

ČZU Praha, PEF, obor Informatika



# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

*PROVOZNĚ EKONOMICKÁ FAKULTA*

## BAKALÁŘSKÁ PRÁCE

*WINDOWS SERVER 2008 R2 - POWER SHELL*

Autor: Aleksandar Idrizović

Vedoucí bakalářské práce: Ing. David Buchtela

Praha 2011



ČZU Praha, PEF, obor Informatika

Poděkování:

Chtěl bych poděkovat Ing. Davidovi Buchtelovi za konzultace, přínosné komentáře k mé práci, a bezvadný pedagogicky přístup i ochotu.

Souhlasím s tím, že s výsledky mé bakalářské práce může být naloženo podle uvážení vedoucího bakalářské práce a vedoucího katedry. V případě publikace budu uveden jako autor.

Prohlašuji, že na celé bakalářské práci jsem pracoval samostatně a použitou literaturu jsem citoval.

V Praze 2011

.....

Aleksandar Idrizović

## WINDOWS 2008 R2 POWER SHELL

Abstrakt: Obsahem práce je problematika optimalizace a utilizace nejrobustnějšího operačního systému od společnosti Microsoft. Popsané technologie patří dnes k těm nejpoužívanějším v enterprise společnosti. V kapitolách jsou popsány užití technologie systémového managementu a síťové služby používané s důrazem na vzdálenou plochu. Na konkrétním příkladu je předvedena instalace a implementace několika systémů na určitém lokálním síťovém segmentu včetně přístupu z nezabezpečené sítě. Výsledky jsou uvedeny formou poznatků získaných při realizaci konceptu autorem.

Klíčová slova:

Microsoft, vzdálená plocha, enterprise

Summary:

The content of this work is the optimization and utilization of the most robust operating system from Microsoft company. The described technologies are those most widely used today in enterprise companies. The chapters describe the technology used for system management and network used, with an emphasis on remote desktop area. The specific example is been shown through installation and implementation of several systems on a local network segment, including access to the unsecured network. Results are given in the form of lessons learned in implementing the concept of the author.

The keywords:

Microsoft, Remote Desktop, enterprise

## Obsah

1	Úvod.....	4
2	Cíl práce a metodika .....	5
3	Teoretický popis užitých technologií a produktů .....	6
3.1	Server 2008 R2 a integrované role .....	7
3.1.1	Vlastnosti a architektura .....	8
3.1.2	Virtualizace .....	11
3.1.3	Active Directory Domain Services .....	12
3.1.4	DNS – Domain Name Services .....	13
3.1.5	RDS - remote desktop services .....	14
3.1.6	Networking .....	17
3.1.7	Souborové služby.....	17
3.1.8	Požadavky na hardware .....	17
3.2	Powershell v2.....	18
3.2.1	Powershell remoting .....	19
3.2.2	Powershell moduly .....	19
3.2.3	Skriptování v Powershellu .....	19
4	Testovací prostředí a cíle .....	20
4.1	Parametry Hardware .....	22
4.2	Konfigurace systému ve virtuálním prostředí.....	22
4.3	Topologie sítě a TCP/IP nastavení.....	24

4.4	Testovací programy .....	24
5	Pozměňovací návrh stávající infrastruktury .....	25
5.1	VmWare ESX 4.1 .....	25
5.2	Windows Server 2008 R2 Standard.....	27
5.3	Master image.....	30
5.4	Instalace doménového Řadiče .....	31
5.5	Windows 7 Professional .....	33
5.6	Utility a měření .....	34
6	Závěr .....	35
6.1	Doporučení.....	36
7	Seznam Literatury .....	38
8	Přílohy.....	40
8.1	CD.....	40
8.2	Seznam tabulek .....	40
8.3	Seznam obrázků.....	40
8.4	Seznam zkratk .....	41

# 1 ÚVOD

Jako téma své bakalářské práce jsem si vybral problematiku, která je mi blízká z mého profesního zaměření. V oboru informačních technologií pracuji již třináct let. Jako partner Microsoftu šestým rokem. Poslední čtyři roky jsem se v České Republice i zahraničí specializoval na nejčastěji zavedené Microsoftové produkty jako jsou Active Directory, Remote Desktop, Exchange server, bezpečnost serverů a stanic, deployment server a VmWare virtualizace. Aktuálně jsem zaměstnán v mezinárodní IT společnosti. Pracovat v takovém prostředí je pro mne velkou výzvou a zároveň příležitostí. Ve svém oboru působím na pracovní pozici konzultanta, kde se pravidelně setkávám s problematikou sítí, bezpečnosti a optimalizace. Konkrétním tématem, které jsem zvolil, jsou produkty společnosti Microsoft s důrazem na VmWare ESX 4.1 hypervisor. Virtualizační technologie považuji za nezbytné v dnešním moderním počítačovém prostředí. Podobný projekt mám na starosti u jednoho z největších zákazníků v České Republice. Za velmi přínosné považuji možnost ověřit si problematiku v praxi - přímo v terénu. Jsem velmi rád, že jsem tyto postřehy mohl vyzkoušet v přímých situacích.

## 2 CÍL PRÁCE A METODIKA

Cílem práce je posoudit přínos užití konkrétních technologií a produktů určených pro optimalizaci serverové infrastruktury Windows. Důraz je kladen na použití praktických nástrojů s cílem co nejlépe využít systémových zdrojů. Vybrané technologie jsou systematicky představeny a popsány v přiměřené míře podrobnosti. Čtenáře seznamují se situací, ve které jsem měl jako autor možnost koncepci testovat na odpovídajícím virtualizačním prostředí.

Nejprve je vysvětlena instalace na testovacím stroji ve virtualizačním prostředí, a potom zavedení a konfigurace služeb. Programové aspekty, které jsou použité v testech jsou popsány a vazba na hardware ve virtualizačním prostředí je zdůrazněna.

Výsledky nasazení technologií jsou prezentovány ve vztahu k nástrojům správy operačního systému. Na závěr jsou uvedena doporučení a zkušenosti získané během práce s popisovanými technologiemi.

Vzhledem k tomu, že se technologie neustále vyvíjejí lze brát tento pohled a řešení jako současné.

### 3 TEORETICKÝ POPIS UŽITÝCH TECHNOLOGIÍ A PRODUKTŮ

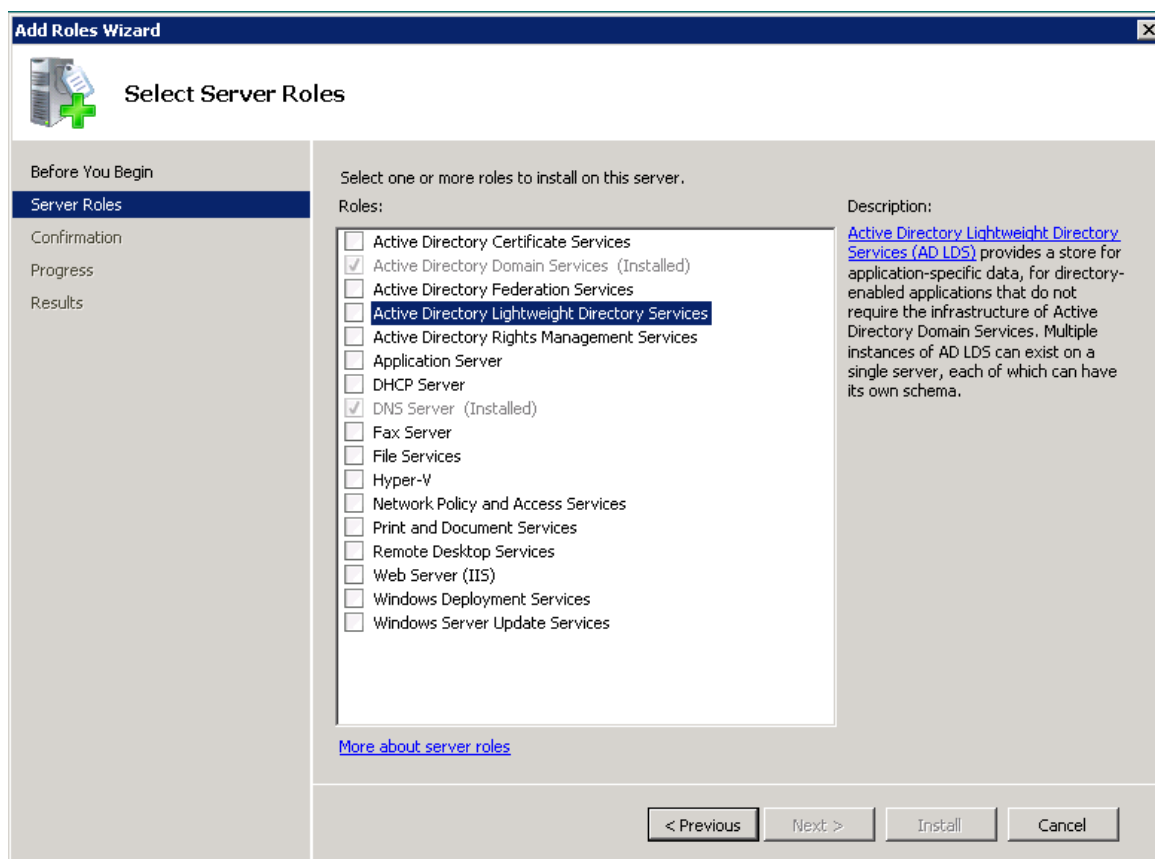
Koncept serverového prostředí, který tato práce představuje, zahrnuje kategorie Microsoft prostředí, a VmWare vSphere 4.1 jako virtuální technologie kterou jsem použil v testovací laboratoři. Popsané jsou dva operační systémy od společností Microsoft. Windows server 2008 R2 Standard a Windows 7 Enterprise jsou prezentovány s hlediska konfigurace a výkonu. Programovací a skriptovací prostředí powershell je vysvětleno a předvedeno v několika ukázkách. Na měření výkonu jsou použité utility CPU hog, IOmeter, vystavena serverová utilita Windows resource Monitor a VmWare monitor. Produkt Openfiler je prezentován jako zajímavé řešení za náhradu nákladného fiber channel diskového pole. Open source komunita nám nabízí opravdu zajímavý a užitečný produkt. Hlavně úplně zadarmo. Openfiler kromě toho, že nahrazuje SAN s blokovým zápisem, funguje také jako NAS, NFS server, a SMB server. Popsána je i základní konfigurace a princip práce s terminálovými službami v prostředí Windows.



### 3.1 SERVER 2008 R2 A INTEGROVANÉ ROLE

Windows Server 2008 R2 je operačním systémem z řady Windows NT od firmy Microsoft, vydaný v roce 2009. Je určen pro serverové sítě. Ačkoliv by se mohlo zdát, že se jedná pouze o update pro Windows Server 2008, R2 je novou verzí operačního systému a na rozdíl od verze 2008, která vychází z verze Vista, používá R2 kód obdobný tomu ve Windows 7. Windows Server 2008 R2 vydal Microsoft 22. července 2009 jako nástupce Windows Server 2008.

Existuje celkem 17 rolí a 42 vlastností v enterprise edici Windows 2008 R2 operačního systému Windows Server 2008 R2, nebo jednoduše R2 v krátkosti, je druhým vydáním Windows Server 2008. Nejde úplně o novou verzi, přidává se však další funkce a vylepšuje stávající verze.



**OBRÁZEK 1: INSTALAČNÍ PRŮVODCE (ROLE)**

### 3.1.1 VLASTNOSTI A ARCHITEKTURA

Windows Server 2008 R2 používá stejný kód jako Windows 7 (Windows NT 6.1). Výrobce proto doporučuje současný běh s klientskými stanicemi, na kterých je nainstalováno Windows 7. Na rozdíl od svého předchůdce Windows Server 2008, tato verze podporuje pouze 64 bitové servery. Z novinek v systému je nutné zmínit .NET Framework 3.5 a IIS 7.5.

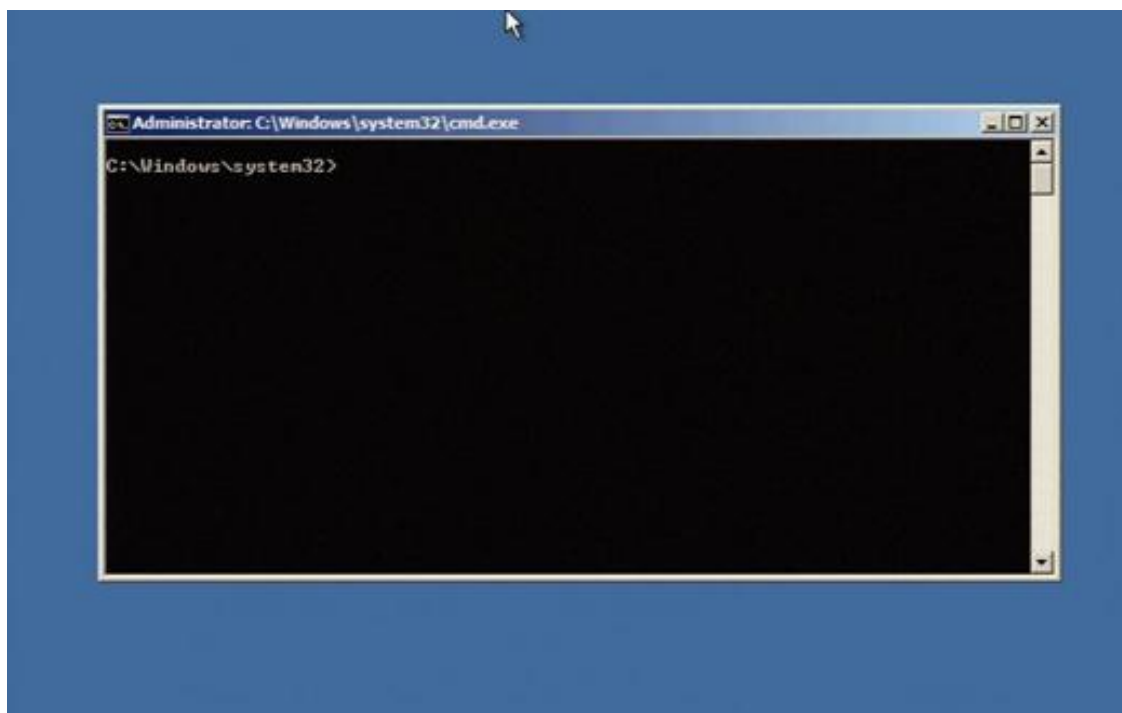
Windows Server 2008 R2 podporuje až 64 procesorů fyzické [15], nebo až 256 logických procesorů v jednom systému. (Poznámka: pouze Datacenter a Itanium vydání mohou využít schopností 64 fyzických procesorů. Enterprise jako příští nejvyšší edice po zmíněných edicích může použít pouze 8 fyzických procesorů).



**OBRÁZEK 2: VÝVOJ MS PRODUKTU OD VERZE 2008 AŽ PO WINDOWS SERVER 2008 R2**

[online: < <http://www.microsoft.com/windowsserver2008/en/us/roadmap.aspx>>]

- Windows 2008 R2 core je speciální verze serveru bez grafického rozhraní. Server Core obsahuje podmnožinu dot NET Framework, takže některé aplikace (včetně ASP.NET webových stránek a Windows PowerShell 2,0) lze používat. Zvýšení výkonnosti bylo hlavní oblastí zaměření pro tuto verzi. Microsoft uvedl, že práce byla provedena ke snížení startu, zvýšení efektivity I / O operaci za použití méně výpočetního výkonu, také obecně se zlepšila rychlost úložných zařízení, zejména iSCSI. Minimální systémové požadavky na paměť jsou jen 384 MB RAM.



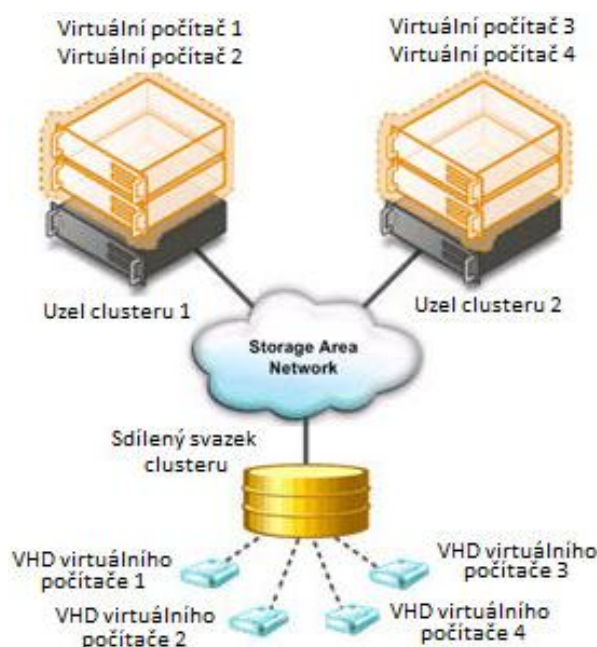
**OBRÁZEK 3: CORE 2008 R2 – OPERAČNÍ SYSTÉM WINDOWS V PŘÍKAZOVÉ ŘADCE**

- Core parkovací systém Windows Server 2008 R2 je schopen využít schopnosti moderních procesorů dynamicky zapnout a vypnout jádra. Pokud Windows Server uznává, že procesory jsou nevyužité, vypne nebo parkuje procesor jádra, kterého není potřeba, což vede k snížení spotřeby energie. V čase kdy procesor poptávky na výkon zvyšuje, tlak na systémové zdroje je oživuje. Windows Server 2008 R2 obnovuje zátěž na jádra jako nezbytné pro zachování systémového výkonu.

- Škálovatelnost - Windows Server 2008 R2 je první verze systému Windows Server pro podporu pouze 64-bitových procesorů. Nyní Windows Server 2008 R2 podporuje až 256 logických procesorových jader pro jedinou instanci operačního systému. Hyper-V - V virtuální stroje jsou schopné adresovat až 64 logických jader v jediném hostiteli. Se zlepšením výkonnosti a efektivity skladování a snížené grafické uživatelské rozhraní (GUI), to dává Windows Serveru 2008 R2 možnost škálovat až na větší zatížení. Navíc, R2 verze Hyper-V taktéž přidává výkonnostní vylepšení, která zvyšují výkon virtuálního stroje a snižují spotřebu. Hyper-V nyní podporuje druhého stupně Address Translation (lamel), který aplikuje nové funkce na dnešní procesory, k zlepšení virtuálního stroje (VM), a výkon při současném snížení provozních nákladů. Hypervisor zpracovává zatížení systému Windows. Tato vylepšení zvyšují schopnost a konsolidaci pracovních úloh, zmenšují počet fyzických serverů, snižují administrativu, spotřebu energie, a rackové náklady.
- SLAT – Second Level Address Translation (Druhá úroveň překladu adres) Windows Server 2008 R2 přidává podporu pro lepší správu paměti nejnovějších procesoru Intel a AMD. AMD pojmenoval svoji novou technologii “RVI“ (Rapid Virtualization Indexing) zatímco u intelu je to EPT ( Extended page Tables). V obou případech umožňuje Hyper-V hypervisor správu paměti, a to zejména z large memory virtuálních strojů (VM), efektivněji a v menší režii rodičovského oddílu. Druhá úroveň Address Translation (lamel) působí tak, že poskytuje dvakrát úroveň překladu adres. Další stránka tabulky slouží k překladu host "fyzické" adresy na fyzické adresy systému.

### 3.1.2 VIRTUALIZACE

Přímá podpora pro virtualizaci serverů, v podobě Hyper-V hypervisoru, byla jedna z nejdůležitějších a velmi očekávaných zlepšení v systému Windows Server 2008. S vydáním Windows Server 2008 R2, Microsoft rozšiřuje Hyper-V virtualizace, kvůli podpoře pro virtualizaci desktopu, a přidává nové schopnosti důležité pro dynamické rozdělení disku, živé migrace a lepší škálovatelnost a redundanci. Virtualizace, však není omezena na virtualizace stroje, ale také na vzdálenou plochu (RDS), virtualizaci aplikací (App-V), a virtualizace desktopu (VDI). Aplikační virtualizace podpory v R2 je lepší, a doplnění ke vzdálené ploše Virtualizace Host (RD Virtualization Host) role služba umožňuje plnou virtualizaci desktopů. Ve verzi R2 je několik oblastí zlepšení z hlediska virtualizace. Jedná se o nové možnosti virtualizace (Live migrace, sdílené svazky clusteru pomocí Failover Clustering a Hyper-V), sníženou spotřebu díky omezení spotřeby energie, novou sadu nástrojů pro správu a nové funkce služby Active Directory, jako jsou "koše" pro smazané objekty anebo Active Directory Recycle Bin. IIS 7.5 rovněž obsahuje aktualizované FTP server služby, powershell snap in for IIS.



OBRÁZEK 4: VIRTUÁLNÍ PROSTŘEDÍ A SAN

[online: < <http://www.microsoft.com/cze/windowsserver2008/R2-virtualization.mspx>>]

### 3.1.3 ACTIVE DIRECTORY DOMAIN SERVICES

R2 verze obsahuje novou sadu nástrojů pro správu Active Directory z Windows PowerShell, nové grafické nástroje pro správu, která je založena na stejných Windows PowerShell rutinách a dlouho-požadovaný mechanismus pro obnovení objektů služby Active Directory které správci nechtěně smazali (Active Directory Recycle Bin). Při zvyšování úrovně funkčnosti doménové struktury služby Active Directory je k dispozici Modul pro Powershell.

The infographic is divided into two main sections: 'Managed Service Accounts' and 'Offline Domain Join'.

**Managed Service Accounts:** This section is titled 'Managed Service Accounts' with a sub-header 'Windows PowerShell Execution Only'. It states that Managed Service Accounts (MSAs) provide automatic password management and simplified SPN management. It notes that Windows PowerShell cmdlets are required to configure and manage accounts for services running on Windows 7/Windows Server 2008 R2, and that MSA passwords are automatically reset to ensure compliance with password policies. A diagram shows a 'Managed Service Account' on a computer connected to an 'Application Server'. A list of requirements includes: 'The same MSAs cannot be used on more than one computer.', 'Services must be individually configured to use a MSA.', and 'To use MSA cmdlets, ensure .NET Framework and the Active Directory module for Windows PowerShell installed.' Below this is the 'Active Directory Administrative Center' section, which is built on Windows PowerShell 2.0 and provides data-driven and task-driven navigation. It supports multiple forests and domains, manages user/computer accounts, organizational unit containers, and groups, filters Active Directory data using query-building search, is installed as part of Windows 7 or Remote Server Administration Tools, and is automatically installed when the AD DS server role is installed on a server.

**Offline Domain Join:** This section is titled 'Offline Domain Join' and explains that it allows computers running Windows 7 and Windows Server 2008 R2 to join a domain without connecting to a domain controller. It lists requirements: 'Djoin.exe must be running on Windows 7/Windows Server 2008 R2.' and 'Appropriate rights are required to join workstations to the domain.' It then details the process in three steps: 1. 'Djoin.exe provisions computer account metadata to AD DS.' which creates computer account metadata (blob in text file) for the destination computer using the 'djoin.exe /provision command'. 2. 'Computer account metadata is inserted into Windows directory of destination computer. Metadata can be saved in unattended operating system installation for destination computer.' using the 'djoin.exe /requestODJ command'. 3. 'When destination computer starts (as a virtual machine or after operating system install), computer is joined to the domain.'

OBRÁZEK 5: WINDOWS 2008 R2 DOMAIN SERVICES

[online:<<http://blogs.technet.com/b/austria/archive/2009/12/05/windows-server-2008-r2-feature-components-poster.aspx>>]

K dispozici je nový nástroj pro vstup pracovní stanice do domény služby AD DS, ve chvíli kdy nemají přístup k řadiči domény, AD Web services Active Directory a provádění Best Practices analyzer (BPA) technologii, která by měla být známa správcům serveru Microsoft Exchange Server. Jako v mnoha jiných oblastech svého operačního systému, Windows Server 2008 R2 využívá Windows PowerShell jako hlavní nový nástroj pro správu Active Directory. Windows Server 2008 R2 obsahuje ne méně než 85 nových rutin pro AD DS a AD LDS, které jsou navrženy tak, aby nahradili stávající (windows cmd příkazovou řádku), jako je Dsget.exe, Dsmode.exe, a Dsadd.exe.

Pro správce u kterých není komfortní práce z příkazové řádky, Windows Server 2008 R2 zahrnuje také služby Active Directory pro správu softwaru (ADAC), nové konzole pro správu, který poskytuje grafické rozhraní pro funkčnost Windows PowerShell rutin.

- Power shell modul - Windows Server 2008 R2 provádí rutiny pro službu Active Directory jako management Windows PowerShell modulu s názvem ActiveDirectory. Windows PowerShell 2.0 je modul soběstačný celek sestávající se z rutin, skriptů, nebo jiného kódu, který je třeba importovat do Windows PowerShell relace, než bude moci přistoupit k jeho funkcím.
- Správa AD Pomoci Powershell Modulu - Windows Server 2008 R2 automaticky nainstaluje Active Directory modul pro Windows PowerShell, když se přidává k AD Domain Services nebo AD Lightweight Directory Services roli. Při povýšení serveru na řadič domény služby AD DS anebo při vytváření instance služby AD LDS, systém nainstaluje a aktivuje Active Directory Web Services, což je vše, co je potřeba pro správu Active Directory systému pomocí Windows PowerShell v daném počítači. Nicméně, správci často chtějí spravovat službu Active Directory z jiného počítače na vzdáleném místě, a můžete tak učinit s Active Directory Modulu a ADAC, pokud používáte systém Windows Server 2008 R2 nebo Windows 7 na vzdáleném počítači. Chcete-li spravovat AD DS nebo AD LDS zdroje z počítače se systémem Windows Server 2008 R2, která není AD DS řadič domény, a že není hostitele instance služby AD LDS, je nutné nainstalovat službu Active Directory modul pro Windows PowerShell a (volitelně) ADAC modul, pomocí Průvodce přidáním funkcí „přístupná“ v Server Manager nebo „počáteční“ konfigurace v úkolech oken.

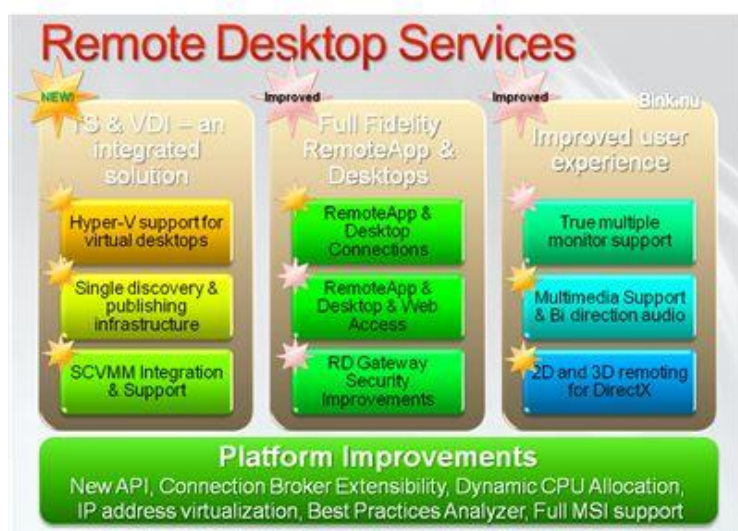
#### 3.1.4 DNS – DOMAIN NAME SERVICES

Podpora rozšíření Domain Name System Security (DNSSEC) je zavedená v systému Windows Server ® 2008 R2 a Windows ® 7. Systémem Windows Server 2008 R2, se lze nyní přihlásit k pomoci DNSSEC podepsaných zón na zajištění bezpečnosti infrastruktury DNS. Nové možnosti v systému DNS:

Možnost podepsat zónu a hostovat podepsané zóny, podpora na změny protokolu DNSSEC, podpora pro DNSKEY, RRSIG, NSEC a DS záznamy. Schopnost uvést znalosti DNSSEC v dotazech, schopnost zpracovat DNSKEY, RRSIG, NSEC a DS záznamy o prostředku a schopnost kontrolovat, zda server DNS, již validoval klienta. Klient DNS (Windows 7) je ve vztahu k DNSSEC řízen prostřednictvím názvů politiky tabulky NRPT, ukládající nastavení, které určuje klient DNS chování. NRPT je typicky řízený prostřednictvím zásad skupiny.

### 3.1.5 RDS - REMOTE DESKTOP SERVICES

Windows Server 2008 R2 zahrnuje významné změny názvu: Místo terminu terminálové služby se nyní používá termin vzdálená plocha a všechny související služby se odpovídajícím způsobem změní. Tabulka 2 ukazuje změny názvu, ale co je opravdu důležité pochopit je mnohem více, než jen změna názvu. Je to změna zaměření a funkčnosti. Správa a řízení RemoteApps a virtuálních desktopů je zlepšena ve Windows Serveru 2008 R2, s přidáním modulu Windows PowerShell (včetně Windows PowerShell poskytovatele) a je zlepšena RD Web Access Konfigurace. Windows Server 2008 R2 přidává vylepšení v RDS, které poskytují více bezproblémovou integraci s Windows 7 klienty, včetně plné podpory pro Windows Aero a více monitorů

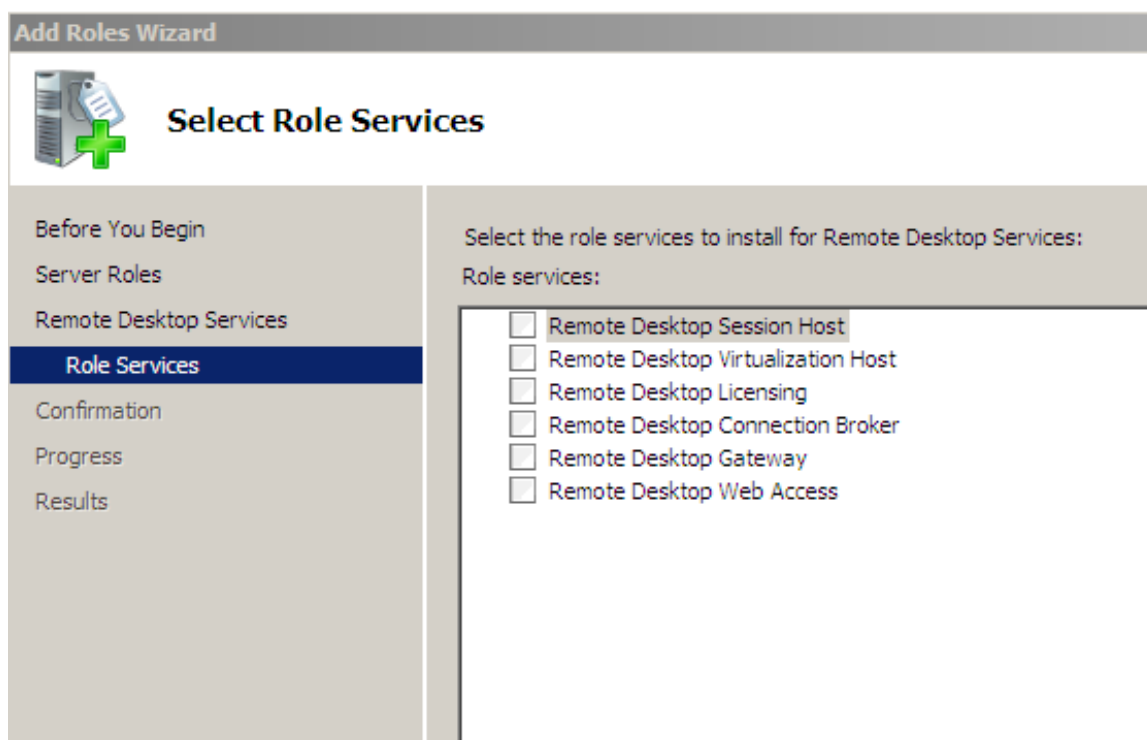


OBRÁZEK 6 PŘEHLED VYLEPŠENÍ V REMOTE DESKTOP SERVICES



## ROZŠÍŘENÉ MOŽNOSTI VZDÁLENÉHO PŘÍSTUPU A VIRTUALIZACE

Společnost Microsoft investovala do dvou klíčových funkcí rozšiřujících možnosti vzdáleného přístupu: VDI a Vzdálená plocha (RDS). VDI je centralizovaná architektura, která umožňuje podnikům soustředit ukládání, spouštění a správu klientských počítačů se systémem Windows do datového centra. Dovoluje spouštět a spravovat systém Windows a další klientská prostředí ve virtuálních počítačích na centralizovaném serveru. Terminálová služba bude nově označována jako Vzdálená plocha (RDS). Vzdálená plocha obsahuje a rozšiřuje všechny funkce, které byly dříve zahrnuty do Terminálové služby. Ve Vzdálené ploše byly zdokonaleny funkce pro správu a výkon, které vylepšují flexibilitu virtualizace prezentace. Díky novým funkcím protokolu RDP (Remote Desktop Protocol) dosáhla společnost Microsoft značného pokroku v rozšíření možností koncových uživatelů. Tyto nové funkce, které Windows Server 2008 R2 umožňuje ve spojení se systémy Windows 7 Enterprise a Ultimate, významně vylepšují možnosti vzdálených uživatelů, kteří mohou pracovat podobně jako uživatelé přistupující k místním výpočetním prostředkům.



**OBRÁZEK 7: VYBĚR ROLI V RDS**

Windows PowerShell provider je způsob, jak zobrazit a procházet informace hierarchickým způsobem, jako kdyby byli disky poskytovatelé v počítači. Ve skutečnosti je souborový systém implementován jako poskytovatel. To znamená, že při zadání `dir c:\` na Windows PowerShell ve skutečnosti poptáváme dětský obsah C svazku přes FileSystem poskytovatele. (dir příkaz alias pro `Get-ChildItem`.) Windows PowerShell provádí v registru systému Windows změny jako poskytovatel, takže si příkazem: `dir HKLM:\System\CurrentControlSet` ověříme co HKey Local Machine registr obsahuje v `System\CurrentControlSet` kontejneru. S powershell poskytovatelem RDS, můžeme na nejvyšší úrovni pracovat s moduly, jako jsou: `RDSConfiguration`, `GatewayServer`, `LicenseServer`, `RDSFarms`, `ConnectionBroker` a `RemoteApp`. S RDS modulem vlastně můžeme nakonfigurovat a spravovat všechny RDS služby a komponenty. Zásady služby Active Directory® integrují virtualizační funkce vzdálené plochy pro aplikace – RAD (Remote Application Deployment) a počítače – VDI (Virtual Desktop Infrastructure), a tím umožňují správcům úsporu času nasazením virtualizovaných aplikací i počítačů na základě zásad. Tyto zásady jsou v systému Windows 7 integrovány natolik, že uživatelé ve většině případů nepoznají rozdíl mezi místně nainstalovanou aplikací a virtualizovanou aplikací.

Dřívější jméno	Změna názvu Windows Server 2008 R2
Terminal Services	Remote Desktop Services
Terminal Server	Remote Desktop Session Host
Terminal Services Licensing	Remote Desktop Licensing
Terminal Services Gateway	Remote Desktop Gateway
Terminal Services Session Broker	Remote Desktop Connection Broker
Terminal Services Web Access	Remote Desktop Web Access
Terminal Services Manager	Remote Desktop Services Manager
Terminal Services Configuration	Remote Desktop Session Host Configuration
Terminal Services Gateway Manager	Remote Desktop Gateway Manager
Terminal Services Licensing Manager	Remote Desktop Licensing Manager
Terminal Services RemoteApp Manager	RemoteApp Manager

TABULKA 1: ZMĚNA NÁZVU TERMINÁLOVÝCH SLUŽEB

### 3.1.6 NETWORKING

Jedním z nejvíce vzrušujících nových funkcí v systému Windows Server 2008 R2 je DirectAccess - nový způsob pro zabezpečené připojení vzdálených klientů k podnikové síti. Nejběžnější metodou připojování vzdálených počítačů na firemní síť je virtuální privátní připojení sítě (VPN), které často vyžaduje třetí klientský software běžící na straně klienta, a může vyžadovat časově náročnou konfiguraci a řešení problémů. Se systémem Windows Server 2008 R2 a DirectAccess, pokud je klient se systémem Windows 7 vzdálený uživatel bez VPN, má vždy přístup k firemním zdrojům, které neohrozí bezpečné aspekty vzdáleného připojení. DirectAccess spolupracuje s Network Access Protection (NAP) ze systému Windows Server 2008 R2. K zajištění všech požadavků na stav systému, je potřeba mít bezpečností aktualizace a antimalware definice nainstalovány. Před povolením DirectAccess připojení se stanice dávají do karantény. Klienty, které jsou připojeny přes DirectAccess mohou interní IT zaměstnanci vzdáleně spravovat. Dále je tímto umožněno, aby byly udržovány na současné úrovni s kritickými aktualizacemi.

### 3.1.7 SOUBOROVÉ SLUŽBY

### 3.1.8 POŽADAVKY NA HARDWARE

Minimální systémové požadavky pro Windows Server 2008 R2

- Procesor Minimálně: 1.4 GHz x64
- Paměť Minimálně: 512 MB RAM (384 MB za Server Core verze)

Maximum: 8 GB (Foundation verze) anebo 32 GB (Standard verze)

anebo 2 TB (Enterprise, Datacenter verze)

- Disk Minimálně: 32 GB anebo více (3.5 GB za Server Core verze)

Foundation: 10 GB anebo více

- Display: Super VGA (800 × 600) anebo monitor s větším rozlišením

Other Keyboard and Microsoft Mouse or compatible pointing device

### 3.2 POWERSHELL V2

Windows PowerShell (dříve známý jako Microsoft Shell, MSH či pod kódovým označením Monad) je rozšiřitelný shell se skriptovacím jazykem od společnosti Microsoft. Produkt je založen na platformě .NET Framework a z toho vyplývá i jeho odlišnost od ostatních shellů, místo textové roury jako je tomu u [UNIX] shellu, obsahuje PowerShell rouru objektovou. Powershell 2.0 je volitelnou součástí systémů Windows XP SP3, Windows Server 2003, Windows Vista SP1 a Windows Server 2008 a integrovanou součástí u systému Windows 7 a Windows Server 2008 R2.

Windows Powershell poskytuje všechny možnosti platformy, na které je postaven, tudíž vše co je obsaženo v Microsoft .NET Frameworku je dostupné i z Powershellu. Díky této provázanosti poskytuje Powershell velké množství funkcí pro správu pomocí tzn. cmdlets (vyslovuje se commandlets), které jsou specializované třídy .NET, implementující určitou operaci. Skripty Powershell (přípona.ps1) jsou kompozicí cmdletů s podporou logických podmínek. Powershell je nástupcem příkazového řádku Windows, tudíž dokáže pracovat s objekty z Visual Basic script, Windows command prompt, Windows API a Windows Management Instrumentation.

Windows PowerShell je jazyk příkazové řádky a skriptovací jazyk, který je určen pro správu systému a automatizace. Postaveno na platformě Microsoft .NET Framework, Windows PowerShell umožňuje IT profesionálům a vývojářům kontrolu a automatizaci správy systému Windows a aplikací.

Windows PowerShell 2.0 přináší více než 100 vestavěných rutin. Verze 2 Powershell je platná od 22. Července 2009

### 3.2.1 *POWERSHELL REMOTING*

Windows PowerShell 2.0 umožňuje spouštět příkazy na jednom nebo více vzdálených počítačích z jednoho počítače se systémem Windows PowerShell. PowerShell vzdálené komunikace umožňuje různé způsoby připojení. Nové funkce, které jsou zavedeny v systému Windows PowerShell 2.0 jsou: Remote Management a graphical management. Pokročilé funkce mají stejné schopnosti a chování jako rutiny. Nicméně, oni jsou psané kompletně v jazyce Windows PowerShell. Windows PowerShell 2.0 umožňuje spuštění příkazu nebo výrazu asynchronně a "v pozadí", a bez interakce s konzolou.

### 3.2.2 *POWERSHELL MODULY*

Moduly umožňují scénář vývojářům a správcům rozdělit a organizovat jejich Windows PowerShell kód soběstačný - opakovaně použitelné jednotky. Kód z modulu spustí ve vlastním soběstačném kontextu a nemá vliv na stav mimo modul.

### 3.2.3 *SKRIPTOVÁNÍ V POWERSHELLU*

PowerShell Integrovaný skriptovací prostředí (ISE) umožňuje spouštět interaktivní příkazy a upravovat a ladit skripty v grafickém prostředí. Mezi hlavní funkce patří barevný-kódovaný syntax, selektivní výkon, grafické ladění textu, podporu Unicode a kontext-pomoc.

## 4 TESTOVACÍ PROSTŘEDÍ A CÍLE

- VmWare Vsphere 4.1

V poslední době se serverová virtualizace začala používat rozsáhle. Málokterá firma dnes neuvažuje přechod na virtualizace. Hlavní důvody jsou úspora elektrické energie, úspory na nákup hardware, rack infrastruktura, škálovatelnost, odolnost vůči poruchám a vysoká dostupnost (HA) a (FT).

Dnes nejznámějším hypervisorem je produkt ESX od společnosti VmWare. ESX 4.1 má podporu pro 256 logických procesoru, 2TB diskového prostoru na jednoho klienta, 10 virtuálních síťových adapteru na klienta, iSCSI virtuální host bus adapter, fibre channel host bust adapter.

Hypervisor se instaluje, přímo na hardware a má relativně nízký footprint. Spolu se servisní konzolou zabírá jen kolem 800 MB RAM.

Servisní konzola používá kolem 800 MB RAM. Zbytek serverových prostředku lze tedy použít na virtuální mašiny. Samotný kernel běží na platformě Linux. ESX jako i Hyper-v podporuje dynamickou manipulaci hardwarevými prostředky, ovšem operační systém také musí mít vlastnosti podporující takové operace. Windows Server 2008 R2 Enterprise edice podporuje upgrade jak paměti, tak procesoru za běhu!

Pokud bych testovací prostředí zprovoznil v rámci hypervisoru na úrovni operačního systému, ani z blízka bych neměl tolik hardwarových prostředků k dispozici. Důvod k tomu je, že sám operační systém by spotřeboval kolem 2GB RAM jen na vlastní provoz. Některé produkty hypervisoru běžících pod operačním systémem jsou Microsoft hyper-v, VmWare server, VmWare Workstation, SUSE Linux enterprise server, Citrix XEN server.

Na testovací prostředí jsem použil VmWare ESX 4.1 hypervisor

ESX 4.1 Na rozdíl od Microsoft Hyper-V nabízí podporu pro více jak 100 operačních systémů. Microsoft hyper-v mimo své produkty pro zatím podporuje jen SUSE linux a RED HAT tedy placené distribuce. VmWare ESX, Microsoft Hyper-v server, Citrix XENserver, SUSE XEN běží přímo na hardware, nabízí více systémových prostředků ale jsou náročnější na správu.

- OpenFiller

Openfiler je operační systém pro správu ukládání dat založený na Linuxu rpath. Je poháněn jádrem Linuxu a OpenSource aplikacemi jako je Apache, Samba, Linux Volume Management, ext3, Linux NFS a iSCSI enterprise target. Openfiler kombinuje tyto všudypřítomné technologie do malého, snadno spravovatelného řešení v čele s výkonným web management rozhraním. Openfiler umožňuje budovat Network Attached Storage (NAS) nebo Storage Area Network (SAN) zařízení, pomocí standardního hardware. Instalace trvá něco kolem 10 minut. Systém je vyvíjen v Anglii a je optimalizován pro platformu i386 a x86\_64 bez grafického prostředí. Již delší dobu používám open filer jako bezplatné SAN řešení. Musím říct, že s produktem jsem výjimečně spokojený. Openfiler vyžaduje poměrně málo systémových prostředků, snadno se spravuje skrz intuitivní webové rozhraní. U jednoho zákazníka máme SAN založený na openfiler v rámci rozsáhlého testovacího prostředí. U dalšího zákazníka provozujeme NAS openfiler jako centrální zálohovací storage.

#### 4.1 PARAMETRY HARDWARE

základní deska: ASUS P5B Premium, chipset: P965

procesor: Intel Pentium Dual-Core E6600 (Wolfdale) 3,06 GHz, cache 2M, 1066 MHz

paměť: Kingston 8GB RAM, 4x2 GB, DDR 2 800 MHz

disk: Western digital Caviar Black 1000 GB, 64MB cache, seriál ATA III

#### 4.2 KONFIGURACE SYSTÉMU VE VIRTUÁLNÍM PROSTŘEDÍ

jméno: **DC-01**

role: doménový řadič

licence: Microsoft serverová licence + CAL pro každého klienta

disk: 20 GB systemovy svazek (virtual)

paměť: 512 MB (virtual)

procesor: 1 jádro (normální priorita)

network: 1GB network adapter (virtual LAN2)

síťová adresa: 192.168.2.1 (LAN2)

maska: 255.255.255.0

výchozí brána: 192.168.2.254

dns server: 127.0.0.1

jméno: **RDS-01**

role: Remote Desktop Server

licence: Microsoft serverová licence + licence na terminál services pro klienta

disk: 20 GB systémový svazek (virtual)

paměť: 768 MB (virtual)

procesor: 1 jádro (normální priorita)

network: 1GB network adapter (virtual LAN2)

síťová adresa: 192.168.2.50 (LAN2)

maska: 255.255.255.0

výchozí brána: 192.168.2.254

dns server: 192.168.2.1



ČZU Praha, PEF, obor Informatika

jméno: **Win7-01**

role: desktop (klient)

licence: Microsoft klientská licence

disk: disk: 30 GB systémový svazek (virtual)

paměť: 1GB MB (virtual)

procesor: 1 jádro (normální priorita)

network: 1GB network adapter (virtual LAN2)

síťová adresa: 192.168.1.100 (LAN1)

maska: 255.255.255.0

výchozí brána: 192.168.1.254

dns server: 192.168.2.1

jméno: **OpenFiler**

role: iSCSI Storage Area Network server

licence: Open source

disk: 300 GB (fyzický)

paměť: 1GB

procesor: 1 jádro (AMD 3200+)

network: 2 x 1Gb network adapter – subnet 192.168.2.0

síťová adresa: 192.168.2.205 (LAN2)

maska: 255.255.255.0

výchozí brána: 192.168.2.254

dns server: 192.168.2.1

jméno: **Router**

role: router mezi vnitřní (LAN2) a venkovní sítí (LAN1)

disk: 20 GB (virtual)

paměť: 512 MB (virtual)

procesor: 1 jádro (normální priorita)

network: 2 x 1Gb network adapter – subnet 192.168.1.0 a 192.168.2.0

síťová adresa 1: 192.168.1.254 (LAN1) síťová adresa 2: 192.168.2.254 (LAN2)

maska: 255.255.255.0, dns server: 192.168.2.1

### 4.3 TOPOLOGIE SÍTĚ A TCP/IP NASTAVENÍ

LAN1 – subnet 192.168.1.0 maska 255.255.255.0 výchozí brána 192.168.1.254

Tato síť zároveň simuluje venkovní síť (nezabezpečenou síť) anebo Internet.

Všechny počítače na tyto sítě komunikují s ostatními počítači skrz výchozí bránu 192.168.1.254

případně skrz LAN1 síťový adapter na virtuálním stroji Router.

LAN2 – subnet 192.168.2.0 maska 255.255.255.0 výchozí brána 192.168.2.254 Tato síť je firemní anebo vnitřní síť (zabezpečená) a nachází se za improvizovanou firewall.

Všechny počítače na této síti komunikují s ostatními počítači skrz výchozí bránu 192.168.2.254 anebo skrz LAN2 síťový adapter na virtuálním stroji Router.

### 4.4 TESTOVACÍ PROGRAMY

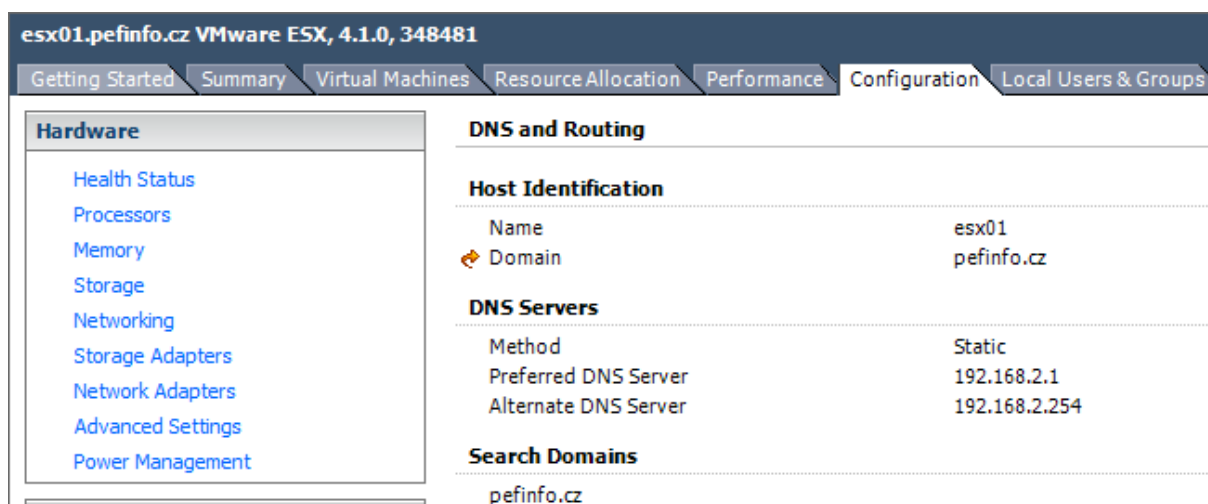
- Remote Desktop LoadSimulation Tools  
Používá se na plánování serverové kapacity a analýzu škálovatelností a výkonu. V různých scénářích měří, kolik klientských připojení zvládne server. Definiuje zátěž jednotlivých anebo hromadných procesů na serveru.
- Windows resource manager
- CPU hog  
Utilita na zátěžový test procesoru. Lze zvolit pomocí parametrů do jaké míry chceme zatěžovat procesor a na jak dlouho.
- IOMeter for iSCSI performance  
Utilita která měří zátěž na SAN a iSCSI systémech. Jedná se o open source utilitu originálně pocházející od Intelu. V testovacím prostředí jsem použil právě IoMeter, abych zjistil, zda optimalizace iSCSI storage pomocí 9000 MTU Jumbo Frames dává smysl a za jakých podmínek.

## 5 POZMĚŇOVACÍ NÁVRH STÁVAJÍCÍ INFRASTRUKTURY

### 5.1 VMWARE ESX 4.1

Instaloval jsem klasickou cestou s DVD média. ESX server ještě lze instalovat vzdáleně s NFS serveru, z USB paměťového média, nebo skrz síť pomocí PXE boot. Velikost root, swap, var, log svazku jsem zvolil dle výchozích voleb. Vybral jsem IP adresu 192.168.2.201, správně vyplnil DNS záznamy, výchozí bránu a jméno windows domény Pefinfo.cz. Nastavil jsem NTP hodnoty na internetový klaster *pool.ntp.org*. Poté co jsem nainstaloval ESX, povolil jsem root účtu přístup na SSH. Dle výchozího nastavení kvůli bezpečnosti, na ESX serveru nemá root nárok připojovat se pomocí SSH.

Postup: `nano /etc/ssh/sshd_config`, v řádku který obsahuje *PermitRootLogin* jsem změnil hodnotu NO na YES, zastavil a znovu nainstaloval službu ssh `service sshd restart`.



**OBRÁZEK 8: NETWORK KONFIGURACE NA ESX SERVERU**

Vytvořil jsem 2 virtuální stroje, Windows server a Windows 7. U každého stroje jsem použil podobné parametry, co se týče velikosti disku, síťového adapteru a paměti.

Rezervace resursu jsem nepoužíval, takže jsem nechal virtuální stroje, aby se stejnou prioritou bojovaly o systémové zdroje.

Name	State	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
DC01	Powered On	31.02 GB	31.02 GB	28	526	19
DC02	Powered On	22.37 GB	22.37 GB	22	753	19
VCENTER	Powered On	23.01 GB	23.01 GB	97	1481	38
RDS01	Powered On	33.03 GB	12.43 GB	18	836	9
ROUTER01	Powered On	16.02 GB	16.02 GB	23	335	9

**OBRÁZEK 9: VIRTUALNI STROJE V TESTOVACIM PROSTŘEDÍ A SYSTEMOVE ZDROJE**

## 5.2 WINDOWS SERVER 2008 R2 STANDARD

První Windows operační systém, který jsem instaloval, byl server DC-01, jenž jsem implementoval z instalačního média, nastavil jsem TCP-IP a instaloval nejnovější update. Zápłaty vždy aplikuji, protože obsahují nejen bezpečnostní nastavení ale i opravené chyby u jednotlivého balíku. Některé zápłaty také zlepšují výkon systému. Poté co jsem stáhnul a nainstaloval zápłaty (systém několikrát znovu nastartoval) nakonfiguroval jsem uživatelské rozhraní Windows server 2008 R2.

Pomocí utility FSUTIL jsem zakázal souborovém systému NTFS použití krátkých 8.3 jmen a také Last Access time stamp nad každou složkou. Obě nastavení zlepšují výkon, ale u některých starších aplikací není vždy doporučeno vypínat 8dot3name! Tato DOS konvence je v operačním systému stále platná z historických důvodů.

```
fsutil 8dot3name set 1
```

```
fsutil behavior set DisableLastAccess 1
```

Powershell

Připravil jsem PS na systému, aby se mohli používat pokročilé funkce. Z bezpečnostních důvodů je zakázáno použití remotesigned hned po instalaci systému, proto je vždy potřeba tuto vlastnost povolit.

```
Get-Executionpolicy (příkaz ověří, zda systém povoluje pokročile funkce PS)
```

```
Get-Help about-signing (návod jak změnit PS signing politiku)
```

```
Set-ExecutionPolicy remotesigned (nastavuje politiku, nyní je možné naimportovat různé moduly powershell)
```

*Správa účtů:* Výchozí účet administrátor jsem přejmenoval na root. Použil jsem Local Security policy.

Postup: *Start – Administrative Tools – Local Security Policy – Local Policy - Security Options – Accounts:Rename administrator account*

## Systémové služby

Posléze bylo potřeba celou řadu služeb zakázat, nebo nastavit na ruční start.

Důvod: takový systém je bezpečnější a má lepší výkon. Připomínám, že v tabulce jsou uvedené služby, které jak ve virtuálním prostředí, tak v produkci lze bezpečně zastavit a zakázat. Pokud by nějaká komponenta vyžadovala běh určité služby, je potřeba změnit stav na „manual“ anebo „automatic“ a službu případně nastartovat. Považuji za zbytečné, aby v testovacím prostředí běžela služba Windows sound a další. Také doporučuji vždy zakázat služby, které nepoužíváme, či je nemůžeme použít, jako například službu „Smart Card“ která má na starosti čipové karty.

<b>Služba</b>	<b>Stav po úpravě</b>
Diagnostic Policy Service	Disabled
Diagnostic Service Host	disabled
Diagnostic Systém host	disabled
Internet Connection Sharing (ICS)	disabled
IP Helper	disabled
Multimedia Clas Scheduler	disabled
Print Spooler	disabled
RPC Locator	disabled
Remote Registry	disabled
Routing and Remote Access	disabled
Secondary Logon	disabled
Smart Card	disabled
Smart Card Removal Policy	disabled
SSDP Discovery	disabled
TPM Base Services	disabled
UPnP Device Host	disabled
Windows Audio	disabled
Windows Audio Endpoint Builder	disabled
Windows Card Space	disabled
Windows Color Systém	disabled
Windows Error Reporting Service	disabled
Windows Font Cache Service	disabled
Windows Remote Management	disabled

TABULKA 2: OPTIMALIZACE SLUŽEB

## Souborové služby

Nad systémovým svazkem jsem odškrtnul volbu: *Allow files on this drive to have contents indexed in addition to file properties*. Jelikož 2008 R2 po instalaci obsahuje kolem 65000 souborů, které jsou uloženy v 15000 složkách, tato operace trvala určitou dobu a bylo potřeba potvrdit změnu vlastnosti. Navíc některé soubory jsou uzamčeny systémem. Tudíž jsem musel navíc zmáčknout také „Ignore“.

Powershell – povolil jsem pokročilou vlastnost Active Directory recycle bin

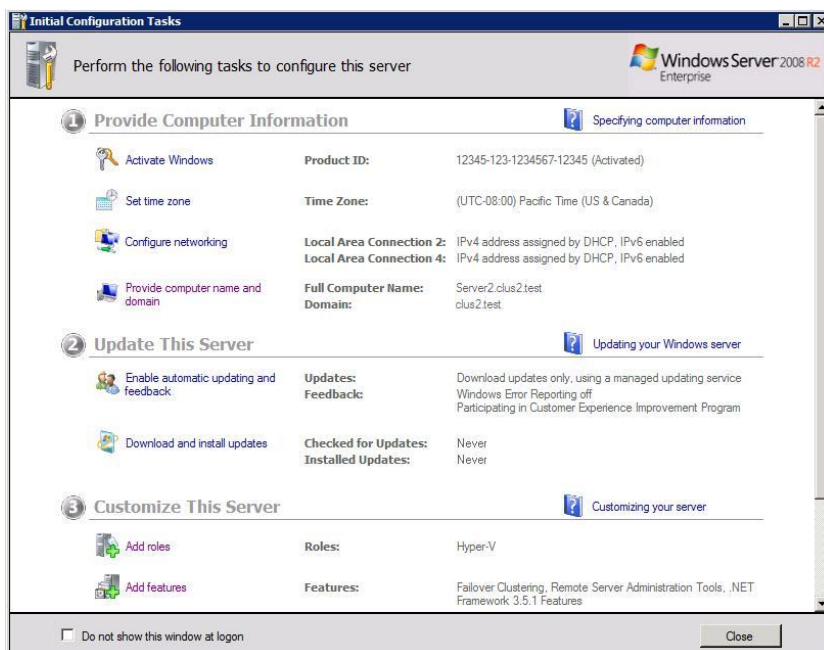
*Set-ADForestMode Active Directory module cmdlet* (syntaxe obecně)

*Set-ADForestMode –Identity pefinfo.cz -ForestMode Windows2008R2Forest*

(nejdříve povolí úroveň forestu Windows Server 2008 R2, operace je nenávratná, poté do domény již nelze přidat DC starší jak 2008 R2!)

*Enable-ADOptionalFeature Active Directory module cmdlet* (syntaxe obecně)

*Enable-ADOptionalfeature 'Recycle Bin Feature' –score forest –target 'pefinfo.cz'*

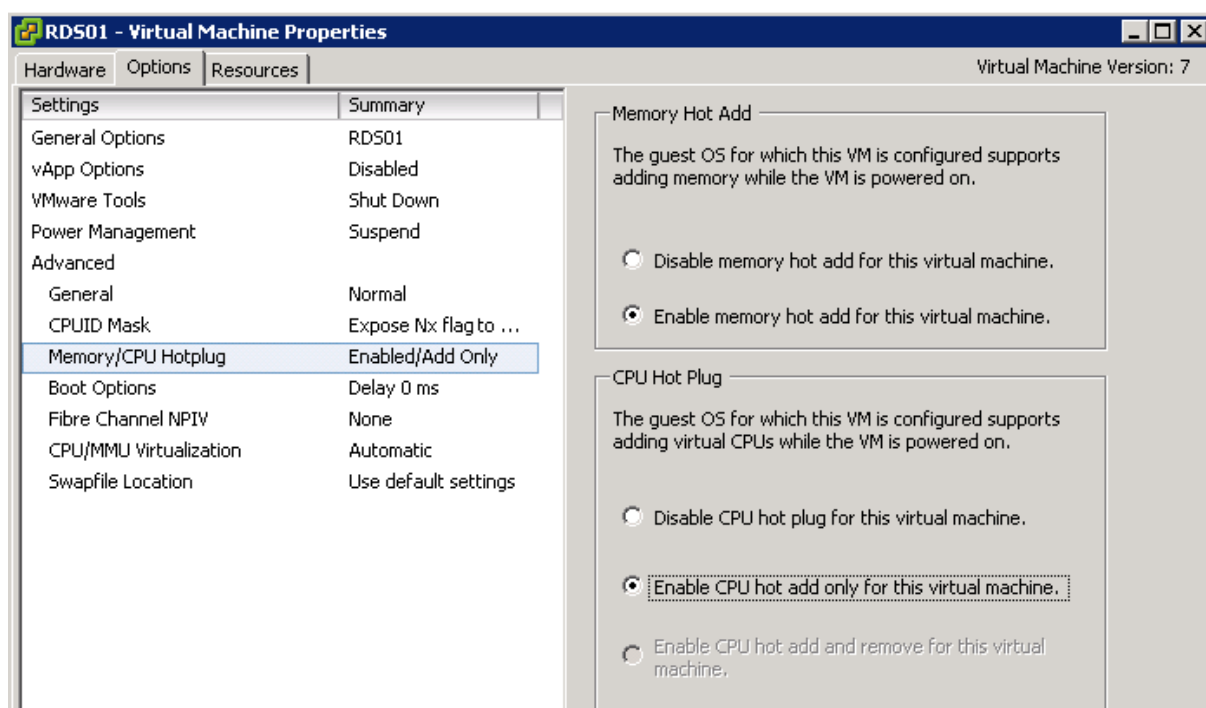


**OBRÁZEK 10: INICIÁLNÍ KONFIGURAČNÍ ÚLOHY OOB**

## Master image

Takto nakonfigurovaný systém jsem klonoval jako VmWare obraz. V pozdější instalaci mi tento postup ušetřil více jak 10 hodin práce. K nainstalování dalšího operačního systému Windows 2008 R2 včetně veškerého nastavení stačí jen vybrat volbu „Deploy from template“ v konzole VmWare vcenter. Následující systém, který jsem instaloval, byl terminálový server RDS-01. Instalace trvala přibližně 10 minut. Oproti několikahodinového nastavování z předchozí instalace je vidět, že úspora času je značná.

Samozřejmě byla potřeba ještě nainstalovat RDS a nakonfigurovat vlastnosti služby. Tentokrát jsem použil powershell příkazy. Nejdříve jsem naimportoval Server Manager modul *Import-Module Servermanager*, potom *Add-WindowsFeature RSAT-RDS –restart*. Pokud si nejsme jisty, jak správně použít jméno role doporučuji spustit příkaz: *Get-WindowsFeature*



**OBRÁZEK 11: MOZNOST ZVÝŠENÍ PAMĚTI A PROCESORU VIRTUÁLNÍHO STROJE ZA BĚHU**



### 5.3 INSTALACE DOMÉNOVÉHO ŘADIČE

Na správu účtu a bezpečnost, jsem zvolil integrovanou roli Active Directory Domain Services. Spustil jsem průvodce, zaškrtnul odpovídající roli a potvrdil nainstalování komponentu .NET Framework verze 3.5

Jelikož systém nevyžadoval restart, bylo možné ihned pokračovat s instalací. Aby Active Directory mohla fungovat a být vůbec nainstalována je potřeba funkční DNS síťové služby. Microsoft Active Directory funguje i s Linux Bind verzi DNS, samozřejmě jsou určité nároky na verze Bind. Například BIND verze 9.5.0-P2-W2 lze použít na Windows 2008 Active Directory. Jsou tři typy zón, které podporuje Windows 2008 DNS server. Jsou jimi: primary, secondary a stub zone. Navíc zóny mohou být integrovány do Active Directory či nemusí. Výhoda integrovaných zón, je v tom, že DNS záznamy a konfigurace jsou uloženy v Active Directory databázi. To znamená zvýšenou bezpečnost a replikace DNS skrz Active Directory.

DNS server se může nainstalovat zvlášť jako role i bez použití Active Directory.

Po spuštění příkazu *dcpromo* jsem zadal parametry nové domény a informace které byly vyžadovány průvodcem. Vždy když se instaluje první doménový kontroler. To znamená založení nového forestu - tedy nového lesu. Typické pro každou organizaci je, že se většinou skládá z „jednoho lesa“. Tomu se říká logická struktura Active Directory. Pod každým lesem může být více stromů a každý strom může obsahovat více domén. Domény jsou organizovány hierarchicky dle Internetové DNS konvence. Čím více se pohybujeme v DNS záznamu vpravo, tím více se přibližujeme kořenové root doméně.

V praxi často jedna doména obsahuje i přes sto tisíc různých objektů. Pracoval jsem 2 roky v organizaci, která měla kolem jednoho milionů záznamů v LDAP-u. Z toho bylo přes půl milionu uživatelů. Objekty mohou být uživatelé, počítače, tiskárny a podobně.

Na ukázkou stacilo vybrat jeden forest a jednu doménu, což je i jediná volba pokud máme jen jeden doménový kontroler. Za jméno domény jsem vybral DNS název pefinfo.cz. Z historických důvodu a díky podpoře Microsoft Windows NT serveru v průvodci *dcpromo* je také nutné vybrat netbios jméno nové domény. Tedy pefinfo bude netbios označení.

Dále jsem vybral uložisko Active Directory databáze dle výchozího nastavení tak, jak to nabídl instalační průvodce (c:\windows\system32\NTDS), jak pro databáze a logy tak pro sysvol složku. Sysvol složka je uložisko, kam se ukládají nastavení group policy, tedy zásady správy.

Zadal jsem heslo na recovery v případě, kdy by byla potřeba udělat obnovu dat. Průvodce začal instalaci a ihned nabídl instalaci DNS služby. Jelikož jsem neinstaloval DNS jako roli a nemám žádnou verzi BIND, potvrdil jsem tudíž instalaci DNS serveru. Před spuštěním dcprom je velmi důležité správně nastavit TCP/IP v síťovém adapteru. Každý DNS server musí nějakým způsobem vědět na který server se má dotazovat. Server DC01 je sám pro sebe primárním DNS serverem.

Instalace skončila, a server se automaticky restartoval, jelikož jsem tu možnost vybral při instalaci. Po úspěšné instalaci Active Directory jsem ručně přidal nový host **A** záznam do DNS. (jméno DC-01.pefinfo.cz, adresa 192.168.2.1). Dále pak další záznamy do DNS serveru: esx01.pefinfo.cz, rds-01.pefinfo.cz, win7-01.pefinfo.cz a jejich odpovídající IP adresy.

Správnost DNS serveru jsem ověřil utilitou nslookup (name server lookup).

1. Test

Příkaz: *nslookup*

Hodnota: Default server: localhost, address: 127.0.0.1

2. Test

Příkaz: *nslookup, set type=ns, pefinfo.cz*

Hodnota: Server: localhost, address:127.0.0.1, pefinfo.cz nameserver=DC-01.pefinfo.cz, dc-01.pefinfo.cz internet address: 192.168.2.1

3. Test

Příkaz: *ping pefinfo.cz*

Hodnota: pinging pefinfo.cz [192.168.2.1] with 32 bytes of data, reply from...

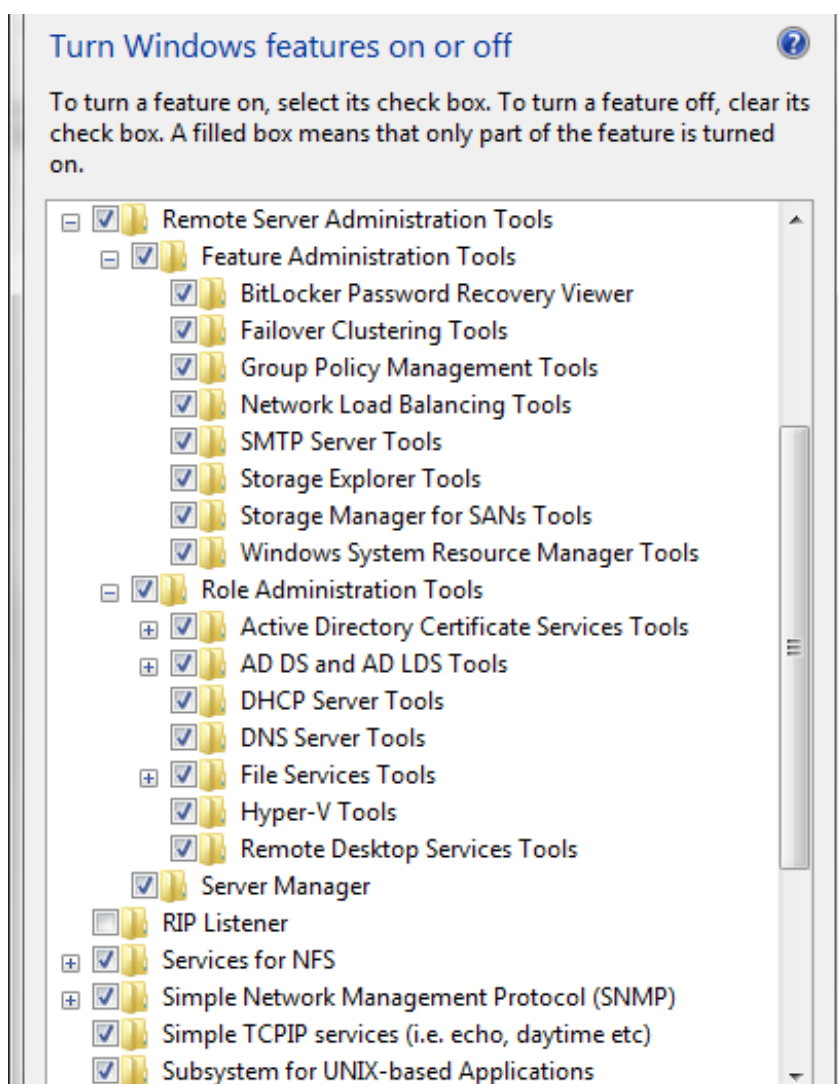
4. Test

Příkaz: *dcdiag /test:DNS*

Hodnota: různé DNS testy vraceli správné hodnoty

## 5.4 WINDOWS 7 PROFESSIONAL

Windows 7 se instaluje stejně jako server 2008 R2 s DVD média a instalační postup je totožný. V grafickém rozhraní lze vybrat disk, na který chceme instalovat operační systém, potom jde upravovat svazky a vybrat tu správnou volbu, kde naistalovat systém. Jelikož na ESX serveru jsem měl k dispozici jen jeden virtuální disk, zvolil jsem výchozí volbu (jen nainstalovat), instalace trvala kolem 20 minut, poté systém nastavil, zabezpečil a optimalizoval. Nakonfigurovaný systém Windows 7 Professional jsem naklonoval a vytvořil další šablonu s názvem Win7PRO.



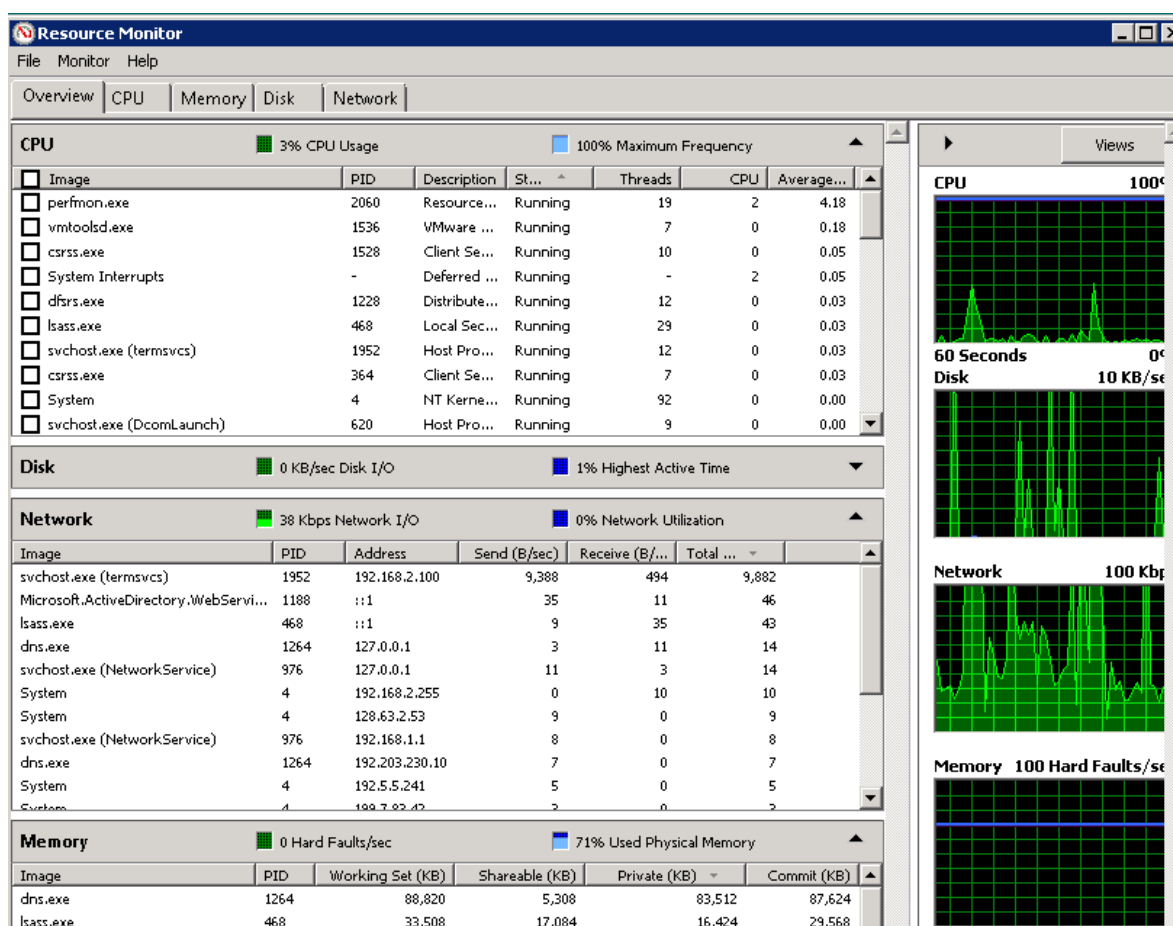
**OBRÁZEK 12: INSTALACE RSAT V GRAFICKÉM ROZHRANÍ WINDOWS 7**

## 5.5 UTILITY A MĚŘENÍ

Nslookup

Resource monitor

- optimalizace sítí – propustnost dat na iSCSI SAN  
(MTU 9000 jumbo frame na OpenFiller SAN serveru)
- optimalizace služeb na serveru 2008 R2



## 6 ZÁVĚR

Na základě zkušeností získaných při důkladném ověřování koncepce, doporučuji v případě implementace technologii společnosti Microsoft zvolit serverový operační systém Windows server 2008 R2. Je to robustní systém, jenž nabízí hodně, je spolehlivý a bezpečný. Co se týče požadavku na hardware, v prezentaci jak lze, takto velký systém snadno provozovat i na skromnějších systémových zdrojích.

Bez virtualizace se již asi neobejdeme. Možná ne každý se mnou bude souhlasit, je však spousta argumentů k zamyšlení na toto téma - promyšlení. Minimálně pasuje do testovacího prostředí, pokud potřebujeme odzkoušet některý jev, nemáme adekvátní „železo“ a nechceme negativně ovlivnit produkční prostředí s eventuálním nevydařeným pokusem.

Co se týče testů na iSCSI, RDS, nebo všeobecně jen více opakovaných pokusů s různými hodnotami velikosti bloku, dává optimální výsledky. Z toho vyplývá potřeba experimentovat, a teprve potom moci vybírat optimální nastavení.

## 6.1 DOPORUČENÍ

Na základě zkušeností získaných při důkladném ověřování koncepce, doporučuji v případě implementace operačního systému Windows Server 2008 R2 v rámci virtualizační a fyzické infrastruktury tyto zásady:

Zakázat služby, které se nepoužívají na každém serveru a na každé stanici.

Vždy optimalizovat systémové služby. Každou službu, která se nepoužívá, doporučuji zakázat. Používat pravidelně vystaveny Windows resource monitor a sledovat výkon systému. Mít dohled a plnou kontrolu nad službou, znamená rozumět systémovým požadavkům.

Intenzivně používat prostředky automatizace a rychlého nasazení systému. Konfigurace auto deploymentu operačního systému často bývá velice náročná, navíc hodně času musíme investovat na učení, dokud se nestaneme odborníkem na auto deployment. Každopádně, pokud ve společnosti spravujeme desítky či stovky počítačů, veškerý investovaný čas se nám musí vrátit.

Pravidelně se informovat v komunitě o nových utilitách a pomůckách. Ze zkušenosti vím, že drtivá většina Microsoft „zlepšováků“ je k dispozici zcela bezplatně..

V případě kdy se na projektu potkám s technickým problémem, který neumím ihned řešit, nejdříve se porozhlédnu na web-u v různých komunitách. Je to často rychlejší než prohledávat-pročítat tištěnou literaturu. Zejména počítačová odborníci v praxi řeší situace, které v knížkách často nejsou k dohledání.

Openfiler lze použít zcela zdarma a můžeme mít hotové SAN / NAS / SMB / NFS řešení s vysokou odolností a uspokojujícím výkonem. Doporučuji produkt několikrát nainstalovat a otestovat různé konfigurace a scénáře před produkcí.

Aplikovat výhody virtualizace tam, kde je to možné.

Využívat Power Shell jako monitorovací nástroj ve Windows a jako prostředí na skriptování.

Doporučuji při stavbě serveru pro virtualizaci podrobně celkovou infrastrukturu.

ČZU Praha, PEF, obor Informatika

Také naplánovat čas, výkony stavět a dimenzovat dle skutečných požadavků služeb a potřeb.

Pokud se systémové prostředky hypervisoru nepřidělují racionálně, může se stát, že některý ze systému nenaběhne, protože nezbytné zdroje již obsadil jiný virtuální stroj.

Používat Open Source produkty na projektech? Jsem názoru, pokud je cokoliv bezplatné, neznamená to ihned, že je to špatné.

Samozřejmě doporučuji při zavádění nových technologií a produktů co nejdříve důkladně naplánovat a potom otestovat, nejlépe v simulačním prostředí.

## 7 SEZNAM LITERATURY

1. Ed Wilson. Windows PowerShell Scripting Guide. Redmond, Washington: Microsoft Press, 2008. 665 s. ISBN 0-7356-2279-5.
2. John Savill. The Complete Guide To Windows Server 2008. Boston, Michigan: Pearson Education, 2009. 1749 s. ISBN 0-321-50272-8.
3. Christa Anderson, Kristin Griffin. Windows Server 2008 R2 Remote Desktop Services resource Kit. Redmond, Washington: Microsoft Press, 2010. 720 s. ISBN 978-0-7356-2737-6.
4. Jeffrey R. Shapiro. Windows Server 2008 Bible. Indianapolis, Indiana: Wiley Publishing, 2008. 1008 s. ISBN 978-0-470-17069-4.
5. William Stanek. Windows Power Shell 2.0 Administrator's Pocket Consultant. Redmond, Washington: Microsoft Press, 2009. 480 s. ISBN 978-0-7356-2595-2.
6. Microsoft. Hlavní důvody pro nasazení systému Windows Server 2008 R2 [Online].[cit.2010-11-15].

URL: <<http://www.microsoft.com/cze/windowsserver2008/why-upgrade.msp>>.

7. Wikipedie. Windows Server 2008 R2 - Wikipedie, otevřená encyklopedie. [Online]. [cit. 2010-12-07].

URL: <[http://cs.wikipedia.org/wiki/Windows\\_Server\\_2008\\_R2](http://cs.wikipedia.org/wiki/Windows_Server_2008_R2)>.

8. Wikipedie. Windows PowerShell [Online]. [cit. 2011-01-12].

URL: <[http://en.wikipedia.org/wiki/Windows\\_PowerShell](http://en.wikipedia.org/wiki/Windows_PowerShell)>.

9. InformationWeek. 9 Reasons Enterprises Shouldn't Switch To Hyper-V. [Online].[cit. 2011-01-06].

URL:<[http://www.informationweek.com/blog/main/archives/2009/12/9\\_reasons\\_enter.html;jsessionid=35COG3341MKZRQE1GHRSKH4ATMY32JVN](http://www.informationweek.com/blog/main/archives/2009/12/9_reasons_enter.html;jsessionid=35COG3341MKZRQE1GHRSKH4ATMY32JVN)>



10. Microsoft. Windows Management Framework (Windows Powershell 2.0, WinRm 2.0, and BITS 4.0) [Online].[cit. 2010-11-17]

URL: <<http://support.microsoft.com/kb/968929>>.

11. Linux website21. Openfiler [Online].[cit. 2010-12-28].

URL: <<http://www.linux.website21.cz/linux/openfiler.html>>

12. Výkonná virtualizace na domácím počítači [Online].[cit. 2010-12-17]

URL:<<http://extrahardware.cnews.cz/vykonna-virtualizace-na-domacim-pocitaci?page=0,1>>

## 8 PŘÍLOHY

Tato kapitola obsahuje seznamy tabulek a obrázků. Uvedené jsou i všechny zkratky.

### 8.1 CD

Bakalářská práce nahrána na CD medium, odevzdaná na katedře Informačního Inženýrství – dokument – XIDRA100\_BP.docx

### 8.2 SEZNAM TABULEK

Tabulka 1: Změna názvu terminálových služeb..... 16

Tabulka 2: Optimalizace služeb: .....28

### 8.3 SEZNAM OBRÁZKŮ

Obrázek 1: instalační průvodce (role)..... 7

Obrázek 2: vývoj MS produktu od verze 2008 až po Windows Server 2008 R2.....8

Obrázek 3: core 2008 R2 – operační systém Windows v příkazové řádce.....9

Obrázek 4: virtuální prostředí a SAN ..... 11

Obrázek 5: Windows 2008 R2 domain services ..... 12

Obrázek 6 Přehled vylepšení v Remote Desktop Services ..... 14

Obrázek 7: Výběr rolí v RDS ..... 15

Obrázek 8: network konfigurace na ESX serveru .....25

Obrázek 9: virtuální stroje v testovacím prostředí a systémové zdroje .....26

Obrázek 10: iniciační konfigurační úlohy OOBE .....29

Obrázek 11: možnost zvýšení paměti a procesoru virtuálního stroje za běhu.....30

Obrázek 12: instalace RSAT v grafickém rozhraní Windows 7.....33

## 8.4 SEZNAM ZKRATEK

AD.....	Active Directory
APP-V.....	Application Virtualization
BIOS.....	Basic Input Output System
BIND.....	Berkeley Internet Domain System (Open source DNS)
CAL.....	Client Access Licence (Microsoft politika na licencování klientů)
CPU.....	Central Processing Unit(Procesor)
DC.....	Domain Controller (Doménový řadič)
DHCP.....	Dynamic Host Configuration Protocol (automatizace síťových nastavení)
DNS.....	Domain Name System (systém přidělování hierarchických jmen v síti)
DOS.....	Disk Operating System (historicky operační systém od Microsoft a IBM)
DS.....	Directory Services (adresářová služba)
ESX.....	Elastic Sky X (VmWare hypervisor)
FT.....	Fault Tolerance (Odolnost vůči poruchám)
HA.....	High Availability (Vysoká dostupnost)
HTTP.....	Hypertext Transfer Protocol (Internetový značkový jazyk)
IIS.....	Internet Information Server (Microsoft WEB server)
IP.....	Internet Protocol
ISCSI.....	Internet Small Computer System Interface (SAN blokový zápis)
ISE.....	Integrated Script Engine

LDAP.....	Lightweight Directory Access Protocol (otevřený protokol přístupu k datům)
LDS.....	LightWeight Directory Services(základní služby Active Directory)
MAC.....	Medium Access Control (fyzická adresa hostu na síti)
MTU.....	Maximum Transmission Unit (nejvyšší možná velikost rámce přenášeného síti)
NAP.....	Network Access Protection
NAS.....	Network Attached Storage (síťové uložště se souborovým zapísem)
NRPT.....	Name Resolution Policy Table (zásady skupin DNS)
NTFS.....	NT File systém (Windows bezpečný souborový systém)
NTP.....	Network Time Protocol (časový server)
OOBE.....	Out-of-Box experience (iniciální konfigurace)
PS.....	Power Shell
PS1.....	Přípona Power Shell
R2.....	Release two(druha produkční verze)
RADIUS.....	Bezpečnostní standard (protokol) ověření komunikace
RAM.....	Random Access Memory (Paměť jen na čtení)
RDS.....	Remote Desktop Services (vzdálená plocha)
RPATH.....	(Linuxová stabilní a vysoce kvalitní distribuce)
RSAT.....	Remote Server Administration Tool
QoS.....	Quality of Service (technologie užívaná na spojích WAN garantující pásmo)
SAN.....	Storage Area Network (síťové uložště s blokovým zápisem)

SSH.....	Secure Shell (zabezpečený síťový protokol pro výměnu dat)
TCP.....	Transmission Control Protocol (protokol pro přenos dat v síti)
URL.....	Uniform Resource Locator (způsob adresování zdrojů v síti Internet)
VDI.....	Virtual Desktop Infrastructure
VPN... ..	Virtual Private Network (komunikační kanál spojující dvě sítě)
VM.....	Virtual Machine (Virtuální stroj)
WAN.....	Wide Area Network (rozsáhlá počítačová síť)