Operačí systémy

Instalace a pokročilá administrace virtualizovaného serverového OS Linux

David Gillar

Katedra ICT v lékařství,

Fakulta biomedicínského inženýrství ČVUT

Podpořeno projektem RPAPS FBMI 2018

Osnova

- Úvod - využití virtualizace pro instalaci Linuxového serveru
- Zabezpečení Linuxového serveru - HOSTS, HOSTNAME, IPTABLES a vzdálená správa
- Nasazení, konfigurace a zabezpečení webového serveru a redakčního systému
- Monitorace a zálohování Linuxového serveru

Úvod - využití virtualizace pro instalaci Linuxového serveru

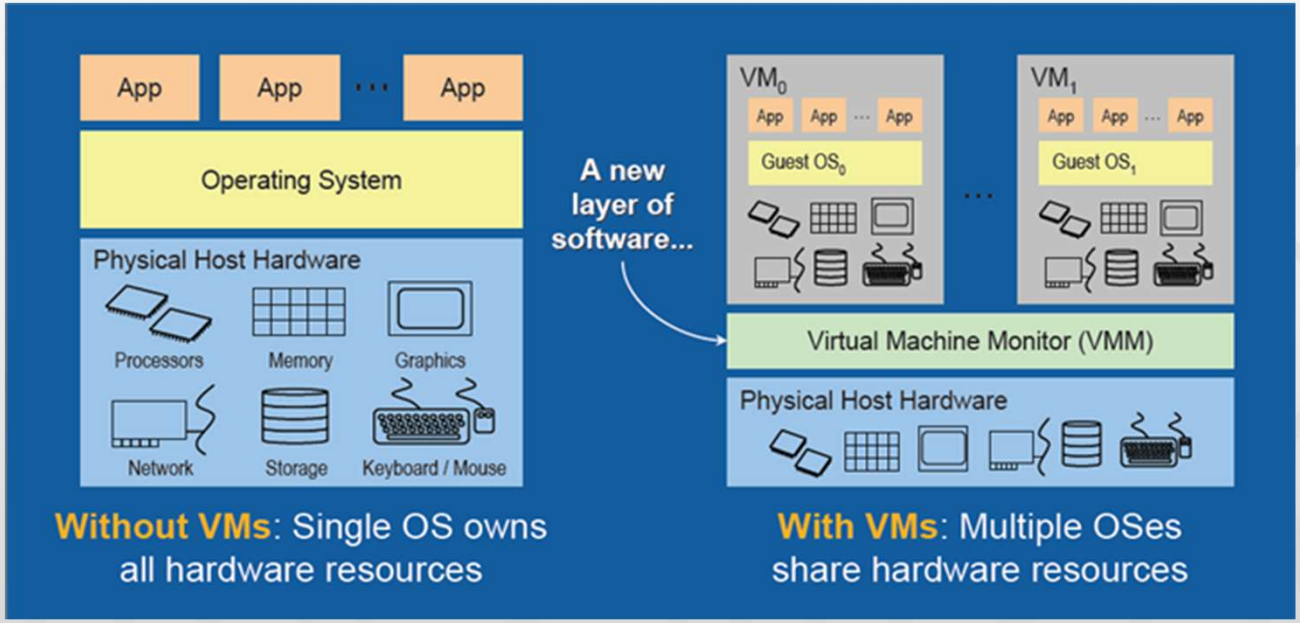
- Nainstalujeme, nakonfigurujeme a připojíme k počítačové síti virtuální stroj s “holým“ Linuxem, do kterého budeme následně přidávat další funkce

Hardwarová podpora virtualizace

- V BIOSU / UEFI počítače, na kterém má běžet virtualizační hypervisor, je potřeba virtualizaci povolit
- Tato možnost je k dispozici jako „Enable Virtualization“, „Enable VT-x“ (procesory Intel), „Enable AMD-V“ (procesory AMD) či podobně
- Do BIOSu se dostaneme většinou pomocí klávesy DEL či F2 po zapnutí napájení
- V případě nezdaru nám pomůže Pan Google

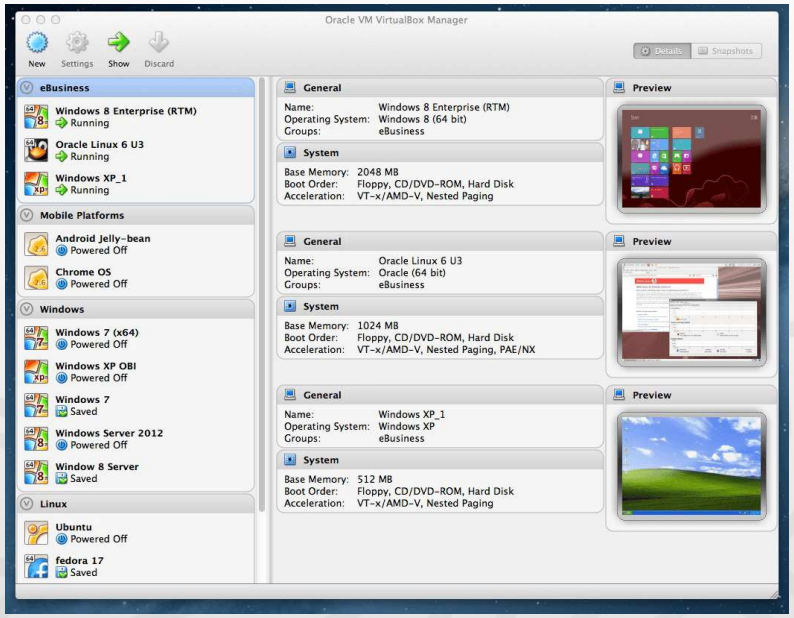
Virtualizace

- Více OS na jednom HW
- Nová vrstva nad OS, která vytvoří virtuální HW vrstvu



Správce virtuálních strojů

- Program, který se stará o virtualizaci prostředků
- Rozděluje prostředky dodávané fyzickým OS mezi více virtuálních strojů (a na nich běžících OS)
- Dnes již přímá podpora ze strany hardwaru (AMD-V, VT-x)



Správce virtuálních strojů II

- Nejpoužívanější nástroje:
  - VirtualBox (Oracle) – multiplatformní, zdarma
  - VMware Workstation (VMware) – částečně placené
  - Hyper-V (Microsoft) – zdarma, pouze pro OS Windows

Microsoft
Hyper-V

Instalace hypervizora

- Nainstalujte si **pouze jeden** Vámi vybraný hypervizor
- Hyper-V se „instaluje“ povolením ve funkcích Windows (Ovládací panely -> Zapnout nebo vypnout funkce Windows -> Zaškrtnout Hyper-V)
- Ostatní nástroje se instalují pomocí instalačních souborů dostupných na oficiálním webu produktu
- Například na dalších slajdech je popsána instalace VirtualBoxu

VirtualBox

- Ke stažení: https://www.virtualbox.org/
- ExtensionPack: Podpora USB zařízení, vzdálené plochy…
- PHPVirtualBox: open-source projekt pro správu VirtualBox přes webové rozhraní: http://sourceforge.net/projects/phpvirtualbox/

VirtualBox II

- Možnost pozastavit VM za chodu (spouštění VM pouze podle potřeby)
- Vytváření snapshotů – stavů VM (obsah virtuálního disku a konfigurace VM)
- Import a export VM (obnova poškozené instance, přenos na jiný HW) = vytvoření appliance

VirtualBox – Instalace

1. Stáhneme aktuální VirtualBox a jeho ExtensionPack
2. Obojí nainstalujeme

Příklad vytvoření vm ve virtualboxu

- Podrobný tutoriál například na: **https://www.virtualbox.org/manual/ch01.html**

Server

- Přizpůsobený operační systém pro dlouhodobý běh, spolehlivost a maximální výkon služeb (servisů)
- Servery založené na Windows: Windows Server 2016, 2012, 2010…
- Servery založené na Linuxovém jádře: Ubuntu server, Debian, Fedora, OpenSUSE, Kali Linux…

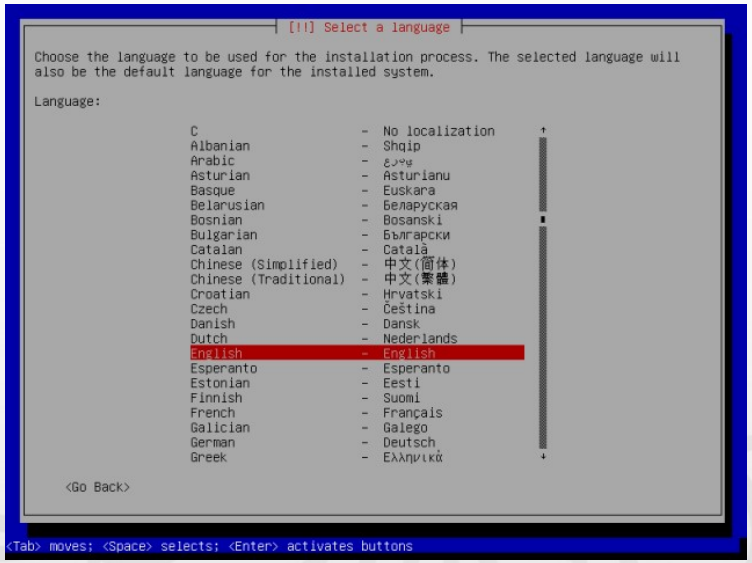
Ubuntu Server

- Budeme používat Ubuntu Server v nejaktuálnější verzi
- Ubuntu Server je bez GUI (správa pouze pomocí konzole), což vede k většímu výkonu a menším nárokům než desktopové Ubuntu (rozdíly ale nejsou příliš velké)
- GUI lze kdykoliv doinstalovat či zakázat (navíc je k dispozici více možných GUI) a tak je možné z Ubuntu Serveru udělat Ubuntu Desktop a naopak

Ubuntu Server I

- Ubuntu udržuje dvě verze – Latest a LTS (long-time support)
- LTS verze mají dlouhodobou podporu a jsou stabilnější
- LTS verze by měli tudíž být používány pro serverová řešení
- V rámci tohoto cvičení budeme používat Latest Ubuntu Server
- Instalační image Latest Ubuntu Serveru (ne LTS) stáhneme z: https://www.ubuntu.com/download/server
- Po stažení připojíme image k mechanice VM a stroj spustíme

Ubuntu Server II



1. Připojíme image
2. Spustíme VM
3. Nastavíme jazyk
4. Nastavíme oblast
5. Nastavíme klávesnici
6. Nastavíme hostname – **prijmeni.biops.fbmi.cvut.cz**, uživatele a heslo
7. Po instalaci nezapomenout odpojit image Ubuntu

Ubuntu server – Rozložení disku

- Můžeme manuálně rozložit disk - vytvoříme swap a root
- Existuje nepsané pravidlo: swap udělat 2x větší než velikost RAM a umístit jej na začátek disku (rychlejší čtení a zápis – především u magnetických disků, ve virtuálním stroji nebo na SSD disku nemá pozice swapu význam)
- Nebo nechat systém automaticky rozložit disk („Guided – use entire disk“) – udělá swap, root a „záchranný oddíl“

Ubuntu server – Konfigurace sítě

- Získávání adresy z DHCP vs. manuální pevná adresa – pokud nemáme udělané DyDNS, pak servery mívají pevně nastavenou IP adresu
- Pozdější editace v /etc/network/interfaces
- Související témata k samostudiu: *síťování, síťové prvky, veřejná vs. lokální IP adresa, IPv4, IPv6, VPN, DHCP*

Ubuntu server – Konzole

- Nejrychlejší ovládání (a na serverové edici jediné) je pomocí konzole
- Jednotlivé příkazy zadané do konzole jsou zpracovávány
- Volání programů s různými parametry, spouštění skriptů…
- Základ je spustit si konzoli…
- V desktopové edici např. programem Terminal, v serverové edici jsme po přihlášení (loginu) rovnou v terminálu

Ubuntu server – Programy

- Nápověda k příslušnému programu:

1. <název programu> --help
2. man <název programu>

Ubuntu server – Správa aplikací I

- Pro instalaci a správu aplikací slouží v Ubuntu Apptitude
- Instalace programu z dostupného distribučního kanálu:

  apt-get install <jméno balíku>
- Odinstalování balíku:

  apt-get remove <jméno balíku>

Ubuntu server – Správa aplikací II

- Aktualizace seznamu dostupných balíků: **apt-get update**
- Upgrade nainstalovaných balíků: **apt-get upgrade**
- „Chytrý“ upgrade balíků: **apt-get dist-upgrade**
- Odstranění nepoužívaných balíků:

  apt-get autoremove
- Odstranění stažených balíků: **apt-get autoclean**

Ubuntu server – Správa aplikací III

- Instalace ze staženého balíku (*.deb – Ubuntu je odvozeno od Debianu):

dpkg -i <balík.deb>

- Odstranění nainstalovaného balíku:

dpkg -r <balík>

Aktualizace virtuálu

- Pro aktualizaci balíčků je nutné být root – tím se stanete zadáním příkazu: **sudo su** a následným zadáním hesla
- Následně si zaktualizujte balíčky pomocí následujících příkazů:

  apt-get update

  apt-get upgrade

  apt-get dist-upgrade

  apt-get autoremove

  apt-get autoclean

Ubuntu server – MC

- Midnight commander
- Správce souborového systému
- Užitečný nástroj bez kterého nelze server spravovat
- Instalace: **apt-get install mc**

Virtualbox guest additions I

- Image CD s programy, které se instalují ve VM
- Programy a služby, které optimalizují OS běžící ve VirtualBoxu (při použití jiného hypervizoru je nemá smysl instalovat)
- Umožňují například automatické přihlašování, sdílenou schránku, sdílené složky, synchronizaci času, vylepšenou grafiku ve VM apod.
- Díky tomu můžeme sdílet složky ve fyzickém OS našemu VM a tyto složky jsou automaticky po startu VM přístupné

Virtualbox guest additions II

1. Ve VirtualBoxu připojíme obraz CD VBoxGuestAdditions.iso do našeho VM
2. Následujícím příkazem vytvoříme složku /mnt/cdrom, pokud již neexistuje: **mkdir /mnt/cdrom**
3. Ve VM poté připojíme (namountujem) toto „vložené CD“ do složky /mnt/cdrom příkazem: **mount /dev/cdrom /mnt/cdrom**

Virtualbox guest additions III

- Skript *VBoxLinuxAdditions.run*, který budeme spouštět, vyžaduje mít nainstalovaný balík DKMS, proto jej nejprve nainstalujeme:

apt-get install dkms -y

- Otevřeme namountované CD ve složce /mnt/cdrom a spustíme skript VBoxLinuxAdditions.run
- Po proběhnutí skriptu odpojíme (un-mountujeme) CD pomocí:

umount /mnt/cdrom

Restart a vypnutí ubuntu serveru

- Pro „odhlášení se“ jako root použijeme příkaz: **exit**
- Pro restart serveru použijeme příkaz: **reboot**
- Pro vypnutí serveru zadáme příkaz: **shutdown -P 0**

Restart a vypnutí ubuntu serveru

- Pro „odhlášení se“ jako root použijeme příkaz: **exit**
- Pro restart serveru použijeme příkaz: **reboot**
- Pro vypnutí serveru zadáme příkaz: **shutdown -P 0**

Zabezpečení Linuxového serveru - HOSTS, HOSTNAME, IPTABLES a vzdálená správa

- Nyní z holého virtualizovaného Linuxu uděláme Ubuntu Server, který připravíme pro bezpečné nasazení serverových služeb instalací a konfigurací základních nástrojů

Ubuntu server – Hosts a hostname

- Soubor /etc/hostname obsahuje název počítače (vyplňovalo se při instalaci) – například havana.albertov.cz
- Soubor /etc/hosts obsahuje seznam hostů a jejich IP adresy (je to předchůdce služeb DNS) a měl by minimálně obsahovat tento záznam:

  127.0.0.1 localhost

- Poté by měl obsahovat záznam o sobě samotném – v příkladu:

  127.0.0.1 havana.albertov.cz havana

Ubuntu server – Vzdálená správa I

- Správa serveru na dálku
- Pomocí konzole, vzdálené plochy nebo webového rozhraní
- Konzole: SSH
- Vzdálená plocha: RDP protokol, TightVNC (http://www.tightvnc.com)
- Webové rozhraní: Webmin (http://www.webmin.com)

webmin

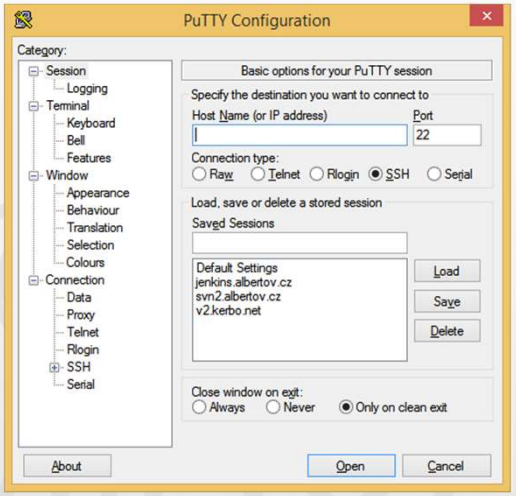
Ubuntu server – Vzdálená správa II

- Servisa SSH: apt-get install openssh-server

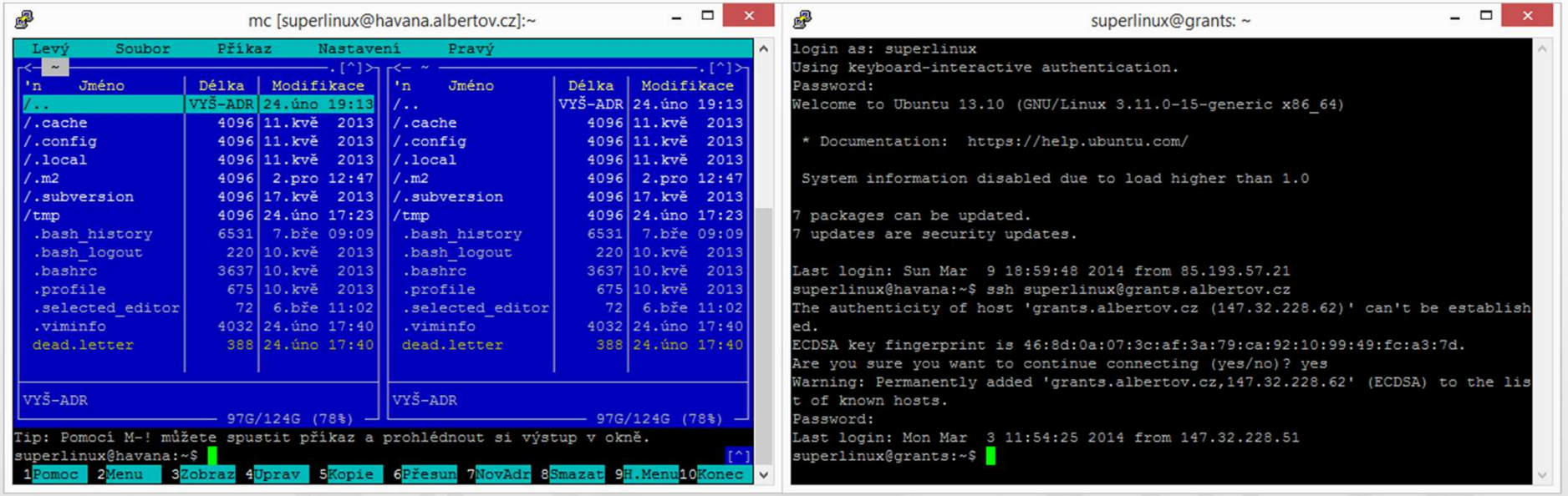
  (ssh = klient pro připojování, ssh server = servisa na straně cílového počítače)
- Konfigurační soubor: /etc/ssh/sshd_config
- Důležité parametry:
  - **Port**, na kterém naslouchá (defaultně na portu 22, změna pro „zmátnutí“ případného útočníka)
  - **IP Adresy**, ze kterých má být povolen přístup (omezení z lokální sítě apod.)
  - **Seznam uživatelů** nebo skupin, které mají mít povolený přístup (omezení přístupu pouze na administrátora)

Ubuntu server – Vzdálená správa III

- Klienti pro přístup pomocí SSH pro Windows:
- PuTTY (http://www.putty.org/)
- Bitvise Tunnelier (http://www.bitvise.com/)
- Bitvise WinSSHD (http://www.bitvise.com/)
- Připojení z Linuxového OS: ssh uživatel:heslo@server
- Připojení z Windows 10 (od r 2018): ssh uživatel:heslo@server
- Připojení z Mac OS: program Terminal
- Existují také pro ostatní (i mobilní) operační systémy



Ubuntu server – Vzdálená správa IV



Ubuntu server – Mailový klient SSMTP I

- Program (nikoliv služba) pro odesílání mailů z konzole, ze skriptů
- Pro notifikace správce, pokud se něco pokazí nebo nepovede (nebo naopak pokud se například provede úspěšně záloha)
- Instalace: apt-get install ssmtp
- Konfigurace: /etc/ssmtp/ssmtp.conf

Ubuntu server – Mailový klient SSMTP II

- Musíme definovat poštovní server, ze kterého budeme odesílat a autentizaci, pokud je potřeba; dále to, zda se jedná o zabezpečenou komunikaci
- Následující konfigurace umožní odesílat z fakultního mailového serveru bez nutnosti autentizace; platí pouze pro odesílání z lokální fakultní sítě

Konfigurace ssmtp

```
root=server@fbmi.cvut.cz # Příchozí adresa mailhub=smtp.fbmi.cvut.cz # SMTP server

rewriteDomain=ppp.fbmi.cvut.cz # Odesílací doména adresy

FromLineOverride=YES # Povolení vlastní adresy odesílatele

UseTLS=NO # Zabezpečené spojení se serverem pomocí TLS
```

Ubuntu server – Odesílání mailů I

- Příklad odeslání mailu z konzole či skriptu:

  ssmtp -t < zprava.mail

- Přepínač ‚-t‘ specifikuje, že adresa příjemce se nachází v předaném souboru
- **zprava.mail** je soubor, který obsahuje samotný mail, který přesměrujeme do vstupu programu ssmtp
- Soubor má striktně daný formát

Ubuntu server – Odesílání mailů II

```
To:prijemce@gmail.com
From:moje.adresa@neconeco.com
Subject:Předmět zprávy

Tělo zprávy. Všimnete si
dvojitého odřádkováni mezi
předmětem zprávy a tělem
zprávy. To je vyžadováno.
```

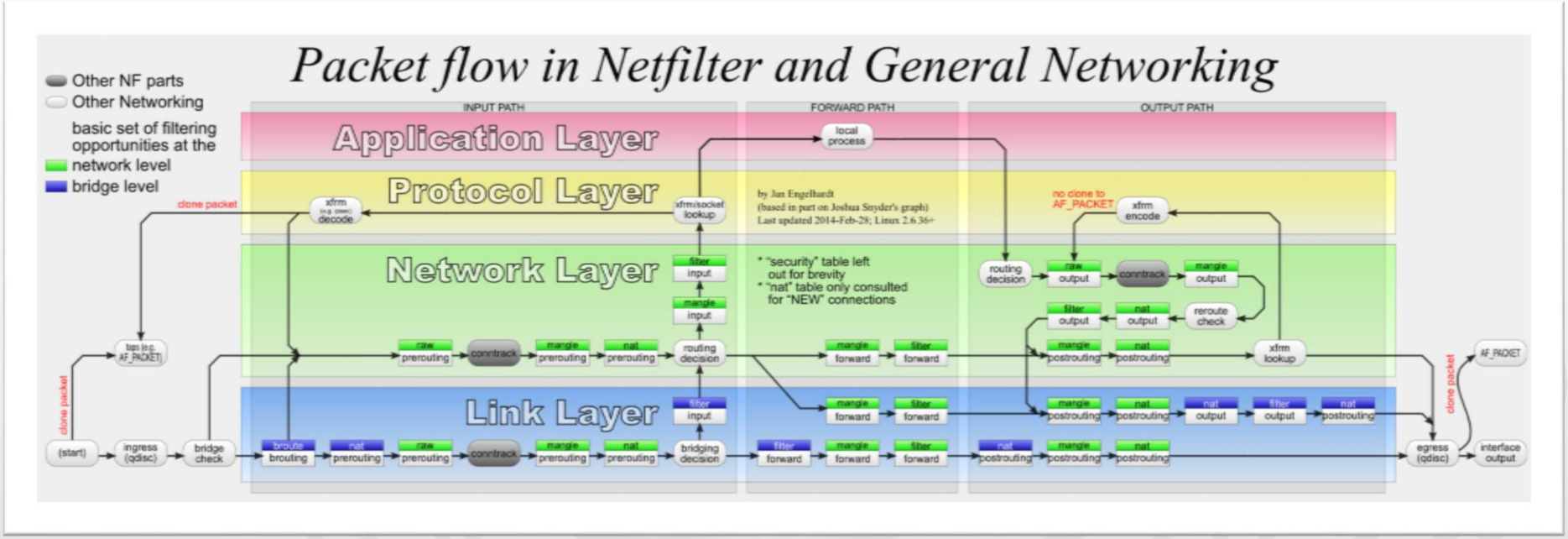
Ssmtp - Alternativy

- Postfix – samotný poštovní server, nikoliv klient k připojení k SSMTP serveru
- Sendmail – také samotný poštovní server
- telnet

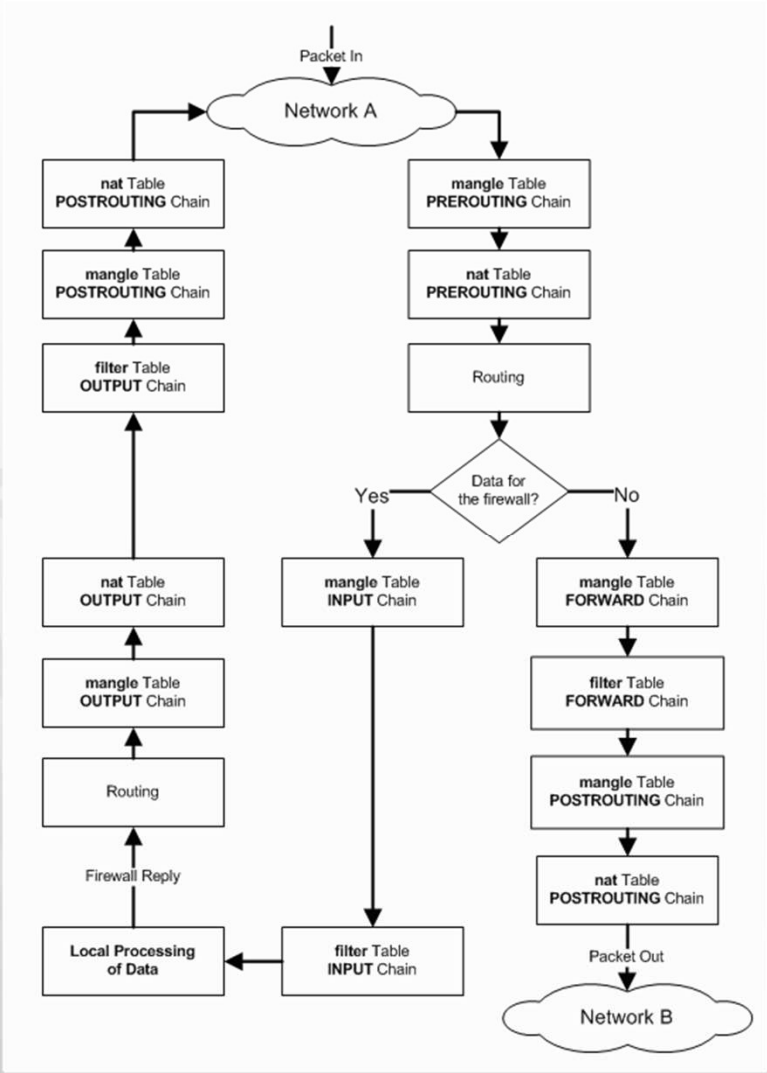
Ubuntu server – Iptables I

- Pravidla, která kontrolují příchozí a odchozí síťová spojení, pravidla se zpracovávají od **prvního** pravidla, proto je dobré mít nejvytíženější porty a protokoly co nejvýše
- Fungují jako Firewall, ale mohou také fungovat jako NAT a PROXY
- Chceme zabránit, aby se kdokoliv mohl připojit na jakýkoliv port, kromě námi povolených (většinou používáme pouze porty 80 pro HTTP, 443 pro HTTPS, 22 pro SSH, 8080 pro alternativní HTTP atd.), dále můžeme například zakázat i ping.

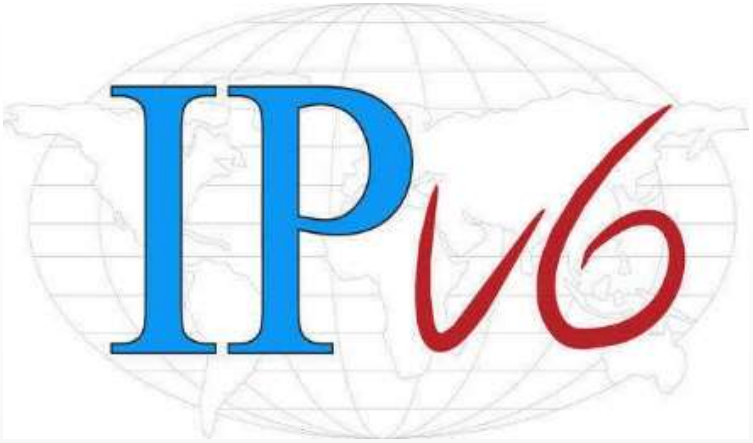
Ubuntu server – IPTABLES packet flow



Ubuntu server – IPTABLES packet processing



Iptables vs ip6tables



- IPTABLES = pro IPv4
- IP6TABLES = pro IPv6
- Jiný název programu pro každou generaci IP protokolu
- Syntaxe a vše ostatní je stejné

Ubuntu server – Iptables II

- Seznam všech aktuálně platných pravidel včetně detailů:

  iptables -L –v

- Vložení pravidla na určité místo X (indexace od 1):

  iptables -I INPUT X <další parametry>

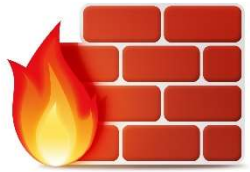
- Přidání pravidla na konec:

  iptables -A INPUT <další parametry>

- Odebrání pravidla z určitého místa (indexace od 1):

  iptables -D INPUT 1

Ubuntu server – Iptables III



- Povolení lokální komunikace – komunikace procesů mezi sebou (localhost; přidáme na první místo (indexace od 1), protože bývá nejvytíženější):

  iptables -I INPUT 1 -i lo -j ACCEPT

- Povolení navazujících a pomocných portů (pozor na přesnou syntaxi!):

  iptables -I INPUT 2 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

- Povolení portu 80 (HTTP) na 3. místě:

  iptables -I INPUT 3 -p tcp --dport 80 -j ACCEPT

Ubuntu server – Iptables IV

- Povolení pingu:

  iptables -I INPUT 4 -p icmp -j ACCEPT

- Logování pokusů o připojení na ostatní porty:

iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied:" --log-level 7

- Odmítnutí ostatních připojení:

  iptables -I INPUT 6 -j DROP

Ubuntu server – Iptables V

- Stejně jako jsme nyní vytvořili filtrovací pravidla pro IPv4, měli bychom vytvořit filtrovací pravidla pro IPv6
- Výše přidaná pravidla přidáme i do v6 tabulek: místo iptables budeme používat příkaz **ip6tables**

Ubuntu server – Iptables VI

- Pravidla se sama neukládají a po restartu o ně přijdeme
- Proto je potřeba:
  1. vytvořit si dva skripty, které pravidla uloží a opět načtou – tyto pravidla skripty budou spouštěny při určitých událostech
  2. Doinstalovat balík iptables-persistent (který dělá ve skutečnosti stejnou práci jako bod 1 – viz zdrojové kódy balíku iptables-persistent na https://packages.ubuntu.com/)

Ubuntu server – Iptables persistent

- Balík spravuje pravidla jak pro IPv4, tak pro IPv6
- Instalace:

  apt-get install iptables-persistent
- Manuální uložení konifgurace iptables (v závislosti na verzi Ubuntu):

  /etc/init.d/iptables-persistent save

  netfilter-persistent save
- Manuální načtení konifgurace iptables (v závislosti na verzi Ubuntu):

  /etc/init.d/iptables-persistent load

  netfilter-persistent load

Ubuntu server – Iptables VII

- Manuální ukládání a načítání pravidel se vynutí vytvořením dvou skripů ve specifických složkách v /etc/network/*****
- Skript *iptablessave* uložíme do složky /etc/network/if-post-down.d
- Skript musí mít atribut executable: chmod +x ./iptablessave

Ubuntu server – Obsah skriptu *iptablessave*

```
#!/bin/sh
iptables-save -c > /etc/iptables.rules
ip6tables-save -c >
/etc/ip6tables.rules
exit 0
```

Ubuntu server – Iptables IX

- Více o konfiguraci iptables: https://help.ubuntu.com/community/IptablesHowTo
- Zprovoznění NAT a PROXY: http://www.karlrupp.net/en/computer/nat_tutorial

Ping serveru

- Z jiného počítače vyzkoušíme, jestli je náš VM připojen k internetu
- Spustíme příkazový řádek a zavoláme:

ping <adresa VM>

- Jak zjistíme IP adresu našeho VM?

ifconfig

…a budeme hledat inet addr u eth0

Nasazení, konfigurace a zabezpečení webového serveru a redakčního systému

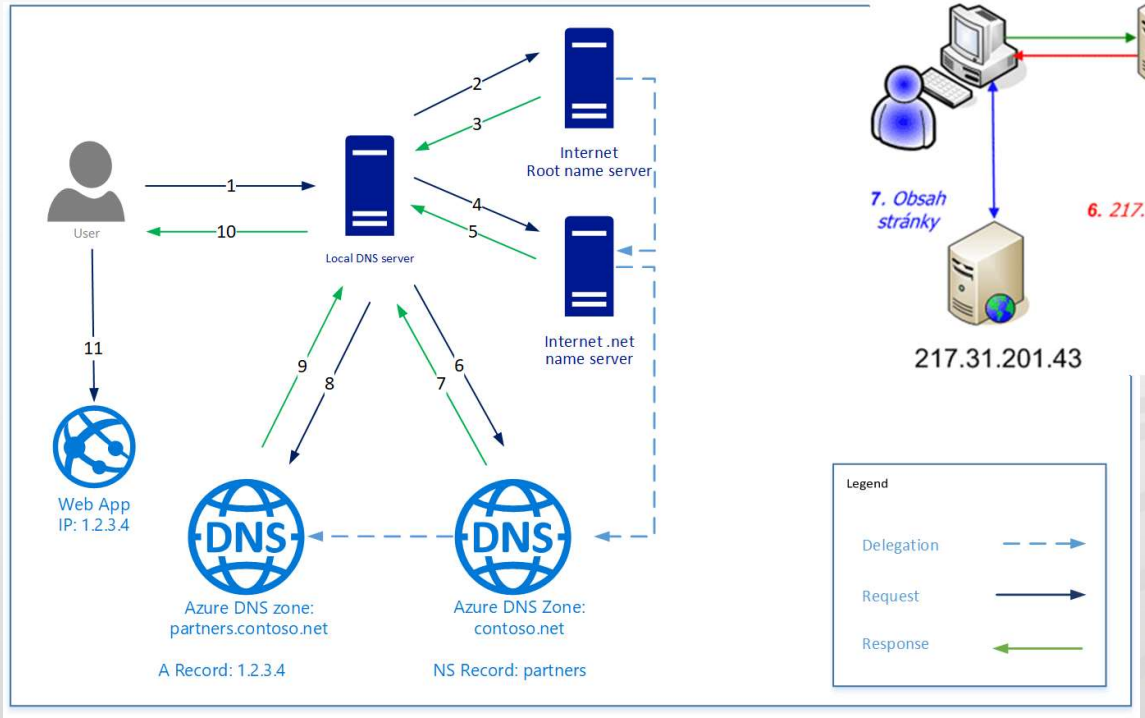
- Nyní nainstalujeme LAMP server, který bude obsahovat webový server, databázový server a podporu skriptování PHP.

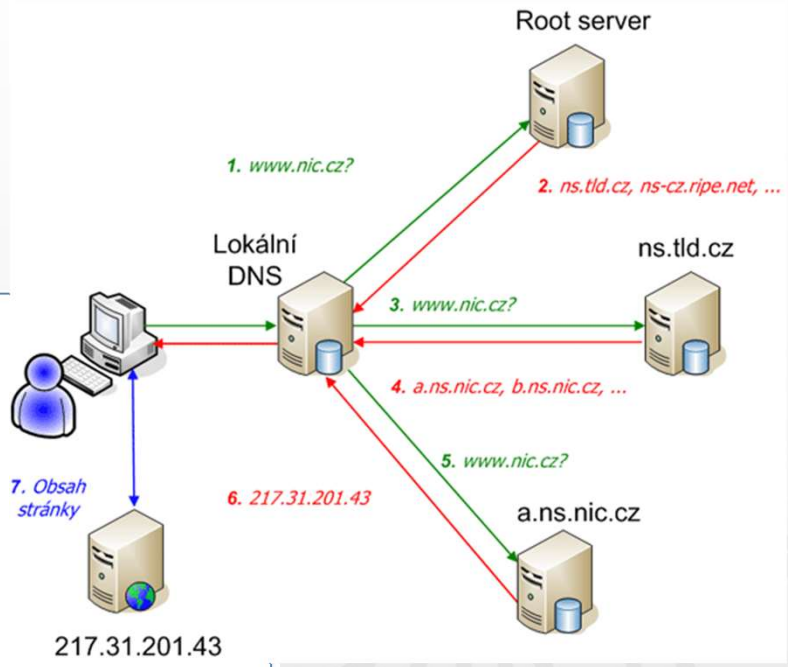
- Ten následně využijeme k instalaci redakčního systému Wordpress

Dočasná editace hosts

- Simulace DNS serveru pro naše vymyšlené domény pouze v rámci tohoto předmětu (po ukončení výuky přidané záznamy smažeme)
- Před odeslání žádosti o přeložení záznamu se prochází soubor **hosts**, ve kterém se hledají záznamy o doméně/adrese
- Pokud záznam najde, použije jej; v opačném případě kontaktuje DNS server
- Lokální forma DNS služby
- Z historických důvodů, předchůdce dnešní DNS služby
- Způsob patchování aktivací některých programů

DNS


User
Local DNS server
Internet
Root name server
Internet .net
name server
Web App
IP: 1.2.3.4
Azure DNS zone:
partners.contoso.net
A Record: 1.2.3.4
Azure DNS Zone:
contoso.net
NS Record: partners
1
2
3
4
5
6
7
8
9
10
11
DNS
DNS
Legend
Delegation
Request
Response


Root server
1. www.nic.cz?
2. ns.tld.cz, ns-cz.ripe.net, ...
Lokální
DNS
ns.tld.cz
3. www.nic.cz?
4. a.ns.nic.cz, b.ns.nic.cz, ...
5. www.nic.cz?
7. Obsah
stránky
6. 217.31.201.43
a.ns.nic.cz
217.31.201.43

Dočasná editace hosts II

- Ve Windows: C:\Windows\System32\drivers\etc\hosts
- V Linuxu a Mac: /etc/hosts
- Pro editaci je nutné být root, respektive otevřít soubor v poznámkovém bloku, který máme spuštěný jako správce
- Potřeba vědět IP adresu VM (příkazem ifconfig)
- Budeme editovat soubor tam, kde máme k dispozici webový prohlížeč (nejlépe ten OS, kde běží hypervizor)
- *<IP adresa VM>* = IP adresa vašeho VM
- *<příjmení>* = vaše příjmení bez interpunkce (například „kucera“)

Dočasná editace hosts – přidání záznamů

<IP adresa VM> mywordpress.<příjmení>.edu

<IP adresa VM> mywebsite.<příjmení>.net

<IP adresa VM> zencart.mywebsite.<příjmení>.net

<IP adresa VM> eshop.mywebsite.<příjmení>.net

<IP adresa VM> joomla.mywebsite.<příjmení>.net

<IP adresa VM> jml.mywebsite.<příjmení>.net

<IP adresa VM> beershop.<příjmení>.cool

<IP adresa VM> www.beershop.<příjmení>.cool

<IP adresa VM> <příjmení>.blog

<IP adresa VM> www.<příjmení>.blog

<IP adresa VM> git.<příjmení>.io

<IP adresa VM> svn.<příjmení>.io

<IP adresa VM> jenkins.<příjmení>.io

<IP adresa VM> docs.<příjmení>.io

<IP adresa VM> bugs.<příjmení>.io

<IP adresa VM> ftp.<příjmení>.io

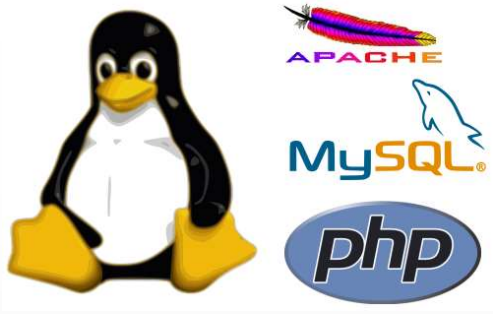
<IP adresa VM> samba.<příjmení>.io

<IP adresa VM> munin.<příjmení>.io

<IP adresa VM> bugs.<příjmení>.io

<IP adresa VM> docs.<příjmení>.io

LAMP



- Zkratka pro **L**inux**, A**pache**, M**ySQL **a P**HP
- Instalace několika způsoby:
  - Pomocí tasksel při instalaci nebo kdykoliv po ní
  - Instalací každého balíku zvlášť
- Podrobný návod na instalaci a konfiguraci: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-instalace-lamp

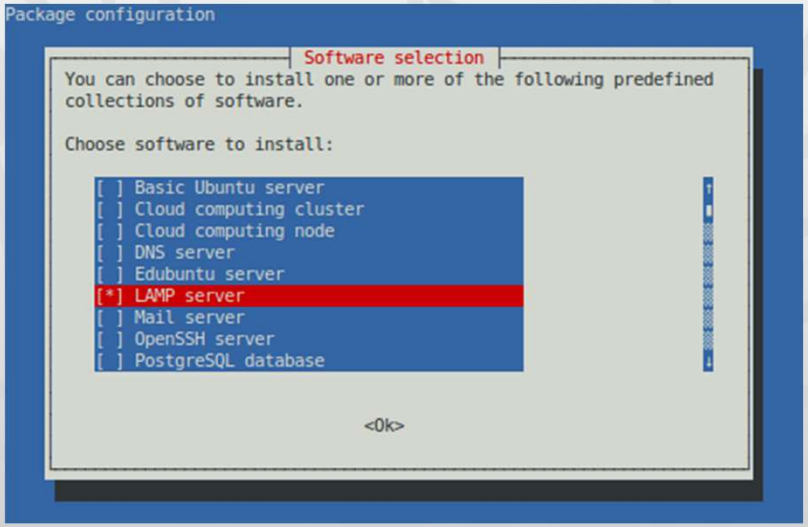
LAMP - TASKSEL

- Instalace tasksel:

  apt-get install tasksel

  tasksel

- Vybereme LAMP server, při instalaci nás vyzve k heslu pro správce databáze



Apache I

- Apache2, http://httpd.apache.org/
- Zkratka **A Patchy Server**
- Softwarový webový server, open-source, multiplatformní a nejrozšířenější
- Podpora mnoha funkcionalit (kromě samotného web serveru):
  - Virtuální weby (dnes si vyzkoušíme)
  - Proxy (příště)
  - SVN server (příště)

Apache II

- Instalace:

  apt-get install apache2

- Ověření: otevření webu v prohlížeči s adresou VM *
- Alternativy:
  - Lighttpd [Lighty]: http://www.lighttpd.net/
  - NGINX [Engine-X]: http://nginx.org/
  - Cherokee: http://cherokee-project.com/
- * Na jakém portu běží HTTP? Máme je povolené v IPTABLES?

Apache III

- Apache defaultně zobrazuje obsah adresáře /var/www/html (dříve /var/www), který je připraven pro webové stránky
- Zde se nachází soubor index.html, který se nám po instalaci defaultně zobrazuje

PHP I

- Původní název: **Personal Home Page**, nyní označováno jako **Hypertext Preprocessor**
- http://www.php.net/
- Programovací jazyk pro vytváření dynamických webových stránek
- Nativní podpora databází, správy souborů, COOKIES atd.
- Možnost psaní desktopových aplikací

PHP II

- Největší vývoj v posledních letech díky Facebooku (který je v něm napsaný)
- Od verze 5 s podporou objektů a OOP konceptů
- Aktuálně verze 7 (generace 7), udržuje se i verze/generace 5
- PHP nabízí možnost přístupu k operačnímu systému hostujícího OS (potencionální slabé místo při špatné konfiguraci, které dovolí přístup na hostující OS)
- Alternativy: Java, Javascript, Python, Ruby, F#, C#, ...

PHP – Instalace I

- Instalace samotného PHP a knihovny, která jej propojí s apache:

  apt-get install php libapache2-mod-php

- Restartujeme apache:

  service apache2 restart

- Ověření, zda PHP funguje: vytvoříme ve /var/www/html soubor index.php s obsahem:

```
<?php phpinfo(); ?>
```

- V prohlížeči poté otevřeme <adresa vm>/index.php a měli bychom vidět detailní konfiguraci PHP (jež byla vrácena funkcí phpinfo())

PHP – Instalace II

- Některé aplikace (redakční systémy apod.) potřebují další doplňky PHP
- Seznam aktuálně dostupných doplňků:

  aptitude search php

- Pozor na doplněk **php-cli** (Command line interpreter), díky kterému je možné pomocí webového prohlížeče provádět na serveru konzolové příkazy (brána pro hackery)

MySQL

- Nejrozšířenější open-source databáze, nyní vlastní firma Oracle
- http://www.mysql.com/
- Alternativy:
  - PostgreSQL: http://postgres.cz/wiki/PostgreSQL
  - Firebird: http://www.firebirdsql.org/
  - MS-SQL: https://www.microsoft.com/

MySQL – Instalace

- Instalace PHP doplňku pro podporu komunikace s MySQL a instalace samotného MySQL:

  apt-get install mysql-server php-mysql

- Během instalace je výrazně doporučeno zadat heslo do databáze (a zapamatovat si jej) pro administrátorský účet

PHPmyAdmin

- Administrace MySQL databáze přes webové rozhraní
- Napsáno v PHP
- Ke stažení na: http://www.phpmyadmin.net
- Možnost instalace pomocí apt-get
- Český návod na: http://www.linuxexpres.cz/praxe/sprava-databazi-pomoci-phpmyadmin

PHPmyAdmin – Instalce

- Instalace:

  apt-get install phpmyadmin

- Při instalaci zvolit (mezerníkem), že používáme apache2
- Ověření: v prohlížeči otevřít adresu <adresa vm>/phpmyadmin
- Username: root, heslo: vložené při instalaci
- Více detailů ohledně správy: http://www.linuxexpres.cz/praxe/sprava-databazi-pomoci-phpmyadmin

Apache – Struktura http serveru I

- Cíl: mít více virtuálních hostů na jednom serveru
- Námi požadovaná struktura v následující tabulce

Apache – Struktura http serveru II

Adresa	Popis
http://<IP adresa VM>/	root zakázat a zamezit přístup do /var/www/html
http://<IP adresa VM>/phpmyadmin	administrace MySQL databáze
mywordpress.<příjmení>.edu	Wordpress systém
mywebsite.<příjmení>.net	Drupal systém
zencart.mywebsite.<příjmení>.net	ZenCart e-shop
eshop.mywebsite.<příjmení>.	Alias pro ZenCart e-shop
joomla.mywebsite.<příjmení>.net	Joomla redakční systém
jml.mywebsite.<příjmení>.net	Alias pro Joomla redakční systém

Apache – Struktura http serveru III

Adresa	Popis
beershop.<příjmení>.cool	OpenCart e-shop
www.beershop.<příjmení>.cool	OpenCart e-shop
<příjmení>.blog	Alias pro Wordpress
www.<příjmení>.blog	Alias pro Wordpress
git.<příjmení>.io	Proxy pro GitLab (uděláme příště)
svn.<příjmení>.io	Proxy pro SVN (uděláme příště)
jenkins.<příjmení>.io	Proxy pro Jenkins (uděláme příště)
ftp.<příjmení>.io	Proxy pro FTP (uděláme příště)

Apache – Konfigurace

- Velice komplexní
- Povolování různých módů: a2enmod … (použijeme příště)
- Správa virtuálních hostů, proxy apod. pomocí souboru /etc/apache2/ports.conf
- Každá změna v konfiguraci se projeví až po restartu služby nebo znovu-načtení její konfigurace
- Příklady konfigurací: http://httpd.apache.org/docs/2.2/vhosts/examples.html

Apache – Ověření a aplikace konfigurace

- Restart služby:

  service apache2 restart

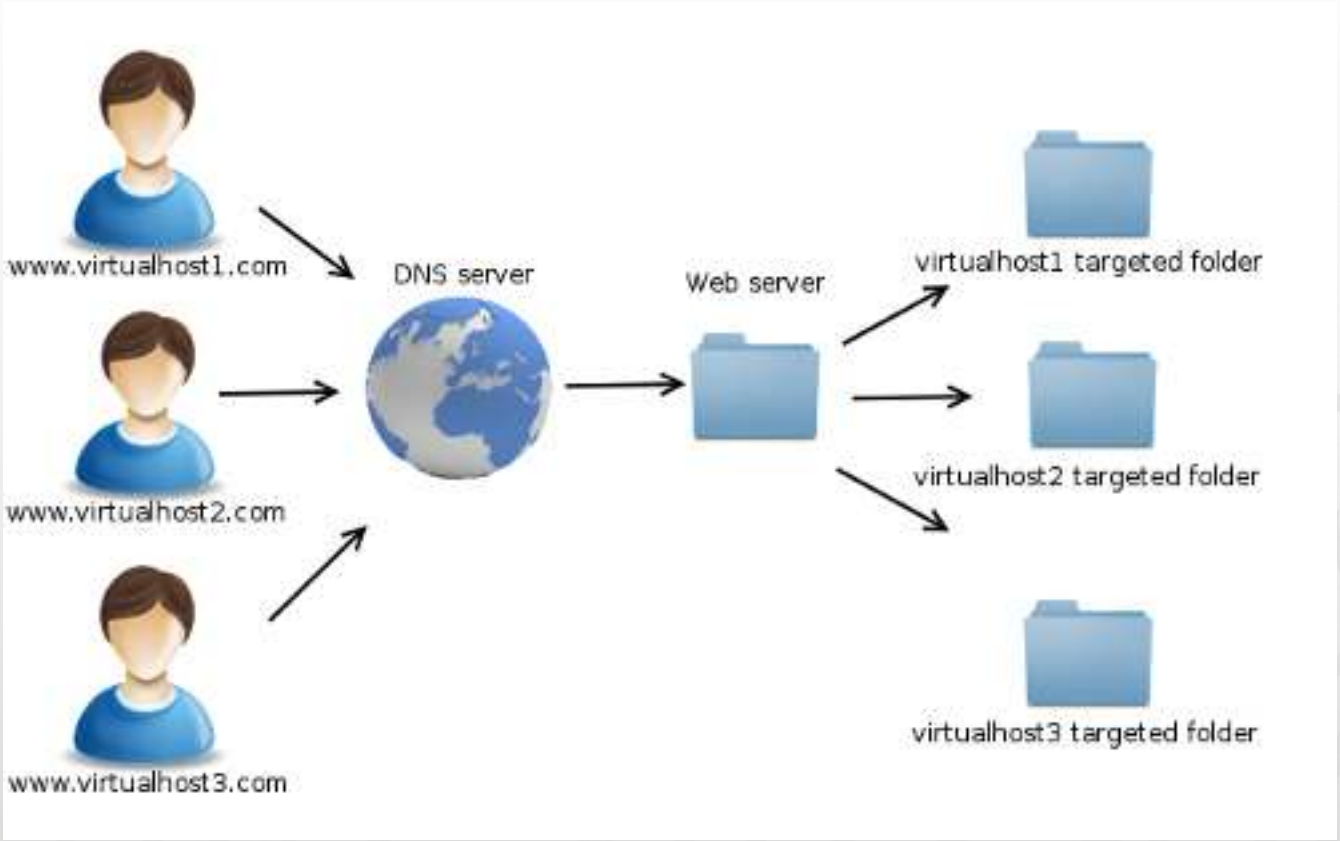
- Znovu-načtení konfigurace:

  service apache2 reload

Apache – Virtuální hostové I

- Na základě HTTP requestu se rozhoduje, který obsah (adresář) se zobrazí
- Možnost filtrování na základě cílového záznamu, cílové IP adresy, zdrojové IP adresy,…
- Důvod: více DNS záznamů ukazující na jeden server a tedy více webů běžících na jednom serveru (= jednom OS) (typicky webhosting)

Apache – Virtuální hostové II



Apache – Virtuální hostové III

- Můžeme rozlišovat na základě jména (name-based) nebo IP adresy (IP-based)
- Více různých webů na různých IP adresách, nebo jednu či více domén směřující na jednu nebo více IP adres
- Problém u HTTPS - jmenné rozlišování z principu nefunguje = na jedné IP adrese a portu je možné provozovat pouze jediný HTTPS (virtuální) web

Apache – Obsah ports.conf

- Naslouchání na portu 80:

```
Listen 80
```

Apache
– Vytvoření hosta pro wordpress

```
<VirtualHost *:80>
        ServerName mywordpress.<příjmení>.edu
        ServerAlias www.mywordpress.<příjmení>.edu
        DocumentRoot /var/www/wordpress
</VirtualHost>
```

Apache
– Vytvoření hosta pro zencart a jeho alias

```
<VirtualHost *:80>
        ServerName zencart.mywebsite.<příjmení>.net
        ServerAlias *.zencart.mywebsite.<příjmení>.net
eshop.mywebsite.<příjmení>.net
        DocumentRoot /var/www/zencart
</VirtualHost>
```

Apache
– Řízení přístupu k souborům a adresářům I

- Příklad: odmítnutí přístupu k zencart z adresy 1.2.3.4:

```
<Directory /var/www/zencart/>
    Order deny,allow
    Deny from 1.2.3.4
    Allow from all
</Directory>
```

Apache
– Řízení přístupu k souborům a adresářům II

- Příklad: odmítnutí přístupu k zencart z adresy 1.2.3.4:

```
<Directory /var/www/zencart/>
    Order deny,allow
    Deny from all
    Allow from 1.2.3.4
</Directory>
```

Apache
– Vypnutí prohlížení adresářové struktury

- Velké bezpečnostní riziko, pokud je prohlížení povoleno
- Do direktivy <Directory> …</Directory> pro příslušný adresář se vloží direktiva „Options -Indexes“:

```
<Directory /var/www/zencart/>
    Options -Indexes
</Directory>
```

Apache – Zakázání přístupu do adresáře

```
<VirtualHost *:80>
   ServerName localhost
   DocumentRoot /var/www/html
   <Directory /var/www/html/>
       Order deny,allow
       Deny from all
   </Directory>
</VirtualHost>
```

Apache – Aliasy

- Aliasy = na určité URL navázaný jiný adresář či jiná webová aplikace (např. web /shop a /opc ukazuje na /var/www/opc):

```
Alias /shop /var/www/opc
Alias /opc /var/www/opc
<Directory /var/www/opc >
   Order allow,deny
   Allow from all
</Directory>
```

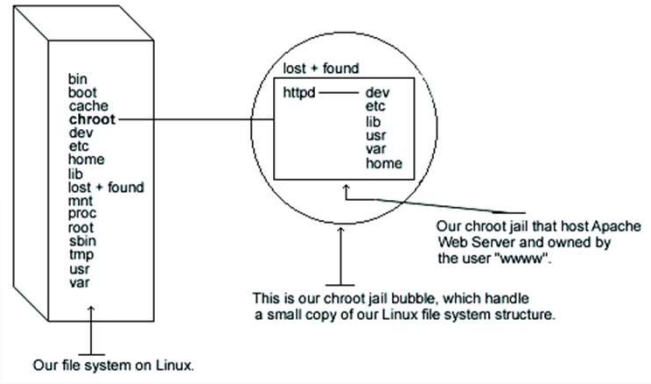
Apache – Mód rewrite

- Mód rewrite = pěkná URL
- Například adresu http://www.example.com/index.php?nazev_clanku=sprava_linuxoveho_serveru přepíše na http://www.example.com/clanky/sprava_linuxoveho_serveru.html
- Povolení módu:

  a2enmode rewrite

- Konfigurace pomocí direktiv RewriteEngine, RewriteBase a RewriteCond

Apache – Mód chroot

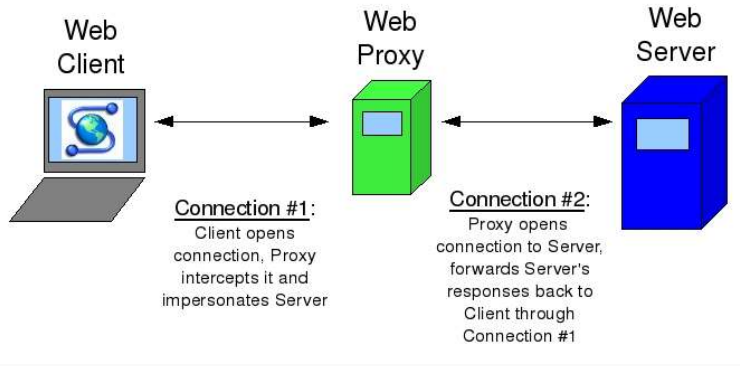


- Zvýšení bezpečnosti
- Udělá pro apache určitý adresář kořenovým adresářem
- Teoreticky se není možné dostat z tohoto adresáře
- Potřeba doinstalovat libapache2-mod-chroot:

  apt-get install libapache2-mod-chroot
- Potřeba povolit mód:

  a2enmod mod_chroot
- A zvolit adresář (v httpd.conf): `ChrootDir /var/www`
- Pozor! Několik souvisejících problémů (více informací na webu)

Apache – Proxy



- Proxy se chová jako zástupce – v tomto kontextu je web proxy zástupce, přes který se dostáváme k cílovému zařízení nebo portu
- Důvody: DMZ, přesměrování na jiný port, …
- Vyzkoušíme příště pro SVN, GIT a Jenkins

Apache – SSL (HTTPS)

- Potřeba povolit SSL mód a v apache a restartovat ho

  a2enmod ssl

  service apache2 restart
- Povolení připravené šablony pro zabezpečený web:

  a2ensite default-ssl
- Potřeba získat certifikát (nechat si podepsat od autority nebo si ho sám podepsat)

Apache – Varování

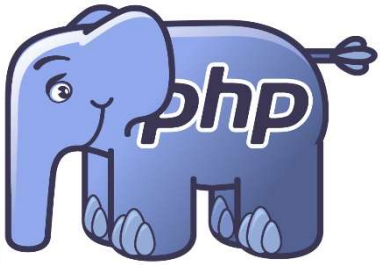
- Časté varování při spouštění nebo restartu apache:

„apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName“

- Řešení:

1. V /etc/apache2/apache2.conf doplnit na konci direktivu `ServerName localhost`
2. V /etc/hostname mít plně kvalifikované jméno (např. kucera.pp.fbmi.cvut.cz)

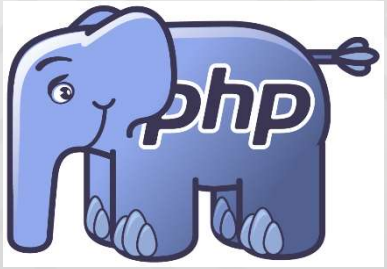
PHP - konfigurace



- Hlavní konfigurační soubor pro apache: /etc/php/<VERZE>/apache2/php.ini
- Velice dobře dokumentovaný soubor
- Detailnější konfigurace: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-konfigurace-lamp-php

PHP
– Důležité parametry a jejich optimální hodnoty I

```
expose_php = Off

memory_limit a max_execution_time : <snížit podle
výkonu serveru>

diplay_erros = Off <- důležitý parametr, v produkční
verzi na Off!

display_startup_errors = Off

allow_url_fopen = Off

allow_url_include = Off
```

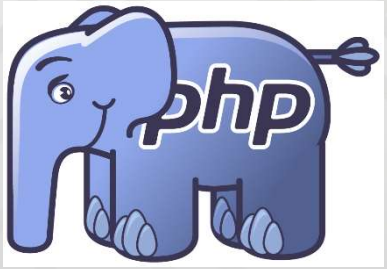


PHP
– Důležité parametry a jejich optimální hodnoty II

```
disable_functions = shell_exec, exec, system, passthru,
proc_close, proc_open, proc_get_status, proc_nice,
proc_terminate, dl, popen, pclose, chown,
disk_free_space, disk_total_space, diskfreespace,
fileinode, max_execution_time, set_time_limit,
highlight_file, show_source, phpinfo, chgrp, symlink
```

- Po úpravě php.ini je potřeba znova načíst konfiguraci:

service apache2 reload



MySQL – Konfigurace I

- Správa pomocí PHPMyAdmin:

1. Vytvoření databáze
2. Vytvoření uživatele, který bude mít přístup do nové databáze
3. Nastavení oprávnění
4. Otestování připojení

- Více informací na:

http://www.linuxexpres.cz/praxe/sprava-databazi-pomoci-phpmyadmin

MySQL – Konfigurace II

- Pro každý systém a eshop vytvoříme vlastní databázi
- Například databáze **wp, jml, zen, opc**
- Vytvoříme uživatele(é) a dáme mu přístup k databázím: buď pro každou databázi jiného uživatele (obecně lepší a bezpečnější) nebo hromadného uživatele, který bude mít přístup ke všem databázím (nepraktické řešení, ale v rámci tohoto předmětu dostačující)

HOSTS a Virtuální hostové v apache

- Pokud nemáme stále upravený soubor hosts v OS, ze kterého budeme přistupovat k našim webům nebo nemáme nakonfigurovaný Apache pro virtuální hosty, nelze následující CMS systémy a e-shopy ověřit (viz *Dočasná editace hosts a Apache – konfigurace* a dále)

CMS

- Content management system(s)
- Redakční systémy
- Příklady:
  - Wordpress: http://cs.wordpress.org/
  - Joomla: http://www.joomlaportal.cz/
  - Drupal: https://www.drupal.cz/

Wordpress

- Využívá PHP a MySQL
- Přes 10 milionů stažení (15 % webových stránek celosvětově)
- Pluginy, skiny, více webů pod jednou správou
- Česká lokalizace: http://cs.wordpress.org/
- Ke stažení: http://wordpress.org/latest.zip
- Možnost instalace pomocí apt-get

Wordpress – Instalace přes apt-get

- Obdobně náročná cesta jako při manuální instalaci
- Samotná instalace:

  apt-get install wordpress

- Dále je potřeba vytvořit symbolický link pro Apache:

  ln -s /usr/share/wordpress /var/www/html/wordpress

- A další kroky…. Viz podrobný návod na: https://help.ubuntu.com/community/WordPress
- My budeme ale instalovat Wordpress **manuálně**

wget

- Konzolová utilita pro stahování souborů z webu
- Např. stažení souboru latest.zip z webu Wordpressu:

```
wget ‘http://wordpress.org/latest.zip‘
```

Wordpress – Instalace

- Rozbalíme stažený archiv do /var/www/wordpress (např. pomocí unzip či nativně v Midnight Commanderu)
- Změníme rekurzivně vlastníka adresáře /var/www/wordpress na www-data:

  chown -R www-data:www-data /var/www/wordpress
- V prohlížeči spustíme adresu: mywordpress.<příjmení>.edu
- Dále postupujeme podle pokynů
- Instalační průvodce je popsán v souboru readme.html

Wordpress – Konfigurace

WordPress

- Vytvořte si blog
- Vytvořte si fórum
- Vyzkoušejte si vložit příspěvek a nový thread to fóra

Joomla a Drupal

- Obdobně jako Wordpress zprovozněte ještě další CMS – Joomla a Drupal
- Drupal se dá také instalovat přes apt-get, nicméně jej nainstalujte opět manuálně
- Vytvořte další virtuální hosty a jejich aliasy dle tabulky
- Vytvořte příslušné složky ve /var/www/ pro každý CMS
- CMS stáhněte, rozbalte, popřípadě změňte rekurzivně opět vlastníka souborů
- Připojte se k CMS přes webový prohlížeč a dokončete instalaci/konfiguraci CMS
- Ověřte funkčnost vložením příspěvku či blogu

Monitorace a zálohování Linuxového serveru

- Nyní zprovozníme monitorování serveru a jeho automatické periodické zálohování

Úprava hosts

- Nastartujte VM a porovnejte jeho IP adresu se záznamy v souboru hosts, jež jsme přidávali minule
- DHCP velice pravděpodobně přidělilo VM jinou IP adresu, proto záznamy v souboru hosts upravte na aktuální IP adresu VM

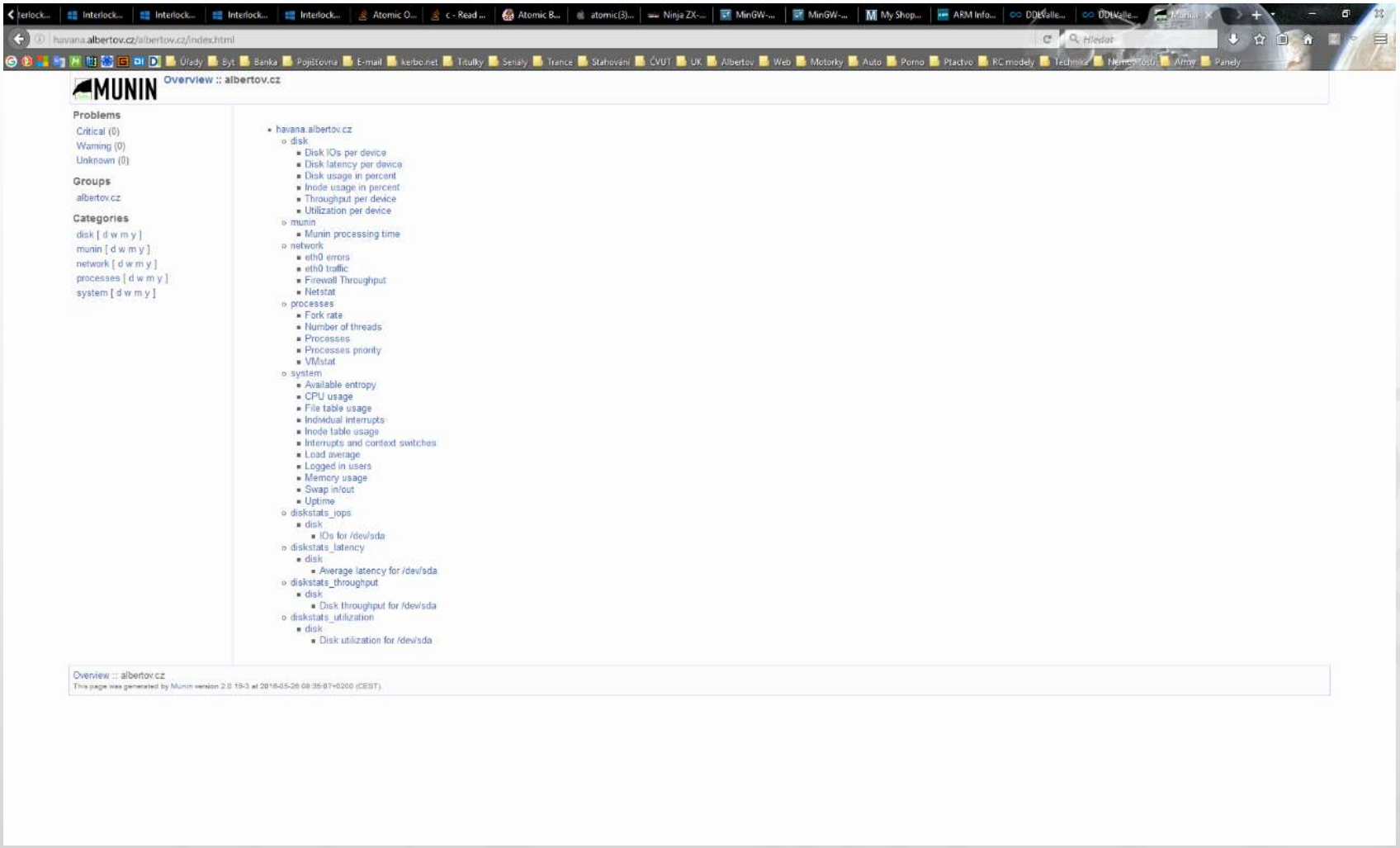
Monitorace serveru

- Sledování využití prostředků (RAM, disk, CPU)
- Sledování běžících služeb
- Sledování dostupnosti serveru
- Indikace napadení serveru
- Příklady:
  - Munin: http://munin-monitoring.org/
  - Nagios: http://www.nagios.org/
  - M/Monit: http://mmonit.com/

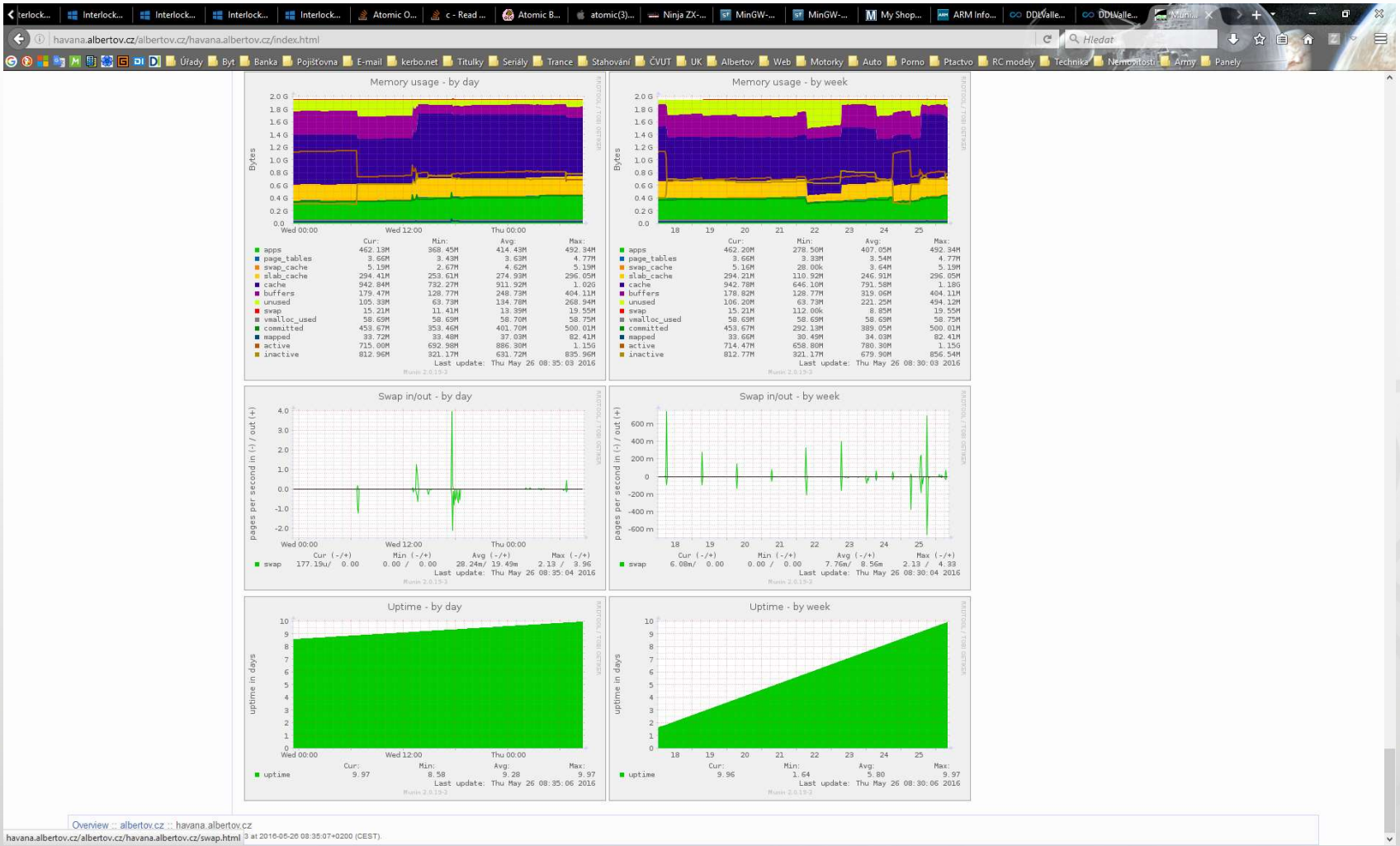
Munin

- **Serverová** část a **uzel** – serverová část sbírá data z uzlů a zobrazuje je
- Sledování HW prostředků, databází, e-mailové fronty, procesů
- Modulární systém – možnost vytvoření vlastního modulu
- Sledování vzdálených systémů (= uzlů)

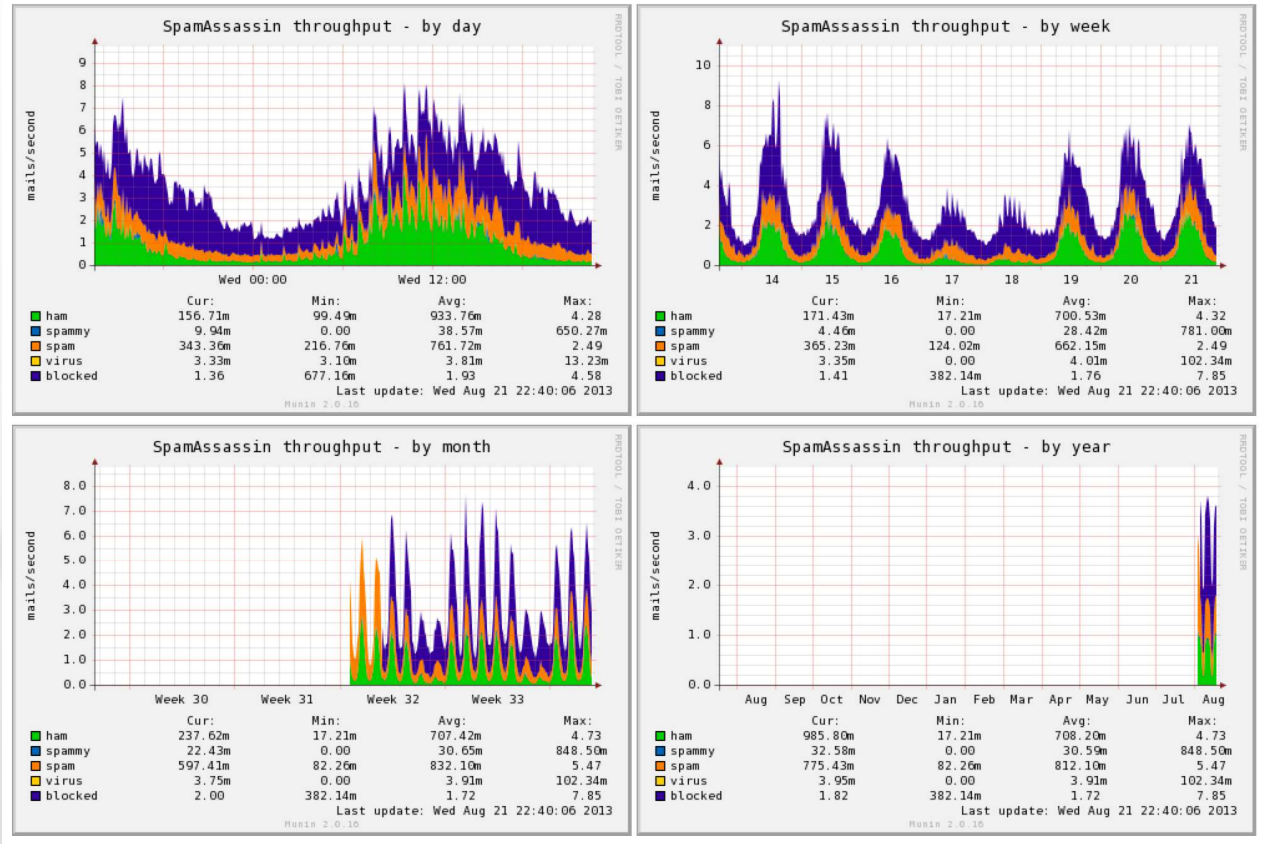
Munin – Ukázka I



Munin – Ukázka II



Munin
– Ukázka sledování spamu na mailserveru



MUNIN

Munin

- Pokud nemáte přidán následující záznam v souboru hosts na OS, ve kterém ověřujete funkčnost, nyní jej přidejte:

<IP adresa VM> munin.<příjmení>.io

Munin – Záznam v hosts

- **Serverová** část a **uzel** – serverová část sbírá data z uzlů a zobrazuje je
- Sledování HW prostředků, databází, e-mailové fronty, procesů
- Modulární systém – možnost vytvoření vlastního modulu
- Sledování vzdálených systémů (= uzlů)

Munin – Instalace

- Instalace serverové části (munin) a uzlu (munin-node):

  apt-get install munin munin-node

- Po instalaci je třeba nakonfigurovat jak server, tak uzel

Munin – Konfigurace

- V našem případě bude server (munin.<příjmení>.io) naslouchat pouze na lokální smyčce (pouze lokální uzel)
- Konfigurační soubor pro serverovou část:

  /etc/munin/munin.conf

- Konfigurační soubor pro uzel:

  /etc/munin/munin-node.conf

Munin – Konfigurace uzlu

- Editace /etc/munin/munin-node.conf:
- Jméno uzlu pro zobrazení (slouží jako pojistka):

  host_name <prijmeni>.ppp.fbmi.cvut.cz
- Seznam povolených adres - serverů, jež se budou k uzlu připojovat, v našem případě pouze localhost (pozor, zápis pomocí regulárního výrazu):

  allow ^127\.0\.0\.1$
- Na které adrese má uzel poslouchat (v našem případě opět pouze localhost):

  host 127.0.0.1

Munin – Konfigurace serveru I

- Nejprve je potřeba připravit adresář, do kterého se bude generovat webový obsah serverové části:

```
mkdir /var/www/munin
chown munin:munin /var/www/munin
chmod 777 /var/www/munin
```

Munin – Konfigurace serveru II

- Editace /etc/munin/munin.conf - povolení a konfigurace proměnných:

dbdir /var/lib/munin

htmldir /var/www/munin

logdir /var/log/munin
rundir /var/run/munin

tmpldir /etc/munin/templates

Munin – Konfigurace serveru III

- Seznam uzlů, ze kterých zobrazovat data:

[<prijmeni>.ppp.fbmi.cvut.cz]

address 127.0.0.1

use_node_name yes

- Direktivou **use_node_name** nastavujeme, zda-li využijeme jméno uzlu, které nám nod posílá (viz konfigurace uzlu)

Munin – Konfigurace apache

- Dvě možnosti:

1. editace apache.conf v adresáři /etc/munin: úprava cest a následné povolení site
2. Přímá editace v /etc/apache2/ports.conf: přidání virtuálního hosta, který bude ukazovat na /var/www/munin

Munin – Restart služeb

- Restart služeb:

service munin-node restart

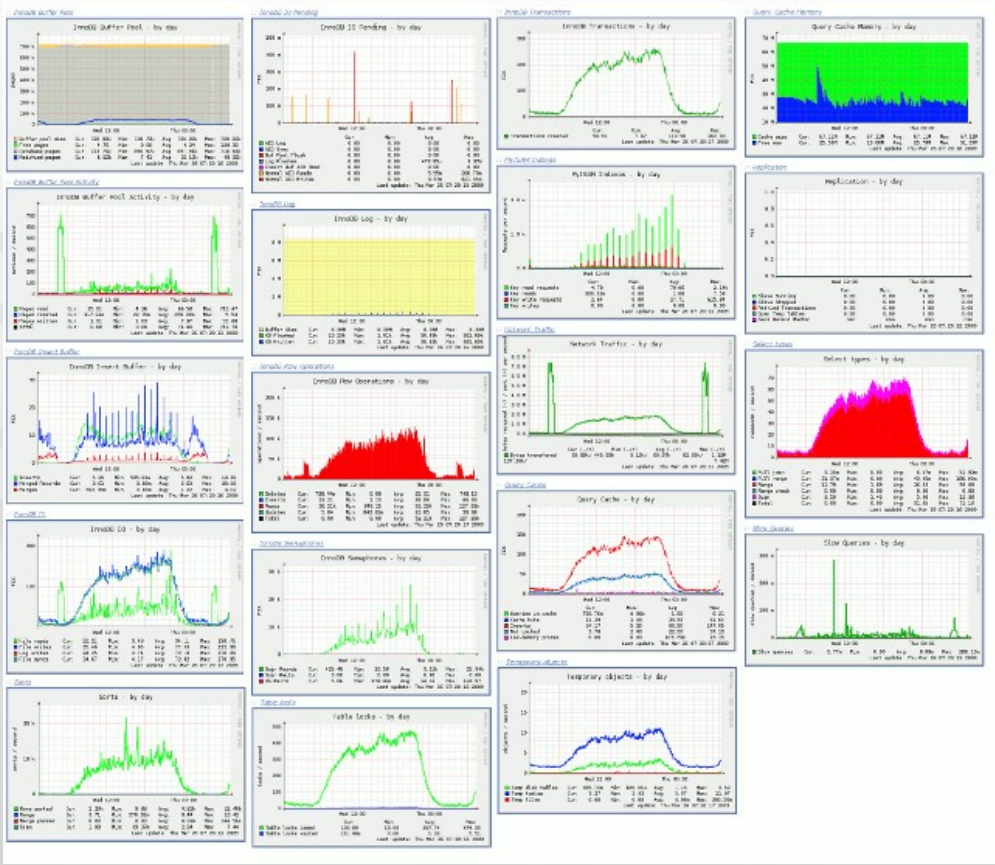
service munin restart

service apache2 restart

- A chvíli počkat, než se vygenerují první statistiky

Munin – Ověření

- Ověření funkčnosti po instalaci: otevření munin.<příjmení>.io v prohlížeči



Munin – Zabezpečení

- Omezení čtení adresáře z různých IP adres (konfigurace apache – cvičení 1 – editace /etc/apache2/ports.conf)
- Dodatečná HTTP autentizace pomocí **.htaccess** a **.htpasswd** (detailněji další cvičení)
- Více na http://linuxdev.dk/articles/monitoring-munin

Munin – Více serverů I

- Na sledované počítače se nainstaluje uzel:

  apt-get install munin-node

- Uzel naslouchá na portu 4949 -> nutno povolit v **iptables**
- Povolení přístupu serverové části (/etc/munin/munin-node.conf) nastavením IP adresy počítače, na které munin běží (regulární výraz!):

  allow ^1\.2\.3\.4$

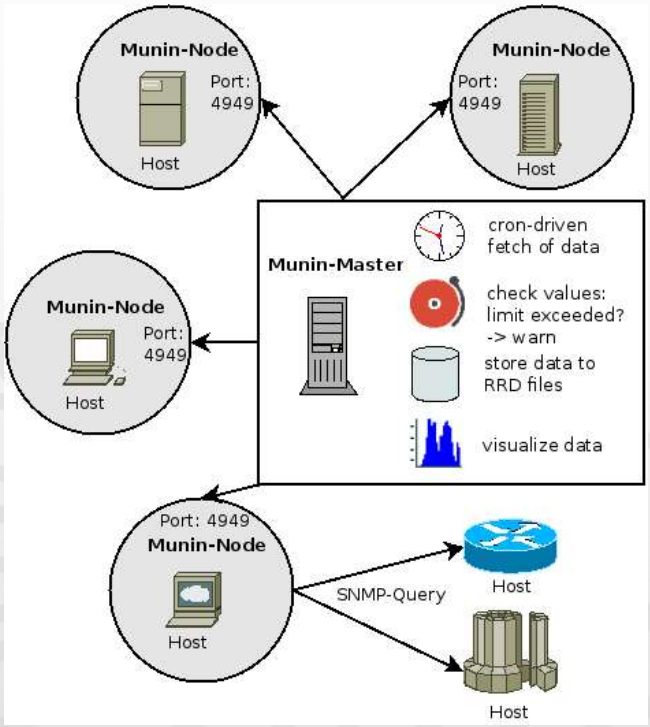
Munin – Více serverů II

- U serverové (centrální) části přidání každého sledovaného serveru v souboru /etc/munin/munin.conf:

  [server1.mojedomena.com]

  address 1.2.3.4

  use_node_name yes



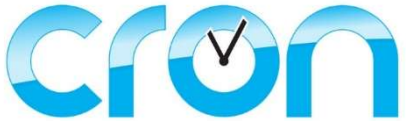
Munin – Více serverů III

- **Praktické vyzkoušení** – u vašeho serveru povolte veřejný přístup ze všech adres (a nezapomeňte povolit v **iptables** port 4949, na němž uzel vysílá) a sdělte kolegovi svoji **IP** adresu
- Kolega si Vás přidá jako nový uzel
- Sledujte servery a využití Vašich kolegů

Munin – Závěr

- Detailní průvodce: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-monitorovani-serveru-munin
- Dokumentace uzlu: http://munin-monitoring.org/wiki/munin-node.conf

CRON I



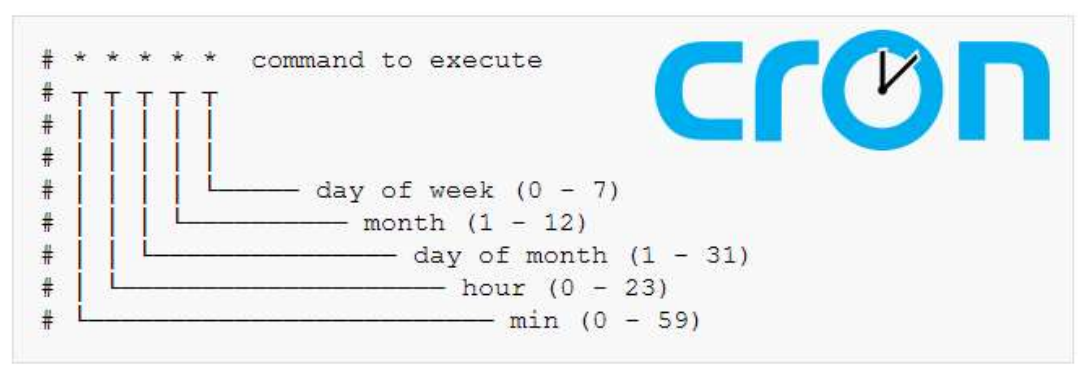
- Správce úloh v Linuxu, obdoba Plánovače úloh (Schedule Manager) ve Windows
- Jednoduché použití – Adresáře /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly a /etc/cron.monthly, do kterých se uloží spustitelný skript (chmod +x), jež provede požadovanou činnost
- Pozor! skript nesmí mít příponu (viz man cron)

CRON II

- Složitější periody nebo specifické časy se nastavují pomocí přidání záznamu do souboru /etc/crontab
- Například ve 14:15 1. dne každý měsíc:

```
15 14 1 * * /srv/backup.sh
```

- Více na: http://www.cyberciti.biz/faq/how-do-i-add-jobs-to-cron-under-linux-or-unix-oses/



CRON
– Mmožné praktické použití

- Záloha SVN repozitářů – 1x týdně
- Záloha GIT repozitářů/Gitlabu – 1x týdně
- Záloha celého SVN serveru – 1x měsíčně
- Záloha konfigurace Jenkinse – 1x měsíčně

Zálohovací skripty

- Zálohováním se v tomto kontextu rozumí zabalení souborů a adresářů do archivu nebo zavolání exportu zálohy z dané služby a odeslání na FTP nebo sdílenou složku (SAMBA)
- Požadavky:
  - (e-mailová) notifikace
  - Připojení na cílové úložiště
  - Ošetření možných chyb
  - Pravidelné spouštění (není přímo součástí skriptu)

Zálohovací skripty – Reálná aplikace

- Shellový skript, který zálohuje SVN repozitáře tak, že je zabalí do archivu s časovou značkou a archiv přesune na SAMBA server a upozorní administrátora o úspěchu nebo neúspěchu

Zálohovací skripty – Ověření

- Použijte a upravte vzorový skript tak, aby zálohoval workspace Jenkinse jeho zabalením do archivu a tento archiv poté pouze přesunul na nějaké jiné místo v serveru (např. /srv/backups)
- Nastavte, aby byl skript spouštěn každé 3 minuty a ověřte, že zálohování funguje
- Poté zálohování zrušte
- Tip: workspace Jenkinse je adresář „workspace“ v domovském adresáři Jenkinse

Děkuji za pozornost!

David Gillar

Katedra ICT v lékařství,
Fakulta biomedicínského inženýrství ČVUT

Podpořeno projektem RPAPS FBMI 2018