Konfigurace MS Windows 2003 serveru

System configuration of MS Windows 2003 server

Vlastimil Palouš

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vlastimil PALOUŠ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Konfigurace MS Windows 2003 serveru**

Zásady pro vypracování:

Proveďte instalaci a konfiguraci MS Windows 2003 serveru v prostředí internetu. Nakonfigurujte doménu a terminálový server.
Navrhněte metodu bezpečného přenosu dat v internetu.
Všechny konfigurace provádějte s ohledem na lokální a síťovou bezpečnost systému.
Dále vypracujte soubor pravidel pro udržování systému v chodu.

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Deitel, H. M.: Operating Systems, Prentice Hall, 2004
Klimeš, C.: Operační systémy 1. Ostravská univerzita v Ostravě, Katedra informatiky a počítačů.
Kokoreva, O.: Registr Microsoft Windows XP, Computer Press 2002
Solomon, D. A.: Windows NT pro administrátory a vývojáře, Computer Press 1999
Tanenbaum, A. S.: Modern operating systems, Prentice Hall, 2002
Resource Kit Microsoft Windows XP

Vedoucí bakalářské práce: **Ing. Martin Sysel, Ph.D.**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **24. května 2007**

Ve Zlíně dne 13. února 2007

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce je zaměřena na základní popis serverového operačního systému Microsoft Windows Server 2003 R2 (jazyková verze EN). Jedná se o nejnovější serverový operační systém společnosti Microsoft. V jednotlivých částech jsou popsány základy instalace, nastavení domény a služby Active Directory, terminálového serveru, připojení k síti a základní údržba a správa systému. V příloze jsou popsány základní metody obnovení a testování bezpečnosti hesla pro ověření identity uživatele.

Klíčová slova: serverový operační systém, Windows Server, instalace, doména, Active Directory, Route and Remote Access, VPN, Events, zálohování, Brute Force, Rainbow Attack..

ABSTRACT

This bachelor work feautures on basic description of server OS, Microsoft Windows Server 2003 R2 (EN). This is the latest server OS by Microsoft. In the several parts is given description of basics of installation process, setting of domain and Active Directory service, terminal server, connection to network and basic maintainance of system. Appendix includes description of recovering method and testing of user ID certification security password.

Keywords: server operating system, Windows Server, installation, domain, Active Directory, Route and Remote Access, VPN, Events, back-up, Brute Force, Rainbow Attack..

Chtěl bych touto cestou poděkovat za pomoc s prací následujícím osobám:

Ing. Martin Sysel Ph.D. (Fakulta aplikované informatiky Univerzity Tomáše Bati ve Zlíně), který byl ochotný mi vždy pomoci při tvorbě této bakalářské práce a pomáhal mi tvořit obsah a náplň této bakalářské práce.

Bc. David Malaník MCP (lektor kurzu Managing and Maintaining a Microsoft Windows Server 2003 Environment, MCP 70-290), který byl ochotný mi poradit se specifickými problémy při nastavování a správy operačního systému a metodami testování bezpečnosti hesla.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

V dnešní době existuje mnoho operačních systémů různých společností a organizací, které lze nejen teoreticky, ale i prakticky, úspěšně nasadit jako serverové řešení. Serverový operační systém společnosti Microsoft je z tohoto pohledu specifický systém, primárně určený pro správu a zabezpečení ostatních operačních systémů a programů společnosti Microsoft používaných na stanicích a jako základ pro další serverové systémy a doplňky společnosti Microsoft i jiných výrobců. Právě z důvodu velkého rozšíření operačních systémů a programů společnosti Microsoft na stanicích jsou i serverová řešení této společnosti hojně využívána.

Cílem této bakalářské práce bylo přiblížit základní metody instalace, nastavení a správy tohoto operačního systému. Velkou výhodou používání tohoto systému je možnost skoro úplné grafické administrace, která zjednodušuje a zlehčuje administrátorské úkony, což ovšem často vede k problémům, že tyto operační systémy mohou být administrovány i uživateli, kteří nejsou plně obeznámeni s problematikou používání daných služeb. Tento fakt přispívá k částečným negativním odezvám na používání tohoto operačního systému.

Samotná správa a nastavení operačního systému Microsoft Windows Server 2003 jsou natolik obsáhlá témata, že není možné je ani základním popisem obsáhnout v této bakalářské práci. Proto jsem se v této práci zaměřil na určité služby a snažil se popsat jejich základní možnosti a základní nastavení tak, aby byly dostupné i začátečníkovi.

1 ZÁKLADNÍ POPIS SYSTÉMU MICROSOFT WINDOWS SERVER 2003

1.1 Základní popis systému

Operační systém Microsoft Windows Server 2003 R2 je nejaktuálnější serverovou platformou společnosti Microsoft. Jedná se o moderní, síťový a uživatelsky příjemně navrhnutý operační systém s nejnovější podporou pro běh aplikací navržených pro nativní aplikační rozhraní 32 bitových, 64 bitových Windows a pro nejnovější běhové prostředí společnosti Microsoft .NET Framework. Operační systém v základní podobě obsahuje servery nejpoužívanějších síťových služeb (DNS, DHCP, VPN, NBNS/WINS atd.), souborových a tiskových služeb a také robustní řešení pro centralizovanou správu a zajištění síťových politik pomocí technologie Active Directory druhé generace, která umožňuje centrální autentizaci a autorizaci klientů prostřednictvím technologie Kerberos, a pomocí centralizované správy Group Policy (Zásad skupiny) v doméně.

Operační systém Microsoft Windows Server 2003 je dostupný pro 32 bitové hardwarové platformy i386, tak i pro 64 bitové hardwarové platformy. Je tak zajištěna zpětná kompatibilita a možnost nasazení nativních 64 bitových aplikací.

Z pohledu administrace je operační systém primárně administrovatelný v grafickém prostředí pomocí MMC konzol. V oblasti administrace však existují i nástroje pro správu v podobě konzolových, řádkových, aplikací. Jsou zde k dispozici sady Support Tools, Recource Kit Tools. Volitelně lze operační systém doplnit o technologii Microsoft Command Shell používající programovací jazyk Monad. Command Shell je nástupce příkazového řádku, který bude plně implementován v serverovém operačním systému Microsoft Longhorn Server, a bude umožňovat plnou administraci serveru pomocí řádkových příkazů a skriptů.

1.2 Typy operačních systémů Microsoft Windows Server 2003

Operační systém Microsoft Windows Server 2003 byl navržen v 5 specifikacích podle způsobu použití.

Jsou to:

- Windows Server 2003 Standard edition
- Windows Server 2003 Enterprise edition
- Windows Server 2003 Web edition
- Windows Server 2003 Datacenter
- Windows Small Business Server 2003

Jednotlivé specifikace se od sebe liší i hardwarovými nároky jako minimální rychlost procesoru, počet procesorů, velikosti RAM paměti a podporou Active Directory. Jednotlivé požadavky na výkon a kompatibilitu hardwaru je možno dohledat ve Windows Catalog List (HCL) podporovaného hardware [7].

1.2.1 Operační systém Windows Small Business Server 2003

Je to speciální úprava operačního systému Microsoft Windows Server 2003 určená pro použití v malých společnostech. Obsahuje různé doplňky (Microsoft Exchange Server, Microsoft ISA Server), které jsou jinak prodávány jako samostatné produkty společnosti Microsoft a pro operační systém Microsoft Windows Small Business Server 2003 byly upraveny (zjednodušeny). Upravení operačního systému je negativně ovlivněno ztrátou některých funkcí jako replikace domén, omezení počtu uživatelů a nutnost provozovat veškerý software na jednom hardware.

2 INSTALACE MICROSOFT WINDOWS SERVERU 2003

2.1 Základní popis instalace operačního systému

Instalace operačního systému Microsoft Windows Server 2003 probíhá ve větší části v grafickém prostředí. Je zjednodušena na základní nastavení nutná provést během instalace. Existuje více možností instalací. Instalaci lze provést z instalačního CD nebo DVD bootovacího disku, z obrazu disku pomocí programů třetích stran nebo pomocí bezobslužné a vzdálené RIS (Remote Instalation System) instalace.

Další důležitou volbou je způsob licencování operačního systému Microsoft Windows Server 2003 podle počtu licencí samotného operačního systému a podle požadavku na technickou podporu společnosti Microsoft. Většinou se používají dva typy licencí operačního systému. Je to Corporate Edition (Multilicence) a Single Edition (Pro jeden hardware). Corporate Edition (Multilicence) se používá při instalacích ve větších organizacích nebo školících střediscích, jedno licenční číslo (Product key) se používá k instalaci více operačních systémů na rozdílných hardwarových platformách a není třeba tyto operační systémy aktivovat. U Single Edition (Pro jeden hardware) je možno jedno licenční číslo použít k instalaci pouze jednoho operačního systému a navíc je nutné tento operační systém do doby 30 dnů aktivovat, jinak přestane fungovat. Aktivace znamená poskytnout společnosti Microsoft aktivačním programem vygenerované číslo online pomocí internetu nebo pomocí telefonní linky, na jehož základě Vám společnost Microsoft poskytne, pokud máte legální kopii instalace operačního systému, aktivační číslo, které vyžaduje operační systém pro aktivaci.

Další typ licence je OEM licence. Je to typ licence, která se prodává s novým hardwarem, ale jeho opakovaná instalace je vázána na tento hardware a je podmíněna omezeným počtem změny hardware. Společnost Microsoft se prodejem této licence zbavuje nároku na technickou podporu, která tímto přechází na prodejce hardware. Licence typu OEM jsou tedy levnější, ovšem u operačního systému typu Microsoft Windows Server 2003 je technická podpora jednou z nejdůležitějších věcí. Pod pojmem technická podpora se rozumí online podpora techniků společnosti Microsoft.

Další důležitou volbou je způsob licencování operačního systému vzhledem k celé síťové struktuře. Pro legální používání operačního systému se síťovou strukturou je potřeba koupit licenci na používání samotného operačního systému, a ještě licence na přístup k operačnímu systému přes síťové struktury. Jedná se o licence, kterými společnost Microsoft zpoplatňuje síťovou komunikaci operačního systému Microsoft Windows Server 2003 a ostatních operačních systémů serverového typu nebo klientských stanic společnosti Microsoft. Existují dva typy licencí, Per Server Licensing (licence na straně serveru) a Per Seat Licensing nebo Per User Licensing (licence na straně ostatních serverů nebo klientských stanic).

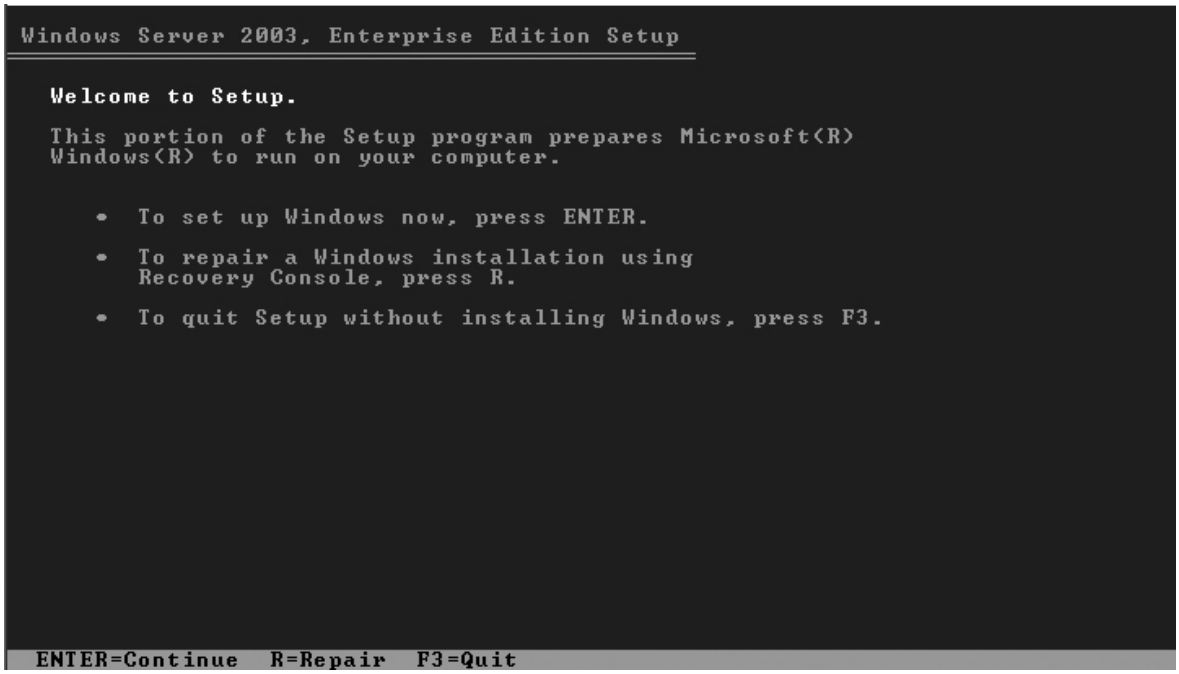
Rozdíl mezi těmito dvěmi způsoby licencování je v počítání přístupů na operační systém. Varianta Per Server Licensing (licence na straně serveru) zpoplatňuje jednou licencí komunikaci každé stanice se serverem v síti bez ohledu na počet uživatelů, kteří tuto stanici využívají. Druhá varianta Per Seat Licensing nebo Per User Licensing (licence na straně ostatních serverů nebo klientských stanic) zpoplatňuje jednou licencí komunikaci každého uživatele se serverem v síti bez ohledu na počet stanic, které tito uživatelé používají. Pokud bude nutné tuto volbu v budoucnu změnit, nelze to provést bez nové instalace operačního systému.

2.2 Instalace operačního systému pomocí bootovacího CD nebo DVD disku

Instalace operačního systému Microsoft Windows Server 2003 pomocí bootovacího CD nebo DVD disku je jedna z možností instalace operačního systému. Pro začínajícího administrátora je to jedna z nejjednodušších možností instalace operačního systému.

Instalace se spouští z bootovatelného CD nebo DVD disku, proto je potřeba nastavit BIOS na bootovaní z CD/DVD mechaniky. Po spuštění instalace provádí instalační program základní kontrolu hardware a kopírování základních souborů instalace. Během tohoto kopírování lze do instalace zasáhnout v případě speciálních požadavků jako instalace na SCSI disky nebo na raidové pole, pro které není instalace standardně připravena. Při tomto požadavku se musí do instalačního programu dodat externí ovladače těchto zařízení.

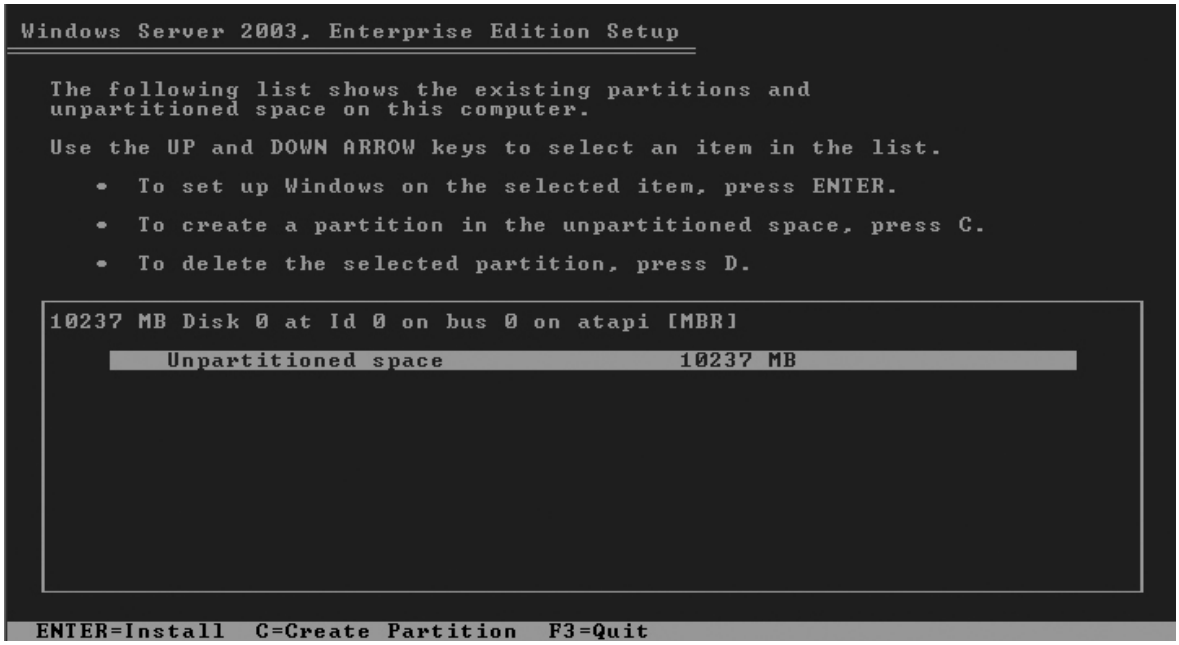
Po zkopírování základních souborů instalace se instalátor zeptá, jestli operační systém nainstalovat nebo spustit Recovery konzoli pro opravu již nainstalovaného operačního systému. Recovery konzole umožňuje provádět zásahy do operačního systému bez jeho spuštění a vyřešit tak některé problémy spojené s fungováním operačního systému. Do Recovery konzole se lze přihlásit pouze uživatelským heslem administrátora. Pokud je v operačním systému nainstalována služba Active Directory, pro přihlášení do Recovery konzole je nutné se přihlásit heslem administrátora, které bylo v operačním systému používáno před instalací a konfigurací služby Active Directory.



Obrázek 1, úvodní obrazovka instalace operačního systému

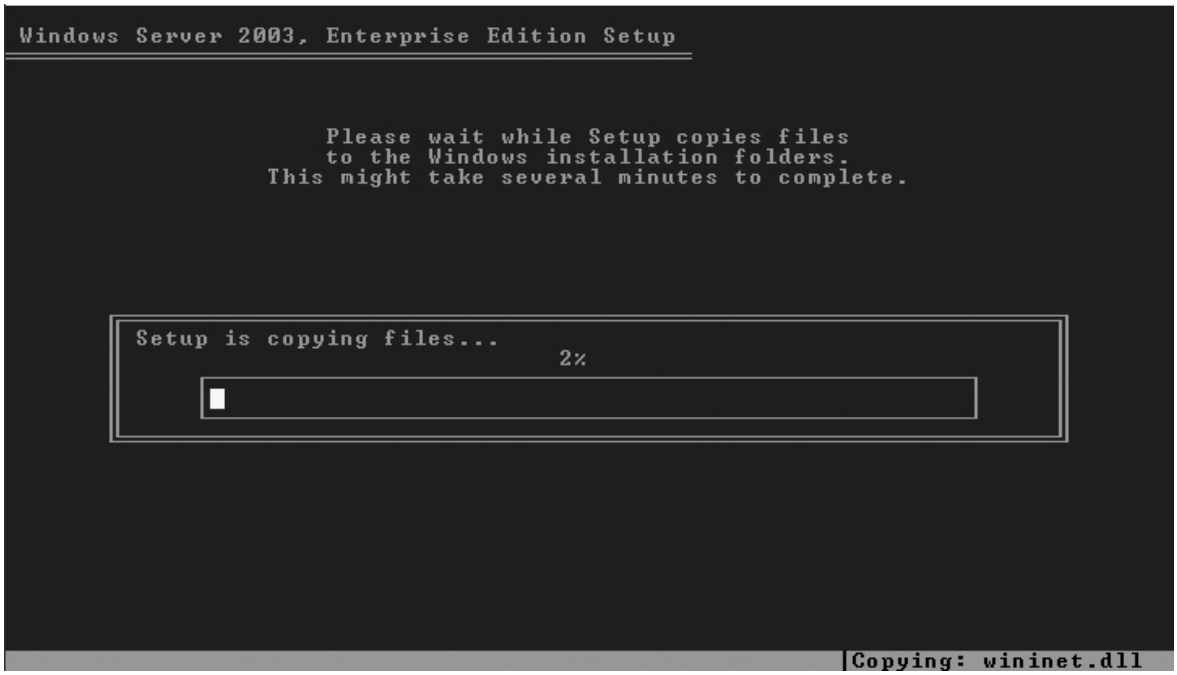
V další nabídce musí administrátor souhlasit s podmínkami společnosti Microsoft pro používání operačního systému Microsoft Windows Server 2003. Pokud s danými podmínkami nebude souhlasit, instalace bude ukončena. Souhlas s licenční smlouvu, která se instalací operačního systému se společností Microsoft stvrzuje, se provádí klávesou F8.

Pak je nutno zvolit disk a oddíl, kam bude operační systém nainstalován. Instalátor umožňuje vytvářet, mazat a formátovat oddíly disku na souborový systém FAT32 a NTFS rychle nebo úplně. Je doporučeno instalovat a používat souborový systém typu NTFS a používat úplné formátování.



Obrázek 2, možnosti práce s disky a oddíly při instalaci

Po zvolení umístění instalace začne instalátor instalovat samotný operační systém.



Obrázek 3, průběh kopírování souborů

Následuje restart instalace a instalátor nabootuje do grafického prostředí instalace.

Obrázek 4, grafické rozhraní instalace

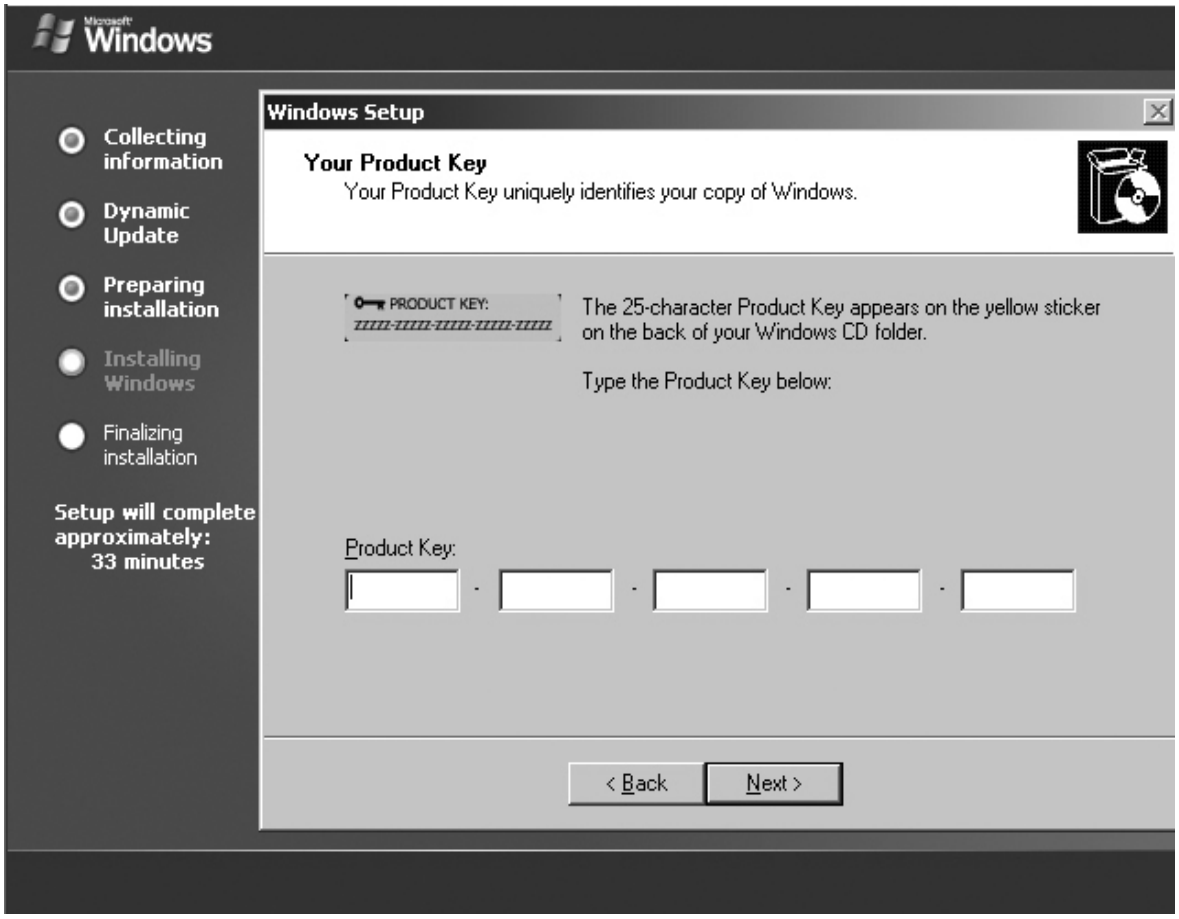
V grafickém prostředí je nutné vyplnit některé údaje důležité pro instalaci operačního systému.

Jsou to následující položky:

Regional and Language Options, kde se nastavují jazykové a zvykové nastavení operačního systému pro zeměpisnou oblast, kde bude operační systém používán.

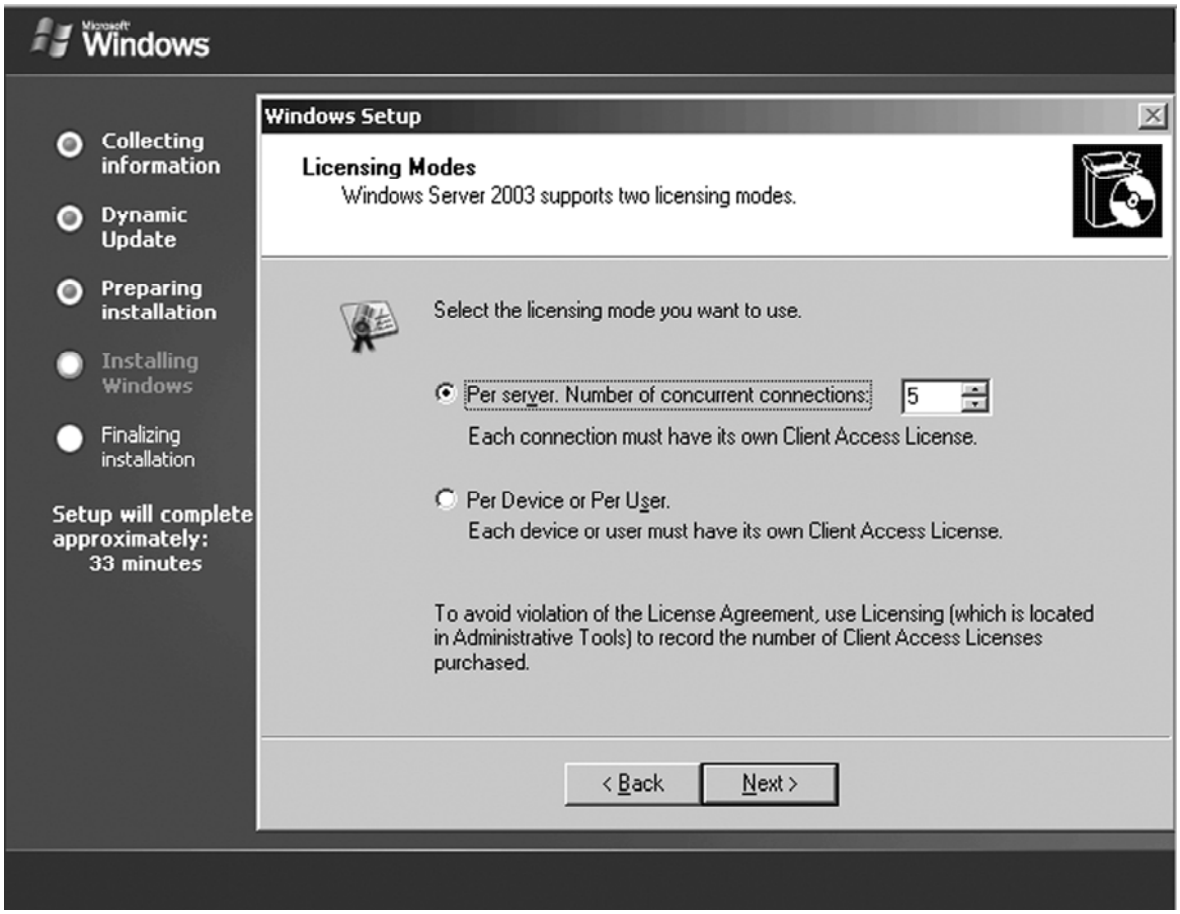
Perzonalize Your Software, kde je potřeba vyplnit jméno (Name) a organizaci (Organization), které budou operační systémy používat.

Your Product Key, zde musíte zadat licenční číslo (Product Key), které jste dostali při koupi operačního systému nebo při koupi hardwaru serveru.



Obrázek 5, zadání Product key (Licenční číslo)

Licensing Modes, Typ licence, zde se nastavuje typ licence pro síťovou komunikaci se serverem. Tento typ licencování je vysvětlen v kapitole 2.1.



Obrázek 6, volba licencování síťové komunikace

Computer name and administrator's password, Jméno počítače a heslo pro účet administrátora. Pokud bude zadáno heslo nesplňující kritéria bezpečného hesla, systém automaticky upozorní, že heslo není bezpečné. Bezpečné heslo by mělo obsahovat minimálně 6 znaků, přičemž alespoň jeden znak by měl být velké písmeno, jeden znak malé písmeno, jeden znak číslo a jeden speciální znak. Pokud bude heslo menší, než 15 znaků, tak bude při standardním nastavení registrů operačního systému uloženo do registrů zašifrované starší metodou šifrování, která je dnes již prolomena. Toto nastavení lze změnit.

Time and Date, Time zone, Nastavení času a data, nastavení Časové zóny.

Network setup, Nastavení sítě, umožňuje již v průběhu instalace nastavit parametry jednotlivých síťových adaptérů.

Tímto krokem nastavení instalace končí, po restarování operačního systému se spustí samostatný operační systém Microsoft Windows Server 2003.

2.3 První spuštění operačního systému

První spuštění operačního systému Microsoft Windows Server 2003 již probíhá z pohledu administrátora jako normální spuštění. Po přihlášení administrátora se zobrazí okno s nabídkou aktualizace operačního systému (Windows Server Post Setup Security Update). Skládá se ze dvou kroků.

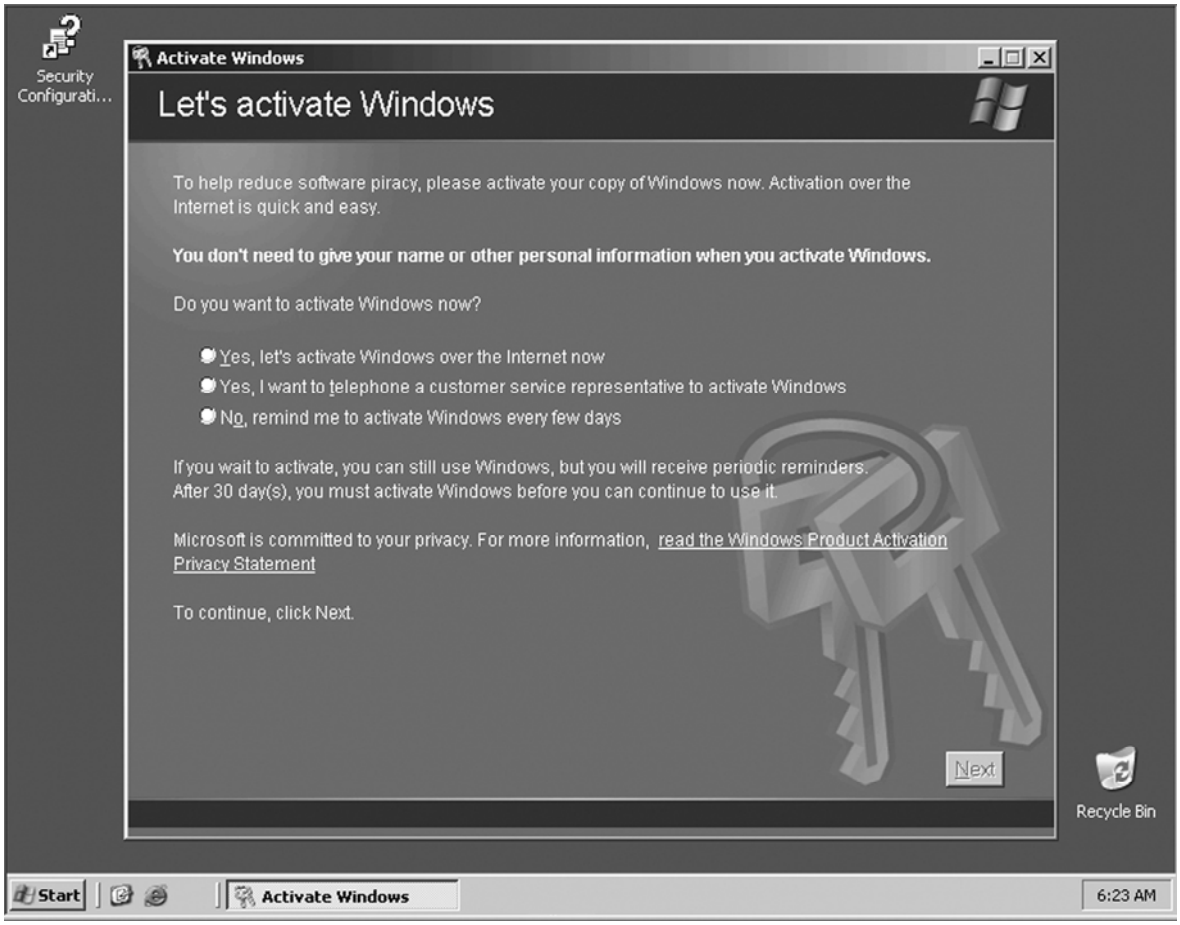
Instalace kritických bezpečnostních aktualizací operačního systému (Install Critical Security Update). Tento krok spustí Microsoft Internet Explorer, který se připojí na webovou stránku online aktualizace produktů společnosti Microsoft *http://update.microsoft.com*. Tímto způsobem lze velmi jednoduše stáhnout a nainstalovat všechny aktualizace všech operačních systémů společnosti Microsoft, pro které zajišťuje softwarovou podporu.

Konfigurace automatické aktualizace operačního systému (Configure Automatic Updates). Tento krok umožňuje nastavit automatické aktualizování operačního systému. Je zde možno nastavit plně automatickou aktualizaci, stahování, ale neinstalování aktualizací, upozorňování na nové aktualizace nebo zakázat automatickou aktualizaci. Toto nastavení je důležité pro pozdější bezproblémové fungování operačního systému, protože jen aktualizovaný operační systém je plně funkční. Všechny volby mají i nevýhody. Pokud bude systém nastaven na automatickou aktualizaci, může dojít k situaci, že po instalaci aktualizace bude operační systém vyžadovat restartování systému, což může v praktickém nasazení způsobovat nežádoucí výpadky části nebo celé síťové struktury. Tento restart operačního systému by neměl být proveden bez schválení administrátora, ale z praxe mohu potvrdit, že pokud není po instalaci určitých aktualizací operační systém restartován do určité doby, z praxe 7 až 14 dnů, restartuje se sám. Pokud bude operační systém nastaven na upozorňování o nových aktualizacích, vyžaduje operační systém manuální potvrzení instalace aktualizací. Nejhorší variantou je zakázání automatických

aktualizací, kdy časem můžou závažná bezpečnostní rizika, až nefunkčnost některých programů.

2.4 Aktivace operačního systému (Activate Windows)

Poslední krokem, který je pro fungování operačního systému Microsoft Windows Server 2003 v určitých typech licencí nutný, je aktivace operačního systému. Aktivace je proces, který pomocí internetu nebo pomocí telefonu ověří legálnost instalace kopie operačního systému. Pokud aktivace nebude provedena do 30 dnů od data instalace, operační systém přestane být po 30 dnech funkční. Součástí aktivace je i možnost registrace operačního systému.



Obrázek 7, aktivace legální kopie operačního systému

2.5 Instalace komponent integrovaných v operačním systému

V operačním systému Microsoft Windows Server 2003 se všechny instalace a nastavení integrovaných komponent mohou provádět v grafickém prostředí. Některé komponenty ani nelze jiným způsobem nainstalovat. Alternativním řešením instalace a nastavením je použití skriptovacího jazyka, ale i tento způsob vyžaduje používání grafického prostředí. Vytvoření a používání skriptů je výhodné při větším množství instalace.

Obrázek 8, nabídka instalace a nastavení služeb

3 DOMÉNA

3.1 Základní popis domény

Doména je jedna z nejdůležitějších síťových prostředí operačních systémů společnosti Microsoft. V prostředí serverových technologií společnosti Microsoft je doména spojena s organizací neurčitého počtu dalších serverových a klientských stanic, tedy je to způsob centralizované správy. Instalace domény v operačním systému Microsoft Windows Server 2003 je vlastně instalace služby Active Directory, což znamená povýšení serveru do role řadiče domény. S instalací a správnou funkcí domény souvisí i instalace a nastavení ostatních síťových služeb jako DNS a DHCP server, které nemusí být nutně provozovány na operačních systémech společnosti Microsoft, ale tato kombinace přináší určité výhody.

Každá doména musí být pojmenována. Toto pojmenování musí být jednoznačné a musí splňovat podmínky mezinárodně dohodnuté gramatiky.

3.2 Plánování oborů a názvů domén

Správný návrh názvů oborů a názvů domén je velmi důležitou a často opomíjenou součástí při zavádění a instalaci domény. Je potřeba detailně analyzovat strukturu a potřeby sítě, kde bude doména zprovozněna, aby nedošlo k nevhodnému nebo špatnému nastavení a pozdějším opravám celého systému nebo jeho částí.

3.2.1 Stromy a doménové struktury

Existují dva základní typy oborů názvů, je to strom a doménová struktura.

Strom :

Obor názvů stromu je jednoduchý, souvislý obor názvů, kde každý název je přímo odvozen z jednoho názvu kořene. Tento typ přímého pojmenování je vhodný pro organizaci, která je jednotná a má jednoduchý název představující základ názvu pro mnoho různých poboček. Tomuto modelu odpovídá řada malých a středně velkých podniků.

Doménové struktury :

Obor názvů doménové struktury je souhrn v zásadě rovnocenných stromů, které nemají žádný jednoduchý společný kořen oboru názvů. Obor názvů doménové struktury je vhodný pro organizaci, která má více oborů zájmů, z nichž každý je označen vlastním samostatným identifikovatelným názvem. Tomuto modelu odpovídají většinou velké podniky, které nemají jednu centrální skupinu informačního systému, ale každá divize má svoji strukturu.

3.2.2 Definování konvence pojmenování

Definování konvence pojmenování definuje způsob pojmenování větví stromu. Existují dva typy konvencí pojmenování, jsou to organizační a zeměpisné konvence pojmenování.

Organizační konvence pojmenování :

Pomocí organizační konvence pojmenování se v doméně vytváří obory názvů, které kopírují strukturu organizace. Pro kořen domény firma.cz se první úroveň může skládat z položek admin.firma.cz, vedeni.firma.cz, finance.firma.cz.

Výhody.

- Odráží organizaci společnosti.
- Je srozumitelný.
- Má přirozenou cestu růstu.
- Umožňuje organizaci zdrojů podle potřebného typu.

Nevýhody.

- Je obtížné jej upravit v případě změny struktury organizace a názvů.
- Může být politicky citlivý.
- Je obtížné jej podporovat v případě rozdělování a slučování poboček.
- Implementace může být odlišná v případě, že jednotlivé pobočky mají více sídel.

Zeměpisná konvence pojmenování :

Pomocí zeměpisné konvence pojmenování se v doméně vytváří obory názvů na základě zeměpisné struktury poboček organizace. Pro kořen domény firma.cz se první úroveň může skládat z položek praha.firma.cz a brno.firma.cz.

Výhody.

- Je apolitický.
- Používá názvy, které jsou pravděpodobně neměnné.
- Nabízí vyšší flexibilitu a rozmanitost.

Nevýhody.

- Neodráží povahu organizace.
- Může vyžadovat zapojení více domén pro potřeby zabezpečení.

3.2.3 Určení způsobu rozlišování názvů

Určení způsobu rozlišování názvů souvisí s používáním interních a externích oborů názvů domény.

Použití stejných interních a externích oborů názvů :

Pokud je použit jediný obor názvů, tak mají všechny počítače stejné názvy v interní síti jako ve veřejné síti internet. Registrační úřad na internetu udržuje jediný obor názvů systému DNS (Domain Name System). Tato možnost obsahuje zvýšené bezpečností riziko pro síťovou strukturu. V takovém případě je schopnost rozlišování názvů mimo společnost omezena na počítače umístěny v DMZ (Demilitary Zone), tedy zóně, která není chráněna bránou firewall. V této zóně by neměly být umístěny servery spravující službu Active Directory.

Výhody.

- Poskytuje jednotné pojmenování interní i externí sítě.
- Umožňuje registraci jednoho názvu.
- Umožňuje uživatelům vlastnit jedinou identitu při přihlašování a identitu pro emaily.

Nevýhody.

- Vyžaduje složitou konfiguraci při použití PROXY serveru.
- Vyžaduje spravování různých zón se stejnými názvy.
- Vyžaduje, aby uživatelé znali možnosti různých zobrazení prostředků v závislosti na používání síťové struktury.

Použití různých interních a externích oborů názvů :

Pokud jsou použity odlišné obory názvů pro interní a externí síťové struktury, může být jméno domény pro okolí odlišné, než pro vnitřní síť. Stejně tak i všechny prostředky umístěny v externí síti používají externí obory názvů a všechny prostředky umístěny v interní síti používají interní obory názvů. Oba tyto obory názvů domén je potřeba registrovat na příslušném Registračním úřadu na internetu.

Výhody.

- Poskytuje jednoznačné rozlišení prostředků v interní a externí síťové struktuře.
- Umožňuje snadnější správu při použití PROXY serveru.

Nevýhody.

- Vyžaduje registraci obou domén.
- Způsobuje, že jména uživatelů pro přihlášení se liší od jmen používaných v emailu.

3.3 Plánování doménové struktury

Při stanovení celkového rozvržení oborů názvů je třeba rozvrhnout také doménovou strukturu. Každý strom doménové struktury se dělí na doménu nebo organizační jednotku. Toto dělení závisí na potřebách replikace, zásadách zabezpečení, dostupnosti zdrojů a kvality připojení.

3.3.1 Doména

Doména je základní jednotkou adresáře Active Directory systému Microsoft Windows Server 2003. Všechny prostředky existující v síti jsou součástí domény a v rámci domény jsou na ně uplatňovány jednotné zásady zabezpečení. Toto zabezpečení je založeno na protokolu Kerberos V5, který umožňuje přenosnost těchto zásad v rámci různých domén.

Řadiče domény systémů Microsoft Windows Server 2003 používají model více hlavních domén. Každý řadič domény má v doméně stejnou autoritu, a pokud některý přejde do režimu offline, ostatní nadále spravují a ověřují doménu. Jakýkoliv řadič v doméně může být zdrojem změny v doméně, která je pak distribuována ostatním řadičům v dané doméně. Tato funkce se nazývá replikace domény.

Doména vymezuje šířitelnost přístupových práv uživatelů definovaných v doméně.

3.3.2 Organizační jednotka

Organizační jednotky vznikly v systému Microsoft Windows Server 2000. Organizační jednotka obsahuje některé vlastnosti domény, ale postrádá doplnění o prostředky. Organizační jednotka je součástí domény a funguje jako zásobník objektů adresářové služby. Sama o sobě představuje větev souvislého oboru názvů a může obsahovat jiné organizační jednotky a umožňuje nastavení oprávnění a práva pro správu bez ohrožení zbývající části domény. Organizační jednotka nevyžaduje samostatný řadič domény a ani není zahrnuta v replikaci. V případě potřeby lze organizační jednotku povýšit na doménu.

4 SLUŽBA ACTIVE DIRECTORY

4.1 Instalace služby Active Directory

4.1.1 Kontrola předpokladů pro instalaci služby Active Directory

Instalace služby Active Directory v operačním systému Microsoft Windows Server 2003 je důležitou změnou ve fungování operačního systému. Proto je výhodné provést kontrolu výchozích požadavků na provoz služby Active Directory [7].

- V síťovém prostředí by měla být dostupná služba překladu jmen DNS. Není nutné, aby byl server DNS provozován na platformě společnosti Microsoft, ale při instalaci služby Active Directory přináší provoz DNS serveru na platformě společnosti Microsoft různé výhody. Velmi výhodnou vlastností služby DNS, která bude používána při instalaci služby Active Directory, je schopnost přijímat žádosti o dynamické záznamy.
- Server, na němž bude provozován řadič domény, by měl mít přiřazeny statické síťové IP adresy.
- Souborový systém na discích serveru musí být typu NTFS.

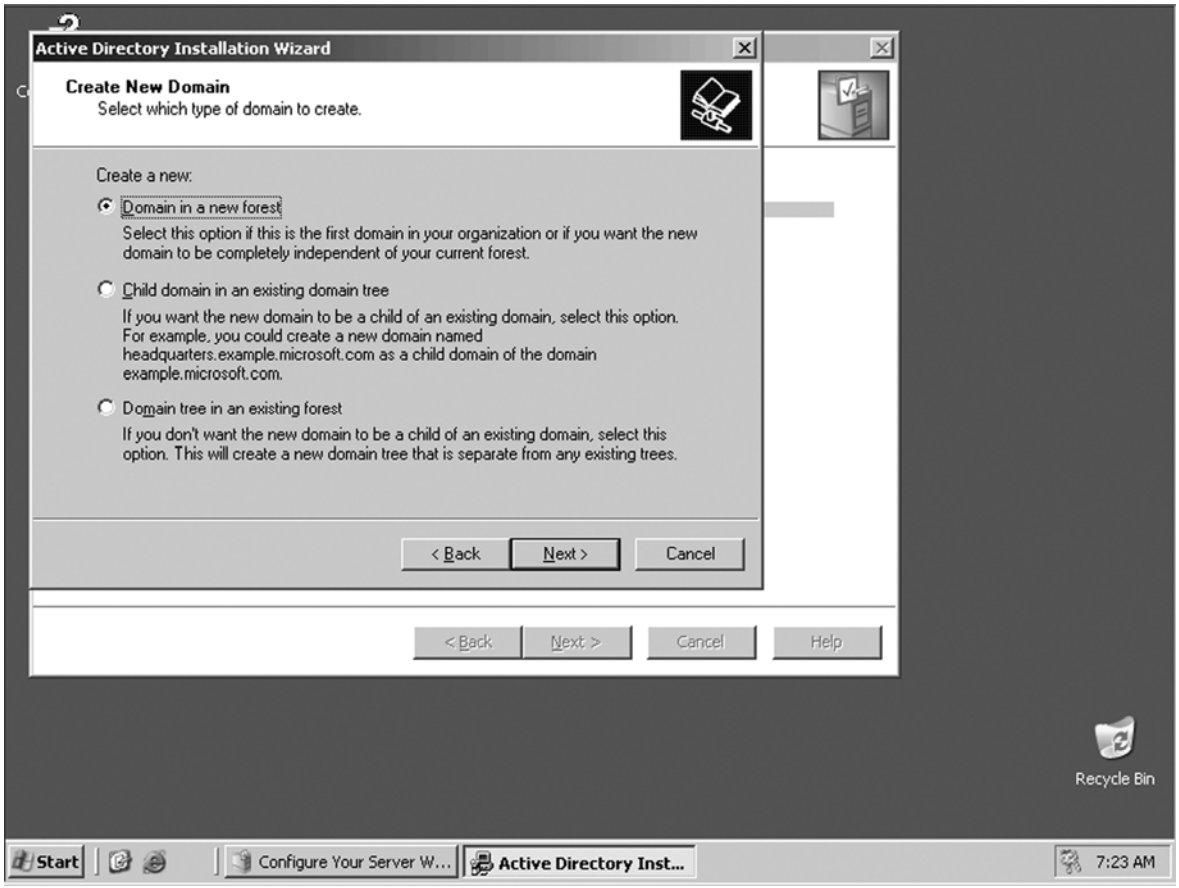
Instalace služby Active Directory se provádí pro zavedení centralizované správy uživatelů, počítačů a služeb v síti. Z toho vyplývá, že aby měla centralizovaná správa v síti smysl, měly by být na stanicích použity operační systémy společnosti Microsoft, které mají implementovanou možnost připojení stanice do domény. V současné době lze najít i neoficiální návody pro připojení různých typů distribucí Linuxu ke službě Active Directory a naopak existují distribuce Linuxu schopné nahradit službu Active Directory pro operační systémy Microsoft umožňující připojení do domény, ale tuto možnost a funkčnost jsem zatím neměl možnost ověřit.

4.1.2 Zavedení služby Active Directory

Nejjednodušší způsob instalace Active Directory je pomocí grafického rozhraní. Tento způsob není automatizovaný, tudíž skoro všechny volby musí administrátor provádět ručně. Instalační průvodce se spouští příkazem *dcpromo.exe*. Tento příkaz slouží jak k zavedení role řadiče domény, tak ke zrušení role řadiče domény.

Po uvítací obrazovce volí administrátor v dalším kroku instalace Typ řadiče domény (Domain Controller Type). Zde se nastavuje, zda je tento řadič v nové zakládané doméně nebo je přidáván další řadič již do existující domény. Pokud je tento řadič další v doméně, tak již nezáleží na pořadí instalace řadiče, jelikož všechny kopie jsou si rovnocenné.

Pokud je vytvářena nová doména, je nutné rozhodnout, kam bude nově založená doména náležet v rámci celé struktury doménového lesa (Forestu). Tato volba se provádí v dalším kroku Vytvořit novou doménu (Create New Domain). Instaluje li se první řadič domény v síti, vybírá se volbu Doména v nové doménové struktuře (Domain in a new forest). Pokud se instaluje další doména v již existující doménové struktuře, zvolí se možnost Dědičná doména v již existující hlavní doméně (Child domain in an existing domain tree). Pokud se instaluje nová hlavní doména v existující doménové struktuře, zvolí se Domain tree in an existing forest. Pokud se instaluje replika v existující doméně, pak se v tomto kroku zadává její jméno a instalátor se pokusí kontaktovat stávající řadič domény pro získání potřebných informací.



Obrázek 9, instalace služby Active Directory

Pokud bylo zvoleno vytvořit novou doménu, v dalším kroku instalátor požaduje zadání jména domény ve tvaru FQDN (Fully Qualified Domain Name). Pokud byl před instalací zprovozněn server DNS s příslušnou zónou, jména DNS serveru a domény při instalaci Active Directory musí odpovídat.

Instalace následuje v dalších krocích:

Potvrzení zkrácení doménového jména pro použití protokolu a aplikačního rozhraní NetBIOS. Toto aplikační rozhraní bude využíváno pro komunikaci se staršími operačními systémy, než je Windows 2000.

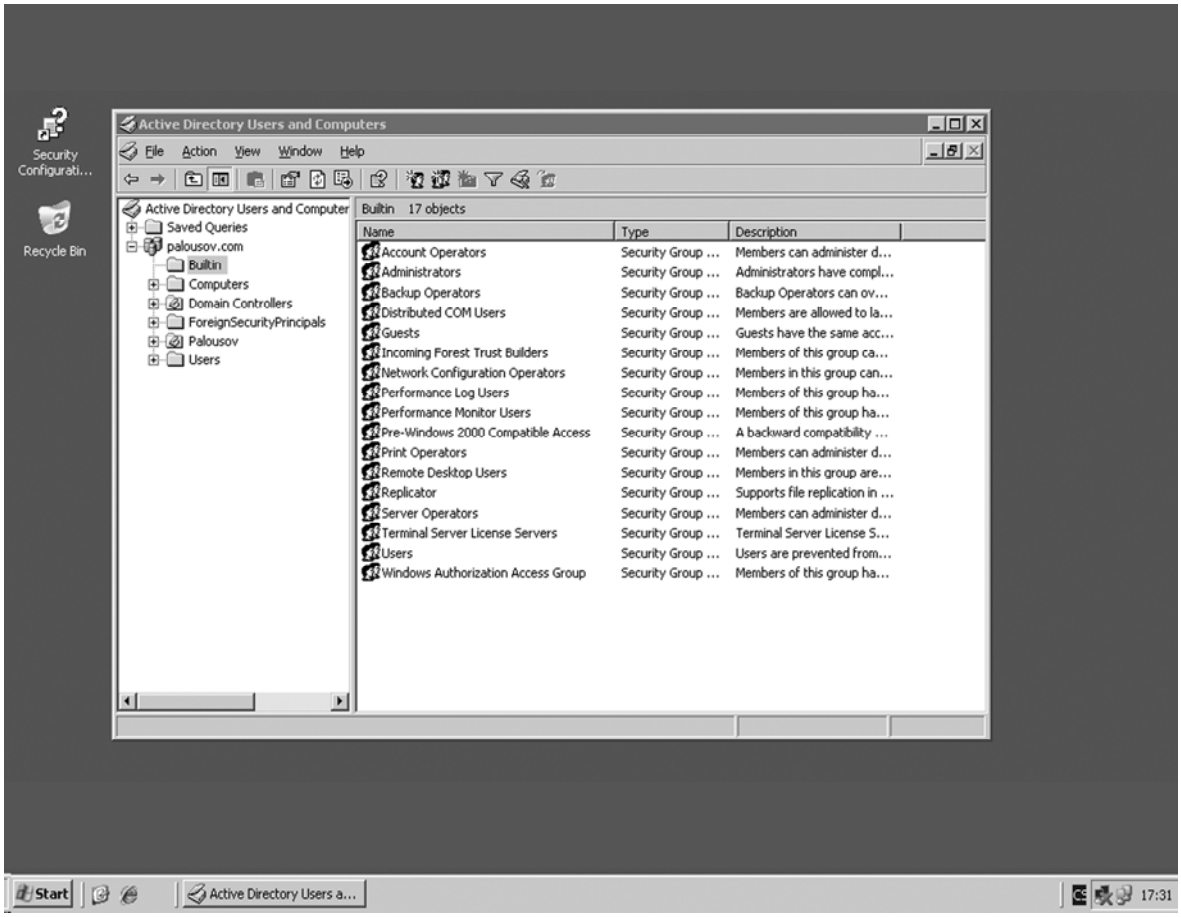
Volba Umístění databáze a protokolu (Databaze and Log Folders). Tato volba nemusí být definitivní, ale v případě budoucího přesunu souborů bude nutné dočasně službu Active Directory pozastavit. Následně se volí umístění složky SYSVOL, která bude replikována s ostatními řadiči domény a bude poskytovat soubory klientům Active Directory. Tato složka musí být umístěna na disku se souborovým systémem NTFS.

Prověření služby serveru DNS, kde bude kontrolovat odpovídající parametry. Pokud tato kontrola z nějakého důvodu neproběhne správně, spustí se průvodce Diagnostika registrace serveru DNS (DNS Registration Diagnostisc). Pokud vznikla chyba nedopatřením, protože v síti server DNS je, ale nepodařilo se ho kontaktovat, je možno instalátor vyzvat k dalšímu prověření. Další možnost je instalace serveru DNS, který je součástí operačního systému, v rámci instalace služby Active Directory. Poslední možnost je ruční správa serveru DNS bez dynamických záznamů.

Nastavení podpory zabezpečení pro klientské operační systémy, které budou používány v doméně. Pokud v síti nejsou klientské počítače s operačním systémem Microsoft starším, než Windows 2000, doporučuje se nezapínat zpětnou kompatibilitu s těmito systémy, protože dochází ke snížení zabezpečení v rámci domény. V dalším kroku se zadává heslo pro spuštění řadiče domény ve speciálním režimu obnovy služeb Active Directory. Toto heslo je odlišné od hesla administrátora.

Nabídka kontroly údajů potřebných pro instalaci, a pokud nemá alespoň jeden síťový adaptér nastavenu pevnou IP adresu, umožní její změnu. Celá instalace se dokončí tlačítkem Finish, po kterém začne operační systém zavádět službu Active Directory. Na závěr instalace je potřeba operační systém restartovat [8].

4.2 Používání Active Directory



Obrázek 10, MMC konzole služby Active Directory

Po instalaci služby Active Directory je služba v defaultním nastavení, kdy jsou založeny základní uživatelské účty a základní skupiny. Nastavování a používání služby je velmi jednoduché a lze ho provádět jak přes grafické rozhranní, tak přes příkazový řádek. Je velmi dobré si před začátkem samotného nastavování rozvrhnout strukturu domény, tudíž i strukturu Active Directory a skupin uživatelů, protože špatná implementace může vést k nepřehlednosti a složitosti nastavování. Při delším používání a větším množství uživatelů a skupin by snad každý administrátor odcenil nástroj pro tvorbu přehledů nastavení podle různých kritérií, což ovšem v současné době není možné.

Velmi dobré je i aditivní nastavování Group Policy jednotlivým uživatelům, skupinám i počítačům, kdy se jednotlivá práva a oprávnění sčítají podle umístění v organizační struktuře Active directory. Co tu ovšem opět chybí, je nástroj pro tvorbu přehledů nastavení.

V závislosti na instalaci dalších služeb a serverů se nabídka nastavení služby Active Directory může měnit, nejlepším příkladem je instalace serveru Microsoft Exchange Server, což je server pro správu emailové pošty společnosti Microsoft, kdy se část nastavení provádí přímo v Active Directory, nebo nastavení přístupu přes Terminal Server a přístup přes VPN připojení uživatelů, kdy se skoro všechna nastavení provádí v Active Directory.

5 TERMINÁLOVÁ SLUŽBA OPERAČNÍHO SYSTÉMU MICROSOFT WINDOWS SERVER 2003

5.1 Základní popis Terminálového serveru

Terminálová služba operačního systému Microsoft Windows Server 2003 je mechanizmus vzdáleného řízení, správy a využívání serverů. Je to tedy jak služba umožňující vzdálenou údržbu operačního systému, tak služba umožňující použití aplikačního serveru pro velký počet uživatelů. Terminálová služba přináší do operačních systémů společnosti Microsoft možnost souběžné práce více uživatelů.

Každý uživatel, který je k serverovému operačnímu systému připojen pomocí Terminálové služby, z pohledu klientských stanic pomocí nástroje Vzdálená plocha (Remote Desktop), využívá systémové a hardwarové prostředky samotného serveru a ne klientské stanice, ze které se připojuje. Uživatel sdílí procesor, paměť RAM a pevné disky serveru. Po připojení k Terminálové službě se klientská stanice stává pouze konzolí pro připojení k Terminálové službě. Každý uživatel má svou vlastní relaci Terminálové služby a každá relace funguje samostatně a nezávisle na ostatních relacích.

Terminálová služba je velmi vhodným řešením pro mobilní uživatele, kteří potřebují pracovat s náročnými aplikacemi a přitom využívají pomalé připojení k síti a nedisponují dostatečně výkonným přenosným hardwarem.

5.2 Hardwarové nároky Terminálové služby

Terminálovou službu je možno nainstalovat na všechny operační systémy Microsoft Windows Server 2003, před instalací je ovšem nutné počítat s odlišnou licenční politikou společnosti Microsoft. Terminálový server pro více, jak 2 současně přihlášené uživatele, vyžaduje zakoupení doplňkové licence. Dalším kritériem při instalaci Terminálové služby je její použití jako aplikačního serveru, kdy je třeba počítat s vysokými nároky na uložení dat aplikací.

Každá relace serveru Terminálové služby využívá minimálně 20 MB RAM paměti pouze k přihlášení. K této velikosti je potřeba přidat hardwarové nároky jednotlivých spouštěných programů. Minimální velikost RAM paměti pro jednu relaci Terminálové služby je 40 MB RAM.

Je složité určit minimální kapacitu procesoru vzhledem k náročnosti jednotlivých uživatelů, podle oficiálních údajů procesor Intel Xeon pracující na frekvenci 2 GHz postačuje při dostačující velikosti paměti RAM k provozu 50 relací. Toto číslo je pouze relativní a slouží k obecné představě hardwarové náročnosti jednotlivých relací.

Velmi důležitým údajem je i rychlost připojení serveru, podle které se odvíjí maximální datový tok a tedy i množství informací, které je schopna si Terminálová služba vyměnit s klientskou stanicí. Podle toho se odvíjí nastavení rozlišení Vzdálené plochy, barevná hlouba Vzdálené plochy a jiné nastavení. Správné nastavení těchto parametrů, popřípadě snížení hodnot těchto parametrů, může zpříjemnit a zkvalitnit práci Vzdálené plochy [7].

5.3 Instalace Terminálové služby

Po instalaci operačního systému Microsoft Windows Server 2003 je Terminálová služba pro vzdálenou správu již nainstalována. Pro její používání je potřeba pouze povolit vzdálené připojení k operačnímu systému a přidělit uživatelům, kteří budou moci používat Terminálovou službu, oprávnění. Takto nastavená Terminálová služba umožňuje současné připojení maximálně dvou uživatelů k serveru.

Pokud se bude využívat Terminálová služba jako aplikační a terminálový server pro více uživatelů, je potřeba tento Terminálový server znovu nainstalovat. Nejjednodušší způsob instalace Terminálové služby je použití grafického průvodce, který je z větší části plně automatický. Během instalace je nutno počítat s vyžádáním instalačního CD nebo DVD média a s restartem operačního systému. Po restartování operačního systému a po přihlášení se zobrazí potvrzení, že byla role Terminál serveru přidána a otevře se okno s nápovědou pro dokončení instalace Terminál serveru. Nejdůležitější z těchto kroků je povolení připojení vzdálených uživatelů k serveru a konfigurace jejich oprávnění.

5.4 Používání Terminálové služby

5.4.1 Instalace programů

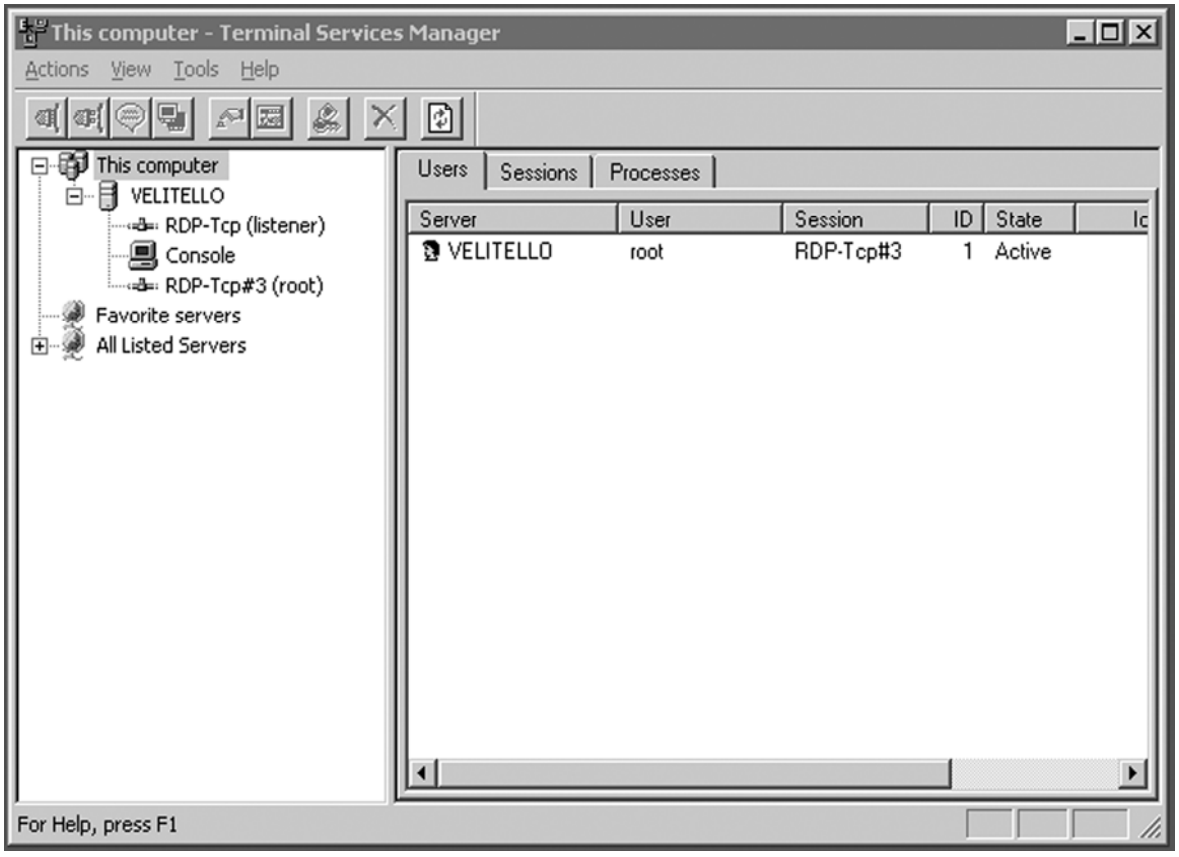
Instalace programů v operačním systému Microsoft Windows Server 2003 s nainstalovanou Terminálovou službou se v režimu Vzdálená plocha neliší od obecného způsobu instalace. V režimu aplikačního serveru je nutné počítat s možností několikanásobného spouštění jednoho programu více uživateli ve více relacích. Programy certifikované pro operační systémy Microsoft umožňují bezproblémové používání v rámci Terminál serveru. Pro režim aplikačního serveru obsahuje Terminálová služba dva režimy provozu, režim instalace a režim spouštění. Operační systém většinou sám rozezná instalaci programu a sám spustí režim instalace. Toto se nestane při instalaci starších aplikací, které nezískaly logo Certificed for Windows. Do režimu instalace je možno se přepnout zadáním příkazu *change* do příkazové řádky nebo instalací programu pomocí nástroje Přidat nebo odebrat programy. Nejdůležitější je neumožnit instalovanému programu po dokončení instalace restart počítače, ale dokončit průvodce instalací aplikace v operačním systému a teprve poté restartovat operační systém [7].

5.4.2 Správa Terminálové služby

Terminálovou službu lze v rámci domény konfigurovat z jediné konzole. Ke správě serverů a uživatelů se používají 3 základní nástroje.

Správce Terminálové služby

Správce Terminálové Služby (*tsadmin.exe*) monitoruje a řídí připojení ke všem serverům Terminálové služby v síti. Ve výchozím nastavení je možno se v jednom okamžiku připojit pouze k jednomu serveru, lze však zvolit připojení ke všem dostupným serverům, poskytujícím Terminálovou službu, najednou.



Obrázek 11, MMC konzole Terminal Services Manager

Konfigurace Terminálové služby

Konfigurace Terminálové služby se spouští na každém Terminálovém serveru pomocí konzoly MMC (Microsoft Management Konsole) a umožňuje provádět změny v nastavení Terminálové služby na Terminálovém serveru. Pomocí modulu MMC lze měnit vlastnosti připojení k Terminálovému serveru. Ve výchozím nastavení je nainstalován pouze protokol připojení Microsoft Remote Data Protocol (RDP) 5.2. Pomocí konzole MMC lze přidávat a konfigurovat další protokoly i třetích stran.

Protokol RDP 5.2 je definován pro zabezpečenou a šifrovanou 128 bitovou komunikaci, maximální nastavení 24 bitové hloubky obrazu, umožňuje připojit místní sériové porty, tiskárny, disky a audio výstup, a umožňuje autentizaci pomocí technologie Smart Card.

Nový operační systém společnosti Microsoft, Windows Vista, uvedený na komerční trh začátkem roku 2007, již používá pro Terminálovou službu protokol RDP 6.0.

Správa licencí služby Terminal Services

Správa licencí služby Terminal Services spravuje licence klientského přístupu CAL (Client Access Licences) v rámci domény nebo pracovní skupiny.

5.4.3 Možnosti přístupu přes Terminálovou službu

Vzdálená plocha

Program Vzdálená plocha (Remote Desktop) je standardně implementován ve všech operačních systémech společnosti Microsoft od operačního systému Microsoft Windows 2000. Lze ho najít v nabídce Programy operačního systému nebo ho lze spustit pomocí příkazu příkazového řádku *mstsc.exe*.

Remote Desktop Web Connection

Od verze operačního systému Microsoft Windows Server 2003 a Microsoft Windows XP SP2 lze pro vzdálené připojení na server použít i službu Vzdálená plocha přes webový prohlížeč (Remote Desktop Web Connection). Tato služba umožňuje otevření konzole v okně webového prohlížeče Microsoft Internet Explorer. Tato služba vyžaduje na straně klienta webový prohlížeč Microsoft Internet Explorer 5.5 a novější a instalaci ActiveX prvku msrdp.cab (umístění v serverovém operačním systému %systemroot%\Web\TSWeb\msdrp.cab).

Spuštění služby Remote Desktop Web Connection se provádí přes webovou adresu *http://jméno serveru/Tsweb*.

Obrázek 12, úvodní obrazovka Remote Desktop Web Connection

Ovládací prvek ActiveX vzdálené plochy zle vložit na webovou stránku vložením značky HTML <OBJECT>, jak je uvedeno v následujícím příkladu:

```
<OBJECT language="vbscript"
   ID="MsRdpClient">
   CLASSID="CLSID:9059f30f-4eb1-4bd2-9fdc-36f43a218f4a"
   CODEBASE="msrdp.cab#version=5,2,xxxx,0
   WIDTH=<% resWidth = Request.QueryString("rW")
      if resWidth < 200 or resWidth VIEWASTEXT > 1600 then
        resWidth = 800
      end if
      Response.Write resWidth %>
    HEIGHT=<% resHeight = Request.QueryString("rH")
      if resHeight < 200 or resHeight > 1200 then
        resHeight = 600
      end if
      Response.Write resHeight %>>
</OBJECT>
```

Řetězec xxxx vyjadřuje číslo sestavení ovládacího prvku. Vývojáři najdou tyto informace na webové stránce *default.htm* v oddílu CONNECT zdroje. Hodnota, na kterou je nastaveno klíčové slovo WIDTH, je šířka v pixelech relace Terminálové služby zobrazená na webové stránce. Hodnota, na kterou je nastaveno klíčové slovo HEIGHT, je výška v pixelech relace Terminálové služby. Hodnota, na kterou je nastaveno klíčové slovo CODEBASE, vyjadřuje umístění souboru obsahujícího kód webového připojení ke vzdálené ploše. Soubor má název msrdp.cab a je umístěn v adresáři, do kterého byl nainstalován ovládací prvek ActiveX vzdálené plochy a webové stránky vzorků. Klíčové slovo PARAMNAME je nastaveno na jeden nebo více parametrů podporovaných souborem msrdp.ocx [10].

Tato možnost vzdálené správy je velmi vhodná hlavně v operačních systémech, kde není standartně nainstalován terminál Vzdálené plochy, což jsou operační systémy Microsoft Windows NT a starší, nebo v operačních systémech, kde uživatel nemá oprávnění spouštět programy, ovšem musí mít oprávnění instalovat a používat ActiveX prvky a webový prohlížeč musí ActiveX prvky podporovat.

Pro instalaci této služby je potřeba mít nainstalovanou službu IIS (Internet Information Services), bez niž nelze TSWeb používat. V informacích o produktu není uvedeno, jestli je komunikace po síti nějakým způsobem zabezpečena a šifrována, nebo alespoň je nějakým způsobem zabezpečen přenos údajů ověřující identitu uživatele, ani to, jestli lze tuto službu provozovat přes zabezpečený protokol HTTPS.

6 PŘIPOJENÍ OPERAČNÍHO SYSTÉMU K SÍTI

6.1 Základní informace o připojení operačního systému k síti

Operační systém Microsoft Windows Server 2003 lze připojit k místní síťové struktuře, místní síti, nebo k veřejné síťové struktuře, síti internet. Po instalaci operačního systému je k dispozici služba RRAS (Routing and Remote Access), která je v neaktivní stavu. Základní nastavení operačního systému je totožné s ostatními operačními systémy společnosti Microsoft. Lze v něm nastavit síťové protokoly, TCP/IP, sdílení souborů a tiskáren a základní ochranu před nežádoucí síťovou komunikací pomocí standardní brány firewall.

Většina použití operačního systému vyžaduje individuální nastavení služby RRAS, která povyšuje operační systém do role správce síťové komunikace s internetem prostřednictvím služby NAT (Network Adress Translation), umožňuje vytvářet a nastavovat VPN (Virtual Private Network) spojení, což jsou zabezpečená a šifrovaná spojení pomocí protokolů IPSec (IP Security) a PPTP (Point to Point Tunneling Protokol), umožňuje nastavovat a spravovat lokální směrování DNS dotazů a zabraňuje nežádoucí síťové komunikaci prostřednictvím pokročilého rozhraní integrované brány firewall.

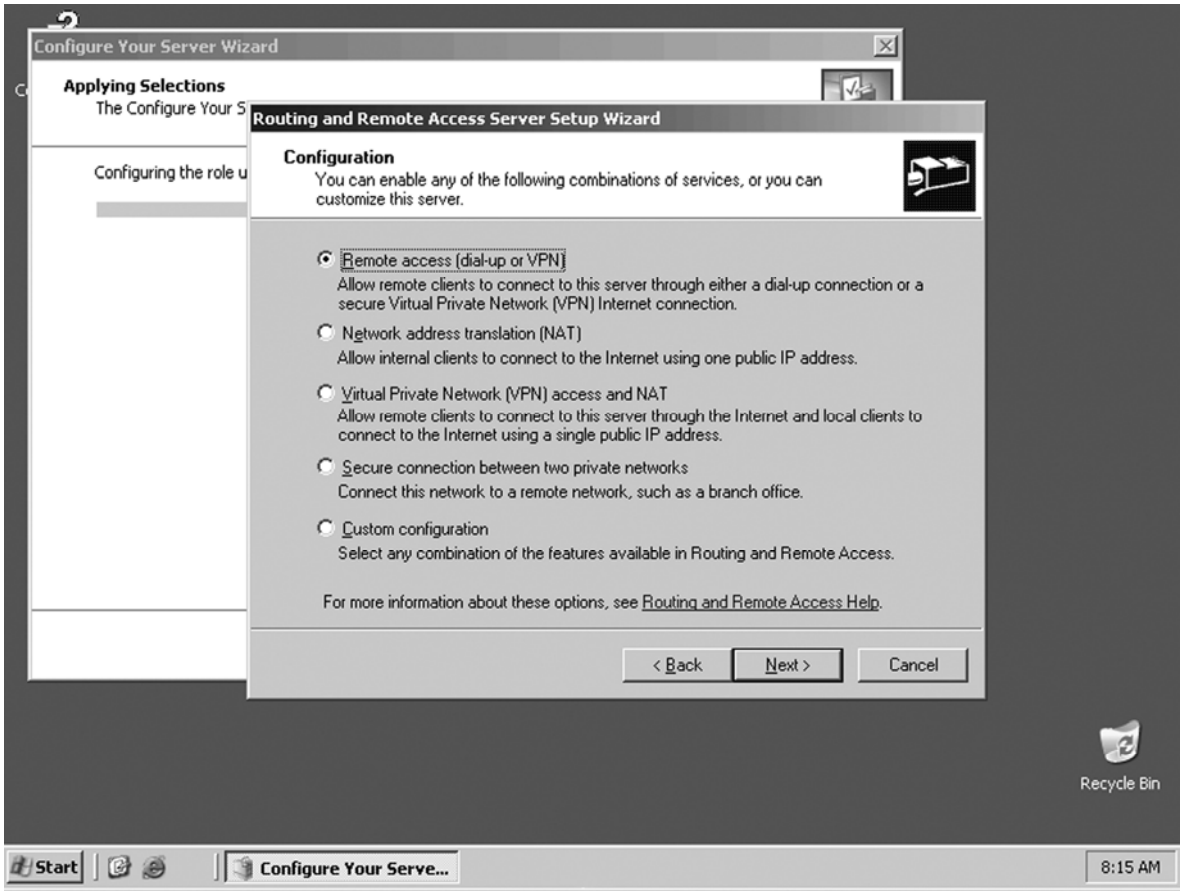
Pokud je vyžadována profesionální ochrana lokální počítačové sítě, společnost Microsoft nabízí doplňkový produkt ISA server, který přebírá většinu funkcí služby RRAS a umožňuje detailní a propracované nastavení včetně zálohování a zpětné kontroly veškeré síťové komunikace. Tento produkt je prodejný samostatně, vyžaduje dokoupení příslušných licencí k legálnímu používání a instaluje se jako doplňkový server pro operační systém Microsoft Windows Server 2003, není jej možno provozovat samostatně.

Pokud se používá server pro VPN spojení, WEB (IIS) a FTP server, musí být alespoň jeden síťový adaptér připojen přes poskytovatele připojení k veřejné síti Internet a musí být zajištěna na tomto síťovém adaptéru veřejná, v ideálním případě i pevná, IP adresa. Veřejná IP adresa znamená IP adresa přístupná z veřejné sítě internet nebo alespoň IP adresa, na kterou jsou přesměrovány porty jednotlivých služeb z veřejné IP adresy poskytovatele. Pevná IP adresa znamená IP adresa, jejíž hodnota není při připojení k poskytovateli přidělována dynamicky a nemění se. Tento požadavek lze obejít použitím služby DynDNS (Dynamic DNS), která umožňuje jednomu DNS záznamu ve veřejné síti internet přiřazovat podle požadavku různé hodnoty IP adres.

6.2 Spuštění služby Routing and Remote Access

Služba RRAS je po instalaci operačního systému neaktivní, tudíž je potřeba ji nakonfigurovat. Tato konfigurace je nejjednodušší v grafickém prostředí operačního systému. V nabídce Nástroje pro správu (Administrative Tools) se spustí nástroj Směrování a vzdálený přístup (Routing and Remote Access). Po spuštění nástroje je nutno v levé části okna označit server, na kterém se služba konfiguruje, a zvolit volbu Nakonfigurovat a povolit směrování a vzdálený přístup (Configure and Enable Routing and Remote Access).

V tomto bodu konfigurace je nutno se rozhodnout, jak službu RRAS nakonfigurovat. Je zde několik možností, které odlišným způsobem automaticky službu RRAS nakonfigurují. Je důležité upozornit, že služba RRAS umožňuje provoz všech těchto nastavení současně, ovšem automatický průvodce neumožňuje nastavení všech voleb současně a neumožňuje několikanásobnou konfiguraci stejné služby RRAS. Pokud bude potřeba v budoucnu službu RRAS překonfigurovat pomocí automatické konfigurace služby RRAS, administrátor bude nucen nejdříve stávající nastavení služby odebrat, a poté vytvořit nové nastavení. Proto je velmi výhodné vybrat v konfiguraci volbu, která nastaví nejvíce služeb, které budou používány v rámci služby RRAS, a další služby nakonfigurovat později ručně.



Obrázek 13, instalace služby Route and Remote Access

Nejčastěji se používá instalace Virtual Private Network (VPN) access and NAT, která umožňuje připojení serveru k síti internet a použití firewallu, připojení k místní síti, sdílení připojení k internetu a používání VPN. Pro instalaci této volby je nutné, aby na serveru byla alespoň 2 síťová rozhraní.

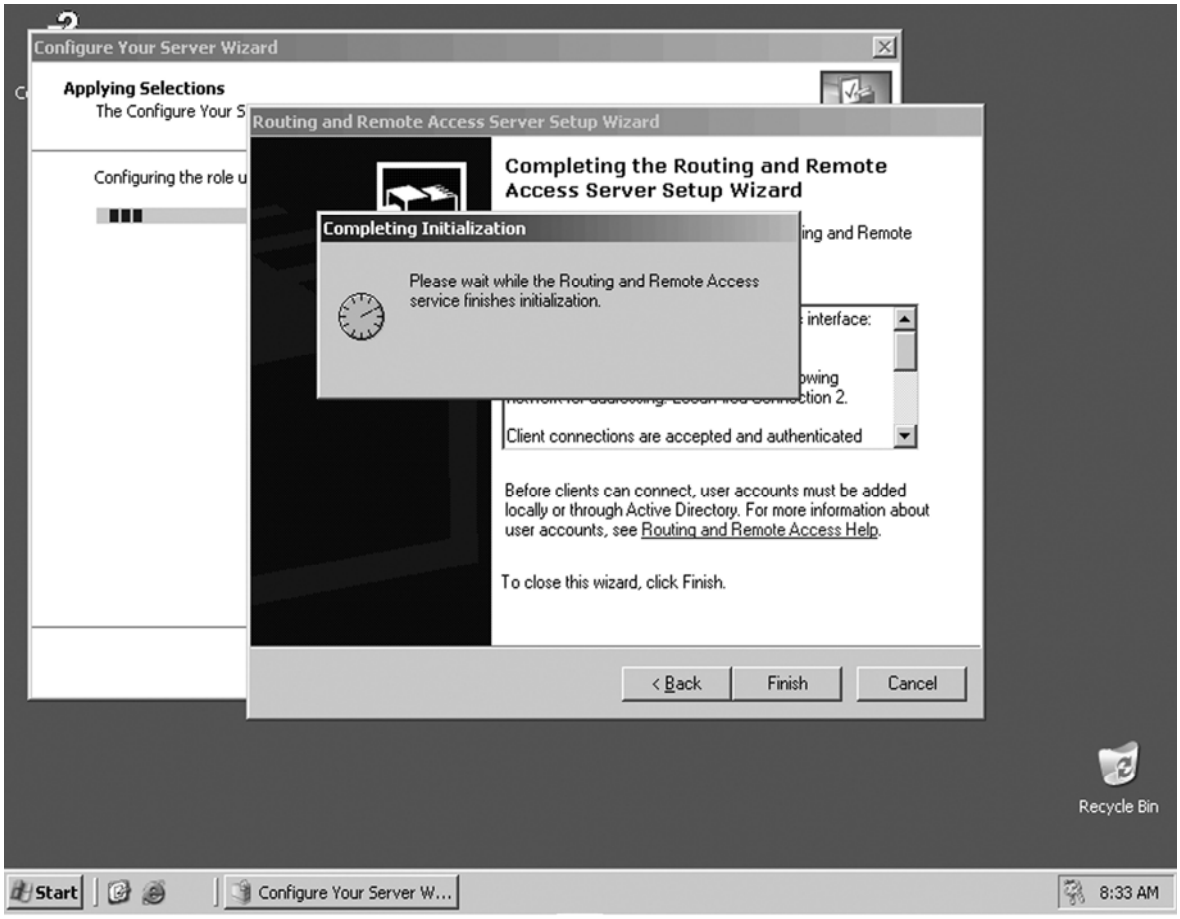
Instalace pokračuje v následujících krocích:

Volba síťového rozhraní, které je připojené k síti internet. Zároveň je možnost aktivovat firewall pro toto rozhraní.

Konfigurace nastavení TCP/IP protokolů vzdálených klientů. Je zde možnost automaticky přidělovat IP adresy z DHCP serveru nebo vybrat IP adresy z definovaného rozsahu.

Nastavení autentifikace vzdálených klientů pomocí Radius serveru.

Zobrazení nastavení služby, dokončení se instalace a spuštění služby.



Obrázek 14, dokončení instalace služby Route and Remote Access

Tímto je instalace služby Route and Remote Access dokončena. V nastavení jednotlivých uživatelů a skupin se doplní nabídka pro Dial in nastavení, kde se nastavují vlastnosti VPN připojení pro daného uživatele nebo skupinu [8].

6.3 Bezpečný přenos dat v internetu

Služba RRAS umožňuje po aktivaci používání služeb VPN (Virtual Private Network), v současné době nejbezpečnější služby pro přenos dat v síti internet. Služba VPN vytváří v síti internet zabezpečený virtuální tunel, kterým spojuje vzdálené klienty nebo jednotlivé servery a emuluje tak existenci místní sítě. Tím je umožněna zabezpečená komunikace klientských zařízení se servery a serverů navzájem pomocí veřejné sítě internet.

Operační systém Microsoft Windows Server 2003 používá 2 typy protokolů pro tvorbu VPN. Je to PPTP (Point to Point Tunelling Protocol), který se využívá pro spojení serverů, a IPsec (IP security), který se využívá pro připojení klientských stanic k serverům.

7 PROVOZ A ÚDRŽBA SYSTÉMU

7.1 Základní informace o provozu a údržbě operačního systému Microsoft Windows Server 2003

Sledování činnosti operačního systému a jeho průběžná údržba jsou jedny z nejdůležitějších věcí, které musí provádět každý administrátor pro bezproblémový provoz operačního systému. Neméně důležitá je funkce zálohování, která umožňuje v případě havárie systému obnovu dat. Operační systém Microsoft Windows Server 2003 je vybaven množstvím monitorovacích mechanizmů, umožňujících velice podrobně sledovat činnosti operačního systému. Tyto monitorovací mechanizmy fungují na pozadí ihned po instalaci systému, ale pro monitoring speciálních funkcí nebo požadavků je potřeba některé mechanizmy, které jsou deaktivovány kvůli snižování výkonu serveru, aktivovat.

7.2 Aktualizace operačního systému

Snad nejdůležitější činností administrátora operačního systému je pravidelná a včasná aktualizace operačního systému. Aktualizace opravuje kritické a důležité chyby v operačním systému, aktualizace hardwarových ovladačů, doplňuje ho o nové nástroje a programy pro správu a údržbu a vylepšuje již používané nástroje a programy.

Operační systém Microsoft Windows Server 2003 obsahuje nástroj pro automatickou aktualizaci, který umožňuje udržovat systém aktuální. Podle nastavení sám kontroluje a instaluje důležité aktualizace a upozorňuje na aktualizace volitelné. Pro pravidelnou aktualizaci zprovoznila společnost Microsoft webové stránky *http://update.microsoft.com*, kde je možné online vyhledat všechny dostupné aktualizace ke všem produktům společnosti Microsoft.

7.3 Změna defaultních nastavení práv a oprávnění

Mezi administrátory operačních systémů Microsoft Windows Server velmi často používaná a pro operační systém umístěný v DMZ (Demilitary Zone), neboli server

připojený k síti internet veřejnou IP adresou bez ochrany firewallem, odborníky doporučovaná je změna nastavení některých práv a oprávnění.

Je to hlavně zakázání nebo přejmenování účtu administrátora, který se stává nejčastěji testovaným účtem pro proniknutí do operačního systému. Tato skutečnost vyplívá z faktu, že každý operační systém od společnosti Microsoft má implicitně zabudovaný právě účet administrátora. Nejčastěji se toto snížení bezpečnosti řeší založením jiného účtu s právy skupiny administrators a domain admins a účet administrátora se zakáže nebo se účet administrátora přejmenuje na jiné uživatelské jméno.

Další doporučované nastavení je zavedení minimálního požadavku na délku a bezpečnost hesla s tím, že se aktivuje ochrana před testováním hesla metodou Brute Force, což je metoda postupného generování hesla. Touto aktivací se zabrání neomezenému testování uživatelského jména a hesla, protože po určitém počtu špatných zadání uživatelského jména nebo hesla se účet uzamkne, a již ho nelze používat do doby, než ho člen skupiny administrators znovu aktivuje. Toto nastavení je velmi výhodné, pokud je na serveru nainstalovaný VPN server. Aby nedocházelo k uzamykání účtů prostřednictvím testování uživatelských jmen a hesel pomocí VPN serveru, je dobré založil účet uživateli pro připojení přes VPN a jiný účet pro přihlášení k samotnému počítači. V případě zablokování VPN přístupu lze pak danému uživateli velmi jednoduše změnit uživatelské jméno pro přístup přes VPN připojení, aniž by bylo nutno přenastavovat jiné služby, jako např. email, oprávnění v doméně atd.

Další zvýšení zabezpečení spočívá ve znemožnění fyzické manipulace neoprávněných osob s hardwarem samotného serveru. Toto zabezpečení je důležité pro všechny servery nezávisle na operačních systémech. Samotné servery jsou vybaveny vstupními jednotkami, které je pro zvýšení bezpečnosti nutno odpojit úplně nebo přístup k jednotkám zabezpečit heslem na úrovni operačního systému nebo BIOSu (Basic Input Output System) základové desky. Tímto způsobem lze velmi jednoduše ochránit operační systém před napadením viry a nežádoucími programy a před nabootováním systémů z přenosných médií, které jsou určeny pro odhalení, změnu nebo reset hesla ověřující identitu uživatele. Servery samotné bývají většinou uzavřeny v klimatizovaných a uzamčených raccích připojeny na záložní zdroje z důvodu nechtěným výpadkům proudu.

7.4 Záznamy událostí (Event logy)

Základním a výchozím mechanizmem podávání zpráv o činnosti operačního systému je generování základních typů událostí do souborů, které se označují Event logy. Po instalaci operačního systému existují 3 základní Event logy.

System log (Systém), log operačního systému, obsahuje záznam událostí týkajících se samostatného systému a běžících služeb (Services).

Application log (Aplikace), log událostí a činností nainstalovaných aplikací.

Security log (Zabezpečení), bezpečnostní log, jsou v něm popsány výsledky auditu a zaznamenává bezpečnostní události systému.

Podle instalace a provozu dalších služeb můžou být Event logy rozšířeny o další záznamy.

DNS log, log DNS serveru.

Directory Service (Adresářová služba), log služby Active Directory.

File Replication Service (Služba replikace souborů), log služby Active Directory.

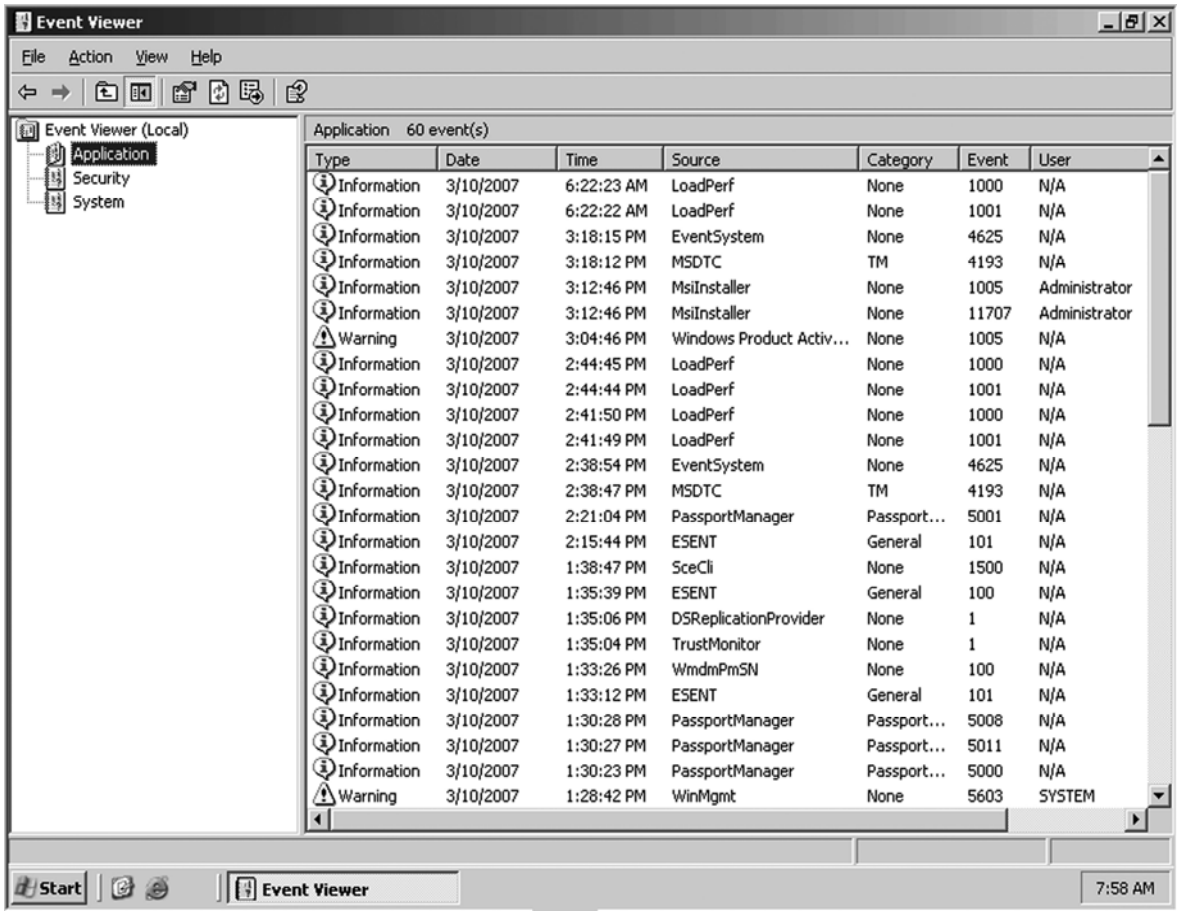
Monad log, log příkazového prostředí procesoru při používání Power Shell.

7.4.1 Event Viewer

Základním programem pro prohlížení zaznamenaných událostí je Event Viewer (Prohlížeč událostí), který se nachází v Nástrojích pro správu (Administrative Tools). Každý záznam uložený do Event logu obsahuje typ záznamu, datum a čas události, zdroj, kategorii a hlavně číslo záznamu (Event ID). Podle tohoto čísla záznamu lze na webových stránkách společnosti Microsoft (Microsoft Knowledge Database) nebo i na jiných specializovaných webových stránkách najít podrobnější vysvětlení dané události a v případě potřeby i doporučené řešení dané události. Lze tak velmi rychle a profesionálně

vyřešit i závažné chyby operačního systému. Program Event Viewer umožňuje i filtrované vyhledávaní uložených záznamů a export daných záznamů.

Administrátoři serverů velmi odcení službu Event logů nejen pro běžnou kontrolu stavu operačního systému, ale hlavně při nečekaných pádech a jiných nežádoucích reakcích. Trochu nešikovné je v některých případech vysvětlení dané události, ovšem podrobnější popis lze najít přímo na internetu. Některé webové stránky dokonce v některých případech poskytují lepší feedback (zpětnou podporu), než samotné webové stránky společnosti Microsoft, hlavně z důvodu veřejných fór, kde si administrátoři navzájem sdělují příčiny a řešení těchto událostí. Mnoho z těchto stránek poskytuje velmi účinná řešení, ovšem až v placených sekcích webových stránek.



Obrázek 15, MMC konzole Event Vieweru (Prohlížeč událostí)

7.4.2 Eventquery

Nástroj Eventquery je skript pro prostředí WSH, který se nachází v adresáři %systemroot%*/System32/* v souboru Eventquery.vbs. Je to nástroj určený pro základní získávání výpisu obsahu logů do příkazové řádky [7].

7.4.3 Log Parser

Nástroj Log Parser není implicitně součástí operačního systému, lze jej však zdarma stáhnout z webových stránek společnosti Microsoft. Výhodou používání nástroje Log Parser je použití odvozeného jazyka SQL, což je velmi výhodné při třídění a vyhledávání záznamů [7].

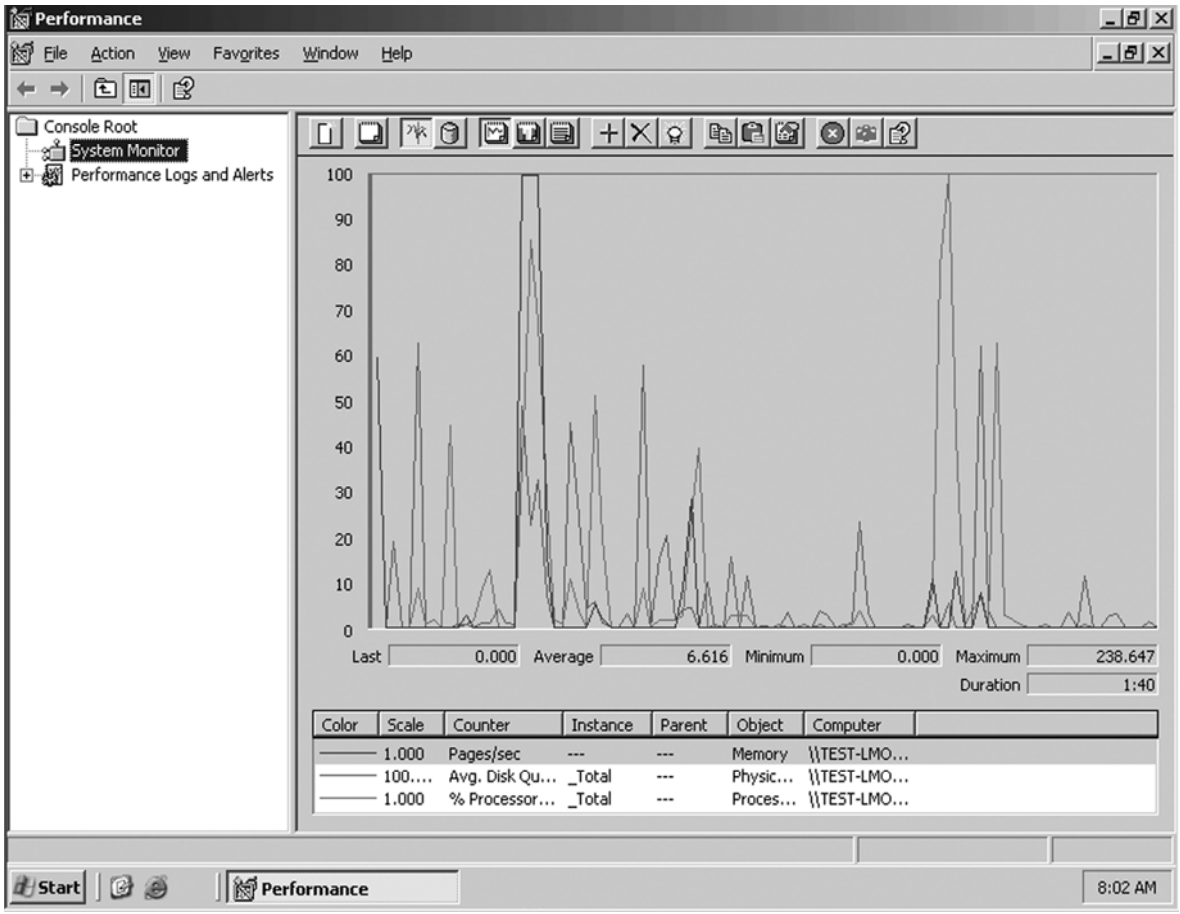
7.4.4 PSLogList

Program PSLogList, Sysinternals corporation, umožňuje zachytávat a sledovat události, jenž nově přibyli v logovacích souborech. Program vypisuje nové záznamy do příkazového řádku. Lze tak velmi pohodlně a jednoduše sledovat činnost systému [7].

7.5 Čítače výkonu (Performance Counters)

Operační systém Microsoft Windows Server 2003 je vybaven nástroji pro sledování částí operačního systému, které měří a dokumentují aktuální stav systému. Jejich činnost je v základním nastavení omezena, protože sledování systému pomocí těchto nástrojů spotřebovává systémové prostředky, tím způsobuje nežádoucí zátěž operačního systému. Používáním těchto čítačů výkonu umožňuje odhalit nedostatečnou výkonnost hardwaru, na kterém je operační systém provozován, poškození části hardwaru nebo neúměrné zatížení části hardwaru a částí operačního systému, a tím reagovat na vzniklé problémy a předejít pádu operačního systému a ztrátě dat.

Množství čítačů, které lze použít, se dovíjí od nainstalovaných součástí a doplňků v operačním systému.



Obrázek 16, MMC konzole Performance Counters (Čítač výkonu)

7.6 Zálohování systému a dat

Zálohování operačního systému a dat v něm uložených je další důležitou součástí údržby. Operační systém sám o sobě obsahuje základní zálohovací nástroj Ntbackup, který je možno použít v podobě grafického rozhraní i v příkazovém řádku pomocí příkazu *ntbackup.exe*. Program Ntbackup umožňuje zálohu nebo obnovu celého operačního systému, jeho částí nebo jen stavu operačního systému (System State). Obnova systému se pak musí provádět v Nouzovém režimu (Safe Mode), zatím co obnova dat se může provádět při normálním běhu systému.

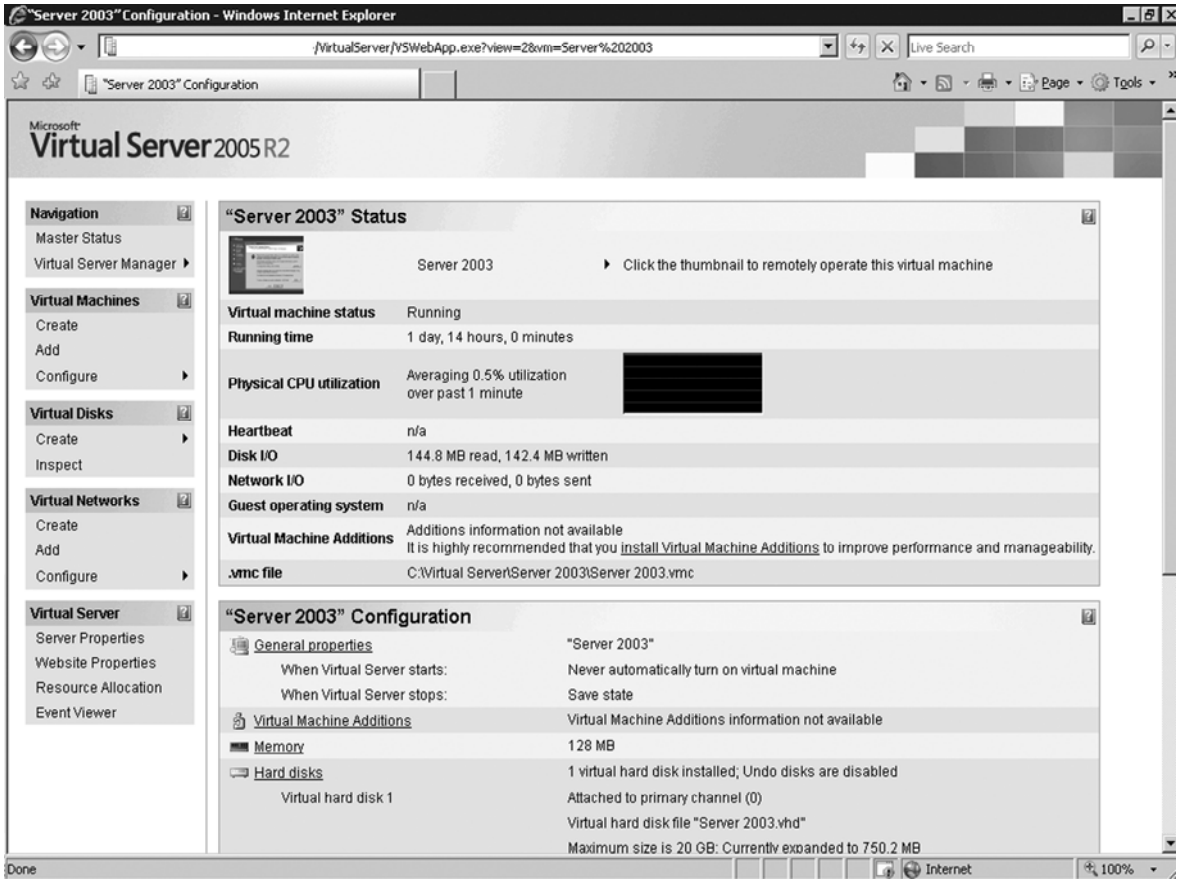
Program Ntbackup simuluje zálohování na externí páskové jednotky do souboru s příponou BKF. Je tedy možné uložit do jednoho souboru více záloh a obnovit jakoukoliv zálohu ze souboru. Program Ntbackup umožňuje jak celkové, tak rozdílové zálohování, čímž umožňuje zrychlovat provádění zálohy a zmenšovat velikost zálohového souboru. Program Ntbackup může fungovat jako služba, tudíž pro zálohování není nutné přihlášení uživatele v operačním systému [7].

Pro zálohování souborů a složek musí mít program, popřípadě administrátor, dostatečná přístupová práva ke složkám a souborům. V základním nastavením je zálohování umožněno uživatelským účtům, které jsou členy skupiny Backup Operators a Administrators, a uživateli, který je vlastníkem zálohovaných složek a souborů nebo musí mít oprávnění typu Číst, Číst a spouštět, Měnit nebo Úplné řízení. Možnost zálohování u uživatele může být omezena velikostí diskové kvóty.

Při obnovení systémového disku je nutno, aby operační systém nabootoval ze spouštěcí diskety, kterou program Ntbackup umí vytvořit. V tomto případě je velmi vhodné vytvořenou disketu vypálit jako bootovací CD, čímž se zabrání poškození dat na disketě a její nefunkčnosti v případě potřeby obnovy systémového disku.

7.7 Microsoft Virtual Server 2005 R2

Microsoft Virtual Server 2005 R2 je freewarový program společnosti Microsoft, umožňující provoz několika různých virtuálních operačních systémů v operačním systému na fyzickém hardwaru. Myšlenka provozu virtuálního operačního systému v jiném operačním systému může administrátorovi usnadnit správu, zabezpečení a zálohování virtuálního operačního systému. V případě poškození hardwaru lze virtuální stanici rychle přemístit do jiného operačního systému bez nutnosti reinstalace virtuálního operačního systému včetně všech programů, které jsou v tomto operačním systému používány, a dat umístěných na virtuálním serveru.



Obrázek 17, webová administrace Virtual Serveru 2005 R2

Virtual Server 2005 R2 umožňuje pomocí webového rozhranní detailní přehled všech činností virtuálních operačních systémů, nastavení hardwarů a síťových služeb virtuálních operačních systémů. Lze tak vytvořit libovolné síťové subsystémy na jednom fyzickém hardwaru, mezi nimiž lze nastavovat komunikační pravidla.

Koncepce virtuálních serverů společnosti Microsoft spěje k úplné virtualizaci všech operačních systémů na fyzickém hardwaru. Podle zveřejněných prezentací společnosti Microsoft by už první operační systém instalovaný na fyzický hardware měl být virtualizovaný a poskytovat dalším operačním systémům virtuální prostor.

ZÁVĚR

Tato bakalářská práce si klade za cíl jednoduchým a pochopitelným způsobem vysvětlit a popsat instalaci a vybrané základní služby serverového operačního systému Microsoft Windows Server 2003 R2. Jelikož i úplný popis těchto vybraných základních služeb by byl velmi obsáhlý a zasloužil by si hlubší vysvětlení, v této práci jsem se snažil pouze o základní teoretický popis a o základní popsání instalace a nastavení těchto služeb podle nejpoužívanějších a nejběžnějších modelů. Jednotlivé kapitoly byly navrhnuty a napsány tak, aby se s problematikou mohl seznámit i začátečník.

Tato práce by si zasloužila důkladnější popis jednotlivých kapitol, což může být námětem diplomové práce.

ZÁVĚR V ANGLIČTINĚ

This bachelor work´s aim is to explain and describe installation and selected basic services of servers OS Microsoft Windows Server 2OO3 R2, in simply and clear way. Although the entire description of these selected basic services would be very extensive and would be worth to make broader explenation, in these work I tried to feature just on basic theoretic description of services and installation and description of setting of those services according to most widely used and most common models. Several chapters were designed and written so, that could be easily understood even though beginners.

This work is worth to elaborate fully description of particular chapters, what can be subject of dissertation.

SEZNAM POUŽITÉ LITERATURY

[1] Deitel, H. M.: Operating Systéme, Prentice Hall, 2004

[2] Klimeš, C.:Operační systémy 1. Ostravská univerzita v Ostravě, Katedra informatiky a počítačů.

[3] Kokoreva, O.: Registr Microsoft Windows XP, Computer Press 2002

[4] Salomon, D. A.: Windows NT pro administrátory a vývojáře, Computer Press 1999

[5] Tanenbaum, A. S.: Modern operating systéme, Prentice Hall, 2002

[6] Resource Kit Microfost Windows XP

[7] RUSSEL, Charlie, CRAWFORD, Sharon, GEREND, Jason. Microsoft Windows Server 2003 : Velký průvodce administrátora. Brno : C.P. Books, a.s., 2005. 1374 s. ISBN 80-251-0579-2

[8] MALINA, Patrik. Microsoft Windows Server 2003: Hotová řešení. Brno: Computer Press, a.s., 2006. 358 s. ISBN 80-251-1096-6

[9] ŠVESTKA, Petr. Microsoft Exchange Server 2003: Hotová řešení. Brno: Computer Press, a.s., 2006. 322 s. ISBN 80-251-1165-2

[10] Stránky společnosti Microsoft [online]. 2007 [cit. 2007-03-20]. Dostupný z WWW: http://www.microsoft.com

[11] Stránky společnosti Microsoft Technet Česká republika [online]. 2007 [cit. 2007-03-20]. Dostupný z WWW: http://www.technet.cz

[12] Stránky Petri IT Knowledgebase [online]. 2007 [cit. 2007-04-20]. Dostupný z WWW: http://www.petri.co.it

[13] Stránky Oxid IT [online]. 2007 [cit. 2007-04-20]. Dostupný z WWW: http://www.oxid.it

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: HESLA PRO OVĚŘENÍ IDENTITY A SLUŽBA ACTIVE DIRECTORY

Přihlašování uživatele a ověření hesla na lokálním počítači nebo serveru, nepřipojeném do domény, probíhá prostřednictvím služby SAM (Security Authentification Manager), neboli Správce zabezpečení účtů, což je databáze, ve které jsou uloženy uživatelské účty a popisovače zabezpečení pro uživatele.

Přihlašování uživatele a ověřování hesla v doméně probíhá primárně pomocí protokolu Kerberos. Nejnovější typ protokolu je Kerberos V5. Kerberos V5 ověřuje identitu uživatele požadujícího ověření i identitu serveru provádějícího požadované ověření. Toto duální ověřování je označováno také jako vzájemné ověření [10].

Princip ověřování prostřednictvím protokolu Kerberos V5

Při použití mechanismu ověřování prostřednictvím protokolu Kerberos V5 jsou vydány lístky pro přístup ke službám v síti. Tyto lístky obsahují zašifrovaná data, včetně zašifrovaného hesla, která požadované službě potvrdí identitu uživatele. S výjimkou zadání hesla nebo pověření karty Smart Card nemůže celý proces ověřování identity uživatel rozpoznat.

Důležitou službou v rámci protokolu Kerberos V5 je služba KDC (Key Distribution Center). Služba KDC je spuštěna v každém řadiči domény jako součást adresářové služby Active Directory, která zajišťuje uložení všech hesel klienta a dalších informací o účtu.

Proces ověřování prostřednictvím protokolu Kerberos V5 probíhá následujícím způsobem:

Uživatel v systému klienta pomocí hesla nebo karty Smart Card prokáže svou identitu službě KDC.
Služba KDC vydá klientovi zvláštní lístek TGT (Ticket-Granting Ticket). Systém klienta pomocí tohoto lístku TGT získá přístup ke službě TGS (Ticket-Granting Service), která je součástí mechanismu ověřování pomocí protokolu Kerberos V5 v řadiči domény.

Služba TGS poté vydá klientovi tzv. lístek služby.
Klient se prokáže tímto lístkem požadované službě v síti. Lístek služby slouží nejen k prokázání identity uživatele pro službu, ale i k prokázání identity služby pro uživatele.

Služby Kerberos V5 jsou nainstalovány v každém řadiči domény a klient služby Kerberos je nainstalován v každé pracovní stanici a na každém serveru. Každý řadič domény funguje jako služba KDC. Klient vyhledá pomocí vyhledávání služby DNS (Domain Name Service) nejbližší dostupný řadič domény. Nalezený řadič domény poté tomuto uživateli slouží v průběhu relace přihlášení uživatele jako upřednostňovaná služba KDC. Pokud se upřednostňovaná služba KDC stane nedostupnou, vyhledá systém pro ověřování jinou službu KDC [11].

Povolení ověřování prostřednictvím protokolu Kerberos V5

Protokol pro ověřování Kerberos V5 je ve výchozím nastavení povolen u všech počítačů připojených během instalace k doméně systému Windows Server 2003 nebo Windows 2000. Protokol Kerberos umožňuje získat přístup k prostředkům v rámci domény a k prostředkům umístěným v důvěryhodných doménách na základě jediného přihlášení.

Určité prvky konfigurace protokolu Kerberos lze řídit prostřednictvím nastavení zabezpečení pomocí protokolu Kerberos, které je součástí zásad účtů. Lze například nastavit dobu platnosti uživatelských lístků protokolu Kerberos V5. Správci mohou použít výchozí zásady modulu Kerberos nebo je mohou přizpůsobit potřebám daného prostředí.

Pokud má být ověřování prostřednictvím protokolu Kerberos V5 úspěšné, musí být na počítači klienta i na serveru spuštěn operační systém Windows 2000, systém řady Windows Server 2003 nebo Windows XP Professional. Pokud se klient s určitým systémem pokusí ověřit svou identitu na serveru s jinou verzí operačního systému Windows, bude při procesu ověřování použit protokol NTLM.

V počítačích používajících při ověřování protokol Kerberos musí být nastavení času synchronizováno do pěti minut s běžným systémovým časem, jinak se ověření nezdaří. V počítačích se systémy řady Windows Server 2003, Windows XP Professional nebo systémem Windows 2000 je aktuální čas aktualizován automaticky, přičemž jako časová služba v síti je použit řadič domény .

Obnovení a testování bezpečnosti hesla pro ověření identity operačních systémů Microsoft

Nejjednodušší způsob prolomení hesla operačních systémů Microsoft, mimo napadení viry a jinými nežádoucími programy, je použití jiného systému pro nalezení a zobrazení, smazání nebo změnění hesla. Tato metoda ovšem vyžaduje fyzický přístup k hardwaru serveru. Používá se většinou při ztrátě administrátorských hesel nebo při potřebě prolomení ochrany operačních systémů. Využívá faktu, že přístup k souborům jiného operačního systému uloženým na disku nebo oddílu z jiného systému je velmi jednoduchý a méně zabezpečený. Samotná hesla uživatelů jsou uložena přímo v registrech a defaultní nastavení operačních systémů společnosti Microsoft, včetně serverových operačních systémů, umožňuje heslo menší, než 15 znaků, ukládat starším typem šifrování, které je dnes prolomeno.

Společnost Microsoft sama poskytuje v Ressource Kits nástroje SRVANY a INSTSRV pro reset administrátorského hesla ve Domain Controlleru. Na této adrese je podrobný návod pro použití těchto utilit [12]:
http://www.petri.co.il/reset_domain_admin_password_in_windows_server_2003_ad.htm.

Zde je několik freewarových programů. Většina z nich jsou Linuxové distribuce schopné pracovat s registry operačních systémů Microsoft. Existují i placené programy.

Offline NT Password Registry & Editor, *http://home.eunet.no/pnordahl/ntpasswd/*.
John the Ripper, *http://www.openwall.com/john*.
EBCD – Emergency Boot CD, *http://ebcd.pcministry.com*.

Další možností prolomení hesla je pomocí programů monitorujících síťovou komunikaci. Jsou to programy, které zachytávají jednotlivé síťové rámce, ze kterých lze odfiltrovat hesla různých služeb a protokolů. Nejjednodušší způsob odchytávání hesel je použití těchto programů na Gateway (Výchozí brána), neboli na uzlu propojující místní síťovou strukturu s další sítí, například síť internet. Existují i programy, které lze použít pro monitorování provozu v síti na samotných stanicích, ovšem musí k tomu být uzpůsobena struktura sítě (použití hubů). Tyto programy jsou většinou Linuxové distribuce.

Při těchto způsobech zachytávání a prolomení hesla je největším problémem samotné zachycení síťové komunikace. Moderní struktura sítí založená na používání

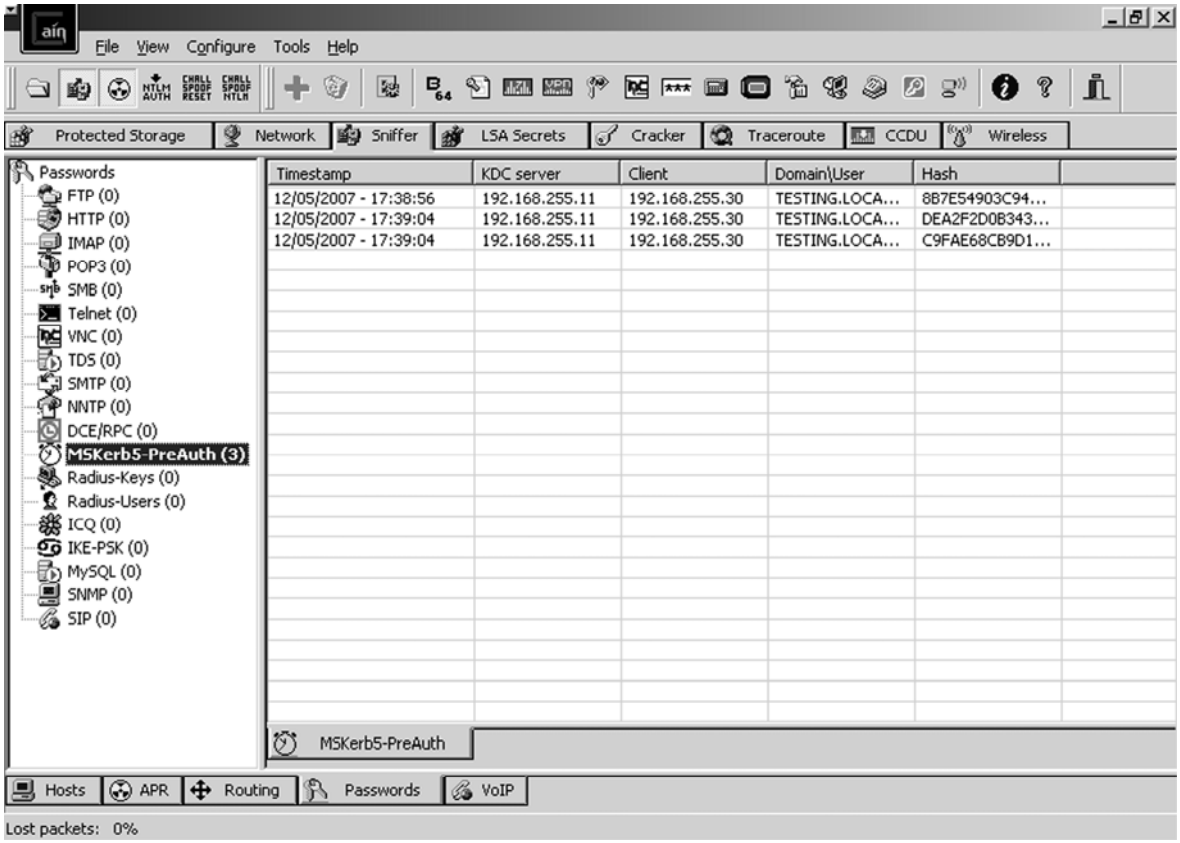
switchů, jako síťových uzlů, které nezávisle propojují komunikaci jednotlivých portů, znemožňuje odposlouchávání síťové komunikace. Některé switche pracující na 3. vrstvě, síťové vrstvě, síťového modelu, jsou vybaveny funkcemi pro přesměrování nebo zrcadlení (mirroring) síťové komunikace.

Pro serverové operační systémy společnost Microsoft vytvořila monitorovací program Network Monitor, aktuální verze 3.0, který je volně stažitelný z webových stránek společnosti Microsoft jako doplněk Administrative Tools serveru. Tento program monitoruje reálný provoz na síťových adaptérech serveru a umožňuje jejich třídění a zpracování. Je jim například možno zachytit pakety obsahující nezabezpečené heslo protokolu FTP. Problém nastává v případě použití šifrování pro přenos hesla po síti, jelikož tento program je pouze monitorovací.

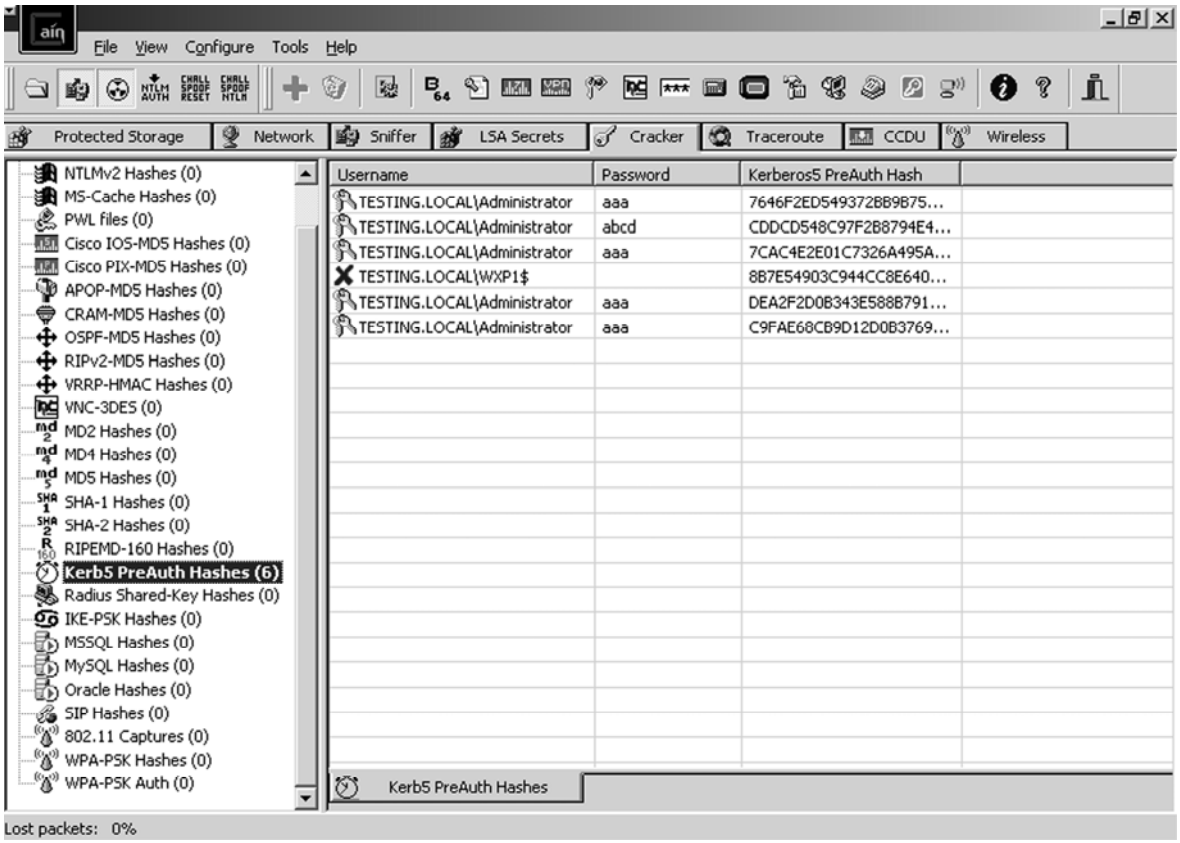
Pro tento případ existují monitorovací programy schopné některé způsoby šifrování hesla prolomit. Mohou používat metodu znalosti samotného šifrovacího algoritmu, metodu Brute Force, opakovatelného testování hesla, nebo metodu Rainbow Attack, což je porovnávání samotného HASH hesla, neboli zašifrované podoby hesla, kdy lze na internetu najít seznamy hashových hesel roztříděných podle alfanumerických a speciálních znaků a podle délky hesla.

Po doporučení jsem pro test zachycení hesla při ověřování uživatele v doméně pomocí protokolu Kerberos V5 použil freewarový program Cain & Abel v4.9.1 pro Windows NT/2000/XP instalovaný na uzel sítě, neboli na server. Tento program je volně stažitelný z webových stránek *http://www.oxid.it* a umožňuje přímo selektivní zachytávání jednotlivých protokolů včetně jejich případného dešifrování pro protokoly HTTP, FTP, POP3, SMTP, Kerberos, Radius Server, WPA-SDK, ICQ atd.

Program sám umí zachytit a roztřídit jednotlivé pakety síťové komunikace podle typu síťové komunikace a zobrazit heslo v zašifrované podobě, pokud je šifrováno. Následně lze použít metodu Brute Force nebo Rainbow Attack pro dešifrování hesla. Při testu jsem se snažil zachytit protokoly typu Kerberos V5. Zachycení protokolů při přihlášení uživatele do domény bylo 100 % úspěšné. Následně jsem se snažil zašifrovanou podobu hesla dešifrovat metodou Brute Force. Dešifrování hesla touto metodou je velmi závislé na vstupních parametrech nastavení, na délce samotného hesla a na výkonu hardwaru.



Příloha PI, obrázek č. 1, zachycení paketů protokolů Kerberos V5 programem



Příloha PI, obrázek č. 2, dešifrování hesla programem

Z testu vyplynulo, že dešifrování hesla touto metodou je velmi závislé na délce samotného hesla a použití velkých písmen, číslic a speciálních znaků, neboli je závislé na stupni bezpečnosti hesla. Vzhledem k času, který je potřebný pro dešifrování hesla s větším počtem znaků, jsem nebyl schopný touto metodou vyzkoušet dešifrovat heslo větší, než 15 znaků, a tím vyzkoušet bezpečnost nové metody šifrování hesla protokolu Kerberos V5.

Následně jsem zkoušel zachytit a dešifrovat heslo při připojení stanice k serveru prostřednictvím VPN serveru. Během testování tento program nezachytil žádné heslo, z čehož lze usuzovat, že pro VPN připojení se používá jiný, bezpečnější způsob ověření identity uživatele, než protokol Kerberos V5. Komunikace při navazování spojení přes VPN byla na straně serveru potvrzena programem Network Monitor , který zachytil protokol PPTP.

Nakonec jsem vyzkoušel zachytit a dešifrovat heslo při přihlášení stanice, umístěné v doméně, k terminál serveru, umístěném na serveru v síti. Opět během testování program nezachytil žádné heslo, takže i služba Terminal server používá jiný způsob ověření identity uživatele.

Použitý hardware:

základní deska MSI K6T, čipová sada VIA T600

procesor AMD Athlon XP 2600+

paměť RAM 512 MB

disk Western Digital 150 GB, SATA, 16 MB cache, 7200 otáček/minutu

operační systém Microsoft Windows Server 2003 R2 EN

Nastavení programu pro dešifrování hesel:

možnost přítomnosti velkých i malých písmen

možnost přítomnosti čísel a speciálních znaků

možnost přítomnosti velkých písmen jak na začátku hesla, tak i na místě dalších písmen

možnost počtu znaků 1 až 16

Výsledky dešifrování hesla při průměrné rychlosti testování 80.000 hesel / sekundu:

znění hesla: aaa	čas: 1 sekunda
znění hesla: abcd	čas: 10 sekund
znění hesla: Abcd	čas: 5 minut
znění hesla: abcddcba	čas: 20 hodin
znění hesla: KristynkaVlastik82Kristynka	předpokládaný maximální čas: $3*10^{12}$ let