

Virtualizáció megvalósítása OpenVZ rendszerrel CentOS 6.4 környezetben



Készítő: Makó Gábor { makgab (at) m-info.hu }
Dátum: 2013. július 5.
Kiadás (verzió): 5.

Tartalom

Előszó

Virtualizáció kialakítása

1. CentOS 6.4 telepítése.
2. OpenVZ repository letöltése
3. OpenVZ telepítése
4. Rendszer beállítása: /etc/sysctl.conf
5. Az /etc/vz/vz.conf beállítása
6. SELinux kikapcsolása
7. Rendszer újraindítása, az openvz (ovzkernel) kernel betöltésével
8. A virtuális gépek, szerverek létrehozása, tesztelése (vz101, vz102, vz103... stb.)
9. Az első virtuális gép (vz101) konfigurálása
 - 9.1 OpenLDAP konfigurációja
 - 9.2 Samba konfigurálása
10. A második virtuális gép (vz102) konfigurálása
 - 10.1 DNS (bind) konfigurálása
 - 10.2 LDAP kliens konfigurálása
11. A harmadik virtuális gép (vz103) konfigurálása
 - 11.2 LDAP kliens konfigurálása
 - 11.2 MySQL telepítése
 - 11.3 PostgreSQL telepítése
12. A negyedik virtuális gép (vz104) konfigurálása
 - 12.2 LDAP kliens konfigurálása
 - 12.2 Apache Web Szerver (httpd) telepítése
 - 12.3 FTP szerver (vsftpd) telepítése
13. Az ötödik virtuális gép (vz105) konfigurálása
 - 13.1 LDAP kliens konfigurálása
 - 13.2 Levelező szerver telepítése
14. Mentések kezelése az OpenVZ-ben
15. Adminisztráció
16. OpenVZ és a ZFS
17. Virtual Ethernet device (veth)

Előszó

Ez a dokumentáció egy elképzelt, tesztkörnyezetben felépített, helyi hálózatban (LAN) kialakított virtualizációs szerver konfigurálását próbálja bemutatni. A virtualizációt az OpenVZ [1] rendszerrel valósítom meg.

A tervezett helyi hálózat kb. 20 felhasználóból állna. Az operációs rendszer egy CentOS 6.4 Linux (RedHat EL kompatibilis) lesz.[2]

Megjegyzem, hogy a Proxmox (<http://www.proxmox.com>) rendszerrel egy azonnal használható Debian alapú virtualizációs rendszert kapunk, melynek dokumentációja szerint egy órán belül üzemelő rendszert kapunk.

Célok:

A virtualizáció célja az erőforrások egyenletes elosztása, a hardver jobb kihasználása. Egy virtuális gépet célszerű létrehozni a külső, internet felől használt szolgáltatások számára (pl. DNS, OpenVPN, WWW).

Célom lesz egy webes felület létrehozása is a menedzseléshez. Erre az „*openvz-web-panel*”-t fogom használni.

A kialakított rendszer a következőképpen néz majd ki:

Virtuális gép neve	Funkció/szolgáltatás
virt.gép #1: vz101	OpenLDAP, Samba (központi azonosítás)
virt.gép #2: vz102	DNS, OpenVPN?
virt.gép #3: vz103	SQL (PostgreSQL, MySQL),
virt.gép #4: vz104	WWW, FTP (apache, vsftpd),
virt.gép #5: vz105	Mail (dovecot imap v. pop3).

(Fizikai gépen v. a vz102-n az OpenVPN telepíthető a külső eléréshez.)

A gép konfigurációja, amin a teszt környezetet kialakítottam:

Intel Core i3 CPU, 8GB RAM, SATA HDD.

Az egyszerűség kedvéért egy merevlemezen alakítom ki a rendszert:

Eszköz	mount pont	kb. méret
/dev/sda1	swap	2Gb
/dev/sda2	/	20GB
/dev/sda3	/vz	56GB

A virtuális gépeket tehetjük (célszerű) külön partícióra. RAID megoldást is alkalmazhatunk az adatbiztonság érdekében.

Az egyes VPS-ek a *private* könyvtár alatt érhetők majd el közvetlen. A *root* könyvtár alatt a mountolt, futó VPS-ek láthatók.

1. CentOS 6.4 telepítése

Első lépés az alap operációs rendszer telepítése, jelen esetben a CentOS 6.4 Linux. Ezt nem részletezném, csak a fontosabb dolgokat jegyzem meg.

Felhasználót külön nem viszek fel a root-on kívül, esetleg a külső eléréshez egy 'admin'-t. CentOS alaptelepítés elegendő. A fizikai gép IP címe (eth0): *192.168.1.67/255.255.255.0*, átjáró/DNS: *192.168.1.1*.

2. OpenVZ repository letöltése

```
wget -P /etc/yum.repos.d/ http://ftp.openvz.org/openvz.repo
rpm --import http://ftp.openvz.org/RPM-GPG-Key-OpenVZ
```

3. OpenVZ telepítése

Ehhez először az ovzkernel-t kell telepíteni, majd az openvz-t:

```
yum install vzkernel
yum install vzctl vzquota ploop
```

4. Rendszer beállítása: /etc/sysctl.conf

```
[...]
# On Hardware Node we generally need
# packet forwarding enabled and proxy arp disabled
net.ipv4.ip_forward = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.default.proxy_arp = 0

# Enables source route verification
net.ipv4.conf.all.rp_filter = 1

# Enables the magic-sysrq key
kernel.sysrq = 1

# We do not want all our interfaces to send redirects
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
[...]
```

A módosítások után futtassuk a "*sysctl -p*" parancsot, vagy indítsuk újra a rendszert.

5. Az /etc/vz/vz.conf beállítása

```
[...]
NEIGHBOUR_DEVS=all
[...]
```

6. SELinux kikapcsolása

```
echo "SELINUX=disabled" > /etc/sysconfig/selinux
```

Vagy állítsuk „*permissive*” módba.

7. Rendszer újraindítása, az openvz (ovzkernel) kernel betöltésével

reboot

GRUB menüjében választandó: `OpenVZ (2.6.32.042stab078.26)`

8. A virtuális gépek, szerverek létrehozása, tesztelése (vz101, vz102, vz103... stb.)

Ellenőrizzük, hogy az *rpm-python* csomag a legfrissebb és 64bit-es architektúrájú!

A template létrehozása, letöltése:

`cd /vz/template/cache`

(wget http://download.openvz.org/template/precreated/contrib/centos-6-x86_64-default.tar.gz)

VPS 101 beállítás a template konfigurációból:

```
vzctl create 101 --ostemplate centos-6-x86_64-default --config vps.basic
```

Bootkor induljon:

```
vzctl set 101 --onboot yes --save
```

A hostnév és IP cím beállítása:

```
vzctl set 101 --hostname vz101.example-hu.com --save
```

```
vzctl set 101 --ipadd 192.168.1.101 --save
```

```
vzctl set 101 --searchdomain example-hu.com --save
```

A socket és névszerver beállítása:

```
vzctl set 101 --numothersock 120 --save
```

```
vzctl set 101 --nameserver 192.168.1.102 --nameserver 192.168.1.1 --save
```

A vz102 VPS-en lesz a DNS, ezért ott a 127.0.0.1 IP címet is fel lehet venni:

```
vzctl set 102 --nameserver 127.0.0.1 --nameserver 192.168.1.102 --nameserver 192.168.1.1 --save
```

A vz101 VPS indítása:

```
vzctl start 101
```

A vz101 root jelszó:

```
vzctl exec 101 passwd
```

A vz101 VPS csatlakozás, belépés a virtuális gépre:

```
vzctl enter 101
```

Kilépés a vz101-ből:

```
exit
```

A vz101 leállítása:

```
vzctl stop 101
```

A vz101 újraindítása:

```
vzctl restart 101
```

A vz101 törlése:

```
vzctl destroy 101
```

A virtuális gépek listázása:

```
vzlist -a
[root@centos ~]# vzlist -a
VEID   NPROC STATUS IP_ADDR   HOSTNAME
101    18 running 192.168.1.101 vz101.example-hu.com
[root@centos ~]#
```

Az erőforrás foglalás:

```
vzctl exec 101 cat /proc/user_beancounters
[root@centos ~]# vzctl exec 101 cat /proc/user_beancounters
Version: 4.3.1
uid   resource      held      maxheld   barrier   limit     failcnt
101:  kmemsize      1508202  1661695  11055923  11377049  0
      lockedpages  0         0         256       256       0
      privvmpages  5430     7102     65536    69632    0
      shmpages     381      381      21504    21504    0
      dummy       0         0         0         0         0
      numproc     19        21        240      240       0
      physpages   2489     2775     0         2147483647 0
      vmguarpages 0         0         33792    2147483647 0
      oomguarpages 2489     2775     26112    2147483647 0
      numtcpsock  5         5         360      360       0
      numflock    3         4         188      206       0
      numpty     0         1         16       16        0
      numsiginfo  0         2         256      256       0
      tcpsndbuf   44720    0         1720320  2703360  0
      tcpvbuf     81920    0         1720320  2703360  0
      othersockbuf 13144    14356    1126080  2097152  0
      dgramrcvbuf 0         8380     262144   262144   0
      numothersock 11        13        120      120       0
      dcachesize  0         0         3409920  3624960  0
      numfile     503      531      9312     9312     0
      dummy       0         0         0         0         0
      dummy       0         0         0         0         0
      dummy       0         0         0         0         0
      numiptent   10        10        128      128       0
[root@centos ~]#
```

A többi virtuális gép a fentiek alapján létrehozható (vz102, vz103, vz104, vz105).

Egy hasonló listát kell látnunk a "vzlist -a" kimeneteként:

CTID	NPROC	STATUS	IP_ADDR	HOSTNAME
101	23	running	192.168.1.101	vz101.example-hu.com
102	17	running	192.168.1.102	vz102.example-hu.com
103	17	running	192.168.1.103	vz103.example-hu.com
104	17	running	192.168.1.104	vz104.example-hu.com
105	17	running	192.168.1.105	vz105.example-hu.com

Az első VPS (vz101) ifconfig kimenete itt látható:

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:134 errors:0 dropped:0 overruns:0 frame:0
        TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:10684 (10.4 KiB) TX bytes:10684 (10.4 KiB)

venet0  Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:127.0.0.1  P-t-P:127.0.0.1  Bcast:0.0.0.0  Mask:255.255.255.255
        UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

venet0:0  Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:192.168.1.101  P-t-P:192.168.1.101  Bcast:192.168.1.101  Mask:255.255.255.255
        UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
```

Az egyes virtuális szervereken célszerű egy csomagfrissítést kérni, de először magát a csomagkezelőt:

```
yum update popd rpm rpm-python yum
yum update
```

9. Az első virtuális gép (vz101) konfigurálása

Belépés a vz101 VPS-be:

```
vzctl enter 101
```

Az openldap installálása:

```
yum install openldap-*
```

Amennyiben nincs fenn az nss_ldap csomagot, tegyük fel:

```
yum install nss_ldap
```

9.1 OpenLDAP konfigurációja, Context: dc=intranet,dc=example-hu,dc=com

Az authconfig-tui eszközzel állítsuk az autentikációt LDAP-ra (User information, User authentication) ls indítsuk el az openldap szolgáltatást (service ldap restart).

```
# /etc/ldap.conf -----  
...  
base dc=intranet,dc=example-hu,dc=com  
uri ldap://127.0.0.1/  
ssl no  
tls_cacertdir /etc/openldap/cacerts  
pam_password md5  
# tudjuk módosítani az adatbázisban  
binddn cn=manager,dc=intranet,dc=example-hu,dc=com  
bindpw secret  
# hol keresse a jelszót, usereket, groupokat  
nss_base_passwd ou=People,dc=intranet,dc=example-hu,dc=com?one  
nss_base_shadow ou=People,dc=intranet,dc=example-hu,dc=com?one  
nss_base_group ou=Group,dc=intranet,dc=example-hu,dc=com?one  
# --- ldap.conf --- #
```

```
# /etc/openldap/ldap.conf ---  
URI ldap://127.0.0.1/  
BASE dc=intranet,dc=example-hu,dc=com  
TLS_CACERTDIR /etc/openldap/cacerts  
# --- ldap.conf --- #
```

```
# /etc/openldap/slapd.conf ---  
...  
# Ne feledjük include-olni a samba.schema-t! #  
include /etc/openldap/schema/samba.schema  
...  
access to dn.base="" by * read  
access to dn.base="cn=Subschema" by * read  
access to *  
by self write  
by users read  
by anonymous auth  
database bdb
```



```

suffix          "dc=intranet,dc=example-hu,dc=com"
rootdn          "cn=manager,dc=intranet,dc=example-hu,dc=com"
rootpw         secret
# rootpw       {crypt}ijFYncSNctBYg
index objectClass eq,pres
index ou,cn,mail,surname,givenname eq,pres,sub
index uidNumber,gidNumber,loginShell eq,pres
index uid,memberUid eq,pres,sub
index nisMapName,nisMapEntry eq,pres,sub
# --- slapd.conf --- #

```

Az authconfig-tui futtatása és az LDAP autentikáció beállítása:

```

# /etc/pam.d/system-auth-ac:
session required pam_mkhome.so umask=0022

```

A /var/lib/ldap/DB_CONFIG állományt se felejtsük el (/etc/openldap/DB_CONFIG.exmaple)!

Az LDAP struktúra létrehozása:

```

#ldap_tree.txt -----
dn: dc=intranet,dc=example-hu,dc=com
objectClass: top
objectClass: organization
objectClass: dcObject
o: Example-Org
dc: intranet

dn: cn=manager,dc=intranet,dc=example-hu,dc=com
objectClass: organizationalRole
cn: manager

dn: ou=People,dc=intranet,dc=example-hu,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=intranet,dc=example-hu,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Group

dn: cn=root,ou=People,dc=intranet,dc=example-hu,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: root
uid: root
uidNumber: 0
gidNumber: 0
gecos: Root

```

```
loginShell: /bin/bash
homeDirectory: /root/
userPassword: secret
```

```
dn: cn=root,ou=Group,dc=intranet,dc=example-hu,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 0
cn: root
memberUid: root
# -----
```

```
# admingrp.txt -----
dn: cn=admin,ou=Group,dc=intranet,dc=example-hu,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 500
cn: admin
memberUid: admin
# -----
```

```
# admin.txt -----
dn: cn=admin,ou=People,dc=intranet,dc=example-hu,dc=com
objectClass: inetOrgPerson
#objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
cn: admin
uid: admin
sn: Admin
givenName: Admin
uidNumber: 500
gidNumber: 500
gecos: Admin
loginShell: /bin/bash
homeDirectory: /home/admin/
userPassword:: c2VjcmV0
# password: secret
mail: admin@192.168.1.101
# -----
```

Töltsük be az LDAP-ba, azaz futtassuk (a *secret* jelszót kell megadni):

```
ldapadd -f ldap_tree.txt -D 'cn=manager,cd=intranet,dc=example-hu,dc=com' -x -W
ldapadd -f admingrp.txt -D 'cn=manager,cd=intranet,dc=example-hu,dc=com' -x -W
ldapadd -f admin.txt -D 'cn=manager,cd=intranet,dc=example-hu,dc=com' -x -W
```

Ezzel az LDAP fa készen van és van benne **root**, **admin** felhasználó.

9.2 Samba konfigurálása

```
# /etc/samba/smb.conf
...
[global]
...
workgroup = SAMBA
server string = Samba Server Version %v
netbios name = vz101
interfaces = lo eth0 192.168.1.0/24
hosts allow = 127. 192.168.1.
security = user
passdb backend = ldapsam:ldap://127.0.0.1:389/
ldap suffix = dc=intranet,dc=example-hu,dc=com
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap admin dn = cn=manager,dc=intranet,dc=example-hu,dc=com
ldap delete dn = no
ldap password sync = yes
unix password sync = yes
...
#===== Share Definitions =====
[homes]
comment = Home Directories
browseable = no
writable = yes
[public]
comment = Public Stuff
path = /usr/local/samba
public = yes
writable = yes
printable = no
```

Ezzel az első (vz101) VPS készen van: OpenLDAP és Samba szolgáltatásokkal.

10. A második virtuális gép (vz102) konfigurálása

10.1 DNS (bind) konfigurálása

Telepítsük fel a **bind** csomagokat, ha szükséges:

```
yum install bind bind-utils bind-chroot caching-nameserver
```

Konfiguráljuk a névszervert:

```
# A /var/named/chroot/etc/named.conf fájl #
options {
listen-on port 53 { 127.0.0.1; 192.168.1.102; };
listen-on-v6 port 53 { ::1; };
directory "/var/named";
dump-file "/var/named/data/cache_dump.db";
```



```

zone "0.in-addr.arpa" IN {
type master;
file "named.zero";
allow-update { none; };
};
zone "example-hu.com" IN {
type master;
file "example-hu.com.db";
allow-update { none; };
};
# --- end of file --- #

```

```

# A /var/named/chroot/var/named/example-hu.com.db fájl #
$TTL 3660
@      IN SOA      example-hu.com.  root.example-hu.com. (
                                7      ; serial
                                3600   ; refresh
                                900    ; retry
                                3600000 ; expire
                                3600   ) ; minimum
      NS      example-hu.com.
@      IN      A      192.168.1.102
vz102  IN      A      192.168.1.102
vz101  IN      A      192.168.1.101
vz103  IN      A      192.168.1.103
vz104  IN      A      192.168.1.104
vz105  IN      A      192.168.1.105
ftp     IN      CNAME   vz104
# --- end of file --- #

```

```

# A /var/named/chroot/var/named/192.168.1.reverse.db fájl #
$TTL 3660
@      IN SOA      localhost root.localhost. (
                                3      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
      NS      localhost.
      PTR     localhost.
102    PTR     vz102.example-hu.com.
101    PTR     vz101.example-hu.com.
103    PTR     vz103.example-hu.com.
104    PTR     vz104.example-hu.com.
105    PTR     vz105.example-hu.com.
# --- end of file --- #

```

Indítsuk el a névszerveret:

```
service named restart
```

10.2 LDAP kliens konfigurálása

Az nss_ldap csomagra szükség lesz:

```
yum install nss_ldap
```

Az authconfig-tui eszközzel állítsuk az autentikációt LDAP-ra (User information, User authentication).

Az LDAP kliens konfigurációs fájlja megegyzik a vz101 VPS-ével, annyi különbséggel, hogy a szerver természetesen nem 127.0.0.1, hanem a vz101 VPS, IP: 192.168.1.101

Az **/etc/pam.d/system-auth-ac** fájlba felveendő:

```
session required pam_mkhome.so umask=0022
```

```
# /etc/ldap.conf -----  
...  
base dc=intranet,dc=example-hu,dc=com  
uri ldap://192.168.1.101/  
ssl no  
tls_cacertdir /etc/openldap/cacerts  
pam_password md5  
# tudjuk módosítani az adatbázisban  
binddn cn=manager,dc=intranet,dc=example-hu,dc=com  
bindpw secret  
# hol keresse a jelszót, usereket, groupokat  
nss_base_passwd ou=People,dc=intranet,dc=example-hu,dc=com?one  
nss_base_shadow ou=People,dc=intranet,dc=example-hu,dc=com?one  
nss_base_group ou=Group,dc=intranet,dc=example-hu,dc=com?one  
# --- ldap.conf --- #
```

11. A harmadik virtuális gép (vz103) konfigurálása

11.1 LDAP kliens konfigurálása

Lásd 10.2 részt

11.2 MySQL telepítése

Telepítsük fel a szükséges csomagokat:

```
yum install mysql-server mysql
```

Állítsuk be, hogy bootoláskor is induljon a 3-as futási szinten:

```
chkconfig --level 3 mysqld on
```

Indítsuk el a szolgáltatást:

```
service mysqld start
```

11.3 PostgreSQL telepítése

Telepítsük fel a szükséges csomagokat:

```
yum install postgresql-*
```

Állítsuk be, hogy bootoláskor is induljon a 3-as futási szinten:

```
chkconfig --level 3 postgresql on
```

Indítsuk el a szolgáltatást:

```
service postgresql start
```

Konfiguráljuk az SQL szerveret:

```
# /var/lib/pgsql/data/pg_hba.conf
...
# TYPE DATABASE USER CIDR-ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all ident sameuser
# IPv4 local connections:
host all all 127.0.0.1/32 ident sameuser
# IPv6 local connections:
host all all ::1/128 ident sameuser
# engedélyezzük a 192.168.1.0/24 tartományból a kapcsolódást a pam modulon keresztül,
# azaz ahol az LDAP autentikációt beállítottuk az authconf-tui programmal
host all all 192.168.1.0/24 pam
# --- end of file --- #
```

```
# /var/lib/pgsql/data/postgresql.conf
listen_addresses = '*'
#port = 5432
max_connections = 100
# --- end of file --- #
```

Állítsuk be a postgres user jelszavát, amennyiben szükséges:

```
passwd postgres
```

Váltunk át postgres userre és adjuk hozzá az admin usert:

```
su - postgres  
createuser admin
```

12. A negyedik virtuális gép (vz104) konfigurálása

12.1 LDAP kliens konfigurálása

Lásd 10.2 részt

12.2 Apache Web Szerver (httpd) telepítése

Telepítsük a *httpd* és *SSL* csomagokat:

```
yum install httpd mod_ssl
```

Állítsuk be, hogy bottoláskor is induljon a 3-as futási szinten:

```
chkconfig --level 3 httpd on
```

Az `/etc/httpd/conf/httpd.conf` konfigurációs állományban állíthatjuk be, hogy hol figyeljen a web szerver - az alapbeállítások jók.

A "Listen 80" sort kikommentezhetjük, mert a `mod_ssl` csomag telepítésével a `https` protokollt engedélyeztük, a 443-as porton. Ez az `/etc/httpd/conf.d/ssl.conf` include fájlban adódott a konfigurációhoz.

Indítsuk is el a szervert:

```
service httpd start
```

Egy böngészőben tesztelhetjük a szervert, pl.: `lynx https://vz104.example-hu.com`

12.3 FTP szerver (vsftpd) telepítése

Telepítsük a `vsftpd` FTP szervert:

```
yum install vsftpd
```

Állítsuk be, hogy bottoláskor is induljon a 3-as futási szinten:

```
chkconfig --level 3 vsftpd on
```

Az `/etc/vsftpd` könyvtárban konfigurálható. Alapértelmezésben `anonymous`-ként is használható az ftp szerver. Amennyiben `chroot`-olt környezetet szeretnénk engedni a usereknek, akkor `vsftpd.conf`-ban engedélyezzük a következő két sort:

```
# --- vsftpd.conf --- #  
...  
chroot_list_enable=YES  
chroot_list_file=/etc/vsftpd/chroot_list
```



```
...
# --- end of file --- #
```

Indítsuk is el a szerveret :

```
service vsftpd start
```

A *chroot list* fájlba soronként írhatjuk be azokat a usereket, akiknek chroot-olt környezetet szeretnénk beállítani. Célszerű minden usernek. Az */etc/vsftpd/ftpusers* fájlban adható meg a be nem engedhető userek neve.

13. Az ötödik virtuális gép (vz105) konfigurálása

13.1 LDAP kliens konfigurálása

Lásd 10.2 részt

13.2 Levelező szerver telepítése

Telepítsük fel a szükséges csomagokat:

```
yum install sendmail sendmail-* dovecot
```

A sendmail MTA szerver programunk alapból jól működik, a localhost-on figyel.

A dovecot POP/IMAP szerver programunk is alapértelmezésben jó, amennyiben csak imap v. pop3 protokollra szeretnénk beállítani, csak az */etc/dovecot.conf*-ban kell egy kicsit módosítanunk:

```
# --- /etc/dovecot.conf --- #
...
protocols = imap pop3
...
# --- end of file --- #
```

A sendmail-t az */etc/mail/local-host-names* fájllal tudjuk beállítani, tudatva a sendmail-el, hogy milyen hosztneveket kell kezelnie:

```
# --- /etc/mail/local-host-names --- #
example-hu.com
vz105.example-hu.com
# --- end of file --- #
```

Az */etc/sendmail.cf* (sendmail.mc) fájlban ha kivesszük az Addr opciót, akkor minden interfészen fog figyelni a sendmail. Alapértelmezésben csak a localhost-on figyel.

Állítsuk be, hogy bottoláskor is induljon a 3-as futási szinten:

```
chkconfig --level 3 dovecot on
chkconfig --level 3 sendmail on
```

Indítsuk is el a szerveret:

```
service dovecot start
service sendmail start
```

14. Mentések kezelése az OpenVZ-ben

Telepítsük a vzdump csomagot, amit azonban le kell tölteni az internetről függőségeivel együtt (cstream):

cstream: http://pkgs.repoforge.org/cstream/cstream-3.1.0-1.el6.rf.x86_64.rpm

vzdump: <http://download.openvz.org/contrib/utls/vzdump/vzdump-1.2-4.noarch.rpm>

```
yum localinstall vzdump-1.2-4.noarch.rpm cstream-3.1.0-1.el6.rf.x86
```

A mentésre az alábbi lehetőségek vannak:

VPSID mentése:

```
vzdump VPSID
```

VPSID snapshot mentés (minimális leállással):

```
vzdump --suspend VPSID
```

Minden konténer mentése, levél küldés root-nak:

```
vzdump --suspend --all --mailto root
```

LVM2 snapshot mentés dumpdir megadásával (VPSID: a VPS azonosító):

```
vzdump --dumpdir /valahol --snapshot VPSID
```

Mentés visszaállítás (VPSID: a VPS azonosító):

```
vzdump --restore /valahol/vzdump-777.tar VPSID
```

ill.

```
vzrestore /valahol/vzdump-777.tar VPSID
```

Készítsünk egy mentést mi is:

```
vzdump --all
```

vagy

```
vzdump 101
```

```
vzdump 102
```

```
vzdump 103
```

```
vzdump 104
```

```
vzdump 105
```

Alapértelmezésben a /vz/dump könyvtár alatt található a mentések (ha nem adunk meg más útvonalat a *-dumpdir* opcióval).

15. Adminisztráció

Egy webes adminisztrációs felületet telepíthetünk a rendszerhez, melyben több fizikai szervert is felvehetünk és menedzselhetjük a VPS-eket.

<http://code.google.com/p/ovz-web-panel/>

Töltsük le az *OpenVZ-Web-Panel* webes rendszert, mely automatikusan feltelepíti a függőségeket és el is indul:

```
wget -O - http://ovz-web-panel.googlecode.com/svn/installer/ai.sh | sh
```

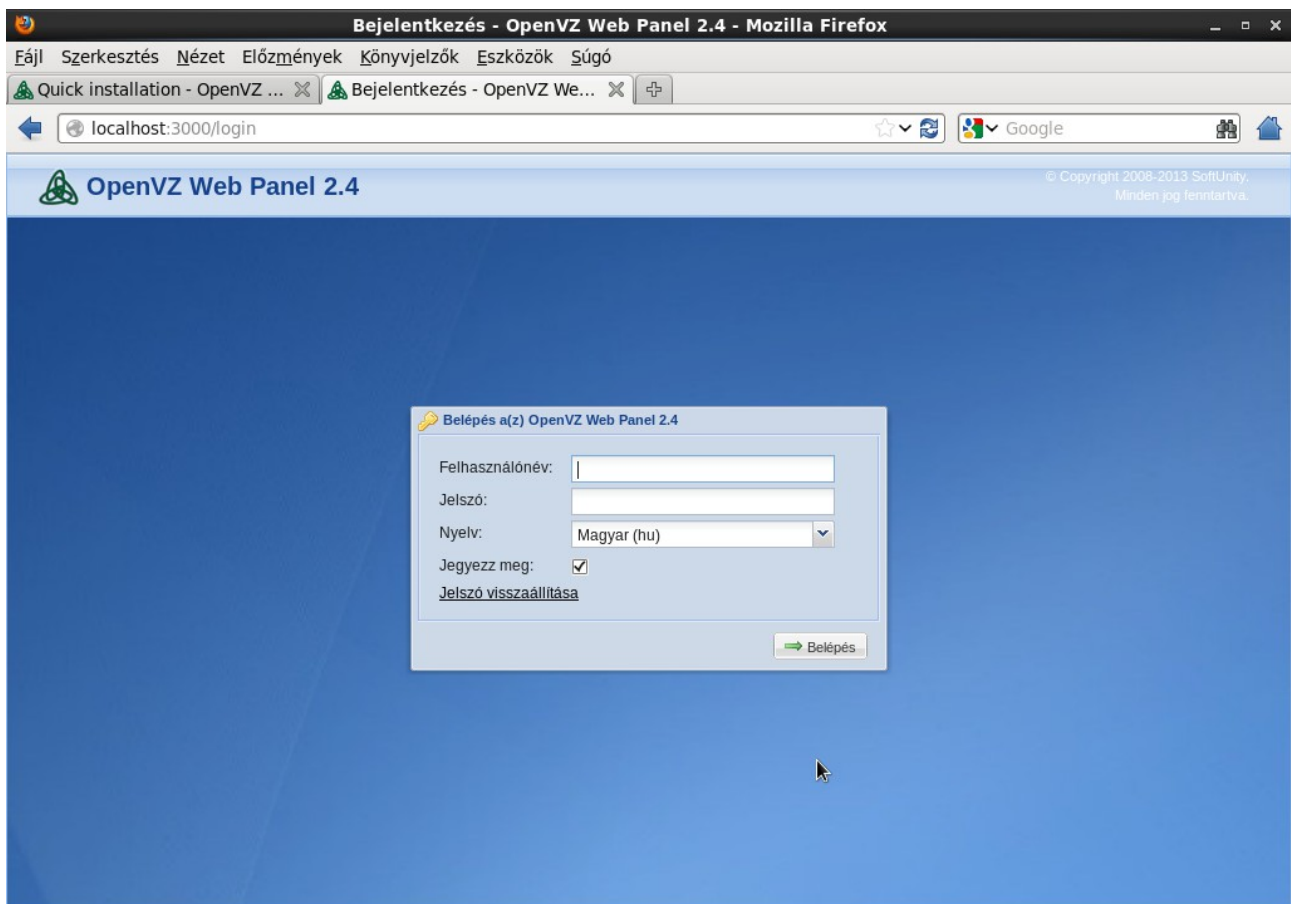
Telepítés után böngészőben meghívhatjuk a felületét:

<http://localhost:3000>

Az alapértelmezett belépés: *admin/admin*

A szolgáltatás így indítható később: `service owp start`

Mivel magyar nyelven is tud, könnyen eligazodhatunk benne:



Műszerfal - OpenVZ Web Panel 2.4 - Mozilla Firefox

Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó

Quick installation - OpenVZ ... Műszerfal - OpenVZ Web Pa...

localhost:3000/admin/dashboard

OpenVZ Web Panel 2.4 © Copyright 2008-2013 SoftUnity. Minden jog fenntartva.

Műszerfal

Keresés Egy szintel feljebb

Bemutató
Az OpenVZ Web Panel egy web alapú grafikus felület az OpenVZ virtualizációs technológiát használó fizikai kiszolgáló gépek vezérésére.

Profil
Bejelentkezve mint admin.

Statistika

Paraméter	Érték
Panel felhasználók	1
Fizikai szerverek	1
Virtuális szerverek	0
Futó virtuális szerverek	0
Megállított virtuális szerverek	0
Lejárt virtuális szerverek	0
Nyitott kérések	0

Menü

Általános

- Műszerfal
- Fizikai szerverek
 - localhost
- IP címek
- Profilom
- Felhasználók
- Kérések
- Feladatok
- Eseménynapló
- Kijelentkezés

Súgó

- Dokumentáció (online)
- Támogatás (online)

Fizikai szerverek - OpenVZ Web Panel 2.4 - Mozilla Firefox

Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó

Quick installation - OpenVZ ... Fizikai szerverek - OpenVZ ...

localhost:3000/admin/hardware-servers/list

OpenVZ Web Panel 2.4 © Copyright 2008-2013 SoftUnity. Minden jog fenntartva.

Fizikai szerverek

Keresés Egy szintel feljebb

Fizikai szerverek listája

Csatlakozás új szerverhez Szerver leválasztása Szinkronizálás Beállítások módosítása Részletek Újrاندítás

Gépnév	Virtuális Szerverek	Leírás
localhost	0	

Menü

Általános

- Műszerfal
- Fizikai szerverek
 - localhost
- IP címek
- Profilom
- Felhasználók
- Kérések
- Feladatok
- Eseménynapló
- Kijelentkezés

Súgó

- Dokumentáció (online)
- Támogatás (online)

A webes felületen szinten mindent elvégezhetünk.

A rendszerünk működésre kész, természetesen finomítani lehet még rajta. :)

16. OpenVZ és a ZFS

A ZFS az Oracle (korábban Sun) fájlrendszere, amely egyfajta kötetkezelőt és szoftveres RAID-megvalósítást is tartalmaz. Fő előnyei [3]:

- Rendkívül kényelmes adminisztráció
- SSD-k ésszerű használata (cache-ként)
- ellenőrző összegek (észleli és esetenként javítja az amúgy észrevétlen hibákat)
- a látszólag különböző rétegbe való funkciók (RAID, kötetkezelés, fájlrendszer) integrálása révén pl. RAID-helyreállításakor csak a foglalt területeket kell szinkronizálnia (és egyéb előnyök is származnak ebből)
- röptömörítés
- in-line deduplikáció
- stb.

Az OpenVZ után a zfs-t fel tudjuk telepíteni a CentOS szerverünkre (<http://zfsonlinux.org>).

```
yum localinstall --nogpgcheck http://archive.zfsonlinux.org/epel/zfs-release-1-2.el6.noarch.rpm
yum install zfs
chkconfig zfs on
service zfs start
```

További csomagokat fog telepíteni a gépünkre, de előtte szükséges lehet:

```
yum install vzkernel-devel vzkernel-headers gcc
```

Az alapértelmezett OpenVZ könyvtár a „/vz”.

Állítsuk le az OpenVZ szolgáltatást:

```
service vz stop
```

Mentsük el, vagy nevezzük át a /vz könyvtárat (pl. */vz.old*).

Jelen esetben van 4 merevlemezünk még a rendszeren kívül (sdb,sdc,sdd,sde), amit *mirror*-ba tesszünk. Hozzuk létre a pool-okat és zfs-eket, egy *vzpool*-t és egy *backuppool*-t:

```
zpool create vzpool mirror sdb sdc -f
zfs create vzpool/vz
zfs set mountpoint=/vz vzpool/vz
zfs mount -a

zpool create backuppool mirror sdd sde -f
zfs create backuppool/backup
```

Lehetőleg a pool-ba közvetlen ne dolgozzunk (pool gyökerébe), mindig hozzunk létre benne egy zfs-t.

A státuszokat így tudjuk ellenőrizni:

```
zfs list
zpool list
zpool status -v
```

Valami ilyesmit kell látnunk:

```
[root@centos]# zfs list
NAME                USED  AVAIL  REFER  MOUNTPOINT
backuppool          145K  3,91G   31K    /backuppool
backuppool/backup    30K   3,91G   30K    /backuppool/backup
vzpool              213M  3,70G   30K    /vzpool
vzpool/vz           213M  3,70G  213M    /vz

[root@centos]# zpool list
NAME                SIZE  ALLOC  FREE   CAP  DEDUP  HEALTH  ALTROOT
backuppool          3,97G  145K  3,97G   0%  1.00x  ONLINE  -
vzpool              3,97G  213M  3,76G   5%  1.00x  ONLINE  -

[root@centos]# zpool status -v
pool: backuppool
state: ONLINE
scan: none requested

config:

NAME                STATE      READ  WRITE  CKSUM
backuppool          ONLINE      0     0     0
  mirror-0          ONLINE      0     0     0
    sdd              ONLINE      0     0     0
    sde              ONLINE      0     0     0

errors: No known data errors

pool: vzpool
state: ONLINE
scan: none requested

config:

NAME                STATE      READ  WRITE  CKSUM
vzpool              ONLINE      0     0     0
  mirror-0          ONLINE      0     0     0
    sdb              ONLINE      0     0     0
    sdc              ONLINE      0     0     0

errors: No known data errors
```

A *vzpool*-ban levő *vz* zfs-t a */vz* útvonalra tettük. Az elmentett *vz* könyvtár tartalmát (*/vz.old*) másoljuk vissza a jelenlegi zfs-en létrehozott */vz* útvonalra, majd indítsuk is el az OpenVZ-t:

```
service vz start
```

Készítsünk egy backup-ot a */vz*-ről:

```
zfs snapshot vzpool/vz@snapnow
```

A *snapshot*-ok a zfs alatt a *.zfs/snapshot* könyvtár alatt találjuk (rejtett könyvtár!).

Majd a *backuppool*-ba küldjük a *snapshot*-ot, mint egy „távoli” mentés:

```
zfs send vzpool/vz@snapnow | zfs receive -d backuppool/backup
```

A *backuppool/backup* alatt megtaláljuk a *vzpool/vz* (azaz a */vz*) másolatát.

Szükség esetén a *snapshot*-ból visszaállíthatók az adatok:

```
zfs rollback vzpool/vz@snapnow
```

További finomításokat is csinálhatunk, pl. *ssh*-val egy másik gépre inkrementális mentés küldhetünk:

```
zfs send -i vzpool/vz@snapnow vzpool/vz@snapnow2 | ssh masikgep zfs receive -d backuppool/backup
```

Törlés az alábbi parancsokkal lehetséges (*snapshot*, *zfs*, *pool*):

```
zpool destroy vzpool
zfs destroy vzpool/vz -r
zfs destroy vzpool/vz@snapnow
```

Szükség esetén növelhető a *zfs* (*expand pool*, *resize*):

```
zpool set autoexpand=on vzpool
zpool online -e vzpool sdb
zpool online -e vzpool sdc
```

Jelenleg a *zfs* 0.6 verziónál tart. Várhatóan a telepítéskor is használható lesz a későbbiekben.

17. Virtual Ethernet device (veth)

Alapértelmezett hálózat interfész a *venet*, amely kívülről nem elérhető (nem látszódik). Amennyiben nem ezt szeretnénk, akkor ún. *veth* (virtual ethernet device) eszközt kell létrehoznunk.

A *veth* és a *venet* eszközök közötti különbség:

Feature	veth	venet
MAC address	Yes	No
Broadcasts inside CT	Yes	No
Traffic sniffing	Yes	No
Network security	Low	High
Can be used in bridges	Yes	No
IPv6 ready	Yes	Yes
Performance	Fast	Fastest

A https://openvz.org/Quick_Installation_CentOS_6 alapján a veth eszköz létrehozása:

Az openvz kernel és utility-k feltelptítése után a *sysctl.conf* beállítása:

```
# /etc/sysctl.conf
net.ipv4.ip_forward = 1
net.ipv4.conf.default.proxy_arp = 0
net.ipv4.conf.all.rp_filter = 1
kernel.sysrq = 1
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.conf.default.forwarding=1
```

A host gépen a *bridge-utils* csomag szükséges, amennyiben még nincs fent:

```
yum install bridge-utils
```

Ha a host gépünk pl. 192.168.1.99/24, a gateway 192.168.1.1 címen van. A 192.168.1.101, 192.168.1.102... stb. címen a konténerek, a virtuális gépek találhatóak.

A host gépen hozzunk létre egy *vmbr0* bridge eszközt:

```
# vi /etc/sysconfig/network-scripts/ifcfg-vmbr0
DEVICE="vmbr0"
BOOTPROTO="static"
IPV6INIT="no"
ONBOOT="yes"
TYPE="Bridge"
DELAY=0
IPADDR=192.168.1.99
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
```

Az *eth0* eszközünk legyen beállítva a *vmbr0* bridge eszközre:

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
ONBOOT="yes"
IPV6INIT="no"
TYPE="Ethernet"
BRIDGE="vmbr0"
```

Az `/etc/vz/vznet.conf` fájlba helyezzük el következő bejegyzést, mely az eszközöket fogja beállítani:

```
#!/bin/bash
EXTERNAL_SCRIPT="/usr/sbin/vznetaddr"
```

Hozzuk létre és konfiguráljuk a **VETH** típusú konténert:

```
# vzctl create 102 --ostemplate centos-6-x86_64 --config vswap-1g

# vzctl set 102 --save --name server102
# vzctl set 102 --save --onboot yes
# vzctl set 102 --save --hostname server102.example.com
# vzctl set 102 --save --netif_add eth0,,,FE:FF:FF:FF:FF:FF
# vzctl set 102 --save --searchdomain example.com
# vzctl set 102 --save --nameserver 8.8.8.8 --nameserver 8.8.4.4
# vzctl set 102 --save --cpus 4
# vzctl set 102 --save --ram 8G
# vzctl set 102 --save --swap 4G
# vzctl set 102 --save --diskspace 100G
# vzctl start 102
# vzctl exec 102 passwd
```

A virtuális gép (VPS, konténer) hálózati beállításait így végezzük el:

```
# cat << _EOF_ > /vz/root/102/etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
HOSTNAME="server102"
IPV6INIT="no"
MTU="1500"
TYPE="Ethernet"
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.102
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
_EOF_

# vzctl exec 102 /etc/init.d/network restart
```

Ezután már csak egy **reboot** kell és működik a rendszer.

Felhasznált irodalom, hivatkozások:

- [1] <http://www.openvz.org>
- [2] http://openvz.org/Quick_installation
- [3] <http://unixlinux.tmit.bme.hu/ZFS>