Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Služby systému Windows Server 2012 a jejich konfigurace ve vybrané firmě

Bakalářská práce

Autor: Ondřej Pipek
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Andrea Vokálová

Hradec Králové duben 2017

Prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval pod vedením vedoucí práce Ing. Andrey Vokálové samostatně a s použitím uvedené literatury.

.....

V Hradci Králové dne 6.4.2017 Ondřej Pipek

Poděkování:

Děkuji vedoucí bakalářské práce Ing. Andree Vokálové za cenné rady, ochotu a připomínky při zpracování této práce.

Anotace

V současné době je velmi mnoho zdrojů týkající se informatiky. Pro některé správce sítě nemusí být jednoduché nalézt podstatné informace týkající se konfigurace a správy Windows Serveru 2012 R2.

Cílem této práce je popsat metodiku pro správu a konfiguraci víceúčelového serveru na platformě Microsoft Windows Server 2012 R2 a jeho využití v malé či střední firmě.

První část práce se zabývá popisem vybraných základních služeb, rozebírá jejich principy, funkce a přínosy při použití. V další kapitole je představena analýza stávající firemní infrastruktury.

Praktická část práce popisuje instalaci a konfiguraci zmíněných služeb, poslední kapitola v praktické části se týká monitorování serveru, jakým způsobem a proč monitorování provádět. Postupy konfigurace jsou vytvořeny tak, aby je zvládl i méně zkušený a problematiky znalý správce sítě.

Klíčová slova:

Microsoft Windows Server 2012 R2, Dynamic Host Configuration Protocol, Domain Name System, Active Directory, Group Policy, Windows Server Update Services

Annotation

Title: Services of Windows Server 2012 and their configuration in a selected company

There is a lot of resources concerning computer science these days. It might be difficult for some network administrators to find relevant information regarding the configuration and management of Windows Server 2012 R2.

The main goal of this thesis is to describe the management and configuration methodic of a multifunctional server on the Microsoft Windows Server 2012 R2 platform and it's utilization in a small or medium company.

In the first part, the paper aims on the description of a certain network services and explains their principles, function and benefits. The next chapter analyzes the current business infrastructure.
The practical part of the thesis describes the installation and configuration of the above mentioned services, the last section of the practical part concerns the monitoring of the server, how and why this needs to be done. The configuration procedures are designed to be understandable even for the less experienced and knowledgeable network administrators.

Key words:

Microsoft Windows Server 2012 R2, Dynamic Host Configuration Protocol, Domain Name System, Active Directory, Group Policy, Windows Server Update Services

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek a vybraných pojmů

WS2012	Windows Server 2012 R2
BOOTP	Bootstrap Protocol
IPv4	Internet Protocol version 4
WINS	Windows Internet Name Service
LLMNR	Link-Local Multicast Name Resolution
TTL	Time To Live
FQDN	Fully Qualified Domain Name
HR	Human resources
LDAP	Lightweight Directory Access Protocol
NTLM	NT LAN Manager
VPN	Virtual Private Network
WSUS	Windows Server Update Services
VLAN	Virtuální LAN
SFP	Small Form-factor Pluggable
L2TP	Layer 2 Tunneling Protocol
PPTP	Point-to-Point Tunneling Protocol
SSL	Secure Sockets Layer
CRM	Customer relationship management
GHz	Gigahertz
RAM	Random-access memory
W	Watt
TB	Terabyte
SAS	Serial Attached SCSI
iDrac	Integrated Dell Remote Access Controller
RAID	Redundant Array of Independent Disks
V	Volt
SYSREP	System Preparation tool
NTFS	New Technology File Systém
BIOS	Basic Input-Output Systém
GUI	Graphical User Interface
TCP	Transmission Control Protocol
RDP	Remote Desktop Protocol

Úvod

Informační technologie získávají na popularitě, stávají se nezbytným pomocníkem v každodenním životě. Téměř každý člověk v České republice dnes používá počítač, chytrá zařízení a s tím související benefity. Skutečnost je tedy taková, že informační technologie nás velmi ovlivňují. Vývoj je velmi rychlý a jen těžko se s ním drží krok.

Zaměstnanci firem nejsou výjimkou, požadují se od nich základy znalosti práce na počítači. Zaměstnanci komunikují pomocí e-mailů s klienty či ostatními kolegy, sdílejí informace v rámci firmy, prezentují firmu skrze webové stránky, používají interní systémy pro zefektivnění práce s klienty a mnoho dalšího.

Základním prvkem firemní sítě, který tyto funkcionality zajišťuje, je jeden nebo několik serverů, měly by být dostatečně výkonné. Na nich musí být nainstalován operační systém. V této práci se budeme zabývat nejnovějším operačním systémem od firmy Microsoft, a to Windows Server 2012 R2 (dále už jen WS2012).

Autor vychází ze zkušeností, které získal praxí ve firmě Centrum andragogiky, s.r.o. Ve firmě působí od roku 2013 jako správce sítě. Stará se o provoz tří firemních serverů a firemních webů, zajišťuje technickou podporu pro zaměstnance firmy, instaluje nová zařízení, tedy počítače, mobilní telefony, tablety, stará se o plynulý chod firemních školení po technické stránce, například o ozvučení a projekci, připravuje podklady pro vedení firmy pro výběr nových zařízení, opravuje, případně řeší opravy tiskáren, nastavuje počítače nových zaměstnanců a podobně.

O společnosti Centrum andragogiky

Centrum andragogiky je vzdělávací a poradenská společnost, poskytující již od roku 2006 komplexní systematické firemní vzdělávání, zefektivňování činnosti firem a organizací. „*Pořádáme otevřené i uzavřené vzdělávací akce, konference, diskuse, nabízíme poradenství, analýzy vzdělávacích potřeb a realizaci uceleného programu. Své služby nabízíme nejen klientům z výrobní a nevýrobní podnikatelské sféry, ale také nepodnikatelským subjektům z různých odvětví. Pro naše klienty jsme již z EU získali téměř 450 milionů korun. Na vlastní projekty jsme čerpali z ESF necelých 37 milionů korun, díky nimž zvýšilo svou odbornost několik stovek pracovníků*“(Kohoutová, 2015).

Firma pořádá konference, kulturní a společenské akce, například rozhovory se známými osobnostmi (Otakar Brousek, Miroslava Besserová), týmové hry, příměstské tábory, lekce jógy, počítačové lekce pro seniory, stylové večírky, svatby.

V roce 2014 dostavělo Centrum andragogiky nové školicí středisko ve Svobodných Dvorech. Tato atypická stavba získala ocenění Stavby roku Královehradeckého kraje 2015 a ocenění TOP INVEST 2014 za nejlepší investiční záměr. Stavba vznikla z bývalé cihelny. (Centrum andragogiky, © 2017)

V čele této společnosti stojí PhDr. Marie Jírů, její majitelka, která získala již mnoho ocenění v oblasti vzdělávání.

Hlavním cílem práce je vytvořit metodiku správy a konfigurace víceúčelového serveru, která by mohla pomoct začínajícím správcům sítě. Práce je rozdělena na dvě části, a to teoretickou a praktickou část.

Začneme krátkou kapitolou o analýze stávajícího prostředí ve firmě Centrum andragogiky. Následuje teoretická část, kde si vysvětlíme vybrané síťové služby, které jsou nezbytné pro fungování WS2012. Následuje popis poštovního serveru Microsoft Exchange 2013 a jeho možností.

V praktické části bude popsána instalace, poté zprovoznění a následně správa základních služeb na serveru. Práce se nebude věnovat popisu všech služeb, které Windows server nabízí. Bylo by to nad rámec této práce. Práce se zaměřuje na služby nezbytné pro chod menší až střední firmy.

1. TEORETICKÁ VÝCHODISKA

Pro nakonfigurování víceúčelového serveru byly použity následující technologie: Microsoft Windows Server 2012, DHCP Server, Active Directory Domain Services, DNS Server, File Server

1.1 Microsoft Windows

Je to už více než 30 let, co se firma Microsoft věnuje vývoji operačních systémů. Společnost byla založena v roce 1975 Billem Gatesem a Paulem Allenem. Nyní má firma široké portfolio produktů a služeb.

Vše to začalo, když společnost v roce 1985 vydala svůj první operační systém Windows 1.0. V této verzi bylo dostupné velmi jednoduché grafické rozhraní, ve kterém bylo možné spouštět programy pro MS DOS.

Další verze pak disponovaly rozrůstajícím se množstvím funkcí jako podpora grafické a zvukové karty, USB zařízení, síťového rozhraní, přidání sofistikovaných klávesových zkratek, souborového manažeru, možnosti přehrát si video a dalších.

Velmi podstatnou věcí je uživatelské rozhraní. Operační systém se pomalu měnil, stával se stále přívětivějším a intuitivnějším. Podobně se vyvíjely i aplikace pro tyto operační systémy. Úplně na začátku nebyla jiná volba než aplikace ovládat v textovém prostředí. (McCaskill, 2016)

První serverová edice operačního systému, Windows nesoucí označení Windows Server je Windows Server 2003. Tato edice poprvé podporovala nezbytné služby, jako jsou Active Directory, DNS Server, DHCP Server, Group Policy. Dalo by se tedy říct, že tato verze je základ všech pozdějších potomků.

1.1.1 Microsoft Windows Server 2012 R2

WS2012 je operační systém od společnosti Microsoft, který byl vydán v roce 2013. Je to nejnovější revize, má společné jádro a další součásti systému s Windows 8.1.

WS2012 má přes 300 nových funkcí a je to první verze Windows Server, kterou lze propojit s cloudem. Staví na funkcích, které známe z Windows Server 2008 R2 (Minasi, 2014).

Cloud je populární technologie, která je postavena na principu uchovávání dat mimo lokální server. Má mnoho výhod i nevýhod. Mezi největší výhody patří jeho flexibilita. Flexibilitou je myšlená dostupnost dat odkudkoliv a kdykoliv. Mezi největší nevýhody patří ztráta kontroly nad daty, musíme se spolehnout na poskytovatele cloudu.

Administrátory jistě potěší, že aktualizace z Windows Server 2012 na Windows Server 2012 R2 je velmi snadná a nenáročná. Nemělo by dojít k žádné ztrátě dat. V podstatě stačí pouze vložit instalační medium do DVD mechaniky, spustit instalaci a po restartu by mělo být vše hotové. V praxi samozřejmě k určitým problémům dojít může.

WS2012 tvoří čtyři edice: Foundation, Essentials, Standart a Datacenter. Liší se metodou distribuce, limity na HW a podporou virtualizace. Tato práce se bude zabývat edicí Standard, která je nejrozšířenější.

Edice	Ideální pro	Porovnání funkcí	Limity
Datové centrum	vysoce virtualizovaná prostředí privátního a hybridního cloudu	Veškeré funkce systému Windows Server s neomezeným počtem virtuálních instancí	
Standart	prostředí s nízkou hustotou nebo nevirtualizovaná prostředí	Veškeré funkce systému Windows Server se dvěma virtuálními instancemi	
Essentials	Prostředí malých podniků pro servery s maximálně dvěma procesory	Jednodušší rozhraní, předem nakonfigurované možnosti připojení ke cloudovým službám; jedna virtuální instance systému Essentials	maximálně 25 uživatelů, maximálně 2 procesory
Foundation	úsporný jednoprocesorový server pro obecné účely	Funkce serveru pro obecné účely bez oprávnění k virtualizaci	maximálně 15 uživatelů, maximálně 1 procesor

Tabulka 1: Srovnání edic WS2012

Zdroj: Vlastní zpracování

Největší změny:

- **Active Directory** – nyní zahrnuje několik užitečných nových funkcí Active Directory Certificate Services, Active Directory Rights Managment Services a Active Directory Domain Services. Důraz je kladen na rychlé a jednoduché aplikování GPO. Grafické rozhraní se také dočkalo vylepšení.
- **Klonování doménových kontrolérů** – možnost zkopírování existujícího doménového řadiče.
- **Active Directory Recycle Bin –** další novinkou je přidaný koš. Je tu pro případ obnovení smazané položky v AD.

- **Work Folders –** umožňuje zpřístupnit souborové úložiště bezpečně do internetu. Podporuje práci offline . Soubory jsou uloženy na serveru i u klienta.
- **Workplace Join –** umožňuje nám nový stupeň ověření v rámci doménového prostředí. Doposud jsme měli buď doménový počítač, který je pro správce zcela důvěryhodný a plně pod jeho kontrolou, nebo počítač, který do domény připojen není, je tedy plně pod kontrolou uživatele. Nyní máme možnost využít jakýsi mezistupeň zvaný Workplace Join. Uživatel má stále počítač plně pod kontrolou, ale v Active Directory je zanesen záznam o tomto počítači a je tedy důvěryhodný.
- **Web Application Proxy** – umožňuje přímo ve Windows Serveru publikovat aplikace bezpečně ven do internetu.
- **Storage-tiering** – rozděluje automaticky data na ta, která používáme častěji, a ta která méně často. Podle toho se pak data přesouvají mezi rychlými a pomalejšími disky.
- **Duplikace běžících VMs** – od WS2012 umožňuje duplikaci virtuálních běžících strojů. (Minasi, 2014)

Minimální a doporučené systémové požadavky

Komponenta	Doporučené	Minimální
Procesor	3.1 GHz 64-bit nebo rychlejší	1.4 GHz 64-bit nebo rychlejší
Paměť	8 GB nebo víc	2 GB nebo víc
Disk	60 GB	160 GB a víc
Monitor	Super VGA (1024 x768) nebo vyšší	Super VGA (1024 x768) nebo vyšší
Ostatní	DVD mechanika, síťový adaptér	DVD mechanika, síťový adaptér

Tabulka 2: Minimální a doporučené systémové požadavky

Zdroj: Vlastní zpracování

1.2 DHCP Server

DHCP (anglicky Dynamic Host Configuration Protocol) je aplikační protokol z rodiny TCP/IP. Umožňuje klientským stanicím v síti komunikovat. DHCP server nastavuje nezbytnou sadu parametrů pro komunikaci v sítí. DHCP protokol je nástupcem BOOTP protokolu, který přiděloval IP adresy na neomezenou dobu.

Není nezbytné, aby stanice byla klientem DHCP serveru. V některých případech je lepší, aby byla stanice nastavena ručně. Ručně se nastavují síťové tiskárny, směrovače, servery atd., zkrátka zařízení, u kterých potřebujeme statickou IP adresu. Pokud by tiskárně přiděloval IP adresu DHCP server, bylo by nutné opakovaně na počítači nastavovat IP adresu, kam má tiskové úlohy posílat.

V malé či střední firmě je možnost klientským stanicím nastavovat nezbytnou sadu parametrů pro komunikaci v síti manuálně. Ale ve větších organizacích by tato možnost byla časově velmi náročná.

„Počítač, kterému se dynamicky přiděluje IPv4 adresa a konfigurace, se nazývá DHCPv4 klientem. Když takového klienta spustíte, klient obdrží z fondu IPv4 adres definovaných síťovému DHCP serveru 32bitovou IPv4 adresu. Tuto adresu má klient

přidělenou na určitou dobu – na dobu výpůjčky. Po uplynutí zhruba poloviny této doby se klient pokusí výpůjčku adresy obnovit. Když neuspěje, pokusí se kontaktovat jiný DHCP server. Neobnovené IPv4 adresy se vrací zpět do fondu adres. Pokud se klient dokáže spojit s DHCP serverem, avšak aktuální IP adresu není možné znovu přiřadit, dostane od DHCP serveru novou IPv4 adresu“ (Stanek, 2015).

Dostupnost DHCP serveru neovlivňuje spouštění operačního systému na stanici, ani autentifikaci a přihlášení uživatele na stanici. Klient DHCPv4 se snaží server vyhledat v průběhu spouštění, pokud neuspěje a dřívější výpůjčka stále platí, klient odešle na výchozí bránu signál ping. V případě úspěchu se pravděpodobně dozví, že se nachází ve stejné síti, kde obdržel původní adresu, tudíž bude moct adresu i nadále používat. V opačném případě, kdy dotaz selže, klient usoudí, že se nachází v jiné síti a nastaví si adresu IPv4 sám. Totéž udělá i v případě, když DHCP server není dostupný, nebo vyprší doba výpůjčky. Klienty DHCPv4 je možné spouštět i v situaci, kdy DHCP server není k dispozici.

1.2.1 Parametry nastavitelné pomocí DHCP

Mezi parametry, které se dají nastavit pomocí DHCP, patří:

- IP adresa,
- maska sítě,
- brána,
- DNS servery.

1.2.2 Porovnání výhod a nevýhod DHCP protokolu

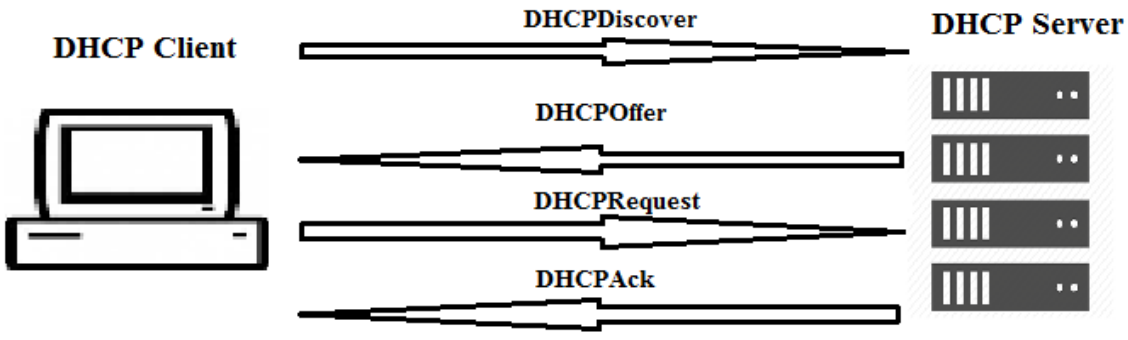
Výhody	Nevýhody
Bezpečná a spolehlivá konfigurace stanic. Protokol DHCP minimalizuje riziko chyby manuální konfigurací IP adres. Při ručním zadáváním IP mohou nastat dva problémy: prvním je chyba v psaní a druhým přidělení IP adresy, kterou již nějaká stanice používá.	V případě poruchy DHCP serveru bez záložního nebude žádné z klientských stanic přidělena nebo obnovena zápůjčka.
Snazší správa sítě.	Pokud je DHCP server nesprávně nakonfigurován, tyto nesprávné parametry se nám automaticky distribuují do klientských stanic.
Centralizovaná a automatizovaná správa sítě.	
Uživatel si nemusí sám nic nastavovat.	

Tabulka 3: Výhody a nevýhody DHCP protokolu

Zdroj: Vlastní zpracování

1.2.3 Princip přidělování IP adresy v DHCP

Klient žádá DHCP server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji má klient rezervovanou. Poté, co doba vyprší, smí server přidělit tuto adresu jiným klientům (Himanshu, 2013).



Obrázek 1: Proces zapůjčení IP adresy
Zdroj: Vlastní zpracování

Celý proces zápůjčky IP adresy klientovi:

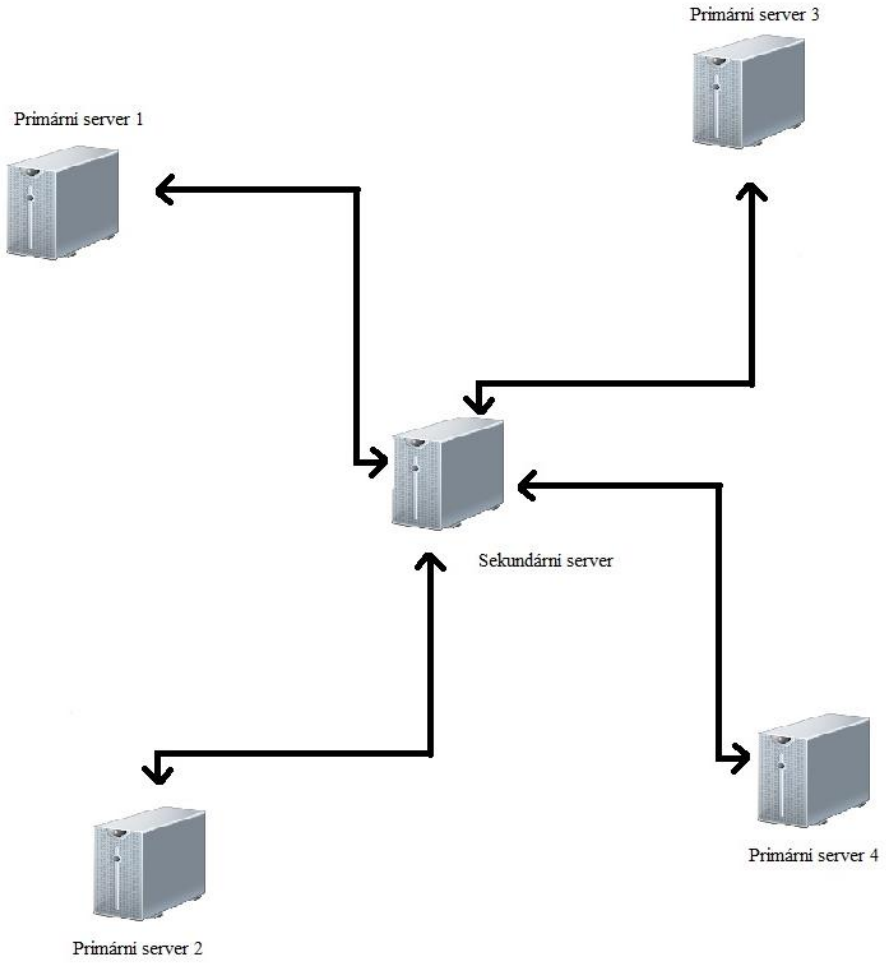
1) Klient DHCP požaduje IP adresu prostřednictvím všesměrového vysílání DHCPDiscover do lokální sítě.
2) Klientovi je nabídnuta IP adresa, když server DHCP reaguje zprávou DHCPOffer, která obsahuje adresu IP a informace o konfiguraci zápůjčky.
3) Klient potvrdí nabídku výběrem nabízené adresy a odpoví serveru zprávou DHCPRequest.
4) Klientovi je přidělena adresa. Server DHCP potvrdí klientovi zápůjčku prostřednictvím zprávy DHCPAck.
5) Poté co klient přijme DHCPAck, nakonfiguruje si vlastnosti protokolu TCP/IP a připojí se k síti. (Himanshu, 2013)

1.2.4 Zastupitelnost DHCP serveru

V rámci plánování sítě je potřeba si rozmyslet, kolik DHCP serverů nainstalovat. Pokud jeden DHCP server selže, měl by být zálohovaný. Je tedy vhodné do každého segmentu sítě nainstalovat alespoň dva DHCP servery. WS2012 umožňuje v případě selhání jednoho DHCP serveru zajistit převzetí služeb záložním serverem. Tímto máme možnost zajistit vysokou dostupnost služeb DHCP. Servery si mezi sebou synchronizují databázi dat, a to ve dvou režimech:

- **vyrovnávání zatížení (Load Balance)** – v tomto režimu dva DHCP servery současně poskytují IP adresy a své prostředky klientským stanicím v dané podsíti. Je potřeba nastavit podíl procentuálního zatížení, v kterém si mají servery požadavky rozdělit. Nejčastěji to bývá 50/50, ale je možné nastavit i jiný poměr, například 70/30, kdy jeden server bude zpracovávat 70 % požadavků a druhý pouze 30 %.
- **aktivní pohotovostní režim (Hot Standby)** – v této situaci máme jeden ze serverů jako primární a druhý sekundární. Sekundární, záložní zastoupí primární, pokud primární selže nebo mu dojdou adresy, které by mohl přidělit. Záložní server disponuje procentuálním podílem dostupných IP adres. Výchozí počet je 5 procent. Primární server může být i sekundárním pro jinou podsíť. Situace může být i taková, že více

primárních serverů sdílí jeden záložní. Tato situace je vidět na obrázku níže. (Stanek, 2015)



Obrázek 2: Zastupitelnost DHCP serveru
Zdroj: Vlastní zpracování

1.3 DNS server

Aby mohly operační systémy Windows snáze komunikovat s ostatními počítači v síti, překládají si jejich názvy. Při překladu dochází k navázání názvu počítače k číselné IP adrese, která se používá při síťové komunikaci. Namísto dlouhé řady číslic se tak může uživatel připojit k počítači, který je označen názvem. (Regan, 2012)

Jeden ze systémů pro překlad je DNS, která je realizován servery DNS.

1.3.1 Služby překládající názvy

Současné operační systémy Windows podporují nativně tři systémy překladu adres:

- DNS (Domain Name System),
- WINS (Windows Internet Name Service),
- LLMNR (Link-Local Multicast Name Resolution).

Nejpoužívanější systém je DNS, proto se jím v této práci budeme detailně zaobírat.

1.3.2 Historie DNS

DNS bylo vyvinuto, když Internet teprve začínal (nazýval se ARPAnet). Byla to malá síť. Tehdy administrátoři ručně vkládali název hostitele do HOSTS souboru, který byl umístěn na serveru v organizaci. Soubor HOSTS se pak distribuoval na všechny stanice v síti. Jakákoliv jiná síť si musela stáhnout soubor HOSTS, pokud chtěla přeložit název hostitele v této organizaci. Situace do budoucna byla neúnosná, musel se vymyslet lepší nový systém. (Panek, 2015)

1.3.3 Co je to DNS

DNS je služba, která převádí název hostitele na IP adresu. Kupříkladu název hostitele www.seznam.cz by služba DNS přeložila na IP adresu 77.75.77.53, díky tomu by nám umožnila s tímto serverem komunikovat. Používání názvu hostitele je pro nás komfortnější a lépe zapamatovatelné nežli dlouhého čísla. Tato situace bude demonstrována na jednoduchém příkladu. Většina z nás vlastní mobilní telefon, často z něj telefonujeme, k vytáčení telefonních čísel využíváme adresář kontaktů. Nedokážeme si zapamatovat telefonní číslo na všechny kontakty v adresáři. Proto je nejjednodušší volbou kontakt si uložit a přiřadit k telefonnímu číslu jméno osoby. Toto je velmi podobná situace, když se chceme podívat na náš oblíbený web nebo najít ve firemní síti sdílenou tiskárnu či server se sdílenými službami, disky atp.. Nejsnazší volbou pro nás je zadat doménu (jméno) webu a ne IP adresu. Služba DNS je pro nás takový „adresář“, ve kterém se vyhledává IP adresa podle název hostitele, který zadáme

třeba do internetového prohlížeče. Název hostitele může být až 255 znaků dlouhý a může obsahovat písmen a číslic, tečky a pomlčky. (Regan, 2012)

Je zde možnost i přeložení IP adresy na název hostitele. K tomu se využívají PTR záznamy.

Službu DNS lze integrovat do služeb WINS, DHCP a AD DS. DNS servery jsou nezbytné při překladu názvů v doménách Active Directory. Bez služby DNS by nebylo možné přijmout, ani odeslat email nebo jednoduše prohlížet webové stránky na internetu.

Celý systém DNS si můžeme představit jako decentralizovanou hierarchickou databázi. Záznam v této databázi se nazývá Resource Record. Resource Record obsahuje vlastníka, třídu, typ a TTL. Třída nabývá hodnot IN (Internet) nebo CH (Chaos). Třída chaos slouží pro experimentální účely. Typ může být A (IPv4 adresy), MX (směrování pošty), AAAA (IPv6 adresy) a další. TTL je délka platnosti záznamu. (Surý, 2011)

1.3.4 Princip DNS

„Služba DNS umožňuje uspořádat skupiny počítačů do domén. Tyto domény jsou uspořádány do hierarchické struktury, kterou lze definovat na základě Internetu pro veřejné sítě nebo na základě rozlehlé sítě pro privátní sítě (označovány taky jako intranety a extranety). Různé úrovně v hierarchii označují jednotlivé počítače, organizační domény a domény nejvyšší úrovně. U úplného názvu hostitele samostatného počítače část *microsoft* představuje organizační doménu a přípona *com* představuje doménu nejvyšší úrovně.

Domény nejvyšší úrovně se nacházejí v kořenovém umístění hierarchie služby DNS, jsou proto také označovány jako kořenové domény. Tyto domény jsou uspořádány geograficky, podle typu organizace a podle funkce. Obvyklé domény, například microsoft.com, jsou také označovány jako *nadřazené domény*. Jsou tak nazývány proto, že jsou nadřazenými doménami organizační struktury. Nadřazené domény lze rozdělit do subdomén, které lze použít pro skupiny nebo oddělení v rámci organizace.

Subdomény jsou často označovány jako *podřízené domény*. Plně kvalifikovaný název počítače (FQDN) ve skupině lidských zdrojů (HR – Human resources) lze například označit jako peter.hr.microsoft.com. V tomto případě část *peter* představuje název hostitele, *hr* je podřízená doména domén *microsoft.com*“ (Regan, 2015).

1.3.5 Krok za krokem DNS

1) Pokud napíšeme URL adresu www.uhk.cz do internetového prohlížeče, internetový prohlížeč hledá odpovídající IP adresu. První server, který reaguje na náš požadavek, se nazývá recursive resolver (program zajišťující rekurzivní překlad). Tento server je typicky u nás doma, v kanceláři nebo u našeho internetového poskytovatele. Resolver ví, jakého DNS serveru se má dál dotázat.

2) Resolver se nejprve zeptá na IP adresu vyrovnávacího DNS serveru, a pokud ji zná, vyrovnávací server nám ji vrátí. Vyrovnávací server slouží pro uchovávání IP adres nedávno hledaných domén.

3) Resolver předá požadavek na kořenový server. Kořenové servery mají uložené informace o Top Level doménách (.cz, .net). Kořenových serverů je na světě 13. Resolver se tedy zeptá kořenového serveru, který je nejblíže, na informace o serveru www.uhk.cz. Ten mu dodá co nejvíce informací o serveru, který zná jmenné servery všech CZ domén. Tyto servery se nazývají autoritativní servery.

4) Resolver se tedy obrátí na autoritativní server, který zná jmenné servery všech CZ domén, s požadavkem o IP adresu serveru www.uhk.cz. Ten odpověď taky nezná, ale zná IP adresu autoritativního serveru uhk.cz.

5) Resolver pošle požadavek na autoritativní server uhk.cz, který mu předá, jaká je IP adresa.

1.4 Active Directory Domain Services

Active Directory je adresářová služba obsažená ve WS2012. Umožňuje nám snadno přidávat, odebírat nebo přemísťovat účty uživatelů, skupin a počítačů. Je zodpovědná za ověření přístupu, správu identit a kontrolu vztahů mezi prostředky.

Primárním protokolem Active Directory je LDAP (Lightweight Directory Access Protocol), standardní protokol pro adresářové služby.

Jednotlivé jednotky nazýváme objekty. Nejčastěji používané objekty jsou uživatelé, počítače a skupiny. Tyto objekty můžeme organizovat do organizačních jednotek. Organizační jednotka je jakýsi kontejner sloužící ke zjednodušení a zpřehlednění správy.

Operační systém WS2012 dává na výběr, zda server bude členským serverem, řadičem domény či samostatným serverem. Rozdíly mezi uvedenými typy jsou zásadní. Členské servery jsou součástí domény, avšak neuchovávají údaje adresářů. Řadiče domény se od členských serverů liší, protože údaje adresářů uchovávají a navíc zajišťují doméně ověřování a adresářové služby. Samostatné servery nejsou součástí domény. Tyto servery mají své vlastní databáze, a proto ověřují požadavky na přihlášení k nim nezávisle.

Domény, které využívají technologii Active Directory, jsou označovány jako *domény Active Directory*. Tyto domény sice mohou fungovat pouze s jediným řadičem, ovšem lepší je nakonfigurovat řadičů více. Pokud se v doméně nachází řadičů více, dochází k replikaci údajů mezi řadiči automaticky. V případě selhání jednoho z řadičů převezme jeho funkci jiný. (Stanek, 2015)

Autentizace v Active Directory probíhá výhradně protokolem Kerberos verze 5 a dalšími standardními protokoly. Služba Active Directory podepisuje a šifruje veškerou komunikaci, která používá LDAP. Podepisování komunikace zaručuje, že data pocházejí od identifikovaného zdroje a jsou nepozměněná. (Stanek, 2009)

1.4.1 Počítače a služba Active Directory

Na počítačích s profesionální či firemní verzí systému Windows lze služby Active Directory využít naplno. Tyto počítače přistupují do sítě jako klienti Active Directory a mají funkce služby Active Directory plně k dispozici. Klienti mohou využívat přechodných důvěryhodných vztahů, které jsou ve stromu domény či v doménové struktuře navázány. Přechodný důvěryhodný vztah se navazuje automaticky v závislosti na struktuře domény a oprávněních v ní nastavených. Tyto vztahy umožňují autorizovaným uživatelům přistupovat ke zdrojům nacházejícím se v doménovém stromě.

Servery zajišťují funkcionalitu dalším systémům a mohou zastávat roli řadičů domény či členských serverů, jak už jsme si řekli. Řadič domény je od členského serveru oddělen, protože je na něm spuštěna služba AD DS (Active Directory Domain Services). Pokud je požadováno ze členského serveru učinit řadič domény, je potřeba nainstalovat na něj službu AD DS.

Každý počítač se systémem Windows 2000 či novějším, který se připojí do domény, má svůj účet. Stejně jako ostatní zdroje se i účty ukládají ve službě Active Directory v podobě objektů. Počítače přistupují do domény prostřednictvím svého účtu. Přístup do sítě získá počítač teprve po ověření účtu.

1.4.2 Autentizace uživatelů

Autentizace je úkon ověření identity uživatele nebo systému. Autentizaci používáme například, pokud se uživatel nebo systém snaží připojit na náš server nebo síťový prvek. Z hlediska bezpečnosti je velmi důležité ověřit, zda je uživatel nebo systém opravdu ten, za koho se vydává. Na základě toho systém rozhodne, jestli povolí nebo zakáže přístup.

Autentizační protokol se používá při autentizaci uživatele. Windows podporují dva autentizační protokoly NT LAN Manager (NTLM) a Kerberos.

Protokol NTLM byl vyvinut firmou Microsoft. Ačkoliv výchozím autentizačním protokolem je Kerberos od Windows 2000, NTLM je stále podporován.

Protokol Kerberos má oproti zastaralému NTLM mnoho výhod. Mezi hlavní výhody patří rychlejší a vzájemná autentizace. Považuje se za bezpečnější.

Protokol Kerberos nám v Active Directory výrazně zvyšuje bezpečnost sítě, zabraňuje odposlechu citlivých informací a poskytuje vzájemné ověření identit obou stran. (Clercq, 2007)

Největším rizikem tohoto protokolu spočívá v dostupnosti centrálního serveru. Centrální server musí nepřetržitě běžet, jinak se uživatelé nemohou přihlásit. Je vhodné riziko minimalizovat více Kerberos servery. Dále je nutné dát si pozor na přísné požadavky na synchronizaci časů serveru a klienta. Kerberos pracuje na bázi tiketů, kterými ověřuje identitu. Tikety mají svou životnost, pokud není čas klienta synchronizován, autentizační proces selže. (Clercq, 2007)

1.5 Group Policy

Jedna z velkých výhod operačních systémů Windows je vysoká flexibilita, lze toho nastavit opravdu mnoho. Pro mnoho správců je to noční můra. Některá nastavení by měla být dostupná pouze pro správce, pokud se jedná o firemní zařízení. Je velmi nežádoucí, aby nám uživatelé měnili např. TCP/IP nastavení jednotlivých počítačů. Proto Microsoft vyvinul funkci Group Policy, která slouží k centralizované správě a kontrole firemních zařízení v doméně.

Lze tedy aplikovat plošně nastavení, vyhovující firemním obchodním a technickým požadavkům. Je možné zúžit výběr zařízení, na které chceme nastavení uplatnit. Group Policy je velmi důležitý nástroj, který zjednodušuje práci správcům ve větších organizacích. Automatizuje řadu úkonů, jako je např. připojení domovských adresářů uživatelů a tiskáren, sjednocení bezpečnostních politik, nastavení VPN připojení a dalších.

1.6 Windows Server Update Services (WSUS)

WSUS je role serveru, která je součástí WS2012, stará se o stahování a distribuci aktualizací pro pracovní stanice s operačním systémem Windows. Také může obsahovat aktualizace pro nejběžnější aplikace od Microsoftu, například pro Microsoft Office a Microsoft SQL Server. Nejjednodušší situací je pouze jeden WSUS Server, který stahuje aktualizace přímo od Microsoftu. Jeden WSUS Server může obsloužit až tisíce klientů. Pokud to dovolí prostředky, je dobré mít více WSUS Serverů z důvodu rozložení zátěže a také jako zálohu. Klientské stanice stahují aktualizace z WSUS Serveru, pokud jsou tak nakonfigurovány. Aktualizace je nejprve schválit, dřív si je stanice nemohou stáhnout.

Pokud se rozhodneme využívat WSUS a zvolíme možnost aktualizace ukládat lokálně na disk serveru, velká výhoda je nižší zatížení připojení k internetu, aktualizace jsou stahovány pouze na server a pak distribuovány po lokální síti. Další výhodou je jednodušší správa aktualizací, pokud se rozhodneme nějaké aktualizace nestahovat, stačí to nastavit na serveru. V opačném případě bychom museli zakázat aktualizaci na každé stanici.

2. Analýza současného prostředí

V této kapitole se zaměříme na analýzu současného stavu síťové infrastruktury ve firmě, kde autor pracuje.

2.1 Počítačová síť

Počítačová síť uvnitř budovy je realizována kabely UTP 5, které dovolují přenášet data rychlostí až 100MBps. Rychlost přenosu zpravidla záleží na délce kabelu a na tom, jaké aktivní prvky byly použity. Všechny kabely jsou vedeny od zásuvek pro strukturovanou kabeláž do patch panelu v rozvaděčové skříni.

Byla použita síťová topologie hvězdicové typu. Centrálním prvkem této hvězdicové topologie je switch typu ZyXEL GS2210-48, který má 44x Gigabit Ethernet portů a 2 Gigabit Ethernet SFP sloty, které zůstaly nevyužity.

Je zde také možnost využít bezdrátové sítě, které tu jsou dvě. Jedna slouží zaměstnancům a druhá pro hosty. Bezdrátové sítě jsou dvě kvůli bezpečnosti. Bezdrátová síť pro hosty má svou vlastní VLAN. VLAN dovoluje síťovým administrátorům rozdělit lokální síť na více segmentů, které se navzájem nemusí vidět. Prostřednictvím této metody je bezdrátová síť pro hosty oddělena od zbytku sítě. Hosté tedy nevidí naše firemní zařízení, které nechceme, aby viděli.

Síť je do internetu připojena prostřednictvím hlavního routeru Mikrotik RB450G přes dva ISP (poskytovatele internetového připojení). Router je nastaven tak, aby zátěž rozložil na oba ISP. V případě, že má jeden internetový provider odstávku, je zde možnost síťový provoz přesměrovat přes jiného poskytovatele.

2.2 Uživatelské účty

Většina zaměstnanců má svůj doménový účet. Uživatelské jméno je ve tvaru jmeno.prijmeni bez diakritiky. Uživatelé si volí heslo, které podléhá politice hesel pomocí Group Policy, používají se komplexní hesla, aby se zabránilo použití lehce prolomitelných hesel.

Externí zaměstnanci mají na stanicích pouze lokální účty. Zaměstnanci mají možnost připojit se do firmy i zvenčí prostřednictvím VPN. VPN technologie umožňuje vytvořit zabezpečený „síťový tunel“ do naší firemní sítě. Při instalaci VPN máme možnost vybrat si z několika síťových protokolů, a to PPTP, L2TP, SSL, OpenVPN. Ve

firmě byl použit PPTP protokol. Zaměstnanci připojující se zvenčí disponují ještě PPTP účtem, který byl založen v PPTP adresáři hlavního routeru.

Dále má každý interní zaměstnanec svůj účet v docházkovém a CRM systému (systém pro řízení vztahu se zákazníky).

2.3 Servery

Ve firmě jsou tři Windows Servery, které pokrývají požadavky zaměstnanců. Na nejstarším a nejslabším serveru je nainstalováno pouze účetnictví. Účetní používají terminálové služby, přes vzdálenou plochu se připojují a pracují. Druhý server je využit jako webový server. Na tomto webovém serveru běží interní informační systém a CRM.

Třetí, nejnovější a nejvýkonnější server slouží pro zbytek služeb. Slouží jako poštovní, souborový, tiskový, DHCP, DNS server. Také je to řadič domény. Právě na tomto serveru je nainstalován operační systém WS2012. Typ serveru je DELL PowerEdge R320, který disponuje procesorem Intel Xeon E5-2403 s frekvencí 1,8 GHz, 4 jádry, 16 GB RAM, 4x1 TB SAS disky, 2x 495W zdroji. Server má dvě síťové karty, jedna je vyhrazena pro vzdálenou správu a druhá pro běžný provoz. Tento výkon je pro nás zatím dostatečný. Je zde možnost případně osadit server dalšími komponenty. Velkou výhodou tohoto serveru od firmy DELL je možnost vzdálené správy přes iDrac (Integrated Dell Remote Access Controller). Tak se u serverů řady PowerEdge jmenuje managment karta, která slouží ke vzdálené správě.

2.4 Zálohování

Zálohování je řešení prostřednictvím programu Cobian Backup v kombinaci se službou zálohování serveru. K záloze databází na webovém serveru se používá funkce mysqldump. Je použit skript, který se pouští při každé záloze souborů na webovém serveru, tento skript využívá mysqldump k záloze databází.

Zálohy se provádí na síťové a USB disky. USB disky jsou hned po zálohování odneseny mimo budovu.

Na serveru, kde je instalován WS2012, je využito RAID pole 5. Tedy data a paritní informace jsou distribuovány po všech discích. Pokud nastane havárie pouze jednoho disku, neznamená to ztrátu dat ani přerušení provozu.

2.5 Záložní zdroje

Kvůli nečekaným výpadkům elektrické energie byl instalován záložní zdroj APC Smart-UPS 1500VA RM 2U 230V, zabezpečující ochranu napájení pro servery. Tento záložní zdroj servery napájí po dobu výpadku nebo než se bezpečně vypnou. Druhou funkcí záložních zdrojů je ochrana proti přepětí.

2.6 Tiskárny

Tisk je zabezpečen prostřednictvím síťových tiskáren Konica Minolta bizhub C258, HP MFP M476dn, OKI MC760. Nainstalovaný Print(tiskový) server velmi zjednodušuje práci při instalaci tiskáren na stanice. Na serveru se tiskárna nainstaluje, nasdílí pro určené klienty, tím se pro ně nainstaluje i příslušná sada ovladačů a na klientské stanici pak stačí tiskárnu připojit, čímž dojde k instalaci ovladačů na klientskou stanici ze sdílené složky na serveru. Pokud nastane havárie serveru, kde je print server nainstalován, žádný z uživatelů nemůže tisknout, a proto je třeba zvážit instalaci záložního print server. Ale to je řešení spíše pro větší organizace.

2.7 Fyzické zabezpečení ICT techniky

Všechny aktivní prvky jsou instalovány v rozvaděčové skříni, která se zamyká. O odvětrání teplého vzduchu z rozvaděčové skříně se stará ventilační panel se 4 větráky.

2.8 Uživatelské stanice

Typ uživatelských stanic není bohužel nijak sjednocen. Důraz je kladen na to, aby na stanicích byla verze operačního systému ve verzi Professional. Bez této verze není možnost připojit stanice do naší firemní domény.

2.9 Zabezpečení dat

Kvůli bezpečnosti dat mají všechny stanice průběžně aktualizovaný operační systém a antivirový program. V administraci hlavního směrovače je otevřeno co nejméně portů ven do internetu. Bezdrátová síť pro hosty je oddělena od zbytku sítě. Pro připojení zvenčí se používá zabezpečený VPN tunel. Firemní zaměstnanci jsou poučeni, jak pracovat se svými vlastními zařízeními, kterými se chtějí připojit do sítě.

Poštovní server využívá softwarový antispamový systém, který se stará o odfiltrování většiny škodlivých mailů pomocí databáze zakázaných IP adres.

V budoucnu, pokud bychom chtěli zaměstnancům zakázat připojení vlastních zařízení do sítě, bychom mohli přenastavit switch (přepínač) tak, aby na každém portu dovolil připojit pouze ta zařízení, které mají specifickou fyzickou adresu síťové karty. Na bezdrátovém směrovači bychom pak museli nastavit možnost připojení pouze těch zařízení, která mají specifickou adresu síťové karty. Jsou zde však metody jak toto zabezpečení obejít, jedna z těchto metod je duplikace fyzické adresy firemního síťového zařízení. Toto však vyžaduje určité znalosti, které většina běžných uživatelů (zaměstnanců) nemá.

2.10 Poštovní služby

Poštovní služby zajišťuje poštovní server Microsoft Exchange 2013. Microsoft Exchange nabízí kromě přijímání a odesílání pošty různé funkcionality, jako je sdílení kalendářů, úkolů a kontaktů, synchronizace dat s mobilním telefonem, delegování přístupových práv k celé poštovní schránce nebo jen její části jiné osobě.

3. Výzkumné šetření

Existuje velké množství literárních a ostatních zdrojů týkající se informatiky. Vzhledem k neustálému vývoji technologií, počet zdrojů, ze kterých lze získat informace, stále roste. Nemusí být vůbec jednoduché vyfiltrovat podstatné a důležité informace.

Cílem výzkumného šetření je zjistit, jakým způsobem se správci sítě dále vzdělávají a kde v případě problému během konfigurace hledají možná řešení. Dále potvrdit nebo vyvrátit stanovené hypotézy.

Výzkum byl proveden metodou hloubkového interview s pěti vybranými správci sítě z Hradce Králové a blízkého okolí. Správci sítě zodpovídali předem připravené otázky. Hloubkové interview se skládalo z 15 otázek.

H1: Většina správců sítě by tuto metodickou příručku označila jako použitelnou v praxi.

Zdůvodnění formulace H1:

Hypotéza H1 bude přijata, pokud minimálně 50 % dotázaných zodpoví na otázku ano.

Zdroj dat pro verifikaci H1:

K ověření verifikace poslouží následující otázka. Myslíte si, že by tato metodická příručka byla pro vás v praxi během konfigurace WS2012 přínosná?

H2: Správci sítě při řešení problému při konfiguraci nejčastěji používají internet.

Zdůvodnění formulace H2:

Hypotéza H1 bude přijata, pokud minimálně 70 % dotázaných zodpoví na otázku ano.

Zdroj dat pro verifikaci H2:

K ověření verifikace poslouží následující otázka. Pokud nastane problém při konfiguraci, jaký zdroj jako první použijete pro hledání vhodného řešení?

4. Konfigurace služeb

V praktické části bude vysvětlena konfigurace služeb, které byly popisovány v teoretické části. Metodická příručka je přizpůsobena pro menší až střední firmu.

Veškeré pořízené materiály v bakalářské práci jsou vlastního zpracování. V jednotlivých kapitolách je postup nastavení vysvětlen slovně a pro lepší pochopení jsou přiloženy snímky obrazovky, které zobrazují nejdůležitější kroky konfigurace.

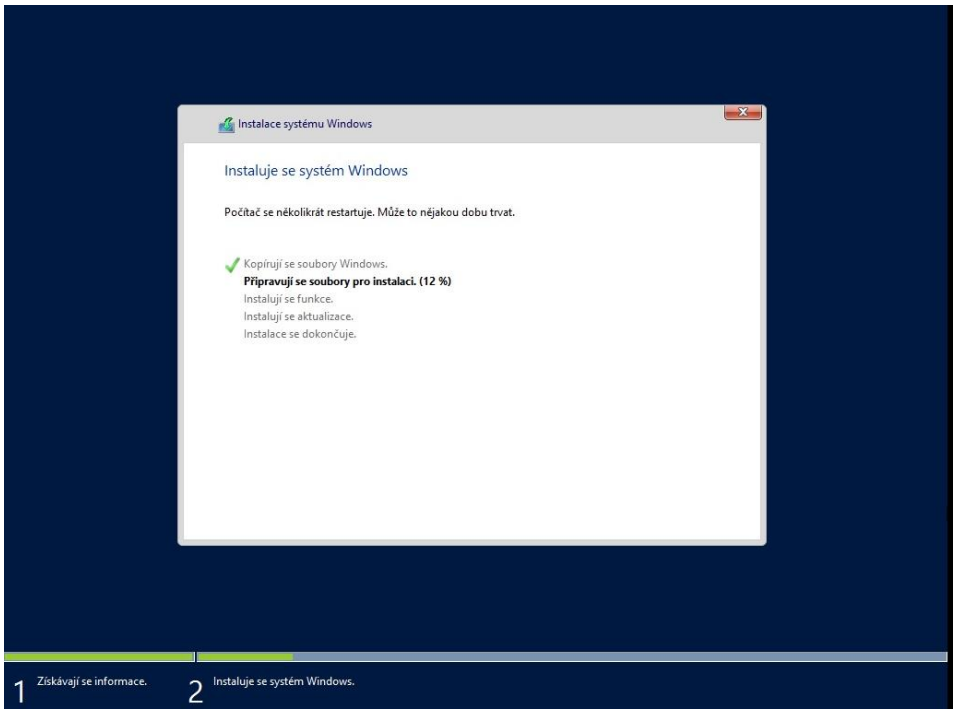
4.1 Instalace

Musíme si předem rozmyslet, jaký způsob instalace zvolíme. Máme zde na výběr z několika možností:

- Ruční instalace z DVD mechaniky nebo sdílené síťové složky, kde jsou instalační soubory uložené
- Bezobslužná instalace pomocí odpovědního souboru autounattend.xml s diskem DVD nebo sdílenou síťovou složkou
- Použitím vytvořené bitové kopie z jiného serveru. Pro vytvoření bitové kopie je vhodné použít nejprve program Sysrep, který nám odebere všechny unikátní identifikátory systému a následně využít Norton Ghost nebo Acronis True Image pro vytvoření obrazu.

Před instalací je vhodné zkontrolovat, zda oddíly disků používají souborový systém NTFS.

My zvolíme ruční instalaci z DVD mechaniky. Samotná instalace není nic složitého. Nejprve vložíme instalační DVD do mechaniky. Po startu serveru zavedeme systém z DVD mechaniky. Jsou zde alespoň dvě metody, jak toho docílit. Můžeme při startu zkusit mačkat F12 (případně F11) nebo v BIOSu přenastavit prioritu DVD mechaniky při zavádění operačního systému. Jakmile se spustí vlastní instalace, musíme zvolit jazyk, časový a datumový formát, rozložení klávesnice, pokud chceme systém aktivovat hned po instalaci, vložit licenční klíč, potom máme na výběr z verzí operačního systému, který chceme instalovat. Můžeme si vybrat mezi verzí s grafickým rozhraním (Server with a GUI), které je většinou přijatelnější, nebo verzi bez grafického rozhraní (Server Core Installation), která se ovládá pouze z příkazové řádky. Dalším krokem je potvrzení licenčních podmínek a zvolení diskového oddílu, kam chceme systém instalovat.



Obrázek 3: Instalace OS

Zdroj: Vlastní zpracování

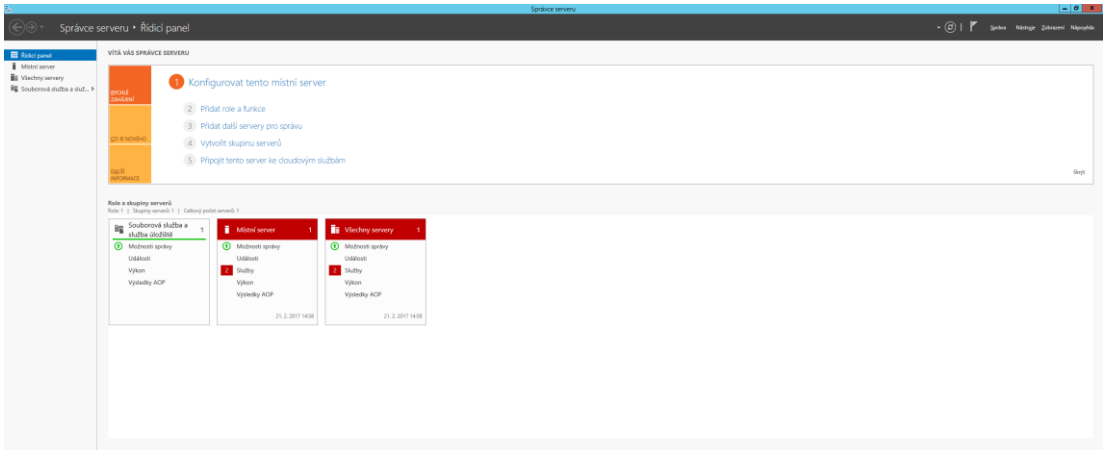
4.2 Seznámení se s prostředím operačního systému

Z grafického hlediska se nová verze od předchůdce velmi liší, naopak se velmi podobá Windows 8 a 10. I zde je dlaždicová nabídka Metro přizpůsobena pro dotykové ovládání. Na práci v prostředí Metro je potřeba si nejprve zvyknout.

Obrázek 4: Grafické rozhraní Metro

Zdroj: Vlastní zpracování

Správce serveru byl celý přepracován. Jeho nabídka nám dovoluje velikou škálu možností, my zde budeme hlavně přidávat a odebírat role. V základu je nainstalována pouze Souborová služba. Správce serveru zobrazuje přehled všech chyb, problémů a jejich možná řešení. Dovoluje nám spravovat i ostatní servery, ne pouze lokální. Můžeme tedy z jednoho místa instalovat např. role, funkce na ostatní servery, které si ve správci přidáme. Servery můžeme seskupovat do logických skupin, tak jak se nám to hodí např. za účelem sledování provozu nebo konfigurace.



Obrázek 5: Správce serveru

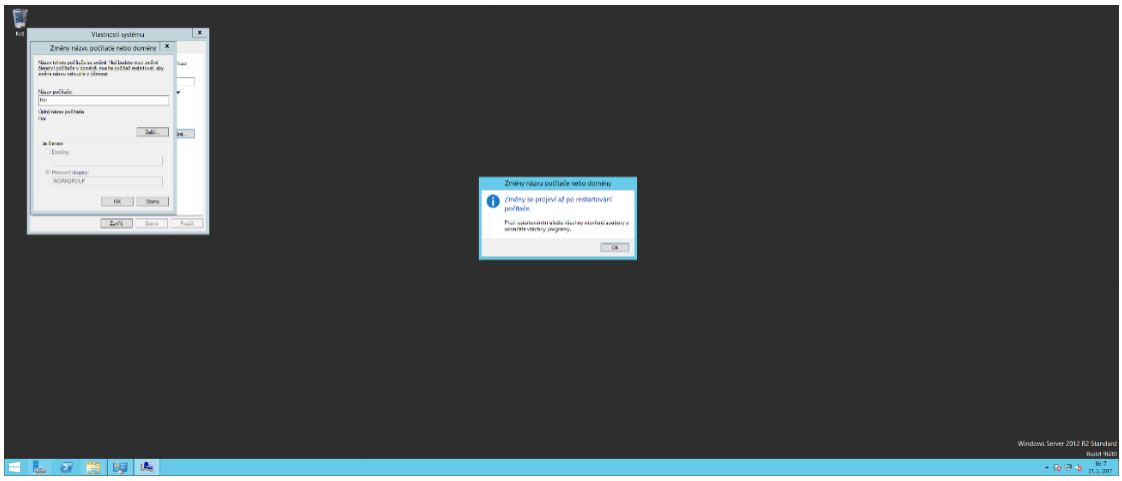
Zdroj: Vlastní zpracování

Skriptovací prostředí PowerShell také prošlo velkou obměnou a je vybaveno novou verzí PowerShell 3.0. V této nové verzi jsme se dočkali nových příkazů a operátorů i zjednodušení občas složité syntaxe.

4.3 První kroky

Nastavení jména serveru

Začneme u toho, že našemu serveru nastavíme jméno, které pak hraje velkou roli v DNS službě. Změnu názvu serveru provedeme v nabídce Vlastnosti systému (Správce systému → Místní Server → Název počítače), zde klikneme na tlačítko Změnit a vyplníme název počítače, např. „Rory“, potvrdíme a následně restartujeme.

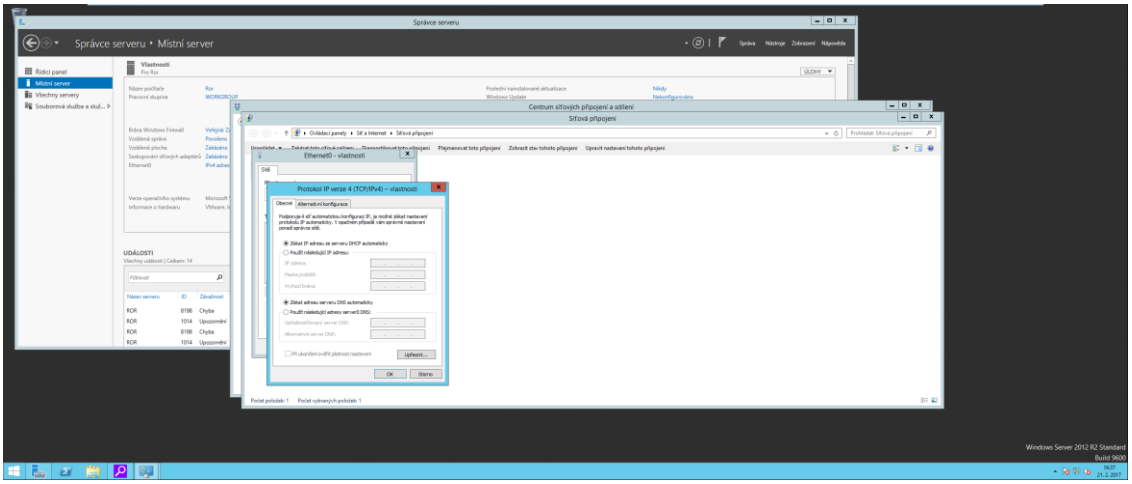


Obrázek 6: Nastavení jména serveru

Zdroj: Vlastní zpracování

Přenastavení TCP/IP protokolu (nastavení statické IP adresy)

Nyní přenastavíme TCP/IP nastavení dle potřeb naší lokální sítě, server by měl mít statickou IP adresu. Toto nastavení provedeme v nabídce Nastavení protokolu IP verze 4 (Ovládací panely → Síť a Internet → Centrum síťových připojení a sdílení → Změnit nastavení adaptéru → pravým tlačítkem na Síťovou kartu zapojené do lokální sítě → Vlastnosti → Protokol IP verze 4 (TCP/IPv4)), zaškrtneme Použít následující IP adresu a vyplníme.



Obrázek 7: Konfigurace TCP/IP protokolu

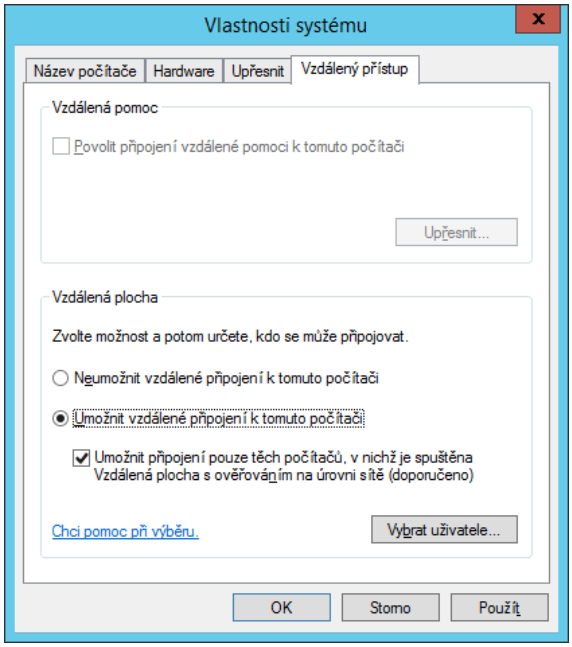
Zdroj: Vlastní zpracování

Povolení připojení přes vzdálenou plochu

Vzdálená správa serveru je nezbytným pomocníkem, IT správci tuto funkcionalitu využívají nepřetržitě. Server je zamknut v rozvaděčové skříni, ale my se k němu můžeme připojit odkudkoliv, pokud to máme na serveru povoleno. Na zařízení, ze kterého se připojujeme, musíme mít k dispozici klienta pro vzdálený přístup. Používá se Remote Desktop Protocol (RDP), server naslouchá na portu 3389. Je vhodné tento port neblokovat, pokud se chceme připojit zvenku k serveru v naší lokální síti.

Před konfigurací je nutné si zkontrolovat, zda účet, kterým jsme přihlášeni, je členem skupiny Administrators. V opačném případě je nutné přihlásit se účtem, který je v této skupině členem.

V nabídce Vzdálený přístup (pravým tlačítkem myši na Tento počítač → Vlastnosti → Upřesnit nastavení systému → záložka Vzdálený přístup) zaškrtneme Umožnit vzdálené připojení k tomuto počítači.



Obrázek 8: Povolení připojení přes vzdálenou plochu

Zdroj: Vlastní zpracování

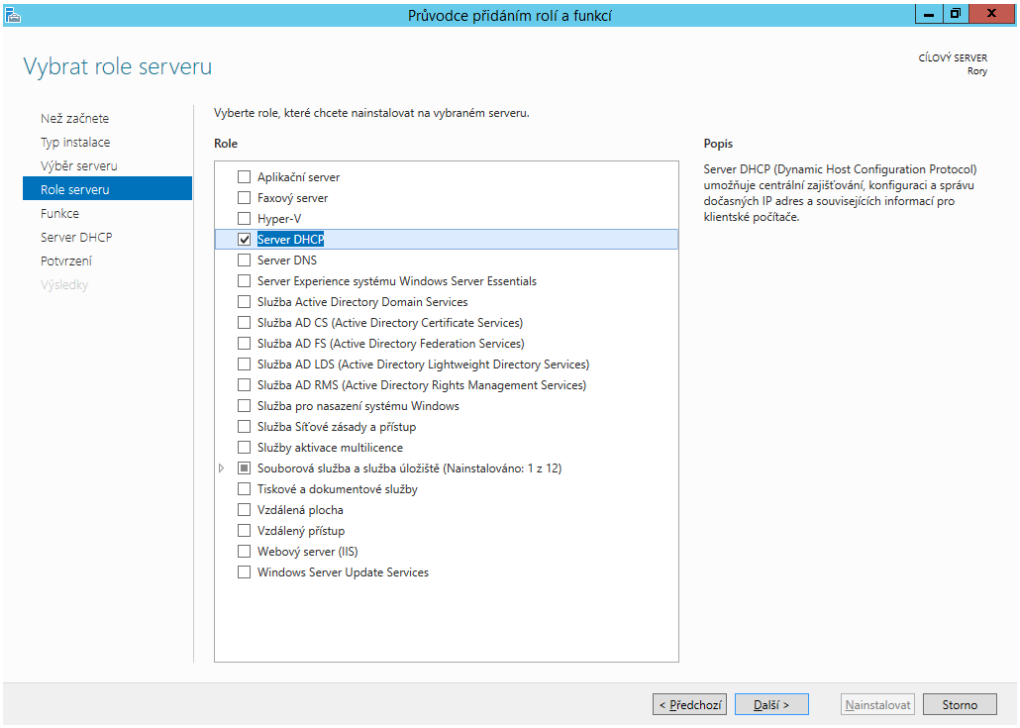
4.4 Role DHCP Server

Nebudeme zde rozebírat důležitost této role. To je patrné z teoretické části, kde jsme DHCP rozebrali dopodrobna. Roli serveru přidáme ve Správci serveru (Přidat role a funkce → Další → Instalace na základě rolí nebo základě funkcí → vybereme server a potvrdíme tlačítkem Další → zaškrtneme Server DHCP a potvrdíme → Další → Nainstalovat).

Instalaci role DHCP Serveru lze provést i přes příkazovou řádku PowerShell spuštěnou se zvýšením oprávněním (kliknout pravým tlačítkem myši na Windows PowerShell, Spustit jako Správce), konkrétněji příkazem *Install-WindowsFeature -Name 'DHCP' –IncludeManagementTools.* V opačném případě, pokud bychom chtěli vidět stav instalace, použijeme *Get-WindowsFeature -Name 'DHCP'*.

Po přidání role se nám ve Správci serveru zobrazí notifikace – žlutý vykřičník. Dále je nutné udělat finálníinstalační úpravy konfigurace (vytvoření skupin DHCP Administrators, DHCP Users pro delegování správy serveru DHCP). Klikneme na žlutý vykřičník, spustí se průvodce (Potvrdit → Zavřít).

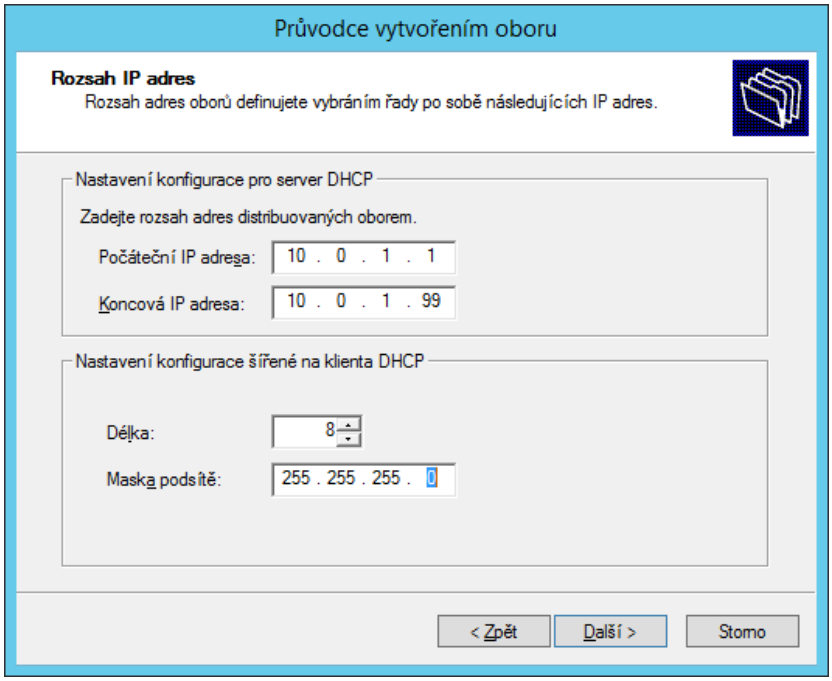
Tato role server příliš nezatěžuje, závisí pouze na počtu klientů a době zápůjček.



Obrázek 9: Přidání role Server DHCP

Zdroj: Vlastní zpracování

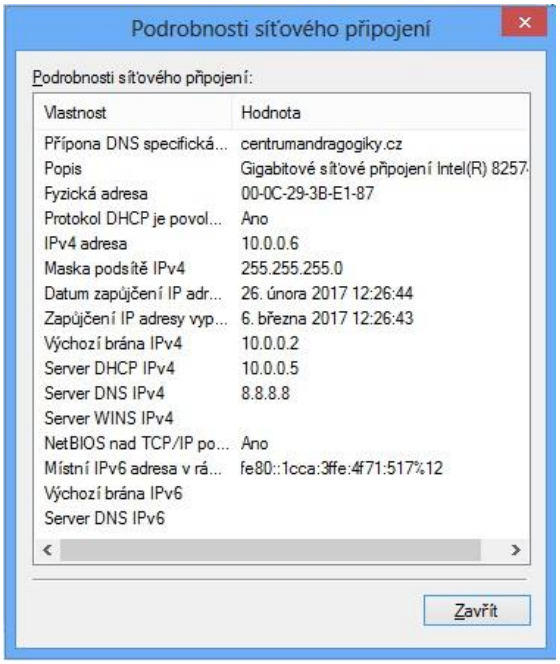
Nyní je potřeba DHCP nastavit (Nástroje pro správu → DHCP). Rozklikneme si DHCP → NÁZEV_SERVERU → klikneme pravým tlačítkem na IPv4 → Nový obor, otevře se nám průvodce, který nás celým procesem provede. Nejprve si zvolíme název oboru, potom rozsah adres, které se budou přidělovat, zde je možnost vyloučit některé adresy (použijeme například tehdy, pokud by v rozsahu byly statické IP adresy přidělené tiskárnám, ip kamerám, jiným serverům, atp.). V dalším kroku volíme dobu trvání zápůjčky. Kratší dobu zápůjčky volíme tehdy, když se v síti střídá velké množství zařízení. Pokud bychom však zvolili naopak příliš krátkou dobu zápůjčky, zbytečně budeme zatěžovat síť i server. Je tedy potřeba najít nějaký kompromis. Později zadáme adresu směrovače nebo výchozí brány a obor aktivujeme.



Obrázek 10: Konfigurace DHCP Serveru

Zdroj: Vlastní zpracování

Pokud jsme vše nastavili správně a v síti máme zapnutý počítač, na kterém je nastavené, aby konfiguraci IP získal ze serveru, počítač by měl získat dynamicky IP adresu a ostatní parametry (viz. Obrázek 10).



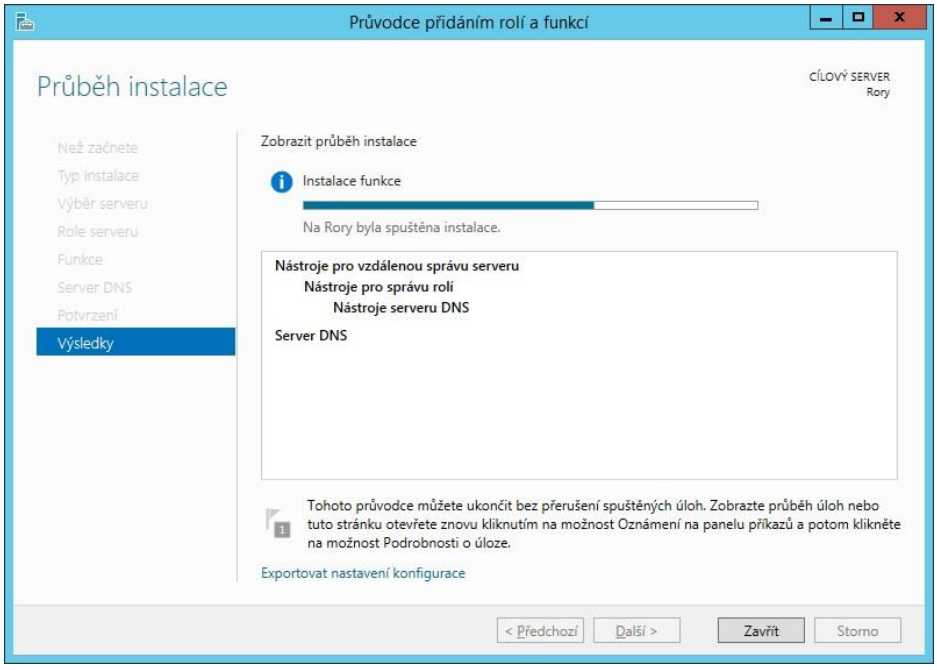
Obrázek 11: Parametry nastavené pomocí DHCP

Zdroj: Vlastní zpracování

Ve vlastnostech protokolu lze zkontrolovat, zda počítač získává IP adresu automaticky (Ovládací panely → Síť a Internet → Centrum síťových připojení a sdílení → Změnit nastavení adaptéru → pravým tlačítkem na Síťovou kartu zapojené do lokální sítě → Vlastnosti → Protokol IP verze 4 (TCP/IPv4)). Zde si zkontrolujeme, zda je zaškrtnuté Získat IP adresu ze serveru DHCP automaticky.

4.5 Role DNS Server

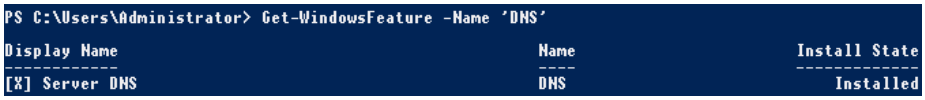
Instalace DNS Serveru začíná obdobně jako u DHCP ve Správci serveru (Přidat role a funkce → Další → Instalace na základě rolí nebo základě funkcí → vybereme server a potvrdíme tlačítkem Další → zaškrtneme Server DNS a potvrdíme → Další → Nainstalovat). Po úspěšné instalaci můžeme kliknout na tlačítko Zavřít.



Obrázek 12: Přidání role DNS Serveru

Zdroj: Vlastní zpracování

V případě instalace přes PowerShell použijeme příkaz *Install-WindowsFeature DNS –IncludeManagementTools*. Výsledek instalace ověříme příkazem *Get-WindowsFeature -Name 'DHCP'*. Pokud vše proběhlo správně, měli bychom vidět Installed. (Viz. Obrázek 13)



Obrázek 13: PowerShell Stav instalace

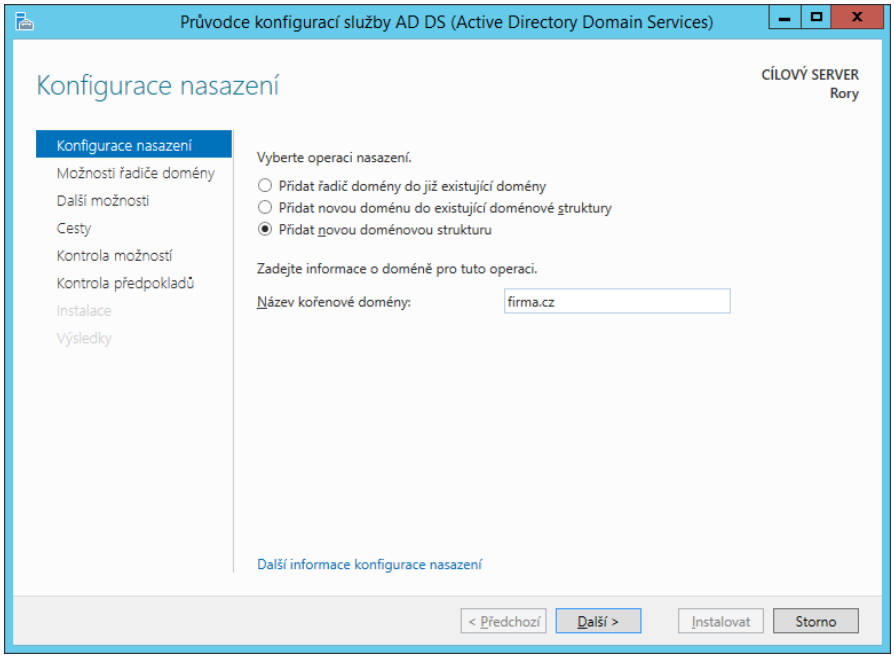
Zdroj: Vlastní zpracování

V tuto chvíli nastavíme přednostní používání našeho DNS Serveru (Ovládací panely → Síť a Internet → Centrum síťových připojení a sdílení → Změnit nastavení adaptéru → pravým tlačítkem na Síťovou kartu zapojené do lokální sítě → Vlastnosti → Protokol IP verze 4 (TCP/IPv4)). Zaškrtneme Použít následující adresy serverů DNS a napíšeme adresu localhostu (sami sebe) *127.0.0.1*.

4.6 Role Active Directory Server

Přidání role provedeme ve Správci serveru (Přidat role a funkce → Další → Instalace na základě rolí nebo základě funkcí → vybereme server a potvrdíme tlačítkem Další → zaškrtneme Služba Active Directory Domain Services a potvrdíme → Přidat funkce → Další → Další → Nainstalovat). Po úspěšné instalaci můžeme kliknout na tlačítko Zavřít). Před dalším krokem je potřeba zkontrolovat, zda heslo správce splňuje minimální požadavky pro složitost hesla (alespoň šest znaků, v heslu se nacházejí alespoň tři znaky z následujících čtyř kategorií – velká písmena, malá písmena, čísla, ne alfanumerické znaky). Také je nutné zajistit, aby administrátorský účet vyžadoval heslo, to lze udělat z příkazové řádky, spuštěné jako správce, zadáním příkazu *net user NazevUzivateleAdmina /passwordreq:yes*.

Po přidání role se ve Správci serveru zobrazí notifikace – žlutý vykřičník, je potřeba povýšit server na řadič domény. Klikneme na Povýšit tento server na řadič domény, spustí se nám průvodce (zaškrtneme Přidat novou doménovou strukturu, zadáme název domény a klikneme na Další → zvolíme Úroveň funkčnosti domény (úroveň funkčnosti volíme podle nejstaršího operačního systému jiného řadiče domény v doménové struktuře. Pokud je v síti pouze jeden řadič, můžeme zvolit maximální úroveň) a zadáme heslo pro obnovení adresářových služeb a klikneme na Další → Další → Další → Instalovat). Server se automaticky restartuje, po restartu se hlásíme už jako *nazev_domeny\Administrator*.



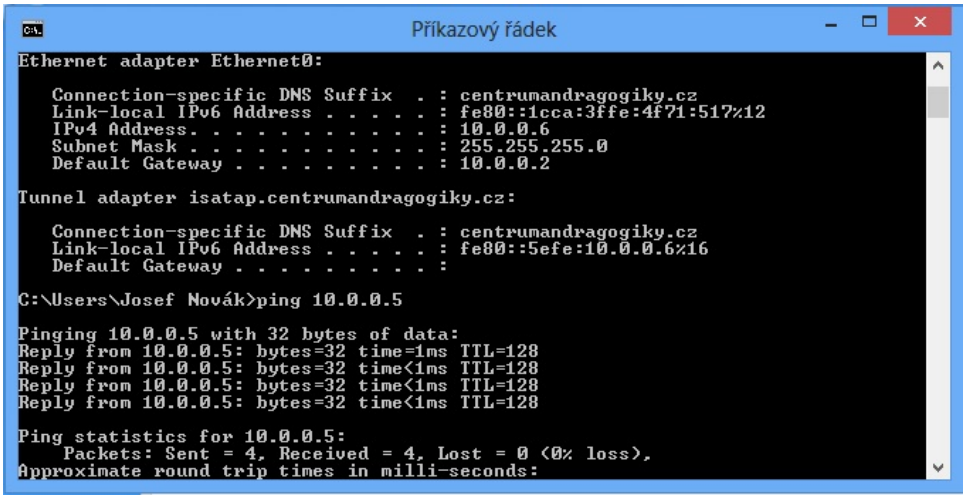
Obrázek 14: Přidání role Active Directory

Zdroj: Vlastní zpracování

4.7 Skupiny a uživatelé v Active Directory

Otestujeme si funkčnost služby Active Directory tím, že připojíme pracovní stanici do domény. Stanice má nainstalovaný operační systém Windows 8, její IP adresa je *10.0.0.6 /24*. IP adresa našeho serveru je *10.0.0.5 /24*. Nejprve otestujeme spojení mezi stanicí a serverem příkazem *ping*. Poté vytvoříme uživatele *Josef Novák* (heslo: *TestNovak23*), který bude ve skupině *ITOddeleni*. Pokud využijeme při práci skupiny, velmi si tím usnadníme práci, dovoluje nám to aplikovat řadu nastavení na ucelenou skupinu uživatelů. A nakonec připojíme stanici do domény.

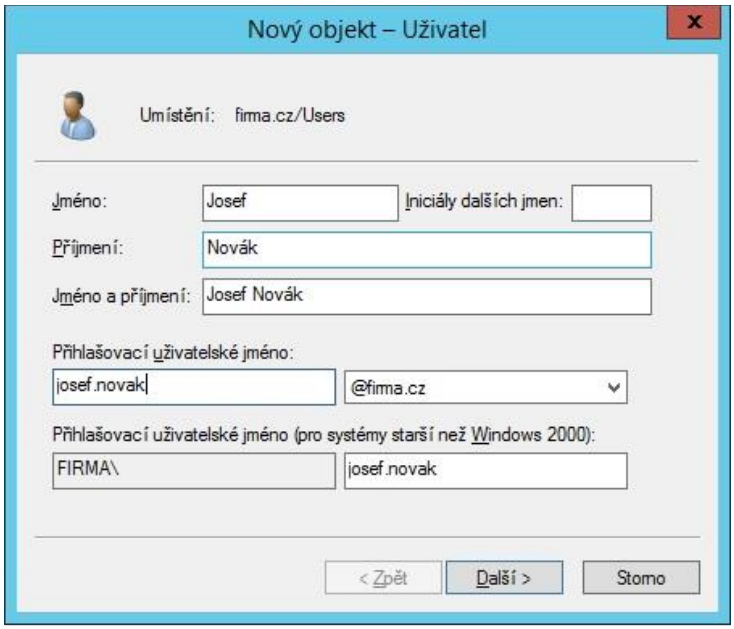
Začneme tedy otestováním spojení, spustíme příkazovou řádku (Win + R), napíšeme příkaz *ping IP_adresa_stanice*. Ping odesílá IP datagramy a očekává odezvu protistrany. V případě kladného výsledku vidíme v závěrečném statistickém souhrnu Sent = 4, Received = 4, tedy odeslali jsme čtyři malé datové pakety a všechny se nám úspěšně vrátily zpět (viz. Obrázek 15).



Obrázek 15: Testování spojení mezi stanicí a serverem

Zdroj: Vlastní zpracování

Přidáme uživatele *Josef Novák* v nabídce Uživatelé a počítače služby Active Directory (Win → Nástroje pro správu → Uživatelé a počítače služby Active Directory), rozklikneme si složku s názvem domény → Users, zde klikneme pravým tlačítkem myši na Users → Nová položka → Uživatel. Vyplníme jméno, příjmení, přihlašovací uživatelské jméno. My zvolíme přihlašovací jméno ve tvaru *jmeno.prijmeni*, tedy *josef.novak*. V dalším kroku zvolíme heslo - v našem případě *TestNovak23*, odškrtneme volbu Při dalším přihlášení musí uživatel změnit heslo, tím si trochu zjednodušíme práci. Jinak bychom museli při dalším přihlášení znovu volit nové heslo.



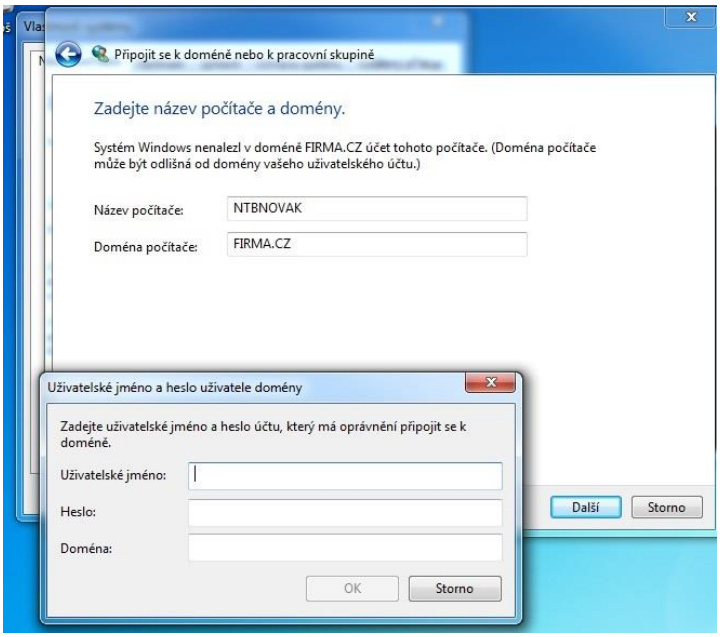
Obrázek 16: Přidání uživatele

Zdroj: Vlastní zpracování

Pokud klikneme dvakrát levým tlačítkem myši na uživatele, otevře se nastavení pro jednotlivého uživatele, můžeme zde přidat více informací k uživateli, odemknout účet, nastavit vypršení platnosti účtu, mapování cestovního profilu, zobrazení a úpravy členství ve skupinách a další.

Obdobně přidáme skupinu *ITOddeleni* (klikneme pravým tlačítkem myši na Users → Nová položka → Skupina). Jeden ze způsobů, jak uživatele do skupiny přiřadit, je kliknout pravým tlačítkem myši na uživatele (v našem případě *Josef Novák*) → Přidat do skupiny → napíšeme název skupiny – *ITOddeleni* → OK.

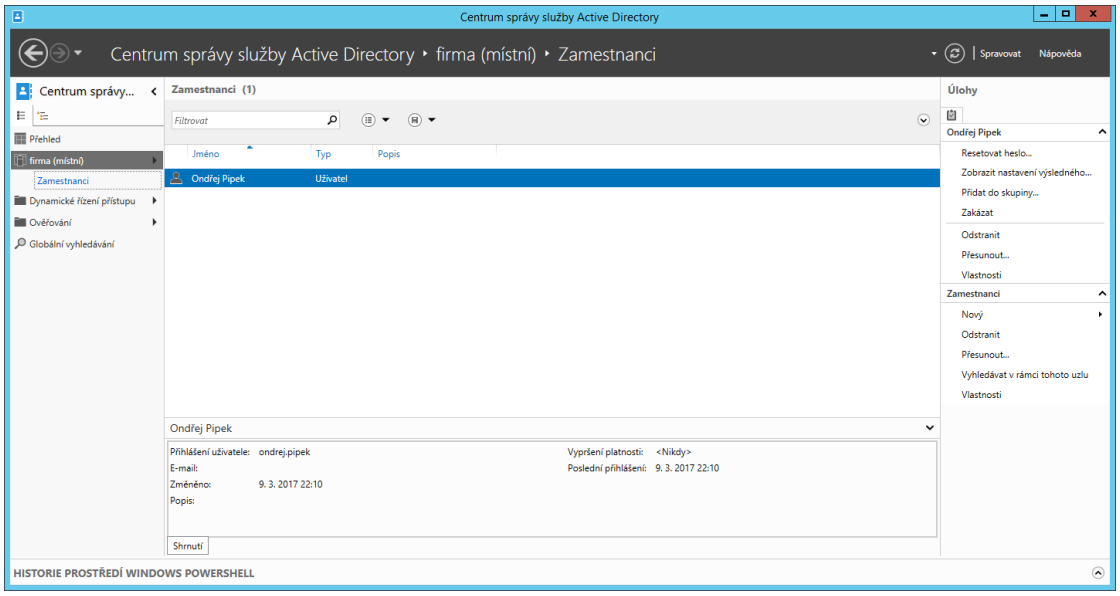
Pracovní stanici připojíme do domény v nabídce Vlastnosti systému (pravým tlačítkem myši na Počítač → Vlastnosti → Upřesnit nastavení systému → záložka Název počítače), klikneme na tlačítko ID sítě (musíme mít operační systém alespoň ve verzi Professional, jinak není toto tlačítko aktivní), zaškrtneme volbu Tento počítač je součástí podnikové sítě a je používán k připojení k dalším počítačům v práci → Společnost používá síť s doménou → Další → vyplníme uživatelské jméno *josef.novak*, heslo *TestNovak23* a název domény *firma.cz* → v dalším kroku vyplníme název počítače a doménu → naposled vyplníme uživatelské jméno, heslo a doménu. Proces je nutné dokončit restartem počítače. Po restartu se přihlásíme uživatelským jménem ve tvaru *doména/uzivatelske.jmeno*.



Obrázek 17: Připojení pracovní stanice do firemní domény

Zdroj: Vlastní zpracování

Druhou možností, jak spravovat uživatele, skupiny, počítače do Active Directory infrastruktury je využít Centrum správy služby Active Directory (Správce serveru → Centrum správy služby Active Directory), je to novinka WS2012, obsahuje vylepšené funkce možnosti správy, má modernější design a práce v něm je přehlednější.



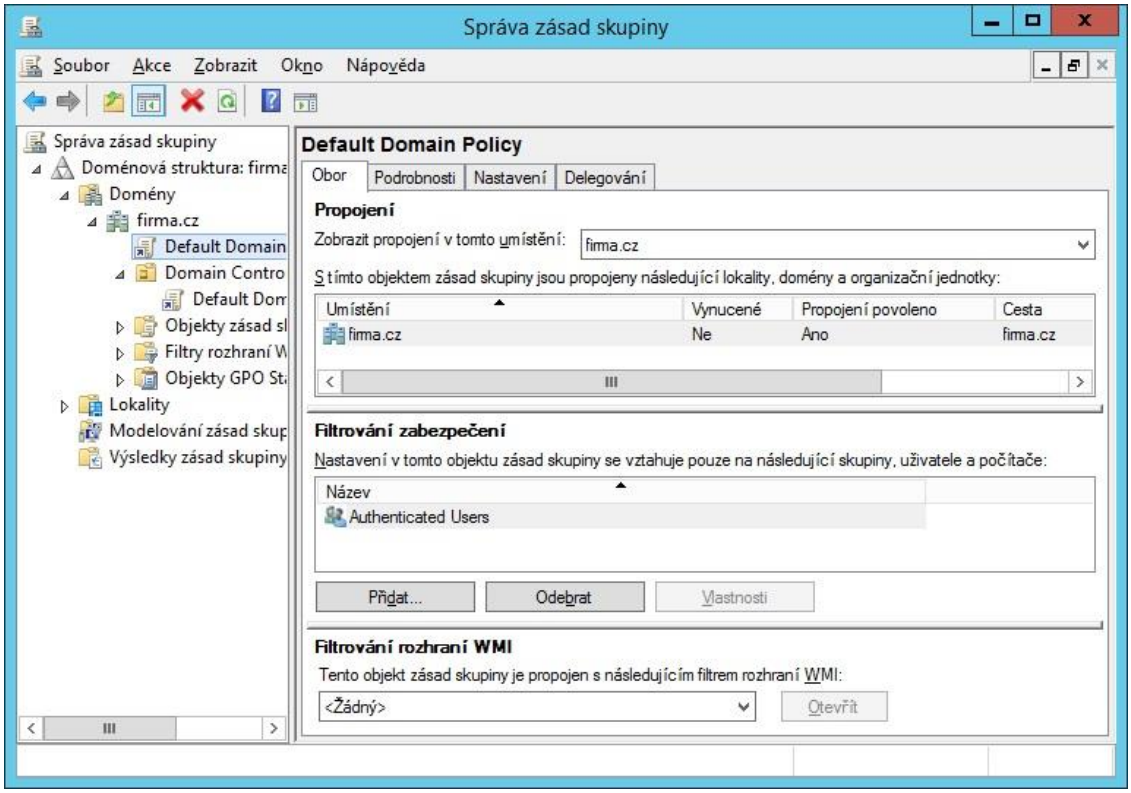
Obrázek 18: Centrum správy služby Active Directory

Zdroj: Vlastní zpracování

4.8 Group policy

Užitečnost skupinových politik bude demonstrována na následujícím příkladu. Celému IT oddělení potřebujeme připojit sdílenou složku na serveru. Složka je uložena na adrese *\\Rory\Share\Realizace*, složka je sdílená a celé IT oddělení má práva alespoň ke čtení složky a souborů ve složce. Pomocí skupinových politik připojíme všem uživatelům v IT oddělení sdílenou složku při přihlašování uživatele.

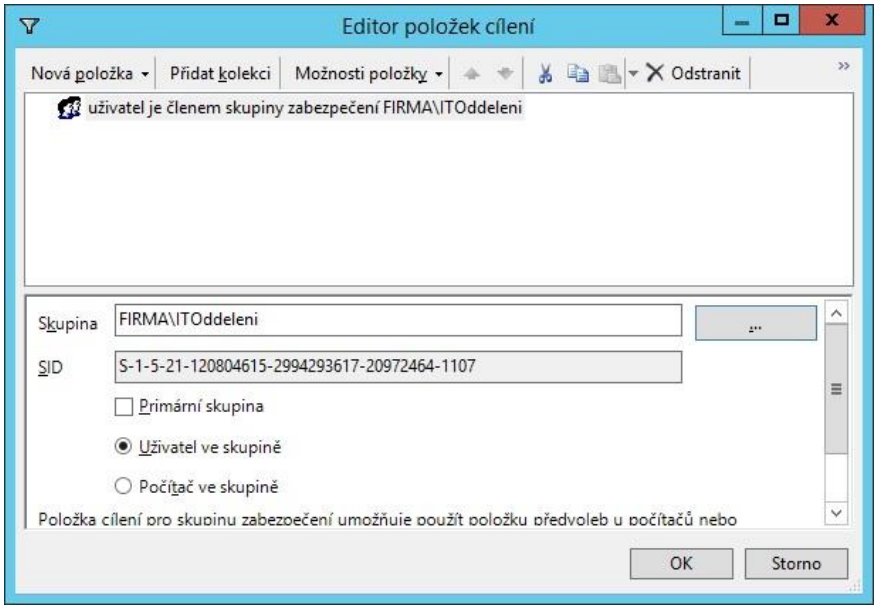
Začneme zapnutím programu Správa zásad skupiny (Správce serveru → Nástroje → Správa zásad skupiny). Rozklikneme si Doménová struktura → Domény → *jméno_domény*. Nyní budeme upravovat Default Domain Policy (pravým tlačítkem myši klikneme → Upravit), Default Domain Policy obsahuje politiky nastavení, které se aplikují na všechny počítače a uživatele v doméně. Nyní se nám otevře Editor správy zásad skupiny, kde si rozklikneme Konfigurace uživatele → Předvolby → Nastavení systému Windows → Mapování jednotek → klikneme pravým tlačítkem myši do bílého prázdného pole → Nová položka → Mapovaná jednotka. Zadáme umístění ve tvaru *\\IP_adresa_serveru\sdílená _složka,* v našem případě tedy *\\10.0.0.5\Share*.



Obrázek 19: Správa zásad skupiny

Zdroj: Vlastní zpracování

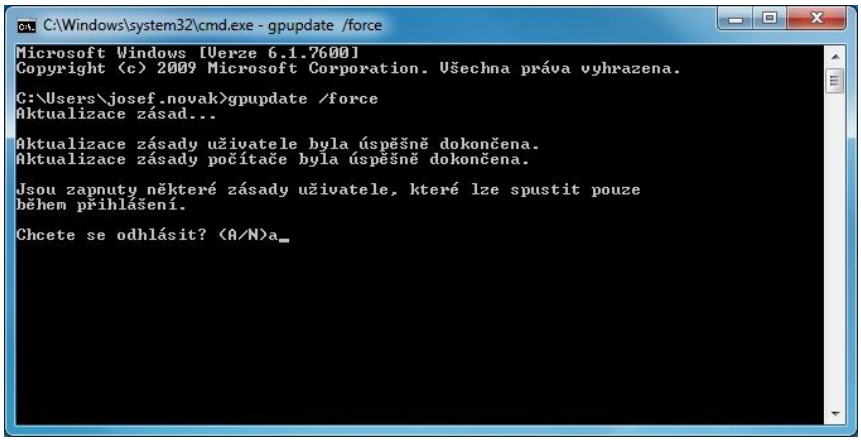
V dalším kroku vyfiltrujeme nastavení pouze na určitou skupinu uživatelů (záložka Společné → zaškrtneme Cílení na úrovni položky → Cílení → Nová položka → Skupina se zabezpečením → klikneme na tři tečky → vyplníme jméno skupiny, tedy *ITOddeleni* → potvrdíme OK).



Obrázek 20: Editor položek cílení

Zdroj: Vlastní zpracování

Na pracovní stanici spustíme příkazový řádek (Win + R), zadáme příkaz pro vynucení aplikace politik *gpupdate /force*. Pokud je to potřeba, odhlásíme uživatele. Při příštím přihlášení vidíme síťovou jednotku připojenou.

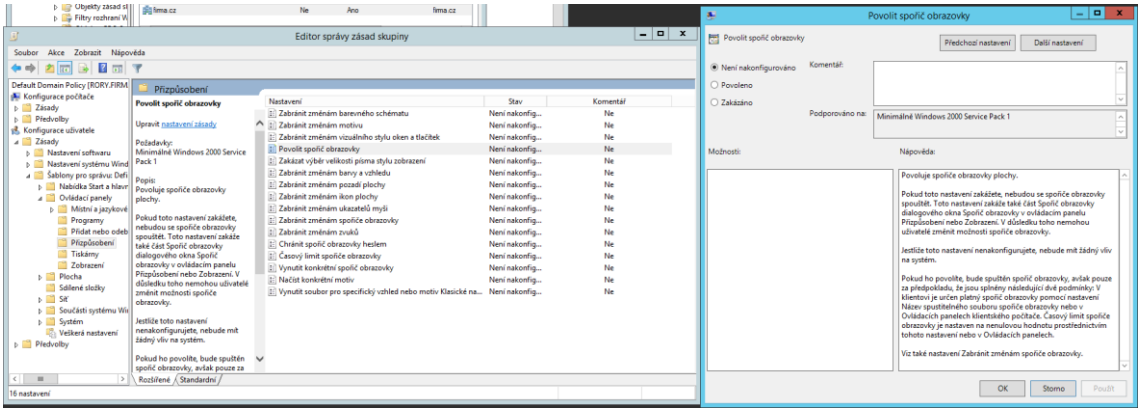


Obrázek 21: Příkazový řádek - vynucení aplikace politik

Zdroj: Vlastní zpracování

Vyzkoušíme si ještě přes skupinové politiky zakázat spořič obrazovky a maximální stáří hesla přenastavíme na 30 dní. Začneme opět ve Správě zásad skupin (Správce serveru → Nástroje → Správa zásad skupiny). Rozklikneme si Doménová struktura → Domény → *jméno_domény*. Budeme upravovat Default Domain Policy (pravým tlačítkem myši klikneme → Upravit), nastavení se tedy bude týkat všech uživatelů a počítačů. Nejprve zakážeme spořič obrazovky, v Editoru správy zásad

skupiny si rozklikneme Konfigurace uživatele → Zásady → Šablony pro správu: Definice zásad → Přizpůsobení → Povolit spořič obrazovky → zaškrtneme Zakázáno → potvrdíme OK. Nyní ještě přenastavíme maximální stáří hesla, rozklikneme si Konfigurace počítače → Zásady → Nastavení systému Windows → Nastavení zabezpečení → Zásady účtů → Zásady hesla → Maximální stáří hesla → Platnost hesla přepíšeme na 30 dnů → potvrdíme OK. Na pracovní stanici zadáme opět příkaz pro vynucení aplikace politik, pokud to bude potřeba, odhlásíme uživatele. Při dalším přihlášení zkontrolujeme, zda je spořič zakázán a nastavené maximální stáří hesla.



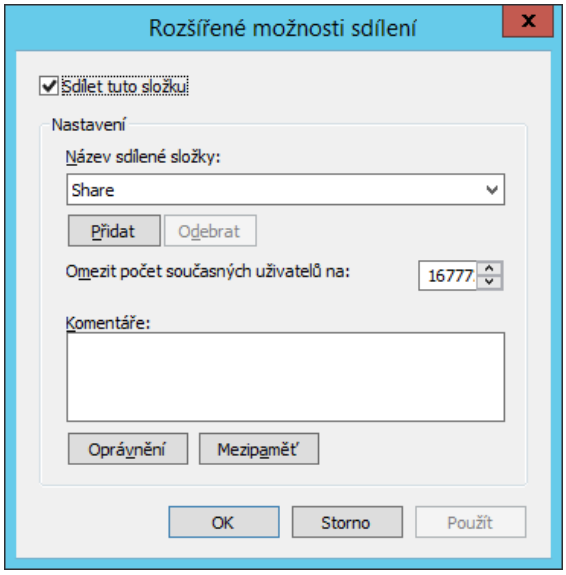
Obrázek 22: Editor správy zásad skupiny, zakázání spořiče obrazovky

Zdroj: Vlastní zpracování

4.9 Sdílení souborů

V tomto případě žádnou roli instalovat nebudeme, Souborová služba je nainstalována v základu. Budeme sdílet složku *Share*, kterou jsme si automaticky připojili jako síťovou jednotku v předchozí kapitole.

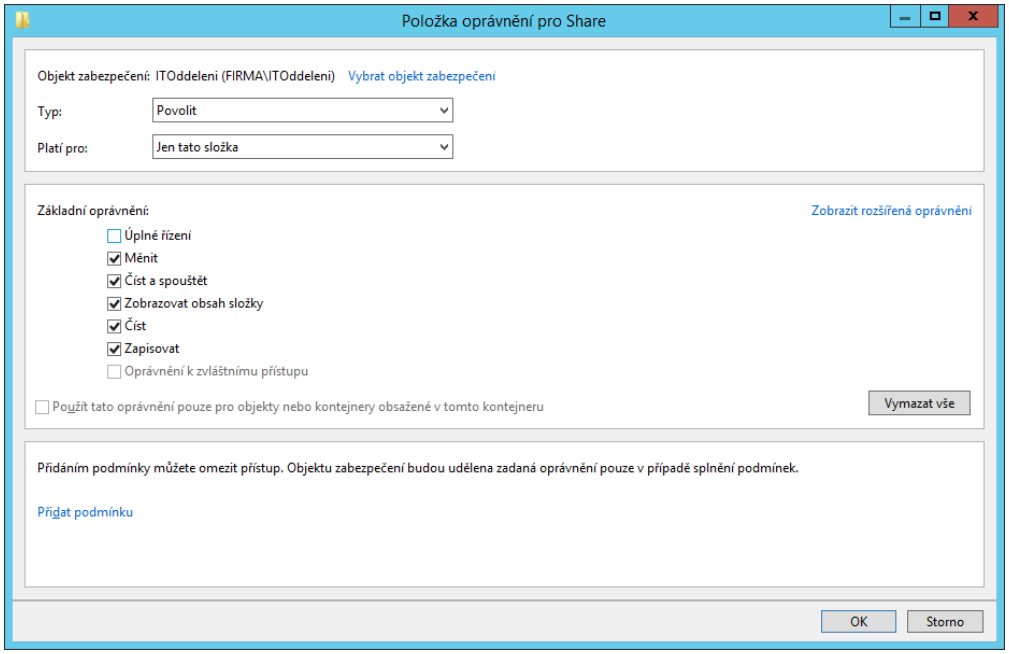
Sdílení se nastavuje ve vlastnostech složky (klikneme pravým tlačítkem myši na složku *Share* → Vlastnosti), vybereme záložku Sdílení → Rozšířeném možnosti sdílení → zaškrtneme Sdílet tuto složku → Oprávnění → odebereme skupinu Everyone → přidáme skupinu Authenticated Users → necháme zaškrtlé oprávnění pouze pro čtení a potvrdíme.



Obrázek 23: Sdílení složky

Zdroj: Vlastní zpracování

Nyní nastavíme přístupová práva ke složce, to znamená, kdo a co může se složkou dělat. Ukážeme si nejjednodušší variantu, skupina *ITOddeleni* bude mít plný přístup do složky Share a všech podsložek a souborů. Klikneme pravým tlačítkem myši na složku → Vlastnosti → zvolíme záložku Zabezpečení → Upřesnit → Přidat → Vybrat objekt zabezpečení → napíšeme *ITOddeleni*, potvrdíme OK → zaškrtneme Měnit, Číst a spouštět, Zobrazovat obsah složky, Číst, Zapisovat → OK. Pokud bychom potřebovali nastavit přístup pouze do některých složek pod složkou Share, na přepínači „Platí pro“ bychom přepnuli Jen tato složka (viz. Obrázek 24), přístupová práva bychom nastavovali o hierarchii níže každé složce zvlášť.

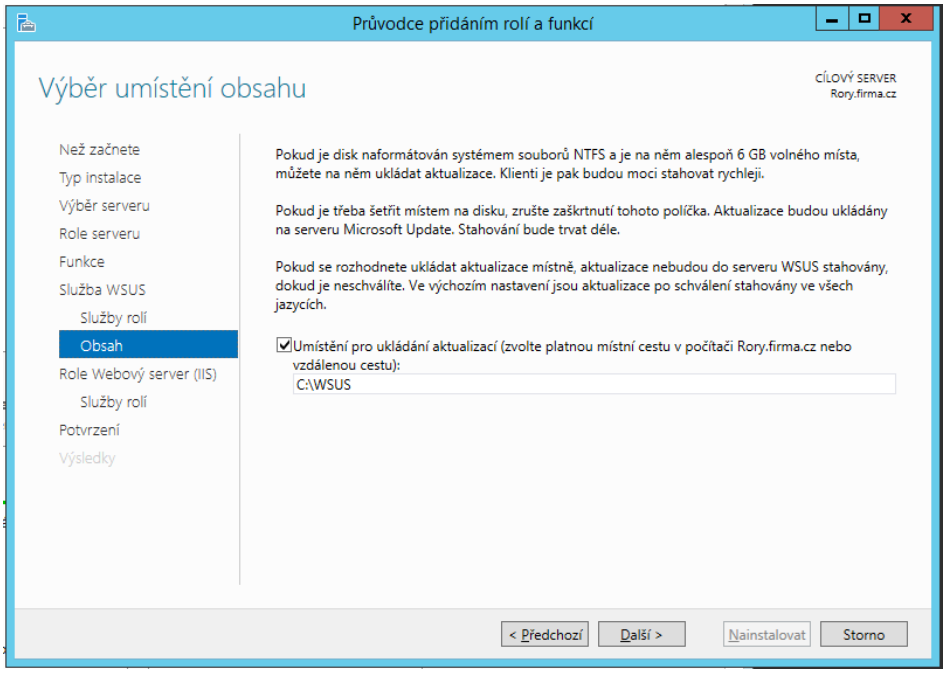


Obrázek 24: Nastavení přístupových práv

Zdroj: Vlastní zpracování

4.10 Windows Server Update Services (WSUS)

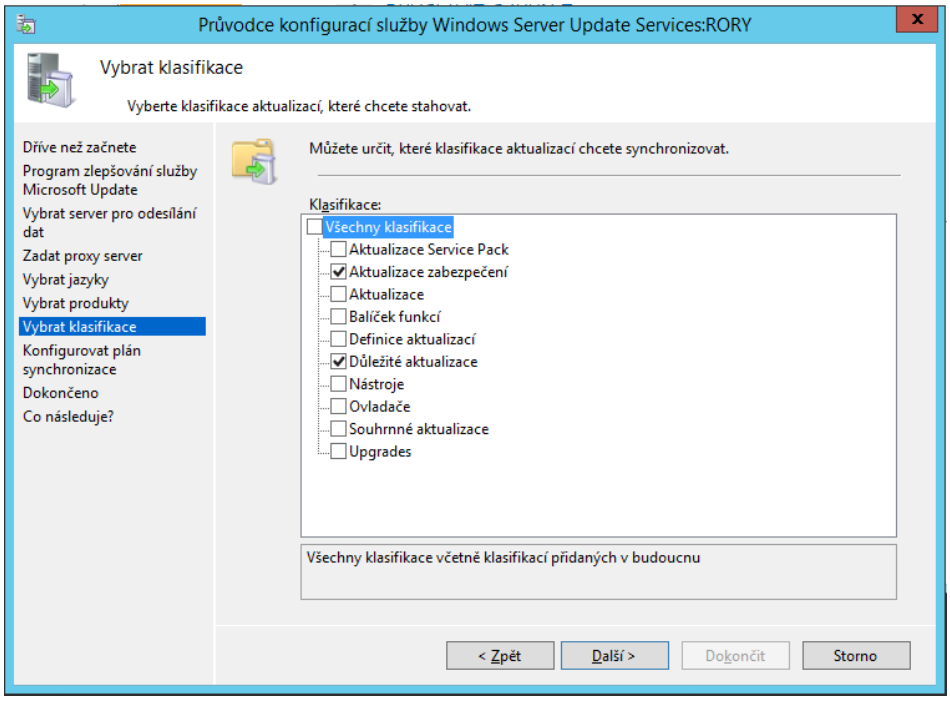
Před instalací WSUS, musí být splněné dva požadavky. Server musí být připojen do domény nebo být doménovým řadičem, nezbytné je připojení k internetu a musí mít statickou IP adresu. Instalaci začneme přidáním role WSUS (Správce serveru → Správa → Přidat role a funkce → Další → vybereme náš server a potvrdíme tlačítkem Další → zaškrtneme Windows Server Update Services → Přidat funkce → Další → Další → zvolíme cestu do složky na disku, kam chceme ukládat aktualizace v našem případě například *C:\WSUS* a potvrdíme tlačítkem Další → při instalaci WSUS je potřeba mít nainstalovaný webový server IIS, pokud ho ještě nainstalován nemáme, v tomto kroku potvrdíme instalaci tlačítkem Další → Další → Nainstalovat), po úspěšné instalaci průvodce zavřeme tlačítkem Zavřít.



Obrázek 25: Přidání role Windows Server Update Services

Zdroj: Vlastní zpracování

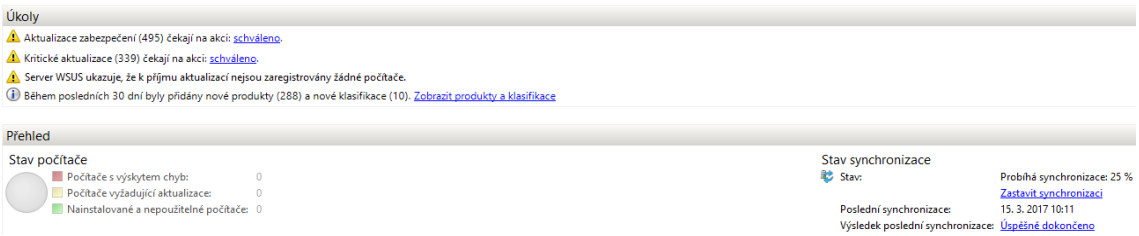
Při spuštění WSUS se otevře průvodce konfigurací (Správce serveru → Nástroje → Windows Server Update Services). Průvodce konfigurací služeb nás provede všemi kroky nastavení (Další → Další → zaškrtneme Synchronizovat z webu Microsoft Update a klikneme na tlačítko Další → pokud používáme proxy server, vyplníme potřebné údaje → stáhneme typy dostupných aktualizací, produkty, dostupné jazyky, tento krok trvá několik minut i déle, záleží na rychlosti internetového připojení, stahování spustíme tlačítkem Spustit připojování → Další → vybereme aktualizace pouze v jazyku Angličtina a Čeština → Další → vybereme produkty, které chceme stahovat, v našem případě pouze Office 2010, 2013 a Windows 7, 8 → Další → vybereme klasifikace, která chceme stahovat, pokud máme rychlé připojení k internetu, můžeme zvolit vše, my vybereme pouze Důležité aktualizace a Aktualizace zabezpečení → Další → zvolíme synchronizovat ručně → Další → zaškrtneme Spustit počáteční synchronizaci → Dokončit).



Obrázek 26: Průvodce konfigurací služby WSUS

Zdroj: Vlastní zpracování

Automaticky se spustí služba WSUS, počkáme, než se dokončí stav synchronizace (v levé rozbalovací nabídce klikneme na jméno našeho serveru). Tento krok trvá průměrně v desítkách minut, ale může i déle, záleží to na rychlosti připojení k internetu. Pokud vše proběhlo v pořádku, výsledek poslední synchronizace je Úspěšně dokončeno.



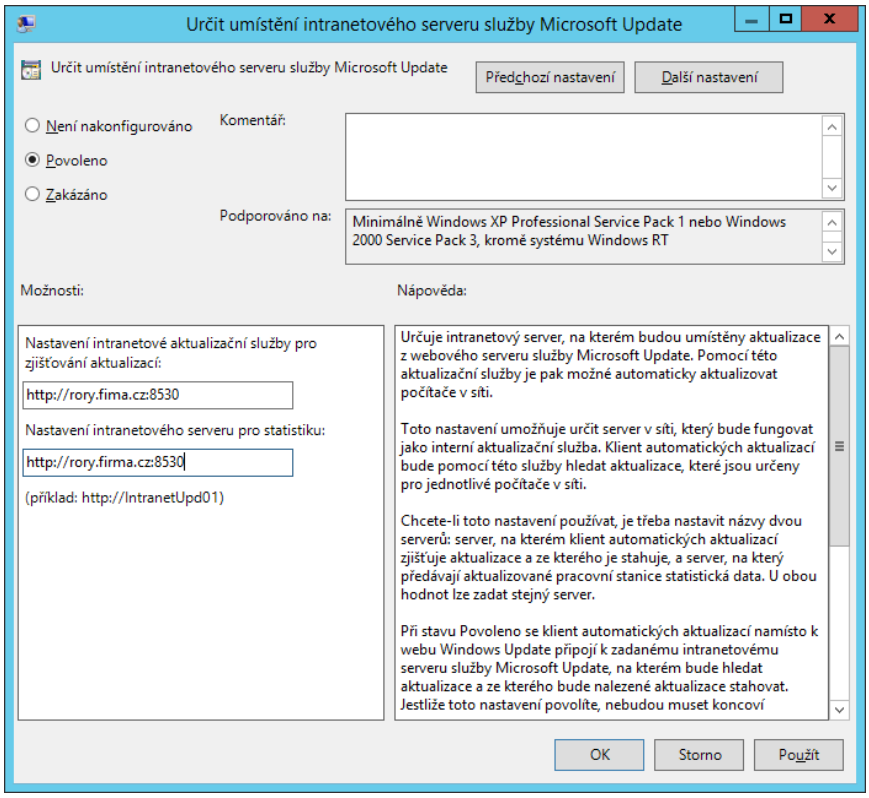
Obrázek 27: Synchronizace WSUS

Zdroj: Vlastní zpracování

Nyní určíme, jak budou počítače zařazovány do skupiny (Možnosti → Počítače → zaškrtneme Použijte zásady skupiny nebo nastavení registru v počítačích → potvrdíme OK). Tuto volbu jsme zaškrtli, protože budeme nastavovat pomocí skupinových politik změnu nastavení v přijímání aktualizací.

Přejdeme do Správy zásad skupiny (Správce serveru → Nástroje → Správa zásad skupiny), budeme upravovat Default Domain Policy (pravým tlačítkem myši

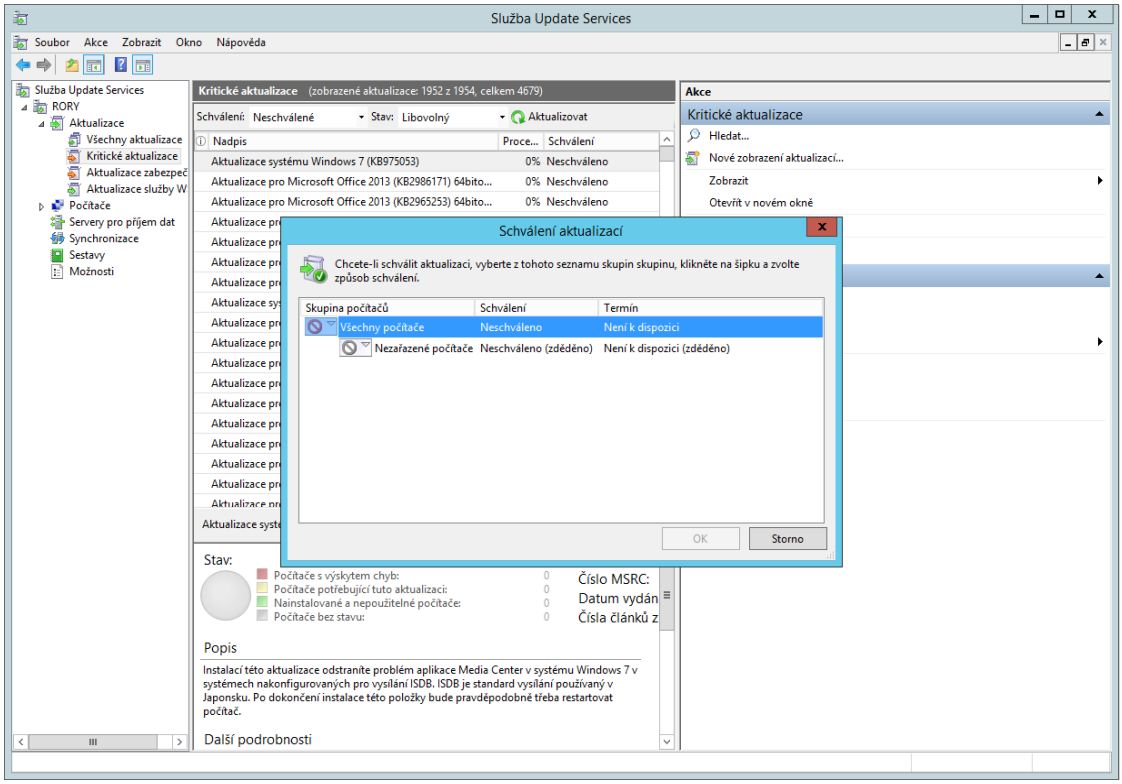
klikneme → Upravit). Otevře se nám Editor správy zásad skupiny, kde si rozklikneme Konfigurace počítače → Šablony pro správu: Definice zásad → Součásti systému Windows → Windows Update. Otevřeme Konfigurace automatických aktualizací → zaškrtneme povoleno a čas zvolíme například 16:00. Rozklikneme Určit umístění intranetového serveru služby Microsoft Update → zaškrtneme Povoleno, vyplníme adresu intranetové aktualizační služby a port, v našem případě *http://rory.firma.cz:8530* a potvrdíme OK. Čas je vhodné zvolit tak, aby aktualizace probíhali v době, kdy uživatelé nebudou pociťovat jako velké omezení případné určité snížení rychlosti odezvy osobního počítače. Větší aktualizační balíčky mohou počítač zatížit a jeho odezvu zpomalit.



Obrázek 28: Určení umístění intranetového serveru služby Microsoft Update

Zdroj: Vlastní zpracování

Na serveru ve Službě Update Services rozklikneme náš server → Kritické aktualizace → otevřeme aktualizaci, kterou požadujeme schválit → klikneme na schváleno k instalaci a potvrdíme OK.



Obrázek 29: Schvalování aktualizací

Zdroj: Vlastní zpracování

4.11 Monitorování serveru

Nejlepší je o problému vědět, předtím než se stane. Proto je dobré server průběžně monitorovat a problém případně vyřešit dřív, než nastane kritická situace. Monitorovat situaci můžeme v integrovaných programech v operačním systému a to například ve Správci serveru, Prohlížeči událostí, Sledování výkonu a prostředků.

Monitorování Správce serveru

V případě více serverů můžeme v konzoli Správce serveru sledovat několik najednou, vše co je potřeba udělat je servery přidat (Správa → Přidat servery).

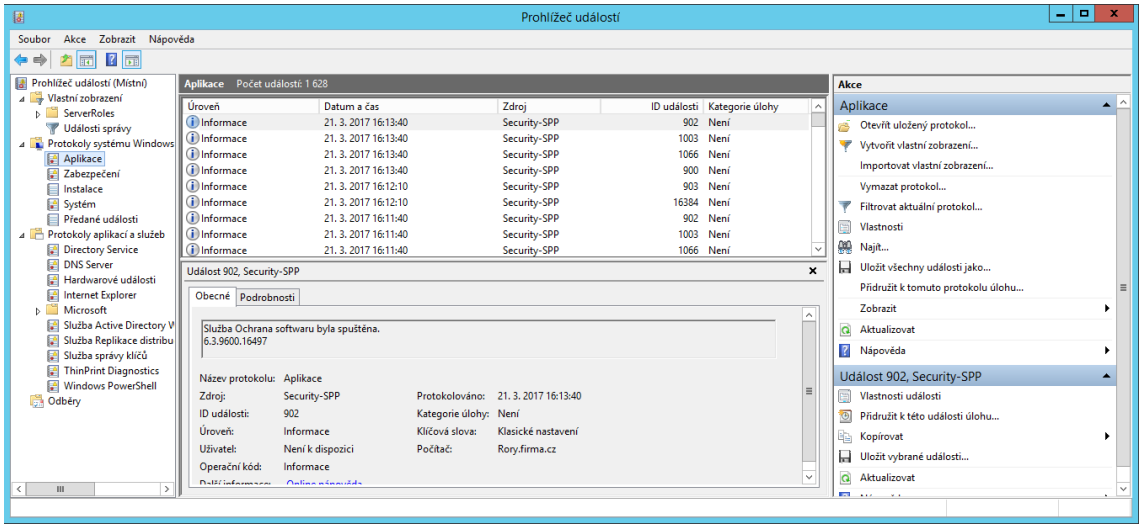
Rozklikneme nabídku Místní server v levém sloupci, otevře se nám okno s jednotlivými sekcemi. My si popíšeme sekce Události, Služby, Analyzátor osvědčených postupů. Oblast Události nám poskytuje přehled o kritických, chybových a varovných událostech. Pokud klikneme na konkrétní událost, otevře se nám stručný popis události. Podstatným parametrem je ID události, podle kterého můžeme na internetu hledat vhodné řešení. Sekce služby zajišťuje přehled o běžících nebo

neběžících službách na serveru. Pokud klikneme na službu pravým tlačítkem, můžeme ji spustit, pozastavit, zastavit nebo restartovat.

Kontrola analyzátorem osvědčených postupů ověří způsob konfigurace podle nejvhodnějšího způsobu definovaným odborníky. Pokud je to potřeba, doporučí, co přenastavit jinak. Ne vždy upozornění nebo chyby znamenají nutně problém, analyzátor může indikovat způsob konfigurace, která snižuje výkon, spolehlivost serveru nebo zabezpečení serveru. Výsledky kontroly můžeme filtrovat. Spuštění kontroly provádíme v grafickém prostředí kliknutím tlačítkem myši na Úlohy → Spustit kontrolu Analyzátorem osvědčených postupů.

Monitorování Prohlížeč událostí

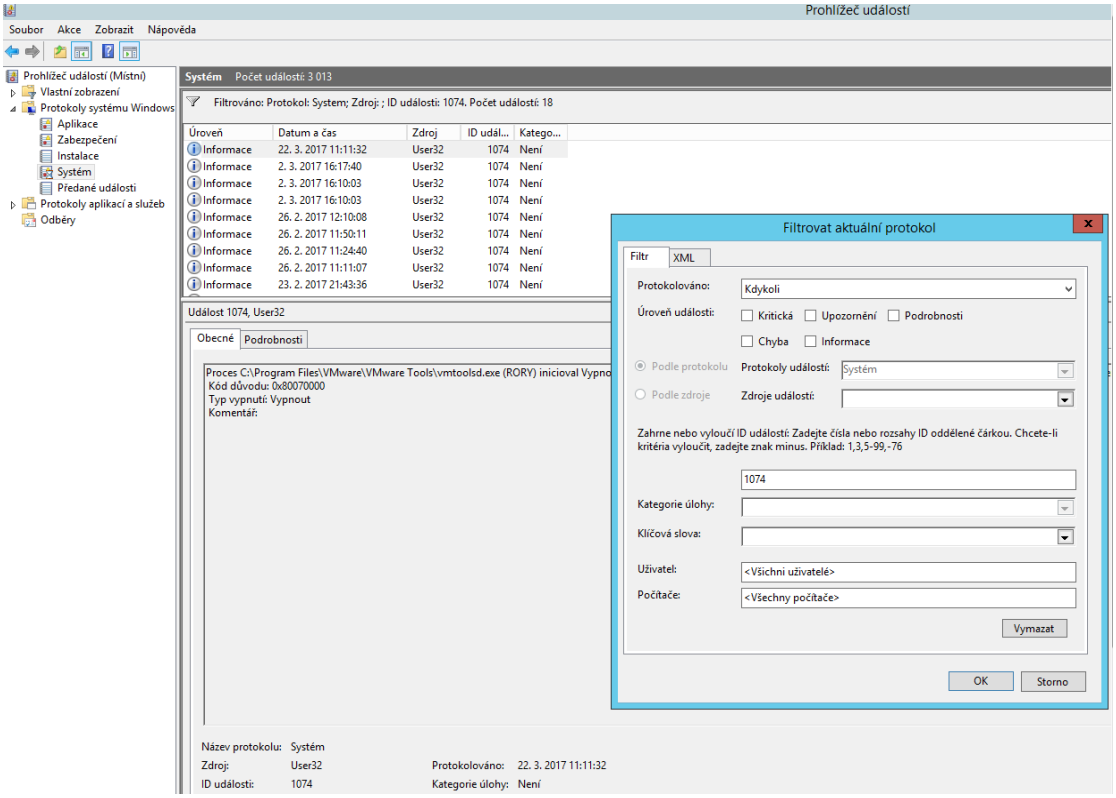
Prohlížeč událostí vytváří přehled o všem, co se v počítači děje. Abychom našli, co potřebujeme, musíme se naučit filtrovat události. Začneme spuštěním Prohlížeče události (Správce serveru → Nástroje → Prohlížeč událostí).



Obrázek 30: Prohlížeč událostí

Zdroj: Vlastní zpracování

Nyní si ukážeme, jak v prohlížeči událostí vyfiltrovat seznam všech vypnutí s datem a časem. V levé části okna si rozbalíme nabídku Protokoly systému Windows, pravým tlačítkem klikneme na Systém → Filtrovat aktuální protokol. Pole ID vyplníme hodnotou 1074 a potvrdíme OK. Nyní se nám otevře přehled vypnutí.



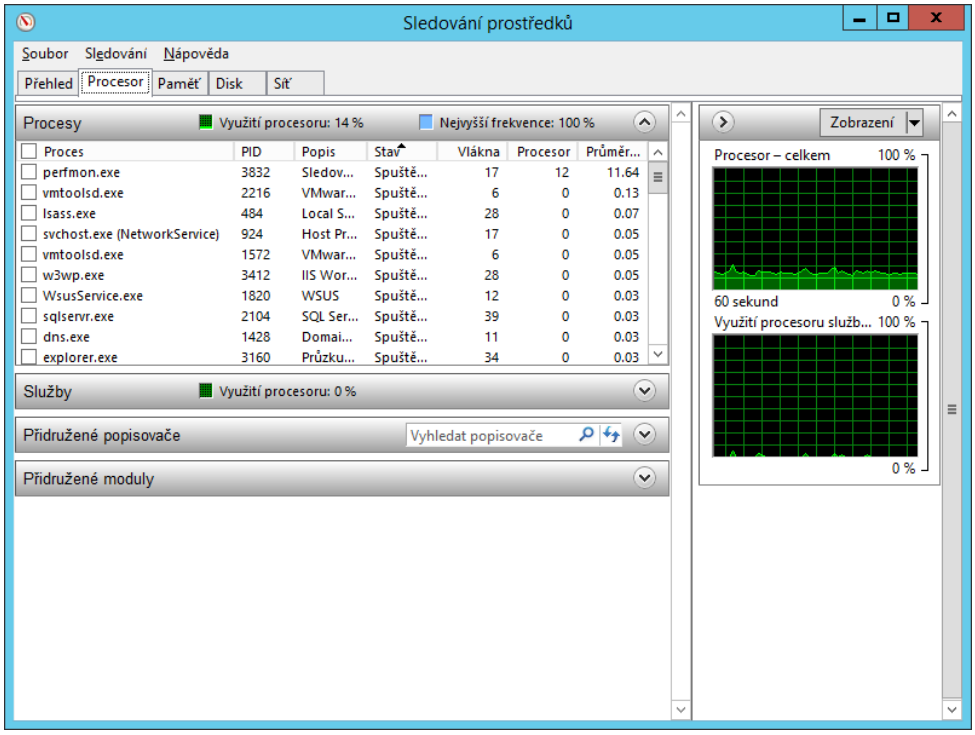
Obrázek 31: Prohlížeč událostí, filtrování událostí podle ID

Zdroj: Vlastní zpracování

Monitorování Sledování prostředků

V programu Sledování prostředků vidíme, jak běžící procesy zatěžují náš hardware serveru v reálném čase. Nejkomplexnější je záložka Přehled, která nám poskytne celkový přehled, uvidíme využití procesoru, disku, sítě a paměti. Pokud chceme sledovat pouze využití například procesoru, využijeme záložku Procesor a podobně tomu je i u ostatních záložek.

Sledování prostředků spustíme ve Správce serveru → Nástroje → Sledování prostředků.



Obrázek 32: Sledování prostředků

Zdroj: Vlastní zpracování

Vyhodnocení hypotéz

V této kapitole budou uvedeny výsledky testovaných hypotéz a základní charakteristika dotazovaných respondentů.

Charakteristika dotazovaných respondentů

Výsledky hypotéz jsou založeny na odpovědích celkem 5 respondentů v hloubkovém interview.

Věková kategorie	Počet
Do 30 let	3
31-45 let	1
46-60 let	1

Tabulka 4: Charakteristika respondentů - věková kategorie

Zdroj: Vlastní zpracování

Pohlaví	Počet
Muž	5
Žena	0

Tabulka 5: Charakteristika respondentů - pohlaví

Zdroj: Vlastní zpracování

Nejvyšší ukončené vzdělání	Počet
Střední s maturitou	2
Vysokoškolské nebo vyšší odborné	3

Tabulka 6: Charakteristika respondentů - nejvyšší ukončené vzdělání

Zdroj: Vlastní zpracování

Délka praxe	Počet
Do 2 let	2
3-15 let	2
16 a více let	1

Tabulka 7: Charakteristika respondentů - délka praxe

Zdroj: Vlastní zpracování

H1: Většina správců sítě by tuto metodickou příručku označila jako použitelnou v praxi.

Výsledek dat pro H1:

Tři z pěti oslovených respondentů na otázku odpovědělo kladně, tedy 60 % z oslovených správců sítě by tuto příručku použili při konfiguraci WS2012.

H2: Správci sítě při řešení problému při konfiguraci nejčastěji používají internet.

Výsledek dat pro H2:

Čtyři z pěti oslovených respondentů na otázku odpovědělo internet, tedy 80 % z oslovených správců sítě se snaží najít vhodné řešení nejprve na internetu.

ZÁVĚR

Cílem práce bylo vytvoření jednoduché metodické příručky, která by měla pomoci začínajícím správcům sítě nebo také přinést potřebné informace lidem, kteří se o správu serverů teprve začínají zajímat. V teoretické části bakalářské práce autor nejprve popsal použité síťové technologie a služby. Další kapitola se týká stávající síťové infrastruktury firmy, ve které autor pracuje. Následuje kapitola o výzkumném šetření, kde jsou potvrzeny nebo vyvráceny jednotlivé hypotézy. Praktická část pojednává o konfiguraci WS2012, kde jsou popsány jednotlivé kroky a vizuálně zobrazeny na přiložených otiscích obrazovky.

Vzhledem k rozsahu práce není možné popsat všechny služby a postupy konfigurace. Každé firemní prostředí je velmi individuální, proto je důležité nastudovat si a pochopit nastavení a pak jej teprve aplikovat ve své vlastní firemní infrastruktuře.

Kvůli stále rostoucímu výpočetnímu výkonu a snižování finančních nákladů se v praxi setkáváme s virtualizací serverů a také s více servery ve firmě. My jsme v této práci popsali jednodušší model, malé firmy pouze s jedním serverem. Tento server obsluhuje všechny požadavky a služby. Server uživatelům zajišťuje sdílení souborů, nastavení síťové komunikace a správu nastavení pracovních stanic.

Navazující výzkum či diplomová práce by se mohla zaměřit ještě i na problematiku poštovních serverů a to konkrétně na Microsoft Exchange, který by se tematicky do obsahu práce hodil. Tento systém je však velice komplexní a jeho detailní popis by byl natolik rozsáhlý, že by přesáhl rozsah bakalářské práce, a proto se jeho představení bude věnovat navazující výzkum autora.

Literární zdroje

CLINES, Steve. a Marcia. LOUGHRY. *Active directory for dummies*. 2nd ed. Hoboken, NJ: Wiley Pub., c2008. ISBN 978-0-470-28720-0.

LYNN, Samara. *Windows server 2012: up and running*. Sebastopol, CA: O'Reilly Media, 2012. ISBN 978-1-449-32075-1.

MINASI, Mark, Kevin GREENE, Christian BOOTH, Robert BUTLER, John MCCABE, Robert PANEK, Michael RICE a Stefan ROTH. Mastering Windows Server 2012 R2. Indianapolis: Sybex, 2014. ISBN 978-1-118-28942-6.

PANEK, William. MCSA Windows Server 2012 R2 complete study guide. Indianapolis, Indiana: Sybex, 2015. ISBN 11-188-5991-X.

STANEK, William R., 2015. Microsoft Windows Server 2012: kapesní rádce administrátora. 1. vydání. Brno: Computer Press, 736 stran. ISBN 978-80-251-3817-5.

STANEK, William R. *Microsoft Windows server 2012 inside out*. Redmond, Wash.: Microsoft Press, c2013. ISBN 978-0-7356-6631-3.

Ostatní zdroje

CENTRUM ANDRAGOGIKY, © 2017. Centrumandragogiky.cz [online]. [cit. 2017-01-04]. Dostupné z: http://www.centrumandragogiky.cz/

CLERCQ, Jan De, 2007. Comparing Windows Kerberos and NTLM Authentication Protocols. In: Windows IT Pro | Microsoft Windows Information, Solutions, Tools [online]. March 25, 2007, [cit. 2017-1-11]. Dostupné z: http://windowsitpro.com/security/comparing-windows-kerberos-and-ntlm-authentication-protocols

KANTŮREK, Tomáš, 2013. Windows Server 2012 R2 – co je nového? [online] 29. září 2013. [cit. 2015-10-22]. Dostupné z: http://www.daquas.cz/articles/621-windows-server-2012-r2-co-je-noveho

KOHOUTOVÁ, Hana, 2015. 7 věcí, které musíte překonat na cestě k dotacím. Jak se stát milionářem [online]. 2015 [cit. 2017-01-05]. Dostupné z: http://jaksestatmilionarem.cz/index.php/vzdelani/blog-vzdelani/584-7-veci-ktere-musite-prekonat-na-ceste-k-dotacim

MSCASKILL, Steve. Tales In Tech History: Microsoft Windows [online] 29. 7. 2016, [cit. 2016-10-25]. Dostupné z: http://www.techweekeurope.co.uk/workspace/pc/tech-history-microsoft-windows-10-195797

SURÝ, Ondřej. Securityworld [online] 2011, [cit. 2016-10-25]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_DNSSEC_062011.pdf

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

Přílohy

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Pipek Ondřej	Severní 767/56, Hradec Králové - Slezské Předměstí	I1301323

TÉMA ČESKY:

Služby systému Windows Server 2012 a jejich konfigurace ve vybrané firmě

TÉMA ANGLICKY:

Services of Windows Server 2012 and their configuration in a selected company

VEDOUCÍ PRÁCE:

Ing. Andrea Vokálová - KIKM

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je vypracovat podrobnou metodickou příručku pro správu a konfiguraci víceúčelového serveru pro malou až střední firmu. V bakalářské práci je nejprve kladen důraz na teoretickou část, kde jsou vysvětleny použité technologie. Praktická část je věnována popisu nastavení těchto technologií.

Úvod
1. Teoretická východiska
2. Analýza současného prostředí
3. Konfigurace služeb
Závěr
Seznam použitých zkratek
Seznam literatury

SEZNAM DOPORUČENÉ LITERATURY:

STANEK, William R., 2015. Microsoft Windows Server 2012: kapesní rádce administrátora. 1. vydání. Brno: Computer Press, 736 stran. ISBN 978-80-251-3817-5.

PANEK, William. MCSA Windows Server 2012 R2 complete study guide. Indianapolis, Indiana: Sybex, 2015. ISBN 11-188-5991-X.

Podpis studenta: Pipek ..... **Datum:** 3.3.2017

Podpis vedoucího práce: Andrea Vokálová ..... **Datum:** 3.3.2017