

Jihočeská univerzita
Pedagogická fakulta Katedra informatiky



**Univerzální administrátor
firemních počítačových serverů**

diplomová práce

vedoucí diplomové práce
PaedDr. Petr Pexa

Tomáš Studený

České Budějovice
2004

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, a že jsem uvedl veškeré použité zdroje.

Obsah

<u>1</u>	<u>ÚVOD</u>	<u>5</u>
<u>2</u>	<u>OPERAČNÍ SYSTÉM WINDOWS 2000 SERVER</u>	<u>6</u>
2.1	INSTALACE WINDOWS 2000 SERVER	6
2.2	KONFIGURACE A SPRÁVA WINDOWS	7
2.3	ACTIVE DIRECTORY A SYSTÉM DNS	11
2.3.1	INSTALACE POTŘEBNÝCH SOUČÁSTÍ SYSTÉMU	11
2.3.2	INSTALACE DOMÉNOVÉHO ŘADIČE	11
2.4	UŽIVATELÉ A POČÍTAČE ACTIVE DIRECTORY	14
2.5	KONFIGURACE SÍTĚ NA PRACOVNÍCH STANICÍCH	16
<u>3</u>	<u>OPERAČNÍ SYSTÉM SUSE LINUX</u>	<u>18</u>
3.1	INSTALACE SUSE	18
3.2	KONFIGURACE A SPRÁVA SUSE - YAST2	20
3.3	KONFIGURACE SÍTĚ	23
3.4	NIS (NETWORK INFORMATION SERVICE)	27
3.5	NFS (DISTRIBUOVANÉ SOUBOROVÉ SYSTÉMY)	29
3.6	SPRÁVA UŽIVATELSKÝCH ÚČTŮ	31
<u>4</u>	<u>WWW SERVER – APACHE</u>	<u>36</u>
4.1	INSTALACE V OPERAČNÍM SYSTÉMU UNIX	36
4.1.1	BINÁRNÍ INSTALACE	36
4.1.2	INSTALACE ZE ZDROJOVÝCH KÓDŮ	37
4.1.3	SPUŠTĚNÍ A ZASTAVENÍ APACHE V PROSTŘEDÍ UNIX	39
4.2	BINÁRNÍ INSTALACE V MICROSOFT WINDOWS	39
4.2.1	INSTALACE	40
4.2.2	SPUŠTĚNÍ A ZASTAVENÍ APACHE V PROSTŘEDÍ MICROSOFT WINDOWS	42

4.3	KONFIGURACE APACHE	43
5	<u>MAIL SERVER - KERIO MAILSERVER</u>	50
5.1	INSTALACE MICROSOFT WINDOWS	50
5.2	PRŮVODCE POČÁTEČNÍ KONFIGURACÍ	52
5.3	ADMINISTRAČNÍ PROGRAM	54
5.4	ZÁKLADNÍ NASTAVENÍ	56
5.5	NÁSTROJE	61
5.6	UŽIVATELSKÉ ÚČTY A SKUPINY	61
5.7	ODESÍLÁNÍ A PŘÍJEM POŠTY	64
6	<u>MAILSERVER – POSTFIX</u>	73
6.1	PŘÍPRAVY PŘED INSTALACÍ	73
6.2	INSTALACE POSTFIXU	74
6.2.1	INSTALACE POMOCÍ YAST2	74
6.2.2	BINÁRNÍ INSTALACE	74
6.3	KONFIGURACE POSTFIXU	76
	<u>LITERATURA A OSTATNÍ POUŽITÉ ZDROJE</u>	84



1 Úvod

Cílem diplomové práce je vytvořit uživatelskou příručku pro správce, resp. administrátory firemních serverů na bázi OS Windows 2000 (NT), Unix (Linux), tedy jakýsi kompletní návod, jak nakonfigurovat a spravovat menší počítačovou síť.

Publikace je určena zkušeným uživatelům jedno ze dvou operačních systémů (Windows, Linux). Nutná je alespoň minimální znalost problematiky počítačových sítí a komunikačních protokolů TCP/IP. Znalost internetu, problematika funkčnosti webového a mail serveru.

Jako první varianta operačního systému pro počítačovou síť je použit nejrozšířenější Windows 2000 resp. Windows 2000 Server. Jako webový server Apache místo služby IIS (Internet Information Services), která je vlastní systému Windows z důvodu jeho oblíbenosti a rozšíření a internetu. Mail server Kerio je plnohodnotná alternativa k MS Exchange pro menší počítačové síť. Kerio není tak robustní a nabízí plnou integraci s adresářovou službou Active Directory.

Druhá varianta operačního systému pro počítačovou síť je použit SuSE linux, který je jedním ze světově nejrozšířenějších poskytovatelů linuxového softwaru a služeb. Použití webového serveru Apache je opět jedno z nejlepších řešení. Mail server Postfix je alternativa k nejrozšířenějšímu Sendmailu. V distribuci SuSE je integrován jako implicitní mail server.

Nutno podotknout, že softwarové vybavení počítačová síť na bázi OS Linux SuSE ze zcela zdarma na rozdíl od OS Windows.



2 Operační systém Windows 2000 Server

Vytvořením operačního systému Windows® 2000 Server se společností Microsoft podařilo uskutečnit cíl, kterého bývá v oblasti softwarového průmyslu dosaženo jen zřídka - nabídnout produkt, který znamená evoluci i revoluci zároveň. Evoluci proto, že systém Windows 2000 vychází ze silných stránek operačního systému Windows NT® Server 4.0. Revoluční význam systému Windows 2000 spočívá ve stanovení nového standardu integrace operačního systému se sítí WWW, aplikacemi a službami pro práci v síti, komunikaci a infrastrukturu.



2.1 Instalace Windows 2000 Server

Přepokládám, že na počítači není žádný jiný operační systém a disk se během instalace bude formátován (ztráta veškerých dat na disku).

1. Zapněte počítač a vložte první CD do mechaniky.
2. Windows Vám dá na výběr ze tří možností. Zvolte možnost *Nainstalovat systém Windows 2000, pak stiskněte Enter.*
3. Zformátujte disk na systém souborů NTFS volbou *Zformátovat disk jako NTFS systém souborů.* Následně proběhne formátování a kontrola disků. Jeli vše v pořádku můžete pokračovat restartováním počítače.
4. Po znova načtení systému Vás již vítá grafické prostředí Průvodce instalací. Tlačítkem *Další* Instalační program začne rozpoznávat hardware a instalovat ovladače. Nastavíme *Národní prostředí a rozložení klávesnice.*



5. Vložit *Aktivační klíč*.
6. Nastavení hesla Administrátora.
7. Další okno Vás vyzve, abyste určili, které součásti se mají nainstalovat a které ne. Vzhledem k tomu, že na serveru budeme používat Active Directory, zaškrtneme položku *Síťové služby* a tlačítkem *podrobnosti...* dostaneme okno *Síťové služby* kde zaškrtneme položky *Domain Name System*, *Active Directory* a *Dynamic Host Configuration protocol (DHCP)*. Každá z těchto položek se dá doinstalovat i později.
8. Nastavení data a času
9. Panel *Síťová nastavení*. Otevřete dialogové okno s varováním: ***Zvolili jste i nadále používat dynamicky přidělenou adresu IP. Pro spolehlivější operace DNS byste měli používat pouze statické adresy IP.*** Instalátor Vám nabídne možnost statickou adresu vložit v dialogovém okně *Protokol sítě Internet (TCP/IP) – vlastnosti*. Doporučená konfigurace viz. kapitola 2.5 a dalším panelu vložíte název budoucí domény. Dále se instalují součásti systému. Systém se restartuje.
10. Systém Windows 2000 Server je připraven k použití.

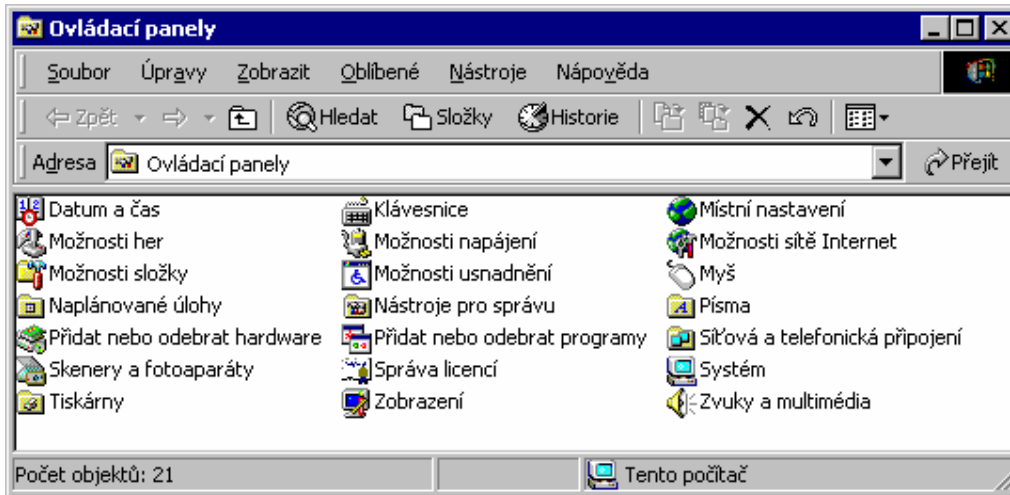
2.2 Konfigurace a správa Windows

Ovládací panely

Ke konfiguraci a správě Windows slouží Ovládací panely. Pomocí jich můžete přidávat a odebírat hardware, přidávat nebo odebírat programy,



konfigurovat síťové připojení nebo spravovat počítač atd. - viz obr. 1.1 .
Ovládací panely spustíte *Start -> Nastavení -> Ovládací panely*.



Obrázek 2.1 Ovládací panely

Nástroje pro správu

Následující nástroje pro správu - viz obr 1.2 jsou součástí operačního systému Windows 2000 Professional i Windows 2000 Server:

Služby Component Services Tyto služby určené pro správce systému slouží k zavádění a správě programů COM+ prostřednictvím grafického uživatelského rozhraní nebo k automatizaci úloh spojených se správou pomocí skriptovacího nebo programovacího jazyka.

Správa počítače Tento nástroj se používá ke správě místních nebo vzdálených počítačů pomocí jediného sloučeného nástroje na pracovní ploše. Správa počítače je kombinací několika nástrojů pro správu systému Windows 2000 do jediného stromu konzoly, který umožňuje snadný přístup k vlastnostem správy určitého počítače.



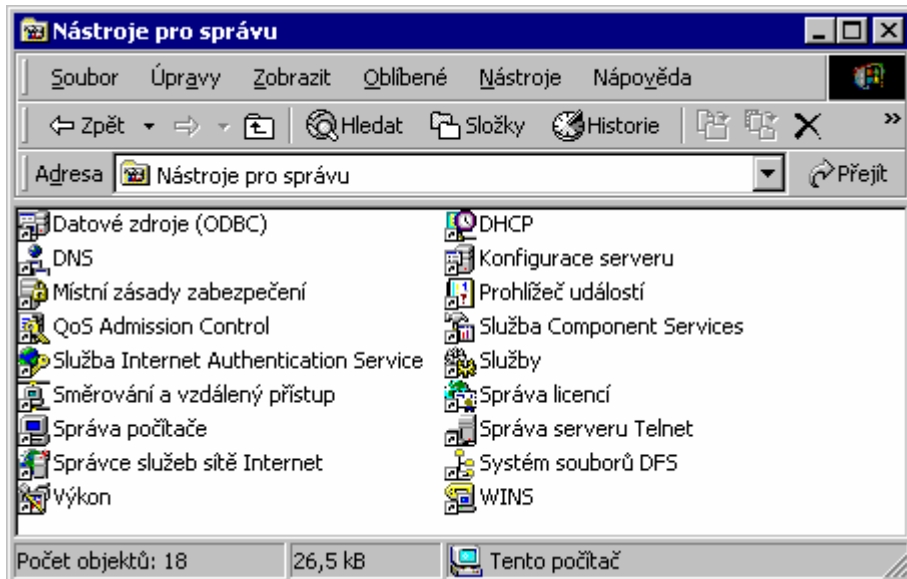
Datové zdroje (ODBC) Programovací rozhraní ODBC (Open Database Connectivity) umožňuje programům získat přístup k datům v systémech správy databází, které jako standard používají k získání přístupu k datům jazyk SQL (Structured Query Language).

Prohlížeč událostí Používá se k zobrazení a správě protokolů systémových událostí, událostí programů a událostí zabezpečení. Prohlížeč událostí shromažďuje informace o problémech hardwaru a softwaru a sleduje události zabezpečení systému Windows 2000.

Místní zásady zabezpečení Tento nástroj slouží ke konfiguraci nastavení zabezpečení místního počítače. V tomto nastavení jsou zahrnuty zásady hesla, zásady zamknutí účtu, zásady auditu, zásady zabezpečení protokolu IP, přiřazení uživatelských práv, agenti pro obnovení zašifrovaných dat a další možnosti zabezpečení.

Výkon Tento nástroj slouží ke shromažďování údajů o činnosti paměti, disků, procesorů, sítě a dalších činnostech a k jejich zobrazení v reálném čase pomocí grafu, histogramu nebo formuláře zprávy.

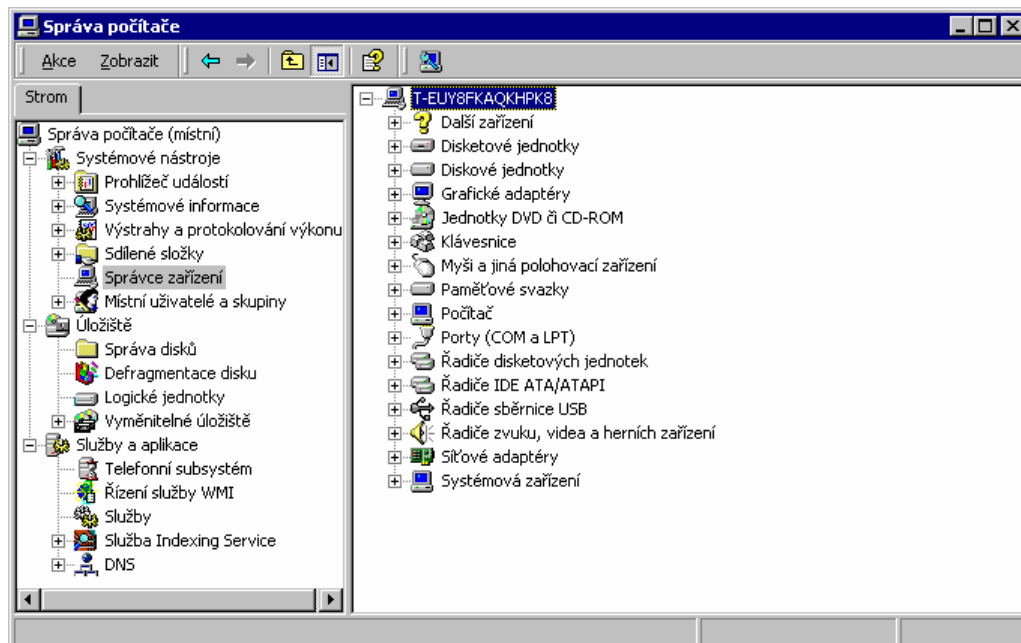
Služby Tento nástroj slouží ke správě služeb v počítači, nastavení zotavovacích postupů v případě chyby služby a k vytvoření vlastních názvů a popisů služeb umožňujících snadné rozpoznání.



Obrázek 2.2 Nástroje pro správu

Správa počítače

Tento nástroj se používá ke správě místních nebo vzdálených počítačů pomocí jediného sloučeného nástroje na pracovní ploše. Správa počítače je kombinací několika nástrojů pro správu systému Windows 2000 do jediného stromu konzoly, který umožňuje snadný přístup k vlastnostem správy určitého počítače – viz obr. 1.3.



Obrázek 2.3 Správa počítače



2.3 Active Directory a systém DNS

Active Directory je adresářová služba systému Windows 2000 Server. Ukládá informace o objektech v síti a usnadňuje správcům a uživatelům vyhledávání a použití těchto informací. Jako základ logického, hierarchického uspořádání informací o adresáři používá služba Active Directory strukturované ukládání dat.

Zabezpečení je integrováno ve službě Active Directory prostřednictvím ověřování při přihlášení a řízení přístupu k objektům v adresáři. Pomocí jediného přihlášení do sítě mohou správci spravovat data a uspořádání adresářů v rámci sítě a oprávnění uživatelé sítě mají přístup k prostředkům kdekoliv v síti.

2.3.1 Instalace potřebných součástí systému

Pokud jste již při instalaci zvolili službu DNS a službu Active Directory můžete tuto kapitolu přeskochit.

V Ovládacích panelech zvolte položku *Přidat nebo odebrat programy* -> *Přidat nebo ubrat součásti systému Windows* -> *Průvodce součástí systému Windows*. Zaškrtneme položku *Síťové služby* a tlačítkem *podrobnosti...* dostaneme okno *Síťové služby* kde zaškrtneme položky *Domain Name System*, *Active Directory* a *Dynamic Host Configuratio protocol (DHCP)* a doinstalujeme potřebné služby.

2.3.2 Instalace Doménového řadiče

Zjednodušeně si můžeme doménu představit jako pracovní skupinu. Počítač se zařazuje do domén, přičemž jeden z nich, který je určen pro správu domén se nazývá **doménový řadič**.

Doménový řadič nainstalujeme pomocí *Start* -> *Programy* -> *Nástroje pro správu* -> *Konfigurace serveru*. Spustíme průvodce službou **Active Directory**



– viz obr 1.4, který znázorňuje po sobě jdoucí panely **Průvodce instalací služby Active Directory**:



Obrázek 2.4 Konfigurace serveru

1. První panel je pouze informační.
2. Na dalším panelu zaškrtněte volbu **Řadič domény pro novou doménu**, žádná doména zatím neexistuje.
3. Dále zaškrtněte volbu **Vytvořit novou větev**, jelikož žádná větev zatím neexistuje.
4. Dosud není žádná struktura vytvořená. Přepněte **Vytvořit novou doménovou strukturu**.
5. Zadejte úplný název DNS nové domény např. fima.cz.



6. V další okně musíme nastavit NetBIOS pro starší typy Windows, i když mi předpokládáme za na stanicích bude Windows 2000.
7. Udává uložení konfiguračních souborů Active Directory. První políčko umístění databáze, druhé umístění souboru protokolu. Pokud nemusíte nechte standardní nastavení.
8. Cesta ke složce Sysvol, do níž budou uloženy serverové kopie systémových souborů domény.
9. Průvodce služby Active Directory Vám oznámí že nemůže navázat spojení se serverem DNS. Tlačítkem OK přistoupíme k samotné konfiguraci DNS serveru.
10. Zvolte možnost **Nainstalovat a nakonfigurovat server DNS na tomto počítači.**
11. Přepněte do polohy **Oprávnění kompatibilní pouze se servery systému Windows**, jelikož jiný používat nebudeme. Je to výhodnější i z hlediska bezpečnosti.
12. Na dalším panelu jste vybídnuti k zadání a potvrzení hesla uživatele Administrátor, pro případ, že byste potřebovali obnovit adresářové služby v režimu **Obnova adresářových služeb.**
13. Další panel shrne vše co jste zatím podnikli.
14. Otevře se dialogové okno Konfigurace služby Active Directory, které Vám nabízí průběžný stav událostí.
15. Instalace je dokončena.



2.4 Uživatelé a počítače Active Directory

Konzoly pro správu a publikování informací v adresáři spustíme *Start -> Programy -> Nástroje pro správu -> Uživatelé a počítače Active Directory*. Jsou v ní předdefinovány některé skupiny počítačů a uživatelů.

Účty počítačů

Ve složce **Domain Controllers** je jediná položka - náš server. Tlačítkem **Vlastnosti** máte možnost změnit některé jeho vlastnosti.

Služba Active Directory nepřipojí k serveru počítač, jehož jméno nemá registrováno. Ve složce **Computers** zadejte příkaz *Nový -> Počítač*.

Vložte název první stanice do pole **Název počítače**. V poli **Uživatel nebo skupina** přiřadíme počítač do skupiny počítačů **Domain Computer**.

Uživatelské účty

Otevřete průvodce zařízením nového uživatele *Nový -> Uživatel* a vyplňte následující tři panely:

1. Základní údaje o uživateli
2. Heslo uživatele.
3. Kontrola vyplněných údajů.

Tlačítkem **Vlastnosti** definujete některé konkrétní nastavení uživatelského účtu ve dvanácti záložkách např. :

- Přihlašovací uživatelské jméno
- Počítače ke kterým se uživatel nesmí přihlásit
- Dialogové okno
- Způsob nakládáním s heslem



- Doba trvání uživatelského účtu
- a další které si probereme dále

Skupiny

Uživatele můžeme řadit do skupin například z důvodů práv přidělené určité skupině.

Přejděme na kartě vlastnosti uživatele na záložku **Je členem** kde můžete uživatele řadit do skupin.

Profil uživatele

Profil se vytváří při prvním přihlášení do systému Windows.

Profil uživatele může být uložen na serveru a uživatel jej může používat na jakémkoliv počítači. V okně vlastností uživatele v záložce **Profil** kde zadáte název serveru a název profilu.

```
\\server\jmeno_uzivatele
```

Domovský disk

Domovský disk vytváříme, aby uživatel měl možnost mít svoje data k dispozici ať se přihlásí z jakéhokoliv počítače v síti.

Postup vytvoření domovského disku:

1. Na serveru vytvoříme adresář např. Domovske_disky do které budeme přidávat domovské disky jednotlivých uživatelů.
2. Vytvořit složku např. jméno uživatele, která bude domovským diskem uživatele.
3. Nastavte sdílení tohoto adresáře v nabídce **Vlastnosti složky**.
4. Otevřete okno vlastností uživatele a přejděte na kartu Profily.



5. Přepínač Domovská složka: přepněte do polohy připojit.
6. V seznamu vyberte označení domovského disku např. H:.
7. Do pole k: napište cestu ke složce ve formátu:

`\\server\\sdílená_položka\adresář`

8. Vraťte se do adresáře uživatele a nastavte sdílení tak, aby měl přístup pouze uživatel.
9. Při přihlášení uživatele by adresář měl být připojen jako disk.

2.5 Konfigurace sítě na pracovních stanicích

Pokud připojujeme stanici v Windows 2000, musíme se k ní nejdříve přihlásit jako Administrátor.

Přejdeme do **Připojení k místní síti** *Místa v síti -> Vlastnosti -> Síťová a telefonická připojení -> Vlastnosti*.

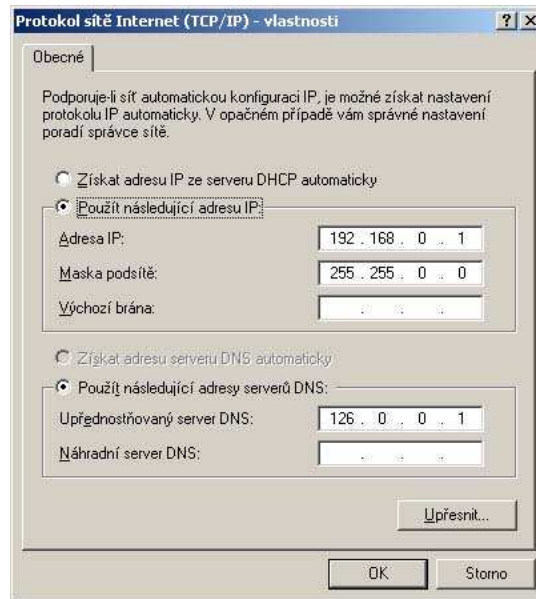
Nainstalovány by měli být následující součásti:

- Klient sítě Microsoft
- Sdílení souborů a tiskáren v sítích Microsoft
- Protokol sítě Internet (TCP/IP)

Pokud se některý z těchto součástí chybí je třeba je doinstalovat tlačítkem *Nainstalovat...*

Nastavení protokolu Protokol sítě Internet (TCP/IP) -> Vlastnosti – viz obr.

1.5.



Obrázek 2.5 Protokol TCP/IP - vlastnosti

Nastavíme IP adresu odlišnou od IP serveru a masku podsítě stejnou. Přepneme přepínač do polohy **Použít následující adresy serverů DNS** a do pole **Upřednostňovat server DNS** napište shodnou adresu jako v témže okně na serveru. Uložte nastavení sítě. Přejděte do *Tento počítač -> Vlastnosti -> Vlastnosti systému -> Identifikace v síti -> Vlastnosti*. Otevře se okno změny identifikace.

Zadejte úplný název počítače , který se musí shodovat s názvy definovanými v kontejneru **Computers** v okně **Uživatelé a počítače služby Active Directory**. Přepínač **Je členem** přepněte do polohy **Domény** a zadejte název domény. Následovně zadejte **Uživatelské jméno a heslo v doméně**.

Síť je nakonfigurována a připravena k použití.



3 Operační systém SuSE linux

Od roku 1992 je SUSE jedním ze světově nejrozšířenějších poskytovatelů linuxového softwaru a služeb. Díky jednomu z největších výzkumných týmů dokáže SuSE poskytovat software připravený pro podnikovou sféru a služby, které se mohou chlubit nezávislosti open source komunity.



3.1 Instalace SuSE

Přepokládám, že na počítači není žádný jiný operační systém a disk se během instalace bude formátován (ztráta veškerých dat na disku).

1. Vložte první CD do mechaniky. Systém bude zaveden z CD a budete si moci vybrat jazyk pro instalaci. Podle zvoleného jazyka pak bude automaticky nastaveno rozložení klávesnice.
2. SuSE Linux zkontroluje veškeré hardwarové vybavení počítače, provede jeho konfiguraci a následně vypíše všechny informace v dialogu na následující straně. Navíc je zde zobrazen také návrh rozdělení pevného disku a typ instalace.

Po kontrole systému máte možnost upravit následující – viz obr. 2.1:

Jazyk Zde je uveden jazyk použitý pro instalaci a běh systému.

Časová zóna Určuje nastavení místního času.

Klávesnice V této položce můžete určit, zda budete chtít používat standardní qwertz klávesnici, nebo programátorskou qwerty, případně jinou.



Myš Je vypsán detekovaný typ myši

Dělení disků Zde vám systém navrhne, jakým způsobem rozdělit disky

Režim Uvádí typ instalace. Při nové instalaci by zde mělo být uvedeno Nová instalace

Spouštění Označuje médium, ze kterého bude systém spouštěn. Standardně by měl být vypsán typ vašeho pevného disku

Software Zde byste měli mít standardní (default) instalaci s kancelářským balíkem. Po provedení změn se vždy vrátíte k tomuto dialogu a stiskem ‘Další’ můžete pokračovat v instalaci.



Obrázek 3.1 YaST instalace SuSE



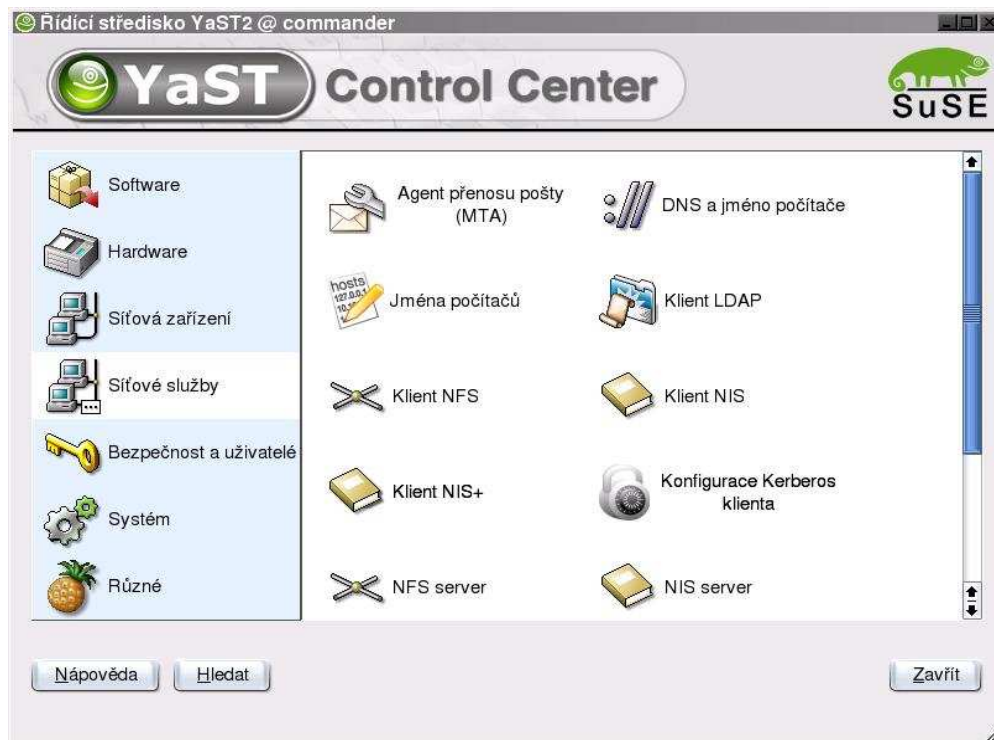
3. Dále Zahájíme instalaci tlačítkem v zeleném poli **Ano**. Pak už záleží pouze na výkonu počítače, za zhruba 15 minut získáte systém s 350ti programovými balíky.
4. Po dokončení instalace musíte ještě provést tři důležitá nastavení předtím, než budete s to pracovat se systémem. Za prvé je třeba určit heslo pro správce systému. Následně je třeba vytvořit alespoň jednoho uživatele a provést konfiguraci obrazovky. Zda budete chtít používat grafické prostředí a následně jeho rozlišení a barevnou hloubku. Dále pak máte možnost provést konfiguraci dalšího hardwaru, nebo to nechat na pozdější dobu. Většina zařízení je automaticky rozpoznána a jejich konfigurace je přednastavena, takže stačí pouze potvrdit nastavení.

3.2 Konfigurace a správa SuSE - YaST2

Konfiguraci a správu vašeho systému zajišťuje program YaST2. Po spuštění YaST2 budete mít v levé části okna záložky s jednotlivými oblastmi systému a v hlavním okně pak moduly pro nastavení jednotlivých komponent. YaST2 zapisuje u většiny modulů nastavení do textových konfiguračních souborů, které je možné v případě potřeby editovat i ručně. Pomocí YaST2 můžete spravovat nainstalovaný software, tj. přidávat nebo odebírat programové vybavení. Navíc zde můžete k operačnímu systému přidat další hardwarové komponenty (např. tiskárny, zvukové karty, skenery), spravovat systémové služby, konfigurovat přístup k Internetu, atd.

Spuštění YaST2

YaST2 můžete spustit pouze jako superuživatel (root). V grafickém prostředí KDE – viz obr. 2.2 klikněte na *Správa -> Systém -> Konfigurace -> YaST2* nebo v textovém režimu příkazem `yast` – viz obr. 2.3. Máte také možnost přistupovat přímo k jednotlivým modulům v YaST2.

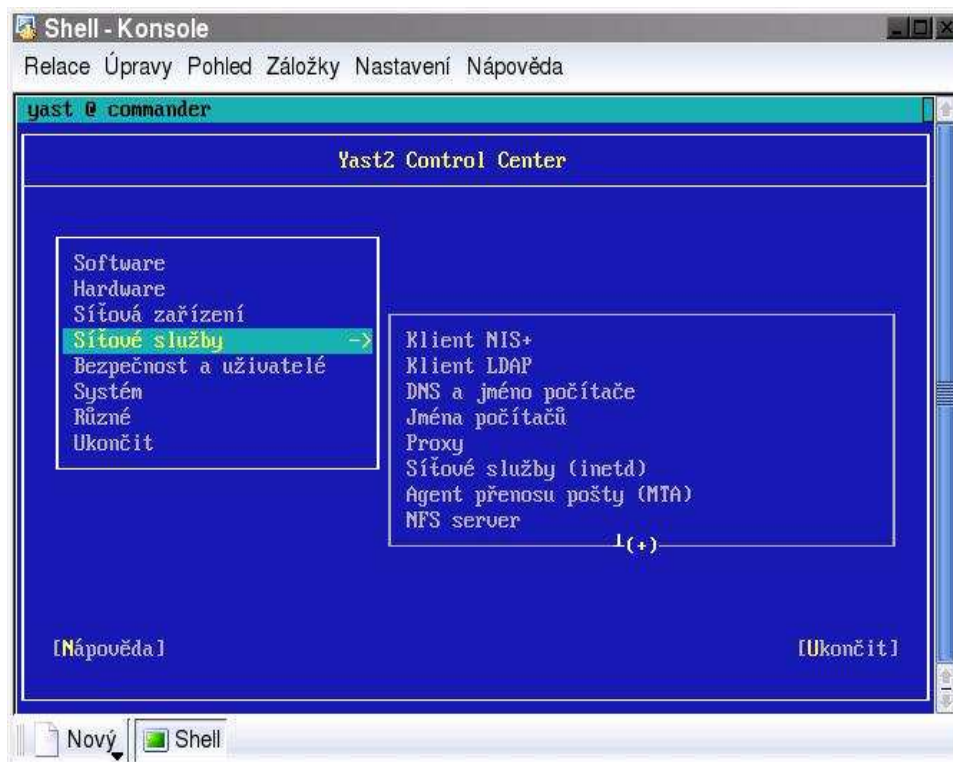


Obrázek 3.2 YaST KDE - Control Center

Control Center

Po spuštění se zobrazí Control Center. V levé části jsou uvedeny hlavní kategorie:

- **Software** – správa a instalace softwaru
- **Hardware** – správa, konfigurace a přidávání hardwaru
- **Sít'/základní** – základní konfigurace sítě a připojení k Internetu
- **Sít'/pokročilé** – konfigurace pokročilejších síťových služeb
- **Bezpečnost & uživatelé** – správa uživatelů a nastavení bezpečnosti
- **Systém** – konfigurace systému
- **Různé**



Obrázek 3.3 Textová verze - Control Center

Pomocí YaST Control Center můžete konfigurovat a spravovat služby, které si popíšeme v dalších kapitolách v textovém režimu:

- konfigurovat síť (Síťová zařízení->Síťová karta)
- vytvářet uživatelské účty (Bezpečnost a uživatelé -> Založit nového uživatele)
- Konfigurovat servery NIS a NIS klienta (Síťové služby->NIS server nebo Klient NIS)
- Konfigurace serveru NFS (Síťové služby->NFS server)

Pokud nemáte jinou možnost je vždy lepší použít pro konfiguraci YaST v jakékoliv podobě (grafické či textové).



3.3 Konfigurace sítě

Konfigurace se provádí na všech počítačích v síti. Ať se jedná o server nebo o samotnou stanici na kterých také běží operační systém SuSE. Postup je všude stejný.

Konfigurace rozhraní pro protokol IP

K nastavení síťových rozhraní a inicializaci směrovací tabulky se používají příkazy `ifconfig` a `route`.

1. Příkaz `ifconfig` se používá pro zpřístupnění rozhraní síťové vrstvě jádra. Tento proces v sobě zahrnuje přidělení IP-adresy, některých parametrů a aktivaci rozhraní.

```
# ifconfig
```

```
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:324 errors:0 dropped:0
            overruns:0 frame:0
            TX packets:324 errors:0 dropped:0
            overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:24268 (23.6 Kb)  TX bytes:24268
            (23.6 Kb)
```

2. Nastavíme IP-adresu a masku podsítě:

```
# ifconfig eth0 192.168.1.10 netmask 255.255.255.0
```



3. Zkontroluje zda je vše nastaveno správně (IP adresa a maska podsítě).

Po zadání příkazu ifconfig dostaneme na výstup:

```
# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr
00:50:DA:DE:6B:0B
          inet addr:192.168.1.10
Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:daff:fede:6b0b/64
Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
frame:0
          TX packets:253 errors:0 dropped:0
overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:15228 (14.8
Kb)
          Interrupt:10 Base address:0xec00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:324 errors:0 dropped:0
overruns:0 frame:0
          TX packets:324 errors:0 dropped:0
overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24268 (23.6 Kb)  TX bytes:24268
(23.6 Kb)
```




4. Dále musíme nastavit směrování. Příkaz `route` umožňuje přidávat nebo odstraňovat směrování ze směrovací tabulky jádra systému. Může být vyvolán následujícím způsobem `route [add|del] target` kde argumenty `add` a `del` určují, zda se bude směrování do cíle `target` přidávat nebo se z něj bude odstraňovat.

```
# route add -net 192.168.1.0 netmask 255.255.255.0
dev eth0
# route add default gw 192.168.1.100
# route
```

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	Metric	Ref	
Use	Iface					
192.168.1.0	*	255.255.255.0	U	0	0	
0	eth0					
default	192.168.1.100	0.0.0.0	UG	0	0	
0	eth0					

Konfigurační soubory

Zde je uveden přehled důležitých síťových konfiguračních souborů , jejich formátů a funkcí.

/etc/hosts V tomto souboru se přiřazují jménům počítačů IP adresy. Pokud se nepoužívá nameserver, musíte zde uvést všechny počítače, na které chcete mít přístup pomocí jména. Každý počítač je na zvláštní řádce, sestávající se postupně z IP adresy, plně kvalifikovaného jména počítače a jeho aliasů , oddělených mezerami nebo tabulátory. Soubor musí být na každém počítači tj. na serveru i na pracovních stanicích aktualizovaný. Nebo soubor nasdílíme ze serveru pomocí NFS služby.



```
# hosts This file describes a number of hostname-to-
address
# mappings for the TCP/IP subsystem. It is mostly
# used at boot time, when no name servers are
running.
# On small systems, this file can be used instead of
# a "named" name server. Just add the names,
# adresses and any aliases to this file...
#
192.168.1.10  Server.firma.cz  Server1
192.168.1.10  Tomik.firma.cz  Tomik
192.168.1.13 Sekretarka.firma.cz  Marticka
192.168.1.100 Brana.firma.cz  Brana
# End of hosts
```

/etc/networks Zde se převádějí jména sítí na síťové adresy. Formát je stejný jako u souboru hosts, pouze síťová jména jsou jako první a za nimi následují adresy .

```
# networks This file describes a number of netname-
to-address
# mappings for the TCP/IP subsystem. It is mostly
# used at boot time, when no name servers are
running.
#
loopback 127.0.0.0
localnet 192.168.1.0
# End of networks.
```



Startovací skripty pro SuSE

Kromě popsaných konfiguračních souborů je zde ještě řada skriptů, které spouštějí síťové programy během startu počítače, a to v okamžiku, kdy systém přejde na některou víceuživatelskou úroveň. Tyto skripty se dají použít pouze pro SuSE.

`/etc/init.d/network` Tento skript se stará o hardwarovou a softwarovou konfiguraci sítě při startu systému. Nastavuje IP adresu, síťovou adresu, síťovou masku a bránu.

`/etc/init.d/inetd` Spustí program `inetd`. To je potřeba, chcete-li se přihlásit k tomuto počítači přes síť.

`/etc/init.d/nfsserver` Spustí server NFS.

`/etc/init.d/ypserv` Spustí server NIS.

`/etc/init.d/ypbind` Spustí klient NIS.

3.4 NIS (Network Information Service)

Jakmile přistupuje v síti více unixových počítačů ke společným prostředkům, je třeba zajistit, aby bylo všude společné označení uživatelů a skupin. Síť musí být pro každého uživatele transparentní ať pracuje na kterémkoli z těchto počítačů, vždy by měl najít stejné prostředí. Toto je umožněno pomocí služeb NIS a NFS.

NIS je databázová služba, umožňuje po síti přístup k souborům `/etc/passwd`, `/etc/shadow` nebo `/etc/group`. NIS se dá použít i pro další úlohy (např. pro `/etc/hosts` nebo `/etc/services` atd.).



Konfigurace NIS klienta

Programy pro zřízení klienta NIS pro SuSE Linux obsahuje balík `ypbind`, série `n`. Postupuje se přitom v následujících krocích:

1. Nastavte NIS doménu v souboru `/etc/defaultdomain`. NIS doménu není DNS doména.

2. Název NIS serveru se zapisuje do souboru `/etc/yp.conf`

```
ypserver 192.168.0.1
```

3. Název NIS serveru (např. `Server.firma.cz`) musí být možné převést pomocí `/etc/hosts`

4. Doplnit položky v `/etc/passwd` a `/etc/group`. Aby bylo možné provést po prohledání lokálních souborů dotaz na NIS serveru, musí být odpovídající soubory doplněny o řádek, který začíná znakem plus. Problematiku Uživatelských účtů si popíšeme v kapitole Správa uživatelských účtů.

5. Posledním krokem pro nastavení NIS klienta je spuštění `ypbind` a tím vlastního NIS klienta.

6. Pak už je třeba pouze restartovat systém nebo restartovat síť příkazy.

```
# rcnetwork restart  
# rcypbind restart
```



Primární a sekundární NIS server

Pro tuto službu instalujte balík `ypserv`, série `n`; podrobný návod najdete v `/usr/share/doc/packages/yp/HOWTO`.

Většinou jsou sdíleny pouze `/etc/passwd`, `/etc/shadow` a `/etc/group`, ale můžete také dát k dispozici `/etc/hosts` (Pokud sdílíme `/etc/hosts` nemusíme nastavovat tento soubor na všech stanicích. V opačném případě je to nutné!) a `/etc/services`. Klienti a servery musí mít stejný název domény, který je možné libovolně zvolit a nemusí odpovídat žádné registrované doméně. Tento název je třeba uvést v souboru `/etc/defaultdomain`.

3.5 NFS (distribuované souborové systémy)

Jak již bylo uvedeno v předchozím kapitole NFS (spolu s NIS) umožňují, aby byla síť pro uživatele transparentní. NFS umožňuje počítačům sdílet souborové systémy v síti, uživatel pak vidí stejné prostředí nezávisle na tom, odkud se přihlásí.

Podobně jako NIS, představuje i NFS nesymetrickou službu je zde server NFS a klient NFS. Počítač může vykonávat obě tyto úlohy, tj. exportovat do sítě své vlastní souborové systémy a připojovat souborové systémy jiných počítačů.

Centrální server NFS mívá obvykle velkou diskovou kapacitu. Jednotliví klienti si z něho připojují povolené adresářové stromy ke svému souborovému systému.

Import souborových systémů

Spuštění serveru NFS již bylo ukázáno v souvislosti s NIS. Je-li tento předpoklad splněn, mohou se souborové systémy exportované z jiného počítače připojovat stejně snadno jako lokální souborové systémy příkazem `mount`.



```
# mount -t nfs Počítač:Vzdálená cesta Lokální cesta
```

Pokud se má například připojit adresář /home počítače Sekretarka namísto adresáře /home na našem počítači, dosáhneme toho následujícím příkazem:

```
# mount -t nfs Sekretarka:/home /home
```

Export souborových systémů

Počítač, který exportuje souborové systémy, se nazývá server NFS. Musí na něm být spuštěny následující síťové služby:

- RPC portmapper (portmap)
- RPC mount démon (rpc.mountd)
- RPC NFS démon (rpc.nfsd)

Tyto služby se spouštějí při startu systému pomocí skriptů:

- /etc/init.d/portmap a
- /etc/init.d/nfssserver.

Kromě spuštění uvedených démonů se ještě musí stanovit, které souborové systémy je povoleno exportovat a na které počítače. K tomu slouží soubor /etc/exports, kde se vždy uvede na samostatnou řádku, který počítač přístup danému adresáři (včetně jeho podadresářů), a s jakými právy.

Oprávněné počítače se zadávají obvykle jejich plnými jmény, včetně domény. Také je možno použít zástupné znaky jako '*' a '?', podobně jako to dělá bash. Lze uvést i IP adresy počítačů nebo celých sítí.

Pokud se nezadá žádný počítač, pak je zde omezení pouze uvedenými přístupovými právy a nikoli počítačem. Přístupová práva se dávají do závorek za jména počítačů. Nejdůležitější volby zde jsou:



- ro - Souborový systém se exportuje pouze pro čtení (standardní).
- rw - Souborový systém se exportuje pro čtení i zápis.

Soubor exports může vypadat například jako soubor:

```
# /etc/exports
#
/home Tomik(rw) Server(rw)
/ Sekretarka(ro,root_squash)
/tmp/ *(rw,root_squash,sync)
# Konec souboru /etc/exports
```

/etc/exports Soubor `/etc/exports` načítají démoni `mountd` a `nfsd`. Pokud se v něm něco změnilo, je třeba `mountd` a `nfsd` opětovně spustit, a to nejnázemně příkazem:

```
# rcnfsserver restart
```

3.6 Správa uživatelských účtů

Vytváření uživatelských účtů

Aby uživatelé mohli pracovat nezávisle na sobě, je třeba se k systému nejdříve přihlásit. Při přihlášení je třeba uvést uživatelské jméno a heslo. Každý uživatel pak má domovský adresář, kde má uloženy vlastní soubory a konfigurace používaných programů.

Každého uživatele lze identifikovat podle jednoznačného celého čísla, tzv. **identifikačního čísla uživatele** (angl. **user ID**, zkráceně **UID**). Jména v



textové podobě a přidělená **uživatelská jména** se udržují ve zvláštní databázi mimo vlastní jádro. Tato databáze obsahuje též další informace o uživateli systému.

Když potřebujete vytvořit nový uživatelský účet, musíte přidat informace o novém uživateli do uživatelské databáze a vytvořit pro něj vlastní domovský adresář.

Správce má dokonce k dispozici opět dvě varianty jak přidat uživatele do systému. Je to příkazová řádka, programy `adduser` a `useradd` a YaST2.

Soubor `/etc/passwd` a další informační soubory

Základní databází uživatelů v systému Unix je textový soubor `/etc/passwd` (password file), v něm jsou uvedeny platná uživatelská jména a další k nim přidružené informace. Každému uživateli odpovídá v souboru jeden záznam řádek, který je rozdělen na sedm polí, jejich oddělovačem je dvojtečka. Význam jednotlivých položek je následující:

1. Uživatelské jméno.

1. Identifikační číslo uživatele.
2. Identifikační číslo pracovní skupiny.
3. Skutečné jméno uživatele, případně popis účtu.
4. Domovský adresář.
5. Příkazový interpret, který se spustí po přihlášení.

```
ldap:x:76:70:User for
OpenLDAP:/var/lib/ldap:/bin/bash
tomik:x:500:100:tomik:/home/tomik:/bin/bash
alias:x:501:500::/var/gmail/alias:/bin/bash
qmaild:x:502:500::/var/gmail/alias:/bin/bash
marie:x:508:100:Marie:/home/marie:/bin/bash
Libor:x:509:100:Libor:/home/Libor:/bin/bash
```




Každý uživatel systému má k souboru `/etc/passwd` přístup ke čtení. Může tedy například zjistit přihlašovací jména ostatních uživatelů. Hesla jsou uložena v souboru `/etc/shadow` zakódovaná.

```
Libor:uRG0luJyU0n9.:12508:0:99999:7:::  
marie:IVER66bPRF7Sg:12508:0:99999:7:::  
gmaild!:12370:0:99999:7:::  
tomik:BrsTm7Sj48rGs:12314:0:99999:7:::
```

Výběr čísel uživatelského ID a ID skupiny

Při použití síťového souborového systému NFS, musíte mít stejná UID a GID na všech systémech v síti. To proto, že i systém NFS identifikuje uživatele podle hodnoty UID.

Když v síti využíváte NFS, budete si muset zvolit některý z mechanismů synchronizace informací o uživatelských účtech. Jednou z možností je systém NIS .

Vytváření uživatelských účtů

Nový uživatelský účet lze vytvořit ručně tímto postupem:

1. Upraví se soubor `/etc/passwd`, například příkazem `vipw`, tak, že se do souboru hesel přidá další řádek nového uživatelského účtu. Program `vipw` soubor `/etc/passwd` uzamkne, takže se ostatní programy nebudou pokoušet jej změnit.
2. Jestli je potřeba vytvořit i novou pracovní skupinu, upraví se podobným způsobem i soubor `/etc/group`, a sice programem `vigr`.

```
uucp:x:14:tomik,marie,Libor  
dialout:x:16:tomik,marie,Libor
```



```
audio:x:17:tomik,marie,Libor
```

3. Příkazem `mkdir` se pro nového uživatele vytvoří domovský adresář.
4. Do nově vytvořeného domovského adresáře se nakopírují konfigurační soubory z adresáře `/etc/skel`.
5. Příkazy `chown` a `chmod` se upraví jejich vlastnická a přístupová práva. Užitečný je v tomto případě jejich parametr `-R`. Správná přístupová práva se mohou trochu lišit, a to podle typického využití toho kterého systému, nicméně příkazy v níže uvedeném příkladu obvykle vyhovují většině případů:

```
# cd /home/newusername
# chown -R username.group
# chmod -R go=u,go-w
# chmod go=
```

6. Zadejte heslo programem `passwd`.

Poté, co bylo v posledním kroku nastaveno heslo, bude nový účet přístupný.

Změny vlastností uživatelských účtů

Je několik příkazů, kterými lze měnit různé vlastnosti uživatelských účtů (tedy příslušných položek v souboru `/etc/passwd`):

`chfn` Mění pole, ve kterém je uloženo skutečné jméno uživatele.

`chsh` Mění nastavený příkazový interpret.

`passwd` Mění přístupové heslo.



Superuživatel může pomocí těchto programů změnit vlastnosti kteréhokoliv účtu. Ostatní nepriviligovaní uživatelé mohou měnit pouze vlastnosti svého vlastního účtu.

Ostatní změny položek souboru `/etc/passwd` se musí dělat ručně. Když například potřebujete změnit uživatelské jméno, musíte přímo upravit databázi uživatelů `/etc/passwd`. Analogicky, kdy. potřebujete přidat či odebrat uživatele z nebo do některé z pracovních skupin, musíte upravit soubor `/etc/group` (příkazem `vigr`). Avšak takovéto úkoly se dělají zřídka a musí se dělat opatrně, protože když například změníte některému z uživatelů jeho uživatelské jméno, nebude mu docházet elektronická pošta a musíte pro něj vytvořit přezdívku., tedy alias.

Zrušení uživatelského účtu

Potřebujete-li zrušit uživatelský účet, smažte nejdříve všechny soubory, které patří uživateli zrušeného účtu, včetně poštovní schránky, aliasů pro elektronickou poštu, tiskových úloh, úkolů spouštěných demony `cron` a `at` a všechny další odkazy na tohoto uživatele. Pak odstraňte odpovídající řádek v souborech `/etc/passwd` a `/etc/group` a `/etc/shadow`. Předtím, než začnete mazat vše ostatní, je lepší zakázat přístup k rušenému účtu. Uživatel tak nebude mít možnost se připojit do systému v době, kdy je jeho účet odstraňován.



4 WWW Server – Apache

Apache zaujímá v prostředí internetu velmi významnou pozici, protože se jedná o dlouhodobě o nejrozšířenější webový server,



který je možné provozovat na různých platformách operačních systémů.

- Je zdarma.
- Nezávislí na platformě operačního systému.
- Rozšiřitelnost velkého množství modulů.

4.1 Instalace v operačním systému Unix

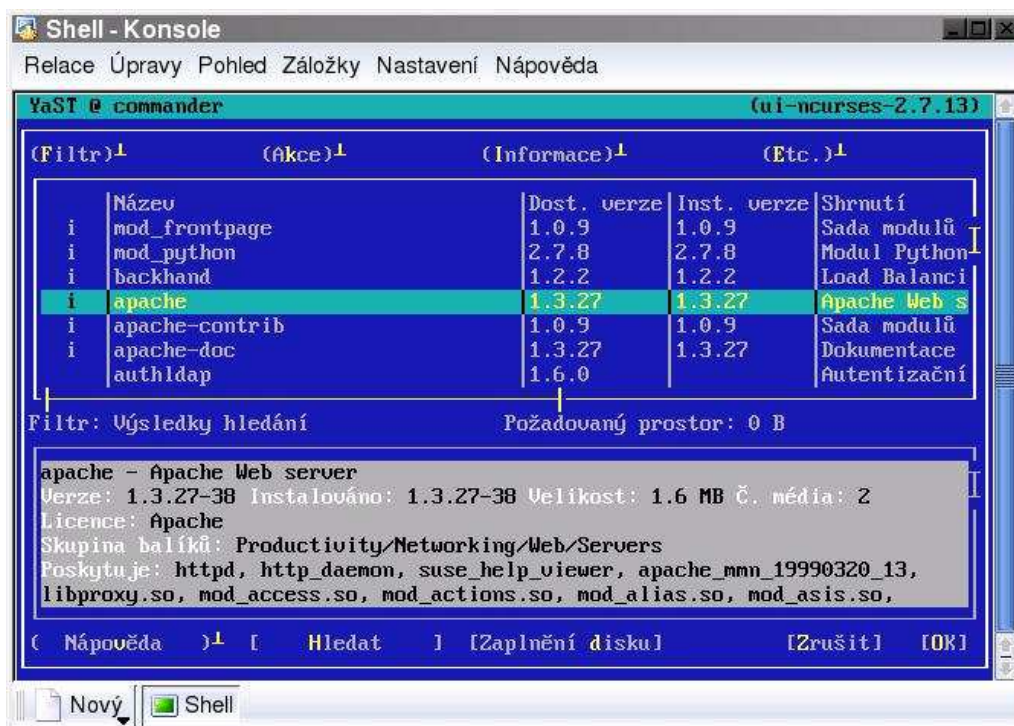
4.1.1 Binární instalace

Binární instalace je velice jednoduchá. Je přímo určená pro konkrétní operační systém. Mnou použitá distribuce SuSE obsahuje vlastní instalační balík Apache odladěný pro tuto distribuci. Instalační soubory jsou dostupné k volnému stažení z <http://www.apache.org/dist/httpd/>.

Je možné instalovat balíček stažený z internetu Apache z příkazové řádky a to příkazem:

```
# rpm -ivh jmeno_souboru.rpm
```

nebo rovnou implementovaný v distribuci SuSE což je samozřejmě jednodušší a doporučená verze instalace. V SuSE YaST2 – viz obr 3.1:



Obrázek 4.1 Instalace Apache YaST

4.1.2 Instalace ze zdrojových kódů

Soubory se zdrojovým kódem

Soubory se zdrojovým kódem jsou vloženy do jediného zkomprimovaného souboru. Pojmenování souboru se skládá ze jména souboru, kde vyčteme verzi Apache a přípony určující typ archivace.

Konfigurace překladu

Pokud jsme v rozbaleném adresáři musíme nejprve spustit skript configure, který je uložen v tomto adresáři. Tento skript otestuje potřebné programové vybavení, nastaví parametry překladače a nastaví cesty ke knihovnám potřebným pro vlastní překlad a cestu pro konečnou instalaci Apache.

```
./configure
```



Výsledkem činnosti bude vytvoření souborů `Makefile`, které budou použity pro překlad zdrojového kódu.

Překlad zdrojového kódu

Pro přeložení programu slouží utilita `make`. Pro svojí činnost používá soubory `Makefile`, které jsme vytvořili předešlím příkazem `./configure`.

```
# make
```

Instalace přeložených souborů

Provádí se pomocí utility `make` s parametrem `install` do adresáře `/usr/local/apache`

```
# make install
```

Test instalace

Nakonec je nutná úprava souboru `httpd.conf`, kde je třeba upravit nastavení direktivy `ServerName`, která obsahuje jméno serveru.

```
ServerName mujweb.cz:80
```

Úspěšnost instalace si ověříme spuštěním Apache pomocí skriptu:

```
# /usr/local/apache/bin/apachectl start
```



4.1.3 Spuštění a zastavení Apache v prostředí Unix

Skript `apachectl` je určen pro správu procesu `httpd`. Je uložen v podadresáři `/bin` kořenového adresáře Apache.

`apachectl` volby

Volba	Popis
<code>start</code>	Start procesu <code>httpd</code> .
<code>startssl</code>	Start procesu <code>httpd</code> s podporou SSL.
<code>restart</code>	Ukončení a opětovný start procesu <code>httpd</code> zasíláním signálu <code>SIGHUP</code> . Neběží-li proces <code>httpd</code> před provedením restartu, je spuštěn. Všechny dětské procesy jsou okamžitě ukončeny.
<code>graceful</code>	Ukončení a opětovný start procesu <code>httpd</code> zasíláním signálu <code>SIGUSR1</code> . Neběží-li proces <code>httpd</code> před provedením restartu, je spuštěn. Na rozdíl od <code>restart</code> nejsou přerušeny dětské procesy, které obsluhují požadavky.
<code>stop</code>	Ukončení a opětovný start procesu <code>httpd</code> zasíláním signálu <code>SIGTERM</code> . Všechny dětské procesy jsou okamžitě ukončeny.
<code>status</code>	Zobrazí informace o stavu Apache.
<code>fullstatus</code>	Úplné zobrazení informace o stavu Apache
<code>configtest</code>	Test konfiguračního souboru <code>httpd.conf</code> .
<code>help</code>	Zobrazení popisu skriptu <code>apachectl</code> .

4.2 Binární instalace v Microsoft Windows

Instalační soubory jsou dostupné na <http://www.apache.org/dist/httpd/binaries/win32/>.
Možné je stáhnout instalační soubor `apache_1.3.24-win32-x86.exe` nebo `apache_1.3.24-win32-x86.msi`.



4.2.1 Instalace

Po spuštění souboru `apache_1.3.24-win32-x86.msi` se zobrazí úvodní okno. Po stisknutí tlačítka Next se zobrazí okno s licenčním ujednáním. Instalace pokračuje otevřením okna s informacemi o Apache. Při pokračování se zobrazí okno s formulářem, ve kterém nastavíte následující údaje, které se vloží do konfiguračního souboru `httpd.conf` – viz obr. 3.2:

- Jméno domény
- Jméno počítače
- E-mailovou adresu administrátora Apache



Obrázek 4.2 Instalace Apache I

- Způsob ovládání Apache: jako službu / ručně z příkazové řádky

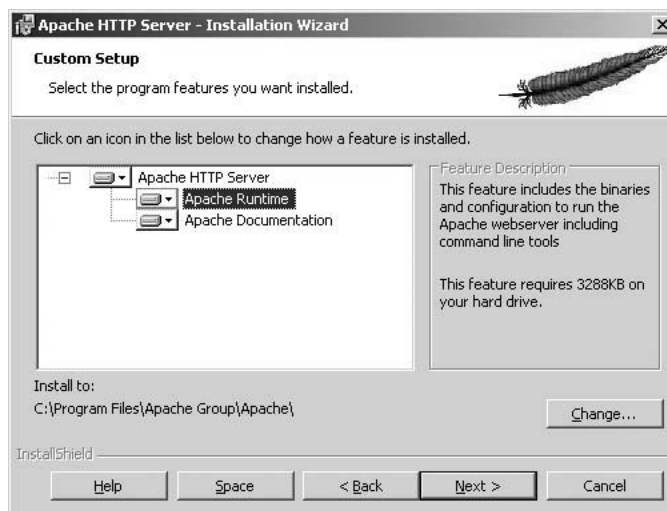
Po vyplnění údajů pokračujeme oknem výběr typu instalace:

- Typická instalace – nainstalují se základní komponenty bez zásahu uživatele



- Uživatelská instalace – výběr komponent

Pokud zvolíme uživatelskou instalaci, zobrazí se další okno, ve kterém zvolíme které komponenty chceme nainstalovat – viz obr. 3.3.



Obrázek 4.3 Instalace Apache II

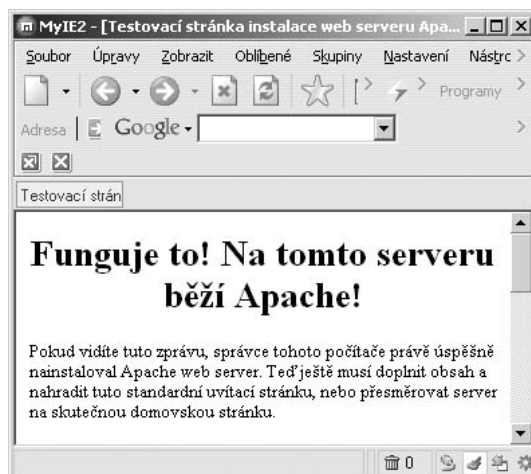
Před vlastním provedením instalace můžeme změnit cílový adresář nebo ponechat standardní adresář `c:\Program Files\Apache Group\Apache1.3`

Po nainstalování Apache se objeví poslední okno s potvrzením úspěšného dokončení instalace.

Test instalace

Editace konfiguračního souboru a příkazy pro řízení činnosti Apache je součástí nabídky *Start -> Programy -> Apache http Server*. Zde v **Control Apache Server** zvolte **Start**. V okně prohlížeče zadejte adresu URL serveru, např. `http://localhost`

Pokud se zobrazí úvodní zpráva, Apache je nainstalován úspěšně – viz obr. 3.4.



Obrázek 4.4 IE – Testovací stránka Apache

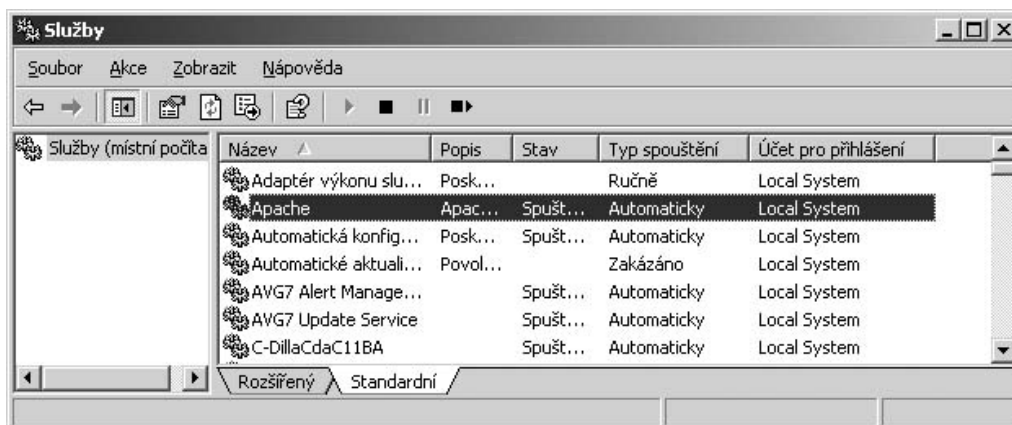
4.2.2 Spuštění a zastavení Apache v prostředí Microsoft Windows

Apache je možné ovládat v OS Windows dvěma způsoby, tuto možnost si vybíráte již při instalaci:

- jako služba OS
- pomocí příkazu konzole

Apache jako služba OS

Pro ovládání slouží modul *Služby*, který je součástí Nástrojů pro správu v Ovládacích panelech – viz obr. 3.5.



Obrázek 4.5 Služby



Tento modul umožňuje řídit běh jednotlivých služeb, ale i konfigurovat služby tak, aby se spouštěly a zastavovali automaticky.

Příkazy Apache z příkazové řádky

spuštění služby

```
c:\Program Files\Apache Group\Apache\bin>apache -n apache  
-k start
```

```
Starting the Apache service  
The Apache service is running.
```

restartování služby

```
c:\Program Files\Apache Group\Apache\bin>apache -n apache  
-k restart
```

```
The Apache service is restarting.  
The Apache service has restarted.
```

ukončení služby

```
c:\Program Files\Apache Group\Apache\bin>apache -n apache  
-k stop
```

```
The Apache service is stopping.  
The Apache service has stopped.
```

4.3 Konfigurace Apache

SuSE linux



Konfigurační soubory serveru Apache se nachází v distribuci suse
/etc/httpd/conf.

Windows 2000 server

Konfigurační soubory serveru Apache ve windows se nachází podle místa instalace Apache standardně Program Files/Apach Group/Apache/conf.

Konfigurační soubory

- **httpd.conf** – Určuje základní vlastnosti programu a jeho chování, definuje cesty k některým dalším souborům.
- **srm.conf** – Zde se konfiguruje logické chování serveru, Soubor velmi výrazně ovlivňuje, jak bude server vypadat z pohledu uživatele.
- **access.conf** – Řeší přístup na server. Soubor určuje přístupová práva. Základní příkazy Directory a Options.
- **mime.conf** – obsahuje základní definici přípon souborů a jim odpovídající MINE typů.

V SuSE i ve Windows jsou všechny direktivy z hlediska jednoduchosti implementovány v souboru httpd.conf.

Editace souboru httpd.conf

S souboru httpd.conf se vyskytuje velké množství direktiv. My se soustředíme pouze na ty nejdůležitější, které nám postačí k plné funkčnosti www serveru.

port – určuje na kterém TCP portu bude server naslouchat



User, **Group** – určují přístupová práva serveru, server by v žádném případě neměl pracovat s přístupovými právy superuživatele root! :

```
User ftp
Group nogroup
```

Adresáře a konfigurační soubory

ServerRoot Určuje, ve kterém adresáři server sídlí.

DocumentRoot Říká, kde bude kořen stromu stránek serverem poskytovaných.

ResourceConfig Uvádí cestu k souboru s definicí zdejších zdrojů `srm.conf`.

TypeConfig Definuje jméno souborů s implicitní sadou přípon souborů a jim odpovídajících MINE typů.

AccessConfig Obsahuje cestu k souboru, popisujícímu přístupová práva na server.

ErrorLog Jméno souboru, do kterého server ukládá protokol o chybách, které se během jeho práce objevily.

```
ServerRoot /www
DocumentRoot html
ResourceRoot conf/src.conf
TypeConfig conf/mime.conf
AccessConfig conf/access.conf
ErrorLog logs/error.log
```



Administrativní údaje

ServerName Obsahuje název serveru, přes který se bude pomocí URL volat.

serverAdmin Definuje email adresu správce serveru.

```
ServerName www.firma.cz  
ServerAdmin webmaster@firma.cz
```

Trvanlivost spojení s klientem

TimeOut Vyjadřuje trpělivost serveru, než od klienta dostane dotaz, a poté, než klient potvrdí příjem odpovědi. Nebude-li reagovat server ukončí spojení.

KeepAlive Určuje maximální počet dotazů, které smí klient položit jedním spojením, aby nedošlo k zahlceni systému.

KeepAliveTimeout Maximální délka přestávky mezi dotazy.

Zpracování chyb

Pokud dojde při vyřizování dotazu k chybě. Server odešle stránku, popisující chybu v textové formě. Apache má implicitní podobu definovanou můžeme ji však změnit

ErrorDocument Chybový_kód cesta – např. špatně zadaná cesta chyba 404. Specifikace stránky pro chybu může vypadat takto: `ErrorDocument 404 chyby/chybneURL.html`.



Informace o činnosti serveru

TransferLog soubor Obsahuje informace o dotazech klientů.

AgentLog soubor Každý dotaz přidá jeden řádek, obsahující informace o klientovi.

Cesty a jejich transformace

UseDir Hodnotou příkazu je jméno adresáře, ve kterém budou umístěny jejich soukromé stránky. Zpravidla URL bývá standardně označovány cestou, která začíná znakem ~, bezprostředně následovaným jménem uživatele: ~sekretarka/index.html.

Alias cesta adresář Alias /pub /ftp/pub způsobí, že projeví-li uživatel zájem o dokument s cestou /pub, bude přeměřován do /ftp/pub, který leží mimo váš www strom.

Redirect Slouží k přeměřování klienta na jiný server. Používá se zpravidla v případě, že stránka byla přestěhována úplně jinam:

```
Redirect /books http://www.jinde.cz/books
```

Zpracování adresářů

DirectoryIndex Určuje, který soubor bude odeslán uživateli, který zadá v URL jen adresář nikoli však konkrétní soubor. Implicitní hodnotou je index.html.



Určení typu souborů

Důležitou činností serveru je rozpoznání typu odesílané informace a její oznámení klientovi v http hlavičkách Content-Type a dalších.

```
vlastní jméno.typ.jazyk.kódování
```

Např. jméno `skola.ps.en.gz` v sobě nese informace, že se jedná o dokument v PostScriptu, jazyku anglickém a kódovaný programem gzip. Význam těchto přípon definují po řadě příkazy:

```
AddType MINE typ přípona  
AddLanguage MINE jazyk přípona  
AddEncoding MINE typ přípona
```

Lze uvést i několik přípon, oddělených mezerami.

acces.conf

Soubor určuje přístupová práva. Základní příkazy `Directory` a `Options`.

```
<Directory adresář>  
...  
</Directory>
```

Uvnitř příkazu `Directory` se zpravidla nachází příkaz `Options`, který určuje co je v daném adresáři povoleno.

```
Options volba volba
```

ExecCGI Z adresáře lze spouštět CGI skripty.

FollowSymLinks Server má sledovat symbolické odkazy.



SymLinksIfOwnerMatch Server má sledovat symbolické odkazy pouze když je vlastník odkazu totožný s vlastníkem souboru, na který odkaz vede.

Includes Jsou povoleny vsuvky.

IncludesNOEXEC Jsou povoleny textové vsuvky, nikoliv však vkládání výsledků programů.

Indexes Neobsahuje-li adresář soubor index.html, server automaticky vytvoří menu zdejších souborů.

MultiViews Server má povoleno automatické vyhledávání jazykových verzí dokumentu a dohodu s klientem, kterou mu zašle.

```
<Directory /www/cgi-bin>
Options Indexes FollowSymLinks ExecCGI
</Directory>
<Directory /www/html>
Options Indexes FollowSymLinksIfOwnerMatch
...
</Directory>
```



5 Mail Server - Kerio MailServer

Kerio MailServer je nejmodernější zabezpečený poštovní server s kolaborativními vlastnostmi vhodný pro firemní prostředí malých a středně velkých podniků a nabízející velkou škálu možností využití elektronické pošty poskytovateli služeb.



Kerio MailServer je vedle MS Exchange 2000 jediným řešením poštovního serveru, které nabízí plnou integraci aplikace Active Directory. Kromě interní databáze uživatelů Kerio MailServeru může administrátor spravovat konta pomocí Active Directory ve Windows 2000.

Vedle níže zmiňovaných funkcí Kerio MailServer nabízí např. :

- Zabezpečená pošta
- Antivirová ochrana
- Antispamové funkce
- Přístup k poště odkudkoli pomocí rozhraní WebMail
- Nástroje pro týmovou spolupráci
- Odesílání a příjem faxů
- Komfort pro uživatele
- Jednoduchá správa
- Podpora aplikace Microsoft Active Directory
- Nenáročnost a vysoká dostupnost

5.1 Instalace Microsoft Windows

Po spuštění instalačního programu se zobrazí průvodce s výzvou nastavení jazyka instalace.

Dále následuje dotaz, jaký typ instalace chcete provést:

- *Typická* - kompletní instalace



- *Minimální* - minimální instalace
- *Vlastní* - umožňuje výběr součástí pro *Kerio MailServer*



Obrázek 5.1 Instalace Kerio MailServeru

Poté je automaticky spuštěn vlastní průvodce nastavením základních parametrů serveru – viz obr. 4.1. Po instalaci se spustí konfigurační průvodce, kde zadáte jméno primární domény a doplníte heslo administrátora. Dále je (volitelně ihned nebo po restartu) spuštěn *Kerio MailServer Engine* (běží jako služba na pozadí). To znamená, že vlastní výkonné jádro programu, a *Kerio MailServer Monitor* jej umožňuje zastavovat, spouštět atd... *Kerio MailServer Monitor* se zobrazuje jako ikona na hlavním panelu – viz obr. 4.2.



Obrázek 5.2 MailServer Monitor



5.2 Průvodce počáteční konfigurací

Instalační program v systému Windows automaticky spouští průvodce, který vám pomůže nastavit základní parametry *Kerio MailServeru*. Tohoto průvodce lze vyvolat také kdykoliv později spuštěním programu fgWizard.exe

Primární doména

Aby bylo možno v *Kerio MailServeru* vytvářet uživatelské účty (příp. skupiny atd.), je třeba založit alespoň jednu lokální doménu.



Obrázek 5.3 Vytvoření domény

Instalační průvodce vás v prvním kroku vyzve k zadání jména primární domény – viz obr. 4.3. Má-li *Kerio MailServer* obsluhovat více domén, zvolte za primární tu, v níž má být definován účet pro správu serveru.

Nastavení administrátorského hesla

Velmi důležitým krokem pro zajištění bezpečnosti vašeho serveru je nastavení administrátorského hesla. Heslo nesmí zůstat nevyplněno a mělo by obsahovat alespoň 6 znaků.

Výběr adresáře pro uložení dat

Kerio MailServer za provozu ukládá poměrně značné množství dat na disk (e-mailové zprávy, informace o uživatelských složkách, záznamy...). Adresář pro uložení dat je také možno změnit kdykoliv později v programu *Kerio Administration Console*.

Komponenty Kerio MailServeru



Kerio MailServer sestává z následujících součástí:

Kerio MailServer Engine Vlastní výkonný program, který realizuje všechny služby a funkce. Běží skrytě na pozadí.

Kerio MailServer Monitor Slouží k monitorování a změně stavu *Engine* (zastaven / spuštěn), nastavení spouštěcích preferencí a snadnému spuštění administrační konzole.

Performance Monitor Modul (plug-in) do systémové aplikace *Performance* pro sledování výkonu (resp. zatížení) jednotlivých komponent aplikace *Kerio MailServer*.

Kerio Administration Console Univerzální program pro lokální či vzdálenou správu produktů Kerio Technologies.

Kerio MailServer Monitor

Kerio MailServer Monitor – viz obr. 4.4 je utilita, která slouží k ovládání a monitorování stavu *Mail-Server Engine*. Je-li *Kerio MailServer Engine* zastaven, objeví se přes ikonu červený kruh s bílým křížkem.



Obrázek 5.4 Kerio MailServer Monitor

Dvojitým kliknutím levým tlačítkem na tuto ikonu lze spustit program *Kerio Administration Console* - viz obr. 4.5. Po kliknutí pravým tlačítkem se zobrazí menu, v němž je možno zvolit následující funkce:



Obrázek 5.5 Kerio Administration Console

Startup Preferences Volby pro automatické spuštění *Kerio MailServeru* a *Kerio Mail-Server Monitoru* při startu systému.

Kerio MailServer Administration Tato volba spouští program *Kerio Administration Console*

Start / Stop Kerio MailServer Spuštění nebo zastavení *MailServer Engine*

Exit Ukončení programu *Kerio MailServer Monitor*

Zálohování a přenos konfigurace:

Veškeré konfigurační informace *Kerio MailServeru* jsou nezávislé na operačním systémem a jsou uloženy ve dvou souborech v adresáři, kde je *Kerio MailServer* nainstalován:

- **users.cfg** Informace o uživatelských účtech, skupinách a aliasech.
- **mailserver.cfg** Všechny ostatní konfigurační parametry.

5.3 Administrační program

Kerio Administration Console – viz obr. 4.6 umožňuje lokální správu i vzdálenou správu.



Obrázek 5.6 Kerio Administration Console

Lokální administrace

Spustíte program Kerio Administration Console (z programové skupiny Kerio nebo pomocí utility Kerio MailServer Monitor). Po stisknutí tlačítka *Připojit* v nástrojovém panelu nebo volbou *Akce -> Připojit* se zobrazí dialog pro přihlášení – viz obr. 4.7.



Obrázek 5.7 Dialog pro přihlášení

Nejprve je třeba vybrat typ serverové aplikace, která má být spravována v tomto případě Kerio MailServer.

Zvolte na tomto počítači (lokálně). Kerio Administration Console se bude připojovat k serveru běžícímu na tomtéž počítači (localhost). Zadejte příslušné uživatelské jméno a heslo (při prvním přihlášení použijte administrátorský účet vytvořený při instalaci, standardně jméno admin s heslem, které jste vyplnili v instalačním průvodci).

Tlačítkem *Připojit* se připojíte k aplikaci Kerio MailServer. Po úspěšném přihlášení se v Kerio Administration Console otevře okno pro správu Kerio MailServer Engine.



Vzdálená administrace

Na počítači, odkud se budete vzdáleně připojovat, je nutné nainstalovat program Kerio Administration Console s modulem pro správu Kerio mailServeru.

5.4 Základní nastavení

Služby

V sekci *Konfigurace* -> *Služby* je možno nastavit parametry jednotlivých služeb *Kerio MailServeru*. Tlačítka *Start* a *Stop* umístěnými pod tabulkou lze službu spustit nebo zastavit. Jedná se o následující služby – viz obr. 4.8.

Služba	Stav	Spouštění	Port	Omezení přístupu
SMTP	Spuštěno	Automaticky	25	
POP3	Spuštěno	Automaticky	110	Lokální síť
Zabezpečený POP3	Spuštěno	Automaticky	995	
IMAP	Spuštěno	Automaticky	143	Lokální síť
Zabezpečený IMAP	Spuštěno	Automaticky	993	
Webmail/WAPmail	Spuštěno	Automaticky	80	Lokální síť
Zabezpečený WebMail/WAPMail	Spuštěno	Automaticky	443	
LDAP	Spuštěno	Automaticky	389	
Secure LDAP	Spuštěno	Automaticky	636	

Obrázek 5.8 Služby

Domény

Kerio MailServer umí obsluhovat několik nezávislých poštovních domén. Každá doména přitom může mít libovolný počet aliasů (tzn. ekvivalentních domén).

Definice domén se provádí v sekci *Konfigurace* -> *Domény* – viz obr. 4.9.

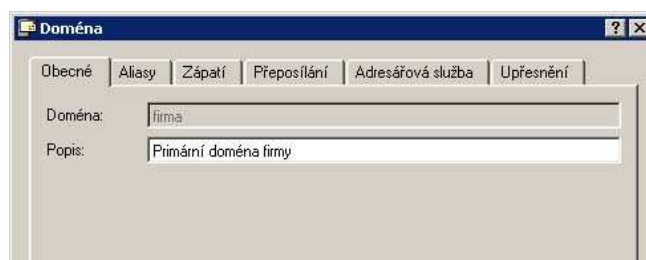
V položce Internetové jméno tohoto serveru by mělo být uvedeno DNS jméno počítače, na němž *Kerio MailServer* běží. Jméno serveru se používá pro identifikaci serveru během SMTP komunikace.



Obrázek 5.9 Domény

Novou doménu je možno vytvořit tlačítkem *Přidat*.

záložka Obecné – viz obr. 4.10:



Obrázek 5.10 Doména – záložka Obecné

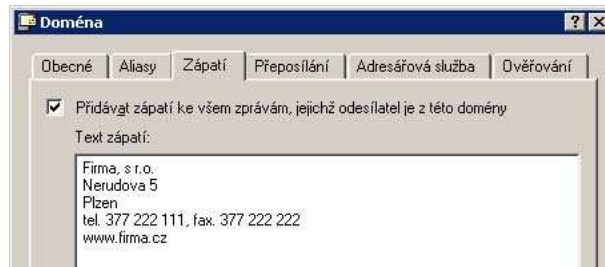
Doména Jméno nové domény.

záložka Aliasy:

V této záložce je možno zadat ekvivalentní domény dané domény.

záložka Zápatí:

Tato záložka poskytuje možnost připojit zápatí ke každé zprávě poslané z této domény – viz obr. 4.11.

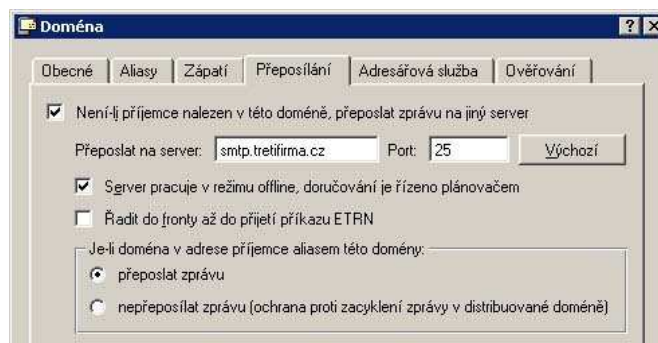


Obrázek 5.11 Doména – záložka Zápatí

záložka Přeposílání:

Záložka *Přeposílání* umožňuje přeposílání zpráv na jiný SMTP server – viz obr. 4.12.

Přeposlat na server DNS jméno nebo IP adresa SMTP serveru, na který budou zprávy přeposílány.



Obrázek 5.12 Doména – záložka Přeposílání

záložka Adresářová služba:

Kerio MailServer může kromě vlastní (interní) databáze uživatelských účtů pracovat také s účty a skupinami, které jsou uloženy v LDAP databázi (v současné době jsou podporovány databáze *Microsoft Active Directory* a *Apple OpenDirectory*).

Mapovat uživatelské účty a skupiny... Volba vypíná/zapíná spolupráci s LDAP databází.



Typ adresářové služby Typ LDAP databáze, kterou bude tato doména používat (*Active Directory*).

Jméno serveru DNS jméno nebo IP adresa serveru, na němž LDAP databáze běží.

Uživatelské jméno Jméno uživatele (ve tvaru tomik@firma.cz), který má práva pro čtení LDAP databáze.

Heslo Heslo uživatele, který má práva pro čtení LDAP databáze.

Jméno Active Directory domény... Pokud se název domény liší od názvu v *Active Directory*, zaškrtněte volbu a doplňte její jméno do pole *Jméno Active Directory domény*.

Mapovat uživatelské účty a skupiny... Volba vypíná/zapíná spolupráci s LDAP databází (je-li tato volba vypnuta, v doméně bude možno vytvořit pouze lokální účty).

Typ adresářové služby Typ LDAP databáze, kterou bude tato doména používat (*Apple Open Directory*).

Jméno serveru DNS jméno nebo IP adresa serveru, na němž LDAP databáze běží.

Uživatelské jméno Jméno uživatele, který má práva pro čtení LDAP databáze.

Heslo Heslo uživatele, který má práva pro čtení LDAP databáze.

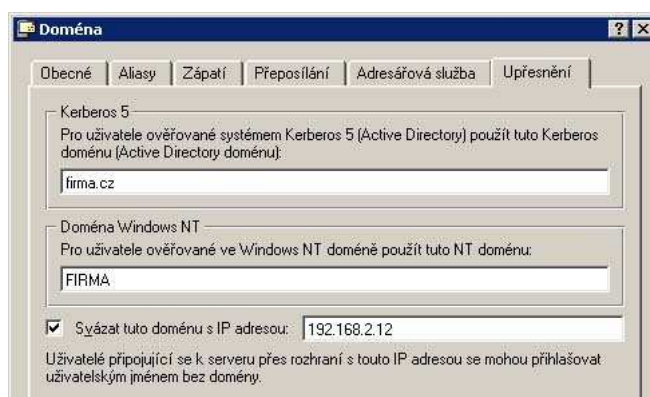


Přípona pro prohledávání LDAP databáze Pokud je zvolen v položce *Typ adresářové služby Apple OpenDirectory*, doplňte do této položky příponu ve tvaru:

dc=subdomena , dc=domena

záložka Uřesnění:

V záložce *Upřesnění* – viz obr. 4.13 je možno nastavit parametry ověřování uživatelů pro vytvářenou doménu:



Obrázek 5.13 Doména – záložka Upřesnění

Kerberos 5 Název oblasti (domény) systému Kerberos, v níž mají být uživatelé ověřováni. V případě ověřování ve Windows 2000 doméně (*Active Directory*) je třeba zde uvést název této domény (např. firma.cz).

Doména Windows NT NT doména, v níž budou uživatelé ověřováni. Počítač, na němž *Kerio MailServer* běží, musí být přidán do této domény.

Svázat s IP adresou V této položce je možno uvést IP adresu rozhraní počítače, na němž *Kerio MailServer* běží.



5.5 Nástroje

Vytvoření či úprava skupiny IP adres

Definice skupin IP adres – viz obr. 4.14 se provádí v sekci *Konfigurace* -> *Definice* -> *Skupiny IP adres*.



Obrázek 5.14 Skupiny IP adres

Nastavení vzdálené správy

Chcete-li *Kerio MailServer* spravovat z jiného počítače, než na kterém běží, je třeba povolit vzdálenou administraci. Komunikace mezi *Kerio MailServerem* a *Kerio Administration Console* je chráněna silným šifrováním, takže vzdálená správa je bezpečná a přenášená data nemohou být odposlechnuta a zneužita. Přístup ke správě by měl vždy být chráněn heslem, přesto lze ochranu ještě zesílit povolením vzdálené správy pouze z určitých IP adres.

Nastavuje vzdálené administrace se provádí v sekci *Konfigurace* -> *Vzdálená správa*.

5.6 Uživatelské účty a skupiny

Uživatelské účty

Uživatelské účty v *Kerio MailServeru* reprezentují fyzické e-mailové schránky. Uživatelské jméno a heslo tedy slouží jako ověření přístupu k této schránce.

Definice uživatelských účtů – viz obr. 4.15 se provádí v sekci *Nastavení domény* -> *Uživatelské účty*.



Obrázek 5.15 Definice uživatelských účtů

Nejprve je nutno v poli *Doména* vybrat lokální doménu, v níž mají být účty definovány. V každé doméně mohou existovat jednak lokální účty, jednak účty uložené v LDAP databázi (např. *Microsoft Active Directory*).

- *Interní* - účet je definován pouze v *Kerio MailServeru* (je uložen v jeho interní databázi)
- *LDAP* - účet je uložen v LDAP databázi (*Active Directory*)

Vytvoření lokálního uživatelského účtu se provádí následujícím průvodcem.

1. základní údaje:

Jméno Přihlašovací jméno (pozor: nejedná-li se o lokální doménu).

Celé jméno Plné jméno (typicky jméno a příjmení daného uživatele).

Ověřování Způsob ověřování uživatele (viz dále).

Účet je zablokován Dočasné zrušení „vypnutí“ účtu bez nutnosti jej odstraňovat.

možné způsoby ověřování:



Interní databáze uživatelů Uživatel je ověřován pouze v rámci *Kerio MailServeru*. V tomto případě je potřeba zadat heslo do položek *Heslo* a *Potvrzení hesla*..

Doména Windows NT Uživatel bude ověřován v doméně Windows NT.

Kerberos 5 Ověření se provede pomocí ověřovacího systému Kerberos verze 5. Tento způsob ověřování používá doména Windows 2000 (*Active Directory*).

2. e-mailové adresy

V tomto kroku průvodce je možno zadat všechny požadované e-mailové adresy daného uživatele.

3. přeposílání zpráv na jiné adresy

Zprávy pro uživatele mohou být volitelně přeposílány na další e-mailové adresy.

4. skupiny

V tomto dialogu je možno (tlačítka *Přidat* a *Odebrat*) přidat nebo odebrat skupinu, do níž má být uživatel zařazen.

5. přístupová práva

Každý uživatel musí mít nastaveny přístupové práva.

- **Přístup jen pro čtení**
- **Přístup pro čtení a zápis**

6. kvóty:

Uživateli lze nastavit určitá omezení na jeho poštovní schránku.



Diskový prostor Maximální prostor ve schránce.

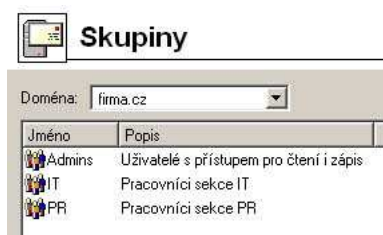
Počet zpráv Maximální počet zpráv ve schránce. Další zprávy budou již serverem odmítány.

7. parametry rozhraní *Webmail*

Toto nastavení nebudeme používat, jedná se o nastavení parametrů rozhraní Webmail.

Skupiny uživatelů

Definice skupin uživatelů – viz obr. 4.16 se provádí v sekci *Nastavení domény* -> *Skupiny*.



Obrázek 5.16 Definice skupin uživatelů

5.7 Odesílání a příjem pošty

Parametry pro doručování

Parametry pro doručování lze nastavit v sekci *Konfigurace* -> *Fronta zpráv* ve dvou záložkách:

záložka SMTP doručování má tyto možnosti:

- Doručovat přímo dle DNS MX záznamů
- Použít nadřazení SMTP server



záložka Volby pro frontu má tyto možnosti:

- Nastavení fronty zpráv
- Notifikace o stavu doručování

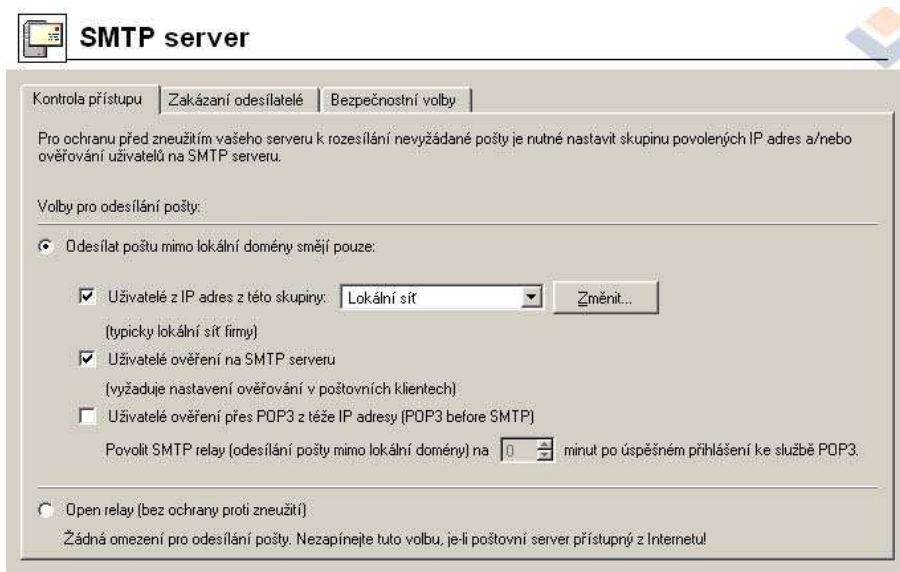
SMTP server

Nastavení parametrů SMTP serveru se provádí v sekci *Konfigurace* -> *SMTP server*. Tato nastavení chrání server na němž běží Kerio MailServer proti zneužití.

Kerio MailServer obsahuje ochranu, která umožňuje definovat, kdo smí přes tento server odesílat e-maily a kam. V principu se může na SMTP server připojit kdokoliv, aby poslal e-mail do některé z lokálních domén. Odesílat e-maily do jiných domén naopak smějí pouze oprávnění (typicky lokální) uživatelé.

záložka Kontrola přístupu

V záložce *Kontrola přístupu* je možno nastavit skupinu povolených IP adres a/nebo ověřování uživatelů na SMTP serveru – viz obr. 4.19.



Obrázek 5.17 SMTP server - záložka Kontrola přístupu

Odesílat poštu mimo lokální domény směřjí pouze Tato volba zapíná režim ověřování odesílatelů dle IP adresy nebo jména a hesla.

- **Uživatelé z IP adres z této skupiny** Zde je možno nastavit skupinu IP adres, z nichž bude možno odeslat e-mail do libovolné domény. V poli *Skupina IP adres* se zobrazují skupiny definované v sekci *Konfigurace / Definice / Skupiny IP adres*.
- **Uživatelé ověření na SMTP serveru** Právo odeslat e-mail do libovolné domény budou mít uživatelé, kteří budou na SMTP serveru ověření uživatelským jménem a heslem. Tuto možnost mají tedy všichni uživatelé, kteří mají v *Kerio MailServeru* vytvořen svůj uživatelský účet.
- **Uživatelé ověření přes POP3 z téže IP adresy** Volba umožňuje uživatelům ověřeným POP3 (uživatelské jméno a heslo), aby se při odesílání pošty nemuseli ověřovat po dobu zadanou v poli *Povolit*



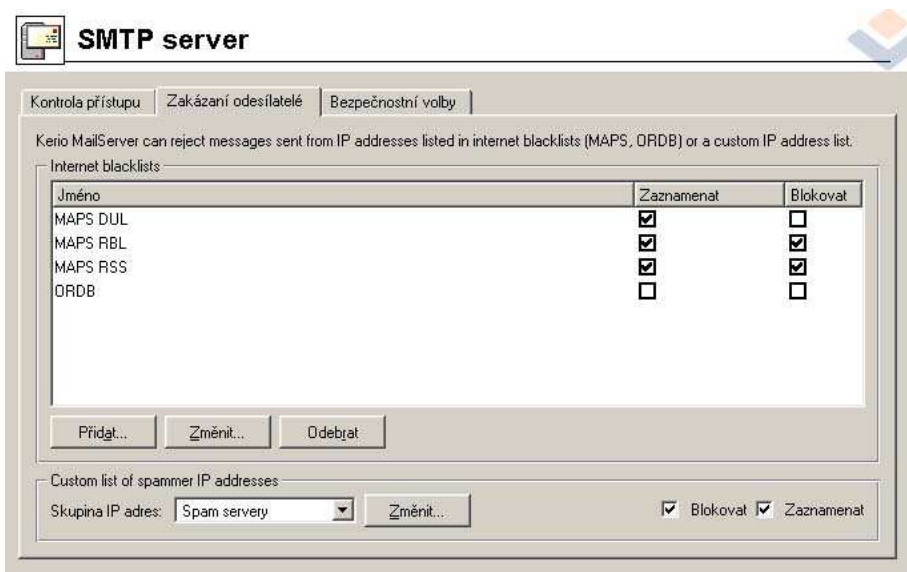
SMTP relay na ... minut po úspěšném přihlášení ke službě POP3 na SMTP server.

Open relay Je-li zvolen tento režim, pak SMTP server nekontroluje uživatele, kteří přes něj odesílají e-mail. Libovolný uživatel tedy může odeslat e-mail do libovolné domény.

záložka Zakázání odesílatelů

Kerio MailServer umožňuje také blokovat příjem zpráv ze serverů, o nichž bylo zjištěno, že rozesílají nevyžádané e-maily. Přitom umí využít veřejné internetové databáze těchto serverů nebo vlastní – viz obr. 4.20.

Definice parametrů této ochrany se provádí v sekci *Konfigurace -> SMTP server, záložka Zakázání odesílatelů*.

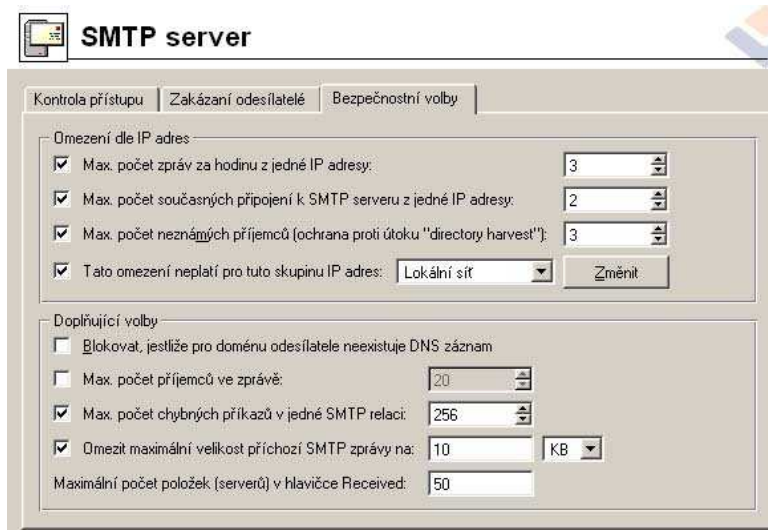


Obrázek 5.18 SMTP server - záložka Kontrola přístupu

Záložka Bezpečnostní volby



Kromě úplného blokování určitých odesílatelů umožňuje *Kerio MailServer* nastavit také obecná omezení, která nebrání v odesílání pošty, ale zamezují např. zahlcení serveru dávkovým odesíláním velkého počtu zpráv či navázáním velkého počtu spojení (tzv. DoS útok) – viz obr. 4.21.



Obrázek 5.19 SMTP server - záložka Bezpečnostní volby

Max. počet zpráv za hodinu ... Maximální počet zpráv, který smí být odeslán z jedné IP adresy během jedné hodiny.

Max. počet současných připojení k SMTP ... Maximální počet současných TCP spojení na port SMTP serveru z jedné IP adresy.

Max. počet neznámých příjemců ... Directory harvest je typ spamového útoku, kdy se na váš SMTP server napojí aplikace generující pomocí slovníků pravděpodobných uživatelských jmen adresy příjemce. Zaškrtnutím položky a doplněním příslušného čísla zajistíte, aby server, který posílá zprávy na neznámého příjemce byl na jednu hodinu zablokován.

Tato omezení neplatí pro tuto skupinu IP adres Skupina IP adres, na niž se výše uvedená omezení nevztahují. Zpravidla to bývá skupina lokálních uživatelů. Tito uživatelé odesílají přes *Kerio MailServer* veškerou svou



odchozí poštu - počet zpráv odeslaných na tento server je proto výrazně vyšší než v případě vnějších uživatelů (serverů), kteří jej používají pouze pro odeslání pošty do některé z lokálních domén.

Blokovat, jestliže pro doménu odesílatele... Při přijetí zprávy *Kerio MailServer* zkontroluje, zda pro doménu odesílatele existuje záznam v DNS, a pokud ne, zprávu odmítne. Toto je ochrana proti smyšleným adresám odesílatelů.

Max. počet příjemců ve zprávě Maximální akceptovatelný počet adresátů v e-mailové zprávě.

Max. počet chybných příkazů ... Spamy jsou často rozesílány speciální aplikací, která se připojí na SMTP server a nebere ohled na chybová hlášení serveru. Po nastavení této volby *Kerio MailServer* automaticky ukončí SMTP spojení, jestliže klient již vyslal daný počet chybných příkazů.

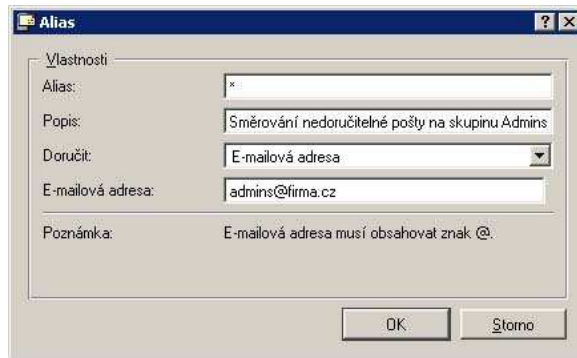
Omezit maximální velikost příchozí SMTP zprávy na Maximální velikost zprávy, kterou SMTP server akceptuje.

Maximální počet položek (serverů) v hlavičce Received Nastavení tohoto parametru slouží především k zablokování zprávy, která se „zacyklila“ mezi několika SMTP servery.

Alias

Alias slouží k vytváření tzv. virtuálních e-mailových adres.

Definice aliasů – viz obr. 4.22 se provádí v sekci *Nastavení domény* -> *Alias*.



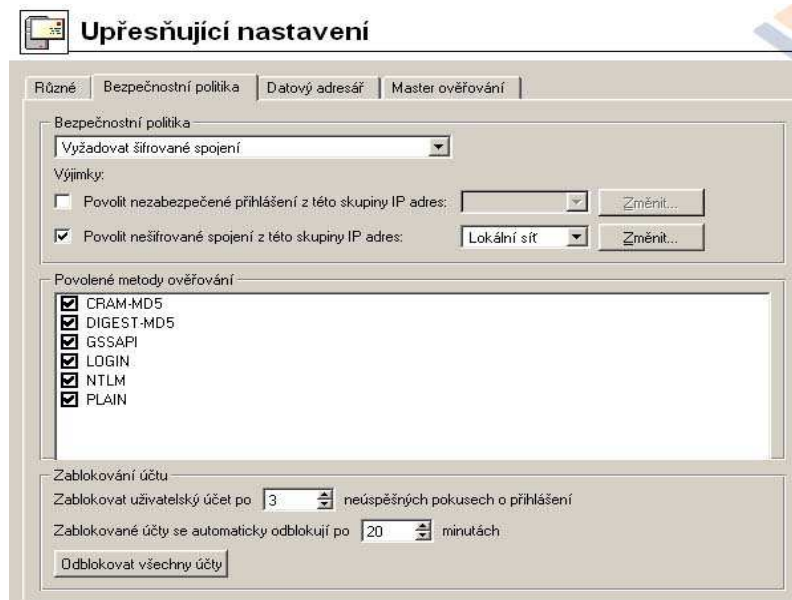
Obrázek 5.20 Definice aliasů

Upřesňující nastavení

V sekci *Konfigurace* -> *Upřesňující nastavení* lze nastavit některé upřesňující parametry poštovního serveru.

Záložka Bezpečnostní politika

Kerio MailServer umožňuje nastavení bezpečnostní politiky – viz obr. 4.23, tzn. minimální požadované úrovně bezpečnosti. Tato nastavení se provádějí v sekci *Konfigurace* -> *Upřesňující nastavení* .

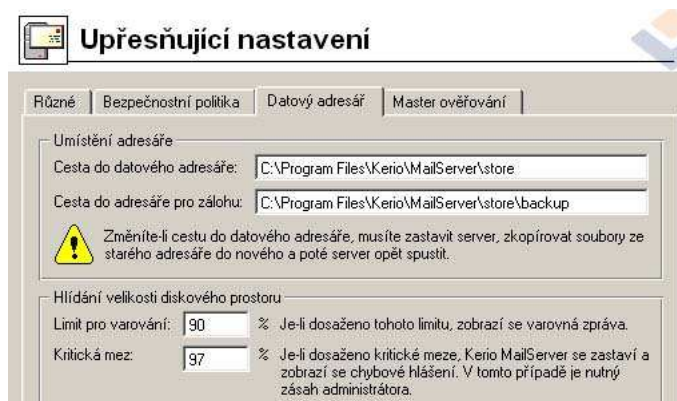


Obrázek 5.21 Upřesňující nastavení - záložka Bezpečnostní politika



Záložka Datový adresář

V záložce *Datový adresář* – viz obr. 4.24 je možno nastavit adresáře pro ukládání zpráv (uživatelské a veřejné složky) a pro zálohování. Do *datového adresáře* se ukládají zprávy v uživatelských a veřejných složkách, záznamy, zprávy k odeslání a soubory, které se právě kontrolují antivirovým programem.



Obrázek 5.22 Upřesňující nastavení - záložka Datový adresář

Záložka Master ověřování

Kerio MailServer umožňuje nastavit univerzální heslo (tzv. *Master Password*), které je možno použít pro přístup k libovolné schránce protokoly IMAP a POP3. Toto heslo lze využít v případech, kdy mají s *Kerio MailServerem* spolupracovat speciální aplikace, které přistupují do velkého počtu schránek. V takové aplikaci pak není nutno zadávat heslo pro každou schránku - stačí uvést heslo *Master Password* – viz obr. 4.25.

Nastavení Master ověřování se provádí ve stejnojmenné záložce sekce *Upřesňující nastavení*.



Obrázek 5.23 Upřesňující nastavení - záložka Master ověřování



6 MailServer – Postfix

Postfix je bezplatný volně šiřitelný software. Vznikl jako alternativa na nejrozšířenější Sendmail. Postfix je rychlejší, snadno spravovatelný, bezpečný a zároveň kompatibilní s Sendmailem pro uživatele.



Kromě níže zmiňovaných funkcí samotného Postfixu může spolupracovat s:

- Amavis (A Mail Virus Scanner) antivirus
- Clamav virus detektorem
- SpamAssassinem antisпамem s online spamovými databázemi Razor a DCC
- atd..

6.1 Přípravy před instalací

Odstranění Sendmailu

Důležité je aby byl před instalací Postfixu odstraněn ze systému mailový server Sendmail. Tak aby nedošlo ke konfliktu těchto dvou programů. Sendmail se nachází v `/usr/libexec/sendmail/sendmail`. Můžete pomocí YaST nebo z příkazové řádky příkazem:

```
# rm /usr/sbin/sendmail
```

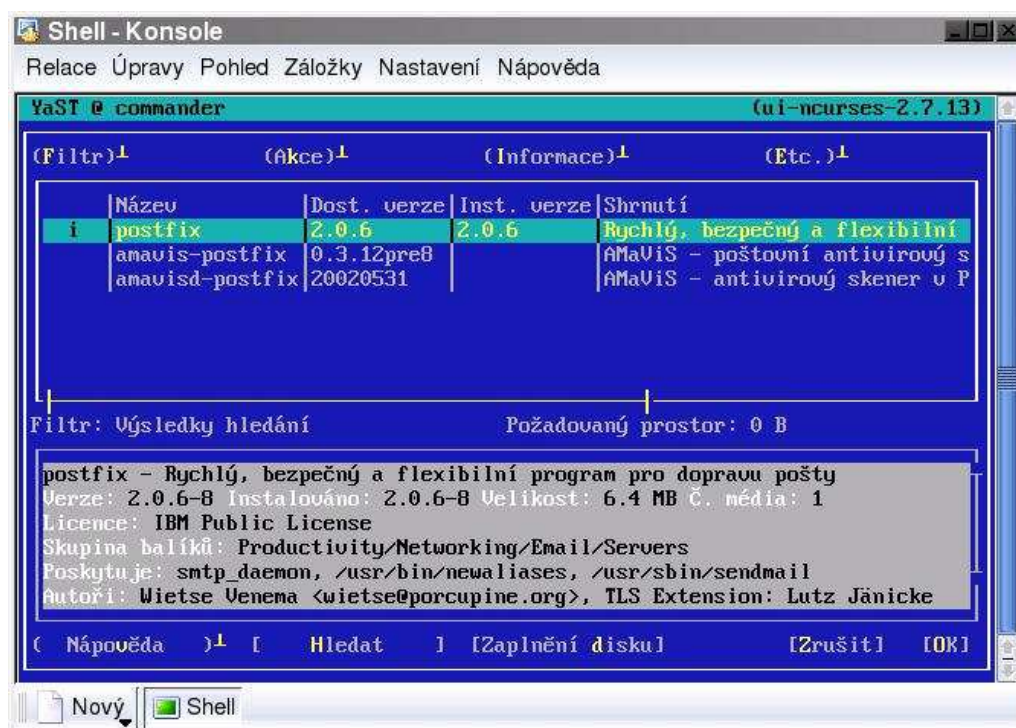


6.2 Instalace Postfixu

Postfix je možno nainstalovat jak binárně tak pomocí YaST. SuSE má Postfix jako implicitní mailový server tzn. že Postfix by měl být již nainstalován pokud jste dávali standardní instalaci.

6.2.1 Instalace pomocí YaST2

Instalace pomocí Yast2 je výhodnější SuSE má již předkompilovanou verzi odladěnou pro tento operační systém. Stačí tedy pouze spustit YaST a nainstalovat tento balíček – viz obr. 5.1, pokud již není standardně nainstalovat s instalací OS.



Obrázek 6.1 YaST instalace Postfix

6.2.2 Binární instalace

Stažení poslední verze postfixu do /root a zkompilevat.



```
# cd /root
# ftp
http://postfix.energybeam.com/source/official/postfix-2.0.16.tar.gz
# tar -zxvf postfix-2.0.16.tar.gz
# cd postfix-2.0.16
# make
```

Instalace a odpovědi na otázky:

```
# make install
```

Answers (most will be the defaults)

```
install_root: /
tempdir: [/root/postfix-2.0.7] or whichever directory the source is in
configdir: /etc/postfix
daemondir: /usr/libexec/postfix
commanddir: /usr/sbin
queuedir: /var/spool/postfix
sendmailpath: /usr/sbin/sendmail
newaliases path: /usr/bin/newaliases
mailq path: /usr/bin/mailq
mail owner: postfix
setgidgroup: postdrop
man page dir: /usr/local/man
sample dir /etc/postfix
readme no
```



6.3 Konfigurace Postfixu

Editace konfiguračního souboru postfixu `/etc/postfix/main.cf`

```
#
# >>>>>>>>> You must restart postfix after editing this
file
# >> NOTE >> to do this use the command:
# >>>>>>>>> # postfix stop;postfix start
#

queue_directory = /var/spool/postfix
daemon_directory = /usr/libexec/postfix

mail_owner = postfix

myhostname = server.firma.cz
mydomain = firma.cz
myorigin = $myhostname
mydestination = $myhostname, localhost.$mydomain,
$mydomain, mail.$mydomain
mynetworks = 10.0.0.0/8, 65.0.0.0/24, 127.0.0.0/8

inet_interfaces = all

header_checks = pcre:/etc/postfix/header_checks

local_recipient_maps =
biff = no
empty_address_recipient = MAILER-DAEMON
queue_minfree = 8000000
message_size_limit = 20000000
mailbox_size_limit = 100000000

smtpd_banner = $myhostname ESMTTP
```



```
transport_maps = hash:/etc/postfix/transport
local_transport = local

smtpd_recipient_restrictions = permit_mynetworks,
reject_unauth_destination, reject_non_fqdn_recipient
#some people also add reject_non_fqdn_sender (but I have
clients that break this rule that I need to receive from)

notify_classes =
2bounce,policy,protocol,resource,software

#content_filter = smtp-amavis:[127.0.0.1]:10024

# Install Time Configuration
sendmail_path = /usr/sbin/sendmail
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
setgid_group = postdrop
manpage_directory = /usr/local/man
sample_directory = /etc/postfix
readme_directory = no
```

queue_directory Udává pracovní adresář. Kde všechna přijatá pošta bude dočasně uložena do té doby , než to je dodána adresátovy.

daemon_directory Specifikuje umístění postfixových programů.

mail_owner Specifikuje uživatelský účet, který bude vlastnit frontu zpráv.

Nastavení hostitelského jména

myhostname Jméno tohoto počítače včetně doménové části. Používá se v záhlaví emailu.



Nastavení jména domény

mydomain Specifikuje doménu počítače.

Nastavení jakou doménu použít pro odchozí poštu

myorigin Toto jméno je přidáno k lokálnímu emailu. Takže jestliže jste poslali zprávu jako root, objevilo se přijato z root@firma.cz.

Nastavení domén pro přijímání

mydestination Toto nastavení říká postfixu jaké domény bude přijímat. Nejedná se užití virtuální domény, nebo pro zálohování MX hostitelé. V našem případě, nastavíme na:

```
neco@server.firma.cz ,  
neco@localhost.firma.cz ,  
neco@firma.cz ,  
neco@mail.firma.cz
```

Ohlašování potíží postmasteru

notify_classes Toto nastavení říká Postfixu jaké druhy zpráv poslat na postmastrův účet. Tady je seznam dostupných voleb:

- **bounce**:(odrazit se) Poslat kopie záhlaví odražené pošty.
- **2bounce**: Poslat nedoručitelný poštu.
- **delay**: (zpoždění) Poslat kopie záhlaví zpožděné zprávy.
- **policy**:(politika) Poslat přepis veškerého SMTP session, když klientova žádost byla odmítnutá kvůli (UCE) politice.



- **protocol:**(protokol) Poslat přepis všech SMTP session v případě chybovému protokolu klienta nebo serveru.
- **resource:**(zdroj) Informovat o nedoručení kvůli problému na zdroji.
- **software:**(software) Informovat o nedoručení kvůli softwarovému problémům.

Nastavení sítě

mynetworks Udává seznam všech sítí, kterým může postfix věřit. Pro rozpoznání SMTP klientů který mají povoleno přenos pošty skrz Postfix.

Toto nastavení říká Postfixu jakou síť považovat za místní. Další parametry jsou počítače v síti od nichž bude možnost přenášet poštu.

V našem případě, jsme dali 127.0.0.0 (pro místního hostitele), 65.0.0.0 (pro jiné počítače na naší externí síti), a 10.0.0.0 (pro jakýkoliv vnitřní počítač).

Význam stylů:

- **class:** (třída) Věřit SMTP klientům ve třídě /B/C.
- **subnet:**(pod-síť) Standardní nastavení. Věřit SMTP klientům v pomocné síti.
- **host:**(hostitel) Věřit jen místním.

Nastavení virtuálních adres

inet_interfaces Parametr specifikuje všechny síťové rozhraní adres kde by Postfix měl naslouchat. Standard je naslouchat na všech aktivních rozhráních. `inet_interfaces = virtual.host.tld` (virtuální doména).

Nastavení filtrování zpráv



header_checks Parametr filtrování podle záhlaví zprávy.

body_checks Parametr filtrování podle těla zprávy.

smtpd_helo_restrictions,

smtpd_sender_restrictions,

smtpd_recipient_restrictions Toto nastavení je užíváno pro popření přístupu k Postfixu založeným na HELO příkazu, odesílatel, nebo příjemce.

Normálně toto nastavení může být užíváno pro NEVYŽÁDANÝ E-MAIL.

Nastavení limitů a velikostí zprávy

queue_minfree Toto nastavení říká postfixu nepřijmout jakoukoliv zprávu jestliže je méně než v našem příkladě 8Mb místa na disku.

message_size_limit Nastaví maximální velikost zprávy. Zprávy větší než udaná hodnota bude odmítnuta.

mailbox_size_limit Nastaví maximální velikost místní poštovní schránky.

Ostatní nastavení

local_recipient_maps Toto nastavení říká Postfixu kde najít jména místních uživatelů a přijmout pro ně poštu.

biff Nastavení říká Postfixu nepoužít biff program, oznámit místním uživatelům, že mají nový email.

empty_address_recipient Toto nastavení je cíl pro nedoručitelný zprávy

<>



smtpd_banner Standarta zobrazená spojovacím počítačům. Z hlediska bezpečnosti neuvádět moc informací.

transport_maps Toto nastavení říká postfixu kde najít zaslací informace.

local_transport Toto nastavení říká postfixu že všechny místní zprávy by měl doručit místním doručovacím agentem.

Install Time Configuration V této části uvádíme nastavení, kdy jsme instalovali Postfix.

Editace souboru /etc/postfix/master.cf

Dále editujeme /etc/postfix/master.cf soubor změnit nastavení pro všechny základní postfixové služby z 'n' to 'y'.

```
#=====
# service  type  private  unpriv  chroot  wakeup  maxproc  command  +
#          (yes)  (yes)   (yes)   (never) (100)
#=====
```

service	type	private	unpriv	chroot	wakeup	maxproc	command	args
smtp	inet	n	-	y	-	-	smtpd	
pickup	fifo	n	-	y	60	1	pickup	
cleanup	unix	n	-	y	-	0	cleanup	
qmgr	fifo	n	-	y	300	1	qmgr	
rewrite	unix	-	-	y	300	-	trivial- rewrite	
bounce	unix	-	-	y	-	0	bounce	
defer	unix	-	-	y	-	0	bounce	
flush	unix	n	-	y	1000?	0	flush	
proxymap	unix	-	-	n	-	-	proxymap	
smtp	unix	-	-	y	-	-	smtp	
relay	unix	-	-	y	-	-	smtp	
showq	unix	n	-	y	-	-	showq	



error	unix	-	-	y	-	-	error
local	unix	-	n	n	-	-	local
virtual	unix	-	n	n	-	-	virtual
lmtp	unix	-	-	y	-	-	lmtp

Nastavení aliasů

Do souboru `/etc/postfix/aliases` uvedeme mailové aliasy, které potřebujeme. Když máme soubor upravený, vygenerujeme z textového souboru hash databázi příkazem `postalias`:

```
# vi /etc/postfix/aliases
```

```
# Postfix User
postfix:  root
# Person who should get root's mail
root:    root@firma.cz
marus   sekretarka@firma.cz
reditel tomik@firma.cz
```

```
# postalias /etc/postfix/aliases
```

Nastavení klientů

Vytvoříme soubor `/etc/postfix/local` a napíšeme do něj seznam domén a adres (na každý řádek jednu), které server bude považovat za cílové adresy.

```
# mkdir local
```



Podobně vytvoříme soubor `/etc/postfix/mynetworks`, který bude obsahovat adresy klientů, pro které budeme maily posílat kamkoliv. Příklad souboru:

```
# mkdir mynetworks
```

```
217.13.91.0/23
10.0.0.0/8
127.0.0.0/8
```

Spuštění Postfixu

Postfix spustíme direktivou:

```
/usr/sbin/postfix start
```

Test připojení k SMTP portu

Nyní se ujistíme, že se můžeme připojit k SMTP rozhraní na port 25 a port 10025. Použijeme tento příkaz:

```
# telnet localhost 25
```

```
The server should respond with:
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mta1.domain.com ESMTP
press ctrl-], then type 'quit' to quit
```

Literatura a ostatní použité zdroje

- [1]Dostálek, Libor a Kabelová, Alena: *Velký průvodce protokoly TCP/IP a systémem DNS*, 3. vyd. Praha, Computer Press 2002, ISBN 80-7226-675-6
- [2]Pecinoský, Josef: *Windows 2000 Server podrobný průvodce začínajícího uživatele*, 1. vyd. Praha, Grada Publishing, Praha 2000, ISBN 80-7169-941-1
- [3]*LINUX Dokumentační projekt* , 1. vyd. Praha, Computer Press 1998, ISBN 80-7226-114-2
- [4]Dirsch, Stefan a kol.: *SuSE Linux systémová a referenční příručka*, SuSE Linux AG. 2002
- [5]Pecinoský, Josef: *Apache.....*, 1. vyd. Praha, Grada Publishing, Praha 2000, ISBN 80-7169-941-1
- [6]Roubal, Zdeněk: *LINUX MultiBOOT, RedHat, Apache, ZČU FAV* 1997
- [7] Kerio MailServer 5 Příručka administrátora, Kerio Technologies 2003

Internetové zdroje

- <http://www.abclinuxu.cz>
- <http://www.root.cz>
- <http://www.windows.cz>
- <http://www.kerio.cz>
- <http://www.suse.cz>
- <http://www.suse.com>
- <http://www.postfix.org>