Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Principy a možnosti využití Windows serveru 2012 R2

Bakalářská práce

Autor: Lenka Folprechtová
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Srpen 2016

Prohlášení:

Prohlašuji, že jsem bakalářskou/diplomovou práci zpracoval/zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 22.8.2016 Lenka Folprechtová

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D., za metodické vedení práce a cenné rady při zpracování této práce.

Anotace

Bakalářská práce se zaměřuje na oblast operačních systémů, konkrétně Windows Server 2012 R2. Popisuje metody používané v systému a rozdíly oproti starším verzím, věnuje se především Active Directory. V práci jsou vybrány a přesně popsány postupy pro používání operačního systému z pohledu uživatele, které pomáhají začínajícím správcům sítě, jak se starat o svou infrastrukturu. Jsou určené pro studijní účely, kompletní verze se bude využívat ve výuce, ale mohou posloužit i veřejnosti. Pomocí názorných obrázků a podrobných návodů jsou konfigurace jasně popsány a vyzkoušeny v praxi.

Annotation

Title: Usage of Windows server 2012 R2 and practices

The barchelor thesis focuses on the area of operating systems, particularly Windows Server 2012 R2. It describes used methods in the system, differences compared to previous versions and it is mainly focused on Active Directory. The thesis chooses and accurately describes procedures how to use the operating system from the user's perspective and how to help novice network administrators how to take care of its infrastructure. They are intended for educational purposes, the complete version will be used in the tuition, but they can also serve the public. The configurations are clearly described and tested in practice by illustrative images and detailed instructions.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Proces digitalizace ve dvacátém století přinesl v oblasti počítačů nové technické a technologické poznatky. Bez počítače si nedokážeme představit běžnou práci v kanceláři nebo v některých případech i každodenní život. Vývoj se posunul tak daleko, že už ani nemusíme sedat za robustní stolní počítače a na každém kroku s sebou můžeme mít vlastní notebook, netbook nebo tablet – svoji soukromou a osobní kancelář. Mikroprocesory (mozek počítače) dnes najdeme téměř v každém elektrickém zařízení. Nezapneme si bez nich televizi ani nenastartujeme auto, nevytiskneme dokument a nevypereme si.

Informační technologie je obor, ve kterém vše jde či přímo kvaltuje rychle dopředu. A jak se vyvíjí hardware, pozadu nezůstávají ani softwarové prostředky. Bez pokroku bychom se neobešli. Pokrok ale závisí na tom, že svoje dosavadní zkušenosti budeme předávat dalším generacím.

Vydání nového Windows Serveru 2012 R2 (dále už jen WS 2012 R2) byl dobrým námětem pro bakalářskou práci. Microsoft Windows je jedním z nejpoužívanějších operačních systémů na světě, ale i přesto nesmí výrobci zaspat dobu a musí pokračovat dál v aktualizacích a přitahování zákazníků. Čím více různorodých materiálů bude k tomuto tématu vypracováno, tím lépe se budou předávat informace, které jsou tak cenné pro jedince, kteří o ně stojí.

2 Cíl práce

Cílem práce je zaznamenat rozdíly mezi Windows serverem 2012 R2 a jeho staršími sourozenci a prostudovat výhody přechodu na nový server.

Bakalářská práce slouží k předávání zkušeností a jako učební a akademická pomůcka. Půjde hlavně o přebudování stávajících studijních materiálů pro předmět Operační systémy 1.

Nejdříve seznámím čtenáře s důležitými pojmy a principy Windows Serveru. Následně v praktické části bylo potřeba prozkoumat a analyzovat stávající materiály k předmětu Operační systémy 1, ukážu, jak byly vyzkoušeny na nové serverové verzi Windows a Windows 8.1.

Popíšu možnosti využití Windows Server 2012 R2 v prostředí podnikové sítě a jeho možnosti v reálném nasazení. V praktické části navrhnu a zrealizuji sadu základních a pokročilých modelových konfigurací. Dalším cílem je prohloubení znalostí o operačních systémech rodiny Microsoft Windows a zlepšení správcovských schopností, hlavně rolí Active Directory.

3 Microsoft Windows

Microsoft Corporation je celosvětově uznávaná firma zabývající se především výrobou a vývojem produktů z oblasti počítačů či aplikačních platforem. Byla založena na jaře v roce 1975 Billem Gatesem a Paulem Allenem.

Microsoft Windows je název pro skupinu operačních systémů s podobnými znaky. Nejznámější je nám modrá barva v logu nebo charakteristická „okna“, se kterými na počítači pracujeme. Microsoft vyvinul pro obyčejné operační systémy i jejich serverové verze, což jsou operační systémy přizpůsobené k práci za extrémního zatížení. Serverový systém je řízen centrálně s jednotnou správou a umožňuje vzdálený přístup přes síť. Potřebujeme profesionálního administrátora, který nám může zajistit, že systém bude naprosto spolehlivý a nepřetržitě v bezchybném provozu.

3.1 Operační systém

Operační systém je nedílnou součástí každého počítače. Je to jakási spojka mezi hardwarovým a softwarovým vybavením. Právě díky operačnímu systému (dále jen OS) dokážeme obsluhovat součásti počítače – procesory, operační paměti, vstupní a výstupní zařízení nebo soubory dat. Bez OS bychom měli pouze „holý počítač“, se kterým se běžní uživatelé moc neztotožňují a neumí na něm zadávat své zakázky (příkazy k provedení). Chybí jim k tomu příjemné uživatelské grafické prostředí, které by nemělo chybět žádnému dnešnímu OS, pokud chce dodavatelská firma prosperovat. OS nám pomáhá v práci, ale také poskytuje cestu k zábavě – přehrávání filmů, různé aplikace, hraní her a přístup k internetu.

OS řídí celý počítač a zjednodušuje efektivitu samotného využívání výpočetního systému. Jelikož jsou údaje naší firmy a zaměstnanců tak choulostivou informací, zajišťuje nám také vysokou bezpečnost před útoky zvenčí.

OS není pouze jeden, kvůli rozmanitosti poptávky jich na trhu najdeme nepřeberné množství od různých výrobců, kteří se předhánějí vydáváním stále nových verzí. Při výběru záleží na našich preferencích a prostředcích, které můžeme do infrastruktury společnosti vložit. Každý chce mít nejvyšší podíl na trhu

a toho dosáhne pouze novými možnostmi a vylepšeními. Mohou se lišit grafickým prostředím, využitím nebo výkonem.

Odnoží operačních systémů jsou operační systémy určené pro serverové počítače. Ty musí zvládnout provoz v extrémních podmínkách a být natolik robustní, aby dokázaly ovládat několik hostitelských stanic, které jsou na ně napojené. Dodavatelé musí předložit špičkové řešení, které nás nezklame a stabilně vydrží téměř nepřetržitý provoz.

3.2 Historie operačních systémů Microsoft Windows

První práce na prvním operačním systému od firmy Windows začaly v roce 1983. Na prvních počítačích byl pouze MS-DOS, až později dostal lepší grafické zpracování, když došlo k vydání Windows 1.0. Firmu ale s příjemnějšími podmínkami pro obyčejného uživatele předběhl Macintosh. Microsoft je dohnal až v roce 1990, jakmile se objevil Windows 3.0. (Kencki, 2010)

Dosáhli většího adresového prostoru a 16barevné prostředí, barevné hloubky. Verze 3.1 dokončila přechod na operační systémy s příjemným uživatelským rozhraním – skvěle podporovala multimédia, objevují se první verze Adobe Photoshop. Po několika dalších verzích, ve kterých se objevila i podpora pro OpenGL nebo pro souborový systém NTFS, v červnu 1998 se vydává Windows 98 s podporou DVD mechaniky a USB zařízení. A jen co se přehouplo milénium, na trh byl uveden Windows 2000. Objevuje se první remote desktop, podpora bezdrátových sítí a další. Někteří tento operační systém oslavují více než třeba Windows XP, který přišel o rok a půl později.

Základem pro serverové OS se stal Windows Server 2003, byl robustní a s propracovanou bezpečností. Přes dlouhou dobu vývoje se Windows Vista spíše nepovedl – spousta chyb a velká nestabilnost zařídila Microsoftu nemálo nespokojených recenzí. Reputaci si napravil až díky Windows 7, který podporoval více procesorů, snažil se o rychlejší start počítače a další. Windows 7 předhonil i držený rekord Windows XP o nejpoužívanější OS. Na řadu přišel už jen Windows 8, který updatoval na verzi 8.1 vracející se na některé osvědčenější způsoby práce z verzí minulých.

4 Windows 8.1

Instalací operačního systému uživatel získá také navíc různé aplikace a doplňky, které mu dobře poslouží v běžném ovládání nebo v kanceláři. Nabízí inovovaný grafický vzhled, kterému se říká Metro, a pokud nepočítáme jeho mobilní verze, je toto uživatelské rozhraní použito jako první právě ve Windows 8.1. Přesto si ale vzhled naší stanice můžeme uzpůsobit podle našich preferencí, aby se nám pracovalo co nejlépe.

Výrobci nám slibovali mnohonásobné zrychlení systému. Podle testování se slib ukázal jako splněný – start, přechod do hibernace a vypnutí systému probíhá téměř o polovinu rychleji než u předchůdce Windows 7. Zlepšení pocítí hlavně vlastníci počítačů s pevným diskem, se SSD už méně. Také grafický výkon se vylepšil, díky spolupráci Microsoft a výrobců s AMD a Nvidia – nemusíme se tedy bát poklesu, pokud pracujeme na stanici s programem, který potřebuje stejně tak kvalitní výkon (a lepší) jako na Windows 7.

5 Windows Server 2012 R2

WS 2012 je v pořadí již šesté vydání Windows Serveru. Je to serverová verze OS Windows 8. Vydání WS 2012 proběhlo 4. září 2012 a rok po něm 18. října 2013 přišel update na WS 2012 R2. Výrobci navíc zjednodušili migraci na novější verzi – Shared Nothing Live migrace umožňuje přenos virtuálu z hostitele WS 2012 na WS 2012 R2 bez nutnosti vypnout virtuální stroj (Kantůrek, 2013). Přechod tedy téměř nezaznamenáte a minulá infrastruktura sítě vám zůstane.

Přišli razantní změny v licenčních podmínkách oproti WS 2008 R2. Nový server přináší spoustu vylepšení ve správě, infrastruktury virtuálních klientských počítačů a jejich přístupu nebo ochrany dat a virtualizace jako takové.

Přechod na novější verzi OS provádíme co nejdříve, přestože se to snadněji řekne, než udělá. Samozřejmě že firma musí znát své prostředky a finanční možnosti. Vždy je ale dobré, když máme tu nejnovější verzi operačního systému, která nám nabízí uživatelům to nejlepší.

Při migraci přesouváme role a funkce a měníme doménové řadiče a odstraňujeme ty staré. Jen málo firem má to štěstí, že za celou svou existenci nemusí měnit svou doménovou strukturu.

5.1 Licenční podmínky a edice

Vývojáři z Microsoft snížili počet licencí (dříve bylo deset základních) na jednoduché čtyři – datacenter, standard, essentials a foundation. Je nutné správně zvážit, jak bude systém provozován a co ve firmě přesně potřebujeme, aby mu byla přidělena správná licence. Záleží na velikosti firmy a požadavky na virtualizaci a práci na cloudových úložištích.

- Datacenter – nabízí veškeré funkce Windows Serveru a neomezené množství virtuálních instancí, je to skvělé řešení pro obrovské společnosti, které potřebují bezchybný provoz, vyhoví požadavkům velkých firem a zvládá náročný provoz s mnoha pobočkami
- Standard – nabízí veškeré funkce Windows Serveru, ale jen dvě virtuální instance, nebo jednu fyzickou a jednu virtuální, identická edice jako datacenter, liší se pouze licenčně
- Essentials – pro společnosti se serverem, který nemá více než dva procesory, máme předem nakonfigurováno, jak jsme připojeni ke cloudovým službám, můžeme připojit k jednomu fyzickému počítači nebo jednoho virtuálního prostředí, limituje nás 25 uživatelských účtů
- Foundation – vydává se jako OEM licence a to pouze na počítače s jedním procesorem pro obecné účely, bez oprávnění na virtualizaci a jsme omezeni pouze 15 uživateli, hodí se tedy pro menší firmy

5.2 Hardwarové nároky

Tabulka 1 Hardwarové nároky WS 2012 R2

Komponenta	Minimální nároky	Doporučené nároky
Procesor	1.4 GHz	2 GHz a více
Paměť	512 MB RAM	2 GB RAM a více
Volné místo na disku	32 GB	40 GB a více
Optická mechanika	DVD-ROM	DVD-ROM
Obraz - monitor	Super VGA (800x600) monitor	XGA (1024x768) monitor

Zdroj: Poulton a Camardella, 2014

Není doporučeno instalovat operační systém na počítač s minimálními požadavky na paměť. Pokud totiž chcete plně využívat všechny služby a výhody určité edice, je lepší mít rezervu – minimální požadavky na konfiguraci se tak mohou lišit. Potřebujete více místa, jestliže instalujete systém přes síť, nebo když máte počítač s větší pamětí RAM (více jak 16 GB), bude operační systém vyžadovat místo na disku například kvůli hibernaci.

5.3 Novinky ve Windows Server 2012 R2

Ti, kdo čekají převratné a radikální změny, budou lehce zklamáni. WS 2012 R2 staví na pevných základech svých předchozích verzí, nicméně také přináší spoustu drobných změn v klíčových oblastech, které nám po sečtení dají nový robustnější a škálovatelný update operačního systému.

Inovován a rozšířen byl hlavně způsob organizace souborů a adresářů – souborový systém. Vývojáři se snaží o nejlepší způsob, jak spravovat naše data nebo jak snížit náklady na jejich uskladnění v diskové kapacitě. Jak na pevném disku, tak na vzdálené počítačové síti. Vydali se správným směrem, protože v poslední době množství uložených dat prudce narůstá a naopak ceny diskových úložišť rychle klesají. A Microsoft reaguje.

Resilient File System (RFS), je souborový systém tak houževnatý, jak napovídá jeho název. Byl vyvinut pro lepší integritu dat, což znamená, že ukládaná metadata má zkontrolována kontrolním výpočtem a zároveň je ukládá na dvě

místa v disku, takže se může kdykoli vrátit do konzistentního stavu. Současně tak, aby zajistil, že všechna uložená data, a to i velkých objemů, nebudou zatěžovat výkon počítače (škálovatelnost).

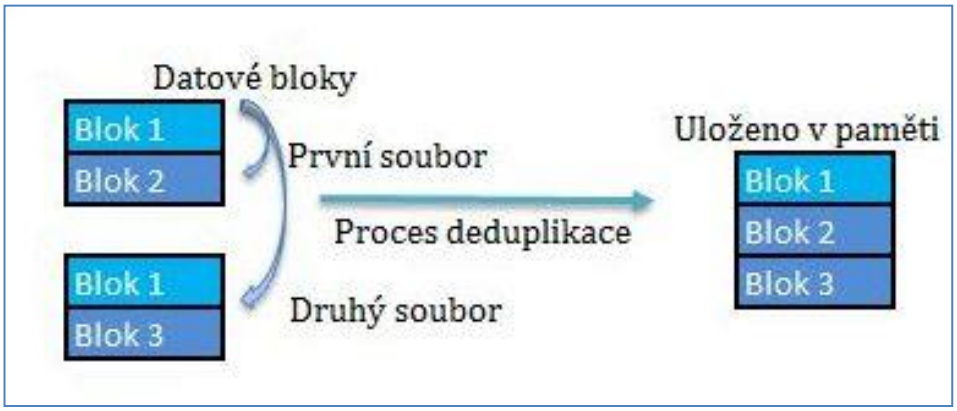
Je plně kompatibilní se starším NTFS, dokonce má většinu sémantických pravidel stejnou. Ale nemůžeme říct, že NTFS plně nahradí. Stále má plno nevýhod (př. nepodporuje deduplikaci a kompresi dat viz níže) a tak RFS nelze použít vždy.

V rámci bakalářské práce nelze předvést celý rozsah novinek a změn. Proto vypíši jen ty nejzásadnější a nejzajímavější.

5.3.1 Deduplikace dat

Tento způsob ukládání dat zajišťuje kompresi více stejných datových bloků do jednoho. Datové bloky jsou rozděleny tzv. chunkovacím algoritmem. Na tento blok je pak uložena v datové struktuře (ta se ukládá do samotného souboru) reference, podle které se dá snadno obnovit původní informace. Tím šetříme místo, protože na jeden blok může „ukazovat“ i více různých souborů. Deduplikace je součástí File Server role.

Dobře viditelné je to na obrázku.



Obr. 1: Proces deduplikace
Zdroj: vlastní zpracování

5.3.2 Sdílený adresový prostor

Cluster je logická jednotka v počítači, do které ukládáme soubory. Jakmile máme vše na jednom místě, snižuje se režie na správu dat, data jsou mnohem více chráněná, mizí problémy s fragmentací a celkově zvyšujeme efektivitu práce s daty.

Počítačový cluster seskupuje více počítačů, aby spolu mohly komunikovat a spolupracovat pomocí počítačové sítě. Tvoří tak jednotný systém, což zlepšuje práci výpočetního systému jednotlivých počítačů a jiné.

„Pokud chcete servery propojit do vysoce dostupného clusteru, potřebujete mezi nimi mít sdílené úložiště. Tento fakt v některých případech komplikoval využití clusteru ve virtuálním prostředí, kdy chcete použít cluster nad virtuálními stroji a zajistit tak vysokou dostupnost služeb jimi poskytovaných. I virtuálním strojům jste museli zpřístupnit sdílené fyzické diskové úložiště, což nebylo zcela optimální řešení. Tato starost s WS 2012 R2 odpadá, můžete totiž jednoduše vzít virtuální pevný disk s příponou .VHDX a zpřístupnit ho více virtuálním strojům najednou. Jednoduché a efektivní.“ (Kantůrek, 2013)

5.3.3 Microsoft VDI

Doba se stále zrychluje a zákazníci vyžadují, aby mohli pracovat odkudkoli a z jakéhokoli zařízení. Pro jejich největší komfort. Zároveň ale také musíme zajistit bezpečnost našich dat a myslet na administraci a správce celé infrastruktury. Microsoft Virtual Desktop Infrastructure (VDI) se posunul o spoustu vylepšení a nových věcí kupředu.

5.3.4 Storage Tiering

Abychom navýšili rychlost přístupu k datům, WS 2012 R2 umí rozlišit, která data používáme častěji než jiná. Bloky dat jsou rozlišeny podle toho, jak často se k nim přistupuje – s některými daty pracují aplikace intenzivně, kdežto jsou i data, která neotevřeme a nepřečteme třeba celý rok, přesto je pro budoucí použití potřebujeme zachovat (Hot data, Cold data). Častěji používaná data se ukládají na rychlé a kvalitní disky a ta méně častá na disky levnější. U disků se ukládá jaký je to typ disku (tzv. „tier“, rychlý či pomalý), podle kterého WS zjistí, kam a co uložit. (Microsoft TechNet, 2013)

5.3.5 SMB 3.0

Server Message Block (SMB) je protokol aplikační vrstvy, který nám dovoluje komunikovat po uzlech v síti a zajišťuje sdílený přístup k tiskárnám nebo souborům. Uvedu pouze pár novinek z celého výčtu.

SMB Multichannel zvyšuje propustnost sítě – využívá vícenásobné připojení k síti. Zvyšuje odolnost proti výpadkům, protože jakmile nefunguje jedna cesta, zpřístupní se další. Využívá celou šířku pásma, může posílat s vysokou rychlostí několik požadavků najednou. Sám také dynamicky vyhledává nové spoje a zařazuje je podle potřeby. (Microsoft TechNet, 2013)

SMB Transparent Failover dovoluje administrátorům provádět údržbu uzlů v počítačovém clusteru a jejich souborových úložišť, bez toho aniž by museli přerušovat serverovou aplikaci a ukládání na tato úložiště. Navíc když dojde k výpadku, uživatelé na určitém uzlu budou automaticky přesměrováni k ukládání na jiných uzlech. (Microsoft TechNet, 2013)

5.3.6 PowerShell

Přestože můžeme všechna nastavení systému provést klasicky přes uživatelské rozhraní, někdy si můžeme práci zjednodušit pomocí PowerShell. Mnohdy je i lepším řešením naučit se pár příkazů a využít toho. Je to v podstatě vylepšená příkazová řádka, která zvládne i zpracování skriptů.

Použijeme ho, pokud chceme na systém nahlédnout takříkajíc pod lupou. Některé příkazy a skripty dokáží náš problém či nastavení řešit podstatně rychlejší cestou, než kdybychom použili klasické uživatelské rozhraní.

5.4 Role a oprávnění k přístupu

K tomu, abychom si svoji práci zjednodušili, abychom používali přímočará a efektivní řešení, ušetřili čas a maximovali výsledky, slouží služba Active Directory. Je to způsob implementace naší databáze, jsou to služby, které nám pomáhají spravovat celou naši infrastrukturu a přístupy ke zdrojům přes síťové prostředky. Jakmile se naučíme s těmito prostředky pracovat, můžeme řídit tok informací ve

firmě z centrálního zdroje a učinit ji tak dostupnou pro celou naši infrastrukturu. Jako administrátorovi nám nabízí celé řešení, jak spravovat počítačovou síť. V té je mnoho objektů, které musíme spravovat a zajistit uživateli, že k nim bude mít spolehlivý přístup – například jsou to servery, aplikace, databáze nebo jiní uživatelé. Služba je od Microsoft a je i součástí WS 2012 R2 s několika novinkami. AD využívá protokol LDAP, Kerberos a DNS.

Data se v AD ukládají hierarchicky, podobně jako v souborových systémech a každý zápis je objektem. Ty mají mezi sebou vztahy, vztahy důvěry a mohou od sebe dědit. Vztahy důvěry a autentizace uživatelů je v AD velmi důležitá, jedna z nejrozsáhlejších částí.

Každý objekt má svoje jedinečné identifikační číslo GUID (Globally Unique Identifier). Ale 128bitové číslo není jednoduché si zapamatovat, držet ho v paměti, přestože je unikátní. Navíc ukládáme do AD miliony objektů a identifikační číslo nesedí do hierarchie adresáře. Proto se pro vyhledávání cesty využívá ADsPaths. Je to odkaz na objekt a využívá je nejen AD. V našem případě je syntaxe těchto cest popsána ve standardu LDAP. Podívejme se na jednoduchý příklad jedné takové cesty:

```
LDAP://dc=mycorp,dc=com
```

Lehce jsme popsali struktury a odkazy na objekty, nyní se podíváme na jednotlivé komponenty v AD.

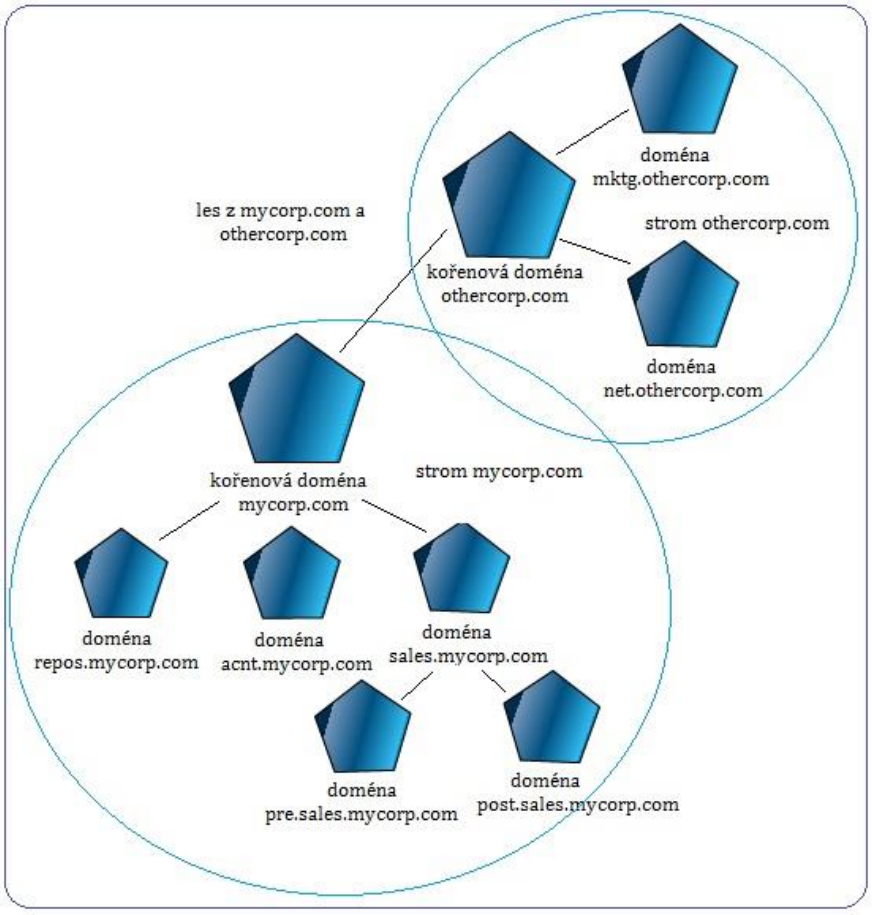
5.4.1 Komponenty Active Directory

Dělíme je na logické a fyzické. Fyzické komponenty (sítě, podsítě, doménový řadič) se starají o chod v síti a skutečné ohraničení naší komunikace. Doménový řadič (Domain controller, často se používá zkratka DC) je přímo určený server, ze kterého se řídí celá nebo pouze část AD. Na tomto počítači běží Windows Server 2012 R2 a je v něm uloženo schéma naší struktury. V doméně může být více DC, ale na jednom DC pouze jedna doména. Standardně máme dva a více DC. Pokud změníme něco v AD, děláme to na jednom počítači, ale vzápětí se provede replikace, která provede změnu i na ostatních DC, pokud nějaké jsou. Jméno domény se skládá z pre-Windows 2000 jména, říkáme mu NetBIOS doménové

jméno (kvůli kompatibilitě, např. mycorp nebo ITAcademy), celé vypadá jako jméno DNS (např. mycorp.com nebo ITAcademy.local).

Logické (les, strom, doména a OU) mají na starosti organizaci objektů a jejich škálovatelnost.

Nejvýše ve struktuře je les, který se může skládat z několika stromů. Každý strom má svou kořenovou doménu (v našem případě mycorp.com), ze které vybíhají pomyslné větve, které nazýváme domény. Což je v podstatě skupina počítačů sdílející stejné místo v adresářové struktuře. Muže být jen jedna nebo i více. Domény v jednom stromě mohou komunikovat mezi sebou, a pokud chceme založit další strom othercorp.com (tedy napojíme naše kořenové domény k sobě a vznikne les), který by mohl spolupracovat s naším mycorp.com, i to lze nastavit.



Obr. 2: Příklad poskládání komponent Active Directory
Zdroj: vlastní zpracování

Na obrázku Obr. 2 vidíme příklad jedné struktury. Obsahuje jeden les, dva stromy a devět domén. Jednotlivé domény se jmenují podle hlavní kořenové. Kořenové domény si navzájem důvěřují a sdílí své zdroje. Další z komponent je organizační jednotka (Organization unit, OU). Ta může například rozdělit doménu nebo v ní udělat specifickou skupinu s vlastními právy. Použije se tehdy, když je potřeba v doméně udělat skupinu, která se může spravovat sama, ale přesto není tak velká, aby se vytvořila nová doména. Distribuuje správu mezi více správců, deleguje pravomoci pro ty, kterým byla udělena práva.

Abychom mohli mít vše pod kontrolou a měli přehled, existuje globální adresář. Ten obsahuje kopii všech objektů v našem schématu a reference na ně, je uložený v doménovém řadiči, každá AD jeden globální adresář má.

Vždy, když tvoříme nové schéma či nový návrh doménové struktury, musíme se důkladně zamyslet, kolik prostředků – finančních a administrátorských – můžeme do projektu investovat. Ideálně by každé oddělení ve firmě chtělo mít vlastní doménový strom, ve kterém budou mít úplnou kontrolu nad svými informacemi. My ale musíme zvážit reálné prostředky, držet se nohama pevně na zemi a vždy dobře promyslet, jak bude naše schéma vypadat a jak bude rozvržené. Čím jednodušší struktura, tím méně práce se správou, snadnější odstranění potíží a síť lépe zabezpečíme. Často je lepší si virtualizovat zkušební prostředí sloužící pro testování změn a konfigurací v Active Directory, kde se vychytají všechny neduhy a podpoří se výsledná stabilita celé sítě. K důkladnému prozkoumání a otestování změn ale často potřebujeme výkonný počítač s aplikací pro to navrženou, na kterém může být spuštěno několik virtuálních operačních systémů současně. Tímto způsobem jsem zkoušela navržená cvičení popsané v praktické části, studenti budou využívat stejnou implementaci.

Je důležité rozvrhnout, kolik rolí a služeb zvládne jeden serverový počítač. Jestli je pro dvě služby jeden serverový počítač málo, nebo nám pro menší společnost o dvaceti lidech stačí dva servery na všechny služby. Nyní se na protokoly a služby a funkce používané v Active Directory podíváme zblízka.

5.4.2 Kerberos a LDAP

Active Directory je rozsáhlá kapitola, jejímž základem jsou adresářové služby a protokol LDAP. Lightweight Directory Access Protocol se stará o ukládání dat do adresářového serveru a jejich získávání, zajišťuje stromovou strukturu adresáře. Používá se hlavně pro přístup k datům, pro práci s uživateli, např. vyhledání informací o nich v databázi (jméno, plat, konfigurace počítače, umístění atd.). Do adresáře ukládá spíše data, která nepotřebují časté změny a žádné složité transakce. Součástí protokolu je také autentizace uživatele.

Slovo Kerberos pochází z řecké mytologie, je to jméno trojhlavého psa, střežícího vchod do podsvětí. Název vystihuje účel i v naší době – protokol vznikl k ochraně sítě, zabraňuje odposlouchávání a umožňuje klientům se autentizovat v síti a komunikovat s ostatními objekty bez problémů. Je ale potřeba, aby byl stále v provozu server, který zajišťuje přihlašování. Popřípadě mít záložní, který nastalý problém vyřeší či další náhradní autentizační řešení. Velkým problémem je také synchronizace času při komunikaci klient/server. Může se stát, že server začne být opožděn, vypne se a všechny služby na něm přestanou fungovat. Problém se dá řešit pomocí Network Time Protokol (NTP), který zajišťuje synchronizaci hodin počítačů v síti, pokud zpožděné pakety nechtěně rozhází čas.

5.4.3 Vztahy důvěryhodnosti

Někdy je potřeba, aby soubory a data sdílely i domény mezi sebou – ať už v jednom stromu či v sousedních. Vztahy důvěryhodnosti definují, jak uživatelé v jedné doméně mohou přistupovat k datům v jiné doméně. Jestliže máme pouze jeden strom, vznikají vztahy typu nadřízená-podřízená doména, jakmile máme stromů více, mezi jejich kořeny vzniká vztah strom-kořen.

Jakmile je vyslána žádost k doméně jinde ve stromu, uživatel je prověřen, jestli má vhodná práva k přístupu k prostředkům. Podíváme se na obrázek 2 – jestli chce uživatel z domény pre.sales.mycorp.com tisknout na tiskárně umístěné v doméně net.othercorp.com, musí se kontaktovat řadiče v doménách sales.mycorp.com, mycorp.com, othercorp.com a net.othercorp.com. Řadiče domény zkontrolují ověření uživatele a aktivují příslušný modul, aby protokol

Kerberos mohl provést autorizaci a dovolit uživateli použít tiskárnu. Poslední věta a příklad parafrázován z knihy. (Price, 2005, s. 45)

5.4.4 Active Directory Certificate Services (AD CS)

Stará se o digitální certifikáty a jejich bezpečnost. Ty se používají k šifrování zpráv a dokumentů. Ověřuje uživatele a zařízení v síti. Microsoft implementuje Public Key Infrastructure (PKI) – což je soubor hardware, software, pravidel a procedur potřebných k vytvoření a spravování digitálních certifikátů.

5.4.5 Active Directory Domain Services (AD DS)

Abychom mohli komunikovat s doménami v síti a využívat služby, které nabízejí, máme zde databázi, která zná celou hierarchii sítě. AD DS je serverová role v AD poskytující služby podobné jako zlaté stránky nebo telefonní seznam. Informace jsou díky ní k dispozici, protože počítačová síť spolupracuje.

Ukládá a spravuje informace ohledně síťových zdrojů, uživatelů v síti a dalších zařízení – řadí je do hierarchické kontejnerové struktury. Struktura dává jasně najevo, jak velký rozsah správce může ovládat a měnit, díky doménové struktuře a organizačním jednotkám v ní.

AD DS také omezuje formát jmen domén a ostatních zařízení, má svá pravidla a limity těchto objektů. Stará se o replikaci dat na další řadiče v doméně. Distribuuje informace v síti, které pak můžou správci vyhledat pomocí globálního adresáře a nezáleží na tom, kde přesně se informace nacházejí. AD DS ví, jak často, co všechno a na které řadiče v doméně má data replikovat.

5.4.6 Active Directory Federation Services (AD FS)

V dnešní době je kladen velký nárok na ověřování identity při přihlašování k internetovým aplikacím. AD FS je řešení, jak ulehčit naši paměť – uživatelům povoluje přistupovat k aplikacím a systémům, přestože jsou v odlišných lokacích, díky technologii Single Sing-On (SSO), si uživatel pamatuje pouze jedno heslo a vše ostatní obstará SSO. Přístup aplikací a uživatelů k informacím a webovým zdrojům je zjednodušen bez nutnosti se stále přihlašovat.

Z desítky hesel k aplikacím se v podstatě stane jedno jediné, přesto ale musíme být důslední a upozornit koncové uživatele v naší síti, ať kladou důraz na strukturu a jejich délku.

5.4.7 Active Directory Lightweight Directory Services (AD LDS)

AD LDS je adresářová služba, pomáhá aplikacím to vyžadujícím pracovat s adresáři. Využívá protokol LADP (Lightweight Directory Access Protocol). Je to podobná služba jako AD DS, rozdíl je v tom, že s AD LDS nemusíme být vázáni na domény ani na řadiče. AD LDS nepracuje s jedním schématem, přesto se může dotazovat AD DS na ověřování přístupových práv.

5.4.8 Active Directory Rights Management Services (AD RMS)

Zabezpečení dat je ve firmě velmi důležité a Microsoft poskytuje službu AD RMS prakticky v každé edici systému Windows Server. Přestože firma nastaví svým souborům a složkám přístupnost, mohou se vyskytnout drobné nedokonalosti. Uživatel buď má právo, nebo nemá právo pro přístup k souboru. Mezitím je ale velký prázdný prostor, ve kterém nemůžeme uživateli nařídit, jak se souborem naložit. Může soubor zkopírovat do jiné složky, smazat, číst nebo ho měnit. Role AD RMS nám může tyto požadavky splnit. Zabráníme tak krádeži dat, které ve většině případů nepochází z útoků zvenčí, ale zevnitř – od našich zaměstnanců, jejichž nevhodné zacházení s firemními daty znevýhodnilo firmu na trhu.

5.4.9 Dynamic Host Configuration Protocol (DHCP)

Standardem protokolu IP, který poskytuje klientům automatické přidělování IP adres z DHCP serveru. Vyhneme se tak konfliktním chybám, které se mohou vyskytnout, když zadáváme IP adresy ručně a uspoří nám spoustu času, pokud máme velkou síť, kde by bylo ruční zadávání naprosto nemyslitelné. Počítačům také posílá masku sítě, výchozí bránu a adresu DNS serveru. Přidělení adres je časově omezené a klient DHCP tuto platnost prodlužuje.

5.4.10 Domain Name System (DNS)

AD je na DNS v podstatě závislé. Některé jeho části bez něho nefungují. Je to internetový standard popisovaný i v TCP/IP, který překládá jména objektů (jména objektů – doménové jméno – domain name) na IP adresy. Podobný princip těsně integruje svoje prostředí i Microsoft. Pro lidské chápání jsou tu jména objektů a pro počítačový pohled jsou IP adresy. Téměř nikdo by si nepamatoval všechny IP adresy webových stránek, které na internetu navštěvujeme. Existuje i reverzní postup, kdy se přeloží IP adresa na jméno objektu, používají se k tomu tzv. PTR záznamy. Jednoduchým příkladem je:

```
12.11.10.in-addr.arpa
```

Tuto adresu později použijeme v praktické části bakalářské práce, při nastavování DNS a zadávání názvu zóny zpětného vyhledávání.

Služba DNS je nejčastějším, velmi oblíbeným objektem útočníků, protože si bez ní klienti nedokáží představit komunikaci s hostitelskými systémy a webovými stránkami.

Službu spravuje jeden nebo více serverů, zóny obsahují záznamy o jménech objektů (Start of Authority, SOA), jména a IP adresy všech serverů v zóně (Name Server, NS) a ostatních hostů (A záznam). Jsou tři typy zón – primární, sekundární a stub zóna.

Rozšířením DNS je služba DNSSEC zajišťující, že data získaná z DNS serveru jsou důvěryhodná, od správného zdroje a při přenosu nebyla narušena a uživatel nakonec nebyl spojen s IP adresou, kterou vůbec nečekal.

5.4.11 Remote Desktop Services (RDS)

Umožňuje administrátorům nebo klientům v síti se připojit přes vzdálenou plochu, popřípadě díky aplikaci RemoteApp. Tímto způsobem můžeme mít i rozdělené místo na disku – lokální a vzdálené úložiště pro naše data.

Jakmile se připojíme pomocí podnikové sítě nebo internetu k počítači, přebíráme za něj všechna práva a celý ho ovládáme, jeho aplikace a další konfigurace systému a to odkudkoli.

5.4.12 File and Storage Services

WS 2012 R2 má ve výchozím stavu nainstalovanou tuto službu pro správu souborových serverů a jejich disků.

Pomocí Správce serveru můžeme spravovat všechny naše servery na ukládání dat pouze z jednoho okna. Vidíme jejich obsazenost a další informace, můžeme je i defragmentovat pomocí uživatelského rozhraní.

New Technology File System (NTFS) verze 5 je nativní souborový systém pro WS 2012 R2, má funkce pro bezpečnost a konzistenci dat, kompresi disku, řízení kvót a další. Poskytuje skvělou podporu pro transakce s daty.

5.4.13 Print and Document Services

Centralizuje úlohy k tisknutí a umožňuje sdílení tiskáren v infrastruktuře. Přesně vidíme a spravujeme tiskové fronty a je nám oznámeno, jakmile je vše vytisknuto či pokud se něco ve zpracování tisku nezdařilo. Vše se děje v souladu se zásadami skupiny.

5.4.14 Hyper-V

Služba poskytující nám prostředí pro virtualizaci více operačních systémů (hostujících) na jednom počítači. Používá se pro zkoušení a opravování nasazených řešení, optimalizaci aplikací, které ve firmě používáme. Než si koupíme nový hardware (např. nový serverový počítač pro službu, kterou chceme nyní provozovat samostatně, jelikož se rozšiřujeme působení firmy, a proto dostáváme více finančních prostředků), můžeme otestovat budoucí infrastrukturu a předem vychytat chyby bez přerušení provozu ve firmě.

WS 2012 R2 představil novou verzi virtuálních strojů – virtuální stroje (Virtual Machines, VM) druhé generace. Jsou výkonnější, bezpečnější a rozsáhlejší než první generace. Největší rozdíl mezi generacemi je v tom, že druhá generace využívá UEFI firmware namísto obvyklého BIOS a chybí jí většina starých emulovaných zařízení.

Druhá generace přináší následující:

- Možnost Secure Boot (povoleno ve výchozím nastavení)
- Boot z SCSI VHD/VHDX – možnost trim, unmap a hot resizing (až 2,2TB MBR)
- Boot z SCSI DVD
- Podpora PXE boot pro standardní síťový adaptér (včetně IPv6)
- Podpora UEFI firmware
- Odebraná podpora IDE, legacy network adaptéru, řadič disketové mechaniky a COM port (COM se víceméně používal pouze pro debugging).
- Rychlejší boot virtuálního stroje o cca 20 %
  (novinky od, Výšek, 2013)

Důvod proč stále používat první generaci je v kompatibilitě se staršími operačními systémy. Druhou generaci spustíme pouze na WS 2012, WS 2012 R2, Windows 8, Windows 8.1 a novější verze a to pouze na 64x bitových verzích systémů. Pokud bychom chtěli virtuální stroj spustit na starší verzi, musíme využít pouze první generaci, protože po vytvoření virtuálního stroje se generace již změnit nedá.

5.4.15 Internet Information Server (IIS)

Po instalaci nám umožňuje používat HTTP, FTP nebo SMTP. Využívá TCP/IP protokolu. V praxi to znamená, že jakmile webový server nastavíme, můžeme využívat možností http a provozovat na něm HTML soubory, tedy webové aplikace a služby založené např. na technologii ASP.NET nebo PHP. Byl vytvořený společností Microsoft právě pro systém Windows, a proto je s ním úzce spjatý.

5.4.16 Windows Server Update Services (WSUS)

Díky Windows Server Update Services je umožněno administrátorům, aby získali nejnovější verze produktů od Microsoft na počítače, kde je nainstalovaný operační systém Windows. Správce může plně ovládat, které aktualizace se nainstalují a na jakých počítačích v síti. Mohou se podívat do celkového skladu všech balíčků, které jsou k dispozici a přečíst si rozsáhlé zprávy o tom, co všechno

se změní po jejich instalaci. Potom mohou snadno přijímat nebo odmítat aktualizace jednotlivě.

WSUS je alternativa ke službě Microsoft Update, na WS 2012 R2 je k dispozici jako role serveru. Služba získává aktualizace z centrálního serveru společnosti Microsoft, čímž se šetří místo – počítače se pouze připojí k serveru a nainstalují potřebné aktualizace, nemusí nic stahovat na svůj disk či ho zatěžovat časově.

6 Praktická část

Praktická část bakalářské práce se skládá z návodů, jak nastavit jednoduché schéma naší sítě. Návody jsou koncipovány pro školní účely, kde je potřeba uzpůsobit prostředí pro výuku. Jsou vyzkoušeny na virtualizační aplikaci a vybrány jsou pouze nejdůležitější části, které odkazují na teoretickou část bakalářské práce. Každá část má své zadání a podrobné řešení s obrázky. Všechny návody a ilustrační obrázky se kvůli rozsahu do bakalářské práce nedají vložit. Veškeré obrázky v návodech jsou vlastní výroby. Návody vycházejí z již používaných učebních návodů pro předmět Operační systémy 1, odkaz na ně se nachází ve zdrojích.

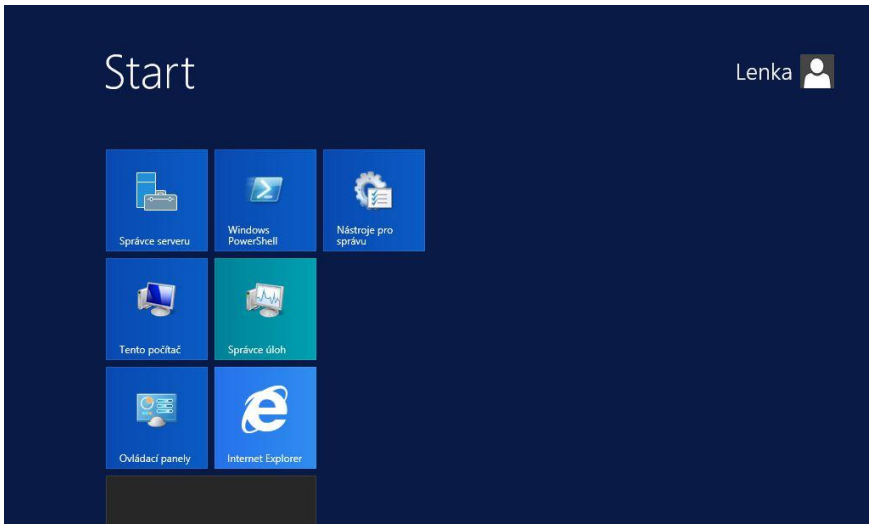
Systémy se dají nastavit i jiným způsobem, návody nejsou vyčerpávajícím seznamem všech možností, jak k výsledku dojít. Jsou zde ale brány ohledy na dosažené zkušenosti studentů, kteří budou návody ve školní výuce procházet.

Jako správci sítě nemáme vždy čas, abychom obíhali celou naši infrastrukturu. Proto existuje vzdálený přístup a spravování více našich serverů najednou. Na vzdálených serverových počítačích můžeme pomocí jedné konzole z jednoho počítače nainstalovat operační systém a následně nastavit vše, co si konkrétní doména přeje. V dnešní době už není potřeba zdůrazňovat, jak je důležitá síť – ať už naše lokální nebo internetová. Ve všech případech vždy sedíme před počítačem, který sdílí své a využívá služby dalších počítačů a různě s nimi komunikuje.

Ještě důležitější je mít dostatek základního kapitálu. Menší firmy mají méně prostředků a peněz, tím pádem i méně serverů. V praxi si mohou dovolit pouze dva, které mají nainstalováno více rolí a funkcí. Velká společnost může žít v pohodlí několika serverů a každý z nich může mít jen jednu roli. Tato bakalářská práce je zaměřena na operační systémy z rodiny Microsoft Windows, přesto v praxi není problém mít několik serverů s WS 2012 R1 a další s nainstalovanými linuxovými distribucemi.

Důležité aplikace a serverové role se dávají na fyzické servery, ostatní můžeme virtualizovat kvůli snížení nákladů. V praxi to znamená, že můžeme mít fyzicky pouze dva serverové počítače (druhý záložní, jakmile první postihne

nehoda), ale čtyři virtualizované stanice díky Hyper-V, na kterých běží firemní aplikace (např. MS SQL Server a MS Exchange Server zajišťující přístup k poště, kontaktům a kalendáři). Vysokou dostupnost nám zajistí technologie WS 2012 R2 Hyper-V Replica – když jeden server vypadne, pracovník má stále přístup k firemnímu SQL Serveru.



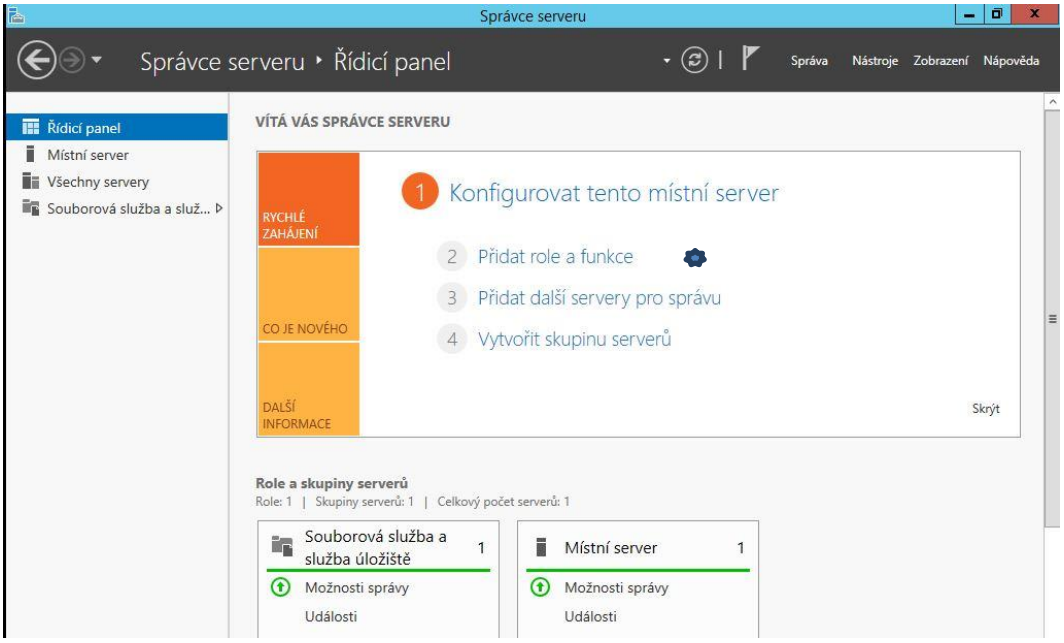
Obr. 3: Nabídka Metro

6.1 První téma – instalace a Hyper-V

6.1.1 Instalace Windows Server 2012 R2

Zvládnout implementovat a spravovat virtualizovanou infrastrukturu se dnes stává klíčovou prací pro administrátory větších i malých firem.

S nástupem WS 2012 se stala možnost virtualizovat jednodušší než kdy dřív. Naučíme se, jak rozmístit a spravovat virtuální stroje. Můžeme využít nástroj PoweShell, což je v podstatě vylepšený a výkonnější příkazový řádek (cmd), který už nemusíme na náš server instalovat, protože je již součástí instalace systému od verze WS 2008. My se naučíme virtualizovat s přívětivějším uživatelským rozhraním, budeme využívat virtualizační platformu Hyper-V. To provedeme tak, že v nabídce Start, v kolonce Nástroje pro správu, spustíme Správce serveru (Server Manager, pokud se sám nespustil), ze kterého můžeme nastavit vše potřebné.

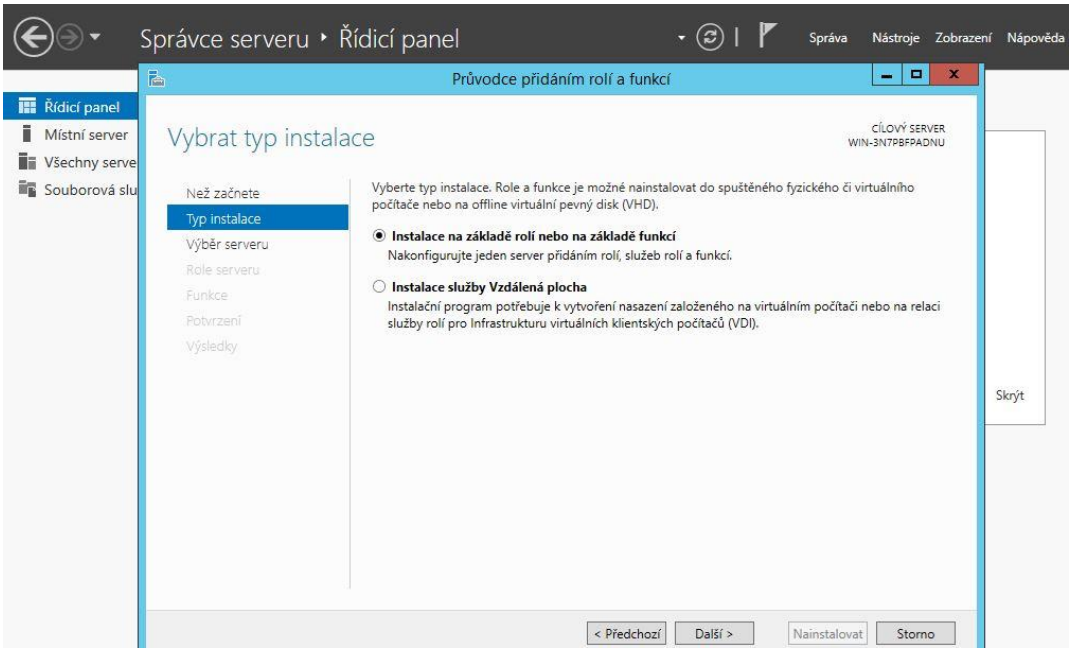


Obr. 4: Řídící panel Správce serveru

Než začneme tvořit virtualizační infrastrukturu, musíme nastavit server, na kterém budeme hostit ostatní stroje. Zatím zde máme jen roli Souborová služba a služba úložiště, která se stará o dostupnost, bezpečnost a rozmístění našich dat. Tato služba je nainstalovaná předem na každém serveru, je jeho nedílnou součástí.

Jakmile položku služby otevřeme, můžeme přidávat nová úložiště a spravovat je z jednoho místa, vidíme zde, kolik místa nám ušetřila deduplikace, procenta zaplnění disků nebo informace o iSCSI.

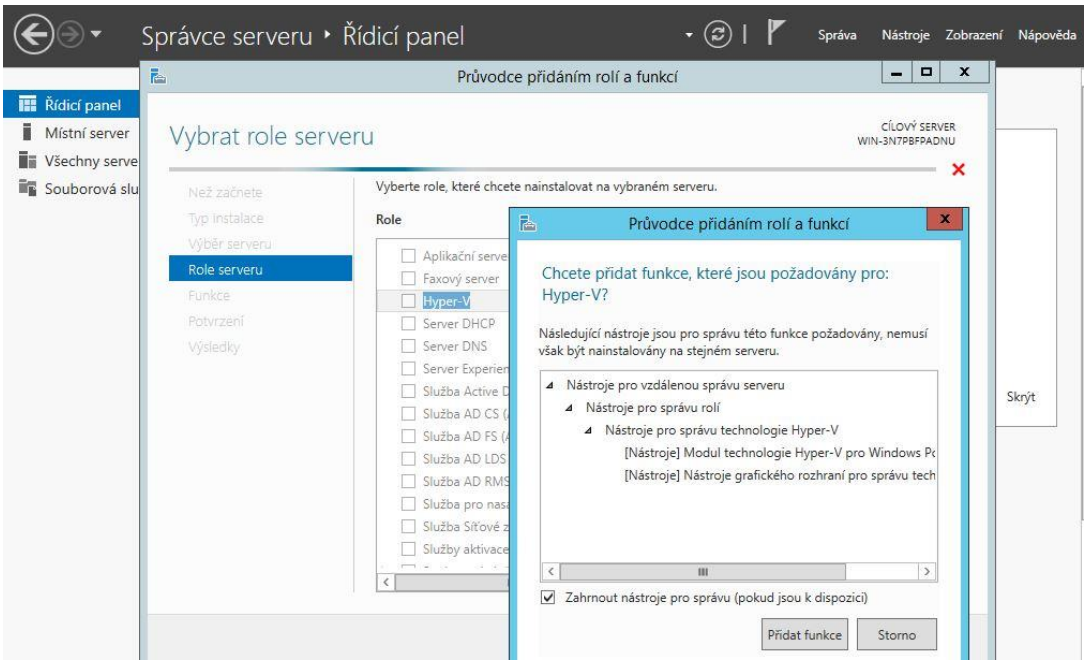
Na našem serveru nevidíme žádné hostované virtuální stroje, proto klikneme na možnost Přidat role a funkce.



Obr. 5: První krok v průvodci

Spustí se grafický průvodce, kde postupně nastavíme parametry.

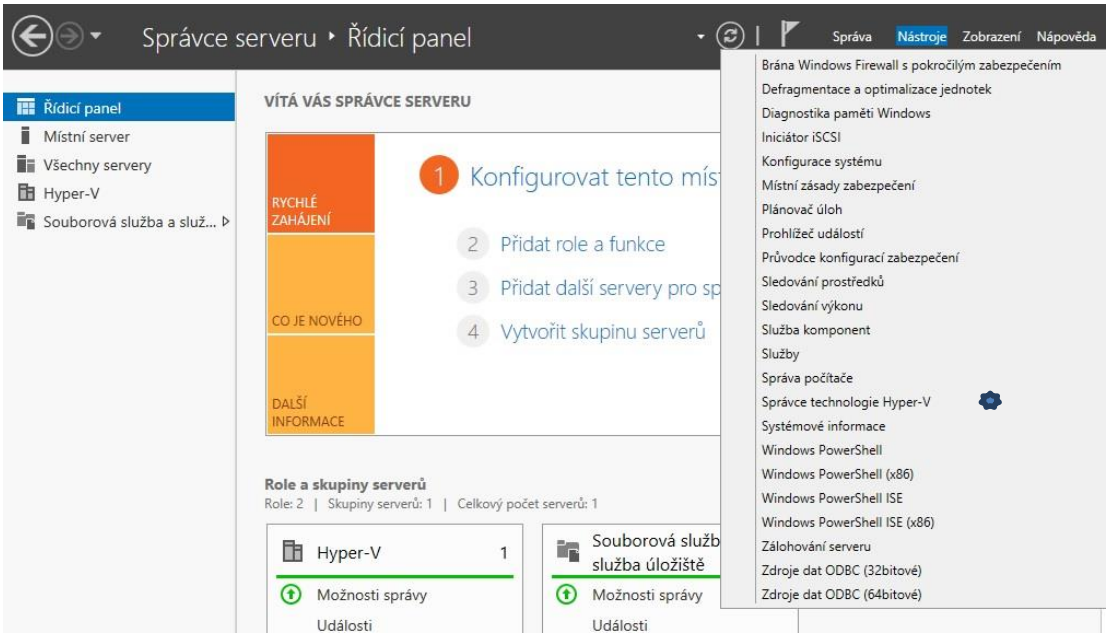
Můžeme nastavit i několik rolí najednou. Zatím ale vybereme pouze Hyper-V a klikneme na Přidat funkce.



Obr. 6: Ukázka výběru rolí

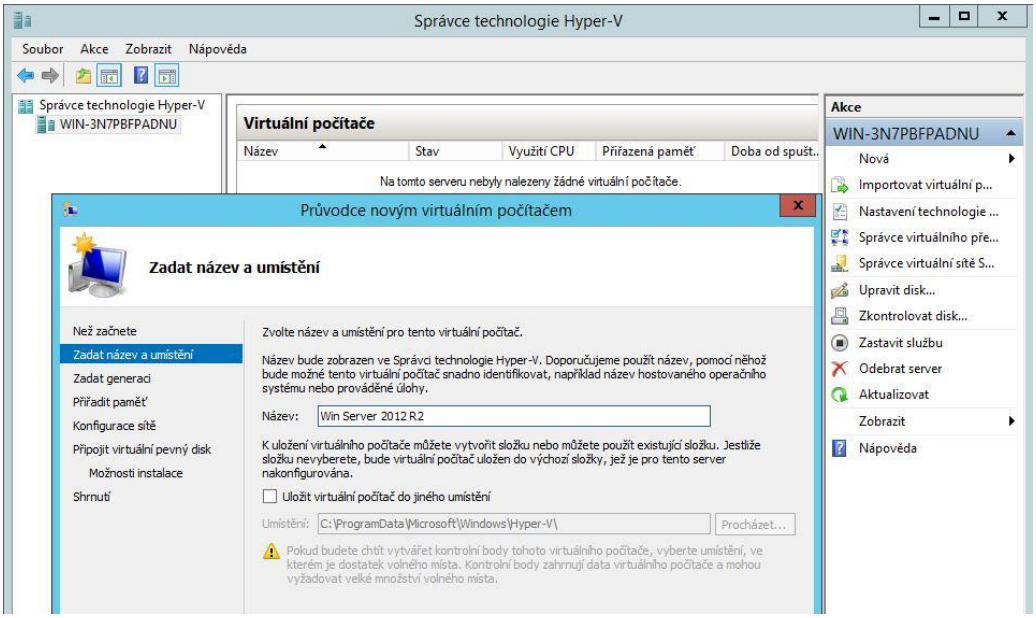
Po potvrzení instalace se ve Správci serveru, v levém menu objeví Hyper-V a v něm náš počítač, ke kterému jsme přidali novou roli.

Nyní ve Správci serveru v nabídce vpravo nahoře otevřeme Správce Hyper-V (Nástroje -> Správce technologie Hyper-V).

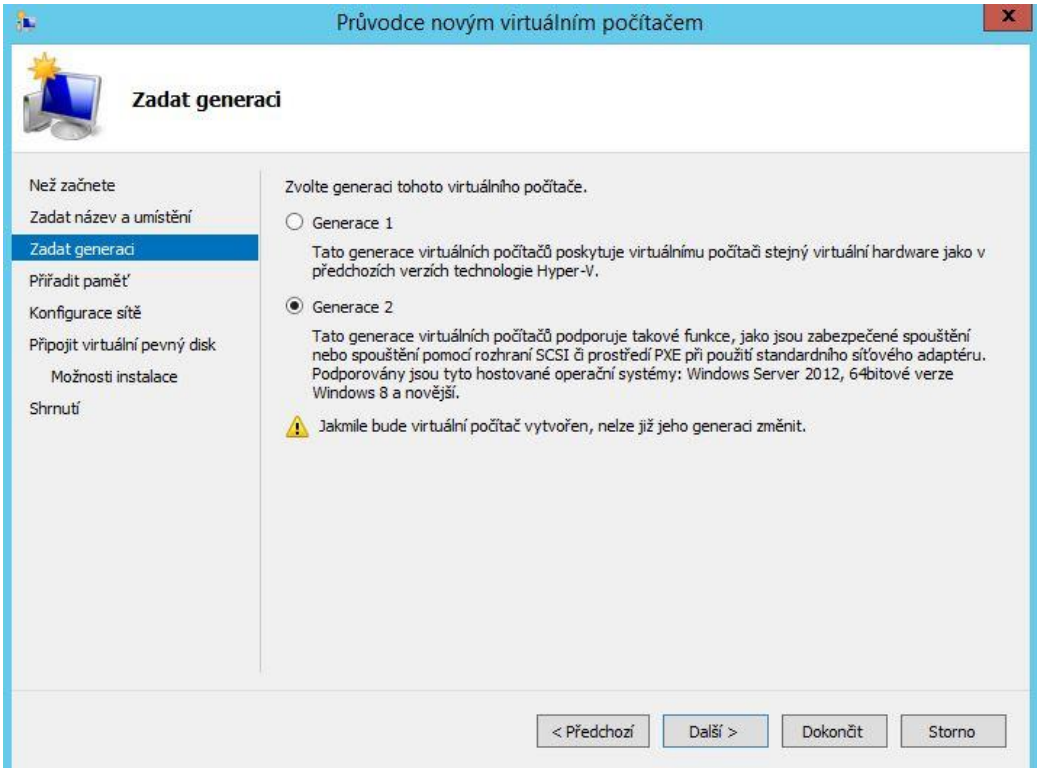


Obr. 7: Spuštění Správce technologie Hyper-V

Zatím nemáme v seznamu žádný virtuální počítač, a proto si zkusíme jeden vytvořit, nainstalovat na něj operační systém a další aplikace. Klikneme vlevo na náš počítač pravým tlačítkem a vybereme možnost Nový virtuální počítač (nebo vpravo Nová -> Virtuální počítač). Název bude Win Server 2012, generace 2, instalace operačního systému ze souboru spustitelné bitové kopie (pomocí možnosti Procházet vložte cestu k souboru ve formátu ISO s operačním systémem Windows Server 2012 R2).



Obr. 8: Zadání názvu virtuálního počítače



Obr. 9: Výběr generace virtuálního počítače

Prozkoumáme i další nastavení, která pro potřeby rozběhnutí našeho systému zatím nejsou nutná, ale jakmile se nový virtuální stroj vytvoří, zobrazí se v seznamu, klikneme na něj pravým tlačítkem -> Nastavení.

Nyní se můžeme připojit ke konzoli virtuálního počítače, klikneme na stroj pravým tlačítkem -> Připojit. Zobrazí se instalační průvodce, ve kterém nastavíme jako jazyk Čeština a spustíme instalaci pomocí tlačítka Nainstalovat. U výběru operačního systému zvolíme Windows Server 2012 Enterprise (úplná instalace). Instalace jádra serveru slouží pro minimalizaci režií a nároků na správu, může také zlepšit zabezpečení, pro naše potřeby ale využijeme celkovou instalaci. Přijmeme licenční podmínky.

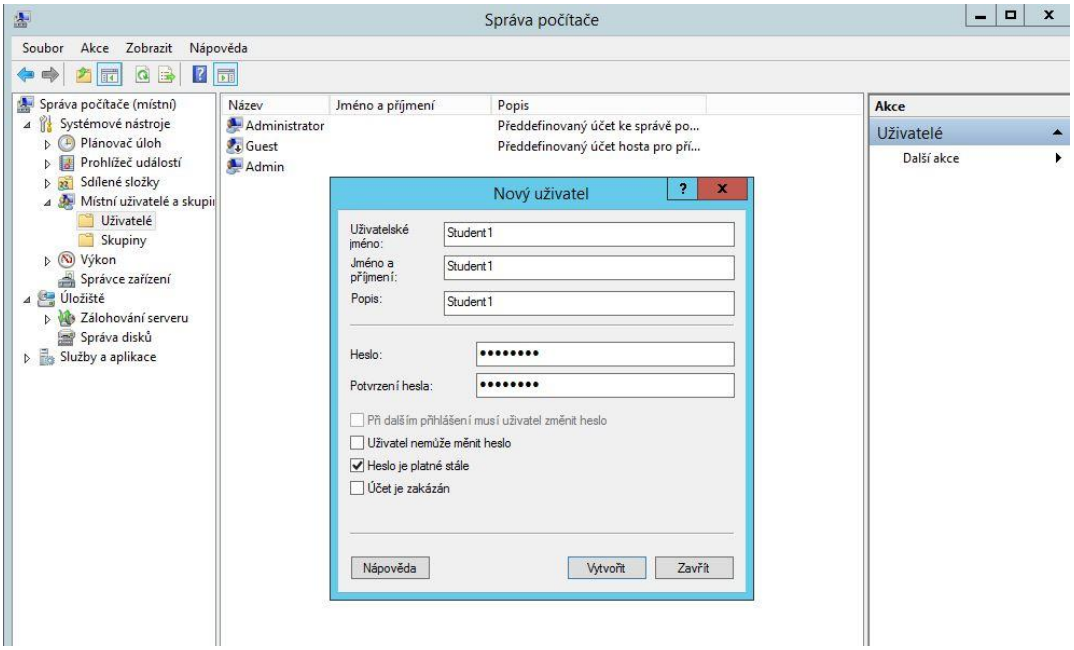
U výběru typu instalace na další obrazovce vybereme Vlastní a poté necháme výchozí stav diskových jednotek. Pokračujeme tlačítkem Další ke spuštění samotné instalace. Jakmile se systém nainstaluje, můžeme změnit heslo Administrátora na 8Cisco16. Nyní je instalace úplná.

6.1.2 Práce s uživateli a přidělování rolí

Jakmile Windows nainstalujeme, vytvoří se první uživatelský účet s administrátorskými právy. To znamená, že se může dostat ke všem nastavením systému a cokoli měnit. Z tohoto účtu můžeme přidávat libovolně další, kterým přiřazujeme přístupová práva. Ne vždy chceme, aby každý mohl nahlédnout do souborů druhého nebo aby všichni dokázali měnit hesla k ostatním účtům. Uživatelské účty zabraňují chaosu, který by z takové situace dřív nebo později vznikl. Účty oddělují data a vlastní nastavení konkrétních uživatelů.

Otevřeme Správu počítače (Start -> Ovládací panely -> Správa počítače, zde už vidíme, že budeme spravovat našeho hosta), v levém menu rozbalíme nabídku Místní uživatelé a skupiny, vybereme Uživatelé. Vidíme tu předdefinované účty, ke kterým můžeme přidávat další.

Vytvoříme uživatele Student1 (pravým tlačítkem na Uživatelé -> Nový uživatel), heslo 8Cisco16, zrušíme přednastavenou možnost „Při dalším nastavení musí uživatel změnit heslo“ a zaškrtneme možnost „Heslo je platné stále“. Při normálním provozu se hodí, pokud si uživatel změní heslo podle svých preferencí, pro naše zkušební účely ale tuto možnost nevyužijeme.



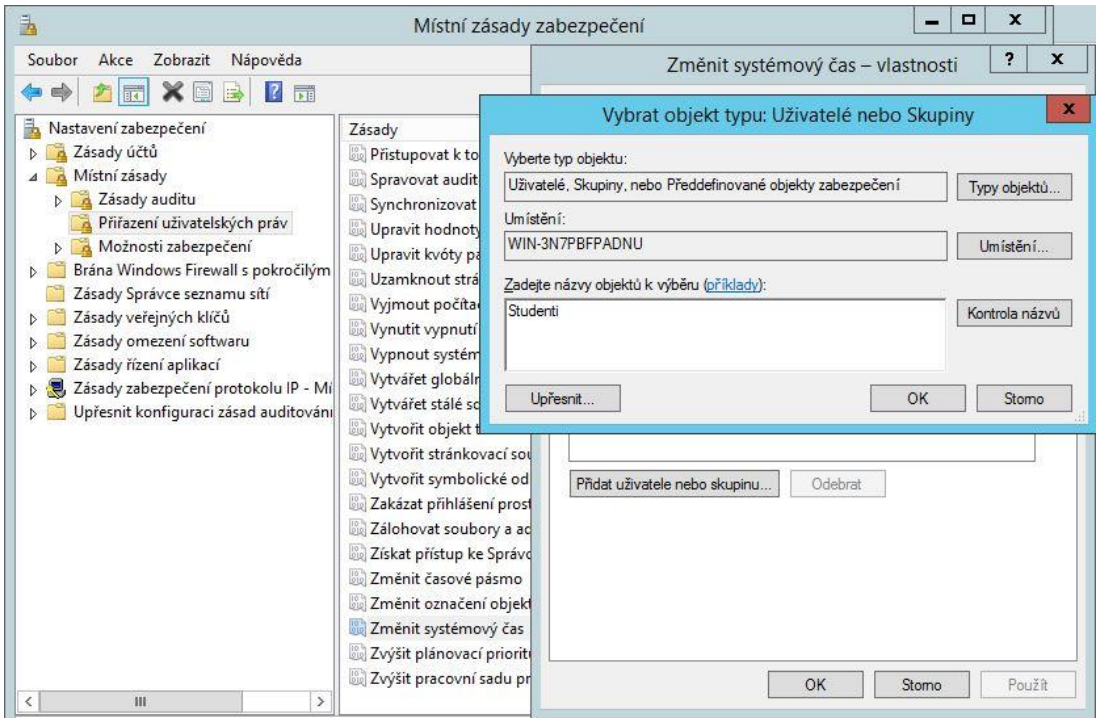
Obr. 10: Vytvoření nového uživatele

Stejným způsobem vytvoříme uživatele Host a Spravce. Uživatele nemáme přidělené žádné skupině – tu vytvoříme, když klikneme pravým tlačítkem na Skupiny -> Nová skupina. I zde najdeme předdefinované skupiny, prozkoumáme jejich možnosti v nastavení. Vytvoříme skupinu Studenti podobně jako uživatele. Teď už můžeme nové uživatele přiřadit do skupin.

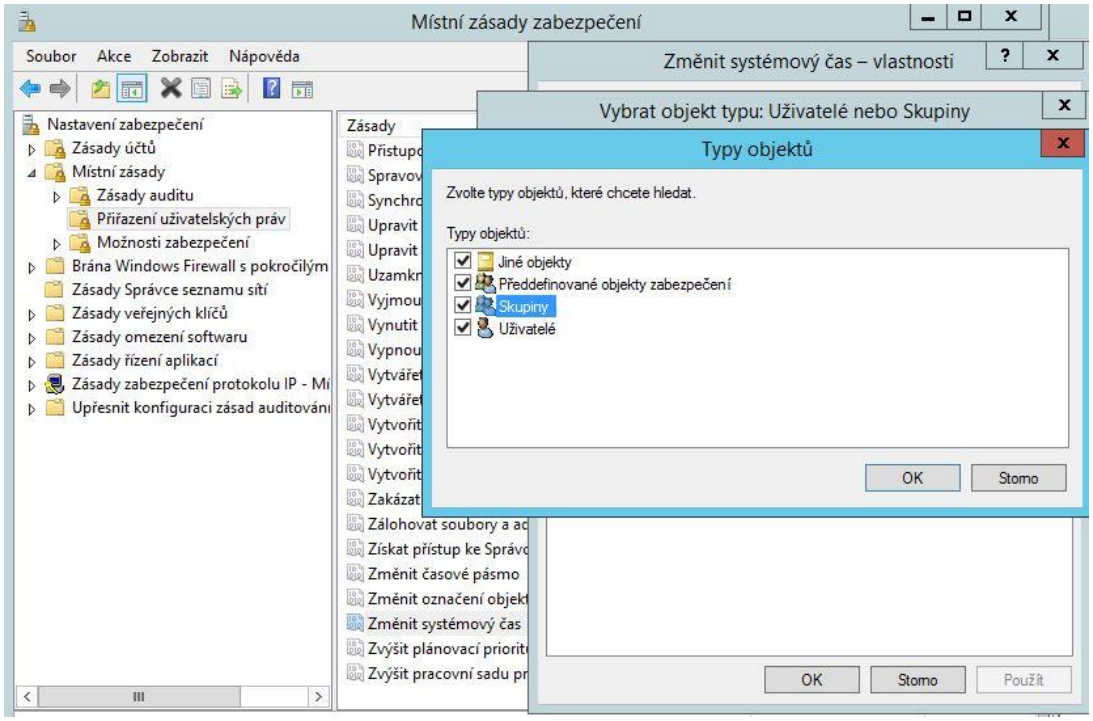
Start -> Nástroje pro správu -> Místní zásady zabezpečení, v levém menu rozbalíme Místní zásady a zvolíme Přiřazení uživatelských práv. Tato práva přiřazujeme skupinám či rovnou uživatelským účtům. Pro každý spuštěný proces v počítači je v paměti vytvořena datová struktura s informacemi o právech uživatele, který proces spustil, tzv. acces token. Je zde jeho login, práva, SID (security ID) a SID skupin, ke kterým patří. SID je to, podle čeho se počítač řídí, když hledá, jestli k něčemu máme přístup nebo nám je přístup zamítnut. Jedinečné identifikační číslo.

Na ukázku přidělíme skupině Studenti právo Změnit systémový čas a Vypnout systém. Najdeme právo, klikneme na něj pravým tlačítkem a zvolíme Vlastnosti -> Přidat uživatele nebo skupinu. Zde musíme povolit, že práva může dostat i celá skupina -> Typy objektů, zaškrtněte Skupiny. Potvrdíme volbu a

v okně přidáme skupinu Studenti (stačí ji napsat do pole názvů objektů a kliknout na Kontrola názvů, nakonec potvrdit OK).

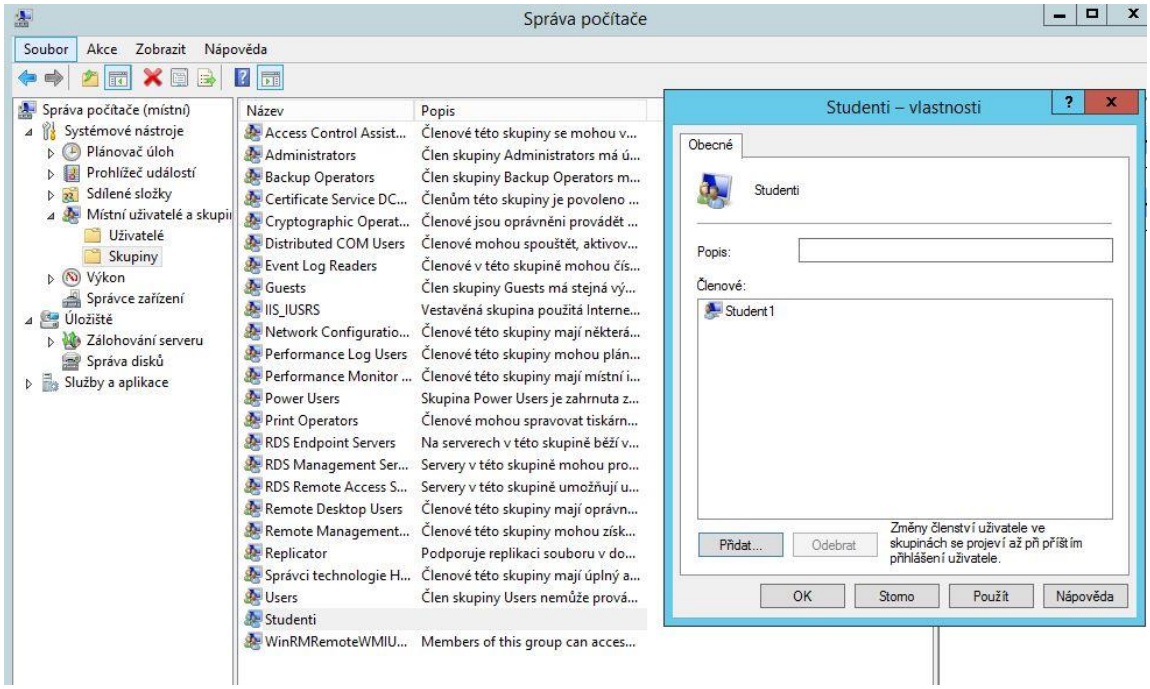


Obr. 11: Přiřazení práv skupině



Obr. 12: Přiřazení práv, typy objektů

Jakmile jsou práva přidělena, můžeme do skupiny přidat uživatele. Skupiny -> najdeme skupinu Studenti a klikneme na ni pravým tlačítkem -> Vlastnosti -> v novém okně stiskneme Přidat a přidáme všechny členy. Obdobně můžeme přidat i v položce Uživatelé do skupiny Studenta.



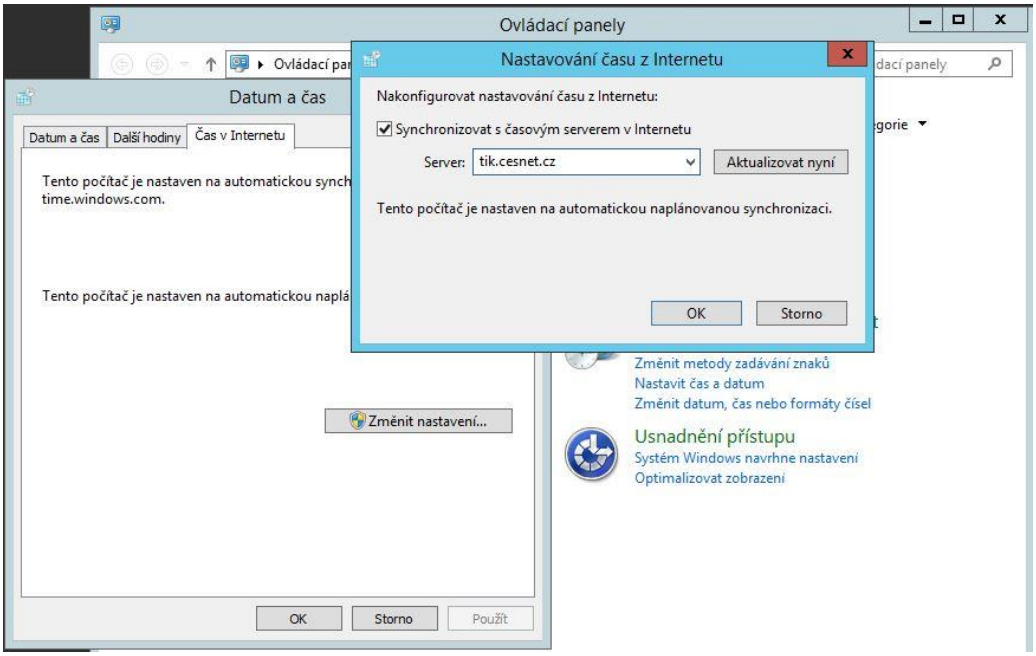
Obr. 13: Přidání uživatele do skupiny

Obdobně přidáme uživatele Spravce do skupiny Administrators a uživatele Host do skupiny Guests. V nabídce Start se nejdříve odhlasíme a nakonec se přihlásíme jako Spravce.

6.1.3 Nastavení časové synchronizace

Nastavíme, aby se čas v počítači automaticky srovnal se servery v internetu. Informace musí počítač na internetu někde získávat, a proto existuje několik serverů, které se starají právě o tohle. My využijeme server tik.cesnet.cz.

Start -> Ovládací panely -> vyhledáme Datum a čas -> na záložce Čas v internetu vybereme Změnit nastavení a do pole napíšeme server, který chceme.



Obr. 14: Nastavení časové synchronizace

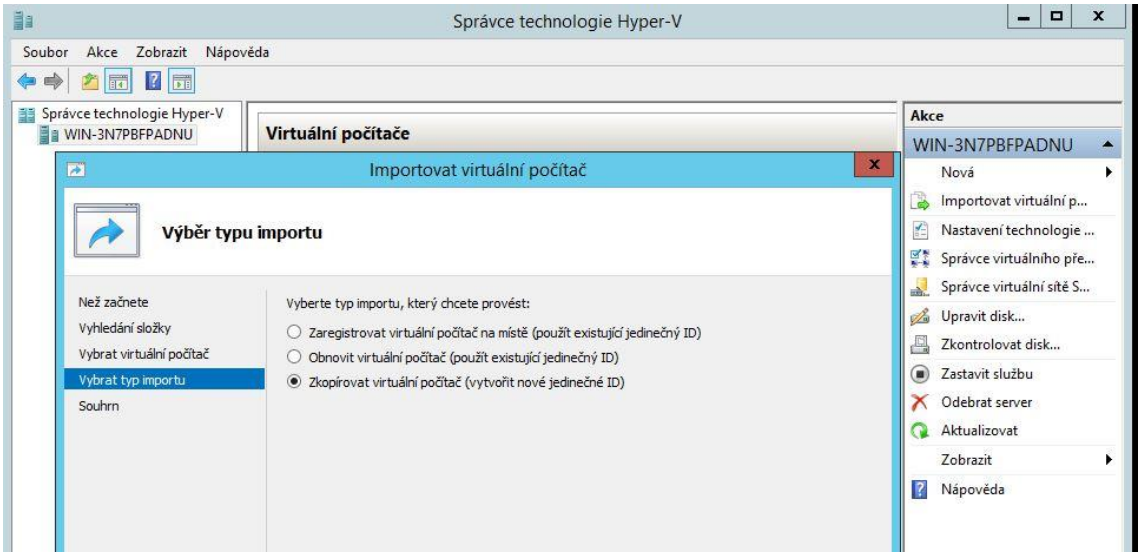
6.2 DNS a DHCP Servery

6.2.1 Server DNS

Z teoretické části bakalářské práce víme, k čemu tyto služby slouží a že bez DNS by Active directory nefungovalo. Proto si ukážeme, jak na server tuto roli přidat a nakonfigurovat.

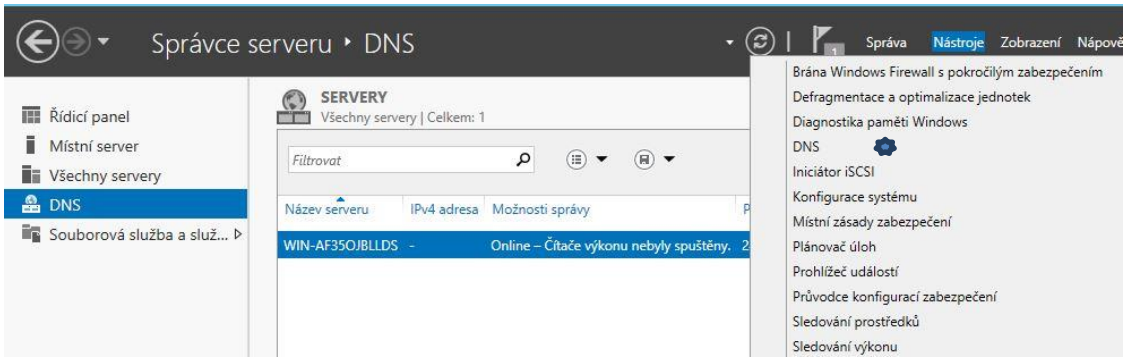
Nejprve si virtualizujeme jednoduchou strukturu se servery. Importujeme do prostředí Hyper-V částečně předkonfigurované virtuální stroje. Na těch jsou přednastaveny statické IP adresy v rozsahu 10.11.12.0/24 a služba AD DC, na které je nastavena hlavní doména ITAcademy s poddoménami SW.ITAcademy a HW.ITAcademy. ITAcademy má primární řadič domény nastaven jako server se jménem Server_ITAcademy, na kterém již běží služba DNS, což nám poskytuje jména do celé domény ITAcademy. Je vypnutý firewall, aby nám jeho funkce neomezovaly spojení mezi objekty v doméně. Služba DNS a DHCP ale chybí na řadičích v podřazených doménách, proto ji nastavíme sami. Nakonec přidáme virtuální stroj s Windows 8 a zařadíme ho do správné domény a nakonfigurujeme tak, aby dostal adresu od služby DHCP automaticky.

Nejprve otevřeme Správce technologie Hyper-V (vpravo nahoře Nástroje -> Správce technologie Hyper-V). V pravém menu klikneme na akci Importovat virtuální počítač, nalezneme složku s připraveným virtuálním strojem, přecházíme průvodcem pomocí tlačítka Další, zaškrtneme možnost Zkopírovat virtuální počítač (vytvořit nové jedinečné ID).



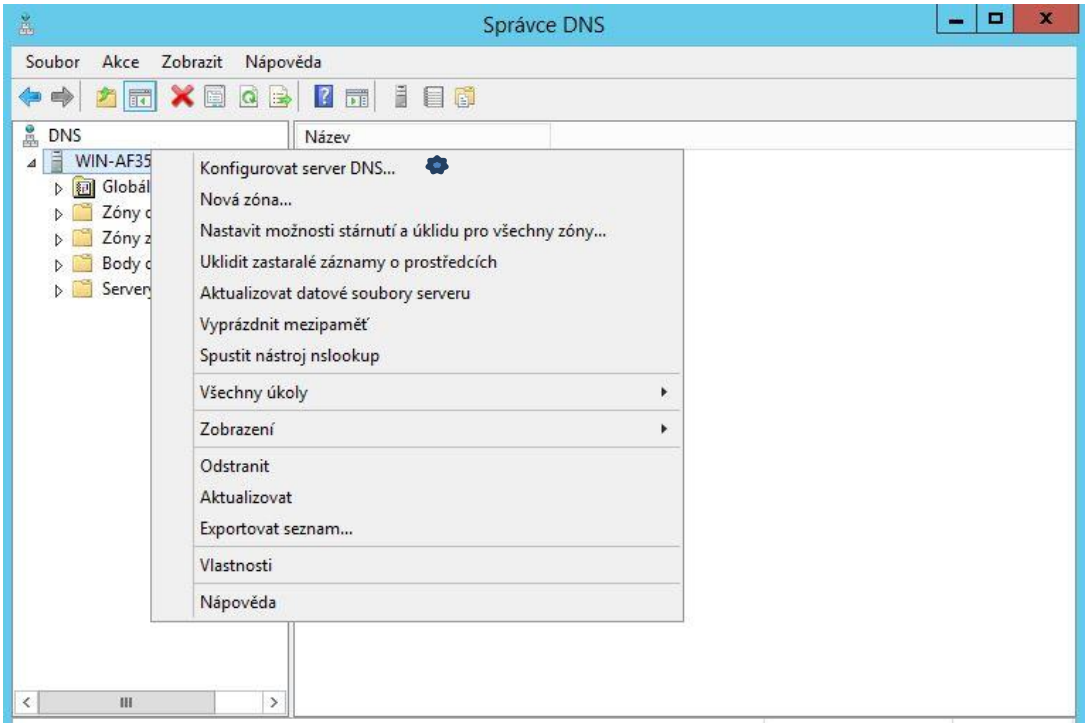
Obr. 15: Importování virtuálního počítače

Jakmile máme servery importované, spustíme je a přihlásíme se na administrátorský účet (heslo: 8Cisco16). Automaticky se spustí Správce serveru, kde přidáme roli DNS.



Obr. 16: Spuštění správce DNS

Jakmile je role nainstalovaná, otevřeme Správce DNS (vpravo nahoře Nástroje -> DNS).



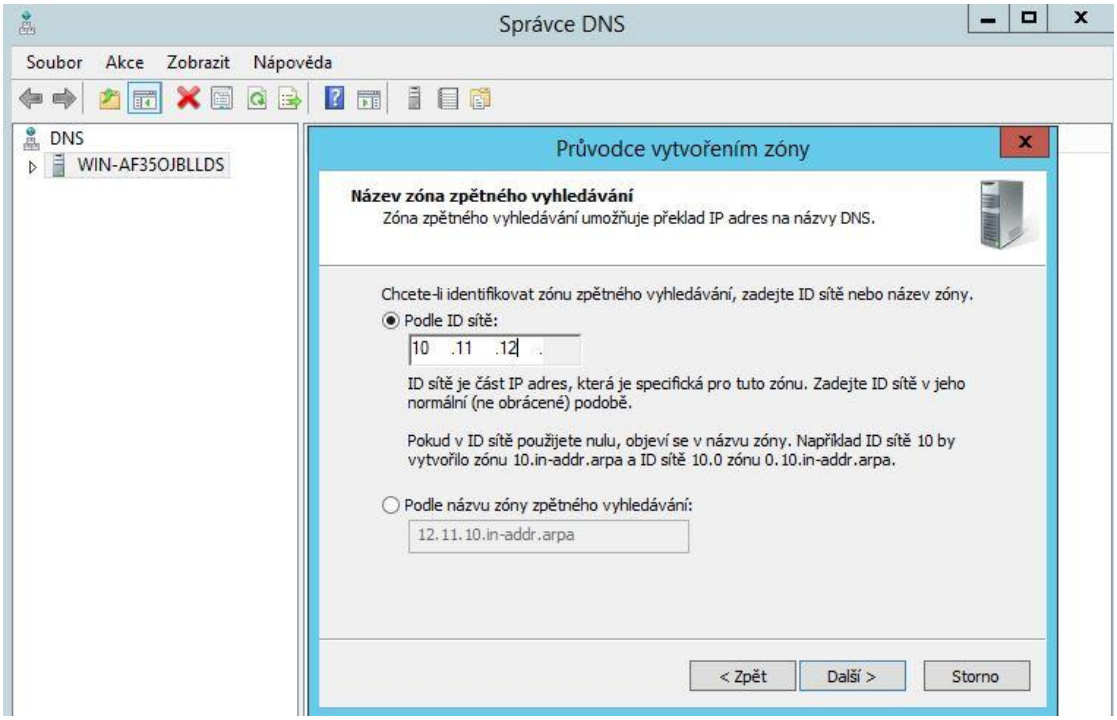
Obr. 17: Spuštění konfigurace DNS

Nyní můžeme Konfigurovat server DNS. Vytvoříme primární zónu dopředného a primární zónu zpětného vyhledávání, zaškrtneme, že chceme replikovat data do všech doménových řadičů v doménové struktuře ITAcademy.local, název nové zóny bude SW.ITAcademy.local, zaškrtneme možnost uložení zóny do adresáře Active Directory, povolovat budeme pouze zabezpečené dynamické aktualizace. Do místa pro IP adresu napíšeme 10.11.12/24, spodní kolonka se doplní sama. Předávat dotazy budeme na server v doméně ITAcademy, ve kterém je adresa již nastavená, vidíme ji na obrázku níže. Nejdříve se vytvoří zóna dopředného vyhledávání a pak uděláme stejnou konfiguraci i u zóny zpětného vyhledávání.

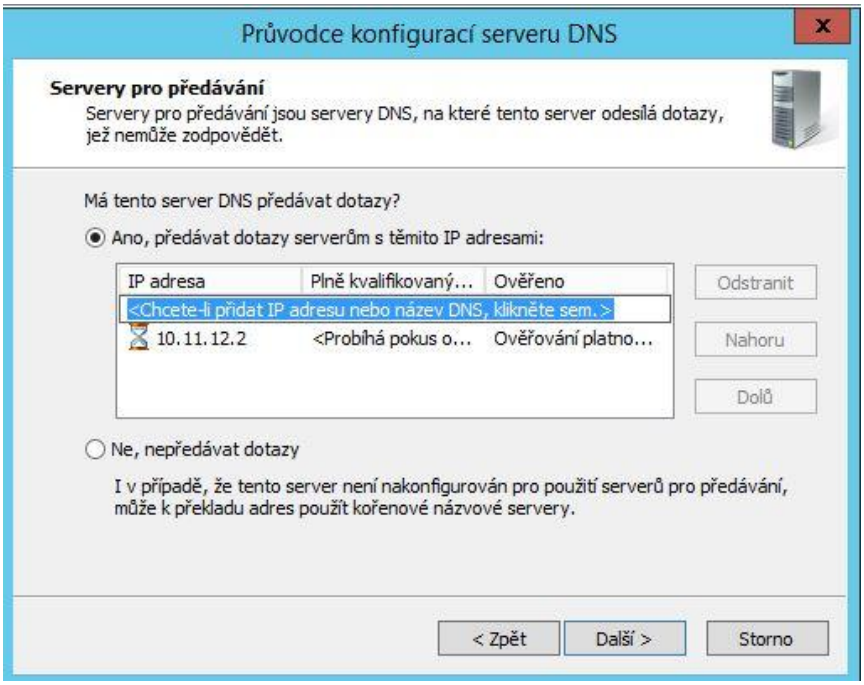
Prozkoumáme novou strukturu, která se vytvořila. Podobně nainstalujeme DNS i na serveru Server_HW_ITAcademy, s názvem zóny HW.ITAcademy.local.

Jakmile je vše dokončené, můžeme na serveru Server_SW_ITAcacemy přidat koncovou stanici s operačním systémem Windows 8 do zóny SW.ITAcademy.local. Nazveme ji Stanice1 a zaškrtneme možnost, že chceme vytvořit přidružený záznam o ukazateli (PTR). Plně kvalifikovaný název této stanice tedy bude Stanice1.SW.ITAcademy.local. a IP adresa 10.11.12.10 (pravým tlačítkem klikneme

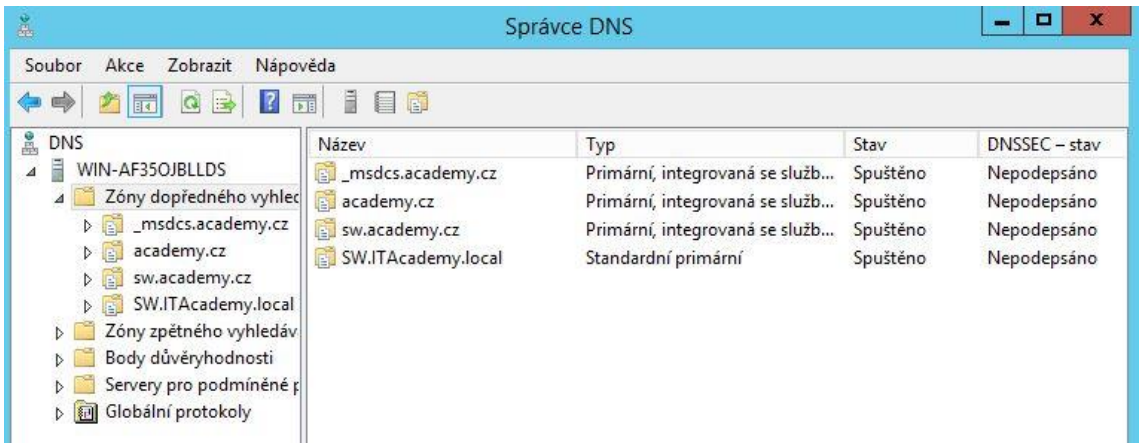
na zónu SW.ITAcademy.local -> Nový hostitel (A nebo AAA)…). Na serveru Server_HW_ITAcademy zase přidáme hostitele Stanice2 s IP adresou 10.11.12.11. Na serveru Server_ITAcademy přidáme do zóny hostitele Stanice3 s IP adresou 10.11.12.12. Tyto záznamy jsou k tomu, aby se jméno počítače spojilo s IP adresou, kvůli sdílení zdrojů.



Obr. 18: Průvodce vytvořením zóny



Obr. 19: Adresa serveru DNS pro předávání dotazů



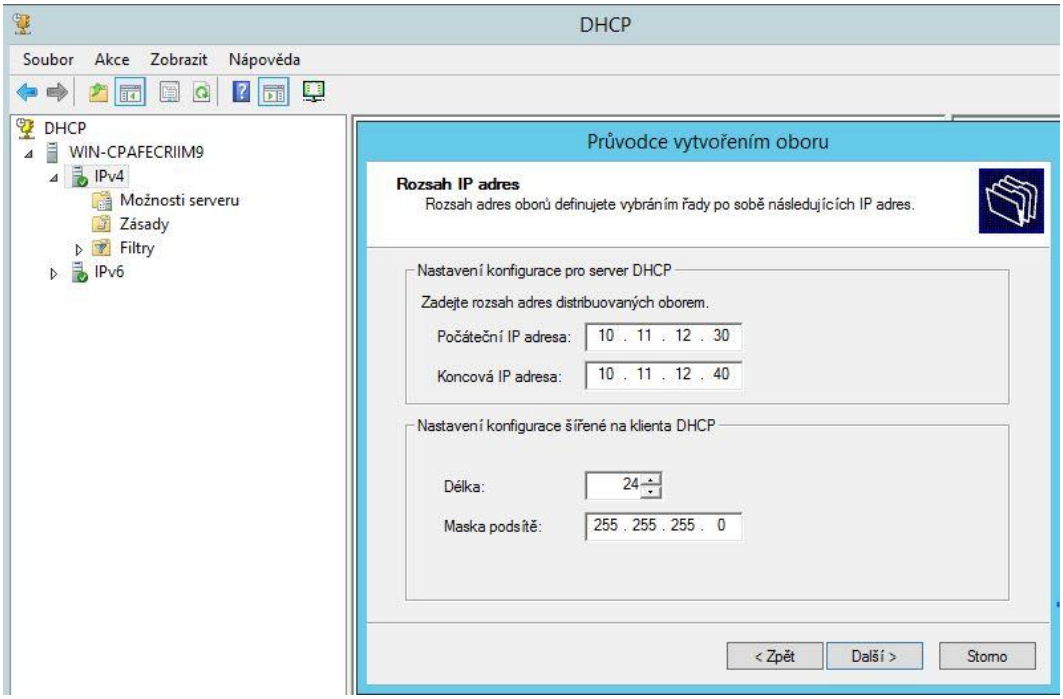
Obr. 20: Nově vytvořené zóny

6.2.2 Server DHCP

Zapneme server Server_ITAcademy a přidáme na něj roli DHCP tak, jak už to umíme. Otevřeme správce DHCP (vpravo nahoře Nástroje -> DHCP). Můžeme si všimnout, že po nás server požaduje další konfiguraci DHCP (rozklikneme vykřičník v horní nabídce -> Kompletní DHCP konfigurace). Zde nastavíme jméno účtu kvůli autorizaci (ITACADEMY/Administrator). Dále se po nás v průvodci bude chtít, abychom nastavili adresu DNS serveru, adresu výchozí brány nebo WINS serverů atd. Tyto adresy máme popsané výše (DNS server 10.11.12.1, výchozí

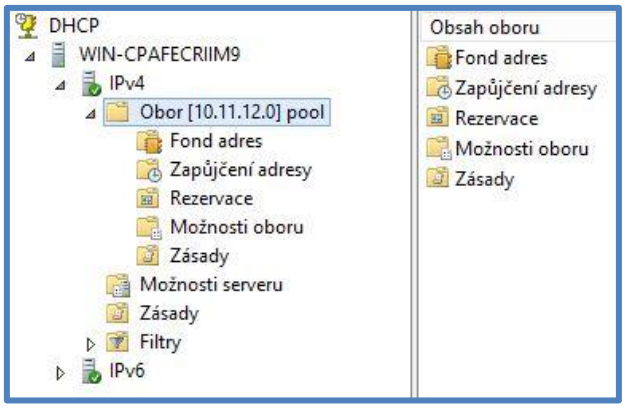
bránu a WINS servery nevyplňujte) a jejich nastavení potom platí pro všechny obory.

Zpátky ve Správci DHCP, klikneme na jméno serveru, potom pravým tlačítkem na IPv4 a vybereme Nový obor. Tím vytvoříme rozsah povolených adres, které bude server klientům přidělovat. Otevře se průvodce, kde nastavíme jméno oboru, počáteční IP adresu 10.11.12.30 a koncovou IP adresu 10.11.12.40. Délka prefixu bude 24, tedy maska podsítě 255.255.255.0. Můžeme zde nastavit také adresy, které patří do oboru, ale nikdy se nebudou přidělovat, protože jsou použity třeba jako výchozí brána nebo jiný server.



Obr. 21: Rozsah IP adres v oboru

Kolik jsme tímto rozsahem získali počet IP adres, které bude server automaticky rozdělovat mezi přiřazené počítačové stanice? Tento údaj zjistíme ve statistických údajích (pravým tlačítkem myši klikneme na obor pool -> Zobrazit statistické údaje).



Obr. 22: Nově vytvořený obor s názvem pool

V možnostech oboru vidíme, že adresy můžeme zapůjčovat na určitou dobu, dokud se znovu neobnoví (třeba v řádu hodin nebo dní). Kratší dobu volíme, pokud máme méně adres a klienti nepotřebují přístup na internet po tak dlouhý čas a delší dobu, když vlastníme síť o stabilnějším počtu klientů. Nebo adresy permanentně rezervujeme pro specifického klienta (pomocí MAC adresy).

Vyzkoušíme, jestli je vše nastaveno správně – připojíme se na stanici s Windows 8. Přiřadíme stanici do domény ITAcademy.local a necháme přidělit IP adresu pomocí DHCP serveru automaticky. Jméno a doménu nastavíme v systémových informacích (PC info), které najdeme v ovládacích panelech (kolonka Systém a zabezpečení -> Zobrazit název tohoto počítače), klikneme na tlačítko Změnit nastavení – v následujícím okně se lehce změní jméno a doména počítače. Jméno počítače má být výstižné a nejlépe krátké, protože slouží k jednoznačné identifikaci v síti – aby nedošlo k záměně, můžeme doplnit i popis počítače, který změníme ve stejném dialogu jako jméno.

Zadáme Je členem domény: ITAcademy.local. Budeme vyzváni, abychom zadali heslo k účtu, který může měnit doménu nebo ji přidávat, v našem případě to je administrátorský účet. Mělo by se objevit oznámení, že jsme v doméně (Vítejte v doméně), potom už jen restartujeme stanici a v následném přihlášení jsme již členy domény. Adresa se přiděluje automaticky od serveru, pokud nezadáme statickou. Nebo se dá změnit vlevo dole na hlavní liště, klikneme pravým tlačítkem na připojení -> Otevřít centrum síťových připojení a sdílení -> Změnit nastavení adaptéru -> vybereme správné připojení a otevře se dialog Připojení k místní síti,

kde najdeme Protokol IP verze 4 (TCP/IPv4) -> zde zaškrtneme, že chceme adresu získat automaticky ze serveru DHCP a adresu serveru DNS.

Otevřeme příkazovou řádku (v nabídce Metro napíšeme cmd a volbu potvrdíme), kde zadáme příkaz ipconfig – vidíme přiřazenou adresu od DHCP serveru. Příkazem nslookup názevServeru, získáme jejich IP adresy. Zadáme název DHCP i DNS severu. Nyní bychom měli mít základní funkčnost.

6.3 Active Directory, základní možnosti nastavení

Administrátor musí mít dokonalý přehled o tom, kdo může měnit konfigurace v počítači a kam smí přistupovat. Pomáhají nám k tomu vztahy důvěryhodnosti mezi doménami a zásady skupiny.

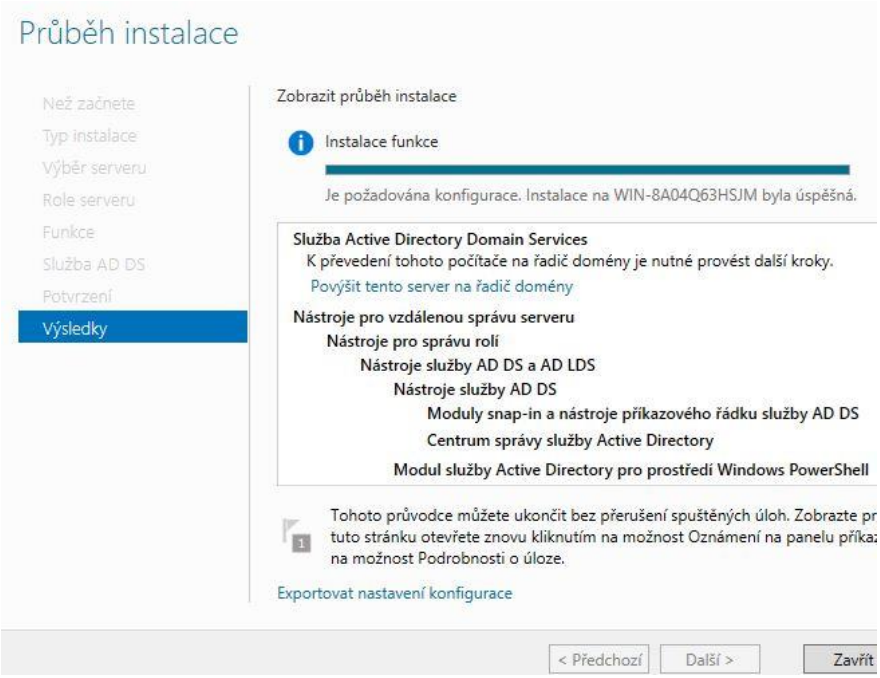
6.3.1 Struktura Domain Services

Importujeme servery do Hyper-V jako v minulém cvičení – Server_ITAcademy, Server_SW_ITAcademy, Server_HW_ITAcademy, stanici Windows8 a nově také server Server_IT. Tentokrát přidělíme statickou IP adresu sami, jak se to dělá, je popsáno v tématu 2.

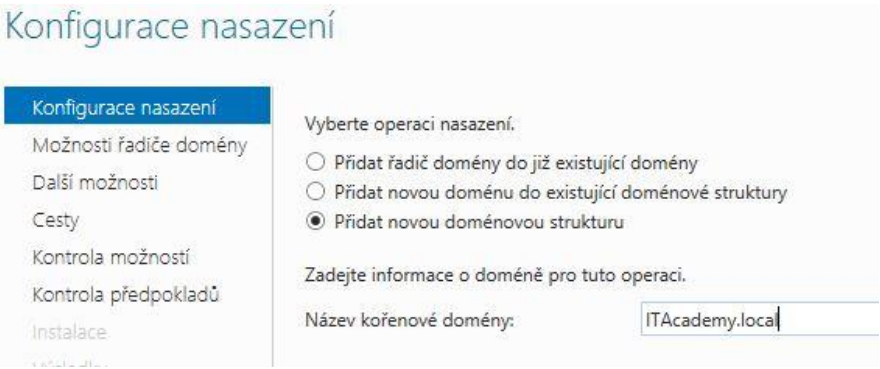
- Server_ITAcademy: 10.11.12.1/24
- Server_SW_ITAcademy: 10.11.12.2/24
- Server_HW_ITAcademy: 10.11.12.3/24
- Server_IT: 10.11.12.4/24
- Stanice Windows8: 10.11.12.5/24

Doménovým řadičem bude server Server_ITAcademy, nainstalujeme na něj Active Directory Domain Services a potom ho povýšíme na doménový řadič. To uděláme ve Správci serveru -> Přidat role a funkce (buď v Řídícím panelu nebo nahoře v levém menu v položce Správa) -> Služba Active Directory Domain Services. Potvrdíme instalaci a po úspěšném doběhnutí se v tomtéž okně zobrazí nabídka Povýšit tento server na řadič domény. V dřívějších verzích Windows Server se povýšení dělalo přes nástroj dcpromo spuštěný v příkazové řádce, Microsoft se ale rozhodl o zjednodušení a obě části se provádí ve správci serveru.

Druhý způsob spuštění je v horním menu, v Oznámení se objeví žlutý vykřičník, kde můžeme konfiguraci dokončit.



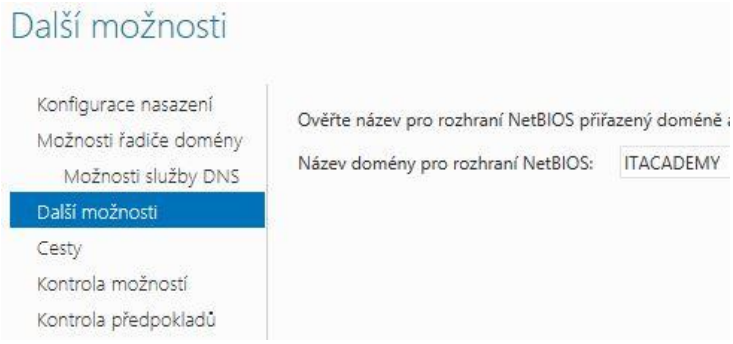
Obr. 23: Instalace AD DS



Obr. 24: Přidání nové doménové struktury

Vytváříme úplně novou doménovou strukturu (zaškrtneme Přidat novou doménovou strukturu) a zadáme název ITAcademy.local. Na další stránce necháme zaškrtnuté pole DNS a Globální katalog a úroveň funkčnosti doménové struktury nastavíme na Windows Server 2012 – to znamená, že v naší infrastruktuře nebude starší verze serverového operačního systému než WS 2012. Úrovní určujeme, jaký

typ řadičů budeme využívat. Obecně nesmí být starší než verze Windows 2003. Vyplníme heslo, kdybychom chtěli resetovat nastavení (8Cisco16) a zobrazí se chybová hláška o DNS – tu můžeme přeskočit, DNS nastavíme později.



Obr. 25: Doménové jméno NetBIOS

V dalším kroku zadáme název NetBIOS – ITACADEMY. V tomto názvu nesmí být tečky a mnoho dalších znaků, nesmí přesáhnout délku 15 znaků. V celém názvu domény se tečky používají pouze jako oddělovač částí.

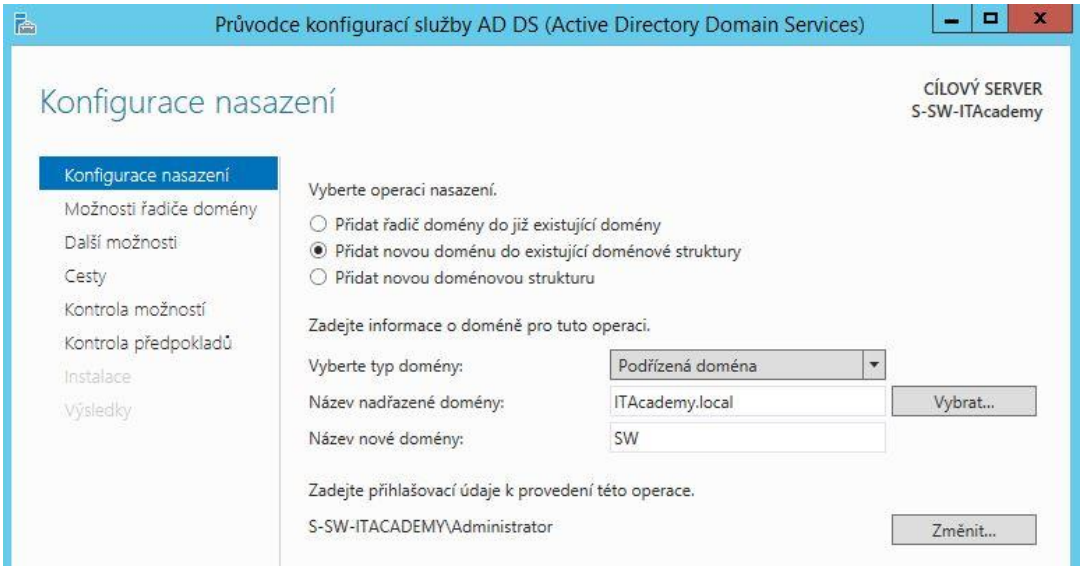
Při volení úložiště doporučuji nechat vše ve výchozí cestě. Při závěrečném shrnutí si můžeme nechat ukázat skript pro PowerShell, který se dá využít při konfiguraci dalších zařízení. Nakonec po instalaci se provede restart systému (pokud jsme nezaškrtli automatické restartování, nyní restartujeme manuálně) a po následném nalogování se již přihlásíme do ITACADEMY/Administrator.

V těchto krocích se na pozadí provádí příkazy `ADprep /forestprep`, `ADprep /domainprep`. Tím připravujeme schéma, které se následně uloží do hlavního řadiče.

Na server Server_SW_ITAcademy přidáme AD DS stejně jako v předchozím kroku a na něm nastavíme IP adresu DNS serveru (ve stejném okně jako jsme nastavovali statickou IP adresu počítače – pod tímto je Použít následující adresy serverů DNS: napíšeme adresu serveru z nadřazené domény 10.11.12.1)

Ze serveru teď vytvoříme řadič podřízené domény SW.ITAcademy.local ke kořenové doméně ITAcademy.local. Vybereme tedy znovu žlutý vykřičník a zde Povýšit tento server na řadič domény. Stejné kroky jako v předchozí části, ale u možností Vyberte operaci nasazení, zaškrtneme Přidat novou doménu do existující

doménové struktury. Níže vybereme, že chceme Podřízenou doménu, název nadřazené domény bude ITAcademy.local a název nové domény SW. Zadáme přihlašovací údaje k účtu administrátora a počítač už sám poskládá plně kvalifikovaný název domény.



Obr. 26: Přidání další domény do existující struktury

Odškrtneme DNS a Globální katalog, to neinstalujeme, jeden již máme, takže bude použita stávající infrastruktura DNS.

Stejným způsobem vytvoříme serverový řadič podřízené domény v doméně HW.ITAcademy.local ke kořenové doméně ITAcademy.local.

Nově jsme importovali server Server_IT, ze kterého chceme vytvořit vedlejší strom napojený na doménu ITAcademy.local. Na ten přidáme AD DS, vytvoříme ze serveru řadič domény a tentokrát DNS instalujeme. Jedinou změnou je pouze, že místo Podřízená doména, zadáme druhou možnost Doména stromové struktury. Další kroky jsou již pro nás známé.

Celou strukturu kontrolujeme v Domény a vztahy důvěryhodnosti služby Active Directory (horní menu -> Nástroje). V levém menu vidíme naši strukturu domén, zde můžeme zjistit, komu naše domény důvěřují (pravé tlačítko nad

doménou -> Vlastnosti). SW.ITAcademy a HW.ITAcademy domény budou důvěřovat ITAcademy a obráceně, vidíme také, že je to jejich nadřazená doména. Ve správci můžeme přidávat nové vztahy důvěryhodnosti (např. jednosměrný příchozí nebo odchozí vztah důvěryhodnosti domény SW.ITAcademy s doménou IT, druhá strana má ale i možnost vztah přijmout či odmítnout).

6.3.2 Skupiny a uživatelé Active Directory

V minulé části jsme využili pro ukázku server Server_ITAcademy a klientskou stanici Windows8. Do prostředí Hyper-V přidáme ještě jednu totožnou stanici a nazveme ji Windows81.

Server má IP adresu 10.11.12.1, je primárním řadičem a má nainstalované DNS. Přihlásíme se na stanici Windows8 a Windows81 jako účet Student a nastavíme IP adresy a adresu serveru DNS (to bude adresa na Server_ITAcademy)

- Windows8 – 10.11.12.13/24
- Windows81 – 10.11.12.14/24

Ověříme spojení ping na server z obou stanic (otevřeme příkazovou řádku, cmd -> ping 10.11.12.1), server musí odpovídat.

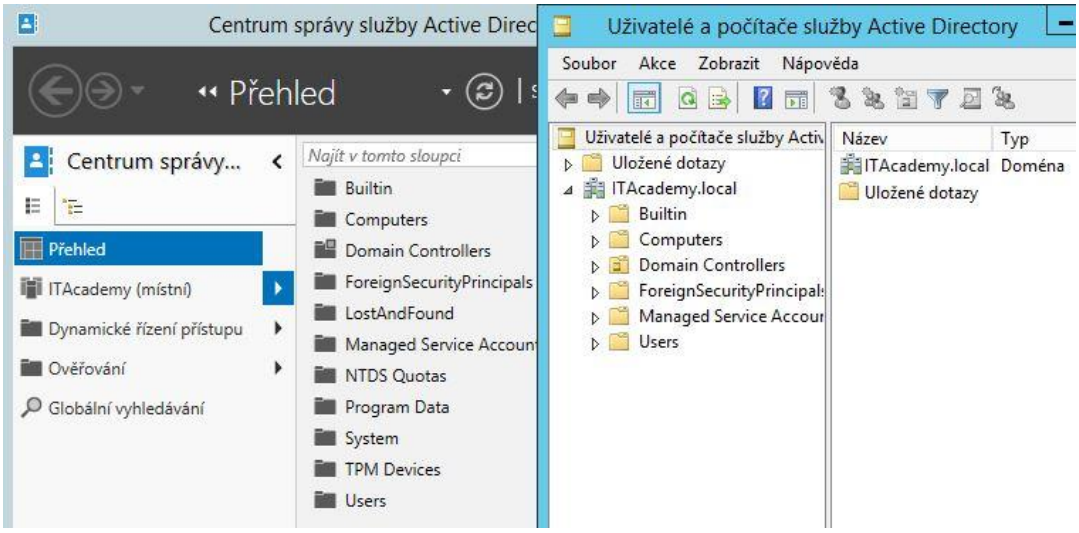
Přidáme obě stanice do domény ITAcademy.local (popsáno výše -> Je členem domény) a už můžeme zkoušet základní administraci.

Na serveru musíme být přihlášeni za uživatele s příslušnými právy, přihlásíme se na Administrator, vytvoříme organizační jednotku a pojmenujeme ji Vedeni. K ní přidáme Uctarna a Zamestnanci. Provedeme to ve Správci serveru nebo v Uživatelé a počítače služby Active Directory. V levé nabídce menu vybereme doménu, do které chceme OU přidat a klikneme na ni pravým tlačítkem -> Nový -> Organizační jednotka, zaškrtneme možnost Chránit před nechtěným odstraněním. Můžeme zde také zvýšit úroveň funkčnosti domény, přidat účty nebo navigační uzly. V jednotce Provoz vytvoříme stanici Montaznik (pravým tlačítkem na Provoz -> Nový -> Počítač). Podíváme se do složky Počítače pod ITAcademy.local, kde najdeme stanici Windows8, tu přesuneme také do OU Zamestnanci (pravým tlačítkem na název stanice -> Přesunout… -> zadáme, kam chceme přesouvat).

Vytvoříme skupinu Ucetni v OU Uctarna (pravým tlačítkem na Uctarna -> Nový -> Skupina), rozsah bude globální a typ skupiny se zabezpečením. Práva, která přidáme skupině, získají všichni uživatelé v ní přiřazené, nemusíme tedy oprávnění k přístupu ke složkám nastavovat jednotlivým účtům zvlášť.

Vytvoříme skupinu Vyroba v OU Zamestnanci, Reditele v OU Vedeni. Vytvoříme uživatele Ucetni1 v OU Uctarna (heslo 8Cisco16, zaškrtneme heslo je platné stále), následně přidáme Ucetni1 do skupiny Ucetni (podobné obrázky jako v tématu 1).

Vytvoříme Reditel v OU Vedeni, přidáme ho do skupiny Reditele. Montaznik1 v OU Zamestnanci bude patřit do skupiny Vyroba. Uživatele můžeme přidávat i hromadně, stačí je označit. V našich možnostech teď můžeme nastavit přihlašovací hodiny (např. nechceme, aby se Montaznik1 přihlašoval o víkendu, nepovolíme sobotu a neděli) nebo zjistit počet uživatelů ve skupině.



Obr. 27: Centrum správy služby AD

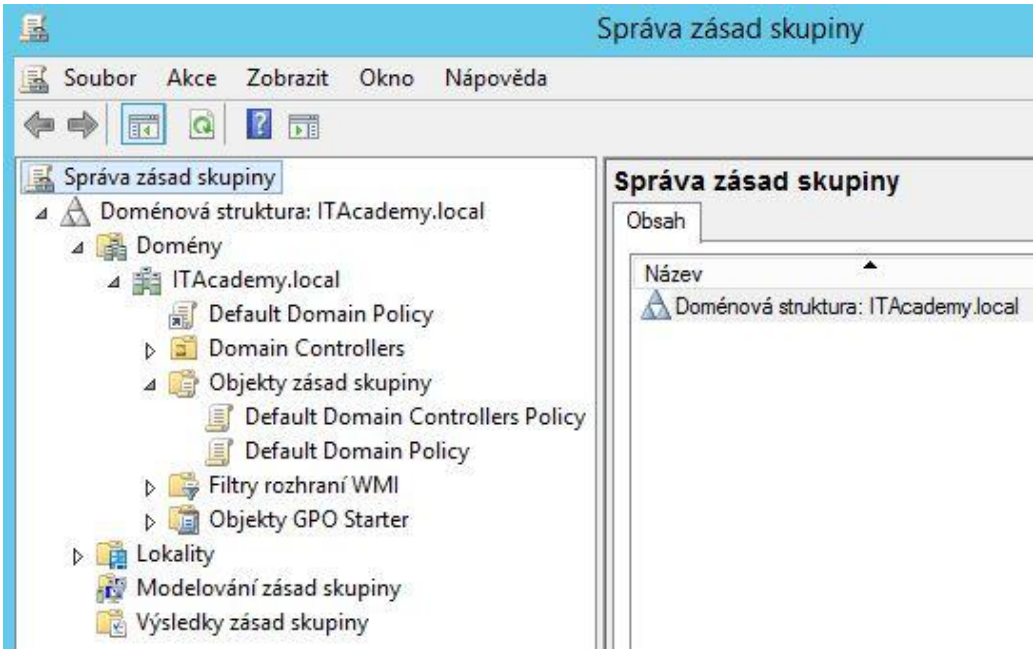
6.3.3 Správa zásad skupiny Active Directory

Pomocí zásad skupiny (Group Policy) můžeme šifrovat komunikaci, zabezpečit oprávnění na složkách, oprávnění na registrech nebo zajistit, aby všichni uživatelé volili komplexní hesla.

Ve Správci serveru otevřeme Správu zásad skupiny (v pravém menu -> Nástroje), můžeme si všimnout, že zde již máme default domain policy, která se vytváří automaticky a obsahuje už několik zásad zabezpečení, které se aplikují na

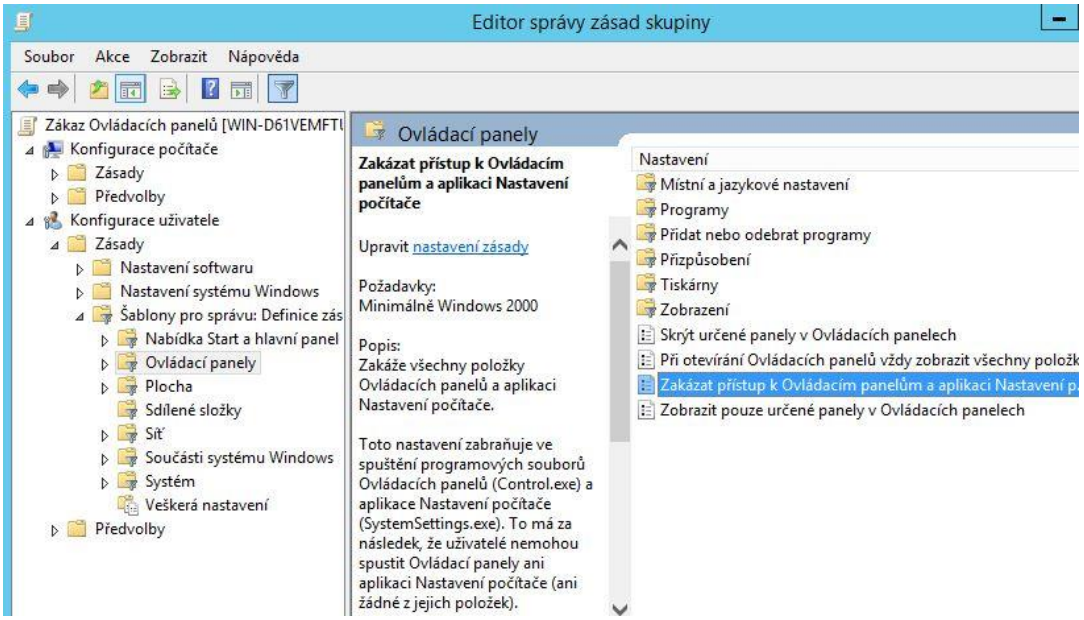
celou doménu. Přesněji obsahují zásady účtů, ve kterých jsou pravidla pro hesla, uzamčení účtů a modul Kerberos. Vedle vidíme default domain controllers policy, pravidla, která platí pro všechny řadiče v doméně.

V tomto správci můžeme nastavit skupinám, uživatelům a ostatním objektům, jaké činnosti budou moci vykonávat.



Obr. 28: Struktura ITAcademy.local a skupiny v ní

Zakážeme skupině Vyroba, aby přistupovala k ovládacím panelům. Klikneme pravým tlačítkem na Objekty zásad skupiny -> Nový -> do dialogu napíšeme název Zákaz ovládacích panelů a po potvrzení se zobrazí pod ostatními pravidly. Znovu na něj klikneme pravým tlačítkem a vybereme Upravit. Rozbalíme Konfigurace uživatele -> Šablony pro správu: Definice zásad. Zde máme spoustu možností zahrnujících zákaz sdílet složky, zákaz přístupu k příkazovému řádku, nastavení programů, které se spustí po zapnutí počítače nebo skrytí některých aplikací jako třeba Správce úloh. Vybereme Ovládací panely a pravým tlačítkem klineme na Zakázat přístup k Ovládacím panelům -> Zapnout filtr -> Upravit.



Obr. 29: Přidělení nových zásad skupiny

V dialogu zaškrtneme Povoleno, což znamená, že zapneme zákaz. Vrátíme se do Správy zásad skupiny a vybereme náš Zákaz ovládacích panelů a v oddělení Filtrování zabezpečení odebereme Authenticated Users, klikneme na Přidat a zadáme skupinu Vyroba -> Kontrola názvů. Ještě připojíme pravidlo k doméně a provedeme update pomocí CPUpdate.exe, což zajistí funkčnost. Pravým tlačítkem na ITAcademy.local -> Připojit existující objekt zásad skupiny -> vybereme Zákaz ovládacích panelů. Zapneme příkazový řádek a zadáme příkaz `gpupdate/force`. Odteď budou uživatelům ve skupině Vyroba chybět Ovládací panely. Pokud chceme povolit ve skupině přistupovat k panelům pouze jednomu člověku, i to lze udělat, ale musíme dávat pozor, v jakém pořadí pravidla připojujeme. Pořadí se dá měnit pomocí šipek. Nejdříve tedy uživateli musíme přístup povolit a teprve potom zakázat všem ostatním.

7 Závěr a doporučení

Informatika je obor, který se neustále mění. Pokud se zabýváme touto oblastí, musíme počítat s tím, že učit se budeme celý život. Myslím si, že tato práce se bude moci použít i v dalších letech pro pozdější verze systémů Windows Server. Slouží hlavně pro studenty na školách, kteří se chtějí co nejrychleji naučit základy, jak spravovat jednoduchou síť, nebo pro již pracující správce, kteří by ji mohli brát jako rychlou pomůcku. Popřípadě pro studenty, kteří ještě nevědí, co přesně v budoucnu dělat a zajímalo by je, jak vypadá svět správce serverů. Nemusí číst desítky knih, to nejdůležitější mají v této práci. Přesto je pro profesionální přístup a široký rozsah vědomostí důležité přečíst mnohem více a získat cenné zkušenosti v praxi.

Já sama jsem si potvrdila, že nestačí přečíst jednu knihu, aby se z vás stal expert na danou oblast. Ne vždy jsem našla spolehlivý návod, který v mém, i když jednoduchém, schématu fungoval. To ani není možné, protože je tolik možností, jak sestavit infrastrukturu sítě. Je potřeba zkoumání a zájem. Doufám, že jestli tuto práci bude číst začínající student, vzbudí se v něm pozornost a začne se o správcovství systémů více zajímat.

8 Seznam použité literatury

[1] DRÁB, Martin. *Jádro systému Windows: Kompletní průvodce programátora*. 1. vyd. Brno: Computer Press, 2011. 472 s. ISBN 978-80-251-2731-5.

[2] Pearson IT Certification. *Installing and Configuring Windows Server 2012 R2* [online]. 2014, poslední revize: 16. 8. 2015 [cit. 2015-08-17]. Dostupné z: http://www.pearsonitcertification.com/articles/article.aspx?p=2248808&seqNum=2

[3] KENCKI, Adam. *Procházka historií Microsoft Windows 1. díl* [online]. 2. 12. 2010, poslední revize: 10.8. 2016 [cit. 2016-08-10]. Dostupné z: http://pcworld.cz/software/prochazka-historii-microsoft-windows-1-dil-16395

[4] Microsoft TechNet. *Přehled novinek ve Windows Serveru 2012 R2* [online]. 5. 9. 2013, poslední revize: 6. 8. 2015 [cit. 2015-08-06]. Dostupné z: http://www.zive.cz/clanky/prehled-novinek-ve-windows-serveru-2012-r2/sc-3-a-170204/default.aspx

[5] Daquas. *Windows Server 2012 R2 – co je nového?* [online]. 25. 9. 2013, poslední revize: 3. 8. 2015 [cit. 2015-08-06]. Dostupné z: http://www.daquas.cz/articles/621-windows-server-2012-r2-co-je-noveho

[6] Microsoft. *Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012* [online]. 5. 3. 2014, poslední revize: 18. 8. 2015 [cit. 2015-08-19]. Dostupné z: https://technet.microsoft.com/cs-cz/library/Hh831669.aspx

[7] Microsoft TechNet. *Server Message Block Overview* [online]. 24. 6. 2013, poslední revize: 20. 8. 2015 [cit. 2015-08-20]. Dostupné z: https://technet.microsoft.com/en-us/library/hh831795.aspx

[8] PCWorld. *Procházka historií Microsoft Windows – 1. díl* [online]. 2. 12. 2010, poslední revize: 21. 8. 2015 [cit. 2015-08-21]. Dostupné z: http://pcworld.cz/software/prochazka-historii-microsoft-windows-1-dil-16395

[9] VÝŠEK, Ondřej. *Porovnání první a druhé generace virtuálních strojů v Hyper-V 2012 R2* [online]. 27. 11. 2013, poslední revize: 7. 8. 2016 [cit. 2016-08-07]. Dostupné z: http://www.optimalizovane-it.cz/windows-server-2012/porovnani-prvni-a-druhe-generace-virtualnich-stroju-v-hyper-v-2012r2.html

[10] PRICE, Brad. *Active Directory: optimální postupy a řešení problémů*. 1. Vyd. Brno: CP Books, 2005. 381 s. ISBN 80-251-0602-0.

[11] ALLEN, Robbie a LOWE-NORRIS, Alistair G. *Active Directory: Implementace a správa Microsoft Active Directory.* 1. Vyd. Praha: Grada Publishing, a.s., 2005. 648 s. ISBN 80-247-0973-2.

[12] TULLOCH, Mitch. *Installing and Configuring Windows Server 2012.* 1. Vyd. Washington: Microsoft Press, 2012. 609 s. ISBN 978-0-7356-7310-6.

[13] BITTO, Ondřej. *Microsoft Windows 8: Podrobná uživatelská příručka.* 1. Vyd. Brno: Computer Press, 2012. 328 s. ISBN 978-80-251-3776-5.

[14] BURDA, Zdeněk. *Využití LDAPu v praxi* [online]. 22. 7. 2007, poslední revize: 9. 8. 2016 [cit. 2016-08-09]. Dostupné z: http://ldap.zdenda.com/

[15] PANEK, William. *MCSA Windows Server 2012 complete study guide: exams 70-410, 70-411, and 70-412*. Sybex, 2013. 922 s. ISBN 11-185-4407-2.

[16] Návody a cvičení na předmět Operační systémy 1, *Windows Server 2008 R2*. Dostupné z: http://www.horalek.org/os/index.html