Megvalósulási dokumentáció

www.npsh.hu

SUSE Labor kialakítása

a Deák téri Evangélikus Gimnázium
részére

Novell

Védjegyek és Jogi nyilatkozat

A jelen dokumentum OpenOffice.org 3 Novell Edition programmal készült.

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

Tartalomjegyzék

I. Architektúra 4
I.1. Hálózati architektúra 4
I.2. Kiszolgálók 4
I.2.1 Tanar-server 4
I.2.2 diak-server 5
II. Szolgáltatások 5
II.1. DHCP szolgáltatás 5
II.2. Névfeloldás 6
II.3. Hitelesítési szolgáltatások 7
II.4. SAMBA Domain vezérlő 8
II.5. Internet átjáró 10
II.6. SQUID webgyorsítótár 10
II.7. Időszinkronizáció 12
II.8. Automatikus telepítés 12

I. Architektúra

A kialakított környezet két kiszolgálót és számos asztali számítógépet foglal magában. A munkaállomások között, felhasználásuk szerint kettőt különböztetünk meg, a tanári és a diák munkaállomásokat. A tanári munkaállomások többnyire Windows operációs rendszert futtatnak, melyek számára a *tanar-server* kiszolgálón futó Samba Primary Domain Controller alapvető domain vezérlő funkciókat biztosít, pl központosított hitelesítés, roaming profile. A diákok munkaállomásainak kiszolgálását a *diak-server* végzi.

Bizonyos szolgáltatások, melyeket elegendő egy kiszolgálón futtatni (pl.: DNS, DHCP, internet átjáró), a *tanar-server* kiszolgálón futnak.

I.1. Hálózati architektúra

A belső hálózaton nincsenek elkülönítve a kiszolgálók és a munkaállomások egymástól, minden eszköz egy IP címtartományt használ.

A tanar-server kétlábú, átjáróként, DNS és DHCP kiszolgálóként üzemel. A hálózatra kötött munkaállomás a DHCP szolgáltatás segítségével automatikusan megkapja az IP címet és a hozzá tartozó beállításokat.

A diak-server egylábú, belső szolgáltatásokat nyújt csak. A legfontosabb szolgáltatások a hitelesítés, az NFS fájlmegosztás és a webgyorsítótár.

A tanári munkaállomások fizikai hálózati cím (MAC cím) alapján közvetlenül, átjárón keresztül férnek hozzá az internethez.

A diákok munkaállomásai a diak-server kiszolgálón futó SQUID webgyorsítótáron keresztül, LDAP hitelesítés után férhetnek hozzá az internetes weboldalakhoz.

I.2. Kiszolgálók

I.2.1 Tanar-server

A kiszolgáló egy Fujitsu Primergy TX100 S1 típusú eszköz, 2x500GB merevlemezzel és 4GB memóriával. A merevlemezek RAID1 tömböt alkotnak.

A kiszolgálóban található szoftveres raid-vezérlőt támogatja a SUSE Linux Enterprise Server, de a telepítés elején a boot kötet beállításainál az uuid alapú csatolást kell beállítani.

A fájlrendszereket LVM2 köteteken hoztuk létre, a következő listában összefoglalva a kötetek nevét és méretét:

- home 8.00G
- install 8.00G
- root 4.00G
- swap 2.00G
- var 2.00G

AZ LVM2 köteteken a swap-et kivéve mindenhol XFS fájlrendszert használunk, így menet közben is bármikor megnövelhető bármelyik kötet az lvextend és xfs_growfs parancsokkal.

A diak-server telepítésének idején az install köteten elhelyeztük a telepítési forrást és NFS szolgáltatást használva telepítettük a diak-server kiszolgálót.

A kiszolgálónak két hálózati interfésze van, egy belső és egy külső. A külső hálózati interfészén keresztül közvetlenül hozzáfér az internethez, melyet a belső munkaállomásokkal meg is oszt.

LDAP hitelesítési forrás fut a kiszolgálón, mely a tanárok hozzáféréseit tárolja az adatbázisban. Ezen a hitelesítési szolgáltatáson keresztül lehet hozzáférni a kiszolgálón futó Samba Domain-hez és a fájlszolgáltatáshoz.

A fontosabb futó szolgáltatások, melyeket az alap csomagválasztékhoz hozzá kellett adni telepítéskor:

- DNS
- DHCP
- internetes átjáró
- ldap címtárszolgáltatás tanároknak
- Samba PDC, fájlszolgáltatás

I.2.2 diak-server

A kiszolgáló típusa megegyezik a tanar-server kiszolgálóéval. A lemezek száma,mérete, konfigurációja és a memória mennyisége is egyezik a két kiszolgálóban.

Ennél a kiszolgálónál is LVM2 alapú kötetkezelőt használunk a rugalmassága miatt. A kötetek neve és méretük:

- home 300.00G
- install 8.00G
- root 5.00G
- swap 2.00G
- var 2.00G

A diak-server kiszolgáló is nyújt LDAP hitelesítési szolgáltatást, de más adatbázisból dolgozik, mint a tanar-server. Itt a diákok hozzáférési információi találhatóak, mellyel a webgyorsítótáron keresztül internetes webol-dalakat lehet megtekinteni.

A diak-server nem Samba szolgáltatást használ a fájlok megosztására, hanem NFS protokollt. A diákok munkaállomásai induláskor a /home kötetet a diak-server kiszolgálótól kapják, ezért minden diák saját állománya egy helyen, a diak-server /home kötetén található.

A diak-server kiszolgáló tartalmazza munkaállomások automatikus telepítéséhez szükséges szolgáltatásokat is. Az install köteten elérhető a SUSE Linux Enterprise Desktop 11 SP1 telepítőkészlete, valamint az érettségi linux csomagválasztéka is. Ezeket NFS megosztáson el lehet érni és az előre létrehozott AutoYAST profilt használva automatikusan lehet telepíteni egy új munkaállomást.

II. Szolgáltatások

II.1. DHCP szolgáltatás

A tanar-server felelős a hálózaton az IP címek automatikus konfigurálásáért. A DHCP beállításainak segítségével az ismert fizikai címmel (MAC cím) rendelkező munkaállomásokat más hálózati beállításokkal látjuk el, mint az ismeretlen, vagy nem definiált munkaállomásokat.

Az alapvető különbség az ismert és nem ismert gépek között az alapértelmezett átjáró beállítása, így a definiált munkaállomások korlátozások nélkül hozzáférhetnek az internetes szolgáltatásokhoz. A DHCP számára nem definiált munkaállomások csak korlátozott módon és korlátozott szolgáltatásokhoz férhetnek hozzá a webgyor-sítótáron keresztül.

A /etc/dhcpd.conf állmány tartalma:

```
ddns-update-style none;
#ismert gepeknek
group {
       option domain-name "deg.sulinet.hu";
       option domain-name-servers XX.XX.XX.XX, YY.YY.YY.YY;
       option routers XX.XX.XX.XX;
       option ntp-servers XX.XX.XX.XX;
```

```
        default-lease-time 14400;

        subnet XX.XX.XX.XX netmask 255.255.255.0 {
               range XX.XX.XX.XX YY.YY.YY.YY;
               default-lease-time 14400;
               max-lease-time 172800;
        }

        host gepnev1 {
               fixed-address AA.AA.AA.AA;
               hardware ethernet aa:aa:aa:00:00:00;
        }
        host gepnev2 {
               fixed-address BB.BB.BB.BB;
               hardware ethernet aa:aa:aa:00:00:01;
        }

}
#diakoknak
group {
         option domain-name "deg.sulinet.hu";
         option domain-name-servers XX.XX.XX.XX;
         option ntp-servers XX.XX.XX.XX;
         default-lease-time 14400;
         subnet XX.XX.XX.XX netmask 255.255.255.0 {
                 range AA.AA.AA.AA BB.BB.BB.BB;
                 default-lease-time 14400;
                 max-lease-time 172800;
         }
}
```

II.2. Névfeloldás

A tanar-server kiszolgálón futó ISC BIND (Berkeley Internet Name Domain) 9.5 szolgáltatás oldja fel a DNS neveket a belső hálózaton futó munkaállomások számára.

Az ismert hálózati munkaállomások alapértelmezett beállítás szerint három DNS névkiszolgálót használnak:

- tanar-server kiszolgálón futó DNS
- sulinet DNS kiszolgáló 1
- sulinet DNS kiszolgáló 2

A nem definiált munkaállomások csak a tanar-server kiszolgálót használják névfeloldásra.

A tanar-server kiszolgálón futó DNS szolgáltatás gyorsítótárazza és továbbítja a DNS kéréseket. Ez a /etc/named.d/forwarders.conf konfigurációs állományban van beállítva:

```
forwarders {
       AA.AA.AA.AA;
       BB.BB.BB.BB;
};
```

A szolgáltatás a deg.sulinet.hu zónát szolgálja ki. A zóna adatbázisa a /var/lib/named/master/deg.sulinet.hu állományban található:

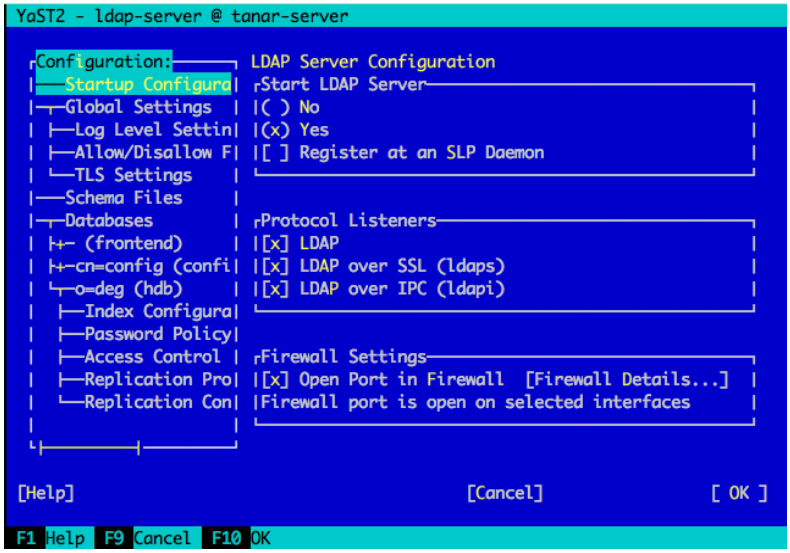
```
$TTL 2d
@            IN SOA       tanar-server.deg.sulinet.hu.     root.tanar-
server.deg.sulinet.hu. (
                          2010083001    ; serial
                          3h            ; refresh
```

```
                                1h              ; retry
                                1w              ; expiry
                                1d )            ; minimum

deg.sulinet.hu.      IN NS          tanar-server.deg.sulinet.hu.
tanar-server  IN A          AA.AA.AA.AA
diak-server   IN A          BB.BB.BB.BB
proxy         IN CNAME      diak-server
```

II.3. Hitelesítési szolgáltatások

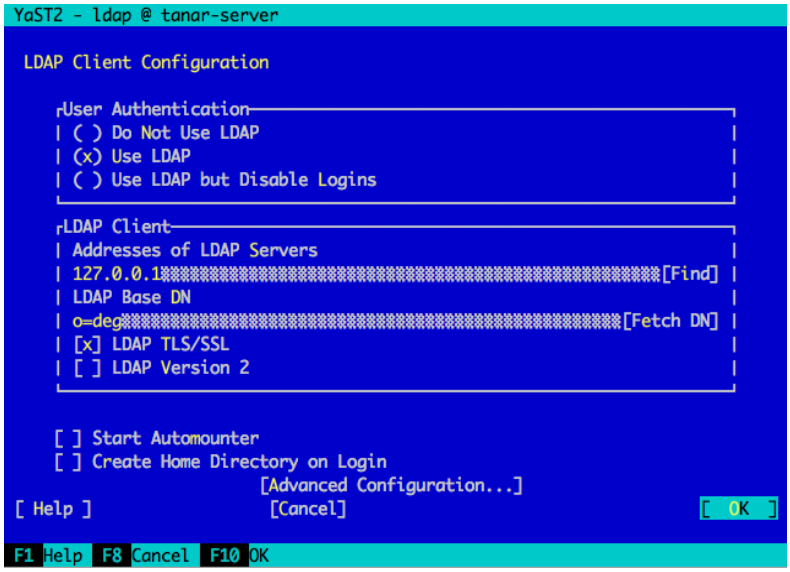
A tanar-server és a diak-server kiszolgálókon egy-egy saját adatbázis található, melyeket más szolgáltatások használnak.



1. ábra: a YaST ldap-server modulja

A szolgáltatást a SUSE Linux Enterprise Server 11 SP1 verziójában elérhető openLDAP nyújtja, melyeket a YaST2 LDAP kiszolgáló moduljával állítottunk be.

Mind a két kiszolgálón az o=deg névbázist használjuk. A felhasználók pedig az ou=people,o=deg egység alatt találhatóak.



2. ábra: a YaST ldap modulja

Mindkét adatbázis adminisztrátora a cn=administrator,o=deg felhasználó.

II.4. SAMBA Domain vezérlő

A tanar-server kiszolgálón futó Samba szolgáltatást elsődleges domén vezérlőként állítottuk be, mely így a Windows munkaállomások számára hitelesítési és fájlszolgáltatásokat nyújt.

A beállítások a /etc/samba/smb.conf állományban találhatóak:

```
[global]
        workgroup = DEGNET
        netbios name = tanar-server
        passdb backend = ldapsam:ldap://127.0.0.1
        printing = cups
        printcap name = cups
        printcap cache time = 750
        cups options = raw
        map to guest = Bad User
        logon path = \\%L\profiles\.msprofile
        logon home = \\%L\%U\.9xprofile
        logon drive = P:
        add machine script = /sbin/yast /usr/share/YaST2/data/add_machine.ycp
%m$
        domain logons = Yes
        domain master = Yes
        idmap backend = ldap:ldap://127.0.0.1
        ldap admin dn = cn=Administrator,o=deg
        ldap group suffix = ou=Groups
        ldap idmap suffix = ou=Idmap
        ldap machine suffix = ou=Machines
        ldap passwd sync = Yes
        ldap suffix = o=deg
        ldap user suffix = ou=Users
        local master = Yes
        os level = 90
        preferred master = Yes
        security = user
```

```
        wins support = No
        username map = /etc/samba/smbusers
        idmap gid = 10000-20000
        idmap uid = 10000-20000
        wins server =
        bind interfaces only = eth1
[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes
[profiles]
        comment = Network Profiles Service
        path = %H
        read only = No
        store dos attributes = Yes
        create mask = 0600
        directory mask = 0700
[users]
        comment = All users
        path = /home
        read only = No
        inherit acls = Yes
        veto files = /aquota.user/groups/shares/
[groups]
        comment = All groups
        path = /home/groups
        read only = No
        inherit acls = Yes
[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No
[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775
[netlogon]
        comment = Network Logon Service
        path = /var/lib/samba/netlogon
        guest ok = yes
        browseable = no
```

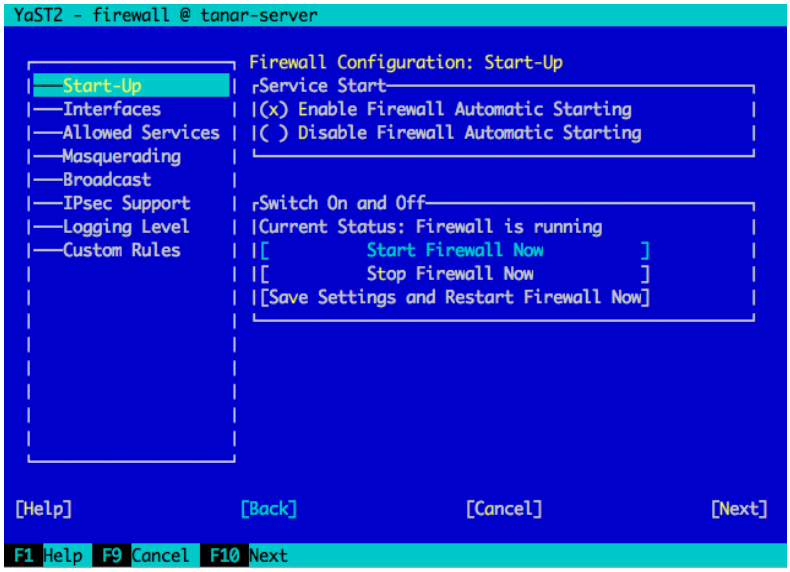
A Samba a felhasználókat az ugyanazon a kiszolgálón futó LDAP adatbázisban tárolja.

A root felhasználó jelszavát az smbpasswd paranccsal legalább egyszer meg kell változtatni, hogy a Samba be tudjon állítani egy NThash/LMhash jelszót a felhasználónak.

Azoknak a felhasználóknak is meg kell változtatni a jelszavukat, akik már létre lettek hozva korábban. Az új felhasználóknak a YaST eltárolja a Samba jelszavukat is az openLDAP adatbázisban, ezért célszerű ilyenkor létrehozni a felhasználókat.

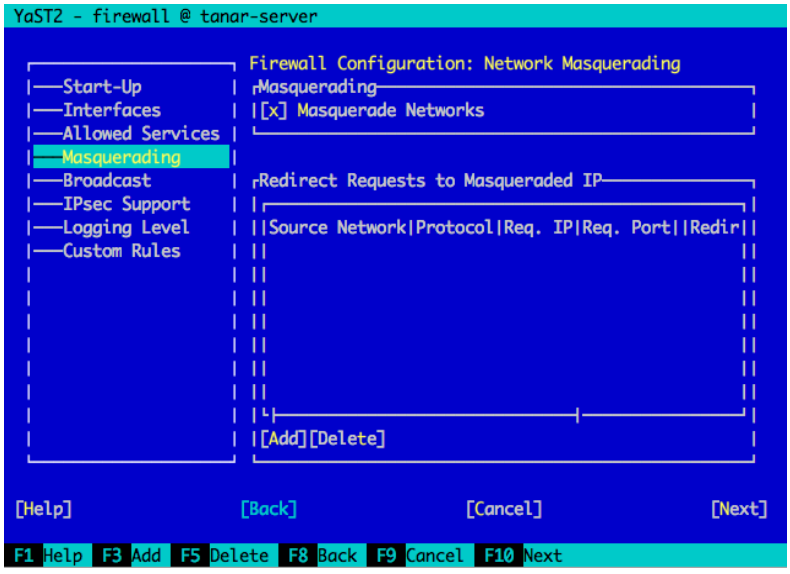
II.5. Internet átjáró

A SUSE Linux Enterprise Server 11 SP1 beépített iptables alapú tűzfalrendszerét használjuk az egyszerű internetes átjáró funkciók kialakítására.



3. ábra: a YaST tűzfal modulja

A tanar-server kiszolgáló tűzfalán beállítottuk a Network Address Translation eljárást és az IP csomagok továbbítását (IP forward).



4. ábra: átjáró beállítása YaST segítségével

Ezt a kiszolgálót internetes átjáróként használhatják a helyi hálózaton elhelyezett eszközök. Amelyik munkaállomás a DHCP szolgáltatástól kapja a hálózati beállításait és ismert hálózati azonosítóval rendelkezik (MAC cím), azok a munkaállomások a tanar-server kiszolgálót használják alapértelmezett átjáróként.

II.6. SQUID webgyorsítótár

A diákok nem férhetnek olyan kötetlenül hozzá az internetes erőforrásokhoz, mint a tanárok. Ezért a diákok gépei nem kapnak alapértelmezett átjárót. Ehelyett a diak-server kiszolgálón futó SQUID webgyorsítótár segítségével hozzáférhetnek az internetes weboldalakhoz.

A SQUID a helyi kiszolgálón futó LDAP adatbázist használja hitelesítési forrásként, és hitelesítés nélkül nem enged hozzáférést semmihez.

A beállításokat tartalmazó konfigurációs állománya a /etc/squid/squid.conf:

```
auth_param basic program /usr/sbin/squid_ldap_auth -b o=deg -Z -v3 -f "uid=
%s"
auth_param basic children 5
auth_param basic credentialsttl 2 hours
auth_param basic realm Squid proxy-caching opensource web server
access_log /var/log/squid/access.log squid
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl localnet proxy_auth REQUIRED
acl SSL_ports port 443
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443
acl CONNECT method CONNECT
acl shoutcast rep_header X-HTTP09-First-Line ^ICY\s[0-9]
acl apache rep_header Server ^Apache

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
http_access allow localhost
http_access deny all

broken_vary_encoding allow apache

icp_access allow localnet
icp_access deny all

http_port 3128
hierarchy_stoplist cgi-bin ?
cache_mem 8 MB
memory_replacement_policy lru
cache_replacement_policy lru
cache_dir ufs /var/cache/squid 100 16 256
minimum_object_size 0 KB
maximum_object_size 4096 KB
cache_swap_low 90
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
emulate_httpd_log off
ftp_passive on

refresh_pattern ^ftp: 1440 20 10080
refresh_pattern ^gopher: 1440 0 1440
refresh_pattern -i  (/cgi-bin/|\?) 0 0 0
refresh_pattern . 0 20 4320

upgrade_http0.9 deny shoutcast
```

```
connect_timeout 2 minutes
client_lifetime 1 days
cache_mgr webmaster

error_directory /usr/share/squid/errors/English
coredump_dir /var/cache/squid
cache_swap_high 95
```

A napló állományok, melyben a lekérdezett weboldalak címei találhatóak a /var/log/squid/ könyvtárban találhatóak. Az aktuális állomány mindig a /var/log/squid/access.log. A naplóban az elért weboldal címe mellett a lekérdezést végző felhasználó belépési azonosítója is szerepel, így könnyen visszakövethető, hogy melyik felhasználó milyen oldalakat ért el a webgyorsítótáron keresztül.

II.7. Időszinkronizáció

A tanar-server az interneten keresztül szinkronizálja a pontos időt. A /etc/ntp.conf állományban a következő időforrásokat definiáltuk:

- 0.hu.pool.ntp.org
- 1.hu.pool.ntp.org
- 2.hu.pool.ntp.org
- 3.hu.pool.ntp.org

A teljes /etc/ntp.conf állomány a következő:

```
server 0.hu.pool.ntp.org
server 1.hu.pool.ntp.org
server 2.hu.pool.ntp.org
server 3.hu.pool.ntp.org
server 127.127.1.0              # local clock (LCL)
fudge  127.127.1.0 stratum 10   # LCL is unsynchronized
driftfile /var/lib/ntp/drift/ntp.drift # path for drift file
logfile   /var/log/ntp          # alternate log file
keys /etc/ntp.keys              # path for keys file
trustedkey 1                    # define trusted keys
requestkey 1                    # key (7) for accessing server variables
```

A tanar-server kiszolgálót a helyi hálózaton futó további kiszolgálók és munkaállomások használhatják időforrásként.

A diak-server kiszolgáló a tanar-server kiszolgálót használja időforrásként, amit a diak-server kiszolgálón a /etc/ntp.conf konfigurációs állományban állítottunk be:

```
server tanar-server
server 127.127.1.0              # local clock (LCL)
fudge  127.127.1.0 stratum 10   # LCL is unsynchronized
driftfile /var/lib/ntp/drift/ntp.drift # path for drift file
logfile   /var/log/ntp          # alternate log file
keys /etc/ntp.keys              # path for keys file
trustedkey 1                    # define trusted keys
requestkey 1                    # key (7) for accessing server variables
```

II.8. Automatikus telepítés

A diákok munkaállomásainak automatikus telepítéséről a SUSE Linux Enterprise rendszerekben megtalálható AutoYAST szolgáltatás gondoskodik. A munkaállomásokat egy előre elkészített profil alapján lehet telepíteni. A profil a diak-server kiszolgálón a /home/autoyast/ könyvtárban található, és autoyast.xml az állomány neve.

A telepítést egy szabályos SUSE Linux Enterprise 11 SP1 telepítő média segítségével el lehet indítani, és a következő indítási paramétereket kell használni:

```
netsetup=dhcp autoyast=nfs://AA.AA.AA.AA/home/autoyast/autoyast.xml
install=nfs://AA.AA.AA.AA/srv/install/SLED11SP1
```

A tanar-server kiszolgálón a /srv/install/deg-sled11sp1.iso állományba beleégettük ezeket a beállításokat. Így azt az iso állományt kiírva egy CD, vagy DVD lemezre azonnal használható testre szabott telepítő kapható, melyet nem kell további indítási paraméterekkel ellátni.

> A telepítő média alapértelmezett indítási bejegyzése nem az automatikus telepítés indítása, mert az mindent letöröl a munkaállomásról.
>
> A médiáról való indítás után az autoinstall menüpontot kell kiválasztani az automatikus telepítés indításához.

Ábrajegyzék

1. ábra: a YaST ldap-server modulja....7
2. ábra: a YaST ldap modulja....8
3. ábra: a YaST tűzfal modulja....10
4. ábra: átjáró beállítása YaST segítségével....10