Linux jako firemní server

1 Výběr správné distribuce

Před instalací a samotným výběrem, je třeba zvážit, jakou linuxovou distribuci použijeme. Pokud jsme velká firma a budeme do budoucna provozovat několik serverů, je vhodné zvolit např. SLES, nebo RHEL, popř. i použít Debian. Určitě se nevyplatí používat Gentoo, jehož správa je při velkém počtu serverů časově náročná.

Pro ukázky budu používat systém Debian Etch

2 Instalovaný a používaný software

Pro použití ve small business segmentu je vhodné použít tyto aplikace:

IPTables – firemní firewall
DHCPd – DHCP server
Samba – pro sdílení dokumentů (sítové disky)
Pure-FTPd – pro možnost sdílení dat s klienty
Postfix – pro předávání systémové pošty

3 Popis, instalace a konfigurace jednotlivých součástí serveru

3.1 Instalace distribuce – holý systém

Nainstalujeme zvolenou distribuci. Pokud máme při instalaci možnost zvolit, jaké balíky (aplikace) se mají instalovat, zvolíme jich co nejméně. Vše potřebné si raději doinstalujeme sami, aby v systému nebyly zbytečnosti

3.2 Rozložení disku

Ze zkušenosti doporučuji pro / užít minimálně 10GB. V případě, že je /var na vlastním oddílu, je možno použít pro / méně. Ale nedoporučuji méně, jak 6GB (člověk nikdy neví, co bude potřebovat).

Jako úložiště firemních dat, je vhodné použít RAID pole. Pokud server nemá hardwarový RAID řadič, netřeba zoufat, lze použít softwarový RAID. Je třeba jej zkompilovat do jádra + nainstalovat obslužné aplikace. Těch je na výběr více, ale doporučuji mdadm.

3.2.1 Vytvoření RAID1 pole

Vytvoření oddílu typu fd (Raid autodetect) se stejnou velikostí. Nad nimi budeme vytvářet pole. Pole lze vytvořit i nad celým diskem, ale je vhodnější jej vytvořit nad oddílem – při jiné velikosti jednoho z disků by mohly nastat zbytečné komplikace.
Vytvoření RAID pole následujícím příkazem: mdadm --create --verbose /dev/md1 --level=1 --raid-devices=2 /dev/sda1 /dev/sdb1
Poté již můžeme připojit RAID pole standardním způsobem (používáme /dev/md1)

3.3 IPTables

3.3.1 Popis

IPTables slouží jako firewall. Namátkou z jeho možností je blokování portů, překklad adres (NAT), zaznamenávání packetů, a. j.

3.3.2 Instalace

Iptables bývají součástí systému. Pro jejich správnou činnost je potřeba povolit (zavést) patřičné moduly do jádra. V systému RHEL lze použít pro konfiguraci utilitu system-config-security

3.3.3 Nastavení

Pro funkci NATu používám tento konfigurační skript, který z venku (eth2) dovnitř pustí pouze FTP a dělá maškarádu na tomto rozhraní

```
#spravna cesta !!!
where=/sbin

$where/iptables –F
$where/iptables –X
$where/iptables –Z

$where/iptables -t nat –F
$where/iptables -t nat –X
$where/iptables -t nat –Z

$where/iptables -A INPUT -i ! lo -j DROP
$where/iptables -A FORWARD -i ! lo -j DROP

$where/iptables -P INPUT DROP
$where/iptables -P OUTPUT DROP
$where/iptables -P FORWARD DROP

#Creating of CHAIS
#.PortTcpDI
#-------DI------
$where/iptables -N DI #data do kernelu
$where/iptables -N DO #data z kernelu

$where/iptables -N WI #data z internetu (UPC)
$where/iptables -N WO #data do internetu (UPC)

$where/iptables -A INPUT -i lo -j ACCEPT
$where/iptables -A OUTPUT -o lo -j ACCEPT

# vnitrni sit
$where/iptables -A INPUT -i eth0 -j DI
$where/iptables -A OUTPUT -o eth0 -j DO

#vnejsi sit
$where/iptables -A INPUT -i eth2 -j WI
$where/iptables -A OUTPUT -o eth2 -j WO

#=============================================================================

#povoleni prichoziho trafficu z venci
$where/iptables -A WI -p all -m state --state ESTABLISHED,RELATED  -j ACCEPT
$where/iptables -A WI -p tcp -m state --state NEW --destination-port 21 -j
ACCEPT #ftp
$where/iptables -A WI -p icmp -j ACCEPT
$where/iptables -A WI -p tcp --dport 113 -j REJECT

#povoleni prichoziho trafficu z vnitrni site
$where/iptables -A DI -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
$where/iptables -A DI -p icmp -s 192.168.1.0/24 -j ACCEPT
$where/iptables -A DI -p all -s 192.168.1.0/24 -j ACCEPT #povoluje zname hosty

#--------------Data -> OUT-----------------------------------------------------

#do vnitrni site cokoliv
$where/iptables -A DO -p all -j ACCEPT
#do vnejsi site cokoliv
$where/iptables -A WO -p all -j ACCEPT
```

```
#MASQUERADE
$where/iptables -t nat -A POSTROUTING -p all -s 192.168.1.0/24 -o eth2 -j
MASQUERADE  #NATka

#FORWARD - zde nemuze kazdy co chce kam chce
$where/iptables -A FORWARD -p all -i eth2 -o eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
$where/iptables -A FORWARD -p all -i eth0 -o eth2 -s 192.168.1.0/24 -j ACCEPT

#misto NATu na lokalnim interface

$where/iptables -D INPUT 1
$where/iptables -D FORWARD 1
```

3.4 DHCPd

3.4.1 Popis

DHCPd je server, který předává klientským počítačům automaticky informace o nastavení sítě (IP adresa, maska, gateway, …)

3.4.2 Instalace

Pokud ISC server DHCPd není nainstalován, nainstalujeme jej následujícím příkazem:

```
apt-get install dhcp
```

3.4.3 Konfigurace

Konfigurační soubor se nachází v /etc/dhcp/dhcpd.conf

Mezi nejdůležitější části patří sekce subnet, která popisuje (nastavuje) parametry, které budou předávány klientům v daném subnetu. Další důležitou částí je sekce host, která popisuje jednotlivé (statické) klienty.

V ukázce konfigurace je situace, kdy se do sítě připojují klienti jak pomocí kabelu, tak pomocí WIFI. Z bezpečnostních důvodů je vhodné klienty separovat.

3.4.4 Ukázka konfigurace

```
ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;

# A slightly different configuration for an internal subnet.
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.50 192.168.0.240;
  option domain-name-servers 192.168.0.1;
  option domain-name "home.soucekl.net";
  option routers 192.168.0.1;
  default-lease-time 600;
  max-lease-time 7200;
}
subnet 192.168.10.0 netmask 255.255.255.0 {
  range 192.168.10.50 192.168.10.240;
  option domain-name-servers 192.168.0.1;
  option domain-name "wifi.soucekl.net";
  option routers 192.168.10.249;
  default-lease-time 600;
  max-lease-time 7200;
}

#desktop
host libor.home.soucekl.net {
```

```
  hardware ethernet 00:16:76:22:59:cf;
  fixed-address 192.168.0.5;
}
```

3.5 Samba

3.5.1 Popis

Funkcí samba serveru je sdílení dat mezi klienty s MS Windows (popř. i dalších OS). Samba server může fungovat i jako autentifikační server pro Windows (náhrada Windwos PDC).

3.5.2 Instalace

Po standardní instalaci není samba server nainstalován. To napravíme následujícím příkazem:

```
apt-get install samba
```

3.5.3 Konfigurace

Konfigurace se nachází v souboru /etc/samba/smb.conf

Konfigurace je velmi dobře dokumentovaná (popř. je ukázka v smb.conf.example).

Mezi hlavní položky patří:

[GLOBALS]
Workgroups jméno domény (pracovní skupiny)
Security nastavení kontroly oprávnění. Jestli je user, nebo share. User – každý má uživatelský účet, Share – podle IP
Interfaces Na těchto rozhraních bude samba naslouchat
Definice v []
Specifikují jednotlivá sdílení.

Při přidávání uživatele při security = user se musí napřed přidat systémový uživatel a poté uživatel do samby (pomocí smbpasswd)

3.5.4 Ukázka konfigurace

```
[global]
   workgroup = Doma
   netbios name = soucek
   server string = Samba Server %v
   printcap name = cups
   load printers = yes
   printing = cups
   printer admin = @adm
   log file = /var/log/samba/log.%m
   max log size = 50
   map to guest = bad user
   security = user
   encrypt passwords = yes
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   interfaces = 192.168.10.1/24 192.168.0.1/24
   wins support = yes

[homes]
   comment = Home Directories
   browseable = no
   writable = yes
[vol1]
   comment = Disk Server
   path = /mnt/vol1/
   valid users = libor
   public = no
```

```
   writable = yes
   create mask = 0765
[web]
   comment = Weby
   path = /www/
   valid users = libor
   public = no
   create mask = 0775
   writable = yes
   force user= apače
[mama]
   comment = Mamin adresar
   path = /opt/samba/mama
   valid users = renata libor
   public = no
   create mask = 0765
   writable = yes
```

3.6 PureFTPd

3.6.1 Popis

Slouží k nahrávání dat pomocí protokolu FTP na server.

3.6.2 Instalace

```
Apt-get install pureftpd
```

3.6.3 Konfigurace

Konfigurace se nachází v /etc/pure-ftpd (debian), nebo se konfiguruje pomocí jednotlivých parametrů v /etc/conf.d/pure-ftpd (gentoo)

Uživatelé se přirávají pomocí programu pure-pw:

```
pure-pw useradd $name -f /etc/pureftpd.passwd -u virtwww -g www-data -d $addr -m
```

Za parametry –u a –g se zadává, jaký uživatel má pod tímto účtem vystupovat na straně serveru.

3.7 Postfix

3.7.1 Popis

Poštovní server Postfix použijeme z důvodu, že je třeba nějakým způsobem se starat o systémovou poštu.

Nejlepší varianta je nechat postfix odesílat poštu na ostatní servery pomocí tzv. smtproute (nadřazený server). Výhoda takovéhoto řešení je lepší správa a monitoring takovéhoto systému.

3.7.2 Instalace

Pokud již není postfix nainstalován, nainstalujeme jej pomocí:

```
Apt-get install postfix
```

Po instalaci se nás systém zeptá na konfiguraci postfixe, vybereme požadovanou konfiguraci (zda odesílat pomocí SMTPRoute, nebo přímo, …) a vše potřebné sám nastaví.

3.7.3 Konfigurace

Pro základní funkcionalitu není třeba, vše se provede v průběhu instalace.

4 Zálohování

Zálohování je možné vyřešit několika způsoby. Záleží na množství zálohovaných dat.

Nejjednodušší je lokálně pomocí CRONem spouštěného skriptu, který bude lokálně (na jinou partition/disk) kopírovat data.

Při větších nárocích je vhodné tímto skriptem získaná data předávat na jiný server a na něm je ukládat.

A v neposlední řadě je vhodné použít zálohovací systém typu klient/server – např. Bacula. Na server se nainstaluje bacula-fd (file deamon), který na pokyn bacula-dir (řídící server) odesílá data bacula-sd (storage deamon) a ten je zpracovává (provádí komprimaci, rotaci, …). Výhodou tohoto řešení je, že každá část systému může běžet na vlastním serveru a také to, že bacula-sd umí (velmi dobře) pracovat se zálohovacími mechanikami (roboty, páskovými mechanikami, …)

5 Zabezpečení

Je vhodné server umístit na „nepřístupné“ místo, které je ale dobře větráno a pokud možno klimatizováno. Ideální je možnost server uzamknout.

Co se týče síťové bezpečnosti, je třeba mít správně nakonfigurován firewall – čili nenechávat nepoužívané porty otevřené. Dále je vhodné použít SSHd a autentifikaci pomocí klíčů (v tom to případě je vhodné autentifikaci heslem v konfiguraci SSHd deaktivovat).

6 Závěr

Takto nainstalovaný server může bez problému být nainstalován v menší firmě (<50 uživatelů). V případě většího nasazení je vhodné zvážit správu uživatelů pro Sambu pomocí LDAP, databázi pro Pure-ftpd mít v MySQL, …

Co se týče hardwarové stránky serveru, je vhodné použít dedikovaný server (pokud naň máme), nebo silnější stanici (zde je třeba brát ohled na spolehlivost hardwaru, spíše nad výkonem). Pro účely malé firmy plně postačuje hardware o následující konfiguraci:

- CPU: Optimálně Intel Xeon nebo Intel Pentium III/IV popř. i Celeron o taktu cca 2GHz
- RAM Optimálně ECC paměti, alespoň 320MB (512MB). Pokud bude server pracovat i jako databázový server, je vhodné pořídit více paměti.
- HDD Optimálně RAID pole jak pro systém, tak pro data. Když by bylo možno, nejlepší je použít Hardwarový RAID – pokud máme spolehlivý řadič.

Veškeré linuxové programy (servery) mají velmi podrobnou dokumentaci a podrobně dokumentované (ukázkové) konfigurační soubory, tudíž touto stránkou se v této práci moc nezabývám.

Mezi mnou doporučované utility patří:

- Htop monitoring vytíženosti serveru
- lsof podrobnosti o procesech
- netstat informace o naslouchajících službách
- Nagios nejedná se o utilitu, ale o monitorovací systém, po kterém se v případě větších sítí je vhodné poohlédnout.

7 Obsah