

# Zápočet 01

## Zadání

1. Nastavte v linuxu raid5 ze všech dostupných disků. (1 bod)
2. Vytvořte nad raidem z předchozího úkolu LVM, skupina se bude jmenovat data a svazek share. (1 bod)
3. Naformátujte tento nově vytvořený svazek jako EXT4 a připojte ho do /home. Nastavte systém tak, aby tato složka byla připojena i po startu systému a to pomocí názvu naformátovaného svazku. (1 bod)
4. Spustěte a nastavte na Linuxu DNS pro doménu test.spos a nastavte doručování pošty pro subdoménu mail.test.spos na Linux server a nastavte pro tento server i reverzní záznam (veřejná IP). (1 bod)
5. Spustěte na Linuxu poštovní server, nastavte doručování pošty pro email hostmaster@mail.test.spos do schránky user1 a webmaster@mail.test.spos do schránky user2. Využijte vytvořené DNS. (2 body)
6. Nainstalujte server pro stahování pošty modernějším z dostupných protokolů s i bez podporou šifrování a ověřte jeho funkčnost. (2 body)
7. Omezte přístup na stahování pošty pro nešifrovaná spojení ze sítě kde se nachází Linux a pro šifrovaná spojení ze sítě ZČU. (1 bod)
8. Nainstalujte www server s podporou PHP5, zakažte funkci phpinfo() a vytvořte stránku, která ověří zakázanou funkci. (1 bod)

# Nastavení sítě

- **Nastavení DHCP**

```
vi /etc/network/interfaces
```

```
auto enp0s3
iface enp0s3 inet dhcp
```

Ovládání kurzoru: →↑↓← (**šipky**)

Před psaním stisknout **i**, následně ukončit editaci **Esc**.

Mazání stisknutím **x**.

Ukončení bez uložení **Esc** a **:q!**.

Ukončení s uložením **Esc** a **:x**.

- **Restartování služby**

```
/etc/init.d/networking restart
```

- **Vypsání přidělené IP**

```
ip addr
```

- **Nainstalování nástroje nano :-)**

```
apt install nano
```

## 1. Nastavení raidu 5

*Nastavte v linuxu raid5 ze všech dostupných disků.*

- **Vypsání dostupných disků**

```
lsblk
```

sdb	8:16	0	200M	0	disk
sdc	8:32	0	200M	0	disk
sdd	8:48	0	200M	0	disk
└sdd1	8:49	0	199M	0	part

- **Smazání oblasti sdd1**

```
cfdisk /dev/sdd
```

- Zvolit [Delete] → [Write] → yes → [Quit]

- **Instalace balíčku mdadm**

```
apt install mdadm
```

- **Založení raidu 5**

```
mdadm -Cv /dev/md0 -l5 -n3 /dev/sd[bcd]
```

- **Vypíše stav raidu (kapacita, typ, počet zařízení...)**

```
mdadm --detail /dev/md0
```

## 2. Vytvoření LVM nad raidem

Vytvořte nad raidem z předchozího úkolu LVM, skupina se bude jmenovat data a svazek share.

- **Instalace balíčku lvm2**  
`apt install lvm2`
- **Vytvoření skupiny pojmenované data**  
`vgcreate data /dev/md0`
- **Vypsání existujících skupin**  
`vgdisplay`
- **Vytvoření logického svazku pojmenovaného share**  
`lvcreate -L 396M -n share data`
- **Vypsání existujících svazků**  
`lvdisplay`

## 3. Naformátování svazku a automatické připojení jako /home

Naformátujte tento nově vytvořený svazek jako EXT4 a připojte ho do /home. Nastavte systém tak, aby tato složka byla připojena i po startu systému a to pomocí názvu naformátovaného svazku.

- **Naformátování share na ext4**  
`mkfs.ext4 /dev/data/share`
  - **Nastavení připojení share jako /home**  
`nano /etc/fstab`
- ```
/dev/data/share /home ext4 defaults 0 2
```
- **Připojení všech oddílů z fstab**  
`mount -a`
  - **Vypsání diskových oddílů včetně použitých FS a přípojných bodů**  
`lsblk -f`
  - **Nastavení názvu svazku na share**  
`e2label /dev/data/share share`
  - **Nastavení připojení tak, aby se provedlo podle názvu svazku**  
`nano /etc/fstab`

```
LABEL=share /home ext4 defaults 0 2
```

*tzn. jen se /dev/data/share přepíše na LABEL=share*

## 4. Nastavení DNS pro doménu test.spos

*Spustíte a nastavíte na Linuxu DNS pro doménu test.spos a nastavíte doručování pošty pro subdoménu mail.test.spos na Linux server a nastavíte pro tento server i reverzní záznam (veřejná IP).*

- **Přidání záznamu do /etc/hosts**

```
nano /etc/hosts
```

```
127.0.0.2      test.spos
```

- **Instalace nástroje bind9**

```
apt install bind9
```

- **Restartování bind9**

```
systemctl restart bind9.service
```

- **Kontrola, jestli bind9 běží**

```
ps aux | grep bind
```

- **Zobrazení posledních řádků systémových logů**

```
tail -n 50 /var/log/syslog
```

- **Přesun do adresáře bind9**

```
cd /etc/bind
```

- **Vytvoření kopie souboru podle šablony**

```
cp db.empty db.test.spos
```

- **Úprava souboru db.test.spos**

```
nano db.test.spos
```

```
test.spos.      IN      A           127.0.0.2
mail.test.spos. IN      A           127.0.0.2
test.spos.      IN      NS          test.spos.
mail            IN      MX          6      mail.test.spos.
```

- **Vytvoření zóny**

```
nano named.conf.local
```

```
zone "test.spos" {
    type master;
    file "/etc/bind/db.test.spos";
    allow-transfer {"any";}
};
```

- **Ověření funkčnosti**

```
host -t NS test.spos localhost
```

## 5. Nastavení poštovního server

*Spustíte na Linuxu poštovní server, nastavíte doručování pošty pro email `hostmaster@mail.test.spos` do schránky `user1` a `webmaster@mail.test.spos` do schránky `user2`. Využijte vytvořené DNS.*

- **Instalace balíčku postfix a bsd-mailx**

```
apt install postfix bsd-mailx
```

Postfix Configuration  
Internet Site  
System mail name: mail.test.spos

- **Úprava nastavení /etc/postfix/main.cf**

nano /etc/postfix/main.cf

```
myhostname = mail.test.spos
```

- **Restartování služby po úpravě main.cf**

service postfix reload

- **Vypsání existujících uživatelů**

cat /etc/passwd

- **Přidání uživatelů user1 a user2**

useradd user1 && useradd user2

- **Nastavení hesla pro uživatele user1**

passwd user1

- **Nastavení aliasů**

nano /etc/aliases

```
hostmaster: user1  
webmaster: user2
```

- **Načtení aliasů po změně /etc/aliases**

newaliases

- **Odeslání pošty na hostmaster@mail.test.spos**

echo "TELO ZPRAVY" | mail -s "PREDMET" hostmaster@mail.test.spos

- **Instalace mailového klienta mutt**

apt install mutt

- **Otevření pošty v nástroji mutt**

mutt -f /var/spool/mail/user1

## 6. Stahování e-mailů

*Nainstalujte server pro stahování pošty modernějším z dostupných protokolů s i bez podporou šifrování a ověřte jeho funkčnost.*

- **Instalace balíčku dovecot pro stahování pošty**

- **Protokol IMAP (modernější)**

- apt install dovecot-imapd

- **Protokol POP3**

- apt install dovecot-pop3d

- **Vytvoření domovského adresáře pro uživatele user1**

mkdir /home/user1

chown user1 user1

- **Přidání oprávnění pro mail uživateli user1**

usermod -g mail user1

- **Spojení IMAP**

nc localhost 143

- **Přihlášení se jako user1**  
a login user1 heslo
- **Seznam**  
a list "" "\*"
- **Počet zpráv ve schránce**  
a status inbox (messages)
- **Podrobnější přehled (počet zpráv, nedávné, nepřečtené)**  
a examine inbox
- **Načíst první zprávu**  
a fetch 1 body[]
- **Odhlášení se**  
a logout

## 7. Omezení přístupu na stahování pošty

*Omezte přístup na stahování pošty pro nešifrovaná spojení ze sítě kde se nachází Linux a pro šifrovaná spojení ze sítě ZČU.*

- **Vypsání pravidel firewallu iptables**  
iptables -nvL
- **Vymazání pravidel firewallu iptables**  
iptables -F
- **Povolení portu TCP/143 (imap) z 10.0.2.x**  
iptables -A INPUT -s 10.0.2.0/24 -p tcp --dport 143 -j ACCEPT
- **Zakázání portu TCP/143 (imap) z ostatních adres**  
iptables -A INPUT -p tcp --dport 143 -j DROP
- **Povolení portu TCP/993 (imap s SSL) ze sítě ZČU (147.228.x.x)**  
iptables -A INPUT -s 147.228.0.0/16 -p tcp --dport 993 -j ACCEPT
- **Zakázání portu TCP/993 (imap s SSL) z ostatních adres**  
iptables -A INPUT -p tcp --dport 993 -j DROP

## 8. Webový server s podporou PHP5

*Nainstalujte www server s podporou PHP5, zakažte funkci phpinfo() a vytvořte stránku, která ověří zakázanou funkci.*

- **Výpis procesů, které využívají port 80 (služba HTTP)**

```
lsof -i :80
```

```
lighttpd 545 www-data 4u IPv4 12760 0t0 TCP *:http (LISTEN)
```

*Na stroji je již nainstalován www server lighttpd.*

- **Přidání starších zdrojů s balíčkem php5**

```
nano /etc/apt/sources.list
```

```
deb http://ftp.cz.debian.org/debian/ jessie main
```

- **Aktualizace zdrojů softwaru po změně sources.list**

```
apt update
```

- **Instalace balíčků php5**  
`apt install php5 php5-cgi`
- **Vytvoření soubor index.php**
  - **Přesun do adresáře**  
`cd /var/www/html`
  - **Záloha stávajícího indexu**  
`mv index.lighttpd.html index.html.backup`
  - **Vytvoření index.php**  
`echo "<h1>BEZI</h1><?php phpinfo(); ?>" > index.php`
- **Povolení PHP**  
`lighttpd-enable-mod fastcgi fastcgi-php`
- **Restartování www serveru**  
`service lighttpd force-reload`
- **Vypsání stránky**
  - **Pomocí curl do terminálu**  
`curl test.spos`
  - **Pomocí prohlížeče links**  
`apt install links`  
`links http://test.spos`
- **Zákaz funkce phpinfo()**  
`nano /etc/php5/cgi/php.ini`  

`disable_functions = phpinfo`
- **Restartování www serveru**  
`service lighttpd force-reload`
- **Vypsání stránky**  
`curl test.spos`

# Zápočet 02

## Zadání

1. Vytvořte RAID5 nad všemi disky v systému kromě / a swapu. (1 bod)
2. Naformátujte tento nově vytvořený svazek jako EXT4 a připojte ho do /home. Nastavte systém tak, aby tato složka byla připojena i po startu systému a to pomocí názvu naformátovaného svazku. (1 bod)
3. Nainstalujte MySQL. Vytvořte uživatele spos s heslem spos\*2018, který bude mít všechna práva na nově vytvořenou db spos a bude se moc připojit pouze z 10.0.0.XXX. Kde XXX je číslo vašeho virtuálu. (1 bod)
4. Vytvořte v db z předchozího bodu tabulku skore, obsahující sloupce id - autoincrement, jmeno - string, datum - datum a cas, skore - integer a naplňte ji alespoň 30 náhodnými a různými výsledky. (1 bod)
5. Nainstalujte webserver s podporou PHP a vytvořte skript, který bude zobrazovat obsah tabulky skore seřazenou podle skore sestupne. Web ať běží na portu 8080. (2 body)
6. Vytvořte další virtuální servery na portech 8181 a 8282 poslouchající pouze na vaší privátní adrese 10.0.0.XXX. Na daných webech se bude zobrazovat číslo portu. (1 bod)
7. Zpřístupněte oba weby pomocí libovolné reverzní proxy / load balanceru s podporou https, který bude používat vlastní self-signed certifikát pro domenu vysledky.spos na veřejné IP adrese vašeho virtuálu. (2 body)
8. Proveďte základní zabezpečení vašeho virtuálu, přihlašování pouze pomocí klíčů, dostupné SSH pouze ze sítě ZCU. (1 bod)

## Jmenné servery

- **Testování správného nastavení DNS**  
ping google.com  
nefunguje
- **Oprava zadaných jmenných serverů**  
nano /etc/resolv.conf

```
nameserver 8.8.8.8
```

## 1. Nastavení raidu 5

*Vytvořte RAID5 nad všemi disky v systému kromě / a swapu.*

- **Instalace mdadm**  
apt install mdadm
- **Nastavení raidu 5**  
mdadm -Cv /dev/md0 -l5 -n3 /dev/sd[bcd]



## 2. Připojení raidu jako /home

*Naformátujte tento nově vytvořený svazek jako EXT4 a připojte ho do /home. Nastavte systém tak, aby tato složka byla připojena i po startu systému a to pomocí názvu naformátovaného svazku.*

- **Naformátování md0 na ext4**  
`mkfs.ext4 /dev/md0`
- **Nastavení připojení share jako /home**  
`nano /etc/fstab`

|          |       |      |          |   |   |
|----------|-------|------|----------|---|---|
| /dev/md0 | /home | ext4 | defaults | 0 | 2 |
|----------|-------|------|----------|---|---|
- **Připojení všech oddílů z fstab**  
`mount -a`
- **Vypsání diskových oddílů včetně použitých FS a přípojných bodů**  
`lsblk -f`

## 3. Nastavení MySQL

*Nainstalujte MySQL. Vytvořte uživatele spos s heslem spos\*2018, který bude mít všechna práva na nově vytvořenou db spos a bude se moc připojit pouze z 10.0.0.XXX. Kde XXX je číslo vašeho virtuálu.*

- **Přidání IP adresy**  
`ip a a 10.0.0.15 dev enp0s3`
- **Instalace MySQL serveru**  
`apt install mysql-server`
- **Přihlášení se**  
`mysql -uroot -pheslo`
- **Vytvoření uživatele spos**  
`CREATE USER 'spos'@'10.0.0.15' IDENTIFIED BY 'spos*2018';`
- **Vypsání uživatelů**  
`SELECT host, user FROM mysql.user;`
- **Vytvoření databáze spos**  
`CREATE DATABASE spos;`
- **Zobrazení existujících databází**  
`SHOW DATABASES;`
- **Udělení oprávnění uživateli spos k databázi spos**  
`GRANT ALL PRIVILEGES ON spos.* TO 'spos'@10.0.0.15;`
  - **Aplikování oprávnění**  
`FLUSH PRIVILEGES;`
  - **Zobrazení oprávnění uživatele spos**  
`SHOW GRANTS FOR 'spos'@10.0.0.15`
- **Změna adresy poslechu**  
`nano /etc/mysql/my.cf`

```
[mysqld]  
bind-address = 10.0.0.15
```

- **Restartování služby MySQL**  
service mysql restart
- **Přihlášení se jako uživatel spos**  
mysql -h10.0.0.15 -uspos -pspos\*2018

## 4. Vytvoření tabulky MySQL

Vytvořte v db z předchozího bodu tabulku skore, obsahující sloupce id - autoincrement, jmeno - string, datum - datum a cas, skore - integer a naplňte ji alespoň 30 náhodnými a různými výsledky.

- **Přepnutí se do databáze spos**  
USE spos;
- **Vytvoření tabulky**  
CREATE TABLE skore(  
    id INT(6) AUTO\_INCREMENT PRIMARY KEY,  
    jmeno VARCHAR(64),  
    datum DATETIME,  
    skore INT(8));
- **Naplnění tabulky daty**  
for i in `seq 1 30`; do echo "INSERT INTO skore VALUES(null,'Jarda',now(),\$i)" |  
mysql -h10.0.0.15 -uspos -pspos\*2018; done
- **Vypsání dat v tabulce skore**  
SELECT \* FROM skore;

## 5. Webserver s PHP

Nainstalujte webserver s podporou PHP a vytvořte skript, který bude zobrazovat obsah tabulky skore serazenou podle skore sestupne. Web ať běží na portu 8080.

- **Instalace webového serveru Nginx**  
apt install nginx
- **Instalace balíčků php5**  
apt install php5 php5-cgi php5-fpm php5-mysql
- **Vytvoření adresáře virtuálního hosta**  
cd /var/www/  
mkdir web8080
- **Vytvoření indexu**  
nano web8080/index.php

```
<?php  
$conn = new mysqli("10.0.0.15","spos","spos*2018","spos","3306");  
$sql = "SELECT * FROM skore ORDER BY skore DESC";  
$result = $conn->query($sql);  
if($result->num_rows > 0) {  
    while($row = $result->fetch_assoc()) {
```

```

    echo $row["skore"]." ";
  }
}
$conn->close();
?>

```

- **Nastavení virtuálního hosta**

```
cd /etc/nginx/sites-available/default
```

```

server {
    listen 8080;
    root /var/www/web8080;
    index index.php;
    location ~ /\.php$ {
        try_files $uri =404;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
        fastcgi_index index.php;
        include fastcgi.conf;
    }
}

```

- **Restartování služby Nginx**

```
service nginx restart
```

- **Zapnutí debugingu v PHP5**

```
nano /etc/php5/fpm/php.ini
```

```

error_reporting = E_ALL
display_errors = On

```

- **Restartování služby PHP5 FPM**

```
service php5-fpm restart
```

- **Vypsání stránky**

```
curl test.spos:8080
```

## 6. Virtuální servery

*Vytvořte další virtuální servery na portech 8181 a 8282 poslouchající pouze na vaší privátní adrese 10.0.0.XXX. Na daných webech se bude zobrazovat číslo portu.*

- **Vytvoření adresářů virtuálních hostů**

```
cd /var/www/
mkdir web8181 web8282
```

- **Vytvoření indexů**

```

echo "8181" > web8181/index.html
echo "8282" > web8282/index.html

```

- **Nastavení virtuálních hostů**

```
nano /etc/nginx/sites-available/default
```

```

server { # 1. ZPUSOB
    listen 10.0.0.15:8181;
    server_name test.spos;
    root /var/www/web8181;
    index index.html;
}

```

```
server { # 2. ZPUSOB
    listen 8282;
    server_name test.spos;
    root /var/www/web8282;
    index index.html;
    location / {
        allow 10.0.0.15;
        deny all;
    }
}
```

- **Restartování služby Nginx**

```
service nginx restart
```

- **Zobrazení v curl**

```
curl 10.0.1.15:8181 --resolve 10.0.1.15:8181:10.0.0.15
```

## 7. Nastavení load balanceru a HTTPS

*Zpřístupněte oba weby pomocí libovolné reverzní proxy / load balanceru s podporou https, který bude používat vlastní self-signed certifikát pro domenu vysledky.spos na veřejné IP adrese vašeho virtuálu.*

- **Nastavení load balanceru a HTTPS v Nginx**

```
nano /etc/nginx/sites-available/default
```

```
upstream spos {
    server 10.0.0.15:8181;
    server 10.0.0.15:8282;
}
server {
    listen 443 ssl;
    server_name test.spos;
    ssl on;
    ssl_certificate /etc/nginx/ssl/server.crt;
    ssl_certificate_key /etc/nginx/ssl/server.key;
    location / {
        proxy_pass http://spos;
    }
}
```

- **Vytvoření certifikátu**

- **Vytvoření adresáře ssl**

```
cd /etc/nginx
mkdir ssl
cd ssl
```

- **Vytvoření souborů certifikátu**

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout server.key -out server.crt
```

- **Zobrazení obsahu v links (potřebuje balíček links)**

```
links https://10.0.0.15
reLoad: ctrl + r
```

## 8. Zabezpečení systému

*Proved'te základní zabezpečení vašeho virtuálu, přihlašování pouze pomocí klíčů, dostupné SSH pouze ze sítě ZCU.*

- **Omezení vzdáleného přihlášení na root a ostatní uživatele**

```
nano /etc/ssh/sshd_config
```

```
PermitRootLogin [no/yes/without-password] # zakázat přihlášení na roota  
PasswordAuthentication no                 # povolit přihlášení heslem
```

- **Restartování služby pro provedení změn**

```
service sshd restart
```

- **Povolení portu TCP/22 (SSH) ze sítě ZČU (147.228.x.x)**

```
iptables -A INPUT -s 147.228.0.0/16 -p tcp --dport 22 -j ACCEPT
```

- **Zakázání portu TCP/22 (SH) z ostatních adres**

```
iptables -A INPUT -p tcp --dport 22 -j DROP
```

# Zápočet 04

## Zadání

1. Nastavte v linuxu sdílení složky /mnt pro Linux i Windows, sdílení ať je viditelné pod názvem TEST a je dostupné pouze pro čtení. Zabezpečení ať kontroluje server. (1 bod)
2. Připojte tento svazek do linuxu (pro připojení použijte IP 10.0.0.XXX, kde XXX je číslo vašeho virtuálu), tak aby byl připojen po startu. (1 bod)
3. Nastavte PostgreSQL databázi. Zajistěte, aby databáze používala pouze IP z předchozího úkolu a port TCP/3333. (1 bod)
4. Vytvořte databázi spos a nastavte uživatele spos, který s heslem ahoj bude mít přístup do této DB přes IP z předchozího úkolu. (1 bod)
5. Vytvořte tabulku datum, která bude mít dva sloupce id a hodnota a skript v libovolném jazyce, který po zavolání bez zásahu uživatele vloží do tabulky údaj o aktuálním čase. (1 bod)
6. Na adrese 10.0.0.XXX a portech 8888 a 8080 spusťte Apache server zobrazující stránku s číslem portu. (1 bod)
7. Pomocí reverzní proxy / balanceru zpřístupněte obsah WWW serveru na veřejné IP linuxu a portu 443/https a použijte self-signed certifikát (2 body)
8. Nastavte DNS pro doménu test.spos tak, aby z interní sítě 10.0.0.0/24 ukazovala IP adresu z předchozích bodů a pro ostatní ukazovala veřejnou IP. Nastavte reverzní záznamy pro obě IP adresy a TXT záznam oznamující, že máte rádi tento předmět (2 bod)

## 1. Sdílení /mnt prostřednictvím CIFS

*Nastavte v linuxu sdílení složky /mnt pro Linux i Windows, sdílení ať je viditelné pod názvem TEST a je dostupné pouze pro čtení. Zabezpečení ať kontroluje server.*

- **Instalace balíčků samba, smbclient a cifs-utils**

```
apt install samba smbclient cifs-utils
```

### **Nastavení sdílení**

```
nano /etc/samba/smb.conf
```

```
[TEST]
comment = Read only share
path = /mnt
writable = no ; stejně jako read only = yes
create mask = 0777
directory mask = 0777
force user = nobody
force group = nogroup
guest ok = yes ; anonymní přístup? stejně jako public = yes
```

- **Restartování služby po změně konfigurace**

```
service smbd restart
```

- **Zobrazení všech sdílení** (potřebuje balíček *smbclient*)  
smbclient -L localhost

## 2. Připojení svazku prostřednictvím CIFS

Připojte tento svazek do linuxu (pro připojení použijte IP 10.0.0.XXX, kde XXX je číslo vašeho virtuálu), tak aby byl připojen po startu.

- **Přidání IP adresy**  
ip a a 10.0.0.15 dev enp0s3
- **Vytvoření adresáře /opt/share**  
mkdir /opt/share
- **Přidání záznamu do fstab**  
nano /etc/fstab
- **Připojení všech oddílů z fstab**  
mount -a
- **Otestování připojení**  
cat /proc/mounts | grep TEST

```
//10.0.2.15/TEST          /opt/share      cifs      guest,uid=nobody,noperm 0 2
```

## 3. Nastavení PostgreSQL

Nastavte PostgreSQL databázi. Zajistěte, aby databáze používala pouze IP z předchozího úkolu a port TCP/3333.

- **Instalace PostgreSQL**  
apt install postgresql postgresql-client
- **Vyhledání konfiguračního souboru**  
find /etc -name postgresql.conf
- **Nastavení**  
nano /etc/postgresql/9.6/main/postgresql.conf
- **Restartování služby**  
service postgresql restart
- **Vypsání použitých portů** (potřebuje balíček *net-tools*)  
netstat -tuln | grep postgres

```
port = 3333
listen_addresses='10.0.0.15'
```

## 4. Vytvoření databáze spos a uživatele spos

Vytvořte databázi spos a nastavte uživatele spos, který s heslem ahoj bude mít přístup do této DB přes IP z předchozího úkolu.

- **Přidání uživatele spos do systému**  
adduser spos
  - **Změna hesla uživateli spos**  
passwd spos
  - **Přidání uživatele a databáze v postgres**  
su - postgres  
createuser --pwprompt spos  
createdb -O spos spos
  - **Přihlášení se jako uživatel spos do databáze spos**  
su - spos  
psql spos
  - **Nastavení pg\_hba.conf**  
nano /etc/postgresql/9.6/main/pg\_hba.conf
- | #TYPE | DB  | USER | ADDRESS     | METHOD |
|-------|-----|------|-------------|--------|
| host  | all | spos | 10.0.0.0/16 | md5    |
- **Restartování služby**  
service postgresql restart
  - **Pokročilé možnosti přihlášení do libovolné db jako libovolný uživatel**  
psql -d database -h 10.0.0.15 -p 3333 -U uživatel
  - **Příkazy PostgreSQL**  
\l vypsání všech databází  
\dt vypsání tabulek  
\q ukončení

## 5. Vytvoření tabulky datum

*Vytvořte tabulku datum, která bude mít dva sloupceky id a hodnota a skript v libovolném jazyce, který po zavolání bez zásahu uživatele vloží do tabulky údaj o aktuálním čase.*

- **Vytvoření tabulky datum**  
CREATE TABLE datum( id serial PRIMARY KEY, hodnota timestamp default NULL );
  - **Skript**  
nano skript.sh
- ```
#!/bin/bash
echo "Vkladam zaznam do databaze ..." `date`
echo "INSERT INTO datum(hodnota) VALUES (now())" | psql spos
```
- **Spuštění skriptu**  
chmod u+x skript.sh  
sh skript.sh
  - **vypsání dat z tabulky**  
SELECT \* FROM datum;



## 6. Apache server

Na adrese 10.0.0.XXX a portech 8888 a 8080 spusťte Apache server zobrazující stránku s číslem portu.

- **Instalace Apache**

```
apt install apache2 php php-mysql
```

- **Stav virtuálních hostů**

```
apachectl -S
```

- **Přidání virtuálních hostů**

```
nano /etc/apache2/sites-enabled/000-default.conf
```

```
<VirtualHost 10.0.0.15:8888>
    ServerName test.spos
    DocumentRoot /var/www/test8888
</VirtualHost>

<VirtualHost 10.0.0.15:8080>
    ServerName test.spos
    DocumentRoot /var/www/test8080
</VirtualHost>
```

- **Vytvoření adresářů virtuálních hostů**

```
mkdir /var/www/test8888
```

```
mkdir /var/www/test8080
```

- **Vytvoření souboru index.html**

```
echo "8888" > /var/www/test8888/index.html
```

```
echo "8080" > /var/www/test8080/index.html
```

- **Přidání poslechu u portů 8080 a 8888**

```
nano /etc/apache2/ports.conf
```

```
Listen 10.0.0.15:8888
Listen 10.0.0.15:8080
```

- **Restartování služby Apache2**

```
service apache2 restart
```

- **Vypsání portů Apache**

```
netstat -tuln | grep apache
```

- **Zobrazení obsahu v curl**

```
curl 10.0.0.15:8080
```

```
curl 10.0.0.15:8888
```

```
curl localhost:80
```

## 7. Zpřístupnění WWW obsahu

*Pomocí reverzní proxy / balanceru zpřístupněte obsah WWW serveru na veřejné IP linuxu a portu 443/https a použijte self-signed certifikát*

- **Vytvoření certifikátu**

```
mkdir /etc/apache2/ssl && cd /etc/apache2/ssl
```

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout spos.key -out spos.crt
```

- Country Name: **CZ**
- State: **Czech Republic**
- Locality **Pilsen**
- Organization **ZCU**
- Unit **FAV**
- Common Name **mail.test.spos**
- Email **webmaster@mail.test.spos**

- **Nastavení virtuálního hosta**

```
nano /etc/apache2/sites-available/default-ssl.conf
```

```
<VirtualHost _default_:443>
    ServerName test.spos
    SSLCertificateFile /etc/apache2/ssl/spos.crt
    SSLCertificateKeyFile /etc/apache2/ssl/spos.key
    <Proxy balancer://test.spos>
        BalancerMember http://10.0.0.15:8080
        BalancerMember http://10.0.0.15:8888
        ProxySet lbmethod=byrequests
    </Proxy>
    ProxyPass / balancer://test.spos/
    ProxyPassReverse / balancer://test.spos/
</VirtualHost>
```

- **Povolení SSL modulu**

```
a2enmod ssl
```

```
a2ensite default-ssl.conf
```

- **Povolení proxy modulů**

```
a2enmod proxy
```

```
a2enmod proxy_balancer
```

```
a2enmod proxy_http
```

```
a2enmod lbmethod_byrequests
```

- **Restartování služby Apache2**

```
service apache2 restart
```

- **Zobrazení certifikátu**

```
less /etc/ssl/private/apache.pem
```

```
less /etc/ssl/certs/apache.pem
```

- **Vypsání portu Apache**

```
netstat -tuln | grep apache
```

- **Zobrazení obsahu v curl**

```
curl --insecure https://10.0.0.15
```

- **Zobrazení obsahu v links**

```
links https://10.0.0.15
```

*reload: ctrl + r*

## 8. Nastavení DNS

Nastavte DNS pro doménu `test.spos` tak, aby z interní sítě `10.0.0.0/24` ukazovala IP adresu z předchozích bodů a pro ostatní ukazovala veřejnou IP. Nastavte reverzní záznamy pro obě IP adresy a TXT záznam oznamující, že máte rádi tento předmět

- **Instalace nástroje bind9**

```
apt install bind9
```

- **Úpravy v /etc/bind**

```
cd /etc/bind
```

- **Vytvoření kopie souboru podle šablony**

```
cp db.empty db.test.spos
```

```
cp db.empty db.test.spos.rev
```

- **Úprava souboru db.test.spos**

```
nano db.test.spos
```

```
test.spos.      IN      A          10.0.0.15
test.spos.      IN      NS         test.spos.
@               IN      TXT        "Boze, proc?"
```

- **Úprava souboru db.test.spos.rev**

```
nano db.test.spos.rev
```

```
@               IN      NS         test.spos.
$ORIGIN         0.0.10.in-addr.arpa
2               IN      PTR         test.spos.
```

- **Vytvoření zóny**

```
nano named.conf.local
```

```
zone "test.spos" {
    type master;
    file "/etc/bind/db.test.spos";
    allow-transfer {"any";}
};
zone "0.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.test.spos.rev";
    allow-transfer {10.0.0.0/24;}
};
```

- **Restartování služby po změně nastavení**

```
service bind9 restart
```

- **Ověření funkčnosti**

```
service bind9 status
```

```
host -t A test.spos localhost
```

```
test.spos has address 10.0.0.15
```

- **Ověření funkčnosti reverzního záznamu**

```
dig -x 10.0.2.15
```



# Zápočet 05

## Zadání

1. Nastavte v linuxu raid5 ze všech dostupných disků, mimo sda1 a sda2 (1 bod)
2. Naformátujte tento nově vytvořený raid jako EXT4 a připojte ho do /opt/share.  
Nastavte systém tak, aby tato složka byla připojena i po startu systému a to pomocí názvu naformátovaného svazku. (1 bod)
3. Nastavte v linuxu sdílení tohoto raidu tak, aby jí bylo možné připojit pro jakýkoliv počítač ze sítě vašeho Linuxu a aby uživatelé v rámci připojeného file systému vystupovali za uživatele nfs\_share. (2 body)
4. Připojte exportovaný share pro čtení i zápis do adresáře /share na vašem Linuxu a ověřte, že skutečně vystupují za uživatele nfs\_share. Zajistěte automatické připojení po startu systému. (1 bod)
5. Spustěte a nastavte na Linuxu DNS pro doménu test.spos a nastavte doručování pošty pro domény mail.test.spos a posta.test.spos na Linux server a nastavte pro tento server i reverzní záznam. (1 bod)
6. Spustěte na Linuxu poštovní server, nastavte doručování pošty pro email hostmaster@mail.test.spos do schránky uživatele user1 a webmaster@posta.test.spos do schránky user2. Využijte vytvořené nastavené DNS. (2 body)
7. Nainstalujte server pro stahování pošty jednodušším z dostupných protokolů, s i bez podpory šifrování a ověřte jeho funkčnost. (1 bod)
8. Omezte přístup na stahování pošty pro nešifrovaná spojení ze sítě, kde se nachází Linux a pro šifrovaná spojení ze sítě ZČU. (1 bod)

## 1. Nastavení raidu 5

*Nastavte v linuxu raid5 ze všech dostupných disků, mimo sda1 a sda2*

- **Instalace mdadm**  
`apt install mdadm`
- **Nastavení raidu 5**  
`mdadm -Cv /dev/md0 -l5 -n3 /dev/vd[bcd]`

## 2. Nastavení oddílu md0

*Naformátujte tento nově vytvořený raid jako EXT4 a připojte ho do /opt/share. Nastavte systém tak, aby tato složka byla připojena i po startu systému a to pomocí názvu naformátovaného svazku.*

- **Naformátování md0 na ext4**

```
mkfs.ext4 /dev/md0
```

- **Automatické připojení do /opt/share**

```
cd /opt
```

```
mkdir share
```

```
chmod 777 share
```

```
nano /etc/fstab
```

```
/dev/md0      /opt/share    ext4    defaults    0        2
```

```
lsblk -f
```

## 3. Sdílení raidu md0

*Nastavte v linuxu sdílení tohoto raidu tak, aby jí bylo možné připojit pro jakýkoliv počítač ze sítě vašeho Linuxu a aby uživatelé v rámci připojeného file systému vystupovali za uživatele nfs\_share.*

- **Instalace NFS serveru**

```
apt install nfs-server
```

- **Přidání skupiny a uživatele nfs\_share**

```
addgroup --gid 6000 nfs_share
```

```
adduser --gid 6000 --uid 6000 nfs_share
```

- **Nastavení nfs\_share jako vlastníka /opt/share**

```
chown nfs_share:nfs_share /opt/share
```

- **Přidání NFS záznamu do exports (IP nastavit dle sítě!)**

```
nano /etc/exports
```

```
/opt/share 10.0.2.0/24(rw,no_subtree_check,all_squash,anonuid=6000,anongid=6000)
```

- **Načtení NFS záznamů po změně**

```
exportfs -a
```

## 4. Připojení sdílení NFS

*Připojte exportovaný share pro čtení i zápis do adresáře /share na vašem Linuxu a ověřte, že skutečně vystupují za uživatele nfs\_share. Zajistěte automatické připojení po startu systému.*

- **Vytvoření adresáře /share a nastavení oprávnění**  
mkdir share && chmod 777 share
- **Přidání záznamu v fstab (pro adresu počítače 10.0.2.15)**

```
nano /etc/fstab
```

```
10.0.2.15:/opt/share /share nfs defaults 0 2
```

- **Připojení všech záznamů z fstab**  
mount -a
- **Ověření, že je nfs disk připojen**  
cat /proc/mounts | grep share
- **Ověření, že zapsaný soubor je ve vlastnictví nfs\_share**  
cd /share  
touch soubor.txt  
ls -la

## 5. Nastavení DNS záznamu

*Spustíte a nastavíte na Linuxu DNS pro doménu test.spos a nastavíte doručování pošty pro domény mail.test.spos a posta.test.spos na Linux server a nastavíte pro tento server i reverzní záznam.*

- **Instalace nástroje bind9**  
apt install bind9
- **Přidání záznamu v hosts**  
nano /etc/hosts

```
10.0.2.15 test.spos
```

- **Úpravy v /etc/bind**  
cd /etc/bind
- **Vytvoření kopie souboru podle šablony**  
cp db.empty db.test.spos
- **Úprava souboru db.test.spos**  
nano db.test.spos

```
$TTL      86400
@         IN      SOA      test.spos.  root.localhost. (
                        11      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        86400    ; Negative Cache TTL
                        )
;
test.spos. IN      A       10.0.2.15
```

```
mail      IN      A      10.0.2.15
posta     IN      A      10.0.2.15
test.spos. IN      NS     test.spos.
mail      IN      MX 6     mail
posta     IN      MX 6     posta
```

- **Vytvoření zóny**

nano named.conf.local

```
zone "test.spos" {
    type master;
    file "/etc/bind/db.test.spos";
    allow-transfer {"any";}
};
```

- **Restartování služby po změně nastavení**

service bind9 restart

- **Ověření funkčnosti**

host -t MX posta.test.spos localhost

```
posta.test.spos mail is handled by 6 posta.test.spos.
```

- **Přidání reverzního záznamu**

- **Přidání zóny**

nano /etc/bind/named.conf.local

```
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.test.spos.rev";
    allow-transfer {10.0.2.0/24;};
};
```

- **Vytvoření kopie souboru podle šablony**

cp db.empty db.test.spos.rev

- **Úprava souboru db.test.spos.rev**

nano db.test.spos.rev

```
$TTL      86400
@         IN      SOA     test.spos.  root.localhost. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                86400      ; Negative Cache TTL
                                )
;
@         IN      NS      test.spos.
$ORIGIN   2.0.10.in-addr.arpa
2         IN      PTR     test.spos.
2         IN      PTR     mail.test.spos.
2         IN      PTR     posta.test.spos.
```

- **Restartování služby po změně nastavení**

service bind9 restart

- **Ověření funkčnosti**

service bind9 status

dig -x 10.0.2.15



## 6. Poštovní server

Spustíte na Linuxu poštovní server, nastavíte doručování pošty pro email `hostmaster@mail.test.spos` do schránky uživatele `user1` a `webmaster@posta.test.spos` do schránky `user2`. Využijte vytvořené nastavené DNS.

- **Instalace poštovního nástroje postfix**  
`apt install postfix`
- **Úprava nastavení `/etc/postfix/main.cf` (Instalace skončí chybou)**  
`nano /etc/postfix/main.cf`  

```
myhostname = mail.test.spos
```
- **Dokončení instalace**  
`apt install -f`
- **Restartování služby po úpravě `main.cf`**  
`service postfix reload`
- **Přidání uživatelů `user1`, `user2` a vytvoření home**  
`adduser user1 && adduser user2`
- **Přidání oprávnění pro mail uživatelům `user1`, `user2`**  
`usermod -g mail user1`  
`usermod -g mail user2`
- **Přesměrování pošty**
  - **Vytvoření souboru `virtual`**  
`touch /etc/postfix/virtual`
  - **Přidání záznamů**  
`nano /etc/postfix/virtual`  

```
hostmaster@mail.test.spos user1@localhost  
webmaster@posta.test.spos user2@localhost
```
  - **Přidání řádků na konec `main.cf`**  
`nano /etc/postfix/main.cf`  

```
virtual_alias_domains = mail.test.spos posta.test.spos  
virtual_alias_maps = hash:/etc/postfix/virtual
```
  - **Restartování služby po úpravě `virtual` a `main.cf`**  
`postmap /etc/postfix/virtual`  
`service postfix reload`
  - **Ověření konfigurace**  
`postconf -n | grep virtual`
- **Ověření přesměrování pošty**
  - **Instalace nástroje `mail`**  
`apt install bsd-mailx`
  - **Odeslání pošty na `hostmaster@mail.test.spos`**  
`echo "TEXT" | mail -s "PREDMET" hostmaster@mail.test.spos`  
`echo "TEXT" | mail -s "PREDMET" webmaster@posta.test.spos`
  - **Čtení pošty v nástroji `mutt`**  
`apt install mutt`

```
mutt -f /var/spool/mail/user1
mutt -f /var/spool/mail/user2
```

## 7. Stahování pošty

*Nainstalujte server pro stahování pošty jednodušším z dostupných protokolů, s i bez podpory šifrování a ověřte jeho funkčnost.*

- **Protokol POP3**

```
apt install dovecot-pop3d
```

- **Vytvoření certifikátu**

```
openssl req -new -x509 -nodes -out "/etc/ssl/certs/dovecot.pem" -keyout "/etc/ssl/private/dovecot.pem"
```

- **Změna nastavení SSL**

```
nano /etc/dovecot/conf.d/10-ssl.conf
```

```
ssl = yes
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key = </etc/ssl/private/dovecot.pem
```

- **Restartování služby dovecot**

```
service dovecot restart
```

- **Zobrazení stavu služby**

```
service dovecot status
```

- **Zobrazení chyby při spuštění služby**

```
journalctl -xe
```

- **Porty využívané službou dovecot**

```
netstat -ltnp | grep dovecot
```

```
110 POP3 bez SSL
```

```
995 POP3 s SSL
```

```
143 IMAP bez SSL
```

```
993 IMAP s SSL
```

- **Spojení s POP3 nešifrovaně**

```
nc localhost 110
```

- **zadání uživatele**

```
USER user1
```

- **zadání hesla**

```
PASS heslo
```

- **počet zpráv**

```
STAT
```

- **seznam zpráv**

```
LIST
```

- **zobrazení zprávy 1**

```
RETR 1
```

- **odhlášení se**

```
QUIT
```

## 8. Omezení přístupu na stahování pošty

*Omezte přístup na stahování pošty pro nešifrovaná spojení ze sítě, kde se nachází Linux a pro šifrovaná spojení ze sítě ZČU.*

- **Vypsání pravidel firewallu iptables**  
`iptables -nvL`
- **Vymazání pravidel firewallu iptables**  
`iptables -F`
- **Povolení portu TCP/110 (pop3) z 10.0.2.x**  
`iptables -A INPUT -s 10.0.2.0/24 -p tcp --dport 110 -j ACCEPT`
- **Zakázání portu TCP/110 (pop3) z ostatních adres**  
`iptables -A INPUT -p tcp --dport 110 -j DROP`
- **Povolení portu TCP/995 (pop3 s SSL) ze sítě ZČU (147.228.x.x)**  
`iptables -A INPUT -s 147.228.0.0/16 -p tcp --dport 995 -j ACCEPT`
- **Zakázání portu TCP/995 (pop3 s SSL) z ostatních adres**  
`iptables -A INPUT -p tcp --dport 995 -j DROP`

# Zápočet 06

## Zadání

1. Proveďte základní nastavení zabezpečení systému: přihlašování jen pomocí klíčů, dostupnost ssh jen ze sítě univerzity (**147.228.0.0/16**), omezte možnosti hádání hesel. (1 bod)
2. Vytvořte nad některým z volných disků LVM, skupina se bude jmenovat **data** a svazek **public-share**. (1 bod)
3. Naformátujte tento nově vytvořený svazek jako EXT4 a připojte ho do /opt/share. Nastavte systém tak, aby tato složka byla připojena i po startu systému. (1 bod)
4. Nasdílejte adresář **/opt/share** pomocí Samby s názvem **SHARED** pro anonymní přístup a připojte toto sdílení do **/mnt/share**. (1 bod)
5. Spustěte a nastavte na Linuxu DNS pro doménu **test.spos** a nastavte doručování pošty pro domény **mail.test.spos** na Váš server. (1 bod)
6. Spustěte na Linuxu poštovní server, nastavte doručování pošty pro email **hostmaster@mail.test.spos** do schránky uživatele **user1** a **webmaster@posta.test.spos** do schránky **user2**. Schránky ať jsou typu **Maildir**. (2 body)
7. Nainstalujte server pro stahování pošty modernějším z dostupných protokolů, s i bez podpory šifrování a ověřte jeho funkčnost. Vygenerujte vlastní self-signed certifikát pro jméno **mail.test.spos**. (2 body)
8. Omezte přístup na stahování pošty pro nešifrovaná spojení ze sítě, kde se nachází Linux a pro šifrovaná spojení ze sítě ZČU. (1 bod)

## 1. Zabezpečení systému

*Proveďte základní nastavení zabezpečení systému: přihlašování jen pomocí klíčů, dostupnost ssh jen ze sítě univerzity (147.228.0.0/16), omezte možnosti hádání hesel.*

- **Omezení vzdáleného přihlášení na root a ostatní uživatele**

```
nano /etc/ssh/sshd_config
```

```
PermitRootLogin [no/yes/without-password] # zakázat přihlášení na roota
PasswordAuthentication no                  # povolit přihlášení heslem
```

- **Restartování služby pro provedení změn**  
`service sshd restart`
- **Povolení portu TCP/22 (SSH) ze sítě ZČU (147.228.x.x)**  
`iptables -A INPUT -s 147.228.0.0/16 -p tcp --dport 22 -j ACCEPT`
- **Zakázání portu TCP/22 (SH) z ostatních adres**  
`iptables -A INPUT -p tcp --dport 22 -j DROP`
- **Balíček fail2ban pro omezení možností hádání hesel**  
`apt install fail2ban`
- **Záznamy pokusů o přihlášení**  
`more /var/log/auth.log`

- **Aktivita služby fail2ban**  
systemctl status fail2ban
- **Nastavení fail2ban**  
cat /etc/fail2ban/jail.conf

```
bantime = 60m          # V zadání nejsou konkrétní hodnoty...
maxretry = 3
```

## 2. Vytvoření LVM

Vytvořte nad některým z volných disků LVM, skupina se bude jmenovat data a svazek public-share.

- **Vypsání dostupných disků**  
lsblk -f
- **Instalace balíčku lvm2**  
apt install lvm2
- **Vytvoření skupiny pojmenované data**  
vgcreate data /dev/sdb
- **Vypsání existujících skupin**  
vgdisplay
- **Vytvoření logického svazku pojmenovaného public-share**  
lvcreate -L 1000M -n public-share data
- **Vypsání existujících svazků**  
lvdisplay

## 3. Naformátování a připojení disku

Naformátujte tento nově vytvořený svazek jako EXT4 a připojte ho do /opt/share. Nastavte systém tak, aby tato složka byla připojena i po startu systému.

- **Naformátování public-share na ext4**  
mkfs.ext4 /dev/data/public-share
- **Nastavení připojení share jako /home**  
nano /etc/fstab

```
/dev/data/public-share  /opt/share  ext4  defaults  0  2
```

- **Vytvoření adresáře /opt/share**  
mkdir /opt/share
- **Připojení všech oddílů z fstab**  
mount -a
- **Vypsání diskových oddílů včetně použitých FS a přípojných bodů**  
lsblk -f

## 4. Nasdílení adresáře pomocí SMB (CIFS)

Nasdílejte adresář `/opt/share` pomocí Samby s názvem `SHARED` pro anonymní přístup a připojte toto sdílení do `/mnt/share`.

- Instalace balíčků `samba`, `smbclient` a `cifs-utils`

```
apt install samba smbclient cifs-utils
```

- Nastavení sdílení

```
nano /etc/samba/smb.conf
```

```
[SHARED]
comment = Jednou ten zapocet dam :-)
path = /opt/share
writable = no ; stejne jako read only = yes
create mask = 0777
directory mask = 0777
force user = nobody
force group = nogroup
guest ok = yes ; anonymni pristup? stejne jako public = yes
```

- Restartování služby po změně konfigurace

```
service smbd restart
```

- Výpis konfigurace `samba`

```
testparm
```

- Vytvoření adresáře `/mnt/share`

```
mkdir /mnt/share
```

- Zobrazení všech sdílení (potřebuje balíček `smbclient`)

```
smbclient -L 10.0.2.15
```

- Připojení disku (potřebuje balíček `cifs-utils`)

```
mount -t cifs //10.0.2.15/SHARED /mnt/share -o guest
```

- Přidání záznamu do `fstab`

```
nano /etc/fstab
```

```
//10.0.2.15/SHARED /mnt/share cifs guest,uid=nobody,noperm 0 2
```

- Otestování připojení

```
cat /proc/mounts | grep SHARED
```

## 5. DNS pro doménu test.spos

Spustíte a nastavíte na Linuxu DNS pro doménu `test.spos` a nastavíte doručování pošty pro domény `mail.test.spos` na Váš server.

- Instalace nástroje `bind9`

```
apt install bind9
```

- Přidání záznamu v `hosts`

```
nano /etc/hosts
```

```
10.0.2.15 test.spos
```

- **Úpravy v /etc/bind**  
cd /etc/bind
- **Vytvoření kopie souboru podle šablony**  
cp db.empty db.test.spos
- **Úprava souboru db.test.spos**  
nano db.test.spos

```
$TTL      86400
@         IN      SOA      test.spos.      root.localhost. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        86400      ; Negative Cache TTL
                        )
;
test.spos.      IN      A      10.0.2.15
mail            IN      A      10.0.2.15
test.spos.      IN      NS     test.spos.
mail            IN      MX     50 mail
```

- **Vytvoření zóny**  
nano named.conf.local
- **Restartování služby po změně nastavení**  
service bind9 restart
- **Ověření funkčnosti**  
host -t MX mail.test.spos localhost

```
zone "test.spos" {
    type master;
    file "/etc/bind/db.test.spos";
    allow-transfer {"any";}
};
```

## 6. Poštovní server

Spustíte na Linuxu poštovní server, nastavíte doručování pošty pro email **hostmaster@mail.test.spos** do schránky uživatele **user1** a **webmaster@posta.test.spos** do schránky **user2**. Schránky ať jsou typu **Maildir**.

- **Instalace poštovního nástroje postfix a bsd-mailx**  
apt install postfix bsd-mailx
- **Úprava nastavení /etc/postfix/main.cf (Instalace skončí chybou)**  
nano /etc/postfix/main.cf
- **Dokončení instalace**  
apt install -f
- **Restartování služby po úpravě main.cf**  
service postfix reload
- **Přidání uživatelů user1, user2 a vytvoření home**  
useradd user1 && useradd user2

```
myhostname = mail.test.spos
```

```
mkdir /home/user1 && chown user1 /home/user1
mkdir /home/user2 && chown user2 /home/user2
```

- **Přidání oprávnění pro mail uživatelům user1, user2**

```
usermod -g mail user1
usermod -g mail user2
```

- **Nastavení aliasů**

```
nano /etc/aliases
```

```
hostmaster: user1
webmaster: user2
```

- **Načtení aliasů po změně /etc/aliases**

```
newaliases
```

- **Nastavení Maildir v main.cf**

```
postconf -e "home_mailbox = Maildir/"
```

- **Restartování služby po úpravě main.cf**

```
service postfix reload
```

- **Otestování zaslání zprávy (potřebuje balíček *bsd-mailx*)**

```
echo "<|>" | mail -s "MOTYLE" webmaster@mail.test.spos
```

- **Otestování doručení zprávy**

```
cat /home/user2/Maildir/new/*
```

## 7. Stahování pošty protokolem IMAP

*Nainstalujte server pro stahování pošty modernějším z dostupných protokolů, s i bez podpory šifrování a ověřte jeho funkčnost. Vygenerujte vlastní self-signed certifikát pro jméno **mail.test.spos**.*

- **Protokol Dovecot s protokolem IMAP**

```
apt install dovecot-imapd
```

- **Vytvoření certifikátu**

```
openssl req -new -x509 -nodes -out "/etc/ssl/certs/dovecot.pem" -keyout "/etc/ssl/private/dovecot.pem"
```

- Country Name: **CZ**
- State: **Czech Republic**
- Locality: **Pilsen**
- Organization: **ZCU**
- Unit: **FAV**
- Common Name: **mail.test.spos**
- Email: **webmaster@mail.test.spos**

- **Změna nastavení SSL**

```
nano /etc/dovecot/conf.d/10-ssl.conf
```

```
ssl = yes
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key = </etc/ssl/private/dovecot.pem
```

- **Restartování služby dovecot**

```
service dovecot restart
```



- **Zobrazení certifikátu**  
`less /etc/ssl/private/dovecot.pem`  
`less /etc/ssl/certs/dovecot.pem`
- **Otestování zobrazením využitých portů službou dovecot**  
`netstat -ltnp | grep dovecot`  
*110 POP3 bez SSL*  
*143 IMAP bez SSL*  
*993 IMAP s SSL*  
*995 POP3 s SSL*

## 8. Omezení přístupu na stahování pošty

*Omezte přístup na stahování pošty pro nešifrovaná spojení ze sítě, kde se nachází Linux a pro šifrovaná spojení ze sítě ZČU*

- **Vypsání pravidel firewallu iptables**  
`iptables -nvL`
- **Vymazání pravidel firewallu iptables**  
`iptables -F`
- **Povolení portu TCP/143 (imap) z 10.0.2.x**  
`iptables -A INPUT -s 10.0.2.0/24 -p tcp --dport 143 -j ACCEPT`
- **Zakázání portu TCP/143 (imap) z ostatních adres**  
`iptables -A INPUT -p tcp --dport 143 -j DROP`
- **Povolení portu TCP/993 (imap s SSL) ze sítě ZČU (147.228.x.x)**  
`iptables -A INPUT -s 147.228.0.0/16 -p tcp --dport 993 -j ACCEPT`
- **Zakázání portu TCP/993 (imap s SSL) z ostatních adres**  
`iptables -A INPUT -p tcp --dport 993 -j DROP`