složce ještě nachází několik následujících souborů[3], jak ukazuje následující obrázek:

[3] **STANEK, William R, Joe RICBARDS a kolektiv,** *Windows® Server 2008 inside out, s.995*



Obrázek 6 Fyzická struktura Active Directory [zdroj: autor]

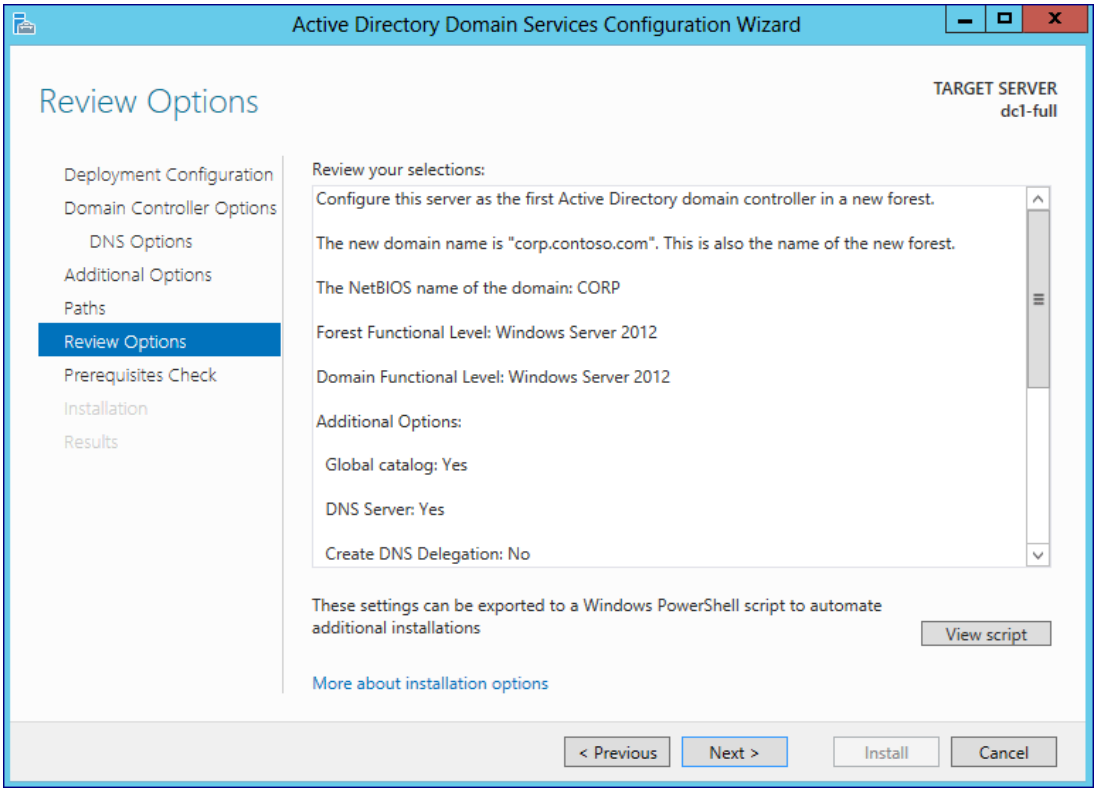
- Temp.edb – soubor je využíván k uchování informací o transakcích, které právě probíhají
- Edbres0001.jrs a edbres0002.jrs – jedná se o soubory s logy, které jsou využity jen tehdy, kdy harddisku, kde jsou umístěny normální logy, dochází volné místo. Velikost každého souboru je 10 MB.
- Edbtmp.log – jedná se o dočasný soubor pro logy
- Edbxxxxx.log – starší logy, které se uchovávají. Xxxxx v názvu je nahrazeno hexadecimálním číslem, které inkrementálně narůstá.
- Edb.log - soubor s transakčními logy. Soubor má fixní velikost 10MB. V případě, že log obsahuje záznamy delší než 10MB, dojde k vytvoření soboru Edbtmp.log, kam se dočasně začnou ukládat všechny další transakce. Soubor Edb.log se přejmenuje na Edbxxxxx.log a ze souboru Edbtmp.log se stane nový Edb.log.
- Edb.chk – tento soubor obsahuje kontrolní body, které značí, jaké transakce byly již zapsány do databáze Active Directory.

3.3 Novinky ve Windows Server 2012

Nové vydání operačního systému Windows Server 2012 sebou přineslo kromě ostatních novinek také zajímavé změny a vylepšení v oblasti Active Directory[4]. Nyní lze například rychleji a jednoduše vytvořit nebo přidat doménový řadič do Active Directory, zvýšit flexibilitu při auditování, autorizovat přístup k souboru a jednodušeji provádět administrativní úlohy ať už lokálně nebo vzdáleně.

- Vytvoření nového doménového řadiče „klonováním" jiného doménového řadiče ve virtuálním prostředí Windows Server 2012 umožňuje vytvoření nového řadiče pouhým „zkopírováním" již funkčního řadiče ve virtuálním prostředí. K tomu, aby bylo možné vytvářet klony doménových řadičů tímto způsobem, je nutné dodržet 2 základní podmínky:
    1. Hypervisor musí podporovat VM-Generation ID (například Windows Server 2012 Hyper-V)
    2. V jedné z těchto umístění (%windir%\NTDS, kořenový adresář vyměnitelného média, adresář, kde je umístěn NTDS.DIT soubor) musí být soubor DCCloneConfig.xml,[5] který obsahuje všechny nezbytné informace pro klonované doménové řadiče
- Windows Server 2012 integruje všechny nutné kroky a kontrolu prerekvizit nutných k nasazení nového doménového řadiče do jednotného grafického prostředí. Nový instalační proces je postaven na Powershellu, integrován do Server Manageru a díky tomu je nové nasazení jednodušší, přehlednější a rychlejší.

[4] http://technet.microsoft.com/en-us/library/hh831477.aspx
[5] Více info zde http://blogs.technet.com/b/askpfeplat/archive/2012/10/01/virtual-domain-controller-cloning-in-windows-server-2012.aspx



Obrázek 7 Konfigurační průvodce AD DS ve Windows Server 2012 [zdroj: http://technet.microsoft.com/]

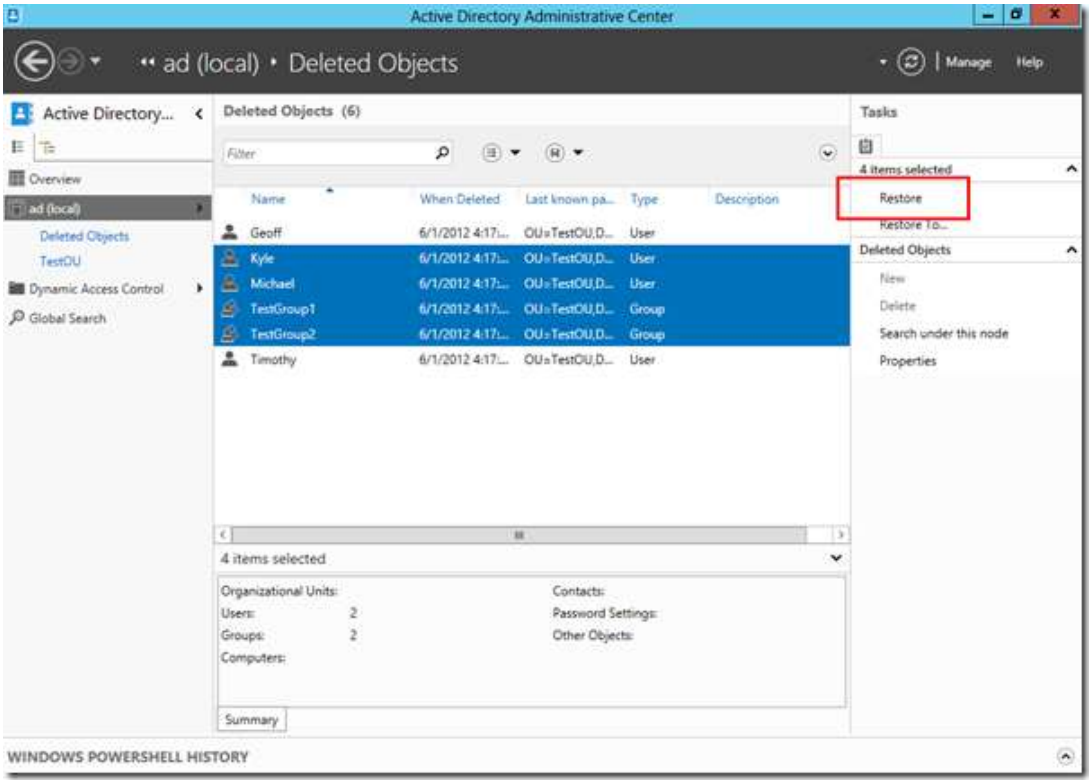
- DirectAccess Offline Domain Join

  Možnost připojení počítače offline do domény již byla v Active Directory od verze Windows Server 2008 R2. Toto připojení však neumožnovalo předkonfigurovat DirectAccess[6] pro využívání sítových zdrojů (servery, aplikace, sdílené složky). K tomu, aby byl počítač takto off-line připojen k doméně a ihned mohl využívat veškeré síťové zdroje, jsou nutné tyto předpoklady: doménové řadiče na kterých běží Windows server 2012 a klientský počítač s operačním systémem Windows 8.[7]

- Grafické rozhraní pro koš v Active Directory

  Koš pro objekty v Active Directory je součástí již od předchozí verze. Nyní však dostal také grafické rozhraní, které urychluje obnovu náhodně smazaných objektů z Active Directory a snižuje čas potřebný pro jejich obnovu.

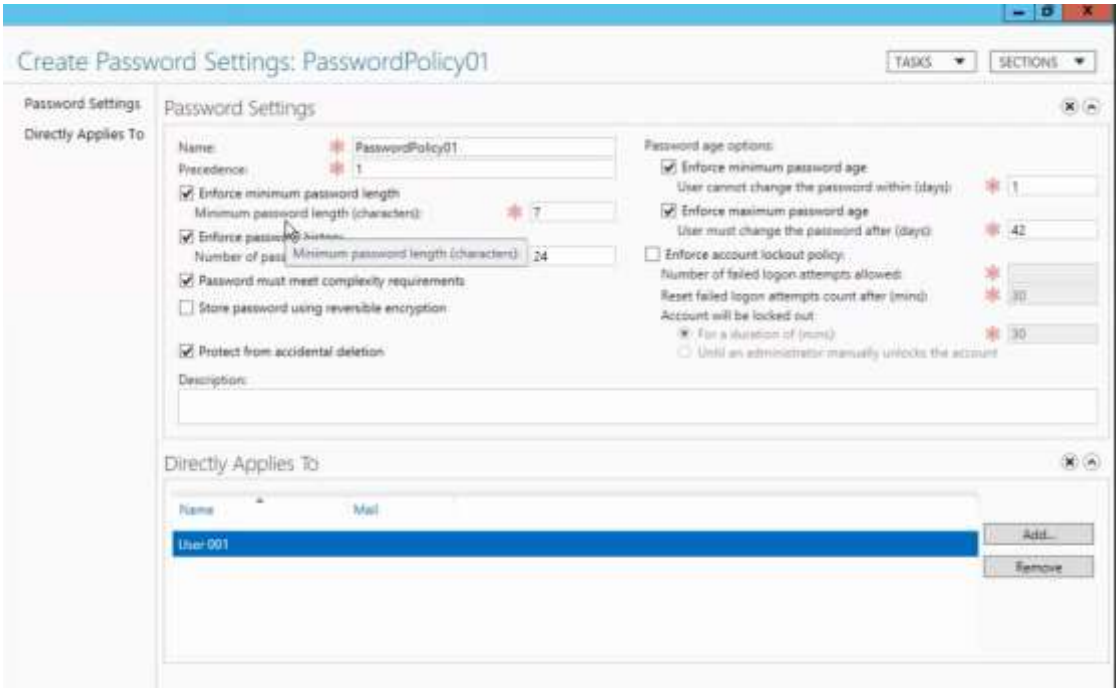
[6] http://cs.wikipedia.org/wiki/Directaccess
[7] http://windowsitpro.com/windows-server-2012/directaccess-windows-server-2012



Obrázek 8 - Koš v AD AC Windows Server 2012 [zdroj: http://4sysops.com]

- Grafické rozhraní pro nastavení politik hesel

  Politiku rozdílných hesel pro různé skupiny uživatelů bylo možné použít již ve verzi Windows Server 2008. Zde dochází opět k vytvoření přehledného grafického rozhraní, které je součástí administračního centra Active Directory. Pokud chceme využívat k nastavení hesel grafické rozhraní, je potřeba mít funkční úroveň domény Windows Server 2008 a mít administrativní centrum Windows Server 2012.



Obrázek 9 GUI pro nastavení politik hesel ve Windows Server 2012 [zdroj: http://www.mstv.cz/it]

- Powershell cmdlet pro replikace a správu topologie

  Pokud jste dříve chtěli spravovat síťovou topologii v Active Directory, bylo nutné používat nejméně 3 rozdílné nástroje: repadmin, ntdsutil a Active Directory sítě a služby (AD Sites and Services). Nyní je možné využít powershell k vytváření a spravování lokací (sites), síťových linků, mostů, subnetů a připojení, replikovat objekty mezi doménovými řadiči a další činnosti spojené se správou topologie. Vše je tak možné řídit z jednoho místa a v jednotném prostředí.

3.3.1 Novinky ve verzi Windows Server 2012 R2

Windows Server 2012 R2 sebou přinesl opět další novinky. Celý seznam novinek a vylepšení je k dispozici na internetu[8]. Nás však zajímají především novinky, které se týkají oblasti Active Directory. Jedná se o pár nových vylepšení, které umožní uživatelům v práci pracovat na svých zařízeních (BYOD - Bring Your Own Device) a zároveň mít přístup k síťovým zdrojům a službám ve firmě:

[8] Viz http://www.daquas.cz/articles/621-windows-server-2012-r2-co-je-noveho

- **Workplace Join**

Uživatelé si mohou přinést své zařízení a na něm přistupovat k podnikové síti a využívat ji. Dříve jsme měli jen zařízení, které buď bylo, nebo nebylo v doméně. Workplace join nabízí mezistupeň mezi těmito možnostmi. Zařízení má přístup k síťovým zdrojům, avšak vlastníkem je stále uživatel a zařízení tak nepodléhá skupinovým politikám ve firmě. Pokud připojíme zařízení pomocí Workplace Join, tak se vytvoří záznam o tomto zařízení v Active Directory a stane se tak pro Active Directory důvěryhodné. Poté již je možné na tomto zařízení přistupovat a využívat síťové zdroje a služby v podnikové síti. V současné době s Windows Server 2012 R2 mohou využívat Workplace join pouze zařízení, na kterých je instalován operační systém Windows 8.1 nebo iOS[9].

- **WorkFolders**

WorkFolders se stejně jako Workplace Join zaměřují na uživatele, kteří chtějí pracovat na svých zařízeních. Tato funkce jim umožní přistupovat k firemním dokumentům a pracovat s nimi i offline. Workfolders jsou spojeny s Active Directory Right Management System a umožňují tak organizaci mít stále kontrolu nad svými daty.

- **Web Application Proxy**

„Web Application Proxy umožňuje přímo ve Windows Serveru velmi jednoduše a bezpečně publikovat aplikace ven do internetu, takže je firemní uživatel může stáhnout a spustit v podstatě odkudkoliv. Scénář BYOD je tak opět o kousek blíž.“[10]

- **Active Directory Federation Services (ADFS)**

Rozšiřuje možnosti Active Directory o ověření uživatelů, kteří přistupují k aplikacím v cloudu (Office 365, Windows Intune, vlastní aplikace vytvořené nad Windows Azure) pomocí jednotného přihlášení (Single Sign-on)

[9] Viz http://technet.microsoft.com/en-US/library/dn280945
[10] tamtéž

3.4 Doménový řadič

Doménový řadič je server, na kterém je nainstalován operační systém Windows Server, naistalována role Doménové Služby Active Directory (Active Directory Domain Services). Na tomto serveru se také nachází replikace databáze Active Directory (soubor NTDS.DIT) a složka SYSVOL.

Doménové řadiče provádějí autentizaci a následně také autorizaci uživatelů. Autentizace uživatelů je důležitou součástí v podnikové prostředí, proto se doporučuje instalovat minimálně 2 doménové řadiče, aby v případě výpadku jednoho, mohl druhý převzít jeho činnost a uživatelé se tak mohli přihlašovat do sítě a využívat síťové zdroje dle svých oprávnění i v případě, že se jeden z doménových řadičů stane nedostupný.

3.4.1 Úrovně funkčnosti domény a doménové struktury

Úrovně funkčnosti byly do Active Directory zavedeny s vydáním Windows Server 2003. Existují dva typy funkčních úrovní[11]:

- Úroveň funkčnosti doménové struktury
- Úroveň funkčnosti domény

Úroveň funkčnosti domény se vztahuje na doménu, zatímco úroveň funkčnosti doménové struktury se vztahuje na všechny domény a stromy v celém lese Active Directory. Každá verze Active Directory vydaná s novou verzí Windows Server zahrnuje novinky a nové vlastnosti, které mohou být plně využity pouze tehdy, když je celá doména nebo celý les na stejné úrovni funkčnosti.

Windows 2008 R2 přišly s možností odpadkového koše. Jedná se o vlastnost, která umožňovala administrátorům obnovit smazané objekty z Active Directory. Dřívější verze Active Directory tuto možnost neměly, a proto pokud jsme měly doménu, nebo les, který obsahoval doménové řadiče nižší verzí operačního systému než Windows Server 2008 R2 a tudíž s nižší úrovní funkčnosti domény nebo doménové struktury, tak jsme nemohli tuto

[11] **STANEK, William R, Joe RICBARDS a kolektiv,** *Windows® Server 2008 inside out, s.* 1017

novinku v Active Directory využívat. Bylo nutné upgradovat všechny doménové řadiče na novější a poté zvýšit úrovně funkčnosti.

Funkční úrovně nám říkají, jakou nejnižší verzi systému Windows Server můžeme tedy použít jako doménový řadič a zároveň jaké funkce budeme v Active Directory moci využívat. Zvýšení funkční úrovně je nevratný krok. Jakmile je jednou zvýšena funkční úroveň, není možné se vrátit na nižší. Jedinou výjimkou[12] je možnost se za určitých podmínek vrátit ve funkční úrovni z úrovně Windows Server 2008 R2 na Windows Server 2008.

Následující tabulky obsahují základní přehled funkčních úrovní, dostupných funkcí a podporovaných doménových řadičů.

Úroveň funkčnosti domény	Dostupné funkce	Podporované doménové řadiče
Windows 2000 native	• Rozšířená práce se skupinami • Využití historie SID	Windows Server 2000, 2003, 2008, 2008 R2
Windows Server 2003	• Možnost přejmenovat doménový řadič • Vylepšení atributu lastLogonTimestamp • Možnost přesměrovat kontejner Uživatele a Počítače • Selektivní autentizace	Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2
Windows Server 2008	• Podpora souborového systému DFS pro SYSVOL • Zlepšení šifrovacího standardu (AES 128 a AES 256) • Možnost specifikovat rozdílná hesla pro uživatele a skupiny	Windows Server 2008, 2008 R2, 2012, 2012 R2
Windows Server 2008 R2	• Zlepšení autentizačního mechanizmu přihlašování uživatelů	Windows Server 2008 R2, 2012, 2012 R2
Windows Server 2012	• Zlepšení Kerberos autentizace. Detailnější informace zde: http://technet.microsoft.com/en-us/library/hh831747.aspx	Windows Server 2012, 2012 R2
Windows Server 2012 R2	• Zákaz používat starší způsoby šifrování při ověřování uživatelů	Windows Server 2012 R2

[12] http://technet.microsoft.com/en-us/library/cc787290(v=ws.10).aspx

	• Nové skupinové politiky pro přihlašování uživatelů	

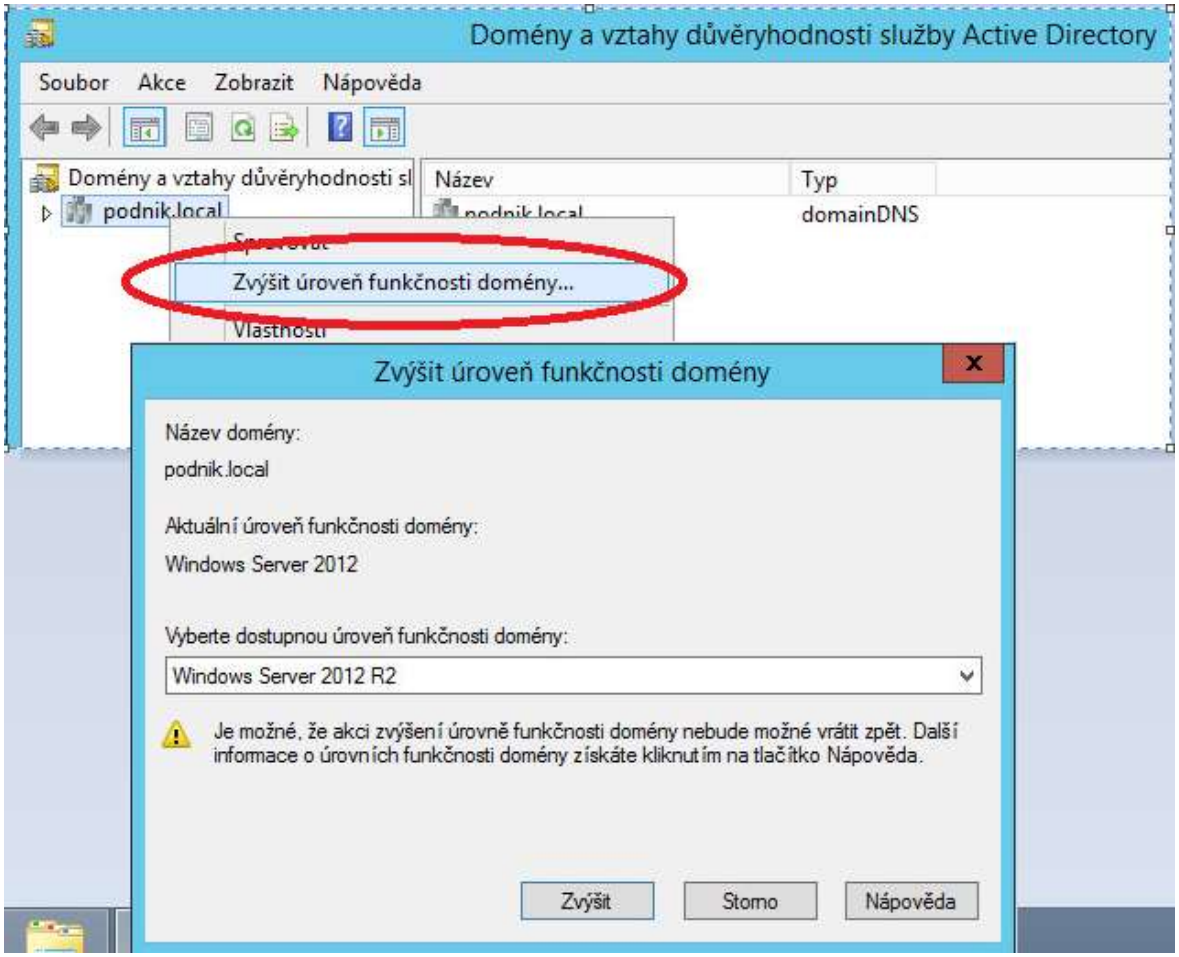
Tabulka 1 Dostupné funkce AD pro různé úrovně funkčnosti domény [zdroj: http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(WS.10).aspx, úprava: autor]

Úroveň funkčnosti doménové struktury	Dostupné funkce	Podporované doménové řadiče
Windows 2000	• Základní funkce AD	Windows Server 2000, 2003, Windows Server 2008, Windows 2008 R2
Windows Server 2003	• Vztahy důvěryhodnosti mezi lesy • Možnost přejmenování domén • Možnost nasadit doménová řadič pouze ke čtení • Zlepšení algoritmu KCC	Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2
Windows Server 2008	• Žádné nové funkce • Všechny nově přidané domény mají standardně nastavenou úroveň funkčnosti domény Windows Server 2008	Windows Server 2008, 2008 R2, 2012, 2012 R2
Windows Server 2008 R2	• Funkce Odpadkový koš v AD • Všechny nově přidané domény mají standardně nastavenou úroveň funkčnosti domény Windows Server 2008 R2	Windows Server 2008 R2, 2012, 2012 R2
Windows Server 2012	• Všechny nově přidané domény mají standardně nastavenou úroveň funkčnosti domény Windows Server 2012	Windows Server 2012, 2012 R2
Windows Server 2012 R2	• Všechny nově přidané domény mají standardně nastavenou úroveň funkčnosti domény Windows Server 2012R2	Windows Server 2012 R2

Tabulka 2 Dostupné funkce AD pro různé úroveň funkčnosti doménové struktury [zdroj: http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(WS.10).aspx, úprava: autor]

Aktuální verzi úrovně funkčnosti domény a úrovně funkčnosti doménové struktury zjistíme, pokud v na doménovém řadiči s operačním systémem Windows Server 2012 ve Správci serveru klikneme na tlačítko **Nástoje** a vybereme položku **Domény a vztahy**

důvěryhodnosti služby Active Directory. V této aplikaci můžeme zjistit aktuální úrovně funkčnosti domény i doménové struktury a zároveň je zde můžeme měnit. Pokud chceme změnit úroveň funkčnosti domény, klikneme pravým tlačítkem na odpovídající doménu a vybereme z nabídky volbu **Zvýšit úroveň funkčnosti domény**. Viz následující obrázek:



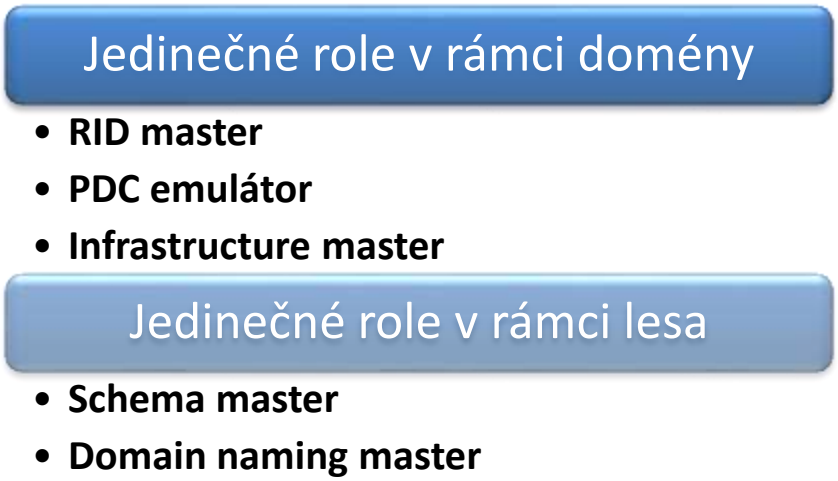
Obrázek 10 Zvýšení úrovně funkčnosti domény [zdroj: autor]

Pokud chceme zjistit nebo zvýšit úroveň funkčnosti doménové struktury, tak ve stejné aplikaci klikneme na položku **Domény a vztahy důvěryhodnosti služby Active Directory** a vybereme možnost **zvýšit úroveň funkčnosti doménové struktury.**

3.4.2 FSMO role doménových řadičů

Všechny řadiče domény používají tzv. multimaster replikace. To znamená, že změna nebo vytvoření objektu v doméně je replikováno na ostatní řadiče domény v dané doméně. Z toho vyplývá, že je jedno, na kterém řadiči se změna provede, protože se zreplikuje na všechny doménové řadiče v doméně. Existuje zde však několik rolí, které jsou replikovány pouze jednosměrně. Tyto role používají tzv. singelmaster replikaci.

Seznam rolí[13], které používají jednosměrné replikace, které zobrazuje následující obrázek:



Obrázek 11 - Přehled FSMO rolí v AD [zdroj: autor]

Schema master a Domain naming master jsou role, které jsou vždy pouze na jednom doménovém řadiči v celém lese (forestu). Všechny ostatní role jsou vždy pro celou doménu. Pokud instalujeme první doménový řadič v lese, tak automaticky tento řadič bude plnit všech 5 rolí zároveň. Postupem času, kdy v našem lese nebo doméně začne být více doménových řadičů, je možné jednotlivé role přesunout na ostatní řadiče.

3.4.3 RID master

RID master předává rozsahy relativních identifikátorů ostatním řadičům v doméně. Tím je zajištěna jednoznačnost těchto identifikátorů v rámci domény. Relativní identifikátor je součástí SID[14], které je generováno vždy při vytváření objektu v doméně. Například při vytvoření nového uživatele, počítače atd. Ve chvíli, kdy se na některém doménovém

[13] STAN REIMER a kolektiv, Active Directory Resource Kit, s. 28
[14] http://en.wikipedia.org/wiki/Security_Identifier

řadiči počet nevyužitých identifikátorů z přiděleného rozsahu blíží kritické hranici (standardně posledních 100), požádá doménový řadič o další rozsah relativních identifikátorů.

Pokud se stane, že RID master je po nějakou dobu nedostupný, tak na některých doménových řadičích mohou vzniknout problémy při vytváření objektů. Pokud například budeme chtít vytvořit objekt typu uživatele na doménovém řadiči, který již vyčerpal svůj přidělený rozsah relativních identifikátorů, tak toto vytvoření selže. Máme zde však možnost vytvořit uživatele na jiném doménovém řadiči, který ještě nevyčerpal svůj přidělený rozsah. Nejlepším řešením je samozřejmě opět zpřístupnit doménová řadič s rolí RID master, anebo tuto roli převést na jiný řadič, který je dostupný.

Roli RID master je možné kdykoliv převést na jiný řadič domény pomocí snap-in konzole Active Directory uživatelé a počítače nebo pomocí příkazového řádku a utility Ntdsutil.

3.4.4 PDC emulátor

Tato role je zodpovědná za časovou synchronizaci mezi řadiči domény, prioritní replikaci hesel a má význam pro konzoli skupinových politik a starší operační systémy. Tato role PDC (Primary Domain Controller) je důležitá u operačních systémů Windows NT, jelikož stanice a servery musely být schopny komunikovat s PDC při procesu změny hesla. Kromě tohoto je PDC emulátor také důležitý při replikaci hesel. Pokud si uživatel změní jméno na jiném řadiči, než který zastává roli PDC emulátoru, tak bude změna hesla urychleně replikována právě na řadič s funkcí PDC emulátoru. Pokud se totiž uživatel s čerstvě změněným heslem pokusí přihlásit k jinému doménovému řadiči (kde bude mít ještě stále staré nezměněné heslo, tedy za předpokladu, že ještě neproběhla replikace) skončí tento pokus chybou. V tomto okamžiku je pokus přihlášení opakován a směrován na PDC emulátor. Pokud uživatel zadal správné nové heslo, je ověřen a přihlášení bude úspěšné.

3.4.5 Infrastructure master

Role Infrastructure master je zodpovědná za aktualizaci group-to-user referencí. Když přesouváme uživatele z jedné domény do jiné nebo při smazání konkrétního uživatele, tak role zajistí, aby se tato změna projevila ve všech skupinách, kterých byl daný objekt členem.

3.4.6 Schema master

Doménový řadič s funkcí Schema master je jediný řadič v doméně, který má právo provádět změny do schématu[15] Active Directory. Pro provedení změny ve schématu je nutné být členem skupiny Schema Admins a být připojen na správný doménový řadič s rolí Schema master. Po provedení změn ve schématu si všechny doménové řadiče v celém lese tyto změny jednosměrně zreplikují.

3.4.7 Domain Naming Master

Domain Naming Master je zodpovědný za přidávání nebo odebírání domén v lese. Doménový řadič s touto rolí kontroluje, zda jméno nové domény je jedinečné (zda již v lese doména s tímto názvem neexistuje). V případě nedostupnosti není možné přidávat nebo odebírat domény v lese.

3.5 RODC – Read Only Domain Controller

S příchodem Windows Server 2008 přibyla možnost instalovat doménový řadič pouze pro čtení tzv. RODC (Read Only Domain Controller). Využití pro takovýto typ doménového řadiče se nachází v pobočkách, popřípadě v místech, kde nemůžeme zajistit fyzickou bezpečnost klasického doménového řadiče. Doménová řadič pouze pro čtení sdílí databázi Active Directory jen s tím rozdílem, že jeho databáze neobsahuje citlivá data (jako například hesla všech uživatelů). Pokud by tedy došlo k nějakému incidentu a někdo nepovolaný by se dostal až k datům uloženým na daném doménovém řadiči, tak by hesla k důležitým uživatelským účtům stejně nezískal. Pokud se totiž nenastaví, které hesla se mají na doménovém řadiči jen pro čtení uchovávat, tak se zde žádná neuchovávají. Jediná hesla, která si ve výchozím nastavení řadič domény jen pro čtení systému ukládá, jsou hesla vlastního účtu počítače a speciálního účtu krbtgt pro příslušný řadič domény jen pro čtení[16].

Můžeme však nastavit, aby se hesla pro konkrétní uživatele, kteří pracují na pobočce, kde se daný doménová řadič jen pro čtení nachází, ukládaly. Pokud se tedy daný uživatel přihlásí na svůj počítač a jeho účet je nastaven, aby replikoval své heslo na daný doménový řadič jen pro čtení, tak si při prvním přihlášení (v tomto případě

[15] http://msdn.microsoft.com/en-us/library/ms675085(v=vs.85).aspx
[16] Více zde: http://technet.microsoft.com/cs-cz/library/cc753223(v=ws.10).aspx

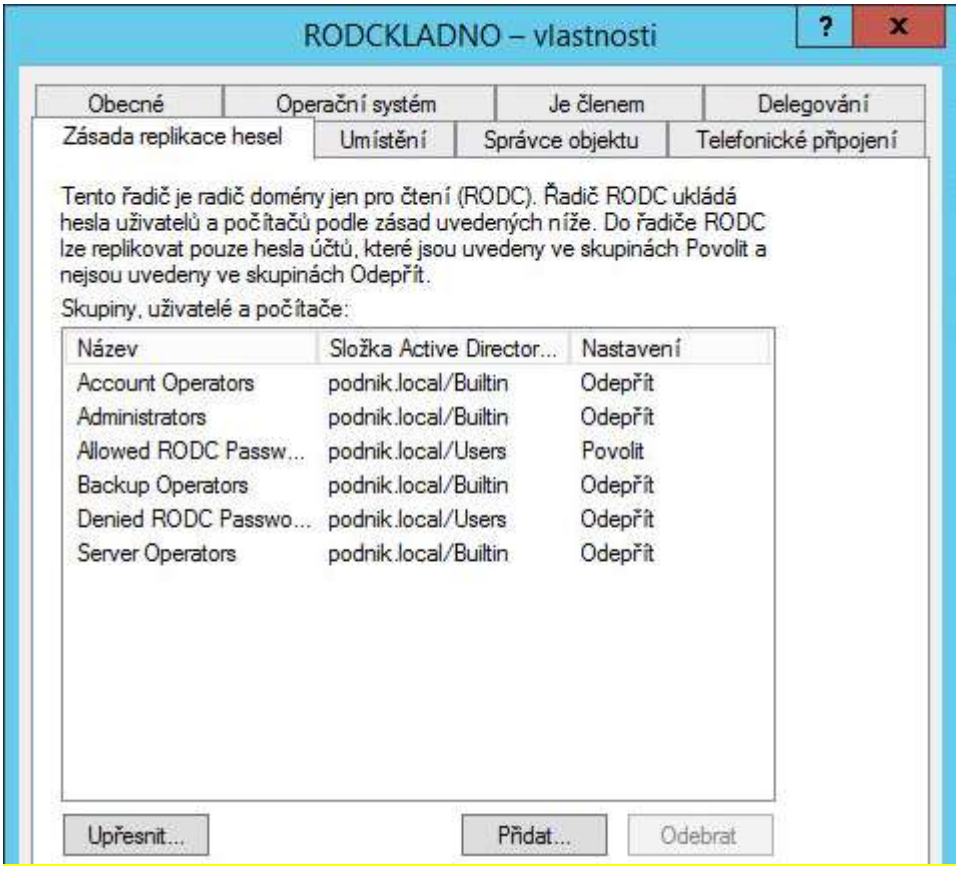
doménový řadič jen pro čtení přepošle výzvu k přihlášení na klasický doménový řadič) tyto informace uloží k sobě a při dalším přihlášení ověří heslo již ze své databáze a nebude se dotazovat klasického doménového řadiče. Standardně jsou tedy na doménovém řadiči jen pro čtení uložena hesla uživatelů, kteří pracují v pobočce, kde se tento doménový řadič nachází. V případě jakékoliv zkompromitování doménového řadiče jen pro čtení tak dochází ke zcizení hesel jen pro účty v dané pobočce, a proto si musí změnit hesla jen tito uživatelé.

Předpoklady pro instalaci RODC:

- Na doménovém řadiči, který v síti funguje jako PDC emulátor, musí být nainstalován operační systém Windows Server 2008 nebo novější.
- Před samotnou instalací je nutné v lese spustit v příkazovém řádku příkaz **adprep /rodcprep**
- RODC musí replikovat s doménovým řadičem, na kterém je nainstalován operační systém Windows 2008 nebo novější a tento řadič musí mít zároveň roli Globálního katalogu
- Úroveň funkčnosti doménové struktury (Forest Functional level) musí být minimálně Windows Server 2003
- Úroveň funkčnosti domény (Domain Functional level) musí být minimálně Windows Server 2003

3.5.1 Nastavení politiky replikace hesel na doménové řadiče jen pro čtení

Pokud je v nějaké naší pobočce vytvořený doménový řadič jen pro čtení, je potřeba mu ještě sdělit, u kterých uživatelských účtů si může uložit hesla. Toho se docílí tak, že v konzoli **Uživatelé a počítače služby Active Directory** v organizační jednotce doménových řadičů (popřípadě na organizační jednotku, kde máme objekt našeho doménového řadiče) se vyvolají **Vlastnosti** daného řadiče. Na záložce **Politika replikace hesel** je možné nastavit skupiny, u kterých je možné povolit nebo zakázat replikaci hesel na konkrétní doménový řadič jen pro čtení. Pokud tedy chceme přidat uživatele nebo skupinu, klikneme na tlačítko **Přidat.** Vše názorně zobrazuje následující obrázek.



Obrázek 12 RODC přidání replikace hesel

3.6 Správa Skupinových politik (Group policy)

Skupinové politiky jsou sadou předvoleb a nastavení, které jsou aplikovány na konfigurace uživatelů a počítačů v Active Directory. Zjednodušují administraci úkonů, které se často opakují a jsou tedy díky zásadám skupin zautomatizovány. Příkladem může být nasazení nového softwaru, konfigurace pracovní plochy, připojení síťových disků, politika hesel atd.

Administrátoři mohou díky Skupinovým politikám provádět z jednoho místa následující úkony:

- Centralizovaně řídit uživatele a počítače v podniku
- Automaticky vynutit jednotlivé politiky a jejich aplikace na konkrétních počítačích a pro určité uživatele
- Zjednodušeně a centrálně řídit úlohy jako aktualizace a instalace aplikací
- Soustavně implementovat bezpečnostní politiku na všechny počítače v podniku
- Efektivně vytvářet a implementovat jednotné počítačové prostředí pro uživatele

Skupinové politiky umožnují jak spravovat uživatele a jejich počítače, tak umožňují jednotnou a efektivní správu doménových řadičů a ostatních serverů v podnikovém prostředí.

Služba Skupinové politiky poskytuje široké možnosti jak spravovat nastavení uživatelů a počítačů v prostředí Active Directory. Následující tabulka zobrazuje oblasti, které mohou být Skupinové politikami spravovány[17]:

Instalace softwaru	Můžeme instalovat, odinstalovat, nebo upgradovat software na základě umístění uživatele nebo počítače v Active Directory
Skripty	Můžeme spouštět skripty při spuštění nebo vypnutí počítače, popřípadě při přihlášení nebo odhlášení uživatele
Bezpečností nastavení	Obsahuje bezpečnostní nastavení jak pro počítače, tak pro uživatele. Lze nastavovat firewall, systémové služby, logy

[17] **Stanek, William R.** *Group policy - Zásady skupin ve Windows s. 55*

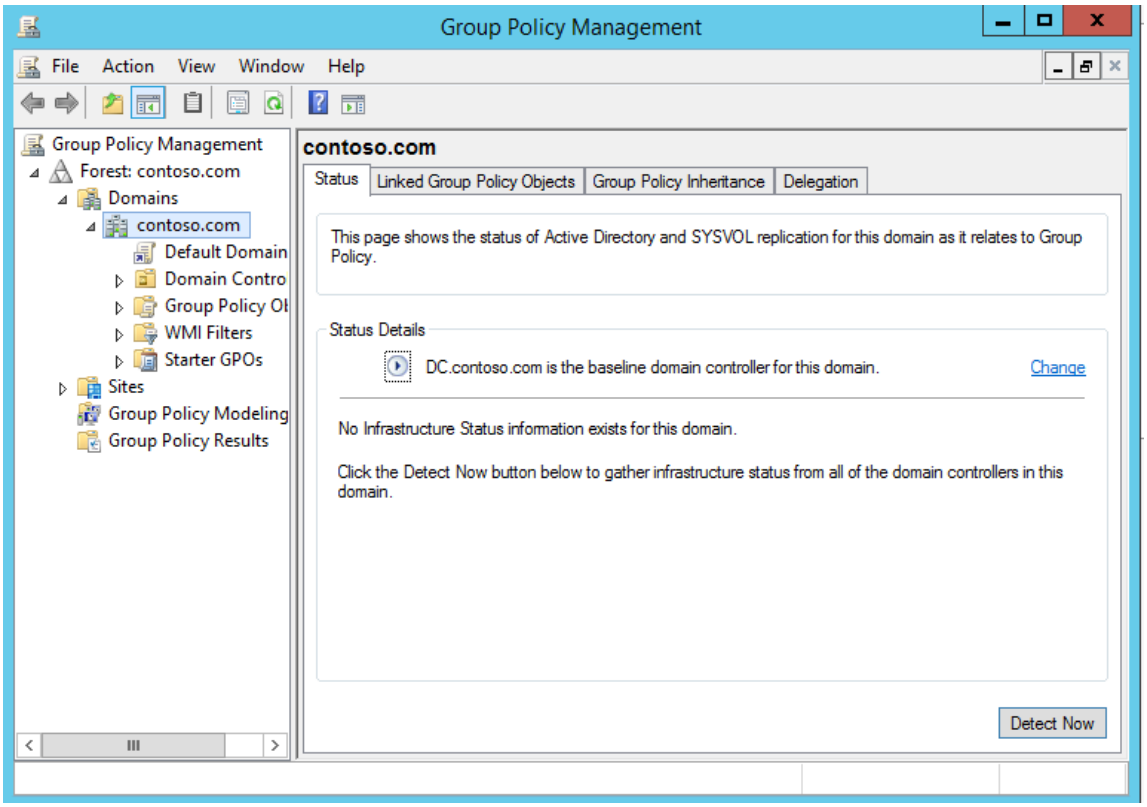
Přesměrování složek	Lze přesměrovat uživatelské složky (složka Dokumenty, Start menu, Plochu, Kontakty, Stažené soubory a další) na síťový disk a tím ulehčit jejich zálohování a dostupnost pokud uživatelé pracují na více počítačích
Quality of Services	Definovaní minimální nebo maximální šířky přenosového pásma a upřednostnění vybraných síťových služeb před ostatními
Nastavení Internet Exploreru	Nastavení menu, oblíbených položek, záložek, úrovní zabezpečení
Šablony pro správu	Možnost řídit nastavení vztahující se k systému Windows jako například nastavení jednotlivých prvků v Ovládacích panelech. Tato volba zahrnuje také mapování sítových disků, definování systémových proměnných, správa lokálních uživatelů a skupin a nastavení služeb a zařízeních.
Tiskárny	Umožnuje povolit nebo zakázat instalaci tiskáren uživateli. Dále umožňuje přiřadit síťové tiskárny uživatelům nebo konkrétním počítačům.
Zákaz instalace dalších zařízení	Omezení zařízení, která mohou být zapojena a použita s PC.
Možnosti napájení	Řízení spotřeby, nastavení jasu, přepínání do režimu spánku atd. Obecně určuje, jakým způsobem bude PC využívat elektrickou energii

Tabulka 3 přehled oblastí pro správu Skupinovými politikami [zdroj: *Windows® Server 2008 Active Directory Resource Kit*, úprava: autor]

Jednotlivé Skupinové politiky je možno vázat na tyto tři komponenty[18]:

- Lokalita (Site)
- Doména (Domain)
- Organizační jednotka (OU)

Pro správu Skupinových politik se využívá konzole Skupinových politik (Group Policy Management). Její základní obrazovku zobrazuje následující obrázek:



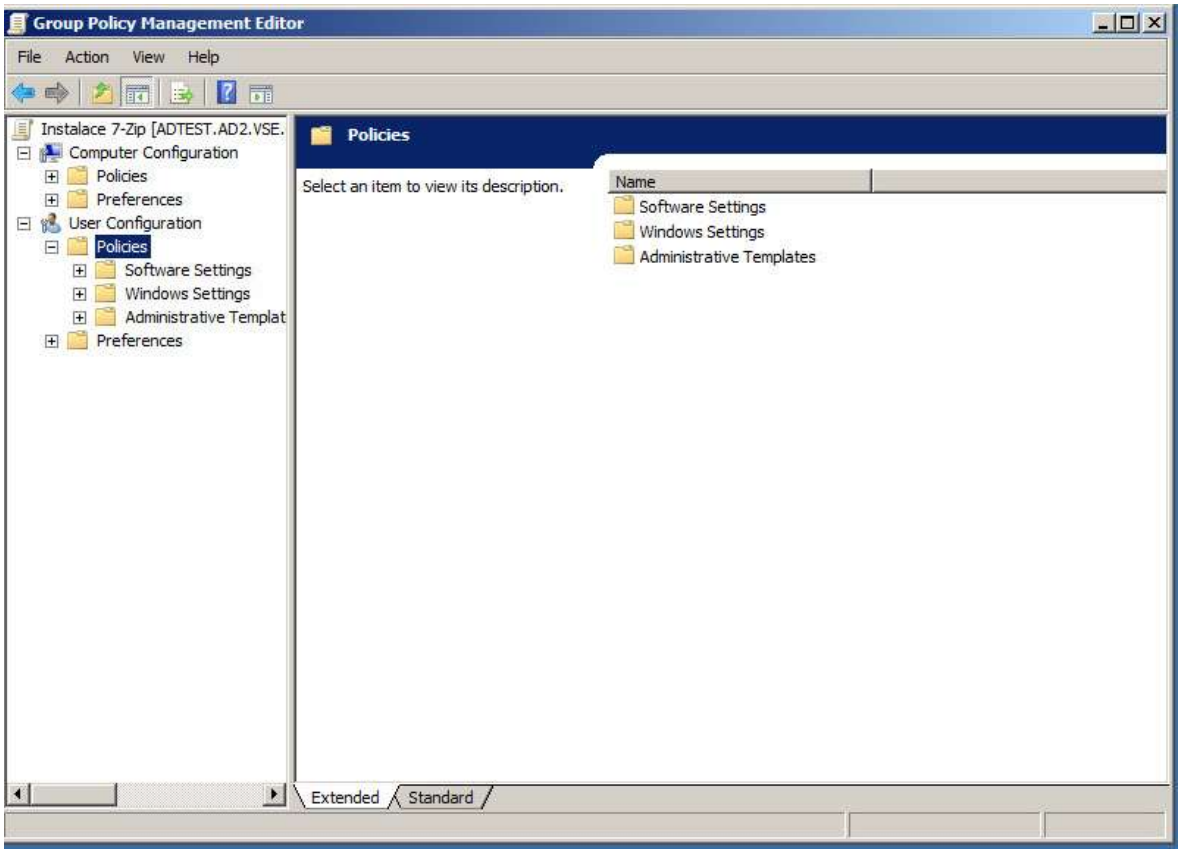
Obrázek 13 Konzole pro správu Skupinových politik[zdroj: Microsoft Virtual Lab]

V této konzoli probíhá veškerá konfigurace Skupinových politik. Základním prvkem Skupinových politik je objekt skupinové politiky. Zjednodušeně lze říci, že každý takovýto objekt obsahuje určitá nastavení, která budou aplikována. Jednotlivé objekty pak můžeme přiřadit na konkrétní domény, lokality a konkrétním organizačním jednotkám, a tím vynutit daná nastavení jen pro určité uživatele nebo počítače nacházející se v daném umístění. Jeden objekt může být přiřazen i více komponentám.

[18] **Stanek, William R.** *Group policy - Zásady skupin ve Windows s. 45*

3.6.1 Objekt skupinové politiky

Každá skupinová politika má 2 strany – počítač a uživatel. Pohled na objekt skupinové politiky jak můžeme vidět na následujícím obrázku. I když můžeme v jednom objektu skupinové politiky konfigurovat obě strany, tak to neděláme. Obecně vytváříme samostatné objekty skupinové politiky pro počítače a pro uživatele. I proto máme v Active Directory objekty typu uživatel a počítač v oddělených organizačních jednotkách.



Obrázek 14 Editace politiky zásad [zdroj: autor]

Objekt skupinové politiky si lze představit pro jednoduchost jako dokument obsahující konkrétní nastavení (jedno nebo několik), která budou systémem vynucena. K tomu, aby byla tato nastavení vynucena jen na požadovaných počítačích, nebo pro požadované uživatele slouží Konzole pro správu Skupinových politik, kde se možné přiřadit objekt skupinové politiky na konkrétní lokalitu, doménu nebo organizační jednotku.

Ve skupinových politikách platí pravidlo dědičnosti. Z toho vyplývá, že pokud vytvořím objekt skupinové politiky a přiradím ho k určité doméně nebo organizační jednotce, tak se pravidla definovaná v tomto objektu zároveň aplikují nejen na všechny počítače nebo uživatele v dané organizační jednotce, ale i na všechny podřazené organizační jednotky.

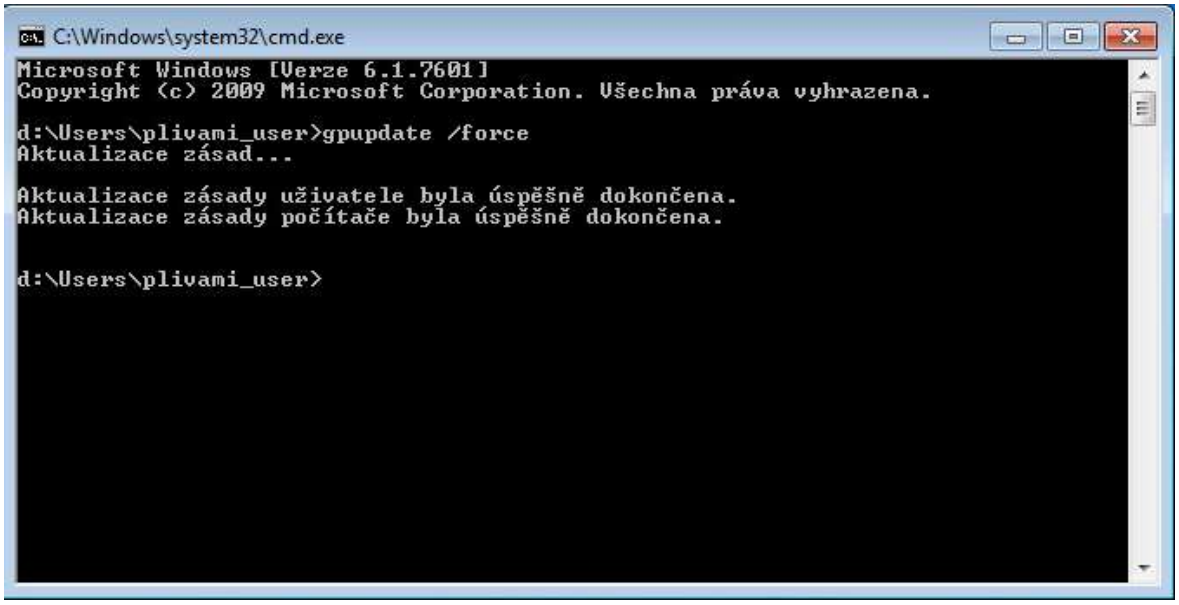
Tato dědičnost může být v některých případech nežádoucí, a proto je možné nad organizačními jednotkami vytvářet blokace, který zamezí aplikaci zděděných skupinových politik na danou organizační jednotku[19].

Zároveň může nastat situace, kdy potřebujeme některou důležitou politiku aplikovat na všechny organizační jednotky i na ty, které obsahují blokace. V tomto případě můžeme nastavit u politiky vynucení (Enforced)[20]. Daná politika tedy bude aplikována na přiřazenou organizační jednotku i na všechny podřazené organizační jednotky a to i v případě, že některá organizační jednotka obsahuje blokaci skupinových politik.

Politiky, které jsou v sekci konfigurace počítače aplikovány při startu počítače a poté každých 90 až 120 minut[21]. Politiky uživatelské konfigurace jsou aplikovány při přihlášení uživatele a poté také každých 90 – 120 minut. Politika, která určuje interval aktualizace skupinových politik, se nazývá Interval aktualizace skupinových politik pro počítače (Group Policy Refresh Interval For Computers a nachází se v sekci Computer Configuration/Administrative Templates/Systém/ Group Policy[22])

V případě, že testujeme nasazení určité politiky, tak zpravidla nečekáme, až se testovaná politika sama projeví (zpravidla do 90 minut) na koncovém počítači, ale vyvoláme aktualizaci skupinových politik manuálně. To se provádí tak, že na koncovém počítači spustíme příkazový řádek (cmd.exe) a zde napíšeme ***gpupdate /force***[23] a stiskneme Enter.

[19] **Stanek, William R.** *Group policy - Zásady skupin ve Windows s. 238*
[20] Tamtéž s. 240
[21] Tamtéž s. 243
[22] **STANEK, William R, Joe RICBARDS a kolektiv,** *Windows® Server 2008 inside out, s.* 1269
[23] **Moskowitz, Jeremy**. *Group policy - Fundamentals, Security and the Managed Desktop* s. 166



Obrázek 15 Manuální aktualizace zásad na koncové stanici [zdroj: autor]

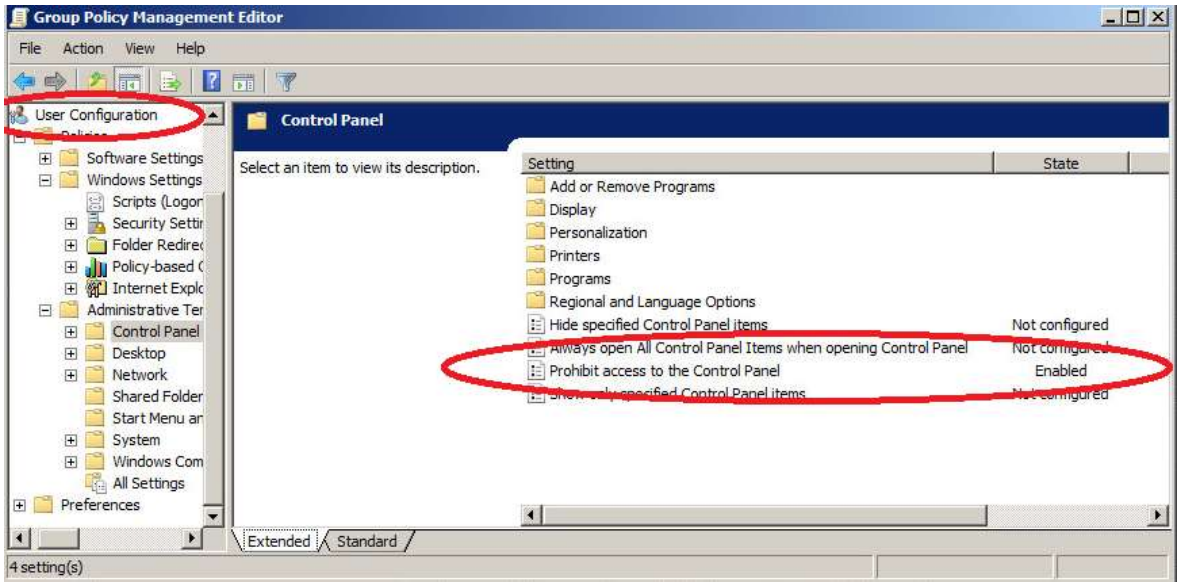
Skupinové politiky jsou aplikovány ve specifickém pořadí: 1. Lokální skupinové politiky (politika na koncovém PC, standardně se nepoužívá v prostředí AD) → 2. politiky aplikované na lokalitu (v praxi se víceméně nepoužívá, pouze ve speciálních případech) → 3. politiky aplikované na doménu[24] → 4. politiky aplikované na organizační jednotku. Pro pořádek je ještě dobré poznamenat, že pokud nějaká další politika přepisuje nastavení jiné politiky, tak je nakonec aplikována politika, která mění dané nastavení jako poslední. Standardně tedy při nějakém konfliktu vyhrává politika, která je aplikována na úrovni organizačních jednotek.

3.6.2 Vytvoření nové skupinové politiky

Jako příklad bych zde uvedl nastavení skupinové politiky, které uživatelům znemožní přístup k Ovládacím panelům v počítači. Nejprve vytvoříme novou politiku. V politice

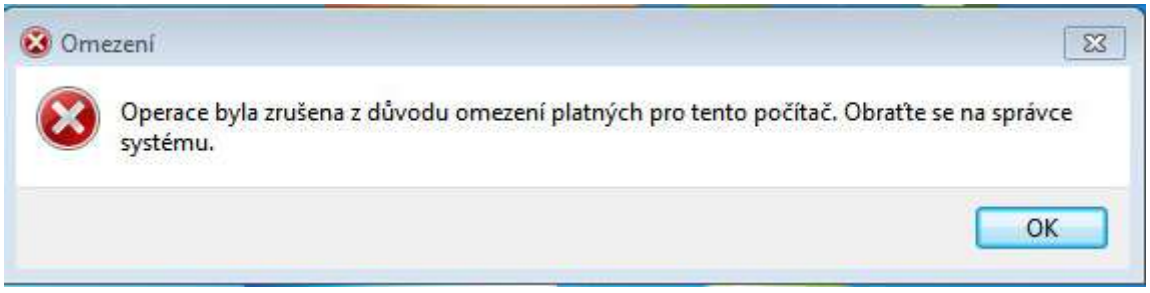
[24] Obecně se moc nevyužívají. Výjimku tvoří Defaultní doménová politika. Jedná se o předpřipravenou politiku, která se aplikuje na celou doménu. Měla by být nejméně restriktivní a v praxi se používá pro nastavení požadavků na heslo a základních nastavení pro celou doménu.

si v uživatelské konfiguraci otevřeme Administrative Templates a zde vybereme Control Panel. Zde už jen vybereme politiku Prohibit access to the Control Panel a změníme její stav z Not Configured na Enabled. Viz následující obrázek:



Obrázek 16 Zákaz přístupu k Ovládacím panelům [zdroj: autor]

Dále tuto politiku uložíme, přejdeme v Konzoli skupinových politik na organizační jednotku s uživateli, kterým chceme tuto politiku vnutit a provedeme přiřazení. Po zhruba 90 minutách nebo dalším přihlášení již uživatelé nebudou moci přistupovat do Ovládacích panelů. Pokud se o to pokusí, zobrazí se jim následující hláška:



Obrázek 17 Výsledek aplikace skupinové politiky[zdroj: autor

3.7 Replikace

Jako replikace v Active Directory označujeme událost, při které dochází ke kopírování provedených změn mezi jednotlivými doménovými řadiči. Pokud přidáme uživatele, odstraníme skupinu anebo změníme uživateli heslo, tak se tato změna provede na doménovém řadiči, na kterém jsme právě přihlášeni. Proces replikace pak zajistí, že se tyto změny dostanou na všechny ostatní doménové řadiče v doméně. Jedná se tedy o proces, který je potřeba tehdy, kdy jsou v doméně nejméně 2 doménové řadiče (dnes většina domén).

To, jak rychle se daná změna přenese na ostatní doménové řadiče, záleží také na topologii Active Directory a počtu doménových řadičů. V zásadě rozlišujeme 2 typy replikací[25]:

- Intrasite replikace (replikace v rámci jedné lokace)
- Site replikace (mezi jednotlivými lokacemi)

Nastavení replikací se provádí přes **Active Directory Sites and Services**.

3.7.1 Intrasite replikace

Jedná se o replikace, které probíhají v jedné lokace (site). Zde je předpoklad, že všechny doménové řadiče jsou propojeny vysokorychlostním připojením. Standardně se tento typ replikací používá, pokud jsou všechny doménové řadiče v jedné geologické lokaci, ale není to nutné. S rozšířením vysokorychlostního připojení je dnes možné nechat doménové řadiče v jedné logické lokaci, i když jsou v různých lokacích fyzicky.

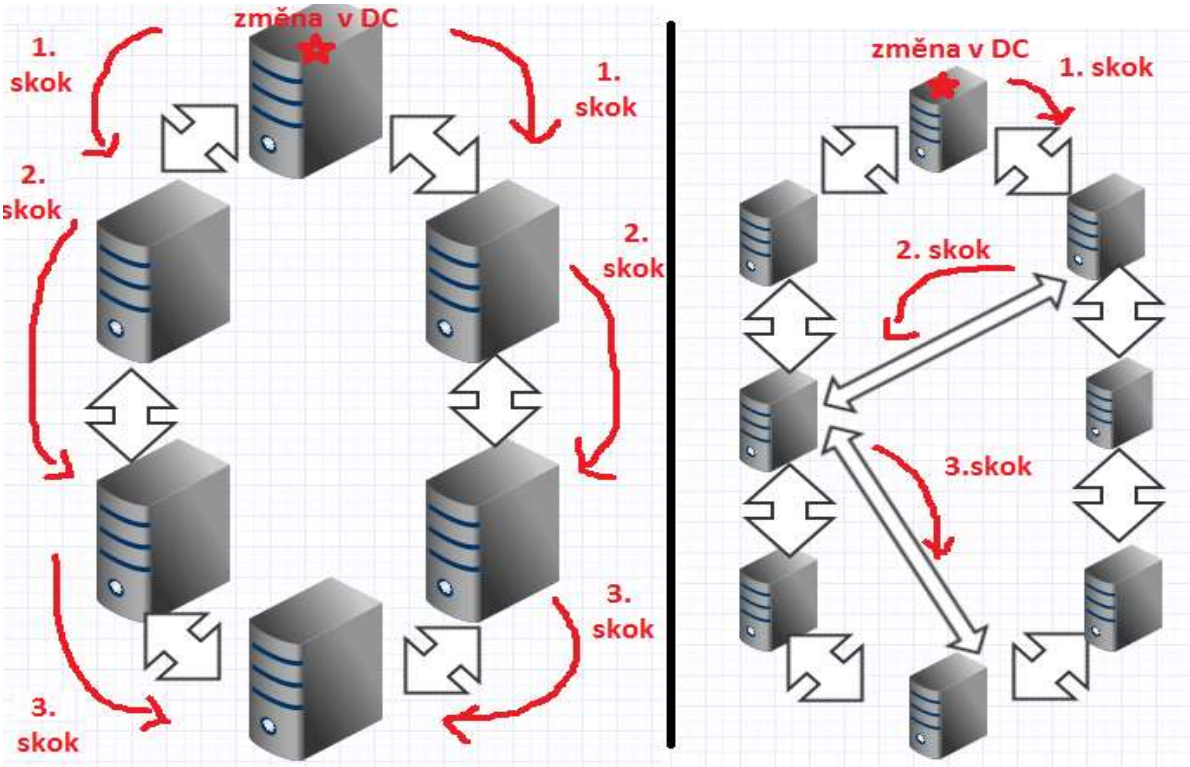
Dnes se doporučuje rozdělení na lokace dle rychlosti linky. Pokud je rychlost pod 0,5 MB/s je vhodné vytvořit mezi touto linkou 2 rozdílné lokace (site)[26].

Replikace probíhají téměř okamžitě a stará se o ně proces zvaný KCC[27] (Knowledge Consistency Checker). Ten automaticky vytváří nejefektivnější návrh replikací a stará se o samotné replikace. Pokud dojde ke změně na některém doménovém řadiči, automaticky

[25] **DESMOND Briana kolektiv.** *Active Directory. 5th edition s.395*
[26] školení Gopas
[27] http://technet.microsoft.com/en-us/library/cc961781.aspx

tuto změnu oznámí ostatním doménovým řadičům a provede replikaci. Rychlost replikace záleží na počtu doménových řadičů v dané lokaci (site) a standardně je nastaven na 18 (15 + 3) vteřin[28] na sousední řadiče (návrh, které řadiče jsou sousední, automaticky provádí KCC). Pokud je počet doménových řadičů v síti takový, že nelze replikace přenést na všechny řadiče přes 3 skoky (sousední řadiče), automaticky KCC upraví cesty replikačního cyklu.

Následující obrázek zobrazuje jak si KCC upraví cesty tak, aby se změny replikovaly na všechny doménové řadiče v lokalitě.



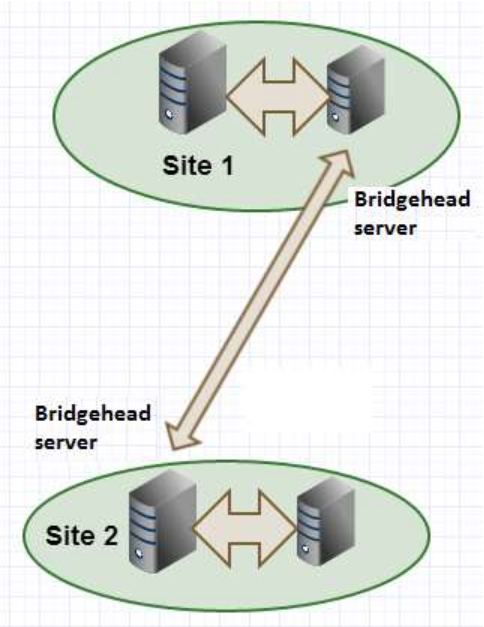
Obrázek 18 replikace ve stejné lokaci (intrasite) [zdroj:autor]

3.7.2 Site replikace

Pokud máme 2 lokace a potřebujeme mezi nimi provádět replikace, jsou v každé lokaci určeny tzv. Bridgeheads servery, které provádějí replikace mezi lokacemi. V každé lokaci se tedy nachází jeden Bridgeheads server a mezi lokacemi probíhá komunikace právě mezi 2 Bridgeheads servery. V každé lokaci se pak změny dále replikují standardně tak, jak bylo popsáno výše. Volbu jaký server bude Briedgeheads server volí systém automaticky[29]. Je

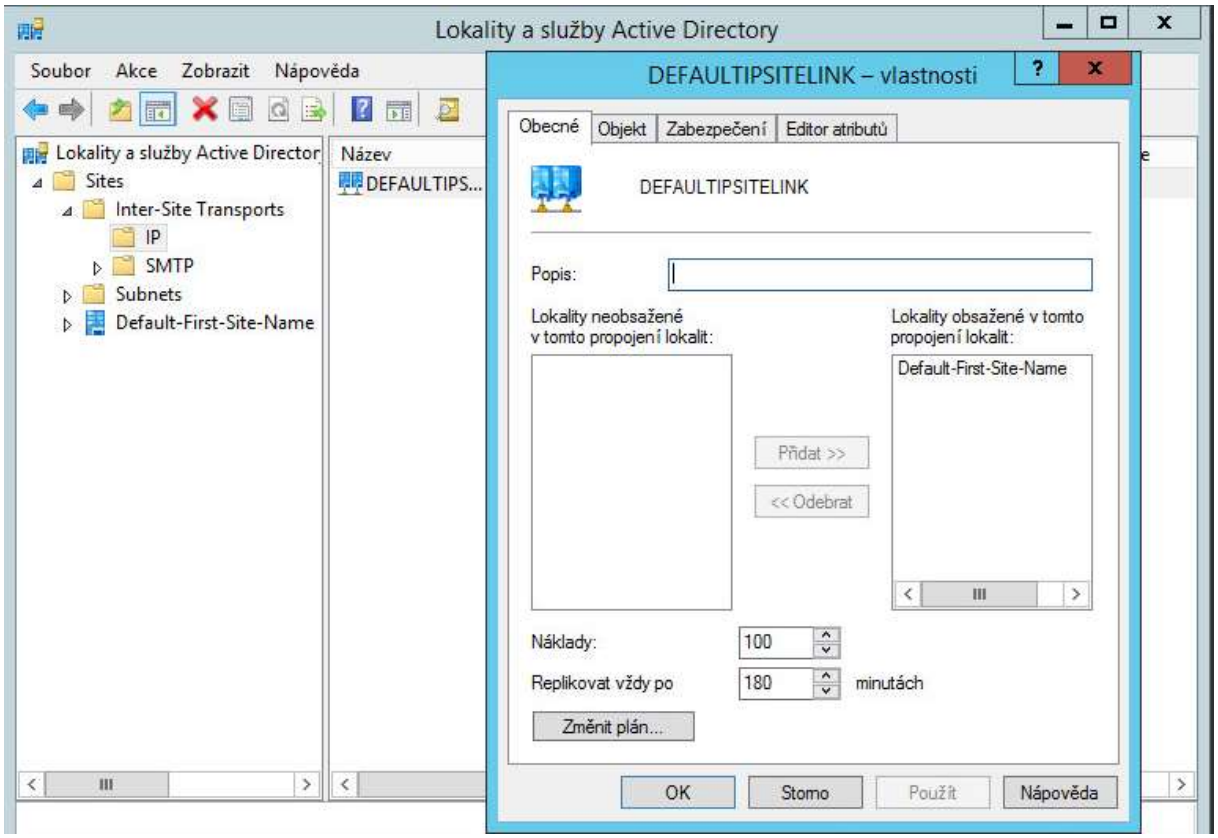
[28] http://technet.microsoft.com/en-us/library/cc728010(v=ws.10).aspx
[29] O toto se stará proces ISTG viz http://technet.microsoft.com/en-us/library/cc755994(v=WS.10).aspx

zde však možnost zvolit Briedgeheads server manuálně. Pokud z nějakého důvodu zvolíme server manuálně, musíme počítat s tím, že v případě nedostupnosti, zničení serveru přestanou replikace mezi lokacemi fungovat. Pokud necháme výběr Bridgeheads serveru automaticky, tak se při nedostupnosti automaticky zvolí jiný server v dané lokaci a replikace fungují nadále.



Obrázek 19 Intersite replikace [zdroj:autor]

Pro informace o replikacích mezi lokalitami se používá příkaz „**repadmin /bridheads“** který vypíše, jaké servery jsou Bridgeheads a pro okamžitou synchronizaci se používá příkaz **„repadmin /syncall“.** Standardně je replikace mezi lokacemi nastavena na každých 180 minut. Toto nastavení lze ovšem také změnit v **AD Sites and Services** ve vlastntostech **Inter-Site Transports – IP.**

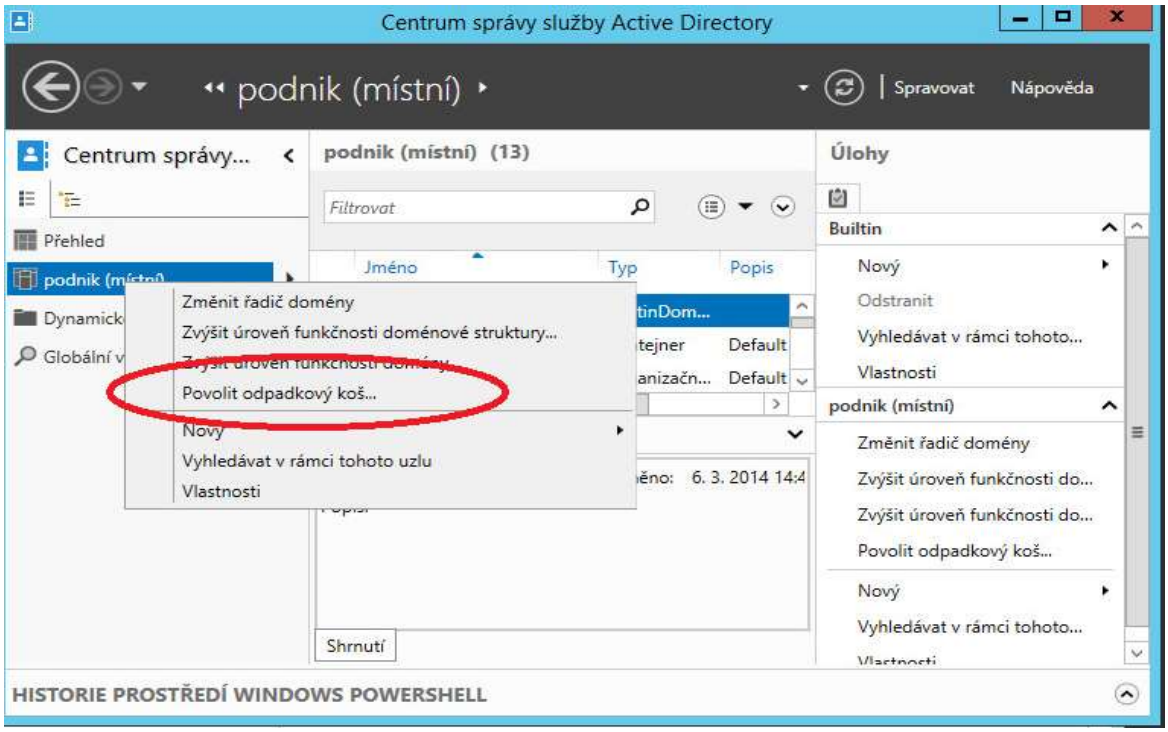


Obrázek 20 Nastavení replikace mezi lokacemi[zdroj:autor]

3.8 Zálohování a obnova Active Directory

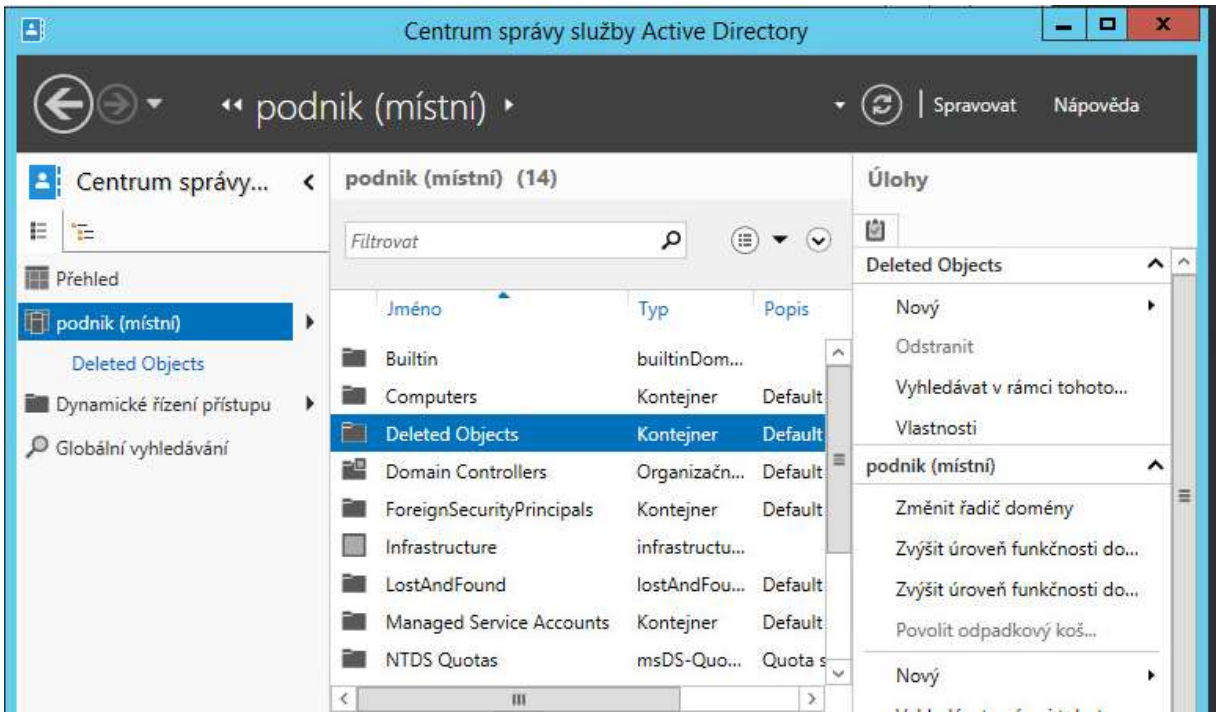
Active Directory je klíčová služba pro jakýkoliv podnik, ve kterém je nasazena. Pokud z nějakého důvodu dojde k její dočasné nedostupnosti, bude práce uživatelů s počítači velmi omezená. Uživatelé se nebudou moci přihlásit k počítači, nebudou fungovat síťové disky a ostatní aplikace závislé na Active Directory. Je tedy důležité, jakýmkoliv výpadkům přecházet důkladnou prevenci, a zároveň být připraven jakoukoliv nedostupnost AD rychle vyřešit.

Nejčastěji se vyskytujícím případem obnovy dat je současné době obnova nechtěně smazaných objektů v Active Directory, který se v nejnovějších verzích Active Directory řeší přes odpadkový koš, který slouží na stejném principu jako koš ve Windows 7. Pokud chceme funkci koše využít, musí být úroveň funkčnosti doménové struktury alespoň Windows Server 2008 R2 a funkce koše musí být povolena v Centru správy služby Active Directory. Administrátor musí být také v případě potřeby připraven na obnovu celé databáze ze zálohy.



Obrázek 21 Povolení funkce koše v AD [zdroj: autor]

Jakmile dojde k povolení koše, tak všechny objekty v Active Directory, které následně smažeme, bude možné obnovit v konzoli Centra správy Active Directory pod položkou Deleted Objects.



Obrázek 22 Možnost obnovy smazaných objektů pomocí koše [zdroj: autor]

3.8.1 Záloha Active Directory

K záloze Active Directory lze od verze Windows Server 2008 používá aplikace Windows Server Backup, která je dostupná jako role serveru. Pokud máme jedno doménové prostředí, stačí nám provést zálohu jednoho doménového řadiče. V případě více doménového prostředí je vhodné provést zálohu nejméně jednoho doménového řadiče v každé doméně.

Záloha doménového řadiče obsahuje následující položky[30]:

- Active Directory – složku NTDS
- Bootovací soubory nutné pro spuštění počítače
- COM+ - databázi registrovanych COM komponent
- Registry

[30] **DESMOND Brian a kolektiv** *Active Directory. 5th edition s. 500*

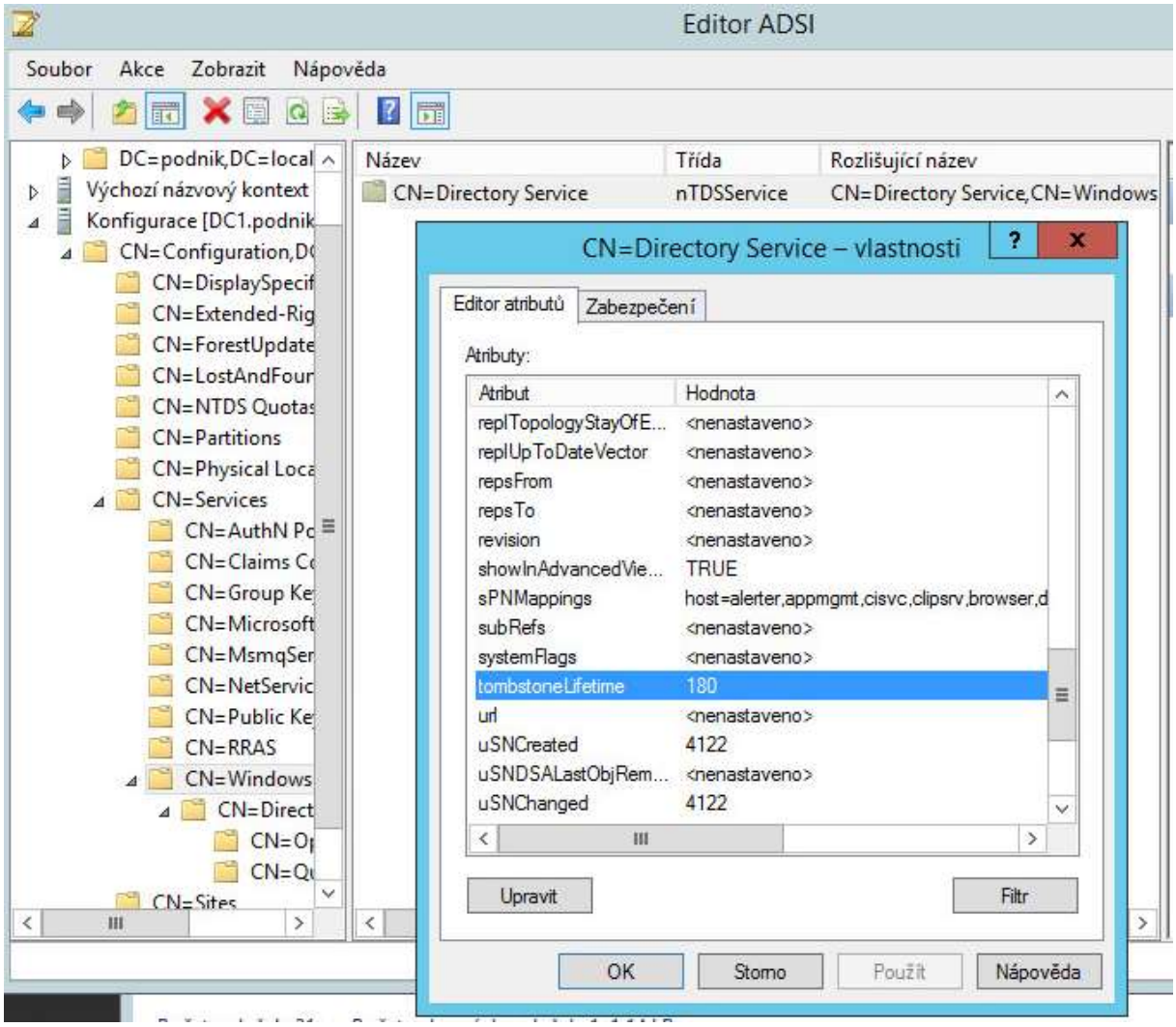
- SYSVOL – složku Sysvol, která obsahuje skupinové politiky a přihlašovací/odhlašovací skripty
- Služby Certifikace – pouze pokud řadič funguje jako certifikační autorita
- Všechny soubory operačního systému

K tomu, abychom mohli provádět zálohování, je nutné být členem skupiny doménových administrátorů nebo skupiny Backup operators.

Samozřejmě lze kromě role Windows Server Backup využít i nástrojů třetích stran. Těmito nástroji se ale v této práci nebudu zabývat. Instalace funkce Windows Backup Server se provádí z konzole Správa serveru, kde v nabídce **Správa** vybereme **Přidat role a funkce** a zvolíme možnost **funkce**, kde v seznamu vybereme možnost **Zálohování serveru**.

Při zálohování Active Directory musíme vzít v potaz, že AD má vlastní způsob zpracování smazaných objektů. Když smažeme objekt v Active Directory, tak se fyzicky nemaže, ale označí se jako neplatný (tombstoned) a nadále je replikován mezi doménovými řadiči. Proměnná tombstone (jejíž standardní hodnota je 180 dní) pak určuje délku, po kterou jsou smazané objekty replikovány, než dojde k jejich fyzickému smazání. Tento mechanizmus zajišťuje, že nedojde k náhodné obnově dříve smazaných objektů, tedy objektů starších než je hodnota u proměnné tombstone. Je tedy nutné pamatovat na to, že standardně nemůžeme obnovit zálohu Active Directory starší než je udávaná hodnota v proměnné thombstone. Změnu[31] hodnoty TombstoneLifetime je možné provést přes ADSI editor.

[31] http://technet.microsoft.com/cs-cz/library/cc784932(v=ws.10).aspx



Obrázek 23 Nastavení hodnoty tombstoneLifetime [zdroj: autor]

Důležité je si všechny kroky při zálohování a při obnově ze zálohy vyzkoušet před ostrým provozem a v pravidelných intervalech testovat jak vytvoření záloh tak bezproblémové obnovení dat ze záloh. Zkrátíme tím dobu potřebnou pro obnovu ze zálohy v případě skutečné havárie. V případě havárie je člověk pod stresem a snaží se obnovit funkčnost Active Directory co nejrychleji. Rozhodně by se nemělo stávat, že případná havárie je situace, kdy dochází poprvé k obnově dat ze zálohy.

Předcházet potřebě obnovy Active Directory lze také tím, že všechny důležité změny budeme nejprve provádět v testovací Active Directory[32].

Pokud nasazujeme Active Directory na fyzické servery, je vhodné použít servery, které mají hardwarovou redundanci. Jedná se o to, že servery jsou vybaveny 2 stejnými hardwarovými komponentami. Například 2 nezávislými zdroji, kdy v poškození jednoho zdroje převezme jeho činnost druhý. Kromě samotného pravidelného zálohování by se měla Active Directory zálohovat před jakoukoliv větší změnou jako je například změna AD schématu nebo hromadný import velkého množství objektů.

Vždy se doporučuje nasadit v každém podniku nejméně 2 doménové řadiče. I zde platí pravidlo redundance a v případě poruchy jednoho z nich jeho funkci převezme druhý řadič. Uživatelé tak prakticky nezasáhne havárie jednoho řadiče a budou moci i nadále běžné pracovat na svých počítačích a využívat síťových služeb.

3.8.2 Obnova Active Directory

Obnově Active Directory je nejlepší se vyhnout, ale když už dojde k situaci, že potřebujeme obnovit databázi Active Directory, je potřeba na ni být připraven. Dobrý plán a příprava nám pomůžou k tomu, že obnova Active Directory nebude tak velký problém, jak se na první pohled může zdát.

Základem, pro úspěšné a rychlé obnovení po havárii, je být připraven na různé typy katastrof. Nejvíce budeme Active Directory obnovovat v případě náhodně smazaných objektů, anebo v případě selhání doménového řadiče. Asi nejčastějšími případ selhání je poškození hardwarové součástky v serveru. Může se jednat o vadný pevný disk, paměťový modul, nebo jinou komponentu, která vyřadí doménový řadič z činnosti. Dalším, avšak méně častým případem havárie, může být přírodní katastrofa.

Obnova Active Directory může být dvojího typu:

- Neautoritativní

[32] Jedná se o Active Directory databázi na které nejsou závislé žádné důležité systémy a kterou máme pro experimentální účely. Jako například testování změn, nebo aplikace důležitých upgradů.

První možnost je normální obnova neboli také neautoritativní obnova. V tomto případě se prostě obnoví ze zálohy Active Directory databáze, o které víme, že je v pořádku. Zjednodušeně tedy vrátíme stav databáze zpátky v čase. Jakmile dojde k obnově a spuštění doménového řadiče, tak si doménový řadič sám vyhledá své replikační partnery a provede všechny aktualizace databáze od doby, do níž byl obnoven. Při tomto způsobu se využívá standardních replikací z ostatních řadičů, které zajistí, že obnovený doménový řadič bude během chvíle opět obsahovat aktuální kopii databáze Active Directory.

- Autoritativní

V situacích, kdy normální obnova není vhodná (například, pokud chceme obnovit již smazané objekty) můžeme použít autoritativní obnovu. Za normálních okolností pokud bychom obnovili jeden doménový řadič ze zálohy, tak by jeho databáze obsahovala smazané objekty. Vlivem replikací by ale zanedlouho došlo k situaci, kdy by se na tento obnovený řadič replikovaly aktuální změny z ostatních řadičů, a proto by došlo opět ke smazání právě obnovených objektů. V tomto případě se při obnově postupuje tak, že se obnovené objekty, které chceme zachovat, označí jako autoritativní a tudíž se při replikacích jeví jako novější (mají vyšší verzi[33]), a tudíž se při replikacích nesmažou, nýbrž replikují na ostatní doménové řadiče.

[33] Viz http://blogs.msdn.com/b/richpec/archive/2011/10/07/the-authoritative-restore-explained.aspx

3.8.3 Obnova FSMO rolí

FSMO role jsou zvláštní role, které jsou v rámci lesa, nebo domény umístěny vždy jen na jednom doménovém řadiči. Samotná databáze Active Directory se vždy nachází na každém řadiči, a proto není problém ji v případě potřeby obnovit. Pokud dojde k tomu, že server, na kterém je nějaká z FSMO rolí, se stane nedostupný, tak je nutné tuto roli přesunout manuálně. Následující tabulka obsahuje seznam FSMO role a kde je můžeme najít na doménovém řadiči:

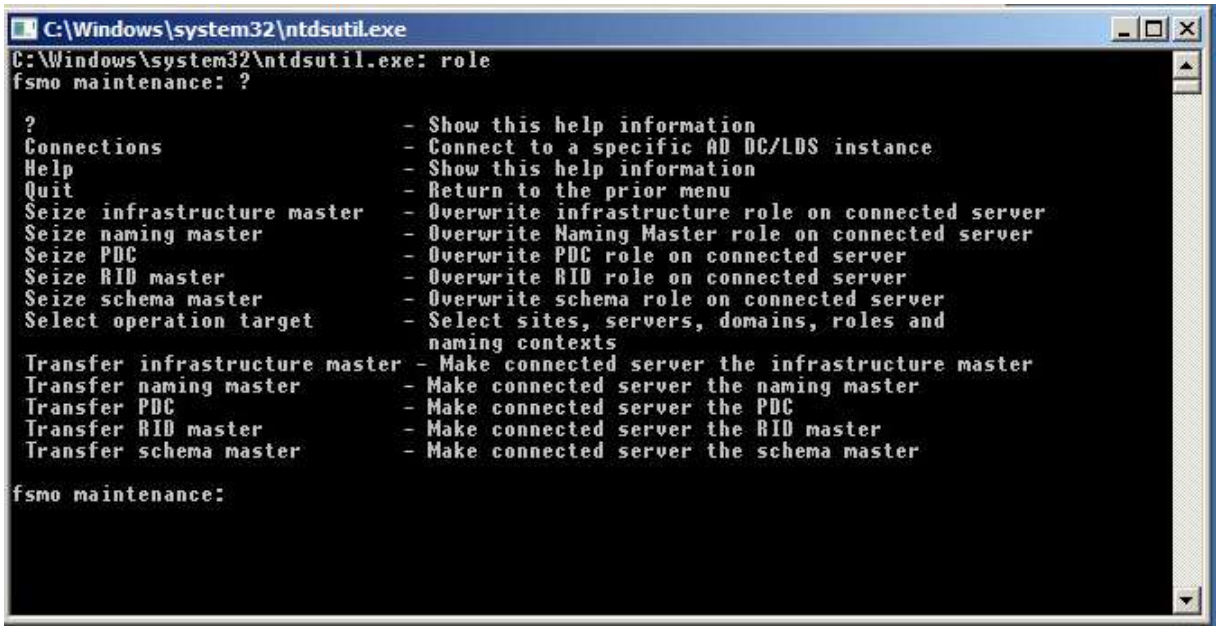
Role	Umístění
Schema master	Schéma služby Active Directory
Domain Naming Master	Domény a vztahy důvěryhodnosti služby Active Directory
RID master	uživatelé a počítače služby Active Directory
PDC Emulator	uživatelé a počítače služby Active Directory
Infrastructure master	uživatelé a počítače služby Active Directory

Tabulka 4 umístění FSMO rolí na doménovém řadiči [zdroj: DESMOND Brian a kolektiv ***Active Directory. 5th s. 533*** **]**

Pokud rádi používáme příkazovou řádku, tak je možné seznam všech FSMO rolí a serverů zjistit, pokud použiji příkaz ***netdom query fsmo /domain:nazevvasidomeny***

Přes tabulku výše lze přenést role jen v případě, že je daný doménový řadič spuštěn. V případě, že je již nedostupný, tak role nejsou přenášeny (z ang. Transfer FSMO role), ale nuceně převedeny na jiný doménový řadič (z ang. Seize FSMO role). K tomu, aby mohly být role nuceně převedeny, se využívá utilita ntdsutil

Pomocí ní lze takto nutně převést všechny zmiňované role. Nejprve se připojíme na doménový řadič, na který chceme nuceně převést nějakou FSMO roli. Poté již v samotné utilitě ntdsutil spustíme příkaz ***roles*** a dále příkaz ***seize*** a konkrétní role. Pro přehlednost následující tabulka uvádí syntaxi k jednotlivým rolím:



Obrázek 24 Utilita pro nucené převedení FSMO rolí [zdroj: autor]

Samotný proces vykonaný touto utilitou má jednu příjemnou vlastnost. Pokud se pokusíme jedním z výše uvedených příkazu nuceně převést roli z jednoho doménového řadiče na druhý, tak i když se dle příkazu jedná o nucené převedení (seize), tak se utilita nejprve pokusí normálně přenést roli (transfer) a až pokud se to nepovede, tak ji převede nuceně.

3.9 Design Active Directory

Při návrhu Active Directory je nutné vzít v potaz, že neexistuje vždy jen jeden správný návrh řešení pro jeden konkrétní podnik. Mezi odborníky převládá názor, že většinou to nejjednodušší řešení je to nejlepší[34]. Zároveň existuje hodně omezení, kterým je nutné se vyvarovat. Nejčastější z nich jsou uvedeny zde:

- Bezpečností hranice pro Active Directory je les a nikoliv doména. Kdokoliv administrátor s právy na jakýkoliv doménový řadič v jakékoliv subdoméně se může stát administrátorem jakékoliv domény v celém lese[35]
- Nikdy nemůžeme odebrat kořenovou doménu v lese bez zničení celého lesa.
- Jeden doménový řadič může být pouze pro jednu doménu
- Aplikace skupinových politik na hluboce zanořenou strukturu organizačních jednotek vede ke zvýšení doby nutné k přihlášení do sítě.

Při návrhu struktury Active Directory v kterémkoliv podniku neexistuje jedno správné řešení.

3.9.1 Design domén

Doména v Active Directory je charakteristická těmito vlastnostmi:

- **Replikační hranice**
  Hranice domény jsou zároveň hranice pro replikace doménové partition a také pro doménové informace uložené ve složce SYSVOL na všech doménových řadičích.
- **Hranice pro síťové zdroje**
  Hranice domény jsou také hranice pro zdroje, ke kterým může uživatel přistupovat. Standardně uživatel z jedné domény nemůže přistupovat ke zdrojům v jiné doméně, pokud explicitně nezíská dané oprávnění.
- **Hranice pro bezpečnostní politiky**
  Některé bezpečností politiky aplikovány na úrovni domény jsou aplikovány na všechny uživatele v doméně. Tyto politiky zahrnují politiku hesel, uzamčení účtů a politiku Kerberos tiketů.

[34] **DESMOND Brian a kolektiv** *Active Directory. 5th edition s. 533*
[35] http://www.wug.cz/zaznamy/191-MS-Fest-2013-Praha-How-to-Hack-AD-Forest-from-a-Subdomain

Ideální je mít jedno doménové prostředí ačkoliv někdy je vhodné nasadit více doménové. Následující přehled zobrazuje rozdíly mezi jedno doménovým a více doménovým prostředím[36]:

Jedno doménové prostředí

Většina malých a středních podniků by měla zvážit nasazení jedno doménové prostředí.

- V doméně může být až přes 1 milion objektů, což je většinou dostatečný prostor a není tudíž nutné kvůli tomu vytvářet více domén
- V případě že chceme nebo je požadována samostatnost jednotlivých oddělení, je možné delegovat správu na úrovni organizačních jednotek
- Pokud ve společnosti často dochází k reorganizaci nebo pohybu uživatelů mezi odděleními, je mnohem jednodušší přesouvat uživatele mezi odpovídajícími organizačnímu jednotkami než mezi rozdílnými doménami

Více doménové prostředí

Většinou se jedná o velké nadnárodní společnosti.

- Omezení replikací. Replikace kopírují všechny změny ve struktuře Active Directory na všechny doménové řadiče. Pro velké společnosti tak mohou být replikace zdrojem vytížení a zpomalení linky mezi pobočkami.
- Omezení přístupu k síťovým zdrojům.
- V případě fúzí společností je nutné zachovat jejich identitu.

Existují 2 základní požadavky při návrhu domén:

1. Navrhnout Active Directory tak, aby odrážela strukturu podniku
2. Minimalizovat počet domén a využít možností organizačních jednotek v Active Directory

Při návrhu prostředí Active Directory je nutné brát v potaz fyzickou strukturu podniku a zároveň strukturu řízení IT v podniku. Obecně existují 4 základní přístupy pří řízení IT v podnicích[37]:

1. Centralizované řízení

[36] **Stan Reimera kolektiv** *Windows® Server 2008 Active Directory Resource Kit.s 174*

[37] převážně ve velkých organizacích dochází často k reorganizacím. Je proto vhodné navrhnout takovou strukturu Active Directory, která bude flexibilně reagovat na dané reorganizační požadavky bez nutnosti dalších výdajů. Ze zkušeností je proto návrh Active Directory založen většinou na geografické poloze nebo organizační struktuře podniku.

V tomto případě je celé IT řízeno z jednoho místa

2. Decentralizované řízení
   V decentralizovaném řešení je IT řízeno lokálně na úrovni poboček nebo na úrovni jednotlivých oddělení popřípadě divizí.
3. Hybrid
   Ve velkých společnostech se jedná o jedno z nejrozšířenějších řešení. Jedná se o to, že určitá část IT (například správa doménových řadičů a konfigurace celopodnikových politik) je řešena centrálně, zatímco například strukturu organizačních jednotek si řeší každé oddělení lokálně.
4. Outsourcing
   Zde je správa IT svěřena do rukou cizí organizaci, která pro náš podnik zabezpečuje chod a správu IT. Rozsah a poskytování služeb záleží na konkrétní organizaci.

Pokud chceme nasadit v prostředí více domén, měly by nás k tomu vést určité důvody. Hlavní důvody pro nasazení více doménového prostředí jsou tyto tři:

- Oddělené replikace

  Mnoho velkých společností zavádí domény dle kontinentů. Důvod je, že v nadnárodní firmě s více doménami se nemusí replikovat všechen obsah z jednoho kontinentu na druhý. Což by mohlo vytěžovat podnikové linky.

- Požadavky na rozdílné Kerberos politiky
- Politiky pro obnovu šifrovaného souborového systému (EFS)

Pokud tedy některá oddělení nebo lokality potřebují speciální politiky šifrování, je vhodné je oddělit do vlastní domény.

Zároveň je potřeba při návrhu domén vzít v úvahu, že domény jsou neflexibilní a také že každá další doména potřebuje pro svůj chod minimálně jeden nový doménový řadič (ideálně 2 a více). Základním doporučením je tedy využít pouze jednu doménu a pouze pokud k tomu bude důvod, tak nasadit více doménové prostředí. Pokud nás k tomu nenutí situace a výše uvedené důvody, tak je vhodné použít jedno doménové prostředí.

3.9.2 Návrh struktury Organizačních jednotek v doméně

Organizační jednotky jsou základním stavebním blokem každé domény. Jejich hierarchické uspořádání je důležité jak z hlediska administrace, tak z hlediska aplikování skupinových politik (Group Policy). Pokud například chceme nastavit jednotnou plochu pro určité počítače, stačí si tyto počítače vložit do jedné organizační jednotky a na tu poté aplikovat politiku nastavení plochy. Pokud chceme, aby určité oddělení (počítače a uživatele v tomto oddělení) spravoval pouze určitý administrátor, můžeme opět všechny objekty počítače pro dané oddělení vložit do jedné organizační jednotky a nastavit možnost administrace danému administrátorovi.

Organizační jednotky mají několik charakteristik:

- Organizační jednotky mohou obsahovat vnořené organizační jednotky a tím tak vytvářet hierarchickou strukturu. Standardně se jakákoliv politika zásad, která se aplikuje na nejvyšší organizační jednotku, aplikuje i na vnořené organizační jednotky. Existují zde však způsoby, kdy je možné toto chování modifikovat[38].
- Uživatel nebo aplikace, který hledá nějaký objekt v Active Directory se nemusí zajímat o to, ve které organizační jednotce se daný objekt nachází.
- Strukturu organizačních jednotek je možné jednoduše změnit i po vytvoření. To je hlavní rozdíl mezi organizačními jednotkami a doménou nebo lesem. Zároveň je zde velmi jednoduché jednotlivé objekty přesouvat mezi různými organizačními jednotkami. Ačkoliv je velmi jednoduché přesouvat objekty z jedné organizační jednotky do druhé a zároveň i jednotlivé organizační jednotky mezi s sebou, je nutné brát zřetel na dopady, které dané přesuny mohou mít a které politiky se na přesunuté objekty budou vztahovat. Proto je vždy důležité si předem jednotlivé změny promyslet a až poté provést.

[38] Viz blokace a vynucení skupinové politiky v kapitole 3.6.1 této práce

Při návrhu organizačních jednotek se začíná od vrcholové úrovně návrhu organizačních jednotek, jelikož po vytvoření a naplnění objekty jsou změny v této části obtížnější. Většinou se při návrhu vychází z nějakého neměnného prvku ve společnosti. Mezi nejznámější návrhy vrcholové úrovně organizačních jednotek tedy patří tyto 2 návrhy[39]:

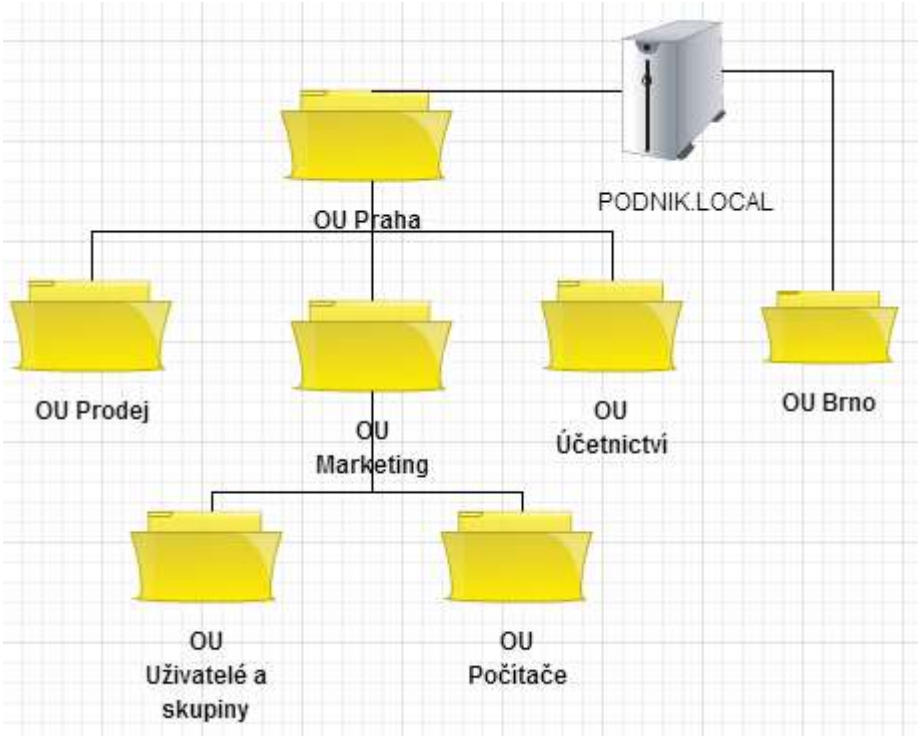
- Na základě geografického umístění společnosti

  Tento model je velmi odolný změnám v organizaci. Pokud už ve společnosti dochází často ke změnám ve struktuře, tak se to jen zřídka kdy dotkne geografického umístění. Tento model je také vhodný ve spolupráci s decentralizovanou správou, kdy každá pobočka nebo centrála má vlastní administrátory. Na druhé straně není tento návrh nejvhodnější, pokud máme v každé pobočce stejná oddělení. V tomto případě by se hodilo mít vrcholovou úroveň založenou na odděleních.
- Na základě jednotlivých oddělení ve společnosti

  V tomto modelu je vrcholová úroveň organizačních jednotek tvořena na základě oddělení ve společnosti. Tento způsob je vhodný pro menší společnosti, které mají pouze jednu centrálu (geografickou lokaci). Nevýhodou ovšem zůstává, že tento návrh je náchylnější při restrukturalizaci společnosti.

Většina společností využívá kombinaci těchto dvou návrhů. Na vrcholové úrovni jsou organizační jednotky založeny na geografickém umístění a na nižší úrovni jsou naopak organizační jednotky založeny na základě jednotlivých oddělení.

[39] **Stan Reimer a kolektiv** *Windows® Server 2008 Active Directory Resource Kit s. 195*



Obrázek 25 Návrh Organizačních jednotek na základě kombinace geografického přístupu a přístupu dle oddělení [zdroj: autor]

3.9.3 Návrh na umístění FSMO rolí doménového řadiče

Když se rozhodujeme, na jaké servery umístit FSMO role, mohou nám pomoci toto doporučení[40]:

- Schema master, Domain naming master a RID master by měli být v lokaci, kde je ještě jeden doménový řadič, se kterým přímo replikují. Důvod je ten, že pokud řadič, na kterém jedna z těchto rolí je, selže, tak bude nutné tyto role přesunout. Ideální je přesunout je na řadič, který je ve stejné síti a je přímý replikační partner řadiče selhaného.

[40]**Stan Reimer a kolektiv** *Windows® Server 2008 Active Directory Resource Kit s.. 213*

- RID master musí být dostupný všem doménovým řadičům, protože pokud některý doménový řadič požádá RID master o další blok relativních identifikátorů, využívá při této žádosti vzdálené volání procedur.

Pokud má firma centrální uložiště, kde jsou uloženy všechny nebo většina uživatelských účtů, tak se doporučuje umístit všechny operační role do stejné lokace.

Doporučení pro design Active Directory[41]:

- Snaha tvořit vše co nejjednodušeji. Nejlepší je mít jen jeden les
- Pokud v organizaci existuje více než jedna doména, je doporučeno mít tzv. oddělenou kořenovou doménu. Pomáhá to oddělit administrátory domény od administrátorů jednotlivých lesů.
- Pokud instalujeme doménový řadič do nějaké pobočky, vytváříme pro tuto pobočku vlastní lokaci. Navíc pokud nemůžeme fyzickou bezpečnost serveru, nainstalujeme doménový řadič pouze pro čtení (RODC)

[41] **Stan Reimer a kolektiv** *Windows® Server 2008 Active Directory Resource Kit.s. 214*

4 Praktická část

Cílem praktické části diplomové práce je nasazení službu Active Directory v podnikovém prostředí. Celé nasazení bude probíhat ve virtuálním prostředí na platformě VMware. K dispozici je 8 virtuálních počítačů s tím, že 3 virtuální počítače budou sloužit jako servery a 5 jako pracovní stanice.

4.1 Zadání praktické části

Navrhněte a realizujte nasazení Active Directory pro určený podnik. Z podniku jsem obdržel následující požadavky:

Popis společnosti

Jedná se o mladou společnost, která podniká v oblasti prodeje a servisu zahradní techniky. V současné době má jednu pobočku v Praze a menší pobočku na Kladně, kde se nachází pouze obchodní zastoupení. V budoucnu by chtěla rozšířit síť svých poboček i do dalších měst po České republice. Pokud dojde k rozšíření poboček, bude každá další pobočka obsahovat vlastní IT oddělení, které bude spravovat její IT infrastrukturu.

4.1.1 Výchozí situace

Firma doposud používala jako operační systém na počítačích svých zaměstnanců Windows XP a nepoužívala žádnou centrální správu počítačové sítě. Na serverech společnosti je nainstalován Windows 2003. Všechny počítače tak byly spravovány samostatně. Uživatelé měli na všech stanicích administrátorské práva. Zároveň všichni uživatelé a jednotlivá oddělení využívali sdílený síťový disk jako společné místo pro spolupráci. V podniku panovalo nejednotné nastavení a s rostoucím počtem zaměstnanců se situace stávala neúnosnou. Neexistuje systematické zálohování. Pokud některý zaměstnanec zálohuje, tak jen díky svému proaktivnímu přístupu.

4.1.2 Cílová situace

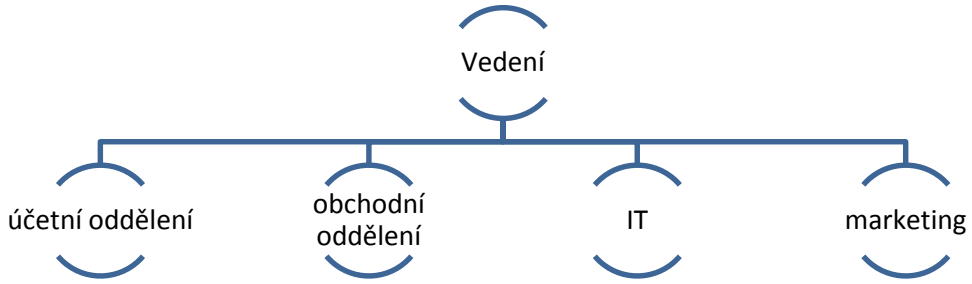
Vytvořit centrální správu počítačové sítě založené na technologii Active Directory od společnosti Microsoft. Zjednodušit a zefektivnit správu uživatelů a síťových zdrojů. Zefektivnit celkovou práci IT oddělení a vytvořit ve firmě moderní IT prostředí, které bude moci růst spolu s firmou. Vzhledem k tomu, že firma nakoupila v minulosti nový hardware

s operačním systémem Windows 7, bude tento systém použit v nově vzniklém prostředí. K nasazení na servery preferuje společnost nejnovější verzi Windows Server 2012 R2.

Specifické požadavky:

- **Uživatelé a skupiny**

  Každý uživatel bude mít svůj vlastní prostor na sdíleném síťovém disku. K tomuto disku bude mít přístup jen on. Zároveň bude každý uživatel zařazený ve skupině dle oddělení. Organizační struktura společnosti je zobrazena na následujícím obrázku:



Obrázek 26 Organizační struktura společnosti [zdroj: autor]

  Každé oddělení bude mít vlastní sdílený prostor na síťovém disku dostupný všem členům daného oddělení.

  Uživatelé nebudou mít na svých počítačích Administrátorský přístup a nebudou moci instalovat svévolně aplikace. Výjimku bude tvořit IT oddělení, které bude mít administrátorské přístupy na všechny počítače ve společnosti.

- **Počítače**

  Počítače budou mít jednotné pozadí a bude na nich nainstalován operační systém Windows 7. Jako operační systém na servery budou využity Windows Server 2012 R2.

- **Programy**

  Každý počítač bude obsahovat 2 základní programy - kancelářský balík LibreOffice a program Foxit na čtení a práci s PDF dokumenty. Účetní oddělení bude mít na svých počítačích instalován ekonomický program POHODA, který se ve firmě využívá na zpracování účetních výkazů. Další software bude volitelně k dispozici a každý uživatel si ho bude moci nainstalovat dle vlastního uvážení. Požadovaný přehled pevně instalovaného softwaru a softwaru k instalaci zobrazuje následující tabulka:

Základní software	• Kancelářský balík LibreOffice • FOXIT pro práci s PDF dokumenty
Volitelný software	• 7-Zip – práce s archivy (ZIP, RAR a ostatní) • Notepad++ - rozšířený textový editor • CCleaner – program na vyčištění, zrychlení počítače • PSPad – universální editor
Specifický software	• Účetní program POHODA – pro počítače v účetním oddělení

Tabulka 5 Přehled instalovaného SW [zdroj: autor]

- **Tiskárny**

  Společnost vlastní 4 síťové tiskárny. 3 tiskárny jsou v Praze a jedna v Kladně. Je nutné zajistit, aby každý uživatel mohl ze svého počítače tisknout. Pro běžné uživatele je k dispozici tiskárna Dell 3130. Obchodní oddělení má navíc možnost tisknout na barevné laserové tiskárně Xerox ColorQube 9300. Vedení má k dispozici ještě tiskárnu Kyocera FS1061DN. V Kladně bude pro uživatele dostupná barevná laserová tiskárna Dell 2145cn Color Laser.

- **Zálohy**

  Bude nastaveno automatické zálohování sdílených pevných disků uživatelů i oddělení. Zálohování bude automatické a bude prováděno 1x denně vždy po pracovní době.

  Zároveň budou pravidelně zálohovány doménové řadiče tak, aby v případě poruchy bylo možné Active Directory co nejrychleji obnovit a zkrátit tak výpadek počítačové sítě a s tím související nefunkčnost síťových služeb.

- **Bezpečnost**

  Bude provedeno základní nastavení v oblasti bezpečnosti. Budou definovány a vynuceny požadavky na tvorbu hesla, definovány politiky uzamčení účtů a nastavena brána Firewall. Všechny tyto nastavení bude možno v budoucnu měnit dle požadavků firmy.

- **Obnova ze zálohy**

  Bude vytvořen a otestován plán obnovy v případě výpadku doménového řadiče. Bude proveden simulovaný výpadek služby s nutností obnovy stavu doménového řadiče ze zálohy

4.2 Zpracování praktické části

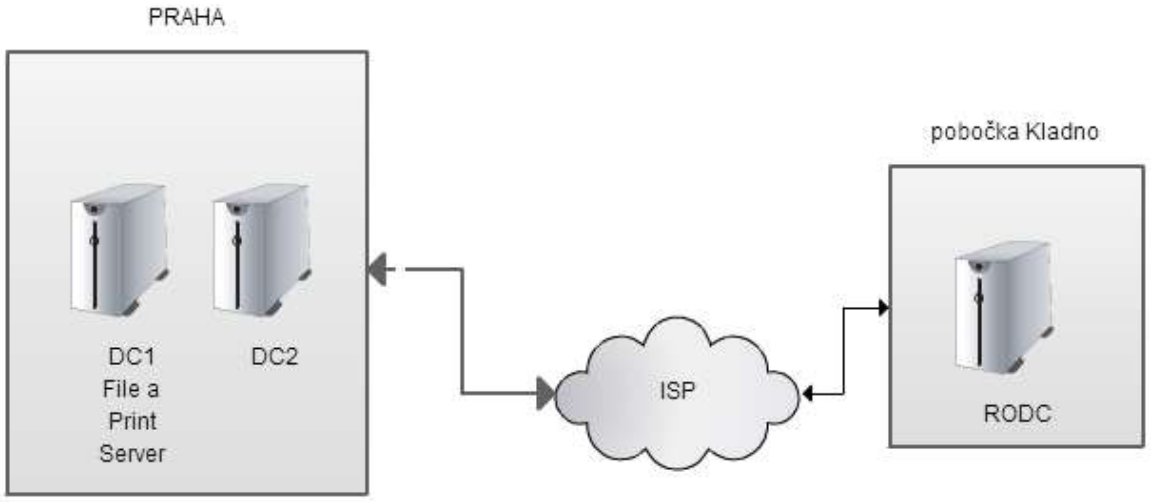
Praktická část se zabývat vlastním návrhem struktury Active Directory, samotnou instalací serverů i klientských stanic a následnou úpravou celého prostředí dle požadavků společnosti.

4.2.1 Návrh struktury Active Directory

Z výše uvedených požadavků a výchozí situace podniku vyplývá, že se jedná o menší firmu, která má potenciál rychle růst. Tomu byla přizpůsobena i navržená struktura Active Directory. Při návrhu byla zvolena 1 doménová struktura[42]. Název domény byl zvolen

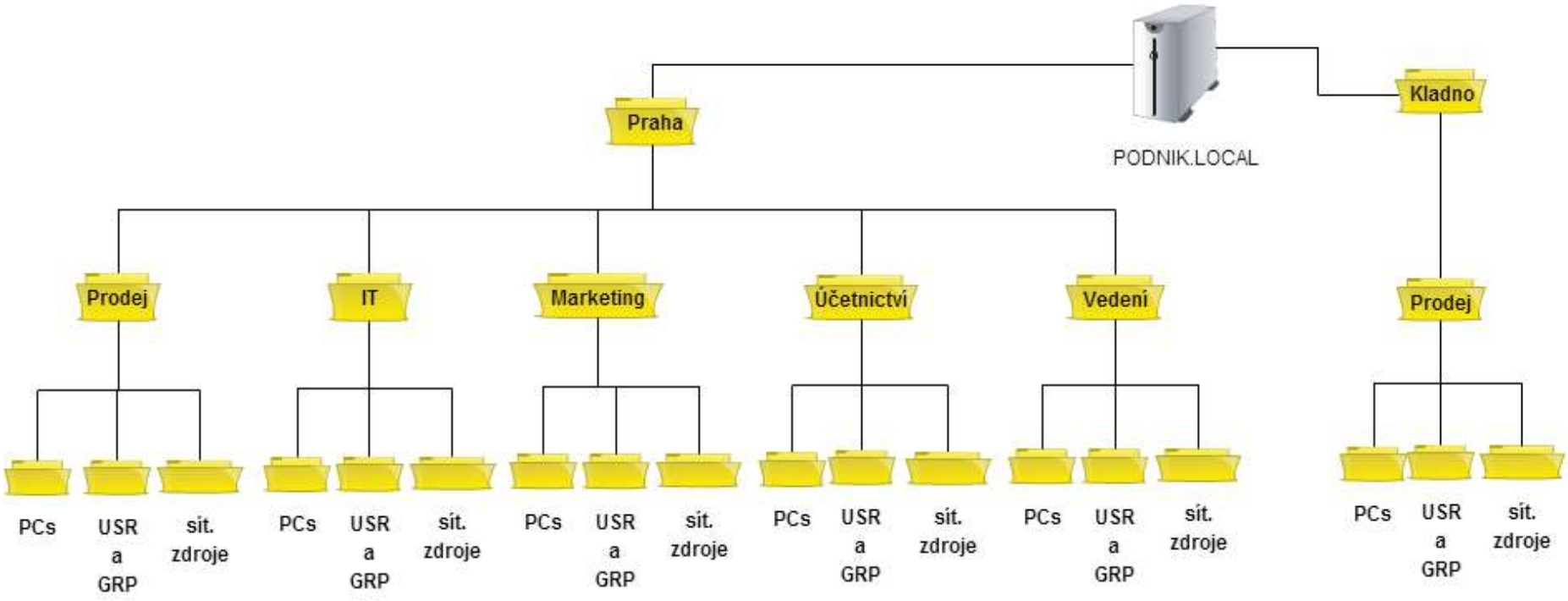
[42] Viz kapitola 3.9.2 této práce

„**podnik.local“.** V případě reálné společnosti bych zvolil její reálné jméno. Fyzické rozvržení serverů pro Active Directory podniku zobrazuje následující obrázek:



Obrázek 27 Rozložení serverů pro AD [zdroj: autor]

Při tvorbě logické struktury Active Directory jsem vycházel z několika poznatků. Za prvé, že firma bude rozšiřovat své pobočky po České republice. Dalším důvodem pro volbu této organizační struktury byla informace, že každá budoucí pobočka bude mít vlastní IT oddělení, které se bude mít pod svou správou zaměstnance, počítače a síťové zdroje pro danou pobočku. Na základě těchto faktů jsem tedy zvolil návrh organizačních jednotek na základě kombinace geografického umístění a rozdělení podniku dle oddělení. Výsledný návrh struktury organizačních jednotek je zobrazen na následující stránce:



Obrázek 28 Struktura Organizačních jednotek v AD pro podnik.local [zdroj: autor]

Jelikož budu jednotlivé IT oddělení mít na správu své pobočky, budou moci administrátoři domény jednoduše delegovat správu jednotlivých poboček lokálním IT oddělením. Zároveň pokud budou některá pobočky provádět vlastní nastavení skupinových politik, nebudou tím ovlivňovat ostatní pobočky.

Rozdělení jednotlivých oddělení na 3 organizační jednotky usnadní přehlednost a správu jednotlivých objektů. V organizační jednotce Uživatele a skupiny byly umístěny objekty uživatelů a skupin vztahujících se k dané organizační jednotce. Jsou tedy logicky odděleny a je možné na ně v případě potřeby cíleně aplikovat skupinové politiky. V organizační jednotce počítače jsou objekty typu počítač. Jejich zařazením do samostatné organizační jednotky opět usnadňuje jejich správu. Poslední organizační jednotkou jsou zdroje. Tato jednotka obsahuje objekty, kterými se řídí přístup k síťovým zdrojům. Díky tomuto granulárnímu rozdělení je tedy možné efektně řídit a spravovat celé síťové prostředí.

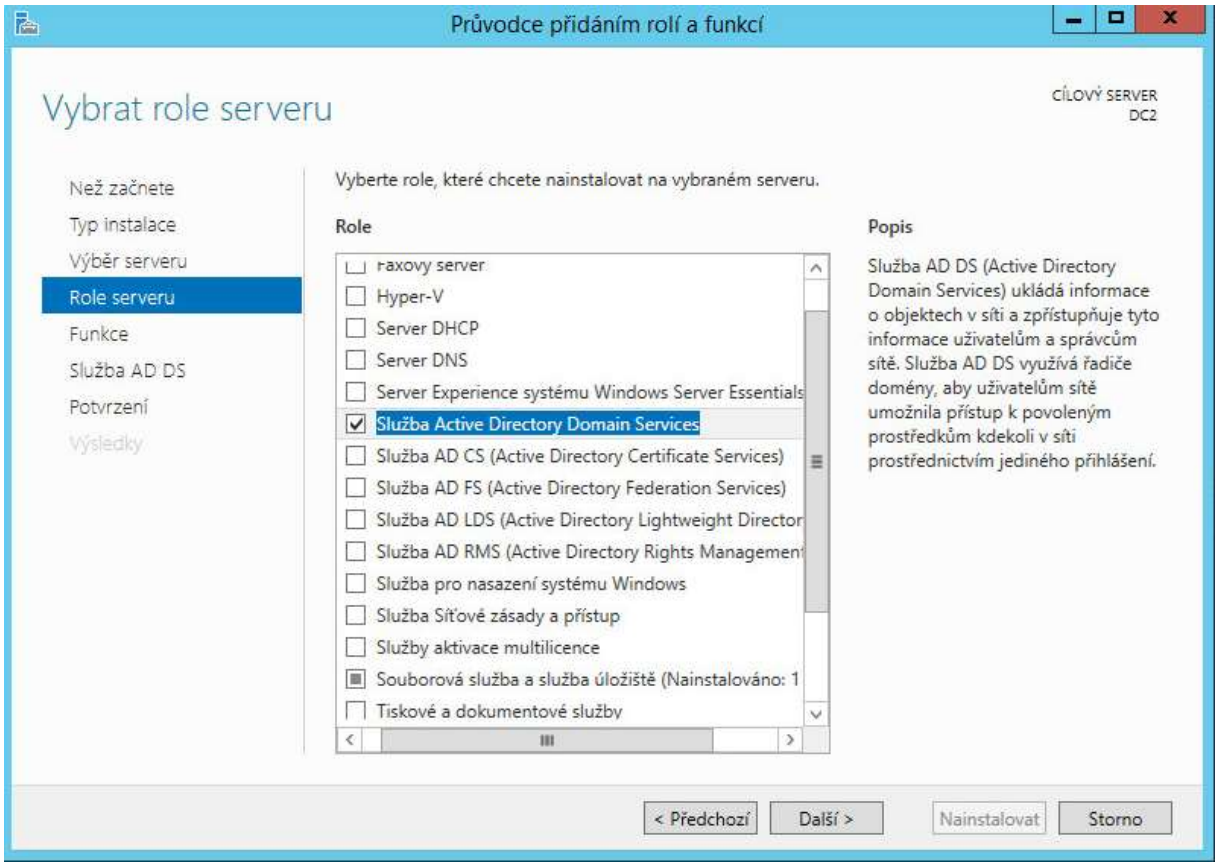
4.2.2 Instalace serverů

Ve virtuálním prostředí jsem měl k dispozici následující hardwarovou konfiguraci pro servery: procesor 1 GHz, RAM 4 GB, HDD 40 GB. Instalace serverů probíhala z ISO souboru připojeného do virtuální CD mechaniky v prostředí VMWare. Na všechny 3 servery byl nainstalován operační systém Windows Server 2012 R2. Jednalo se o klasickou instalaci z grafického prostředí. Jako výchozí jazyk byla zvolena čeština.

Obrázek 29 Instalace serveru [zdroj: autor]

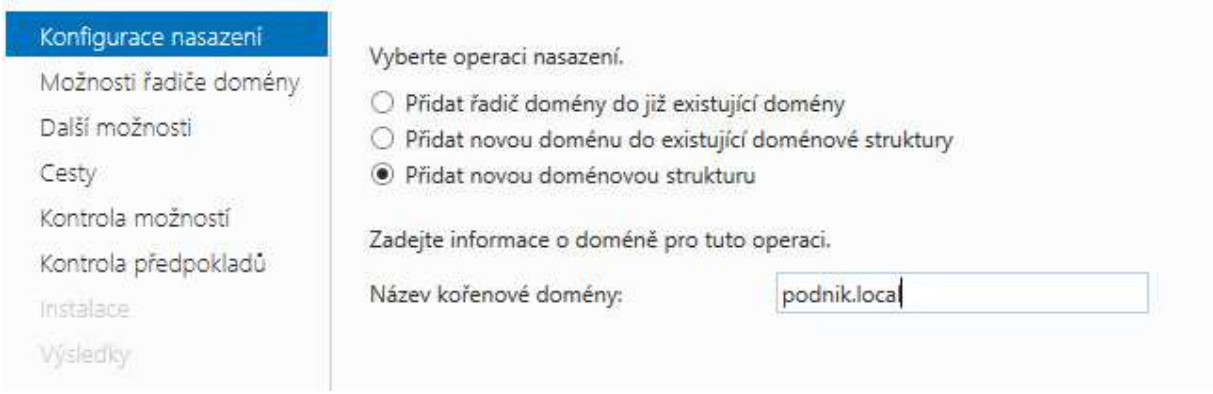
4.2.3 Instalace Active Directory

Po instalaci serverů přišla na řadu instalace samotné Active Directory. Ve správci serveru se vybrala možnost **Přidat role a funkce** a vybrala se možnost **Služba Active Directory Domain Service**.



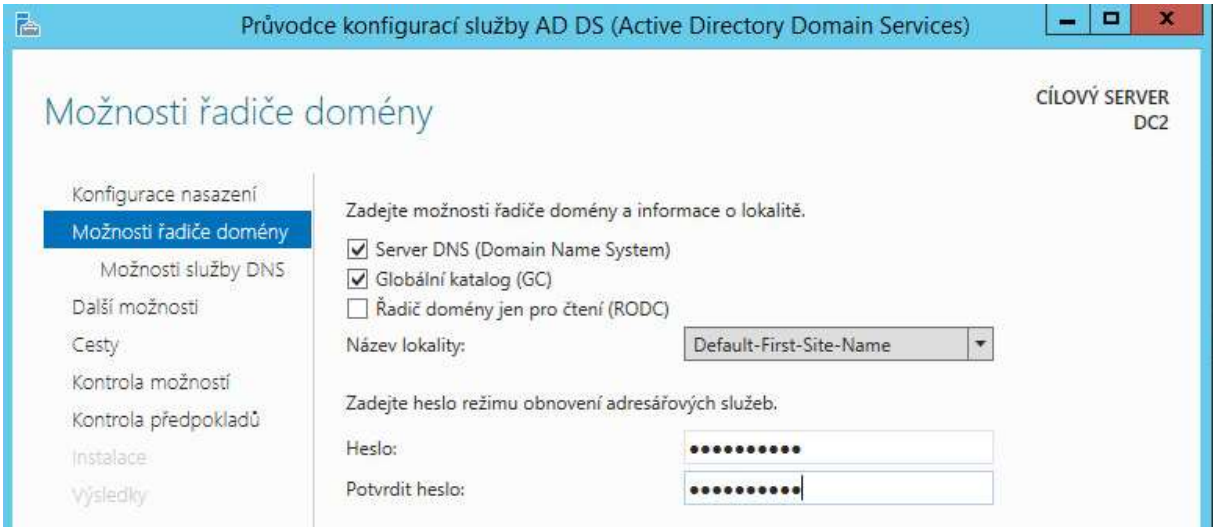
Obrázek 30 Instalace služby Active Directory [zdroj: autor]

Po instalaci Active Directory bylo nutné vytvořit doménovou strukturu. Vzhledem k tomu, že se jednalo o instalaci prvního doménového řadiče v doménové prostředí, vybrala se možnost **Přidat novou doménovou strukturu** a zadal se název kořenové domény. V dalším kroku se nastavilo heslo pro obnovení adresářových služeb pro případ, že bude nutné Active Directory obnovit ze zálohy.



Obrázek 31 Vytvoření domény podnik.local [zdroj: autor]

Poté se následující dialog jen potvrdil a tím vznikla doména **podnik.local**. Vznik samostatné domény však ještě nic neznamená. Dalším krokem bylo připojení druhého doménového řadiče do domény. Na druhém serveru se nejprve provedla instalace služby Active Directory. Poté se při konfiguraci vybrala možnost **Přidat řadič domény do již existující** a zadaly se údaje doménového administrátora. Dále se jen nastavilo, zda server bude doménový řadič jen ke čtení, či standardní doménový řadič a nastavilo se heslo pro režim obnovení adresářových služeb, které je potřeba při obnově Active Directory.Heslo bylo nastaveno stejně jako u prvního doménového řadiče.



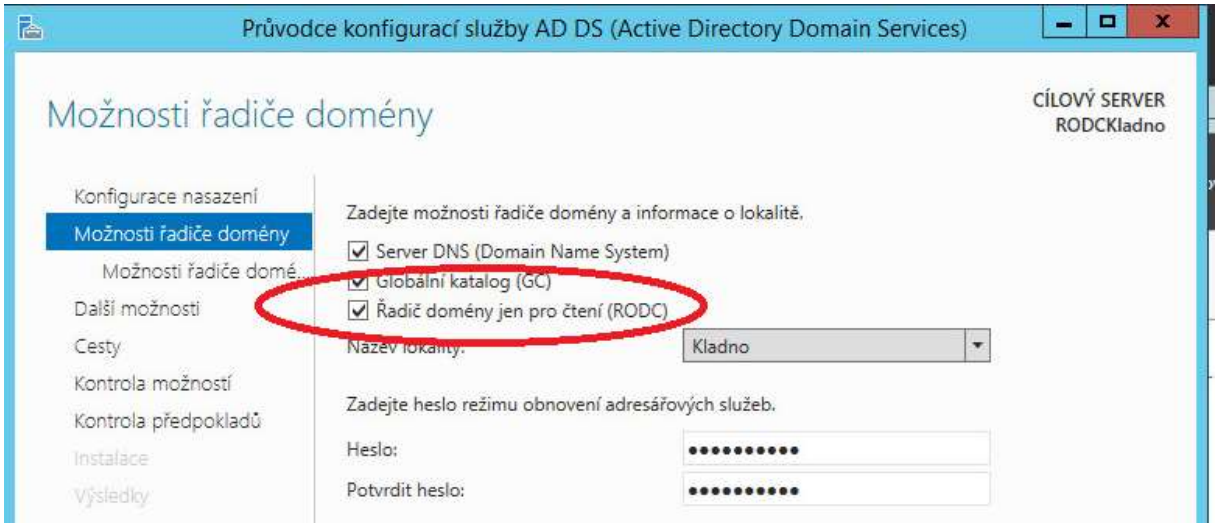
Obrázek 32 Instalace 2. doménového řadiče [zdroj: autor]

Dále už se jen vybrala možnost, odkud budu chtít replikovat, kde jsem zvolil možnost z libovolného doménového řadiče (v dané době existoval jen jeden). Poté nastal proces replikace z prvního doménového řadiče. Po skončení již oba doménové řadiče sdílejí

stejnou databázi Active Directory a jakékoliv změny na jednom z řadičů se automaticky replikují i na druhý.

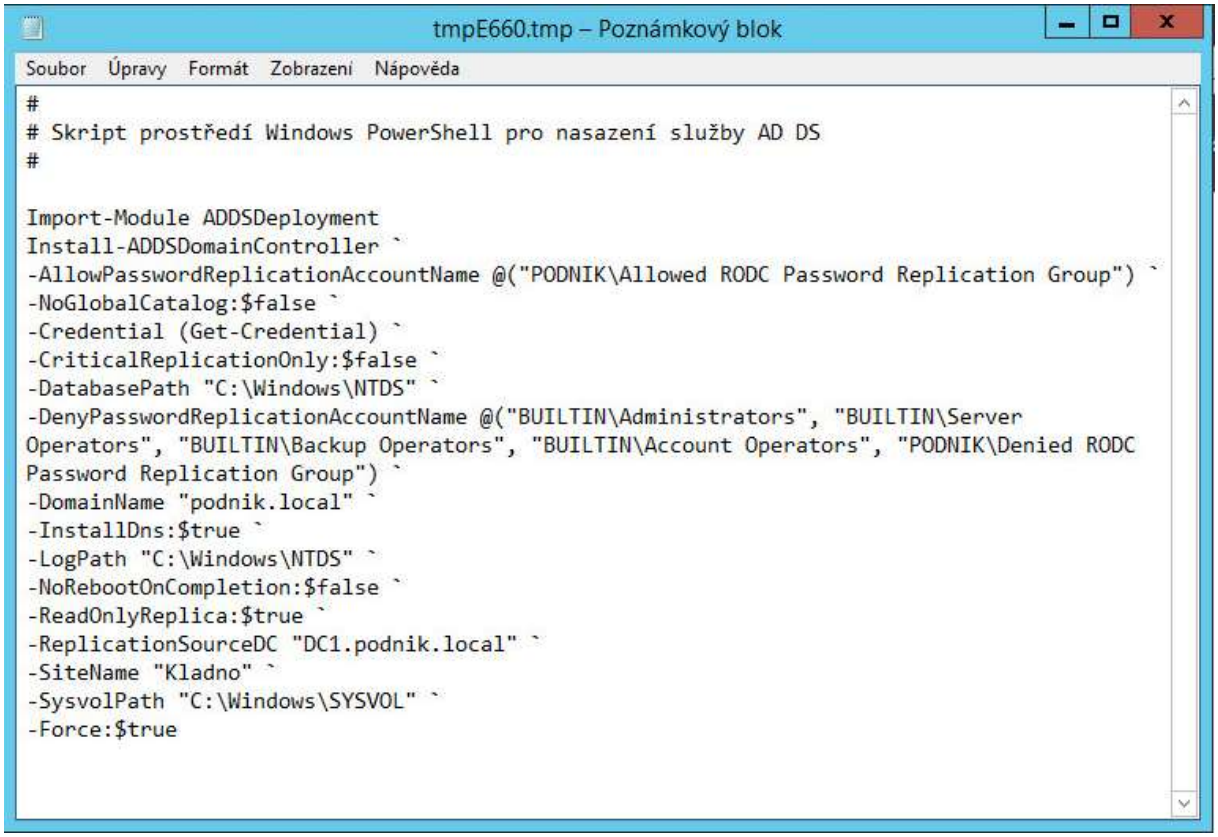
Výsledkem je tedy vytvoření domény podnik.local která prozatím obsahuje 2 doménové řadiče (DC1.podnik.local a DC2.podnik.local).

Posledním server, který na který byla instalována služba Active Directory, se nacházel na pobočce v Kladně. Tento server bude obsahovat databázi Active Directory jen pro čtení. Průběh instalace se moc nelišil od instalace standardního doménového řadiče, jen se při volbě **Možnosti řadiče domény** zaškrtla volba **Řadič domény jen pro čtení (RODC).** Následoval výběr replikačního partnera (zvolil jsem DC1.podnik.lokal). Služba se nainstalovala a zreplikovala obsah aktuální Ative Directory databáze na svůj disk. Tato replikace ovšem v základním nastavení neobsahuje hesla uživatelů.



Obrázek 33 Instalace Řadiče domény jen pro čtení [zdroj: autor]

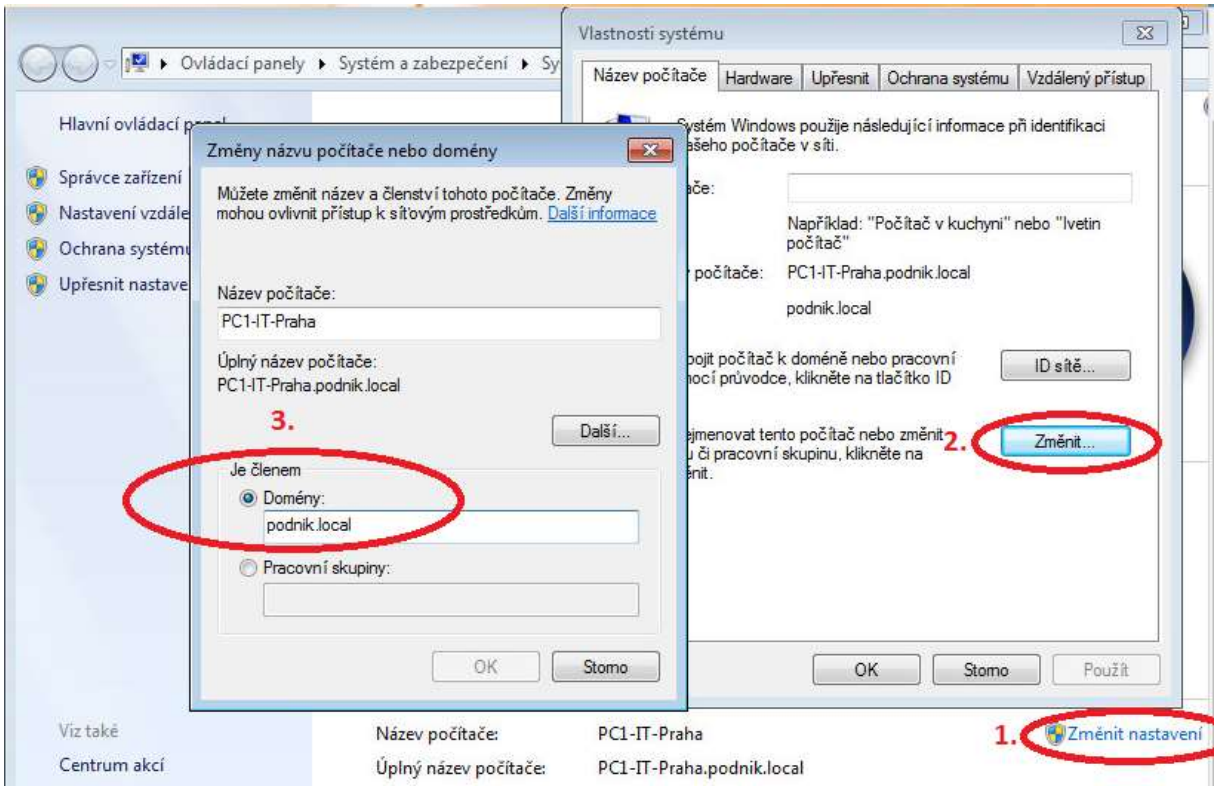
Při každé instalaci rolí (zde Active Directory Domain Services) má administrátor možnost vytvořit z aktuální instalace Powershell skript, kterým je možné provést stejnou instalaci role na další servery. Pokud tedy instalujeme více serverů, je vhodné využít tento skript k urychlení práce, neboť ve vygenerovaném skriptu stačí upravit proměnné položky (jméno serveru, replikační partner, lokalita) dle potřeby a skript spustit na dalším serveru. Příklad takového skriptu, který vytvoří doménový řadič pouze pro čtení je zobrazen na následujícím obrázku:



Obrázek 34 Powershell skript pro vytvoření RODC [zdroj: autor]

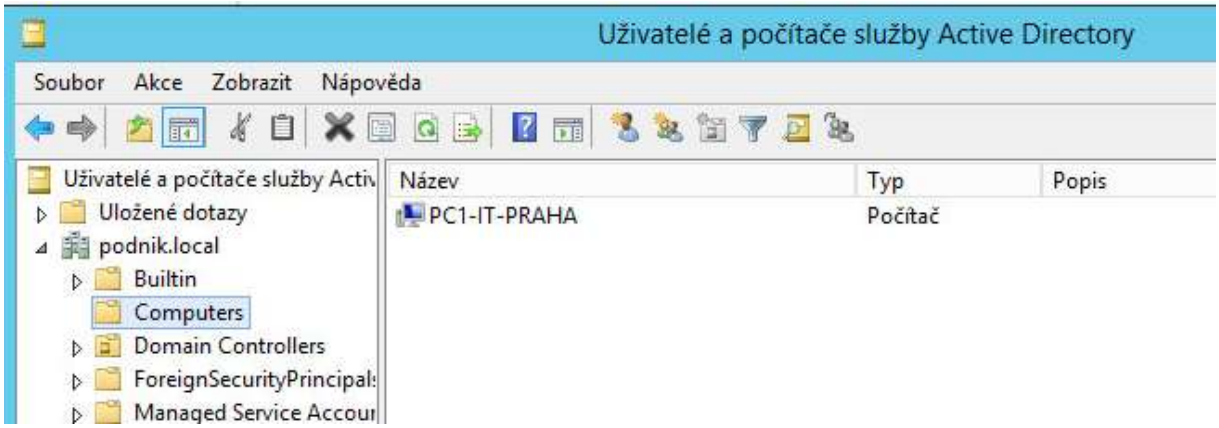
4.2.4 Instalace klientských stanic

Pro instalaci klientských stanic byl na základě požadavků firmy vybrán operační systém Windows 7 Profesional x64. Po instalaci bylo provedeno přiřazení počítače do domény **podnik.local.** Každý počítač byl manuálně přidán do domény **podnik.local.** Přidání se provádí na kartě Systém (na kartu se dostaneme, pokud pravým tlačítkem klikneme na ikonu **Počítač** v nabídce Start a vybereme **Vlastnosti**). Na kartě Název počítače klikneme na tlačítko Změnit a zde vybereme přepínač: Je členem **Domény**. Dále již jen napíšeme název připojované domény a vyplníme pověření účtu, který může přidávat počítače do domény. K tomu, aby mohl uživatel přidávat počítače do domény, musí být doménový administrátor nebo členem skupiny Account Operators.



Obrázek 35 Připojení počítače do domény [zdroj: autor]

Dále je nutné jen restartovat počítač a po restartu ho již můžeme spravovat pomocí Active Directory. Standardně se počítač objeví v kontejneru Computers v části Uživatelé a počítače služby Active Directory. Odtud ho následně přesuneme do požadované organizační jednotky.

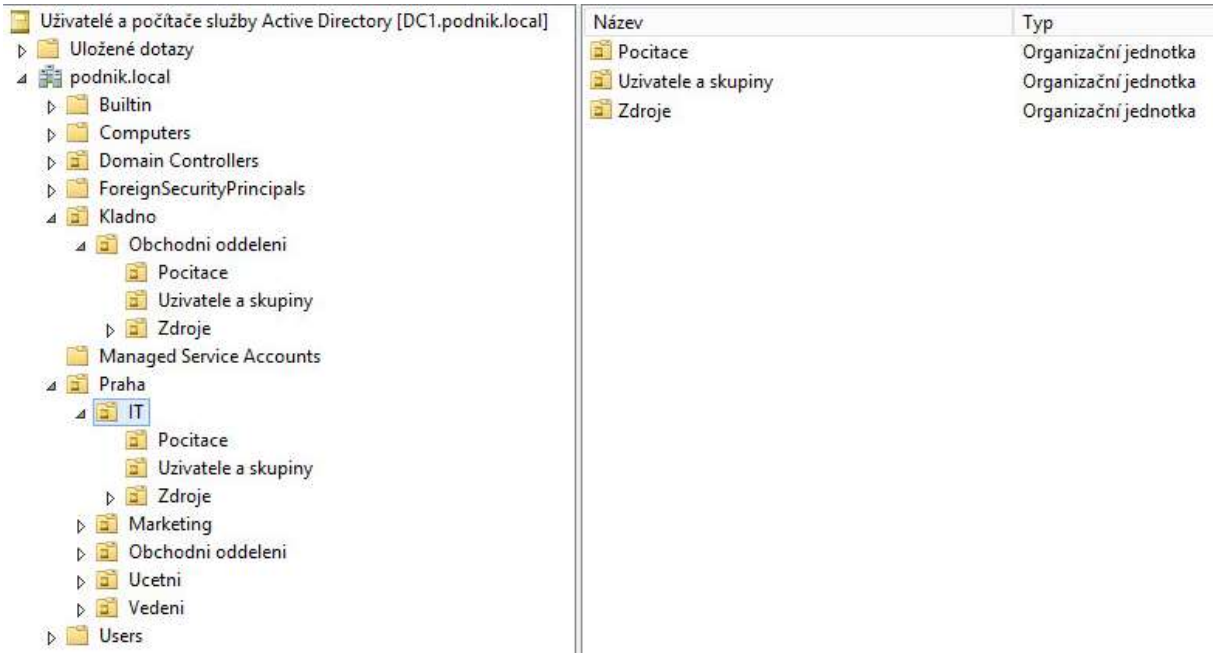


Obrázek 36 Nově vložené PC do Active Directory [zdroj: autor]

Takto jsem postupoval se všemi počítači a přidal je tak do domény. V mém případě se jednalo o 5 počítačů. V prostředí reálné firmy by se přidávání nových počítačů mohlo řešit předpřipraveným imagem, který by už obsahoval připojení do domény[43].

4.2.5 Nastavení Active Directory

Po instalaci jsem v Active Directory vytvořil strukturu organizačních jednotek dle návrhu uvedeném v kapitole 4.2.1 této práce. Vytvoření probíhalo v konzoli **Uživatelé a počítače služby Active Directory**. Výsledek této práce je vidět na následujícím obrázku:

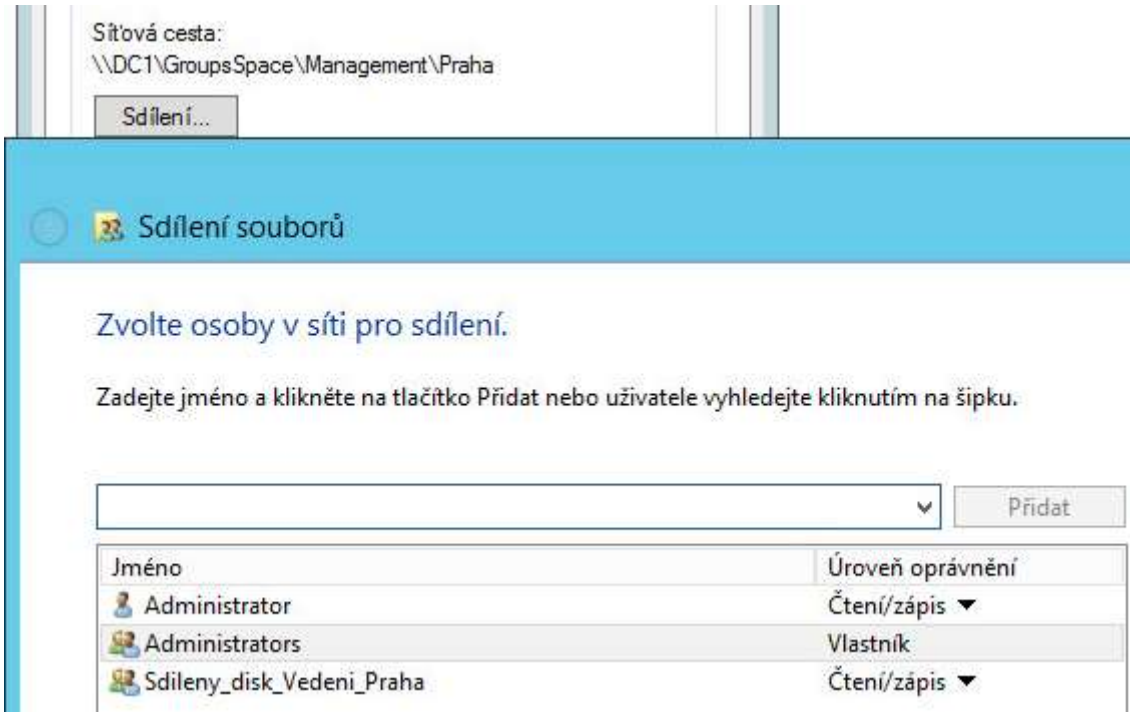


Obrázek 37 Vytvořená struktura OU pro firmu podnik.local

Poté bylo v Active Directory vytvořeno 12 skupin. Každé oddělení mělo svou skupinu označenou **GROUP_XXXX_lokalita**[44], která bude obsahovat všechny členy daného oddělení a zároveň byla vytvořena pro každé oddělení skupina **Sdilený_disk_XXXX_lokalita**[45] pro přístup k sdílenému síťovému disku.

[43] http://technet.microsoft.com/cs-cz/library/cc732280(v=ws.10).aspx
[44] kde **XXXX** označuje název oddělení a **lokalita** umístění
[45] kde **XXXX** označuje název oddělení a **lokalita** umístění

Přístup k síťovým zdrojům je lepší též řešit přes samostatnou skupinu. Výhoda je, že pokud později nutně potřebujeme dohledat, zda má konkrétní uživatel přístup k danému síťovému zdroji, stačí nám prozkoumat pouze jednu skupinu.



Obrázek 38 Nastavení přístupu k síťovým zdrojům pro oddělení Vedení[zdroj: autor]

Dále byli vytvořeni jednotliví uživatelé. Podnik poskytl seznam svých pracovníků ve formátu CSV[46]. Seznam obsahoval pro každého uživatele 3 informace – jméno, příjmení a oddělení, ve kterém pracovník pracuje. Pro dávkové vytvoření uživatelů jsem vytvořil Powershell skript[47], který vytvoří uživatele, nastaví mu defaultní heslo „Heslo12345“, které si bude muset při prvním přihlášení změnit, podle oddělení ho přiřadí do konkrétní organizační jednotky a přiřadí mu domovský adresář na souborovém serveru. Tento adresář se bude uživateli automaticky mapovat při každém přihlášení jako disk H:/. Na konci skriptu dojde k přiřazení uživatele do konkrétní skupiny opět dle oddělení. Skupiny GROUP_xxxx_lokalita obsahují po provedení skriptu uživatele jednotlivých oddělení. Pokud máme všechny

[46] http://tools.ietf.org/html/rfc4180
[47] http://letitknow.wordpress.com/2013/04/03/create-active-directory-users-with-powershell/

uživatele z oddělení v jedné skupině, lze určitá dále přiřazovat práva dané skupině a zpřehlední se tím správa pověření.

```
$csvcontent = Import-CSV -Path c:\user.csv
foreach ($user in $csvcontent){

New-ADUser -AccountPassword (ConvertTo-SecureString "Heslo12345" -AsPlainText -Force) `
           -ChangePasswordAtLogon $true `
           -Company "Podnik.local s.r.o" `
           -DisplayName ($user.Firstname+" "+$user.Lastname) `
           -Enabled $true -Name ($user.Firstname+" "+$user.Lastname) `
           -SamAccountName $user.Lastname `
           -givenname $user.Firstname `
           -surname $user.Lastname `
           -userprincipalname ($user.Lastname + "@podnik.local") `
           -Path ("OU=Uzivatele a skupiny,OU="+$user.oddeleni+",OU=Praha,DC=podnik,DC=local") `
           -HomeDrive "H" `
           -HomeDirectory ("\\DC1\HomeUsers\"+$user.Lastname)

switch($user.oddeleni){

      IT{ Add-ADGroupMember -Identity GROUP_IT_Praha -Members $user.Lastname }

      Marketing{ Add-ADGroupMember -Identity GROUP_Marketing_Praha -Members $user.Lastname }

     "Obchodni oddeleni"{Add-ADGroupMember -Identity GROUP_Obchodni_Oddeleni_Praha -Members $user.Lastname}

      Vedeni{Add-ADGroupMember -Identity GROUP_Vedeni_Praha -Members $user.Lastname }

      Ucetni{ Add-ADGroupMember -Identity GROUP_Ucetni_Praha -Members $user.Lastname }
                }
    }
```

Obrázek 39 Powershell skript na hromadný import uživatelů [zdroj: autor]

Daný skript jsem spustit na doménovém řadiči DC1 a soubor s uživateli (user.csv) nahrál na C:/. Po provedení skriptu byly vytvořeni uživatelé pro pobočku v Praze. Obdobně jsem vytvořil uživatele i pro pobočku v Kladně. Jediný rozdíl ve skriptu pro uživatele v Kladně byl v tom, že jejich domovský adresář se nacházel na serveru v Kladně a nikoli v Praze.

Po vytvoření uživatelských skupin a uživatelů byly vytvořeny síťové tiskárny. K tomu, abychom mohli vytvářet síťové tiskárny, bylo nejprve nutné na serveru přidat roli **Tiskový server**. Po přidání jsem vytvořil v modulu **Správa tisku** síťové tiskárny. Pro Prahu jsem vytvořil tiskový server na serveru DC1 a pro Kladno na RODCKladno. Oprávnění tisknout na jednotlivých tiskárnách zobrazuje následující tabulka:

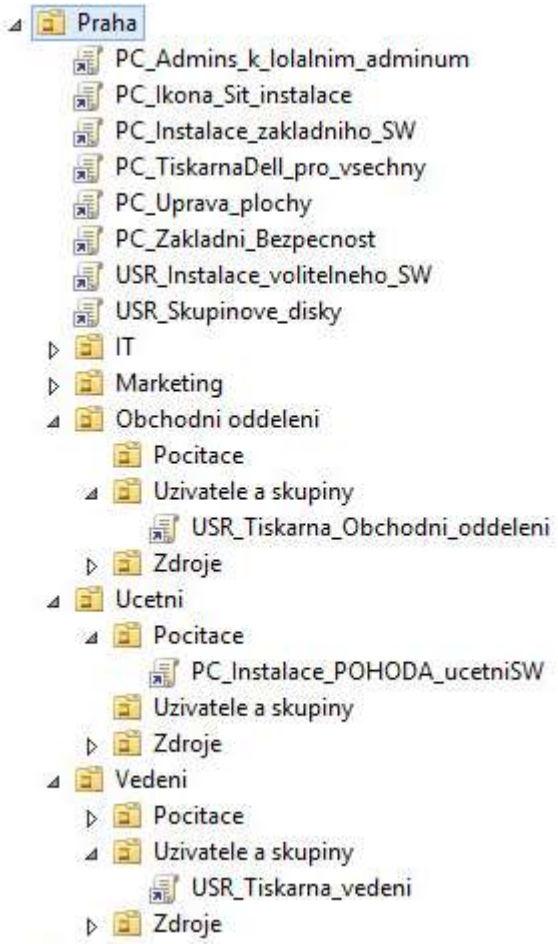
Tiskárna	Kdo může tisknout
Dell 3130	všichni
Kyocera FS1061	GROUP_Vedení_Praha
Xerox ColorQube 9300	GROUP_Obchodni_oddeleni_Praha
Dell 2145cn Color Laser	GROUP_Obchodni_oddeleni_Kladno

Tabulka 6 Oprávnění k tisku dle tiskáren [zdroj: autor]

Pro automatickou instalaci tiskáren do počítačů pro konkrétní uživatele jsem využil skupinové politiky. Přesný způsob bude vysvětlen v následující kapitole.

4.2.6 Nastavení skupinových politik

Skupinové politiky jsem využil k provedení konkrétních nastavení v oblastech bezpečnosti, nasazení tiskáren, instalaci softwarových balíčků a automatickému mapování síťových disků. V této kapitole rozeberu jednotlivě vytvořené skupinové politiky. Částečný seznam aplikovaných politik je zobrazen na následujícím obrázku:



Obrázek 40 Vybrané aplikované skupinové politiky

- Základní bezpečnost

Politika **PC_Pozadavky_na_hesla,** aplikovaná na celou doménu, definuje požadavky na složitost hesel pro uživatele, definuje délku platnosti hesla a určuje, kolik hesel si bude systém uchovávat v paměti.

Zásady účtu/Zásada hesel

Zásady	Nastavení
Heslo musí splňovat požadavky na složitost	Povoleno
Maximální stáří hesla	90 dní
Minimální délka hesla	5 znaků
Minimální stáří hesla	30 dní
Ukládat hesla pomocí reverzibilního šifrování	Zakázáno
Vynutit použití historie hesel	1 hesel zapamatováno

Obrázek 41 Nastavení politiky hesel [zdroj: autor]

Politika **PC_Admins_k_lokalnim_adminum** nám zajišťuje, že všichni členové skupiny Administrators jsou zároveň také lokálními administrátory na všech počítačích ve společnosti.

Politika **PC_Zakladni_bezpecnost** obsahuje souhrn politik, které představují základní nastavení bezpečnostních politik v podniku. V mém případě politika definuje nastavení uzamknutí počítače po 5 neúspěšných pokusech o přihlášení na dobu 30 minut. Dále určuje zákaz ukládání uživatelských hesel do mezipaměti[48], nastavuje bránu Firewall a určuje, které EXE soubory nebude možné spouštět.

Systém skrýt

Zásady	Nastavení	Komentář
Nespouštět určené aplikace systému Windows	Povoleno	

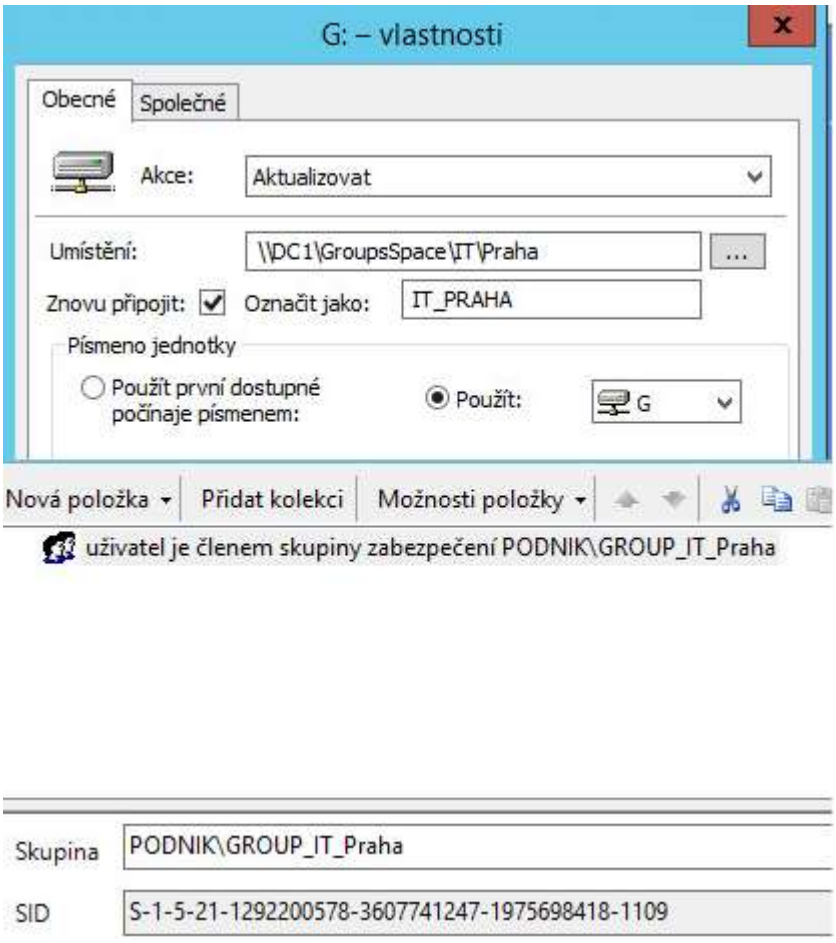
Seznam zakázaných aplikací
skype.exe
miranda32.exe

Obrázek 42 Zakázané aplikace [zdroj: autor]

[48] Tyto údaje je možné z počítače získat a poté využít pro prolomení uživatelského hesla.

- Mapování sítových disků

Tato politika (**USR_Skupinove_disky**) mapuje síťový disk pro uživatele jednotlivých oddělení. Každý uživatel, který patří do konkrétního oddělení tak má přístup k disku pro sdílenou práci v rámci daného oddělení. Disk se uživateli zobrazí automaticky po přihlášení jako disk G:\. Příklad mapování pro uživatel v IT oddělení v Praze zobrazuje následující obrázek. Při mapování je využito cíleného mapování na uživatele ve skupině GROUP_IT_Praha. Tímto způsobem bylo provedeno mapování pro všechny oddělení ve společnosti.



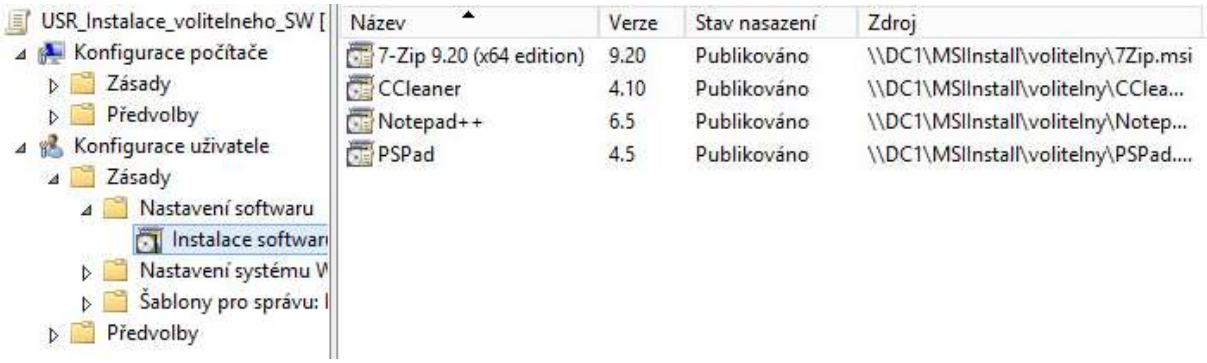
Obrázek 43 Mapování disku G:\ pro IT Praha [zdroj: autor]

- Tiskárny

Tiskárny jsou instalovány na koncové stanice 4 politikami. První politika **PC_TiskarnaDell_pro_vsechny** aplikovaná na organizační jednotku Praha zajistí distribuci této tiskárny na všechny počítače v lokalitě Praha. Výsledkem tedy bude skutečnost, že každý uživatel uvidí po přihlášení tuto tiskárnu v nabídce **Zařízení a tiskárny**. Politika **USR_Tiskarna_Obchodni_oddeleni** přidá do nabídky **Zařízení a tiskárny** další tiskárnu, ale jen pro uživatele patřící do obchodního oddělení v Praze. To samé provede politika **USR_Tiskarna_vedeni**, která přidá tiskárnu Kyocera FS1061 pro vedení společnosti. Politika **PC_Kladno_Tiskarna_Obchodni_oddeleni** přidá tiskárnu pro obchodní oddělení v kladenské pobočce.

- Instalace softwaru

Instalaci softwaru jsem rozdělil do 3 politik. První (**PC_Instalace_zakladniho_SW**), která instaluje základní požadovaný software (LibreOffice a Foxit PDF reader), druhá (**USR_Instalace_volitelneho_SW**), která umožňuje uživatelům si nainstalovat volitelně další software (7-Zip, Notepad++, CCleaner, PSPad) a třetí (**PC_Instalace_PohodaSW**), která instaluje účetní software Pohoda jen pro účetní oddělení.



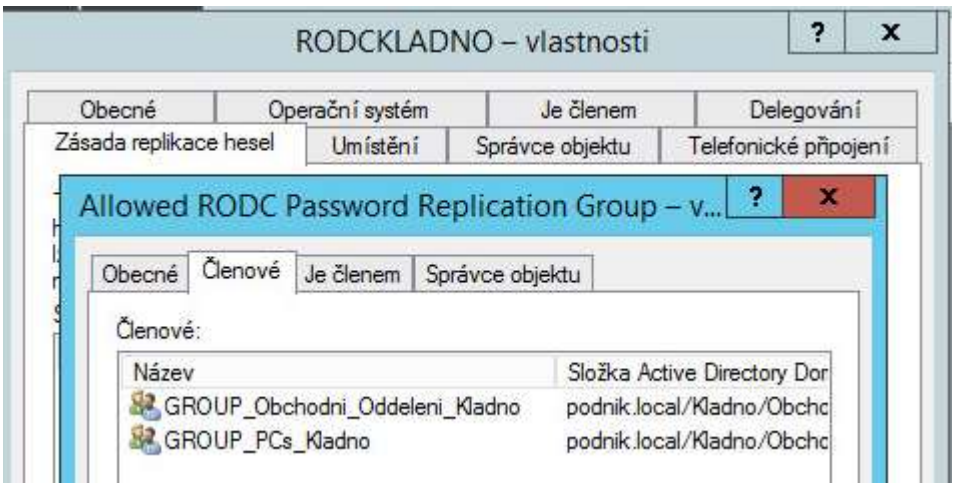
Obrázek 44 skupinová politika Instalace volitelného SW [zdroj: autor]

Další politika **PC_Ikona_sit_instalace** přidá na plochu ikonu, odkud si uživatelé mohou volitelný software instalovat.

Skupinové politiky umožnují instalovat software jen pokud je instalační soubor typu MSI[49]. Pokud jsou některé instalátory programů dostupné pouze v klasickém EXE formátu, je možné pomocí speciálních nástrojů (AdminStudio, Advanced Installer aj.) vytvořit z klasických EXE souborů MSI soubory. Výhodou MSI souborů je fakt, že je možné upravit instalátor pro potřeby konkrétního podniku.

4.2.7 Nastavení doménového řadiče jen pro čtení (RODC)

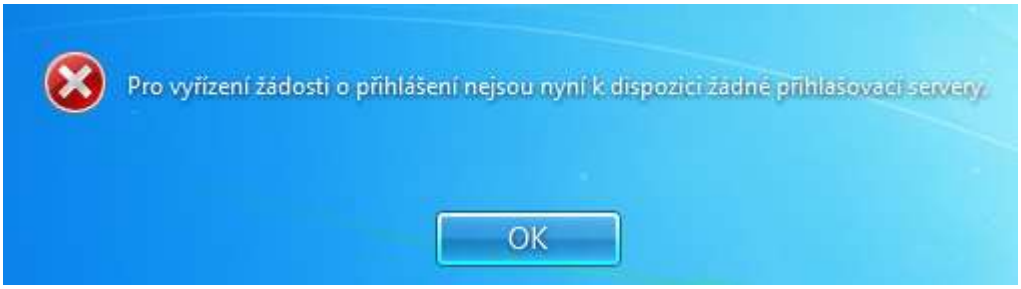
Proces instalace doménového řadiče jen pro čtení se až na jedno zaškrtnutí neodlišoval od instalace standardního doménového řadiče. Vlastním nastavení doménového řadiče jen pro čtení je činnost, kdy je potřeba tomuto doménovému řadiči dát seznam uživatelů, o kterých si bude moci uchovávat hesla a tedy bude mít možnost je i v případě nedostupnosti standardního doménového řadiče ověřit. Natavení se provádí v konzoli **Uživatelé a skupiny služby Active Directory** ve vlastnostech daného doménového řadič. Přidal jsem zde tedy skupinu GROUP_Obchodni_Oddeleni_Kladno, která obsahuje všechny uživatele z kladenské pobočky. Zároveň jsem přidal i skupinu GROUP_PCs_Kladno, která obsahuje všechny počítačové účty počítačů umístěných v kladenské pobočce, neboť každý účet počítače má také své heslo a při přihlášení uživatele v doméně se ověřuje i heslo účtu počítače. Nastavení RODC pro pobočku v Kladně tedy vypadalo následovně:



Obrázek 45 Nastavení RODC v Kladně [zdroj: autor]

[49] http://technet.microsoft.com/en-us/library/cc978328.aspx

Funkčnost jsem vyzkoušel tak, že jsem odpojil síťové rozhraní doménovým řadičům DC1 a DC2 a z počítače, jenž je členem skupiny GROUP_PCs_Kladno jsem se pokusil autentizovat. Nejprve jsem zkusil přihlášení pod uživatelem z pobočky v Praze. Toto přihlášení se nezdařilo. Viz následující obrázek:



Obrázek 46 RODC nepovoleny uživatel [zdroj: autor]

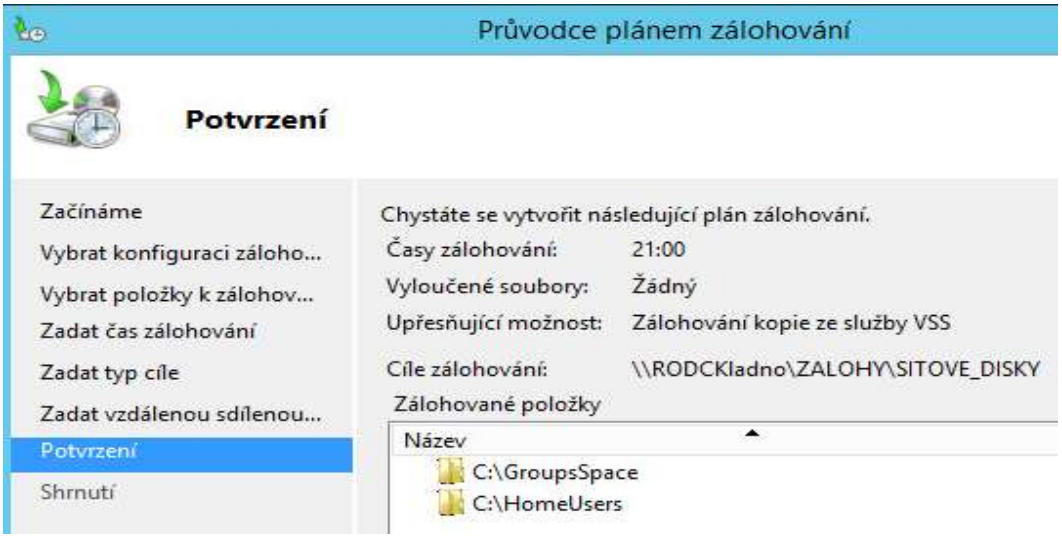
Následně jsem se zkusil přihlásit pod uživatelským účtem, který je členem skupiny GROUP_Obchodní_oddeleni_Kladno. V tomto případě se vše povedlo v pořádku, došlo k ověření uživatelského jména a hesla uloženého na řadiči RODCKladno a uživatel tak mohl s počítačem normálně pracovat.

4.2.8 Nastavení zálohování

Zálohování síťových disků, osobních složek uživatelů a doménových řadičů bylo provedeno nástrojem **Zálohování serveru** (wbadmin), který je dostupný jako jedna z funkcí Windows Serveru 2012 R2. Samotné zálohování jsem rozdělil do 2 činností:

- Záloha síťových disků, osobních složek uživatelů prováděná denně po pracovní době
- Záloha doménového řadiče Active Directory prováděná 1x měsíčně

Při zálohování síťových disků byla zvolena možnost zálohovat do sdílené síťové složky. Nevýhodou této možnosti je, že každá záloha automaticky přepisuje tu předchozí a tudíž je záloha vždy dostupná jen jeden den zpátky v čase. Tuto možnost jsem zvolil, jelikož jsem ve virtuálním prostředí neměl samostatný pevný disk nebo volný diskový svazek, na který bych mohl zálohovat. V reálné situaci bych si na zálohy vyhradil samostatný disk nebo diskové pole. Následující obrázek zobrazuje plán nastavení záloh pro sdílené složky a domovské adresáře uživatelů.



Obrázek 47 Zálohováni sdílených složek [zdroj: autor]

Zálohování doménového řadiče probíhá zálohováním stavu systému v konkrétním čase. Protože máme jen jedno doménové prostředí, stačí nám zálohovat jeden doménový řadič. V mém případě jsem zvolil zálohu doménového řadiče DC1. V nástroji **Zálohování serveru** jsem provedl zálohu celého stavu systému doménového řadiče na sdílené uložiště. V praxi by se opět zálohovalo na vyčleněný disk, popřípadě diskové pole.

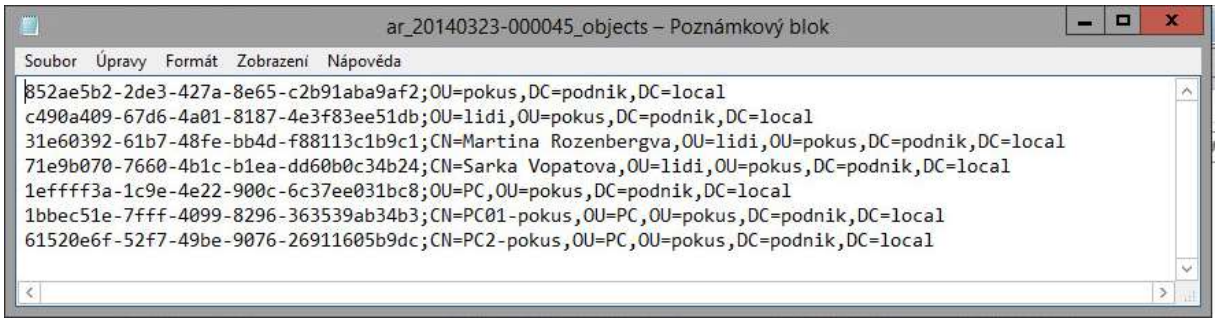
4.2.9 Autoritativní obnova doménového řadiče

Provedl jsem simulaci autoritativní obnovy databáze Active Directory ze zálohy. V praxi se může jednat o případ, kdy někdo náhodně smaže objekty v Active Directory a zároveň je jeho úroveň funkčnosti doménové struktury nižší než Windows Server 2008 R2 a tudíž nemůže využít funkci odpadkového koše.

Nejprve jsem vytvořil strukturu organizačních jednotek, které budou později „omylem smazané“. Poté jsem provedl zálohu stavu systému na doménovém řadiči DC2 pomocí nástroje **Zálohování serveru**. Následovalo smazání vytvořených objektů a provedení autoritativní obnovy. Samotná obnova se prováděla v **Režimu oprav adresářových služeb**. Obnovil jsem stav systému ze zálohy a poté jsem pomocí utility **ntdsutil** označil „omylem smazané“ objekty jako autoritativní, takže se při další replikaci nesmažou a naopak se

zreplikují na všechny doménové řadiče v doméně. Celý proces obnovy trval 15 minut (záloha stavu sytému měla 10GB). V případě, že je záloha větší, bude i obnova trvat déle.

Po vytvoření autoritativní obnovy byl vytvořen log, který obsahoval seznam objektů, u kterých došlo k autoritativní obnově. Log z mé obnovy zobrazuje obnovu 7 objektů.



Obrázek 48 Log z autoritativní obnovy objektů v AD [zdroj: autor]

5 Výsledky a doporučení

V souladu se zadáním byla nejprve nastudována daná problematika. Dále byla představena služba Active Directory jako nástroj pro správu počítačové sítě v podniku. Výsledkem práce byl vlastní návrh, implementace a konfigurace služby Active Directory dle požadavků na počítačové prostředí v podniku, které bylo požadováno vedením společnosti. Tato činnost se odehrávala ve virtuálním prostředí, kde měl autor k dispozici 3 virtuální servery a 5 virtuálních stanic, které představovaly uživatelské počítače.

Po instalaci operačního systému a role služby Active Directory na servery následovalo vytvoření podnikové domény a její struktury dle návrhu. Na základě teoretických poznatků, velikosti společnosti a doporučení byl pro tento podnik zvolen jedno doménový model Active Directory. Struktura organizačních jednotek byla navržena s ohledem na budoucí plánované rozšiřování poboček podniku. Byla zvolena kombinace geografického umístění a rozdělení podniku dle oddělení. Pokud by se společnost v budoucnu rozhodla přejít na jiný model řízení IT v podniku, bude možné změnit pouze strukturu organizačních jednotek a nebude se muset předělávat celé doménové prostředí.

Samotná konfigurace Active Directory zahrnovala několik částí – vytvoření uživatelů a skupin, počítačů, příprava a automatickou instalaci programů, zajištění základní bezpečnosti a tvorba zálohy a její prověření. V této části bylo provedeno vytvoření uživatelů na základě seznamu z podniku, připravení MSI balíčků k jednotlivým programům a pomocí skupinových politik nastavena jejich instalaci konkrétním uživatelům nebo počítačům. Základní bezpečnost byla opět provedena pomocí skupinových politik, kde byly vytvořeny požadavky na tvorbu hesla, zákaz ukládání hesel do mezi paměti počítačů, nastavena brána firewall a zákaz spouštění nežádoucích programů. Dále byly vytvořeny pravidelné zálohy síťových disků a také záloha doménového řadiče. Na závěr byla nasimulována možná katastrofa nechtěného smazání objektů v Active Directory a provedena autoritativní obnovu těchto objektů ze zálohy. Přínos této práce spočívá ve vytvoření počítačového prostředí, díky kterému je možné efektivně spravovat počítače a uživatelské účty spolu se síťovými zdroji v daném podniku.

Doporučení pro společnost by autor viděl v budoucím rozšíření bezpečnosti, kde by navrhl přihlašování uživatelů s využitím čipových karet a zavedení auditovaní v Active Directory. Další doporučení by viděl ve změně nastavení zálohování, kdy bylo z důvodu omezených zdrojů zálohováno na síťové uložiště. V praxi by doporučoval zálohovat na dedikované diskové pole, popřípadě na samostatné pevné disky.

6 Závěr

V úvodu diplomové práce je probrána služba Active Directory, která slouží ke správě podnikových sítí na platformě Microsoft Windows, kde pracuje s informacemi o podnikových uživatelích, počítačích a službách a zároveň umožňující uživatelům využívat sdílené síťové zdroje v podniku. Práce se zaměřuje na logickou i fyzickou architekturu této služby a zároveň na novinky, které přináší nejnovější verze operačního systému Windows Server 2012 R2. Poté se práce zabývá doménovým řadičem jako základním stavebním prvkem Active Directory. Je zde vysvětlena jeho činnost a jsou zde probrány FSMO role, které mají specifický význam pro správný chod celého Active Directory prostředí. Následuje kapitola zabývající se skupinovými politikami, které umožňují definovat a vynutit jednotné prostředí pro konkrétní uživatele a počítače, centrálně řídit nastavení počítačů, instalovat vzdáleně software a implementovat bezpečnostní politiku na jednotlivé počítače v podnikovém prostředí. V další kapitole je probrán postup replikací mezi doménovými řadiči jak v rámci jedné lokality, tak mezi jednotlivými lokalitami. Předposlední kapitola se zabývá způsoby zálohy a obnovy doménových řadičů a obnovou a přesunutím rolí, které jednotlivé řadiče mohou obsahovat. Závěr teoretické části se zabývá způsoby obecného návrhu domén a organizačních jednotek na základě fyzické struktury podniku a struktury IT oddělení v podniku.

Praktická část se zabývá návrhem a implementací Active Directory v konkrétním prostředí a na základě specifikovaných požadavků. Jsou zde využity znalosti získané z teoretické části této práce, které jsou aplikovány na konkrétní požadavky podniku. Celá praktická část je implementována ve virtuálním prostředí VMWare. Nejprve byl na základě struktury firmy a struktury IT oddělení proveden návrh struktury Active Directory. Následovala instalace operačního systému Windows Server 2012 R2 na servery a instalace operačního systému Windows 7 na klientské počítače. Po této činnosti byla provedena instalace služby Active Directory a její konfigurace. Vytvoření uživatelů bylo provedeno skriptem na základě dodaného seznamu uživatelů a jejich začlenění ve společnosti. Následovala konfigurace skupinových politik, které zajišťovaly přístup uživatelů k síťovým zdrojům, nastavení bezpečnostních politik na podnikových počítačích, instalace požadovaného softwaru a instalace síťových tiskáren. Na závěr praktické části bylo provedeno nastavení zálohování

síťových disků a provedena záloha doménového řadiče spolu s autoritativní obnovou Active Directory ze zálohy. Definované cíle diplomové práce byly splněny.

7 Citovaná literatura

1. **Stanek, William R.** ***Mistrovství v Microsoft Windows Server 2008.*** Brno : Computer Press, 2009. 978-80-251-2158-0.

2. **Stanek, William R.** ***Group policy - Zásady skupin ve Windows.*** Brno : Computer Press, 2010. 978-80-251-2920-3.

3. **Stan Reimer, Conan Kezema, Mike Mulcare, and Byron Wright with the Microsoft Active Directory Team.** ***Windows® Server 2008 Active Directory Resource Kit.*** Redmond : Microsoft Press, 2008. 9780735625150.

4. **Plíva, Michal.** ***Semestrální projekt na předmět Počítačové sítě.*** Praha : Michal Plíva, 2010.

5. **STANEK, William R, Joe RICBARDS, Robbie ALLEN a Alistair G LOWE-NORRIS.** ***Windows server 2008 inside out. 5th edition.*** Redmond, WA : Microsoft Press, 2008. 978-0735624382.

6. **DESMOND Brian, Joe RICBARDS, Robbie ALLEN a Alistair G LOWE-NORRIS.** ***Active Directory. 5th edition.*** Sebastopol : O'Reilly Media, 2013. 978-1-449-32002-7.

7. **Moskowitz, Jeremy.** ***Group policy - Fundamentals, Security and the Managed Desktop.*** Indianapolis : Wiley Publishing, 2010. 978-0-470-58185-8.

8. **Moser, Tom. Virtual Domain Controller Cloning in Windows Server 2012.** [Online] [Citace: 3. 10 2013.] http://blogs.technet.com/b/askpfeplat/archive/2012/10/01/virtual-domain-controller-cloning-in-windows-server-2012.aspx.

9. **Savill, John. www.windowsitpro.com.** [Online] [Citace: 07. 07 2013.] http://windowsitpro.com/windows-server-2012/directaccess-windows-server-2012.

10. **http://technet.microsoft.com.** [Online] [Citace: 15. 6 2013.] http://technet.microsoft.com/en-us/library/cc961781.aspx.

11. **http://technet.microsoft.com.** [Online] [Citace: 16.6 2013.] http://technet.microsoft.com/en-us/library/cc728010(v=ws.10).aspx.

12. **http://technet.microsoft.com.** [Online] [Citace: 16. 6 2013.] http://technet.microsoft.com/en-us/library/cc755994(v=WS.10).aspx.

13. **DAQUAS. Windows Server 2012 R2 – co je nového?** [Online] DAQUAS. [Citace: 13. 11 2013.] http://www.daquas.cz/articles/621-windows-server-2012-r2-co-je-noveho.

14**. Microsoft.** [Online] [Citace: 11. 13 2013.] http://technet.microsoft.com/en-US/library/dn280945.

15. **technet. What's New in Active Directory Domain Services.** [Online] [Citace: 12. 12 2013.] http://technet.microsoft.com/en-us/library/hh831477.aspx.

16**. DirectAccess. Wikipedie.** [Online] [Citace: 20. 12 2013.] http://cs.wikipedia.org/wiki/Directaccess.

17**. technet.** [Online] [Citace: 20. 1 2014.] http://technet.microsoft.com/en-us/library/cc787290(v=ws.10).aspx.

18. **Understanding active directory functional levels.** [Online] [Citace: 2. 2 2014.] http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(WS.10).aspx.

19. **Security Identifier.** [Online] [Citace: 5. 12 2013.] http://en.wikipedia.org/wiki/Security_Identifier.

20**. Microsoft Technet.** [Online] [Citace: 24. 1 2014.] http://technet.microsoft.com/cs-cz/library/cc784932(v=ws.10).aspx.

21. **Windows User Group. *WUG.*** [Online] [Citace: 2. 12 2013.] http://www.wug.cz/zaznamy/191-MS-Fest-2013-Praha-How-to-Hack-AD-Forest-from-a-Subdomain.

22. **CVS formát.** [Online] [Citace: 12. 2 2014.] http://tools.ietf.org/html/rfc4180.

23. **Powershell - hromadné vytvoření uživatelů .** [Online] [Citace: 2. 26 2014.] http://letitknow.wordpress.com/2013/04/03/create-active-directory-users-with-powershell/.

24**. Technet MSI soubory.** [Online] [Citace: 8. 3 2014.] http://technet.microsoft.com/en-us/library/cc978328.aspx .

8 Přílohy