Megvalósulási dokumentáció

www.npsh.hu

Informatikai infrastruktúra fejújítása

a BME Elektronikus Eszközök Tanszéke részére

Novell

Védjegyek és Jogi nyilatkozat

Copyright © Novell, Inc. Minden jog fenntartva.

A Novell, és termékei a Novell, Inc. bejegyzett védjegyei az Egyesült Államokban és más országokban. A bejegyzett védjegyek teljes listája a Novell weboldalán található: http://www.novell.com/company/legal/trademarks/tmlist.html.

A Linux Linus Torvalds bejegyzett védjegye. Az egyéb védjegyek a birtokos cégek tulajdonát képezik.

A jelen dokumentáció kizárólag a BME Elektronikus Eszközök Tanszéke, ügyfél címe részére készült, ezért egyéb területen, más szervezetnél történő alkalmazásokhoz a Novell Consulting és a Novell Professional Services Hungary nem járul hozzá. A jelen anyag nem másolható, fénymásolható, továbbítható vagy tárolható, csak a Novell Professional Services Hungary előzetes írásos engedélyével.

A jelen dokumentum OpenOffice.org 3.2.1 Novell Edition programmal készült.

Novell Professional Services Hungary
1124 Budapest, Csörsz u. 45.
Tel.: +36 1 4894600 Fax.: +36 1 4894601

Tartalomjegyzék

I. Projekt bemutatása

A projekt célja az Ügyfél meglévő heterogén, nehezen karbantartható hálózati szolgáltatásainak egyszerűsítése konszolidációja, új hardveren.

A rendszer elsődleges feladatai közé tartoznak:

- email (SMTP, IMAP, webmail) szolgáltatás
- tűzfal, router funkciók
- web kiszolgálás (intra és extranet)
- DHCP
- DNS
- címtár
- hálózat felügyelet

Az eredeti rendszer ezeket a funkciókat számos szerveren elosztva, különböző operációs rendszerek alkalmazásával valósította meg (OpenBSD, FreeBSD, Linux disztribúciók). Ezek fenntartása több szempontból is nehézkessé vált. A fenntartáshoz sok operációz rendszer alapos ismeretére van szükség, az eltérő eszközök gondot okoznak a betanulás során. Ezek a rendszerek már úgymond elöregedtek, rajtuk számos forrásból nehezen kiismerhető struktúrában kerültek fel alkalmazások ami tovább nehezíti a biztonságos üzemet.

A projekt folyamán két fizikai számítógépen kiépítettünk egy rendszert, mely összesen egy operációs rendszert tartalmaz, mely gyártói támogatással rendelkezik és ahol lehet, a támogatott csomagokból építkeztünk. Az Ügyfél alkalmazottai a rendszer üzemeltetésével kapcsolatos tanfolyam vettek részt, ezzel is könnyítve a helyben történő probléma megoldást és üzemeltetést.

A továbbiakban projekt eredményeképpen felállt rendszert ismerteti nagyobb mélységben a dokumentum. A dokumentum biztonsági okokból nem tartalmaz pontos címeket, tűzfal szabályokat és egyéb olyan információkat amik a rendszer biztonsági kitettségét elfogadhatatlan mértékben fokozná. A dokumentumot az Ügyfél képviselőinek jóváhagyásával, a HUEDU program feltételeinek megfelelően tesszük közzé.

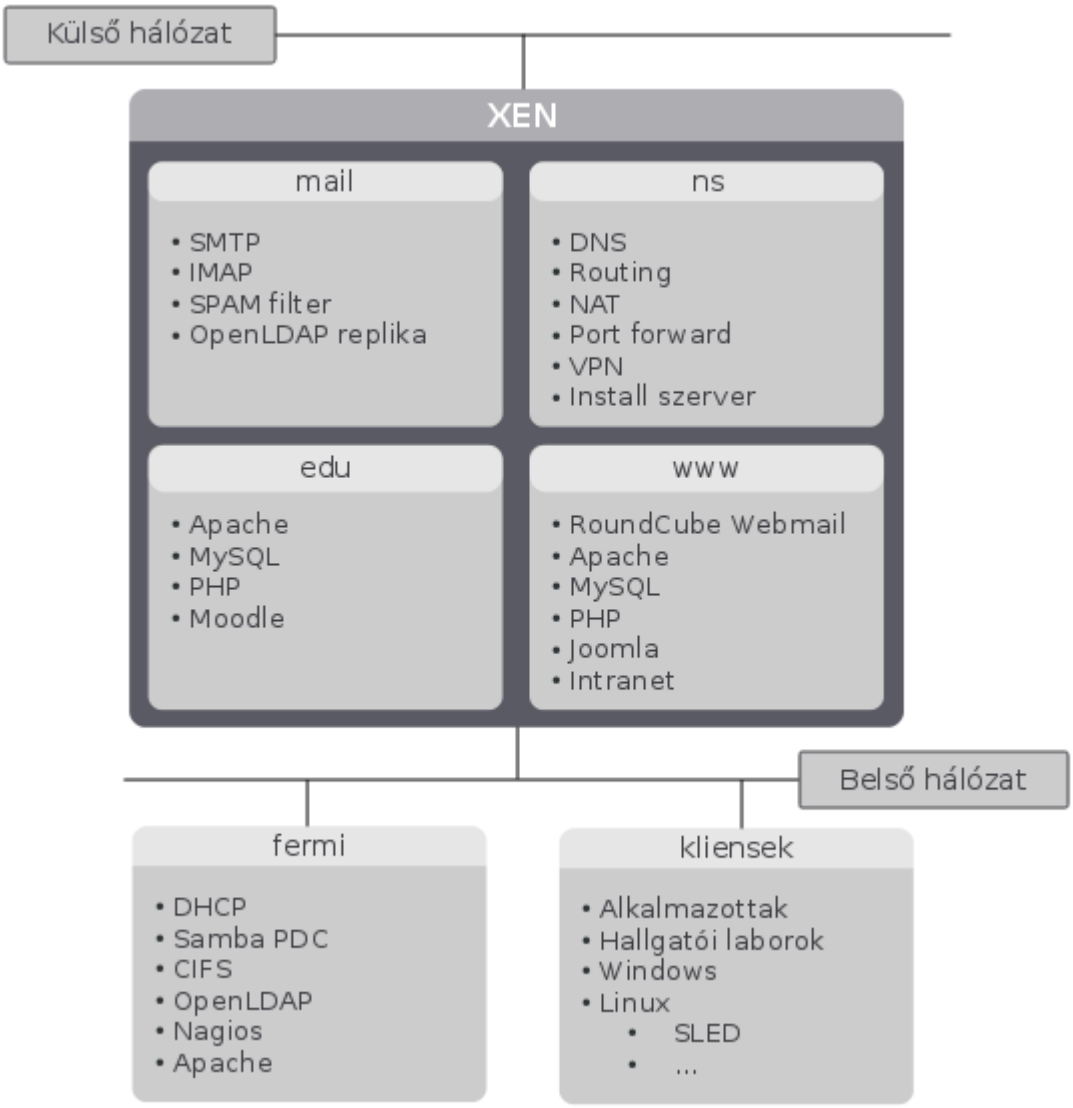
II. Architektúra vázlatok

II.1. Hálózat és szolgáltatások

A hálózatot két részre bonthatjuk, a belső ún. védett oldalra és a külső, Internet forgalomtól nem védett ún. kitett oldalra, A két oldal közti kapcsolatot a XEN virtualizációs platformon futó egyik virtuális gép kapcsolja össze, ez a gép végzi a routolási címfordítási és tűzfal feladatokat. Ennek megfelelően ebben a gépben két hálózati csatolót használunk.

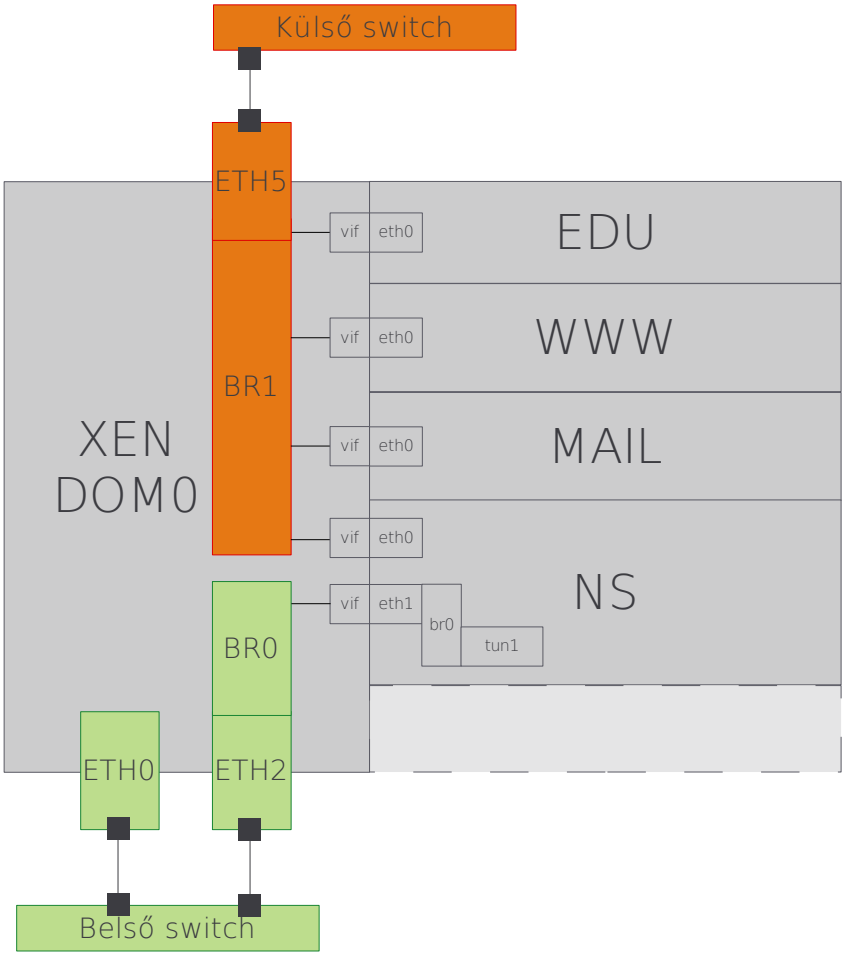
A belső oldalon találhatóak a laborok, a belső szolgáltatásokat futtató fizikai kiszolgálóval és a tanszéki munkaállomásokkal egyetemben.

Az alábbi ábra ismerteti a különböző szolgálatások elhelyezkedését az infrastruktúrában:


Külső hálózat
XEN
mail
• SMTP
• IMAP
• SPAM filter
• OpenLDAP replika
ns
• DNS
• Routing
• NAT
• Port forward
• VPN
• Install szerver
edu
• Apache
• MySQL
• PHP
• Moodle
www
• RoundCube Webmail
• Apache
• MySQL
• PHP
• Joomla
• Intranet
Belső hálózat
fermi
• DHCP
• Samba PDC
• CIFS
• OpenLDAP
• Nagios
• Apache
kliensek
• Alkalmazottak
• Hallgatói laborok
• Windows
• Linux
• SLED
• ...

II.2. Virtualizációs platform

Az Ügyfél által vásárolt új kiszolgálón az erőforrások optimális kihasználása végett virtualizációt alkalmazunk. Így több rendszer futhat egy fizikai kiszolgálón.



III. Alkalmazások és operációs rendszerek

III.1. XEN domU rendszerek közös beállításai

A www, mail, ns, és edu nevű kiszolgálók virtualizáltan futnak. Ezeken néhány beállítást eszközöltünk az optimális teljesítmény elérése érdekében.

III.1.1 I/O ütemező deadline-ra állítva

Az I/O ütemezőt érdemes kiiktatni a virtuális gépen belül, mivel a dom0 már ütemezi a diszk I/O-t. Az alábbi script részlet erre utasítja a kernelt.

/etc/init.d/boot.local

```
echo noop > /sys/block/xvda/queue/scheduler
```

III.2. xen.eet.bme.hu

A virtualizációs környezet privilegizált domainje, az ún. dom0

III.2.1 Hálózati beállítások

Egyedül az eth0 csatolónak van IP címe, ezért ezt a domaint csak belülről lehet elérni. Ez biztonsági okokból fontos mivel ebből a virtuális gépből lehetséges a teljes körű hardware kezelés és a többi virtuális gép kezelése is.

ip cím	interface	bridge	vm
x.x.x.x	eth0	-	-
-	eth2	br0	ns
-	eth5	br1	ns, mail, www, edu

III.2.1.1 Default router

A default router beállítás el lehet hagyni amennyiben nem kell a gépnek internet hozzáférés. Ebben az esetben a biztonsági elérése frissítések miatt döntöttünk az Internet elérés engedélyezése miatt.

/etc/sysconfig/network/routes

```
default x.x.x.254 - -
```

III.2.1.2 DNS konfiguráció

```
search eet.bme.hu
nameserver x.x.x.254
nameserver 152.66.115.1
nameserver 152.66.116.1
```

III.2.2 Diszk konfiguráció

A fizikai gépben, így a dom0-ban elérhetően, két 500G SATA diszk van, és egy darab 146G SAS diszk az integrált RAID vezérlőre kötve.

III.2.2.1 Partíciók

```
Disk /dev/sda: 500.1 GB, 500107862016 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          25      200781   fd  Linux raid
autodetect
/dev/sda2              26       60801   488183220   fd  Linux raid
autodetect

Disk /dev/sdb: 500.1 GB, 500107862016 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *           1          25      200781   fd  Linux raid
autodetect
/dev/sdb2              26       60801   488183220   fd  Linux raid
autodetect


Disk /dev/cciss/c0d0: 146.8 GB, 146778685440 bytes
```

```
            Device Boot      Start         End      Blocks   Id  System
/dev/cciss/c0d0p1               1       17844   143331898+  8e  Linux LVM
```

III.2.2.2 Szoftver RAID

Mivel a beépített hardveres RAID vezérlőhöz nincs elegendő diszk, szoftver RAID-et alkalmaztunk a megfelelő hibatűrés kialakításához. A

/etc/mdadm.conf

```
DEVICE containers partitions
ARRAY /dev/md0 UUID=ffef1c73:e82e5373:4664b992:42179855
ARRAY /dev/md1 UUID=3f4b99b2:df4761e7:89e56793:7651ee89
```

Az md0 tömb az sda1 sdb1 partíciókból az md1 tömb az sda2 sdb2 partíciókból áll, RAID1 konfigurációban. A tömböket a YaST segítségével alap beállításokkal hoztuk létre.

III.2.2.3 LVM konfig

A logikai kötet kezelő alkalmazásával megfelelően rugalmas diszk menedzsment megoldást kapunk ami elengedhetetlen virtualizált környezetekben.

III.2.2.3.1 Volume group

A sas kötet az sdc diszkre míg a system kötet az md1 tömbre épül.

```
VG     #PV #LV #SN Attr   VSize   VFree
sas      1   3   0 wz--n- 136.69G 22.69G
system   1   6   0 wz--n- 465.57G 27.57G
```

III.2.2.3.2 Logikai kötetek

Az alábbi logikai köteteket definiáltuk.

```
LV        VG     Attr   LSize
install   sas    -wi-ao  10.00G
migration sas    -wi-ao 100.00G
swap      sas    -wi-ao   4.00G
edu       system -wi-ao  30.00G
mail      system -wi-ao 320.00G
ns        system -wi-ao  10.00G
root      system -wi-ao  10.00G
var       system -wi-ao   8.00G
www       system -wi-ao  60.00G
```

Minden virtuális gép kap egy saját logikai kötetet. Ezen felül ideiglenes adattárolásra használt (migration), és az install szervernek helyet adó (install) kötetek kaptak helyet a SAS diszken. Itt helyezkedik el a swap kötet is.

III.2.2.4 fstab

A csatolt fájlrendszerek listája:

```
/dev/sas/swap        swap                swap    defaults              0 0
/dev/system/root     /                   ext3    noatime,acl,user_xattr 1 1
UUID=e081941b-ddef-4b57-8fcd-3af0c202ecfa /boot   ext2       noatime,noacl
1 2
/dev/system/var      /var                ext3    noatime,acl,user_xattr 1 2
proc                 /proc               proc    defaults              0 0
sysfs                /sys                sysfs   noauto                0 0
debugfs              /sys/kernel/debug   debugfs noauto                0 0
usbfs                /proc/bus/usb       usbfs   noauto                0 0
devpts               /dev/pts            devpts  mode=0620,gid=5       0 0
```

```
/dev/sas/migration   /srv/migration       xfs     defaults              0 0
```

III.2.3 Virtuális gépek listája

név	típus
XEN	dom0
edu	domU
mail	domU
www	domU
ns	domU

```
Name                                ID   Mem VCPUs      State   Time(s)
Domain-0                             0  4923    16     r-----  72894.3
edu                                  7  2048     8     -b----  11866.2
mail                                 6  2048     8     -b----  19451.6
ns                                   3  1024     2     -b----  10804.4
www                                  8  2048    10     -b----  12341.2
```

> Minden domain automatikusan indul, a dom0 bootolása során

III.2.3.1 edu

```
name="edu"
description="None"
uuid="26221fe4-e77d-8a71-ddd1-f2548807683c"
memory=2048
maxmem=4096
vcpus=8
maxvcpus=12
on_poweroff="destroy"
on_reboot="restart"
on_crash="destroy"
localtime=0
keymap="en-us"
builder="linux"
bootloader="/usr/bin/pygrub"
bootargs=""
extra=""
disk=[ 'phy:/dev/system/edu,xvda,w', ]
vif=[ 'mac=00:16:3e:00:00:03,bridge=br1', ]
vfb=['type=vnc,vncunused=1']
```

III.2.3.2 mail

```
name="mail"
description="None"
uuid="b87716a2-cc3c-942c-a8a1-ce23c7f94409"
```

```
memory=2048
maxmem=4096
vcpus=8
maxvcpus=12
on_poweroff="destroy"
on_reboot="restart"
on_crash="destroy"
localtime=0
keymap="en-us"
builder="linux"
bootloader="/usr/bin/pygrub"
bootargs=""
extra=""
disk=[ 'phy:/dev/system/mail,xvda,w', ]
vif=[ 'mac=00:16:3e:00:00:05,bridge=br1', ]
vfb=['type=vnc,vncunused=1']
```

III.2.3.3 ns

```
name="ns"
description="None"
uuid="ab59b575-fef4-7df4-57d3-a5f05cb8f3b8"
memory=1024
maxmem=4096
vcpus=4
maxvcpus=12
on_poweroff="destroy"
on_reboot="restart"
on_crash="destroy"
localtime=0
keymap="en-us"
builder="linux"
bootloader="/usr/bin/pygrub"
bootargs=""
extra=" "
disk=[ 'phy:/dev/system/ns,xvda,w', 'phy:/dev/sas/install,xvdb,w']
vif=[ 'mac=00:16:3e:00:00:01,bridge=br1', 'mac=00:16:3e:00:00:02,bridge=br0'
]
vfb=['type=vnc,vncunused=1']
```

III.2.3.4 www

```
name="www"
description="None"
uuid="32442446-2ec8-743f-f6d2-44032f1aa48c"
memory=2048
maxmem=4096
vcpus=10
maxvcpus=12
on_poweroff="destroy"
on_reboot="restart"
on_crash="destroy"
localtime=0
keymap="en-us"
builder="linux"
bootloader="/usr/bin/pygrub"
bootargs=""
extra=""
disk=[ 'phy:/dev/system/www,xvda,w', ]
```

```
vif=[ 'mac=00:16:3e:00:00:04,bridge=br1', ]
vfb=['type=vnc,vncunused=1']
```

III.3. ns.eet.bme.hu

Ez a virtuális gép látja el a DNS kiszolgálási, tűzfal és router funkciókat, valamint itt terminálódik a VPN hozzáférés is.

III.3.1 Hálózati beállítások

ip cím	interface	bridge
x.x.x.x	eth0	-
x.x.x.x	eth1, tap0	br0

III.3.1.1 Default router

Ez a gép a BME infrastruktúra részét alkotó routernek továbbít minden kimenő forgalmat.

/etc/sysconfig/network/routes

```
default 152.66.72.30 - -
```

III.3.1.2 DNS konfiguráció

```
search eet.bme.hu
nameserver x.x.x.x
nameserver 152.66.115.1
nameserver 152.66.116.1
```

III.3.2 Diszk konfiguráció

A dom0 system/ns logikai kötetén belül gazdálkodik ez a virtuális gép.

III.3.2.1 Partíciók

```
Disk /dev/xvda: 10.7 GB, 10737418240 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *           1          25      200781   83  Linux
/dev/xvda2              26        1305    10281600   8e  Linux LVM
```

III.3.2.2 LVM konfig

III.3.2.2.1 Volume group

```
  VG     #PV #LV #SN Attr   VSize VFree
  system   1   2   0 wz--n- 9.80G 4.00M
```

III.3.2.2.2 Logikai kötetek

```
  LV   VG     Attr   LSize
```

```
  root system -wi-ao   9.30G
  swap system -wi-ao 512.00M
```

III.3.2.3 fstab

```
/dev/system/swap     swap                swap       defaults           0 0
/dev/system/root     /                   ext3       noatime,acl,user_xattr
1 1
/dev/xvda1           /boot               ext2       noatime,noacl    1 2
proc                 /proc               proc       defaults         0 0
sysfs                /sys                sysfs      noauto           0 0
debugfs              /sys/kernel/debug   debugfs    noauto           0 0
devpts               /dev/pts            devpts     mode=0620,gid=5  0 0
/dev/xvdb            /srv/install        ext3       noatime,noacl    1 2
/srv/install/sles11sp1x64.iso /srv/ftp/sles11sp1x64 iso9660 loop,ro   0 0
/srv/install/SLED-11-SP1-DVD-i586-GM-DVD1.iso /srv/ftp/sled11sp1i586 iso9660
loop,ro 0 0
/etc/openvpn /var/openvpn/etc/openvpn/  none   bind,defaults       0 0
```

A csatolt ISO image-ek a dom0 sas/install kötetén vannak, itt /dev/xvdb néven jelennek meg. Az ISO image-ek adják a csomagokat a telepített SUSE szervereknek és munkaállomásoknak.

III.3.3 Szolgáltatások listája

szolgáltatás	alkalmazás neve
DNS	ISC bind
VPN	OpenVPN
tűzfal	Linux netfilter, egyedi script

III.3.4 ISC bind konfigurációja

III.3.4.1 Forwarderek

/etc/named.d/forwarders.conf

```
forwarders {
        152.66.115.1;
        152.66.116.1;
};
```

III.3.4.2 Zónák

A /etc/named.conf összes zónadefinícióját (hint, localhost) ki kell szedni. Mivel a tanszék split view DNS-t használ, minden zónát a view-kon belül kell megadni.

/etc/named.conf.include

```
view "internal" {
        match-clients { x.x.x.x/16; 127.0.0.1/32; };

        zone "eet.bme.hu" {
                type master;
                file "master/db.eet.bme.hu.internal";
```

```
        };
        zone "72.66.152.in-addr.arpa" {
                type master;
                file "master/db.152.66.72";
        };
        zone "x.x.in-addr.arpa" {
                type master;
                file "master/db.x.x.internal";
        };
        zone "localhost" in {
                type master;
                file "localhost.zone";
        };
        zone "0.0.127.in-addr.arpa" in {
                type master;
                file "127.0.0.zone";
                allow-transfer { none; };
        };
        zone "." in {
                type hint;
                file "root.hint";
        };

};
view "external" {
        match-clients { any; };

        zone "eet.bme.hu" {
                type master;
                file "master/db.eet.bme.hu.external";
                allow-transfer { 152.66.72.39; 152.66.115.1; };

        };
        zone "72.66.152.in-addr.arpa" {
                type master;
                file "master/db.152.66.72";
                allow-transfer { 152.66.72.39; 152.66.115.1; };

        };
        zone "localhost" in {
                type master;
                file "localhost.zone";
        };
        zone "0.0.127.in-addr.arpa" in {
                type master;
                file "127.0.0.zone";
                allow-transfer { none; };
        };
        zone "." in {
                type hint;
                file "root.hint";
        };
};
```

III.3.4.3 Chroot

A named a nagyobb biztonság érdekében chrootolva fut, a /var/lib/named könyvtárban. A zónák ebből kifolyólag a /var/lib/named/master könyvtárban találhatóak.

/etc/sysconfig/named

```
NAMED_RUN_CHROOTED="yes"
```

III.3.5 OpenVPN konfigurációja

Az OpenVPN bridge üzemmódban működik. A YaST2-ben hoztunk létre egy TAP csatolót, tap0 névvel. Ezt bridgeltük össze az eth1 csatolóval, a br0 bridge-ben. A teljes konfiguráció YaST-on át készült.

/etc/openvpn/openvpn.conf

```
dev tap0
dev-type tap
port 11194
server-bridge ....
...
...
...
user openvpn
group openvpn
chroot /var/openvpn
comp-lzo
verb 3
mute 20
dh /etc/openvpn/dh1024.pem
ca /etc/ssl/certs/YaST-CA.pem
cert /etc/openvpn/ovpn.pem
key /etc/openvpn/ovpn.pem
crl-verify /etc/openvpn/crl.pem
tls-auth /etc/openvpn/ta.key 0
replay-persist /var/run/openvpn/openvpn.persist
writepid /var/run/openvpn/openvpn.pid
status /var/run/openvpn/openvpn-status.log
keepalive 10 120
persist-key
persist-tun
daemon
```

III.3.6 Tűzfal konfigurációja

A tűzfal a komplex helyi követelmények miatt nem valósítható meg a YaST keretrendszeren át, ezért egyedi fejlesztésű scriptet alkalmaztunk. Ezt biztonsági okokból nem tesszük itt közzé. A tűzfal scriptet egy init script indítja el boot idején.

III.4. www.eet.bme.hu

Ez a szerver szolgálja ki a webes szolgálatatások többségét. Itt találhatóak a tanszék weboldalai és a webmail felület is.

III.4.1 Hálózati beállítások

ip cím	interface
x.x.x.x	eth0

III.4.1.1 Default router

Ez a gép a kitett oldalon van, ezért a BME routere a default gateway.

/etc/sysconfig/network/routes

```
default 152.66.72.30 - -
```

III.4.1.2 DNS konfiguráció

```
search eet.bme.hu
nameserver 152.66.72.29
nameserver 152.66.115.1
nameserver 152.66.116.1
```

III.4.2 Diszk konfiguráció

III.4.2.1 Partíciók

A virtuális gép egyetlen diszkje a dom0-ban létrehozott system/www köteten van.

```
Disk /dev/xvda: 64.4 GB, 64424509440 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *           1          25      200781   83  Linux
/dev/xvda2              26        7832    62709727+  8e  Linux LVM
```

III.4.2.2 LVM konfig

III.4.2.2.1 Volume group

```
  VG     #PV #LV #SN Attr   VSize  VFree
  system   1   4   0 wz--n- 59.80G 5.80G
```

III.4.2.2.2 Logikai kötetek

```
  LV   VG     Attr   LSize
  root system -wi-ao  4.00G
  swap system -wi-ao  1.00G
  var  system -wi-ao  4.00G
  www  system -wi-ao 45.00G
```

III.4.2.3 fstab

```
/dev/system/swap     swap              swap   defaults                0 0
/dev/system/root     /                 ext3   noatime,acl,user_xattr  1 1
/dev/xvda1           /boot             ext2   noatime,noacl           1 2
/dev/system/www      /srv/www          xfs    noatime                 1 2
/dev/system/var      /var              ext3   noatime,acl,user_xattr  1 2
proc                 /proc             proc   defaults                0 0
sysfs                /sys              sysfs  noauto                  0 0
```

```
debugfs              /sys/kernel/debug  debugfs      noauto              0 0
devpts               /dev/pts           devpts mode=0620,gid=5        0 0
/srv/www/data/people      /home         none   bind                   0 0
```

III.4.3 Szolgáltatások listája

szolgáltatás	alkalmazás neve
http szerver	Apache2
Adatbázis	MySQL
Webmail	RoundCube

III.4.4 Apache http szerver konfigurációja

/etc/sysconfig/apache2

```
APACHE_CONF_INCLUDE_FILES=""
APACHE_CONF_INCLUDE_DIRS=""
APACHE_MODULES="actions alias auth_basic authn_file authz_host
authz_groupfile authz_default authz_user authn_dbm autoindex cgi dir env
expires include log_config mime negotiation setenvif ssl suexec userdir
php5"
APACHE_SERVER_FLAGS="SSL"
APACHE_HTTPD_CONF=""
APACHE_MPM=""
APACHE_SERVERADMIN=""
APACHE_SERVERNAME=""
APACHE_START_TIMEOUT="2"
APACHE_SERVERSIGNATURE="off"
APACHE_LOGLEVEL="warn"
APACHE_ACCESS_LOG="/var/log/apache2/access_log combined"
APACHE_USE_CANONICAL_NAME="off"
APACHE_SERVERTOKENS="Minimal"
APACHE_EXTENDED_STATUS="off"
```

/etc/apache2/vhosts.d/eet.bme.hu.conf

```
<VirtualHost *:80>
    ServerAdmin webmaster@www.eet.bme.hu
    ServerName www.eet.bme.hu
    ServerAlias www
    DocumentRoot /srv/www/joomla
    ErrorLog /var/log/apache2/error_log
    CustomLog /var/log/apache2/access_log combined
    HostnameLookups Off
    UseCanonicalName Off
    ServerSignature Off
    Alias /staff/run "/srv/www/data/staff/staff.php"
    Alias /html_templates "/srv/www/data/html_templates"
    Alias /jegyzetek "/srv/www/data/jegyzetek"
    Alias /people "/srv/www/data/people"
    Alias /pub "/srv/www/data/pub"
    Alias /publications "/srv/www/data/publications"
```

```
    Alias /staff "/srv/www/data/staff"
    Alias /staffimages "/srv/www/data/staffimages"
    Alias /szakirany "/srv/www/data/szakirany"

    Redirect Permanent /omail http://webmail.eet.bme.hu
    Redirect Permanent /mail http://webmail.eet.bme.hu
    Include /etc/apache2/aliases.conf
    <IfModule mod_userdir.c>
          UserDir /srv/www/data/people
    </IfModule>
    Alias /new "/srv/www/joomla"
    <Directory "/srv/www/joomla">
          Options Indexes FollowSymLinks
          AllowOverride None
          Order allow,deny
          Allow from all
    </Directory>
    <Directory "/srv/www/data/people">
          Options Indexes
          AllowOverride AuthConfig Limit
        Order allow,deny
        Allow from all
    </Directory>
    <Directory "/srv/www/data/pub">
        Options Indexes
        AllowOverride AuthConfig Limit
        Order allow,deny
        Allow from all
    </Directory>
    <Directory "/srv/www/data/publications">
        Options Indexes
        AllowOverride AuthConfig Limit
        Order deny,allow
        Allow from all
    </Directory>
    <Directory "/srv/www/data/">
        Options None
        AllowOverride All
        Order allow,deny
        Allow from all
    </Directory>
<Directory "/srv/www/data/people/ress/vieea307">
        AuthName "Elektronika (VIEEA307) - belepesi nev/jelszo az eloadason"
        AuthType Basic
        AuthUserFile /etc/apache2/htpasswd
        require user infoel
</Directory>
<Directory "/srv/www/data/people/nagyg/vieea307">
        AuthName "Electronics (VIEEA307)- username/password is given by the lecturer "
        AuthType Basic
        AuthUserFile /etc/apache2/htpasswd
        require user infoel
</Directory>
</VirtualHost>
<VirtualHost *:443>
         ServerAdmin webmaster@www.eet.bme.hu
```

```
        ServerName www.eet.bme.hu
        ServerAlias www
        DocumentRoot /srv/www/joomla
        ErrorLog /var/log/apache2/error_log
        CustomLog /var/log/apache2/access_log combined
    <Directory "/srv/www/htdocs">
        Options none
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
        Alias /new "/srv/www/joomla"
    <Directory "/srv/www/joomla">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
        SSLEngine on
        SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
        SSLCertificateFile /etc/ssl/servercerts/servercert.pem
        SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
        <Files ~ "\.(cgi|shtml|phtml|php3?)$">
            SSLOptions +StdEnvVars
        </Files>
        <Directory "/srv/www/cgi-bin">
            SSLOptions +StdEnvVars
        </Directory>
        SetEnvIf User-Agent ".*MSIE.*" \
                  nokeepalive ssl-unclean-shutdown \
                  downgrade-1.0 force-response-1.0
        CustomLog /var/log/apache2/ssl_request_log   ssl_combined
</VirtualHost>
```

/etc/apache2/vhosts.d/intranet.eet.bme.hu.conf

```
<VirtualHost *:80>
    ServerAdmin webmaster@www.eet.bme.hu
    ServerName intranet.eet.bme.hu
    ServerAlias intranet
    DocumentRoot /srv/www/intranet
    ErrorLog /var/log/apache2/intranet-error_log
    CustomLog /var/log/apache2/intranet-access_log combined
    HostnameLookups Off
    UseCanonicalName Off
    ServerSignature Off
    <Directory "/srv/www/intranet">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from 152.66.72.0/24
    </Directory>
</VirtualHost>
<VirtualHost *:443>
        ServerAdmin webmaster@www.eet.bme.hu
        ServerName intranet.eet.bme.hu
        ServerAlias intranet
        DocumentRoot /srv/www/intranet
```

```
        ErrorLog /var/log/apache2/intranet-error_log
        CustomLog /var/log/apache2/intranet-access_log combined
    <Directory "/srv/www/intranet">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
        SSLEngine on
        SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
        SSLCertificateFile /etc/ssl/servercerts/servercert.pem
        SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
        <Files ~ "\.(cgi|shtml|phtml|php3?)$">
            SSLOptions +StdEnvVars
        </Files>
        <Directory "/srv/www/cgi-bin">
            SSLOptions +StdEnvVars
        </Directory>
        SetEnvIf User-Agent ".*MSIE.*" \
                  nokeepalive ssl-unclean-shutdown \
                  downgrade-1.0 force-response-1.0
        CustomLog /var/log/apache2/ssl_request_log   ssl_combined
</VirtualHost>
```

/etc/apache2/vhosts.d/roundcubemail.conf

```
<VirtualHost *:80>
    ServerAdmin webmaster@www.eet.bme.hu
    ServerName mail.eet.bme.hu
    ServerAlias mail webmail.eet.bme.hu roundcube.eet.bme.hu webmail
    DocumentRoot /srv/www/roundcubemail
    ErrorLog /var/log/apache2/roundcube-error_log
    CustomLog /var/log/apache2/roundcube-access_log combined
    HostnameLookups Off
    UseCanonicalName Off
    ServerSignature Off
    <Directory "/srv/www/roundcubemail">
        Options none
        AllowOverride all
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
<VirtualHost *:443>
        ServerAdmin webmaster@www.eet.bme.hu
        ServerName mail.eet.bme.hu
        ServerAlias mail webmail.eet.bme.hu roundcube.eet.bme.hu webmail
        DocumentRoot /srv/www/roundcubemail
        ErrorLog /var/log/apache2/roundcube-error_log
        CustomLog /var/log/apache2/roundcube-access_log combined
    <Directory "/srv/www/roundcubemail">
        Options none
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
        SSLEngine on
        SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

```
            SSLCertificateFile /etc/ssl/servercerts/servercert.pem
            SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
            <Files ~ "\.(cgi|shtml|phtml|php3?)$">
                SSLOptions +StdEnvVars
            </Files>
            <Directory "/srv/www/cgi-bin">
                SSLOptions +StdEnvVars
            </Directory>
            SetEnvIf User-Agent ".*MSIE.*" \
                       nokeepalive ssl-unclean-shutdown \
                       downgrade-1.0 force-response-1.0
            CustomLog /var/log/apache2/ssl_request_log   ssl_combined
</VirtualHost>
```

III.4.5 MySQL szerver konfigurációja

Alapkonfigurációval működik.

III.4.5.1 Felhasználók

Minden alkalmazás dedikált felhasználóval kapcsolódik a MySQL-hez. Minden felhasználó csak az adott adatbázishoz fér hozzá.

III.5. edu.eet.bme.hu

Ez a szerver futtatja az oktatással kapcsolatos alkalmazásokat. Mivel ez ezek az alkalmazások magasabb biztonsági kockázatú információkat tárolnak, elválasztottuk őket a www-n futó egyéb alkalmazásoktól. A virtuális gép a dom0 system/edu kötetén van.

III.5.1 Hálózati beállítások

ip cím	interface
152.66.72.28	eth0

III.5.1.1 Default router

/etc/sysconfig/network/routes

```
default 152.66.72.30 - -
```

III.5.1.2 DNS konfiguráció

```
search eet.bme.hu
nameserver 152.66.72.29
nameserver 152.66.115.1
nameserver 152.66.116.1
```

III.5.2 Diszk konfiguráció

III.5.2.1 Partíciók

```
Disk /dev/xvda: 32.2 GB, 32212254720 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *           1          25      200781   83  Linux
```

```
/dev/xvda2              26        3916    31254457+  8e  Linux LVM
```

III.5.2.2 LVM konfig

III.5.2.2.1 Volume group

A virtuális gép a dom0 system/edu nevű kötetéből gazdálkodik.

```
PV         VG     Fmt  Attr PSize  PFree
/dev/xvda2 system lvm2 a-   29.80G 8.00M
```

III.5.2.2.2 Logikai kötetek

```
VG     #PV #LV #SN Attr   VSize  VFree
system   1   4   0 wz--n- 29.80G 8.00M
```

III.5.2.3 fstab

```
/dev/system/swap    swap          swap   defaults                  0 0
/dev/system/root    /             ext3   noatime,acl,user_xattr    1 1
/dev/xvda1          /boot         ext2   noatime,noacl             1 2
/dev/system/www     /srv/www      xfs    noatime                   1 2
/dev/system/var     /var          ext3   noatime,acl,user_xattr    1 2
proc                /proc         proc   defaults                  0 0
sysfs               /sys          sysfs  noauto                    0 0
debugfs             /sys/kernel/debug   debugfs      noauto       0 0
devpts              /dev/pts            devpts mode=0620,gid=5    0 0
/srv/www/vhosts/moodle/    /var/www/    none   bind
```

III.5.3 Szolgáltatások listája

szolgáltatás	alkalmazás neve
http szerver	Apache2
Adatbázis	MySQL
Moodle	Moodle

III.5.4 Apache http szerver konfigurációja

/etc/sysconfig/apache2

```
APACHE_CONF_INCLUDE_FILES=""
APACHE_CONF_INCLUDE_DIRS=""
APACHE_MODULES="actions alias auth_basic authn_file authz_host
authz_groupfile authz_default authz_user authn_dbm autoindex cgi dir env
expires include log_config mime negotiation setenvif ssl suexec userdir
php5"
APACHE_SERVER_FLAGS=""
APACHE_HTTPD_CONF=""
APACHE_MPM=""
APACHE_SERVERADMIN=""
APACHE_SERVERNAME=""
APACHE_START_TIMEOUT="2"
```

```
APACHE_SERVERSIGNATURE="on"
APACHE_LOGLEVEL="warn"
APACHE_ACCESS_LOG="/var/log/apache2/access_log combined"
APACHE_USE_CANONICAL_NAME="off"
APACHE_SERVERTOKENS="OS"
APACHE_EXTENDED_STATUS="off"
```

/etc/apache2/vhosts.d/a_moodle.conf

```
<VirtualHost _default_:80>
    ServerAdmin timar@eet.bme.hu
    ServerName moodle.eet.bme.hu
    ServerAlias moodle
    DocumentRoot /var/www/html
    ErrorLog /var/log/apache2/moodle-error_log
    CustomLog /var/log/apache2/moodle-access_log combined
    HostnameLookups Off
    UseCanonicalName Off
    ServerSignature On
    Include /etc/apache2/conf.d/*.conf
    <Directory "/var/www/html">
       Options Indexes FollowSymLinks MultiViews
       AllowOverride All
       Order allow,deny
       Allow from all
    </Directory>
</VirtualHost>
```

/etc/apache2/vhosts.d/infoc.conf

```
<VirtualHost *:80>
    ServerAdmin czirkos@eet.bme.hu
    ServerName infoc.eet.bme.hu
    ServerAlias infoc
    DocumentRoot /srv/www/vhosts/infoc/
    ErrorLog /var/log/apache2/infoc-error_log
    CustomLog /var/log/apache2/infoc-access_log combined
    HostnameLookups Off
    UseCanonicalName Off
    ServerSignature On
    Include /etc/apache2/conf.d/*.conf
    <Directory "/srv/www/vhosts/infoc">
       Options Indexes FollowSymLinks
       AllowOverride None
       Order allow,deny
       Allow from all
    </Directory>
</VirtualHost>
```

/etc/apache2/vhosts.d/mahara.conf

```
<VirtualHost *:80>
    ServerAdmin timar@eet.bme.hu
    ServerName mahara.eet.bme.hu
    ServerAlias mahara
    DocumentRoot /srv/www/vhosts/mahara/mahara_html
    ErrorLog /var/log/apache2/mahara-error_log
    CustomLog /var/log/apache2/mahara-access_log combined
    HostnameLookups Off
    UseCanonicalName Off
```

```
        ServerSignature On
        Include /etc/apache2/conf.d/*.conf
        <Directory "/srv/www/vhosts/mahara/mahara_html">
           Options Indexes FollowSymLinks
           AllowOverride None
           Order allow,deny
           Allow from all
        </Directory>
    </VirtualHost>
```

/etc/apache2/vhosts.d/tehetseg.conf

```
    <VirtualHost *:80>
        ServerAdmin timar@eet.bme.hu
        ServerName tehetseg.eet.bme.hu
        ServerAlias tehetseg
        DocumentRoot /srv/www/vhosts/tehetseg/tehetseg_html
        ErrorLog /var/log/apache2/tehetseg-error_log
        CustomLog /var/log/apache2/tehetseg-access_log combined
        HostnameLookups Off
        UseCanonicalName Off
        ServerSignature On
        Include /etc/apache2/conf.d/*.conf
        <Directory "/srv/www/vhosts/tehetseg/tehetseg_html">
           Options Indexes FollowSymLinks
           AllowOverride None
           Order allow,deny
           Allow from all
        </Directory>
    </VirtualHost>
```

III.5.5 MySQL szerver konfigurációja

Alapkonfigurációval működik.

III.5.5.1 Felhasználók

Minden alkalmazás saját felhasználóval kapcsolódik a számára dedikált adatbázishoz. Más adatbázisokhoz nem fér hozzá a felhasználó.

III.6. mail.eet.bme.hu

Ezen a kiszolgálón futnak a levelezéssel kapcsolatos alkalmazások, a webmail kivételével. A virtuális gép a dom0 system/mail kötén van.

III.6.1 Hálózati beállítások

ip cím	interface
152.66.72.27	eth1

III.6.1.1 Default router

/etc/sysconfig/network/routes

```
    default 152.66.72.30 - -
```

III.6.1.2 DNS konfiguráció

```
search eet.bme.hu
nameserver 152.66.72.29
nameserver 152.66.115.1
nameserver 152.66.116.1
```

III.6.2 Diszk konfiguráció

III.6.2.1 Partíciók

```
Disk /dev/xvda: 343.6 GB, 343597383680 bytes
    Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *           1          25      200781   83  Linux
/dev/xvda2              26       41773   335340810   8e  Linux LVM
```

III.6.2.2 LVM konfig

III.6.2.2.1 Volume group

```
VG     #PV #LV #SN Attr   VSize   VFree
system   1   4   0 wz--n- 319.80G 10.80G
```

III.6.2.2.2 Logikai kötetek

```
LV   VG     Attr   LSize
imap system -wi-ao 300.00G
root system -wi-ao   4.00G
swap system -wi-ao   1.00G
var  system -wi-ao   4.00G
```

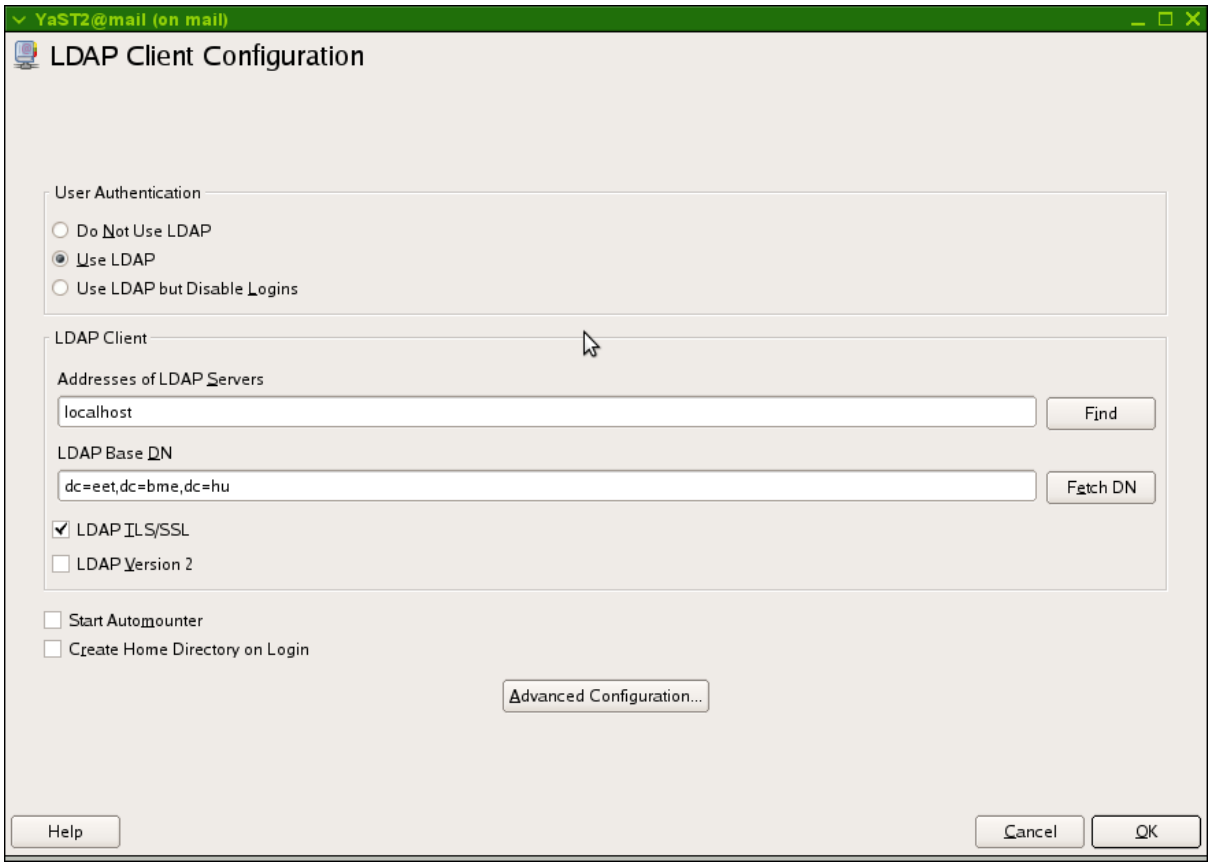
III.6.2.3 fstab

```
/dev/system/swap     swap               swap     defaults               0 0
/dev/system/root     /                  ext3     noatime,acl,user_xattr 1 1
/dev/xvda1           /boot              ext2     noatime,noacl          1 2
/dev/system/var      /var               ext3     noatime,acl,user_xattr 1 2
proc                 /proc              proc     defaults               0 0
sysfs                /sys               sysfs    noauto                 0 0
debugfs              /sys/kernel/debug  debugfs  noauto                 0 0
devpts               /dev/pts           devpts   mode=0620,gid=5        0 0
/dev/mapper/system-imap /var/spool/imap xfs      noatime                2 2
```

III.6.3 Szolgáltatások listája

szolgáltatás	alkalmazás neve
SMTP szerver	postfix
IMAP szerver	cyrus
Spam szűrő	Spamassassin, Amavis

III.6.4 User forrás



III.6.5 Postfix SMTP szerver konfigurációja

/etc/sysconfig/postfix

```
POSTFIX_RELAYHOST=""
POSTFIX_MASQUERADE_DOMAIN=""
POSTFIX_LOCALDOMAINS="eet.bme.hu, mail.eet.bme.hu, www.eet.bme.hu, moodle.eet.bme.hu"
POSTFIX_NULLCLIENT="no"
POSTFIX_DIALUP="no"
POSTFIX_NODNS="no"
POSTFIX_CHROOT="no"
POSTFIX_UPDATE_CHROOT_JAIL="no"
POSTFIX_LAPTOP="no"
POSTFIX_UPDATE_MAPS="yes"
POSTFIX_MAP_LIST="virtual transport access canonical sender_canonical relocated sasl_passwd:600
relay_ccerts"
POSTFIX_RBL_HOSTS=""
POSTFIX_BASIC_SPAM_PREVENTION="off"
POSTFIX_MDA="local"
POSTFIX_SMTP_AUTH_SERVER="no"
POSTFIX_SMTP_AUTH="no"
POSTFIX_SMTP_AUTH_OPTIONS=""
POSTFIX_SMTP_TLS_SERVER="no"
POSTFIX_SMTP_TLS_SERVER_LEGACY_SUPPORT="no"
POSTFIX_SMTP_TLS_CLIENT="no"
POSTFIX_SSL_PATH="/etc/postfix/ssl"
```

```
POSTFIX_TLS_CAFILE="cacert.pem"
POSTFIX_TLS_CERTFILE="certs/postfixcert.pem"
POSTFIX_TLS_KEYFILE="certs/postfixkey.pem"
POSTFIX_SSL_COUNTRY="XX"
POSTFIX_SSL_STATE="Some state"
POSTFIX_SSL_LOCALITY="Some locality"
POSTFIX_SSL_ORGANIZATION="Some Organization"
POSTFIX_SSL_ORGANIZATIONAL_UNIT="Some Organizational Unit"
POSTFIX_SSL_COMMON_NAME="A common name"
POSTFIX_SSL_EMAIL_ADDRESS="postmaster"
POSTFIX_ADD_MAILBOX_SIZE_LIMIT="0"
POSTFIX_ADD_MESSAGE_SIZE_LIMIT="10240000"
POSTFIX_REGISTER_SLP="yes"
POSTFIX_ADD_MYNETWORKS_STYLE="subnet"
POSTFIX_SYSTEM_MAIL_SENDER=""
```

/etc/postfix/main.cf - kivonatos

```
myhostname = mail.eet.bme.hu
mydestination = $mydomain, $myhostname, www.eet.bme.hu, moodle.eet.bme.hu,
localhost.$mydomain, localhost
defer_transports =
mynetworks = 152.66.72.0/24, 127.0.0.0/8
mailbox_transport = cyrus
smtpd_recipient_restrictions =
permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination,reject
_rbl_client b.barracudacentral.org, reject_rbl_client bl.spamcop.net, r
eject_rbl_client zen.spamhaus.org
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = yes
smtp_enforce_tls = no
smtpd_tls_security_level = may
smtpd_tls_auth_only = yes
smtp_use_tls = no
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/cyrus/postfix_crt.pem
smtpd_tls_key_file = /etc/cyrus/postfix_key.pem
alias_maps = hash:/etc/aliases
mailbox_size_limit = 0
message_size_limit = 67108864
content_filter = smtp-amavis:[127.0.0.1]:10024
```

III.6.6 Cyrus IMAP szerver konfigurációja

/etc/imapd.conf

```
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
sievedir: /var/lib/sieve
admins: cyrus
allowanonymouslogin: no
autocreatequota: 10000
reject8bit: no
quotawarn: 90
timeout: 30
poptimeout: 10
dracinterval: 0
drachost: localhost
sasl_pwcheck_method: saslauthd
```

```
lmtp_overquota_perm_failure: no
lmtp_downcase_rcpt: yes
allowplaintext: 1
altnamespace: 1
tls_cert_file: /etc/ssl/servercerts/servercert.pem
tls_key_file: /etc/ssl/servercerts/serverkey.pem
tls_ca_file: /etc/ssl/certs/YaST-CA.pem
```

/etc/pam.d/imap

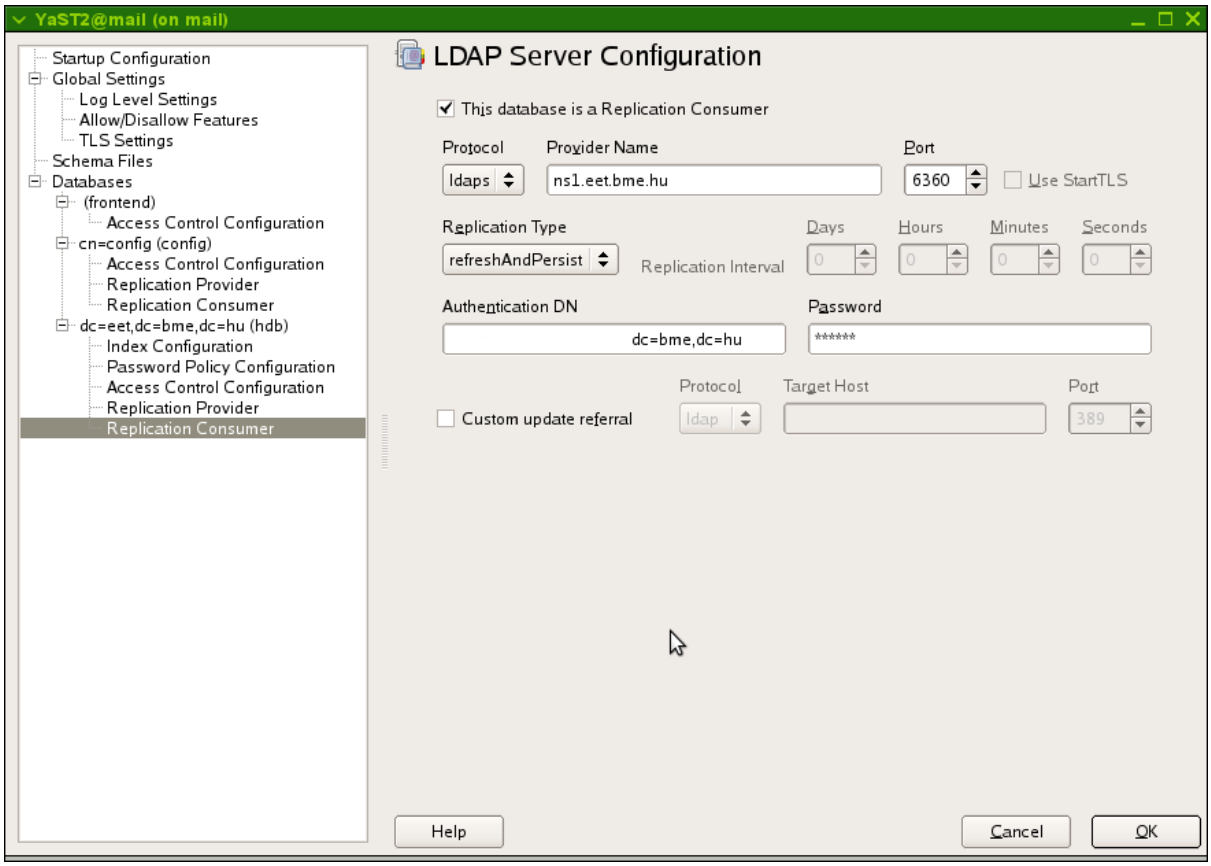
```
#%PAM-1.0
auth     include        common-auth
auth     [user_unknown=ignore success=ok ignore=ignore auth_err=die
default=bad]        pam_securetty.so
account  include        common-account
password include        common-password
session  required       pam_loginuid.so
session  include        common-session
```

III.6.7 OpenLDAP replika

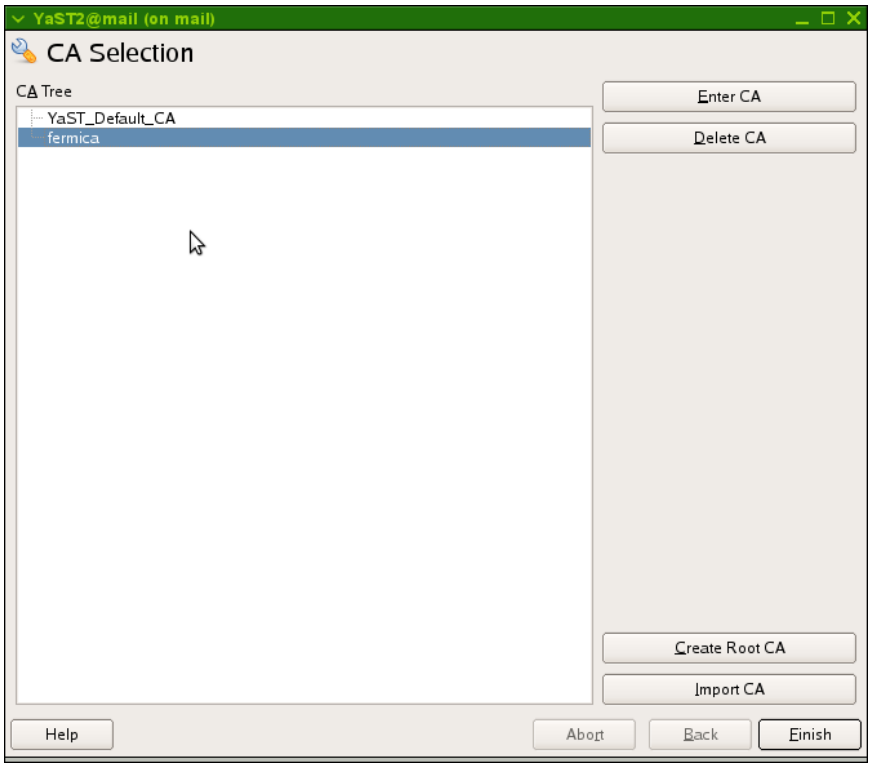
Az OpenLDAP replikáció az ns1.eet.bme.hu kiszolgálón át port forwarding használatával a fermi.eet.bme.hu OpenLDAP szerverről szinkronizál.

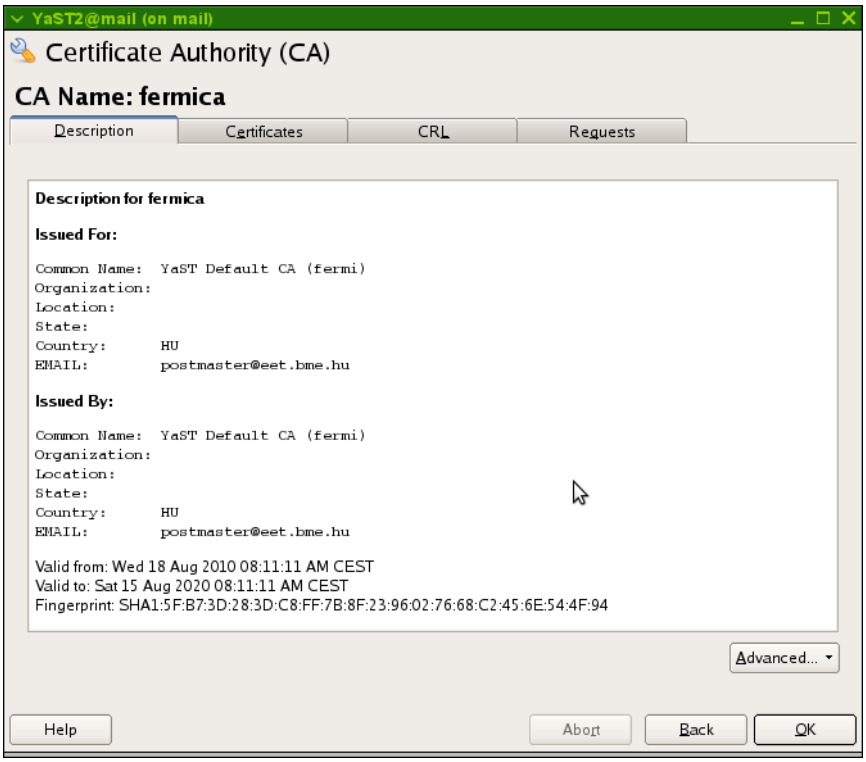
LDAP master ldaps://ns1.eet.bme.hu:6360/

A replikáció konfigurációja a Yast2 ldap-server moduljában készült.



A OpenLDAP replikációhoz szükséges a fermi.eet.bme.hu CA importálása a rendszeren. Az alábbi képek mutatják be a vonatkozó felületet.





III.7. fermi.eet.bme.hu

A fermi a védett oldali feladatokat ellátó kiszolgáló. Önálló fizikai kiszolgáló.

III.7.1 Hálózati beállítások

ip cím	interface
152.66.72.28	eth0

III.7.1.1 Default router

/etc/sysconfig/network/routes

```
default x.x.x.x - -
```

III.7.1.2 DNS konfiguráció

```
search eet.bme.hu
nameserver x.x.x.x
nameserver 152.66.115.1
nameserver 152.66.116.1
```

III.7.2 Diszk konfiguráció

Két darab SATA diszk van a gépben, ezekre építünk egy szoftver RAID tömböt.

III.7.2.1 Partíciók

```
Disk /dev/sda: 250.1 GB, 250059350016 bytes
   Device Boot      Start   End      Blocks   Id  System
/dev/sda1   *           1   25      200781   fd  Linux raid autodetect
/dev/sda2              26   30401   243995220   fd  Linux raid autodetect


Disk /dev/sdb: 250.1 GB, 250059350016 bytes
   Device Boot      Start   End      Blocks   Id  System
/dev/sdb1   *           1   25      200781   fd  Linux raid autodetect
/dev/sdb2              26   30401   243995220   fd  Linux raid autodetect
```

III.7.2.2 Szoftver RAID

/etc/mdadm.conf

```
DEVICE containers partitions
ARRAY /dev/md0 UUID=495ae6f0:4276dec6:86825774:07810f15
ARRAY /dev/md1 UUID=cdd82591:3be83d39:7dad4e3e:97ee5ed7
```

Az md0 tömb az sda1 sdb1 partíciókra épül, az md1 tömb az sda2 sdb2 eszközökre.

III.7.2.3 LVM konfig

III.7.2.3.1 Volume group

```
  VG     #PV #LV #SN Attr   VSize   VFree
```

```
  system   1   4   0 wz--n- 232.69G 14.69G
```

III.7.2.3.2 Logikai kötetek

```
  LV   VG     Attr   LSize
  home system -wi-ao 200.00G
  root system -wi-ao   8.00G
  swap system -wi-ao   2.00G
  var  system -wi-ao   8.00G
```

III.7.2.4 fstab

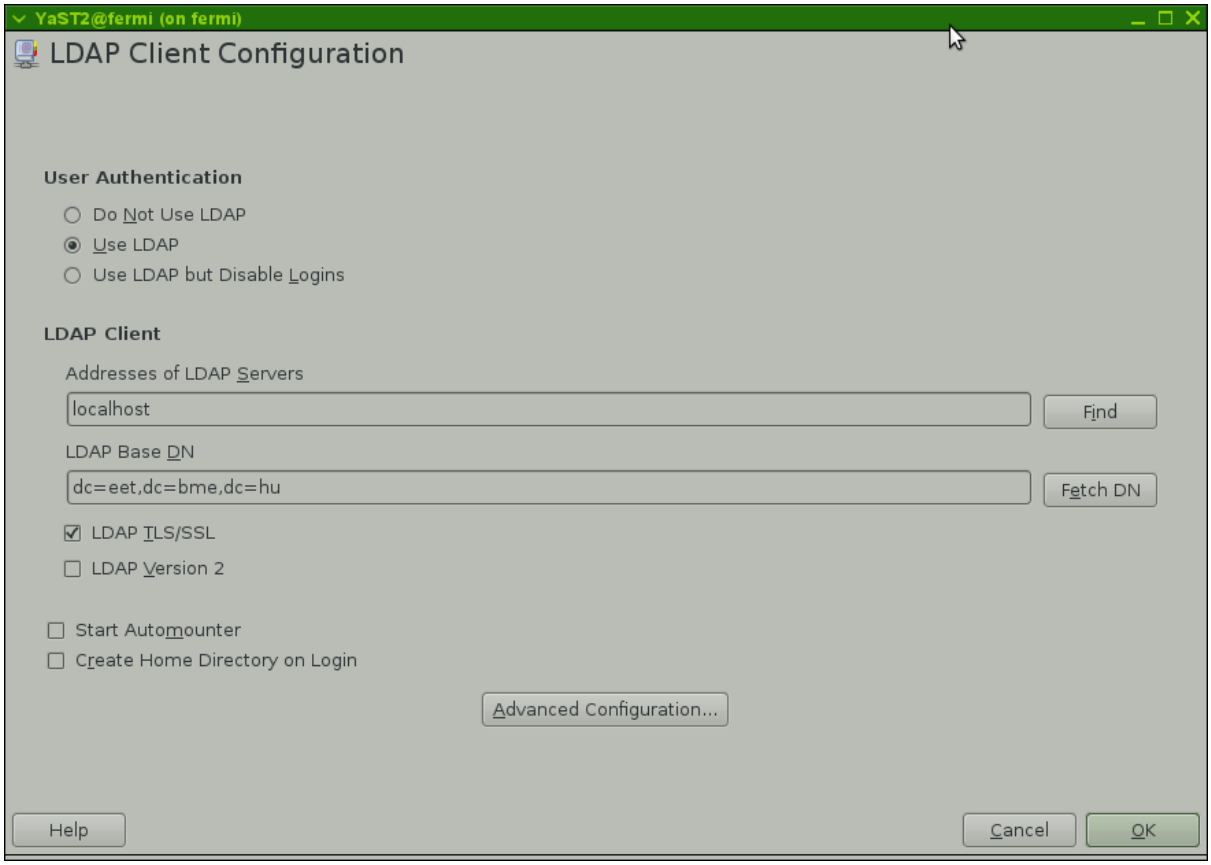
```
/dev/system/swap     swap                swap       defaults              0 0
/dev/system/root     /                   ext3       noatime,acl,user_xattr 1 1
UUID=f92ef192-5102-44cc-8634-07f9bb51df35 /boot   ext2       noatime,noacl         1 2
/dev/system/var      /var                ext3       noatime,acl,user_xattr 1 2
proc                 /proc               proc       defaults              0 0
sysfs                /sys                sysfs      noauto                0 0
debugfs              /sys/kernel/debug   debugfs    noauto                0 0
usbfs                /proc/bus/usb       usbfs      noauto                0 0
devpts               /dev/pts            devpts     mode=0620,gid=5       0 0
/dev/system/home    /home  xfs    defaults,noatime    0 0
```

III.7.3 Szolgáltatások listája

szolgáltatás	alkalmazás neve
LDAP címtár	OpenLDAP
CIFS kiszolgáló	Samba
DHCP szerver	ISC DHCPD
Felügyelet	Nagios
HTTP szerver	Apache

III.7.4 User forrás

A felhasználók a helyben futó címtárban tárolódnak.



III.7.5 Samba

A Samba végzi a CIFS kiszolgálást. A Samba szervert szintén integráltuk a címtárral.

/etc/samba/smb.conf

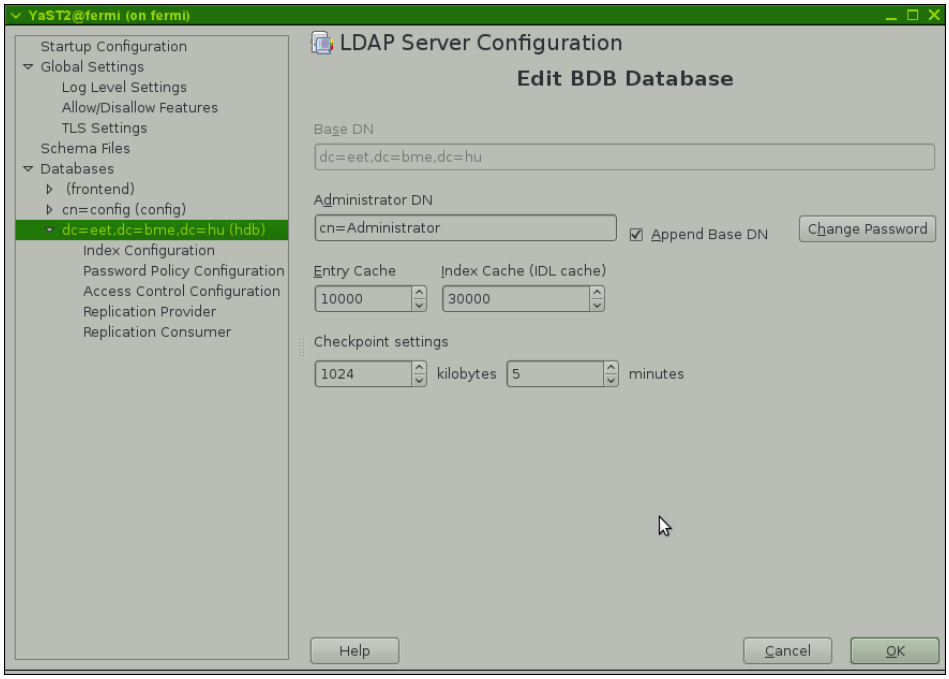
```
[global]
        add machine script = /sbin/yast /usr/share/YaST2/data/add_machine.ycp %m$
        server string = Fermi
        comment = Fermi
        domain logons = Yes
        domain master = Yes
        idmap backend = ldap:ldap://localhost
        ldap admin dn = cn=Administrator,dc=eet,dc=bme,dc=hu
        ldap delete dn = No
        ldap group suffix = ou=group
        ldap idmap suffix = ou=Idmap
        ldap machine suffix = ou=Machines
        ldap passwd sync = Yes
        ldap replication sleep = 1000
        ldap ssl = Start_tls
        ldap suffix = dc=eet,dc=bme,dc=hu
        ldap timeout = 5
        ldap user suffix = ou=people
```

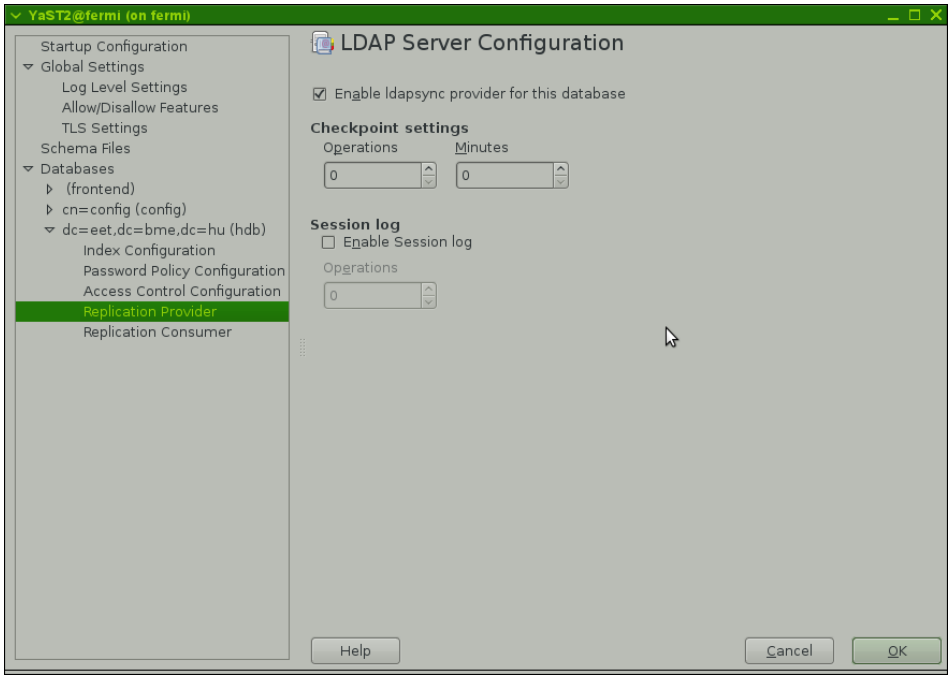
```
        local master = Yes
        os level = 65
        passdb backend = ldapsam:ldap://localhost
        preferred master = Yes
        security = user
        wins support = No
        workgroup = EET
        netbios name = fermi
        wins server =
       logon path = \\%L\profiles\%U
       logon home = \\%L\%U\.9xprofile
[netlogon]
        comment = Network Logon Service
        path = /home/samba/logon
        write list = root
[profiles]
       comment = Network Profiles Service
       path = /home/samba/profile
       read only = No
       browsable = no
       writeable = yes
       store dos attributes = Yes
       create mask = 0600
       directory mask = 0700
[users]
        comment = Users
        inherit acls = Yes
        path = /home
        read only = No
        veto files = /aquota.user/groups/shares/
[homes]
        admin users = admin
        browsable = no
        writeable = yes
[www]
        comment = Sajat weboldal
        path = /srv/people/%u
        browseable = yes
        read only = no
[dosappl]
  path = /home/samba/dosappl
  writeable = yes
[install]
  path = /home/samba/install
  writeable = yes
[patent]
  path = /home/samba/patent
  writeable = yes
  create mode = 0770
  directory mode = 0770
[Hidralon]
  path = /home/samba/Hidralon
  writeable = yes
  create mode = 0770
  directory mode = 0770
[SE2A]
```

```
  path = /home/samba/SE2A
  writeable = yes
  create mode = 0770
  directory mode = 0770
[JEMSHIP3D]
  path = /home/samba/JEMSHIP3D
  writeable = yes
  create mode = 0770
  directory mode = 0770
[KOZLED]
  path = /home/samba/KOZLED
  writeable = yes
  create mode = 0770
  directory mode = 0770
[F2L]
  path = /home/samba/F2L
  writeable = yes
  create mode = 0770
  directory mode = 0770
[NanoPack]
  path = /home/samba/NanoPack
  writeable = yes
  create mode = 0770
  directory mode = 0770
[PVMET]
  path = /home/samba/PVMET
  writeable = yes
  create mode = 0770
  directory mode = 0770
[BelAmi2]
  path = /home/samba/BelAmi2
  writeable = yes
  create mode = 0770
  directory mode = 0770
[ambient]
  path = /home/samba/ambient
  writeable = yes
  create mode = 0770
  directory mode = 0770
[LOGITHERM]
  path = /home/samba/LOGITHERM
  writeable = yes
  create mode = 0770
  directory mode = 0770
[vegzos]
  path = /home/samba/vegzos
  writeable = yes
```

III.7.6 OpenLDAP

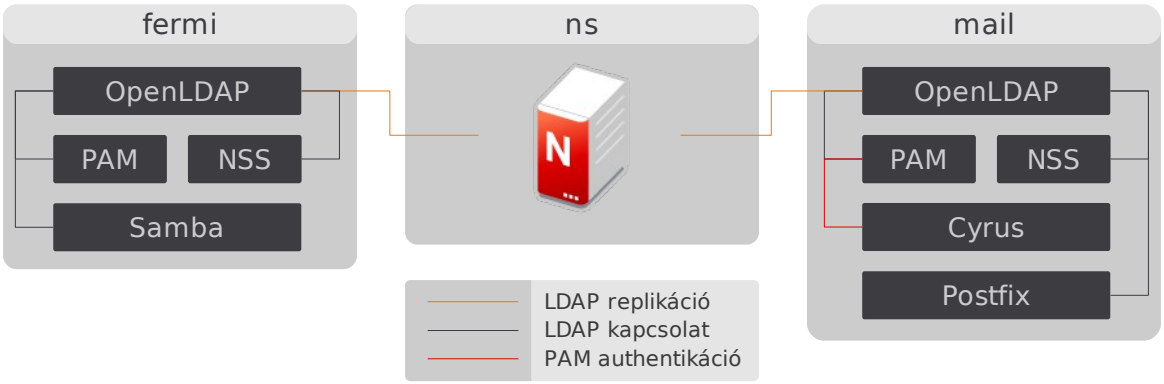
A helyi címtár OpenLDAP-ra épül. Az alkalmazás kezeléséhez a YaST-ban megtalálható minden szükséges eszköz.





III.7.6.1 LDAP architektúra

A lenti ábra bemutatja az LDAP-ot használó alkalmazások és a címtár viszonyát és kapcsolatait.



III.7.7 DHCPD

/etc/dhcpd.conf

```
option domain-name "eet.bme.hu";
option domain-name-servers x.x.x.x;
option routers x.x.x.x;
option ntp-servers time.bme.hu;
ddns-update-style none;
default-lease-time 86400;
```

III.7.8 Nagios

A nagios konfigurációja a /etc/nagios könyvtárban van. A konfiguráció alapértelmezés szerint maradt, kivéve a külön említett esetekben.

A Nagios mellé telepítettünk egy **PNP4Nagios** nevű csomagot, amivel trend jellegű információkat tud a monitoring rendszer gyűjteni. A csomag a dokumentációja szerinti konfigurációval fut. A szolgáltatás kimenete a Nagios webes felületével integrált.

cgi.cfg

```
authorized_for_system_information=*
authorized_for_configuration_information=*
authorized_for_system_commands=*
authorized_for_all_services=*
authorized_for_all_hosts=*
authorized_for_all_service_commands=*
authorized_for_all_host_commands=*
```

A nagiosban használt parancsok és template-ek a /etc/nagios/objects könyvtárban vannak.

commands.cfg

```
#NRPE
define command{
        command_name    nrpe_ck_swap
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_swap
}
define command{
        command_name    nrpe_ck_disk
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_disk
}
```

```
define command{
        command_name    nrpe_ck_disk_fermi
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_disk_fermi
}
define command{
        command_name    nrpe_ck_loadavg
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_loadavg
}
define command{
        command_name    nrpe_ck_memory
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_memory
}
define command{
        command_name    nrpe_ck_postfix_q
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_postfix_q
}
define command{
        command_name    nrpe_ck_proc_ovpn
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_ovpn
}
define command{
        command_name    nrpe_ck_proc_amavis
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_amavis
}
define command{
        command_name    nrpe_ck_proc_saslauthd
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_saslauthd
} define command{
        command_name    nrpe_ck_proc_vb
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_vb
}
# PNP4NAGIOS
define command {
    command_name    process-service-perfdata
    command_line    $USER1$/process_perfdata.pl
 }

define command {
    command_name    process-host-perfdata
    command_line    $USER1$/process_perfdata.pl
 }
```

templates.cfg

A kiemelt rész minden service template-ben azonos, csak az elsőnél szerepel a dokumentációban.

```
define service{
        name                            ssh-service
        use                             generic-service
        check_command                   check_ssh!xxxx
        max_check_attempts              4
        normal_check_interval           5
        retry_check_interval            1
        register                        0
        }

define service{
        name                            http-service
```

```
        use                             generic-service
        check_command                   check_http
        }

define service{
        name                            https-service
        use                             generic-service
        check_command                   check_https
        }

define service{
        name                            smtp-service
        use                             generic-service
        check_command                   check_smtp
        }
define service{
        name                            imap-service
        use                             generic-service
        check_command                   check_imap
        }

define service{
        name                            imaps-service
        use                             generic-service
        check_command                   check_imaps
        }

define service{
        name                            dns-service
        use                             generic-service
        check_command                   check_dns!eet.bme.hu
        }

define service{
        name            swap
        check_command    nrpe_ck_swap
        use                             generic-service
}
define service{
        name            disk
        check_command    nrpe_ck_disk
        use                             generic-service
}
define service{
        name            fermi_disk
        check_command    nrpe_ck_disk_fermi
        use                             generic-service
}
define service{
        name            loadavg
        check_command    nrpe_ck_loadavg
        use                             generic-service
}
define service{
        name            memory
        check_command    nrpe_ck_memory
```

```
        use                             generic-service
}
define service{
        name            mailq
        check_command    nrpe_ck_postfix_q
        use                             generic-service
}
define service{
        name            proc_ovpn
        check_command    nrpe_ck_proc_ovpn
        use                             generic-service
}
define service{
        name            proc_amavis
        check_command    nrpe_ck_proc_amavis
        use                             generic-service
}
define service{
        name            proc_sasl
        check_command    nrpe_ck_proc_saslauthd
        use                             generic-service
}
```

A hostok konfigurációja a /etc/nagios/servers könyvtárban található.

00hostgroups.cfg

```
define hostgroup{
        hostgroup_name  linux-servers
        alias           Linux Servers
        members         mail,fermi,ns,edu,www,xen
        }
```

linux-servers.cfg

```
define service{
        use                             swap
        hostgroup_name                  linux-servers
        service_description             Swap
        }
define service{
        use                             memory
        hostgroup_name                  linux-servers
        service_description             RAM
        }
define service{
        use                             loadavg
        hostgroup_name                  linux-servers
        service_description             Load average
        }
define service{
        use                             mailq
        hostgroup_name                  linux-servers
        service_description             Mailq length
        }
define service{
        use                             disk
        hostgroup_name                  linux-servers
        service_description             Disk space
```

```
        }
```

edu.cfg

```
define host{
        use                     linux-server
        host_name               edu
        alias                   edu
        address                 152.66.72.28
        }
define service{
        use                             generic-service
        host_name                       edu
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             ssh-service
        host_name                       edu
        service_description             SSH
        }
define service{
        use                             http-service
        host_name                       edu
        service_description             HTTP
        }
```

fermi.cfg

```
define host{
        use                     linux-server
        host_name               fermi
        alias                   fermi
        address                 x.x.x.x
        }
define service{
        use                             generic-service
        host_name                       fermi
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             ssh-service
        host_name                       fermi
        service_description             SSH
        }
define service{
        use                             https-service
        host_name                       fermi
        service_description             HTTPS
        }
define service{
        use                             generic-service
        host_name                       fermi
        service_description             LDAP
        check_command                   check_ldap!dc=eet,dc=bme,dc=hu
        }
```

```
define service{
        use                             generic-service
        host_name                       fermi
        service_description             LDAPS
        check_command                     check_ldaps!dc=eet,dc=bme,dc=hu
        }
```

mail.cfg

```
define host{
        use                     linux-server
        host_name               mail
        alias                   mail
        address                 152.66.72.27
        }
define service{
        use                             generic-service
        host_name                       mail
        service_description             PING
        check_command                     check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             ssh-service
        host_name                       mail
        service_description             SSH
        }
define service{
        use                             smtp-service
        host_name                       mail
        service_description             SMTP
        }
define service{
        use                             generic-service
        host_name                       mail
        service_description             LDAP
        check_command                     check_ldap!dc=eet,dc=bme,dc=hu
        }
define service{
        use                             imap-service
        host_name                       mail
        service_description             IMAP
        }
define service{
        use                             imaps-service
        host_name                       mail
        service_description             IMAPS
        }
```

ns.cfg

```
define host{
        use                     linux-server
        host_name               ns
        alias                   ns
        address                 152.66.72.29
        }
define service{
        use                             generic-service
        host_name                       ns
```

```
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             ssh-service
        host_name                       ns
        service_description             SSH
        }
define service{
        use                             dns-service
        host_name                       ns
        service_description             DNS
        }
```

www.cfg

```
define host{
        use                     linux-server
        host_name               www
        alias                   www
        address                 152.66.72.26
        }
define service{
        use                             generic-service
        host_name                       www
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             ssh-service
        host_name                       www
        service_description             SSH
        }
define service{
        use                             http-service
        host_name                       www
        service_description             HTTP
        }
```

xen.cfg

```
define host{
        use                     linux-server
        host_name               xen
        alias                   xen
        address                 x.x.x.x
        }
define service{
        use                             generic-service
        host_name                       xen
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             ssh-service
        host_name                       xen
        service_description             SSH
        }
```

III.7.9 NRPE

A Nagios ellenőrzések egy részét közvetlen módon, szolgáltatás ellenében végezzük (HTTP, IMAP, SMTP, DNS), míg másokat ügynökön keresztül. Az ügynök neve NRPE. A konfigurációja az alábbi, minden gépen amit ellenőrzés alá vonunk (a forrás IP-t a fermi látható IP-jére kell állítani).

/etc/nagios/nrpe.cfg

```
log_facility=daemon
pid_file=/var/run/nrpe/nrpe.pid
server_port=5666
nrpe_user=nagios
nrpe_group=nagios
allowed_hosts=127.0.0.1,x.x.x.x
dont_blame_nrpe=0
debug=0
command_timeout=60
connection_timeout=300
include_dir=/etc/nagios/nrpe
```

/etc/nagios/nrpe/commands.cfg

```
command[check_disk_fermi]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -x /srv/people -x
/dev/shm -x /dev
command[check_disk]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -x /dev/shm -x /dev
command[check_loadavg]=/usr/lib/nagios/plugins/check_load -r -w 5,7,7 -c 7,9,10
command[check_memory]=/usr/lib/nagios/plugins/check_memory -p -w 128 -c 64
command[check_swap]=/usr/lib/nagios/plugins/check_swap -w 95 -c 90
command[check_postfix_q]=/usr/lib/nagios/plugins/check_mailq -w 10 -c 20 -M postfix
command[check_proc_ovpn]=/usr/lib/nagios/plugins/check_procs -C openvpn -c 1:
command[check_proc_amavis]=/usr/lib/nagios/plugins/check_procs -C amavisd -c 1:
command[check_proc_saslauthd]=/usr/lib/nagios/plugins/check_procs -C saslauthd -c 1:
command[check_proc_vb]=/usr/lib/nagios/plugins/check_procs -C vbscand -c 1:
```

III.7.10 Apache

Az apache a fermi szerveren csak a Nagios kiszolgálására lett telepítve. Az Apache a címtárból authentikálja a felhasználókat.

/etc/apache2/conf.d/nagios.conf

```
ScriptAlias /nagios/cgi-bin "/usr/lib/nagios/cgi"
<Directory "/usr/lib/nagios/cgi">
   SSLRequireSSL
   Options ExecCGI
   AllowOverride None
   Order allow,deny
   Allow from all
   AuthType Basic
   AuthBasicProvider ldap
   AuthName "Nagios"
   AuthLDAPURL ldap://localhost:389/ou=staff,ou=people,dc=eet,dc=bme,dc=hu?
uid?sub
   AuthzLDAPAuthoritative off
   Require valid-user
</Directory>
Alias /nagios "/usr/share/nagios"
<Directory "/usr/share/nagios">
   SSLRequireSSL
   Options None
```

```
   AllowOverride None
   Order allow,deny
   Allow from all
   AuthType Basic
   AuthBasicProvider ldap
   AuthName "Nagios"
   AuthLDAPURL ldap://localhost:389/ou=staff,ou=people,dc=eet,dc=bme,dc=hu?
uid?sub
   AuthzLDAPAuthoritative off
   Require valid-user
</Directory>
```

/etc/apache2/conf.d/nagios-pnp.conf

```
<IfDefine PNP4NAGIOS>
 Alias /pnp  /usr/share/pnp
 <Directory /usr/share/pnp>
    Options None
    order allow,deny
    allow from all
   AuthType Basic
   AuthBasicProvider ldap
   AuthName "Nagios"
   AuthLDAPURL ldap://localhost:389/ou=staff,ou=people,dc=eet,dc=bme,dc=hu?
uid?sub
   AuthzLDAPAuthoritative off
    php_admin_flag safe_mode off
 </Directory>
 <IfDefine SSL>
  <IfDefine !NOSSL>
   <IfModule mod_ssl.c>
    SSLOptions +StdEnvVars
    <Directory /usr/share/pnp>
      Options None
      SSLRequireSSL
      order allow,deny
      allow from all
   AuthType Basic
   AuthBasicProvider ldap
   AuthName "Nagios"
   AuthLDAPURL ldap://localhost:389/ou=staff,ou=people,dc=eet,dc=bme,dc=hu?
uid?sub
   AuthzLDAPAuthoritative off
      php_admin_flag safe_mode off
    </Directory>
   </IfModule>
  </IfDefine>
 </IfDefine>
</IfDefine>
```