

POLITEHNIKA NOVA GORICA

POSLOVNO-TEHNIŠKA ŠOLA

DIPLOMSKA NALOGA

**ZASNOVA STREŽNIŠKEGA SISTEMA ZA DELO ŠTUDENTOV  
V RAČUNALNIŠKI UČILNICI**

Bojan Korečič

Mentor: doc. dr. Bogdan Filipič

Komentor: doc. dr. Andrej Filipčič

Nova Gorica, 2006

## ZAHVALA

...in pride dan, ko svoje sanje znova spraviš na plan.

Pot do izobrazbe je strma, a ko učenje postane hobi, je tudi ta premagljiva. Tako mi je po štirih letih znova uspelo preplezati to pot in dodati še eno potrditev tistim, ki niso verjeli vame.

Najprej naj se zahvalim mentorju doc. dr. Bogdanu Filipiču in komentorju doc. dr. Andreju Filipiču za vso pomoč, vodenje in svetovanje pri praktičnem usposabljanju in pripravi diplomske naloge. Zahvala tudi vsem, ki so mi pomagali priti do te diplomske naloge: g. Miranu Kovaču, g. Mateju Horvatu, ge. Adrijani Pisk, ge. Nataši Frelj ter ostalim profesorjem in asistentom na šoli, ki so me poučevali.

Posebna zahvala Politehniko Nova Gorica in doc. dr. Tanji Urbančič, ki mi je omogočila praktično usposabljanje na Poslovno-tehniški šoli, ter ge. Tanji Nemeč za jezikovni pregled diplomske naloge.

Hvala bratu Janu, očetu Jordanu in materi Bruni.

## **IZVLEČEK**

Diplomsko delo obsega analizo in postopek postavitve ter upravljanje strežniškega sistema, ki omogoča vsakemu študentu svoje delovno okolje na kateremkoli računalniku v računalniški učilnici Politehnike Nova Gorica ter centralno upravljanje uporabniških računov. Analiziran je vsak od petih elementov sistema: operacijska sistema Windows in Linux ter trije strežniki. Strežnik Samba omogoča sobivanje obeh operacijskih sistemov in prenosljivost uporabniškega profila. Strežnik Kerberos nudi močno avtentikacijo in zagotavlja varno povezavo med strežnikom in odjemalcem, strežnik LDAP pa vsebuje centralno bazo uporabniških računov z njihovimi informacijami. Tako zasnovan sistem je poskusno nameščen in pripravljen za prenos v računalniško učilnico. Dodatno so analizirani še nekateri strežniki in aplikacije, kot so spletni strežnik Apache, programski jezik PHP, spletni poštni odjemalec SquirrelMail in internetni forum phpBB, ki bodo razširili zmožnosti sistema.

## **ABSTRACT**

This diploma thesis encompasses an analysis, installation procedure and maintenance of a server system that makes it possible for every student to have his/her own working area on any computer in the Politehnika Nova Gorica computer classroom, and central management of user accounts. Five elements of the server system have been analysed: Windows and Linux operating systems, and three servers. The Samba server allows coexistence of both operating systems in the same network and user profile roaming. The Kerberos server offers strong authentication and secure communication between server and client. The LDAP server maintains the central base of user accounts and their information. The system is installed experimentally and ready to be transferred to the computer classroom. Additional servers and applications that will extend the system functionality are described, such as the Apache web server, PHP programming language, SquirrelMail webmail client and phpBB internet form.

## **KLJUČNE BESEDE**

avtentikacija, centralizirani uporabniški računi, operacijski sistem Linux, operacijski sistem Windows, prenosljivost uporabniškega profila, strežnik Kerberos, strežnik LDAP, strežnik Samba

## **KEY WORDS**

authentication, centralized user accounts, Linux operating system, Windows operating system, user profile roaming, Kerberos server, LDAP server, Samba server

## KAZALO

1	UVOD .....	1
1.1	Cilji in vsebina diplomske naloge .....	1
1.2	Dogovor o zapisu.....	2
2	SISTEM V RAČUNALNIŠKI UČILNICI .....	3
2.1	Opis učilnice.....	3
2.2	Izbira elementov .....	4
3	ANALIZA ELEMENTOV PREDLAGANEGA STREŽNIŠKEGA SISTEMA ...	6
3.1	Operacijski sistem Windows .....	6
3.1.1	Popularnost .....	6
3.1.2	Varnost.....	6
3.1.3	Delovna skupina in Windows domena .....	7
3.2	Operacijski sistem Linux.....	7
3.2.1	Unix .....	7
3.2.2	Linux.....	8
3.2.3	Pravni status Linuxa .....	8
3.2.4	Večje distribucije Linuxa.....	9
3.2.5	Lastnosti Linuxa .....	9
3.2.6	Varnost.....	10
3.2.7	Grafični vmesnik .....	11
3.2.8	Ukazna lupina .....	12
3.3	Strežnik Samba.....	12
3.3.1	Zakaj Samba?.....	13
3.3.2	Samba – verzija 3.....	13
3.4	Strežnik LDAP .....	14
3.4.1	Kaj je imenik?.....	15
3.4.2	Imenik – zbirka podatkov .....	15

3.4.2.1	Razmerje med pogostostjo branja in pisanja .....	16
3.4.2.2	Možnost razširitve imenika .....	16
3.4.2.3	Porazdeljenost podatkov .....	16
3.4.2.4	Ponavljjanje vsebine .....	16
3.4.2.5	Učinkovitost.....	17
3.4.2.6	Standardi.....	17
3.5	Strežnik Kerberos .....	17
3.5.1	Termini Kerberosa .....	18
3.5.2	Delovanje Kerberosa.....	19
3.5.2.1	Prvi stik.....	19
3.5.2.2	Zahteva po storitvi .....	20
4	POSKUSNA POSTAVITEV IN UPRAVLJANJE SISTEMA .....	21
4.1	Zasnova strežniškega sistema.....	21
4.1.1	Delovna orodja.....	22
4.2	Postavitev sistema .....	22
4.2.1	Namestitev operacijskega sistema Linux.....	23
4.2.1.1	Priprava na namestitev.....	23
4.2.1.2	Nastavitev sistema .....	24
4.2.2	Konfiguracija strežnika LDAP .....	26
4.2.3	Konfiguracija strežnika Kerberos .....	27
4.2.3.1	Omogočanje PAM podpore za Kerberos.....	28
4.2.3.2	Uporaba LDAPa in Kerberosa.....	29
4.2.4	Konfiguracija strežnika Samba .....	30
4.2.5	Namestitev in konfiguracija skript Idealx smbldap-tools.....	34
4.2.6	Popolnitev LDAP strežnika .....	34
4.2.7	Konfiguracija prenosljivosti uporabniškega profila .....	35
4.2.8	Urejanje privzetega profila .....	35
4.2.9	Vključitev računalnika v domeno .....	37
4.3	Vzdrževanje sistema.....	38
4.3.1	Vzdrževanje strežnika.....	38

4.3.2	Vzdrževanje odjemalcev .....	39
4.4	Upravljanje sistema .....	39
4.4.1	Dodajanje uporabniškega računa .....	39
4.4.2	Brisanje uporabniškega računa .....	40
4.4.3	Spreminjanje podatkov o uporabniku .....	40
5	DODATNI STREŽNIKI IN APLIKACIJE .....	42
5.1	Spletni strežnik .....	43
5.1.1	Strežnik Apache .....	43
5.1.2	Konkurenca .....	44
5.1.3	Spletni imenik uporabnika .....	45
5.2	Programski jezik PHP .....	45
5.3	Spletni poštni odjemalec .....	46
5.3.1	Poštni odjemalec SquirrelMail .....	47
5.4	Internetni forum .....	47
5.4.1	Forum phpBB .....	48
6	ZAKLJUČEK .....	49
6.1	Nadgradnja sistema .....	49
6.2	Sklep .....	50
7	LITERATURA .....	51

## KAZALO SLIK

Slika 1: Shema računalniške učilnice .....	3
Slika 2: Namizje KDE in grafični vmesnik Konqueror .....	11
Slika 3: Shema delovanja strežnika Kerberos.....	19
Slika 4: Zasnova strežniškega sistema.....	21
Slika 5: Namestitvene nastavitve za SUSE Linux .....	23
Slika 6: Konfiguracija strežnika OpenLDAP .....	25
Slika 7: Okno za prijavo v operacijski sistem SUSE Linux .....	26
Slika 8: Nastavitev odjemalca Kerberos .....	27
Slika 9: Izbira delovne skupine za odjemalec Samba.....	30
Slika 10: Nastavitve strežnika Samba.....	31
Slika 11: Nastavitev shem strežnika LDAP .....	32
Slika 12: Register operacijskega sistema Windows .....	36
Slika 13: Vključevanje računalnika v domeno .....	37
Slika 14: Sporočilo ob vključitvi računalnika v domeno.....	38
Slika 15: Program GQ za urejanje podatkov o uporabnikih.....	41
Slika 16: Shema postavitve dodatnih strežnikov in aplikacij .....	42
Slika 17: Časovni pregled deležev nameščenih spletnih strežnikov.....	44
Slika 18: Uporabniški vmesnik spletnega poštnega odjemalca SquirrelMail.....	47
Slika 19: Primer uporabe foruma phpBB .....	48

## KAZALO TABEL

Tabela 1: Zmožnosti strežnika Samba – verzije 3 .....	14
Tabela 2: Spremembe v registru operacijskega sistema Windows.....	37



## 1 UVOD

Računalniki so se že tako zakoreninili v naša življenja, da brez njih skoraj ne znamo živeti. Povezani v svetovni splet pa so postali pravi mali vsevedi in vsem v veliko pomoč. Prav zaradi take zakoreninjenosti in razširjenosti računalnikov že marsikdo pride dnevno v stik z več kot enim računalnikom. Tako imamo en računalnik doma, drugega na delu, pa še prenosnega, po možnosti občasno uporabimo še kakega v etočki in na vsakem od teh računalnikov kmalu pogrešamo svoje domače delovno okolje in datoteke.

Sam sem se z računalnikom v računalniški učilnici Politehnike Nova Gorica prvič srečal v drugem letniku, ko sem ga moral uporabljati zaradi študijskih obveznosti. Računalniki so bili povezani med sabo in v internet. Tako je bilo potrebno vse, kar smo naredili pri uri, shranjevati na diskete, kar je postalo zelo nadležno, saj se je marsikdaj kaj zalomilo: ali sem pozabil diskete ali so bile datoteke prevelike ali pa so se diskete pokvarile. Drugi možen način dela je bil, da sem datoteke pustil v računalniku, pri tem pa sem moral poskrbeti, da sem naslednjič uporabljal isti računalnik. Pri tem sem upal, da mi ne bo kdo datotek zbrisal, saj je do njih imel dostop vsak in je z njimi lahko počel, kar je hotel.

Tako se je že takrat v računalniški učilnici Politehnike Nova Gorica pojavila potreba po sistemu, ki bi omočil vsakemu študentu svoje delovno okolje na kateremkoli računalniku.

### 1.1 Cilji in vsebina diplomske naloge

Glavni cilj te diplomske naloge je postavitvev in upravljanje strežniškega sistema, ki bo omočil vsakemu študentu svoje delovno okolje na kateremkoli računalniku v računalniški učilnici ter centralno upravljanje uporabniških računov. V ta namen bomo pregledali in preučili najprimernejši sistem strežnikov, ki bo zadovoljil potrebe računalniške učilnice.

V drugem poglavju bomo pregledali obstoječi sistem v računalniški učilnici ter s preučitvijo literature in virov predlagali najprimernejši sistem, ki bo izpolnjeval zahtevani cilj.

V tretjem poglavju bomo analizirali vsak element strežniškega sistema z njegovo nalogo, delovanjem, prednostmi in slabostmi.

V četrtem poglavju pa bomo opisali, kako se tak strežniški sistem postavi, vzdržuje in upravlja.

V zadnjem, petem poglavju bomo pregledali, katere dodatne strežnike bi se lahko namestilo in s tem razširilo zmožnosti strežniškega sistema v računalniški učilnici.

## **1.2 Dogovor o zapisu**

Pri pisanju diplomske naloge sem izhajal iz svojega znanja, pridobljenega na srednješolskih in visokošolskih izobraževalnih ustanovah. Tako predpostavljam, da so tudi bralcu znane osnove o osebnih računalnikih, računalniških omrežjih in operacijskem sistemu Windows, a morda nima znanja o operacijskem sistemu Linux, kateremu zato posvečam nekaj več pozornosti.

V diplomskem delu se držimo naslednjih dogovorov o zapisu:

`Pisalni stroj` – uporabljamo za ponazoritev zaslonske interakcije kot tudi za primere izvorne kode, skript ukazne lupine ali za izpis datotek, kot so nastavitvene datoteke.

»« – narekovaji predstavljajo tipko, ki jo je potrebno pritisniti, izbiro med več ponujenimi vrednostmi ali vrednost oziroma vsebino, ki jo je potrebno vpisati.

## 2 SISTEM V RAČUNALNIŠKI UČILNICI

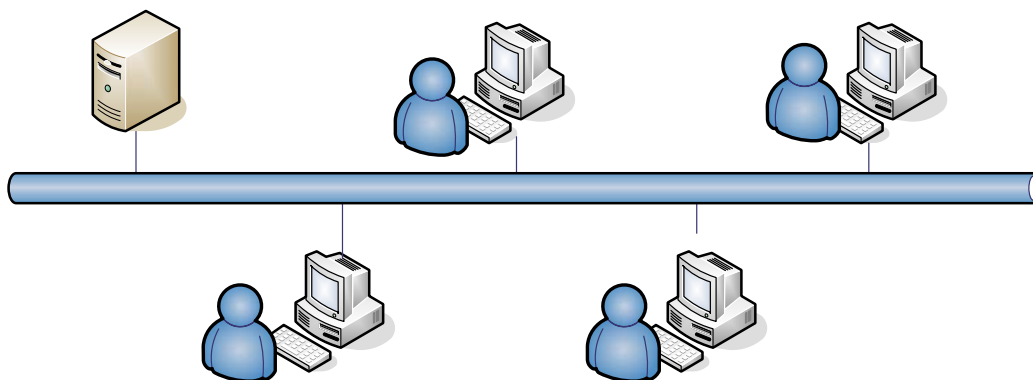
### 2.1 Opis učilnice

Računalniška učilnica Politehnike Nova Gorica (PNG) je namenjena izvajanju študijskega programa šol, ki delujejo v okviru te ustanove.

V njej se nahajajo:

- požarni zid z avtomatsko konfiguracijo omrežja v učilnici,
- strežnik Alpha za celoten servis računalnikov z operacijskim sistemom Linux,
- 16 računalnikov (delovnih postaj) z operacijskima sistemoma Windows XP in Linux Fedora 2.

Vsi računalniki so v isti delovni skupini ter povezani v internet (slika 1), med učilnico in omrežjem PNG je požarni zid, strežnik Alpha pa je v omrežju PNG.



**Slika 1: Shema računalniške učilnice**

Sedanje nastavitve sistema v računalniški učilnici ne omogočajo mrežne uporabe računalnikov s sistemom Windows, svojega delovnega okolja vsakemu študentu na kateremkoli računalniku ter centralnega upravljanja uporabniških računov, zato je potrebno sistem preurediti tako, da bo vse to omogočal.

## 2.2 Izbira elementov

Na odjemalcih oziroma delovnih postajah morata biti nameščena operacijska sistema Windows in Linux (podpoglavji 3.1 in 3.2), ker se za potrebe nekaterih predmetov (npr. Računalništvo in numerične metode) uporablja operacijski sistem Linux, pri ostalih predmetih pa operacijski sistem Windows.

Da bi združili oziroma izkoristili obstoječi sistem in pri tem privarčevali na denarju in času, je rešitev v sistemu, ki je v osnovi zgrajen na operacijskem sistemu Linux, ki z nadgradnjo s strežnikom Samba (podpoglavje 3.3) omogoča tudi delovanje operacijskega sistema Windows. Poleg tega sistem z operacijskim sistemom Linux omogoča bistveno več kot sistem z operacijskim sistemom Windows. Tako smo za osnovo strežnika izbrali operacijski sistem Linux, natančneje distribucijo SUSE Linux Enterprise Server 9.

Za centralno bazo podatkov o uporabniških računih oziroma uporabnikih smo izbrali imenik LDAP (podpoglavje 3.4), zaradi zmožnosti nadgradnje, preglednosti in vse večje razširjenosti protokola LDAP. Razširjen imenik LDAP omogoča tudi integracijo s strežnikom Samba.

Pri prijavi v sistem mora biti uporabnikova identiteta preverjena, to nalogo zelo dobro opravi strežnik Kerberos (podpoglavje 3.5). Prav tako strežnik Kerberos sodeluje z imenikom LDAP.

Distribucija SUSE Linux Enterprise Server 9 je bila izbrana tudi zato, ker ima že vse elemente (Samba verzija 3.0.4, OpenLDAP, Kerberos 5) integrirane in je zato njihova nastavitve manj zahtevna.

Uporabniški profil v operacijskem sistemu Windows vsebuje osebne nastavitve posameznega uporabnika. Z njihovo prenosljivostjo dosežemo, da ima uporabnik ne glede na to, na katerem računalniku dela, vedno pred seboj svoje nastavitve in datoteke. Strežnik Samba omogoča operacijskemu sistemu Windows vključitev v domeno z avtentikacijo. S tem pridobimo možnost gostovanja uporabniškega profila na strežniku in prenašanja profila na katerikoli računalnik v domeni.

Prenovljeni sistem bo tako sestavljen iz petih elementov, strežnikov Kerberos, LDAP in Samba, ki so postavljeni na operacijskem sistemu Linux, ter dveh odjemalcev z

operacijskima sistemoma Windows in Linux. Vsak izmed elementov je v nadaljevanju podrobneje analiziran glede na njegovo nalogo, delovanje, prednosti in slabosti.

## **3 ANALIZA ELEMENTOV PREDLAGANEGA STREŽNIŠKEGA SISTEMA**

### **3.1 Operacijski sistem Windows**

Pod blagovno znamko Microsoft Windows se skriva cela paleta operacijskih sistemov za osebne in strežniške računalnike. Osebni računalniki so namenjeni predvsem osebni uporabi. Strežniki pa so namenjeni zagotavljanju storitev aplikacijam, do katerih dostopa uporabnik s svojega računalnika. Operacijski sistem Windows je zaprtokodni operacijski sistem, ki je v lasti podjetja Microsoft Corporation, kar pomeni, da ima podjetje nad njim avtorske pravice ter nadzor nad njegovo distribucijo.

#### **3.1.1 Popularnost**

Operacijski sistem Windows je nameščen na 90% vseh osebnih računalnikov, kar predstavlja zelo velik tržni delež. Razlog za tako razširjenost tiči že v prevladi MS-DOS-a iz zgodnjih let osebnih računalnikov in v tem, da je operacijski sistem Windows osnova za Microsoft Office in večino računalniških iger ter da je večina programske opreme napisane izključno za operacijski sistem Windows (Microsoft Windows, 2005).

Največji napredek novejših operacijskih sistemov Windows (od Windows 95 in NT 4.0 naprej), zaradi katerega so postali tako popularni, je v namizju in objektno orientiranem grafičnem vmesniku – GUI (angl. Graphical User Interface). Tako je sedaj mogoče opraviti veliko enostavnih nalog in celo nekatere zahtevnejše z malo računalniškega znanja.

#### **3.1.2 Varnost**

Nizka varnost je že mnogo let glavna slabost operacijskega sistema Windows in zaradi njegove razširjenosti mnogo hekerjev (angl. hacker), računalniških kriminalcev, raje cilja nanj kot na ostale operacijske sisteme, kot so Linux, Unix, Mac OS X, FreeBSD itd. Večina modernih operacijskih sistemov je zasnovanih tako, da poskrbijo za varnost in večuporabniški način delovanja v omrežnem okolju, zato imajo relativno manj varnostnih problemov. Operacijski sistem Windows je bil prvotno razvit kot enouporabniški operacijski sistem brez omrežne povezave, zato

varnosti takrat niso dali velikega poudarka in v kombinaciji s pomanjkljivo kodo je operacijski sistem Windows tarča nešteti virusov in črvov, ki povzročijo predvsem veliko finančno škodo.

Kevin Mitnick (2004) v študiji *Time to live on the network* navaja, da je neposodobljen Windows XP zdržal na internetu, ne da bi bil ogrožen, le štiri minute. AOL/National Cyber Security Alliance (2004) v študiji *Online Safety Study* ugotavlja, da je bilo 80% uporabnikov operacijskega sistema Windows okuženih z vsaj enim zlonamernim (angl. spyware/adware) programom, 63% pa jih je že imelo opravka z virusom.

### **3.1.3 Delovna skupina in Windows domena**

Delovna skupina (angl. Workgroup) je en računalnik ali skupina računalnikov z istim imenom delovne skupine z namenom souporabe tiskalnikov in imenikov. Takemu omrežju pravimo tudi mrežni model enak enakemu. Delovna skupina v operacijskem sistemu Windows ne omogoča centralizacije uporabniških računov in avtentikacije, ki jo omogoča Windows domena. Mrežni model delovne skupine je zadostno funkcionalen, dokler gre za zaprt krog manjšega števila računalnikov. V večjih omrežjih model delovne skupine postane omejujoč dejavnik.

Zato je Microsoft za potrebe velikih omrežij z operacijskim sistemom Windows NT 3.51 uvedel domene. Domena je skupina računalnikov v omrežju, ki si delijo informacije, te pa upravlja program domenski nadzornik. Naloga domenskega nadzornika se vrti okrog varnosti, vključno z avtentikacijo dostopa do domene.

Z Windows 2000 pa je Microsoft uvedel Active Directory, ki je nadgradnja Windows domene. Avtentikacija v Active Directory je osnovana na protokolih LDAP in Kerberos.

## **3.2 Operacijski sistem Linux**

### **3.2.1 Unix**

Unix je prenosljiv večopravilni večuporabniški računalniški operacijski sistem in je zaščiten kot blagovna znamka. Prvotno ga je razvila skupina v AT&T Bellovih

laboratorijih (Bell Labs). Verjetno najbolj znan Unixu podoben prost operacijski sistem je Linux, ki ga ne smemo enačiti z Unixom, se pa obnaša podobno kot Unix. Linuxovo jedro namreč nima nobene zveze z AT&Tjevim Unixom, zato ni upravičeno do imena Unix (Unix, 2005). Kadar je torej govor o Unixu, imamo lahko v mislih tudi Linux kot prosto in neodvisno izvedbo Unixa.

### **3.2.2 Linux**

Linux je Unixu podoben prost operacijski sistem s prosto dostopno izvorno kodo, zaščiten s Splošnim dovoljenjem GNU (Linux, 2005).

Pri tem se moramo zavedati, da je razvoj Linuxa odprt in porazdeljen (razdelek 3.2.4) kot večina odprtokodnih programov, medtem ko je razvoj zaprtokodnega programja zaprt in centraliziran. Za razvoj Linuxa ni odgovorna nobena organizacija. Vsakdo z dovolj znanja ima možnost pomagati pri razvoju in razhroščevanju napak jedra, pisanju dokumentacije in pomoči novim uporabnikom. Odprtost tudi pomeni, da je trenutna razvojna verzija vedno javno dostopna (z zamikom tedna ali dveh) in jo lahko kdorkoli uporablja. Rezultat tega je, da izdaja, ki prinaša novo funkcionalnost, skoraj vedno vsebuje tudi napake, po drugi strani pa to pomeni tudi izjemno hiter razvoj, tako da so napake najdene in odpravljene zelo hitro, dostikrat v nekaj urah, saj se z njimi ukvarja veliko ljudi. Namen, skrit za razvojem Linuxa, ni izdaja popolne kode brez hroščev, temveč razvoj proste izvedbe Unixa (Lugos – Kaj je Linux, 2005).

### **3.2.3 Pravni status Linuxa**

Linux je avtorsko delo Linusa B. Torvaldsa in drugih razvijalcev. Čeprav je Linux dosegljiv s celotno izvorno kodo, ni nikogaršnja last ali javna last (angl. public domain), niti ni tako imenovani program na pokušino (angl. shareware), temveč pravno zavarovano avtorsko delo, ki pa je prosto dostopno pod pogoji, navedenimi v GNU General Public License (GPL). Programi, ki tečejo v Linuxu, so vsak posebej avtorsko zavarovani, mnogi med njimi prav tako z GPL, nekateri drugi programi pa z drugimi licencami (GPL, LGPL, BSD, MIT ipd.).



### 3.2.4 Večje distribucije Linuxa

Večje in bolj znane distribucije Linuxa so: Debian, Red Hat, Mandriva, Slackware, Gentoo, SuSE in druge. Distribucij Linuxa je več sto in celo Slovenci imamo tri svoje distribucije: Pingo, Slo-tech in Slix. A pomnite, Linux je jedro. Programje pa je del distribucije in ne Linuxa. Vsaka distribucija ima lastne namestitvene in vzdrževalne pripomočke, ki olajšajo namestitev in upravljanje sistema. Vsaka distribucija cilja na drugačno občinstvo, zato je izbira prave distribucije izmed množice le-teh včasih prav težka naloga.

### 3.2.5 Lastnosti Linuxa

Kaj lahko zmore Linux, je napisno v naslednjih vrsticah (Anderson in sod., 2002). Linux je:

- večopravilni: več programov v njem lahko teče hkrati,
- večuporabniški: več ljudi lahko hkrati dela na istem računalniku,
- večarhitekturni: teče na več različnih mikroprocesorjih, ne le na Intelovih,
- večprocesorski: podpira simetrično večprocesnost SMP (angl. symmetric multiprocessing), Linux uporabljajo tudi v več ohlapno povezanih večprocesorskih aplikacijah, med drugimi tudi sistemi Beowulf in Fujitsujev superračunalnik,
- mrežno računalništvo (angl. grid computing) teče le pod Linuxom (npr. projekt Enabling Grids for E-science (EGEE) ima 20.000 povezanih centralnih procesnih enot).

Poleg tega omogoča:

- zaščito pomnilnika med procesi, tako da en sam program ne more ogroziti stabilnosti celotnega sistema,
- nalaganje programov na zahtevo: Linux prebere z diska v pomnilnik samo tiste dele programa, ki so dejansko potrebni,

- deljene pomnilniške strani: več programov lahko bere iz istega pomnilnika in šele, ko program poskusi pisati v pomnilnik, Linux stran (blok 4 KB) pomnilnika prepíše nekam drugam, kar prinese dve prednosti: večjo hitrost in manjšo porabo pomnilnika,
- navidezni pomnilnik s shranjevanjem na disk po eno stran naenkrat (angl. paging) namesto shranjevanja pomnilniške slike celotnega procesa (angl. swapping) na ločen razdelek ali v datoteko ali pa na obe mesti,
- izpis vsebine pomnilnika (angl. core dump) ob nepravilnem zaključku programa, kar dovoljuje analizo z iskalnikom napak ne le med tekom programa, ampak tudi po tem, ko se je zrušil,
- podporo številnih neangleških ali posebnih tipkovnic, enostavno pa je tudi dodati podporo novim,
- več navideznih konzol: več (do 64) neodvisnih prijav prek konzole, ki jih lahko preklapljamo s kombinacijo tipk (neodvisno od strojne opreme za prikaz),
- podporo več datotečnih sistemov, med njimi System V, MS-DOS, FAT, EXT2, XFS, HFS, UFS, GFS, AFS,
- podporo omrežja TCP/IP, skupaj s storitvami ftp, telnet, NFS, SMB itd.

### 3.2.6 Varnost

Če je nizka varnost največja šibkost operacijskega sistema Windows, je le-ta pri operacijskem sistemu Linux s stabilnostjo njegova največja prednost.

Dr. Nic Peeling in dr. Julian Satchell v Analysis of the Impact of Open Source Software navajata "Za Windows je poznanih okoli 60.000 virusov, približno 40 za Macintosh, in 5 za Unix, in mogoče 40 za Linux. Večina virusov za okolje Windows ni škodljivih, ampak nekaj sto je zelo nevarnih in povzročajo veliko škodo. Dva ali trije virusi za Macintosh so bili široko razširjeni in pomembni. Noben virus za Unix in Linux pa ni bil široko razširjen." (Peeling, Satchell, 2001, str. 21)

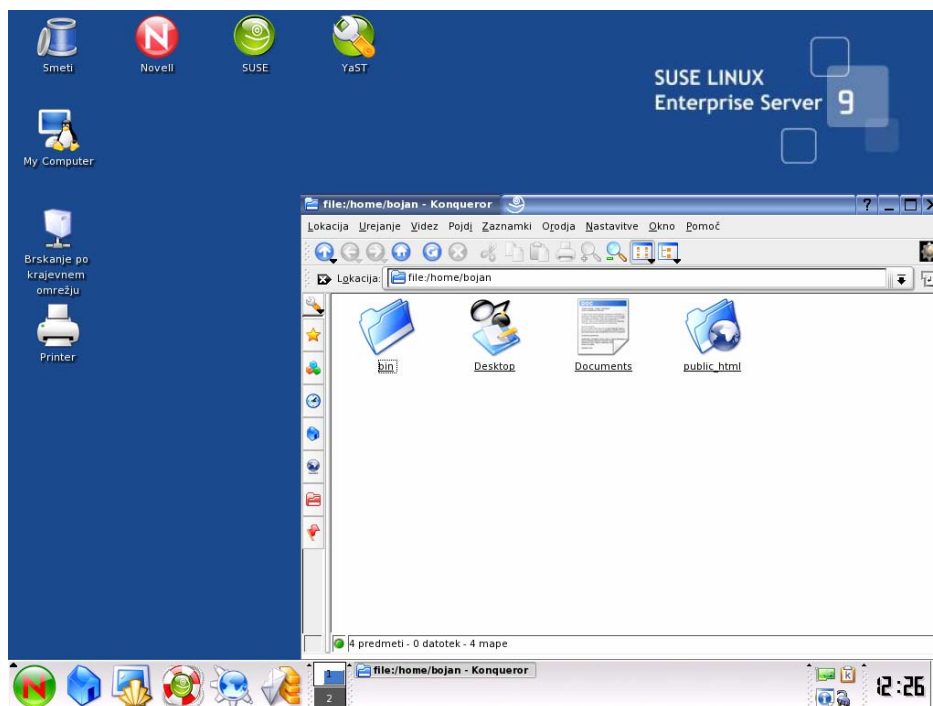
Tudi če na Unixu osnovani operacijski sistemi postanejo dominantni na osebnih računalnikih, ne bo nikoli toliko težav z virusi, črvi ter ostalimi zlonamernimi programi, kot jih doživljamo dandanes na računalnikih z operacijskimi sistemi Microsoft Windows.

### 3.2.7 Grafični vmesnik

Okenški sistem X Window System različice 11, znane kot Xorg (Xfree86) oziroma prosto namizje (angl. freedesktop), je grafični uporabniški vmesnik (GUI) in je bil prvotno razvit na Massachusetts Institute of Technology (MIT). Komercialni proizvajalci so od takrat napravili okenški sistem X za industrijsko standardni GUI za platforme Unix. Zdi se, da vsaka delovna postaja Unix na svetu zdaj poganja neko obliko sistema X (Welsh in sod., 1999).

Linux, opremljen z XFree86, med drugimi upravljalniki namizja podpira namizna okolja KDE in GNOME. Vsako uporablja drug nabor knjižnic in ponuja različne stopnje videza in občutka operacijskega sistema Microsoft Windows.

V namizju KDE se nahaja program Konqueror (slika 2), ki je podoben Raziskovalcu (angl. Explorer) v operacijskem sistemu Windows, vendar je zmogljivejši in funkcionalnejši od Raziskovalca.



Slika 2: Namizje KDE in grafični vmesnik Konqueror

Poleg grafičnega vmesnika Konqueror za manipulacijo z imeniki in datotekami lahko uporabljamo tudi konzolo, kjer Linux pokaže vso svojo moč. Konzolo lahko do neke mere primerjamo z MSH (Microsoft Shell) v operacijskem sistemu Windows.

### **3.2.8 Ukazna lupina**

Ukazna lupina je enako kot vse v sistemu Linux le eden od nameščenih programov. Njen namen je uporabniku omogočiti sporazumevanje z jedrom, predvsem seveda poganjanje programov, s katerimi izvajamo željena opravila. Sporazumevanje je znakovno: uporabnik s tipkovnico vpisuje ukaze in bere odgovore z zaslona. V okolju DOS to postori program `command.com` (Cvjetović in sod., 2000).

### **3.3 Strežnik Samba**

Samba je skupek aplikacij v Unixu, ki uporabljajo Server Message Block (SMB) protokol. Operacijski sistemi Microsoft Windows in operacijski sistem OS/2 uporabljajo SMB za souporabo datotek in tiskalnikov ter podobne operacije. S tem protokolom Samba omogoča sistemu Unix komunikacijo z istim omrežnim protokolom kot Microsoft Windows in se pojavi kot drugi Windows sistem na omrežju s perspektive odjemalca z operacijskim sistemom Windows.

Čeprav bi bilo verjetno normalno, da se uporablja strežnik Windows za souporabo datotek in tiskalnikov v omrežju, ki vsebuje Windows odjemalce, je kar nekaj tehničnih razlogov, da to delo opravlja strežnik Samba. Samba je zanesljiv program, ki teče na operacijskem sistemu Unix, kar se kaže v majhnem številu težav in nizkih stroških vzdrževanja. Samba se dobro izkaže pri velikih obremenitvah, tako je tudi dvakrat hitrejša od operacijskega sistema Windows 2000 na računalniku z enako strojno opremo. Samba ima prav tako cenovno prednost, saj je brezplačna in za odjemalca ni potrebna nobena licenca (Jay Ts, Eckstein, Collier-Brown, 2003). Zaradi tega jo uporabljajo korporacije, banke in ostale finančne institucije, državna uprava in vojaške organizacije, šole, knjižnice, galerije, družine itd.

Samba vzdržuje in dopolnjuje skupina prostovoljcev, ki jo vodi Andrew Tridgell. Kot operacijski sistem Linux je tudi Samba distribuirana kot odprtokodni program pod licenco GPL.

### 3.3.1 Zakaj Samba?

Kot smo že prej razložili, Samba omogoča, da Windows in Unix sobivata v istem omrežju, vendar so v nadaljevanju navedeni nekateri specifični razlogi, zakaj bi hoteli vključiti strežnik Samba v omrežje.

- Nočete plačati ali si ne morete privoščiti strežnika z operacijskim sistemom Windows, vendar si želite njegove funkcionalnosti.
- Cena licenc za dostop CAL (angl. Client Access Licenses - CALs), ki jih potrebujemo za vsakega odjemalca, ki uporablja strežnik Windows, je previsoka.
- Hočete imeti skupen prostor za podatke in imenike uporabnikov za prehod z Windows na Unix strežnik ali obratno.
- Hočete souporabljati tiskalnike med Windows in Unix računalniki.
- Hočete imeti podporo skupini računalnikov, katerih uporabniki imajo tako operacijske sisteme Windows kot Unix.
- Hočete integrirati avtentikacijo in vzdrževanje ene baze uporabniških računov tako za Unix kot Windows sisteme.
- Hočete omrežiti Unix, Windows, Macintosh (OS X) in ostale sisteme z uporabo enega protokola.
- Windows strežnik je neprimeren in pomanjkljiv za velike organizacije zaradi nezmožnosti nadgradnje, neprimerne administracije, ne nudi Unix servisov ipd.

### 3.3.2 Samba – verzija 3

V tabeli 1 smo strnili naloge, ki jih lahko izvede ali ne more izvesti Samba tretje verzije. Mnogo Windows domenskih protokolov, eden takih je Active Directory, je v lasti Microsofta in niso dokumentirani, zato mora biti izvedena razgradnja (angl. reverse-engineering) le-tega, preden ga Samba lahko podpira. Tako Samba tretje

verzije še vedno ne more vedno delovati kot rezervni strežnik v večini vlog in Active Directory še vedno ni v celoti podprt.

**Tabela 1: Zmožnosti strežnika Samba – verzije 3**

Zmožnosti, ki jih strežnik Samba podpira
datotečni strežnik
tiskalniški strežnik
Microsoft DFS strežnik
primarni domenski nadzornik
Windows 95/98/Me/NT/2000/XP avtentikacija
primarni lokalni pregledovalnik
rezervni lokalni pregledovalnik
primarni domenski pregledovalnik
Zmožnosti, ki jih strežnik Samba ne podpira
rezervni domenski nadzornik
Active Directory
rezervni strežnik WINS

### 3.4 Strežnik LDAP

Preprost protokol za dostop do imenika LDAP (angl. Lightweight Directory Access Protocol) je odprt standard, ki je bil razvit z namenom optimizacije in poenotenja imenikov. LDAP definira standardno metodo za dostop in upravljanje informacij v imenikih. Zasnovan in optimiziran je tako, da omogoča hitro branje velikega števila podatkov v imenikih, njihovo spreminjanje pa je precej redko glede na branje. Je učinkovit, enostaven za implementacijo, a hkrati visoko funkcionalen. Deluje po principu odjemalec/strežnik, kar pomeni, da se morata odjemalec in LDAP strežnik držati točno določenih pravil, če želita komunicirati med seboj (Sodnik, 2002).

Osnovne zmožnosti LDAP-a, ki jih je potrebno omeniti, so naslednje:

- hranjenje posebnih informacij o določenih uporabnikih,
- upravljanje kontaktov,

- hranjenje slik,
- evidence dokumentov,
- zagotavljanje varnosti itd.

### **3.4.1 Kaj je imenik?**

V vsakdanjem življenju se pogosto srečujemo z različnimi vrstami imenikov. Primeri so telefonski imenik, vodič po televizijskem programu, razni nakupovalni katalogi, ipd. Te lahko poimenujemo tudi nepovezani (angl. offline) imeniki. Pogosto najdemo v računalniškem svetu imenike, katerih namen in zgradba sta podobna. Te največkrat poimenujemo kar povezani (angl. online) imeniki.

Večina imenikov, s katerimi imamo opravka v vsakdanjem življenju, je namenjenih iskanju določenih informacij, bodisi iskanju prave knjige v knjižnici, naročanju obleke iz kataloga, iskanju podatkov o nekem poslovnem partnerju ipd.

Osnovne štiri značilnosti povezanih imenikov, po katerih se tudi najbolj razlikujejo od prej omenjenih nepovezanih imenikov, so:

- dinamičnost,
- prilagodljivost,
- varnost in
- prilagojenost uporabniku.

### **3.4.2 Imenik – zbirka podatkov**

Na imenik lahko gledamo kot na posebno zbirko podatkov. V osnovi se ti dve strukturi ne razlikujeta pretirano, razlike med njima nastopijo šele, ko jih postavimo v določeno okolje oziroma izrazimo namen njune uporabe. Glavne razlike lahko razčlenimo v šest točk, ki so v nadaljevanju podrobneje opisane.

#### ***3.4.2.1 Razmerje med pogostostjo branja in pisanja***

Ena od najpomembnejših lastnosti imenikov je, da njihovo vsebino veliko bolj pogosto pregledujemo kot spreminjamo. V povprečju posamezno informacijo v imeniku preberemo od 1.000 do 10.000-krat pogosteje kot jo zapišemo ali spreminjamo. Tipičen primer takšne informacije so podatki o osebah, njihovih telefonskih številkah, naslovih, skratka, vsi takšni podatki, ki se redko spreminjajo.

Za klasične zbirke podatkov to ponavadi ne velja, saj v njih hranimo informacije, ki se pogosto obnavljajo, na primer evidenca finančnih transakcij v neki banki.

#### ***3.4.2.2 Možnost razširitve imenika***

Tip vsebine, ki jo lahko hranimo v imeniku, definira t.i. shema imenika (angl. directory schema). To so pravila, katerim so podrejene informacije v imeniku oziroma delo z njimi. Značilno je, da ta shema ni fiksna, temveč se lahko sproti prilagodi novim potrebam uporabnikov ali aplikacij.

Čeprav lahko v klasičnih zbirkah podatkov hranimo veliko različnih tipov informacij, ki so organizirane na različne načine, jih z definicijo zbirke omejimo.

#### ***3.4.2.3 Porazdeljenost podatkov***

Do neke mere lahko porazdelimo vsebino klasične relacijske zbirke podatkov. V tem primeru ponavadi shranimo posamezne tabele na različne računalnike. Delo s takimi podatki, npr. opravljanje različnih poizvedb, je sicer mogoče, vendar močno trpi učinkovitost oziroma hitrost delovanja. Zato se taka organizacija relacijske zbirke podatkov uporablja redkeje.

Nasprotno pa je osnovna lastnost imenikov možnost porazdelitve vsebine na več strežnikov. Ta način organizacije pride do izraza predvsem pri podjetjih, ki imajo sedeže na različnih lokacijah, vsak del organizacije pa želi sam upravljati s svojim delom imenika. Bistveno pri tem je, da za druge zunanje uporabnike imenik deluje kot enota in njegova porazdeljenost sploh ni opazna.

#### ***3.4.2.4 Ponavljanje vsebine***

Ponavljjanje vsebine pomeni, da hranimo isto informacijo v več različnih imenikih, na različnih lokacijah zaradi različnih vzrokov, kot so zanesljivost, razpoložljivost, lokalnost in učinkovitost. Tudi klasične zbirke podatkov včasih omogočajo



ponavljanje vsebine, a ponavadi le za majhno število kopij, saj je problem v zahtevi po popolni konsistentnosti podatkov.

#### ***3.4.2.5 Učinkovitost***

Učinkovitost zbirk podatkov ponavadi merimo s številom operacij oziroma transakcij na sekundo. Neko veliko zbirko podatkov lahko opišemo kot učinkovito, če je sposobna opraviti približno 100 operacij na sekundo. Pri imenikih je ta zahteva nekje med 1.000 in 10.000 operacij na sekundo. Te operacije so ponavadi preprostejše kot pri klasičnih zbirkah podatkov.

#### ***3.4.2.6 Standardi***

Pri klasičnih zbirkah podatkov imamo opravka s t.i. psevdo-standardi, na primer poseben jezik za poizvedovanje v relacijskih zbirkah podatkov – SQL (angl. Simple Query Language). Ti poskrbijo, da lahko podatke preprosto prenesemo z ene zbirke podatkov v drugo, jih popravljamo in urejamo.

Pri imenikih so standardi zelo pomembni. Vsak ponudnik aplikacije, ki omogoča dostop do imenika, se mora strogo držati standarda, saj mora aplikacija delovati z vsakim imenikom. Tu pride do izraza LDAP. Ta zagotavlja standardni model imenika in protokol za dostop do njega.

### **3.5 Strežnik Kerberos**

Današnji računalniki nimajo oči, ušes ali nosu. Tudi če bi jih imeli, je trenutna tehnična zmogljivost teh naprav nezadostna za vsesplošno uporabo v avtentikacijske namene. Medtem je trenutna metoda avtentikacije ljudi za dostop do računalnika le geslo. Geslo je odločilna informacija, ki določa, ali je oseba za tipkovnico dejansko tista, ki se je prijavila (Garman, 2003).

Pri tem se pojavita dva problema. Prvi problem je v tem, da si ljudje težko zapomnimo dolge in komplicirane nize števil in črk ali celo znakov, ki naredijo geslo varno. Tako ponavadi uporabljamo za gesla svoja imena ali datum rojstva. Na žalost taka gesla niso gesla, saj niso varna in jih napadalec, ki napada računalnik, lahko ugane.

Drugi problem je tehnične narave. Medtem, ko v računalnik vpisujemo geslo in se na zaslonu prikazujejo zvezdice ali celo ni prikaza, mora informacija potovati po omrežju do drugega računalnika. Najbolj pogosta metoda, ki jo uporabljajo računalniki za pošiljanje gesel prek omrežja, je v nešifrirani obliki (angl. clear text). Pošiljanje nešifriranega gesla prek omrežja lahko primerjamo s kričanjem gesla prijatelju, ki je na drugem koncu dvorane, polne ljudi.

Kerberos je mrežni avtentikacijski protokol, ki reši ta dva problema. Zmanjša število gesel, ki si jih mora posameznik zapomniti za uporabo omrežja, na eno – Kerberos geslo ter vključuje šifriranje, kar rešuje drugi problem in zagotavlja, da občutljivi podatki avtentikacije nikoli ne potujejo po omrežju v nešifrirani obliki. Z vključitvijo varnostnega avtentikacijskega mehanizma Kerberos v omrežje pridobijo tako uporabniki kot administratorji sistema.

Kerberos večkrat imenujejo tudi zaupanja vredni posrednik, ker mu zaupajo vsi odjemalci. Kerberos omogoča tudi enkratno prijavo (angl. single sign on – SSO). To pomeni, da se uporabnik samo enkrat prijavi oziroma avtenticira in za vse nadaljnje prijave do ostalih storitev v omrežju, do katerih ima pravico dostopati, poskrbi Kerberos. Nekateri aplikacije, ki podpirajo avtentikacijski sistem Kerberos, so telnet, telnetd, rlogin, rsh, rcp, rshd, popper, push, ftp, ftpd, su, imapd in pine.

Prvotni Kerberos je razvilo podjetje MIT. Poleg MIT Kerberosa obstaja še nekaj izvedb Kerberosa. Tako je v SUSE Linux Enterprise Server 9 implemenitana brezplačna različica Heimdal Kerberos 5.

### **3.5.1 Termini Kerberosa**

V tem razdelku so pojasnjeni nekateri termini avtentikacijske metode Kerberos (Network Authentication, 2005).

***Avtentikacija*** (angl. authentication) je v računalništvu proces, v katerem se mora strežnik prepričati, da je uporabnik res tisti, ki trdi, da je.

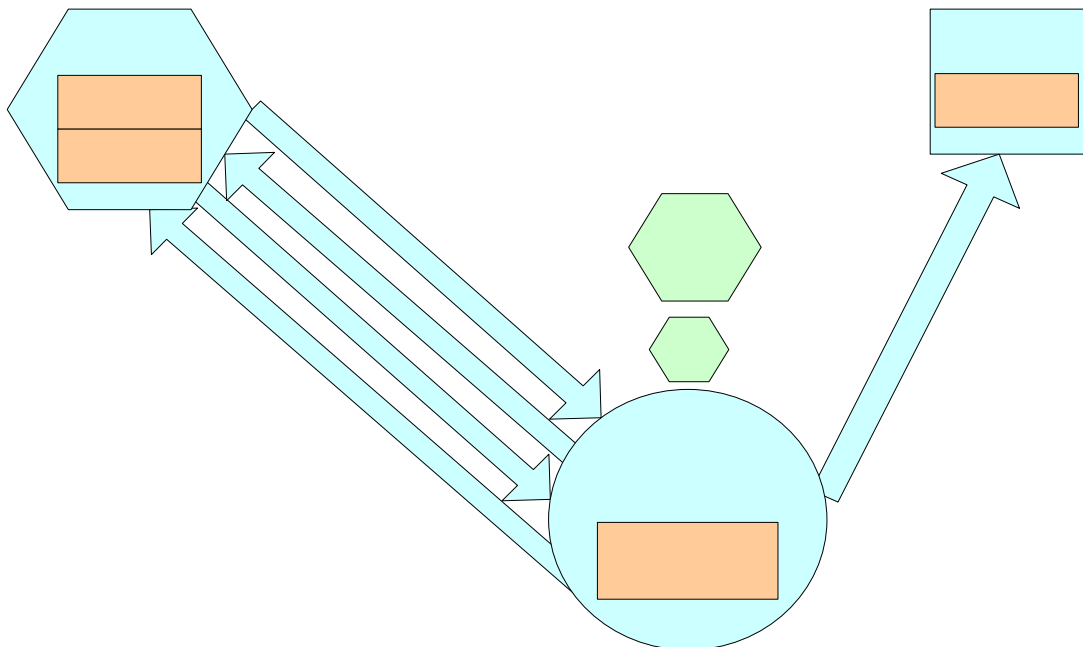
***Vstopnica*** (angl. ticket) je poverilnica, ki jo uporablja odjemalec za avtentikacijo. Vstopnica vsebuje ime strežnika, ime odjemalca, IP naslov odjemalca, trenutni čas, življenjsko dobo in sejni ključ. Vse to je šifrirano s ključem.

**Sejni ključ** (angl. session key) je začasni privatni ključ, ki ga generira Kerberos. Znan je odjemalcu in strežniku, za katerega je bila izdana vstopnica, ter se uporablja za šifriranje komunikacije med njima.

**Strežnik, storitev** (angl. server, service) – storitev se nanaša na izvedbo specifičnega dejanja, ki ga izvaja strežnik. Strežnik lahko izvede več storitev oziroma dejanj.

### 3.5.2 Delovanje Kerberosa

Na sliki 3 je shematično prikazano delovanje Kerberosa, ki je v nadaljevanju opisano.



Slika 3: Shema delovanja strežnika Kerberos

#### 3.5.2.1 Prvi stik

Uporabnik se sreča s Kerberosom med prijavo v sistem. Ko uporabnik vpiše uporabniško ime, se to pošlje strežniku Kerberos. Če strežnik tega pozna, torej če ga ima v svoji bazi, izda TGT (angl. Ticket-Granting Ticket) vstopnico in jo zašifrira z uporabniškim ključem, ki ga poznata le strežnik Kerberos in uporabnik, saj je izpeljan iz uporabniškega gesla. Sedaj uporabnik vpiše geslo, ki je pretvorjeno v uporabniški ključ, ki lahko dešifrira paket. Ko je paket dešifriran, se geslo in ključ izbrišeta iz spomina delovne postaje. S tem uporabnik pridobi TGT vstopnico, ki

Strežnik  
Kerberos

Strežniško  
geslo

Uporabnikovo  
geslo

Storitev

TGT, šifriran z

Zahteva po

vstopnica, šifrirana s str

omogoča nadaljnje delo in dostop do sistema. Če je geslo napačno, uporabnik ne more priti do TGT vstopnice in se prijaviti v sistem.

#### ***3.5.2.2 Zahteva po storitvi***

Če katerakoli aplikacija na odjemalcu zahteva storitev od kateregakoli strežnika v omrežju, mora aplikacija dokazati svojo identiteto. Zahtevo po storitvi in vse potrebne informacije za izdajo storitvene vstopnice, ki so šifrirane s sejnim ključem, ki ga poznata samo strežnik in odjemalec, so poslane strežniku Kerberos. Ta uporabi svojo kopijo sejnega ključa za dešifriranje paketa. Po dešifriranju paketa strežnik Kerberos izdela storitveno vstopnico, ki je šifrirana s strežniškim ključem, ki je izpeljan iz strežniškega gesla, ki ga poznata samo strežnik Kerberos in strežnik do katerega dostopa aplikacija. Nato odjemalec pošlje zahtevo po storitvi skupaj s storitveno vstopnico strežniku, ki dešifrira paket, preveri identiteto s pomočjo vstopnice in izvrši zahtevano storitev.

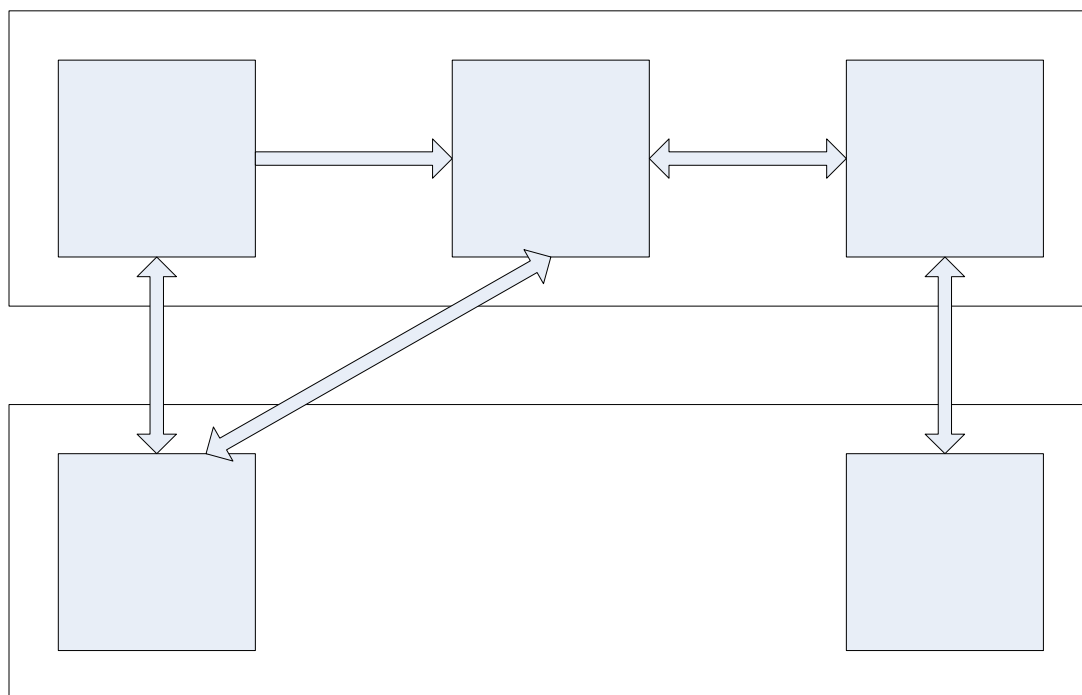
## 4 POSKUSNA POSTAVITEV IN UPRAVLJANJE SISTEMA

Navedeni sistem je bil nameščen in testiran na enem izmed računalnikov na Politehniko Nova Gorica. Testiranje je potekalo tako, da sem na računalnik namestil vse potrebne strežnike in jih nastavljal ter postavljen sistem testiral. Za odjemalce sem uporabil virtualni računalnik oziroma program VMware, ki omogoča postavitve virtualnih računalnikov. Strežniški sistem je bil tako postavljen in testiran.

Natančnejši postopek z vsakim korakom postavitve in upravljanje navedenega strežniškega sistema je opisan v končnem poročilu praktičnega usposabljanja z naslovom Postavitev mrežnega sistema v računalniški učilnici (Korečič, 2005).

### 4.1 Zasnova strežniškega sistema

Na sliki 4 je prikazana zasnova predlaganega strežniškega sistema z vsemi petimi elementi in njihovimi medsebojnimi interakcijami.



Slika 4: Zasnova strežniškega sistema

Strežnik LDAP hrani vse podatke o uporabnikih v svojem imeniku – centralna baza uporabniških računov. Strežnik Samba omogoča operacijskemu sistemu Windows dostop do datotek, ki so v skupni rabi, in gostovanje profila. Strežnik Kerberos

poskrbi za varno prijavo in komuniciranje med odjemalcem z operacijskim sistemom Linux in strežnikom.

Ko se uporabnik prijavi v sistem z operacijskega sistema Windows, ta stopi v kontakt s strežnikom Samba, ki podatke o uporabnikih najde v imeniku LDAP in uporabnika oziroma odjemalca avtenticira. Ko je uporabnik avtenticiran, se njegov profil prenese na trenutni delovni računalnik. S časom lahko postane profil uporabnika zelo obsežen (tudi 100 MB in več) in je prenašanje takega profila prek mreže dolgotrajno in zamudno, zato se nekatere mape, ki najhitreje postanejo velike, preseli neposredno na strežnik. To pomeni, da te mape in njihova vsebina domujejo na strežniku in se ne prenašajo s profilom. Ko uporabnik konča z delom, se odjavi iz sistema in pri tem se njegov profil s trenutnega delovnega računalnika prenese na strežnik.

Pri prijavi uporabnika z operacijskega sistema Linux NSS (angl. name server switch) poišče informacije o uporabniku v imeniku LDAP ter se z znanim uporabniškim imenom avtenticira s pomočjo Kerberosa. Ko je uporabnik oziroma odjemalec avtenticiran, ima dostop do svojega imenika in datotek, ki so na strežniku. Prav tako lahko uporabnik pregleduje in upravlja imenik LDAP, če le ima dovoljenje za to.

#### **4.1.1 Delovna orodja**

Za postavitev navedenega strežniškega sistema potrebujemo dovolj zmogljiv računalnik, na katerem bo nameščen SUSE Linux Enterprise Server 9 z vsemi tremi strežniki.

Programska oprema, potrebna za postavitev strežniškega sistema:

- SUSE Linux Enterprise Server 9, 6 zgoščenk (angl. CD),
- skripte Idealx smbldap-tools (<http://www.idealx.org/prj/samba/>).

#### **4.2 Postavitev sistema**

V nadaljevanju je opisan postopek postavitve strežniškega sistema na strežniku. Na odjemalce je potrebno le namestiti operacijski sistem Windows in/ali operacijski sistem Linux. Ker so na računalnikih v računalniški učilnici že nameščeni operacijski sistemi, se opisovanju njihovega nameščanja ne bomo posvečali. Naj ob tem

omenimo, da gre pri nameščanju operacijskih sistemov Windows in Linux v večini primerov le za sledenje navodilom, ki se izpisujejo na ekran, saj se večina operacij izvede samodejno.

## 4.2.1 Namestitev operacijskega sistema Linux

Namestitev Linuxa bi lahko razdelili na dva dela:

- pripravo na namestitev,
- nastavitev sistema.

V nadaljevanju je razložena namestitev SUSE Linux Enterprise Server 9.

### 4.2.1.1 Priprava na namestitev

Po vstavitvi CD-ja v CD-predvajalnik se računalnik zažene s CD-ja (angl. boot from CD) in preide v fazo priprave na namestitev, kjer najprej sprejmemo licenco in izberemo jezik namestitve ter posledično tudi jezik celotnega vmesnika sistema. Po določitvi jezika se izvede razpoznavanje strojne opreme in izbira vrste namestitve. Pri tem nam YaST ponudi seznam namestitvenih nastavitev (slika 5). YaST je skupek namestitvenih in vzdrževalnih pripomočkov z grafičnim vmesnikom, značilnih za SUSE distribucije Linuxa.



Slika 5: Namestitvene nastavitve za SUSE Linux

V seznamu namestitvenih nastavitev lahko spremenimo:

- sistem,
- način namestitve,
- razpored tipkovnice,
- miško,
- particioniranje,
- programsko opremo,
- zaganjanje sistema,
- časovni pas,
- jezik,
- privzeti delovni nivo.

Ko smo vse prilagodili našim zahtevam, lahko operacijski sistem Linux namestimo. Trajanje nameščanja je odvisno od samega računalnika in količine programske opreme, ki jo želimo namestiti. Tako traja namestitev od 20 minut do dve uri. Namestitev od nas zahteva le menjavanje CD-jev v primeru, da imamo distribucijo Linuxa, ki je na večjem številu CD-jev, kot je v našem primeru. Ko je namestitev končana, se računalnik avtomatsko pripravi na prvi zagon.

#### ***4.2.1.2 Nastavitev sistema***

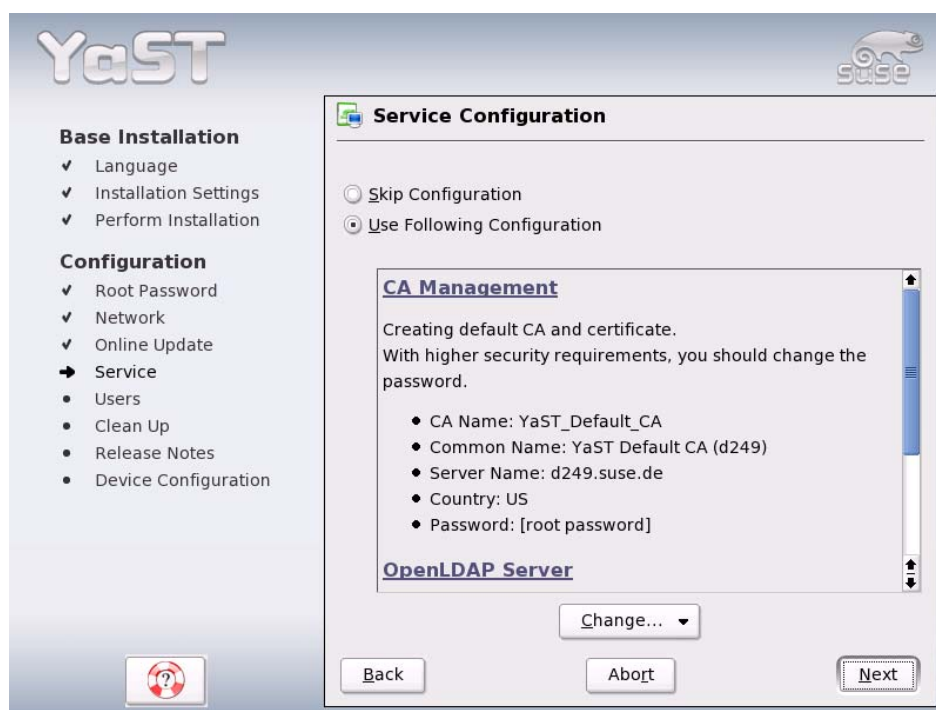
Po namestitvi Linuxa je potrebno sistem še konfigurirati. Najprej je potrebno vpisati geslo korenkega (angl. root) uporabnika, ki je sistemski administrator z najvišjimi (vsemi) privilegiji. Naj pri tem omenimo, da smo v primeru slabo sestavljenega gesla na to opozorjeni. Slabo sestavljeno geslo namreč poveča verjetnost vdora v sistem.

Sledi nastavitev omrežja, za katero sistem sam prepozna povezave oziroma naprave za povezavo na omrežje (omrežni vmesnik, povezava DSL, adapter ISDN, modemi, namestnik (proxy), oddaljeno upravljanje VNC). Po končanih nastavitvah omrežja imamo možnost njihovega testiranja. V primeru, da je povezava uspešna, je možno



prenesti tudi zadnje popravke sistema s strežnika SUSE le v primeru, da smo nanj naročeni.

Konfiguracija strežnika OpenLDAP in upravljanje s certifikacijskimi pooblastili CA (Certificate Authority Management) je naslednja nastavitvev (slika 6), ki se pojavi na zaslonu računalnika. Tukaj se računalnik sam nastavi na zelene nastavitve, pri tem pa moramo biti pozorni na nastavitve strežnika OpenLDAP.



Slika 6: Konfiguracija strežnika OpenLDAP

Nastavitve strežnika OpenLDAP morajo biti podobne naslednjim nastavitvam :

- Base DN: dc=p-ng,dc=si – osnovni DN (angl. Distinguished Name)
- Root DN: cn=Administrator,dc=p-ng,dc=si – administrativni DN
- LDAP Password: [root password] – geslo, ki ga uporablja korenski uporabnik (root DN)

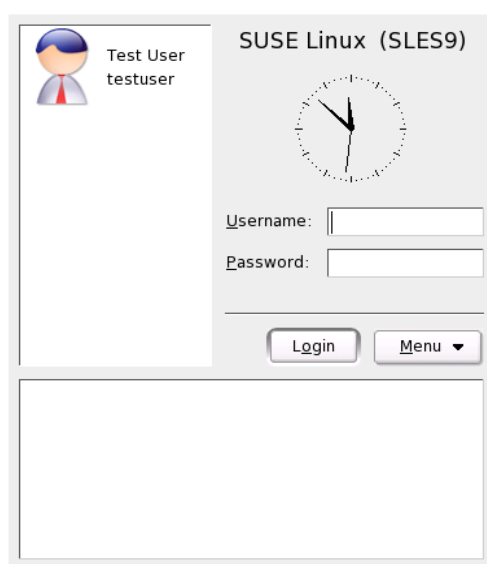
Pri postopku avtentikacije uporabnika izberemo metodo LDAP, ker Kerberos avtentikacije ni na voljo. Pri izbiri avtentikacije z LDAP-jem je potrebno nastaviti še odjemalec za LDAP.

Sledi vpis novega uporabnika, LDAP uporabnika. LDAP uporabnik je zato, ker smo prej nastavili, da je avtentikacija izvedena prek LDAP strežnika. To tudi pomeni, da so vse informacije o uporabnikih v imeniku LDAP.

Na koncu moramo nastaviti še strojno opremo. V našem primeru se je nastavila naslednja strojna oprema:

- grafična kartica,
- zvočna kartica.

Večina nastavitvev se opravi samodejno, največkrat pa je potrebno dodatno popraviti nastavitve grafične kartice. Ko končamo z nastavitvami, se na ekranu prikaže okno za prijavo v SUSE Linux (slika 7).



**Slika 7: Okno za prijavo v operacijski sistem SUSE Linux**

Ko vpišemo uporabniško ime in geslo, se naloži namizje KDE in najdemo se pred zaslonom/namizjem (slika 2), ki je podoben kot v operacijskem sistemu Windows.

#### **4.2.2 Konfiguracija strežnika LDAP**

Strežnik LDAP se je avtomatsko nastavil že ob namestitvi sistema (razdelek 4.2.1.2).

### 4.2.3 Konfiguracija strežnika Kerberos

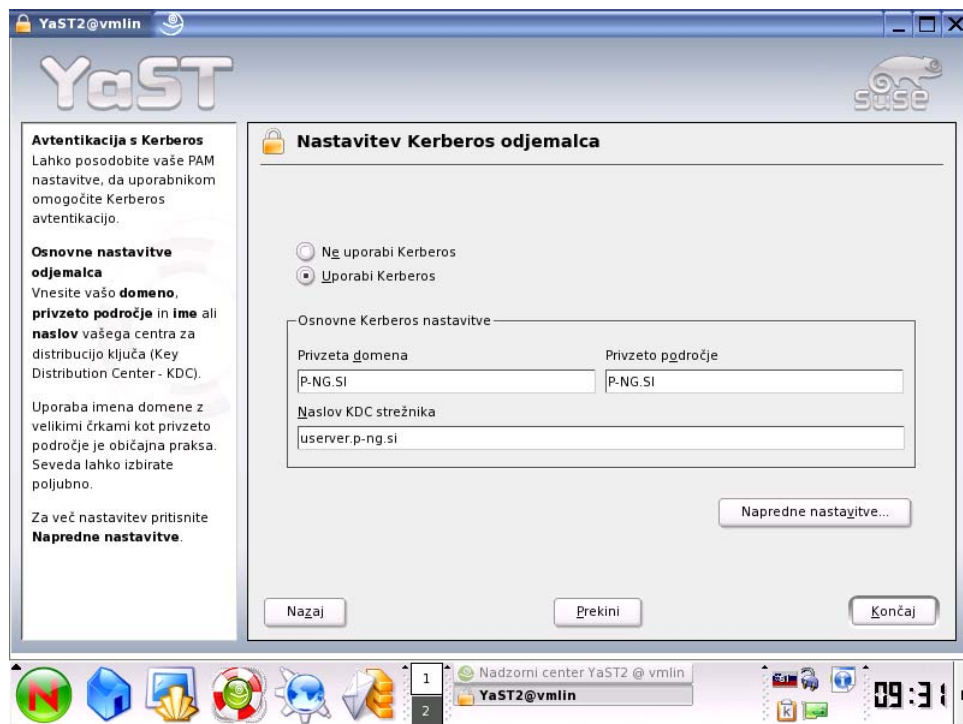
Preden lahko začnemo uporabljati Kerberos, ga je potrebno namestiti. Pri tem je potrebno namestiti naslednje datoteke, ki so del distribucije:

- heimdal,
- heimdal-lib,
- heimdal-tool.

Po namestitvi sledi konfiguracija odjemalca Kerberos. To lahko storimo na dva načina:

- prek nadzornega središča YaST,
- z urejanjem datoteke `/etc/krb5.conf`.

S pomočjo nadzornega središča YaST omogočimo uporabo Kerberosa ter vpišemo privzeto domeno, privzeto področje in naslov KDC (angl. Key Distributon Center) strežnika – izdajatelja vstopnic (slika 8).



Slika 8: Nastavitev odjemalca Kerberos

Naslednja faza je inicializacija baze, v kateri Kerberos shranjuje vse informacije o računih. Najprej se nastavi glavni ključ, ki se uporablja za varovanje baze pred razkritjem. Po kreiranju področja lahko ustvarimo uporabniške račune:

```
kadmin -l
kadmin> add bojan
Max ticket life [1 day]: »pritisni enter«
Max renewable life [1 week]: »pritisni enter«
Principal expiration time [never]: »pritisni enter«
Password expiration time [never]: »pritisni enter«
Attributes []: »pritisni enter«
bojan@P-NG.SI's Password: »vpiši geslo«
Verifying password: »ponovno vpiši geslo«
```

Ko smo to kreirali, je potrebno še zagnati strežnik KDC. Da pa ne bi vedno znova po nepotrebnem ročno zaganjali KDC-ja, sistem nastavimo tako, da se pri zagonu avtomatsko zažene še strežnik KDC.

#### ***4.2.3.1 Omogočanje PAM podpore za Kerberos***

SUSE Linux ima možnost integracije avtentikacijskega modula PAM (angl. Pluggable Authentication Modules), ki je program oziroma vmesnik za avtentikacijo. Pam\_krb5 pa je avtentikacijski modul oziroma vmesnik za dostop do Kerberosa.

To funkcijo omogočamo, če v datoteki /etc/security/pam\_unix2.conf naredimo naslednje spremembe:

```
auth: use_krb5 nullok
account: use_krb5
password: use_krb5 nullok
session: none
```

Ko so te spremembe opravljene, vsak uporabnik pri prijavi v sistem uporablja Kerberos.

#### 4.2.3.2 Uporaba LDAPa in Kerberosa

OpenLDAP uporablja mrežni protokol SASL (angl. Simple Authentication and Security Layer), ki je namenjen varni povezavi med programom, ki zahteva avtentikacijo, ter sistemom za avtenticiranje, ki je v našem primeru Kerberos. Ideja je v tem, da se lahko avtentikacija zamenja s povsem drugačnim sistemom ali pa se uporablja več avtentikacij naenkrat (npr. Kerberos, mysql, plain text db, pam itd.). Avtentikacija imenika LDAP je izvedena s pomočjo GSSAPI/SASL (angl. General Security Services Application Program Interface), ki ni nameščen, zato ga je potrebno dodatno namestiti z namestitvijo datoteke `cyrus-sasl-gssapi-*.rpm` (Network Authentication, 2005).

Nato je potrebno dodati račun za LDAP strežnik (`ldap/userver.p-ng.si`) v Kerberos bazo in izvoziti v datoteko (`krb5.keytab`), ki jo za delovanje potrebuje LDAP strežnik:

```
kadmin> add -r ldap/userver.p-ng.si
Max ticket life [1 day]: »pritisni enter«
Max renewable life [1 week]: »pritisni enter«
Principal expiration time [never]: »pritisni enter«
Password expiration time [never]: »pritisni enter«
Attributes []: »pritisni enter«
kadmin> ext_keytab ldap/userver.p-ng.si
```

LDAP strežnik teče kot uporabnik in skupina `ldap`, datoteko `krb5.keytab` pa lahko bere le korenski (angl. `root`) uporabnik. Zato je potrebno spremeniti LDAP strežnik tako, da teče kot `root`, ali pa omogočiti skupini `ldap` branje datoteke `krb5.keytab`.

Sedaj se prepričamo ali pride do uporabe avtentikacije Kerberos pri prebiranju imenika LDAP.

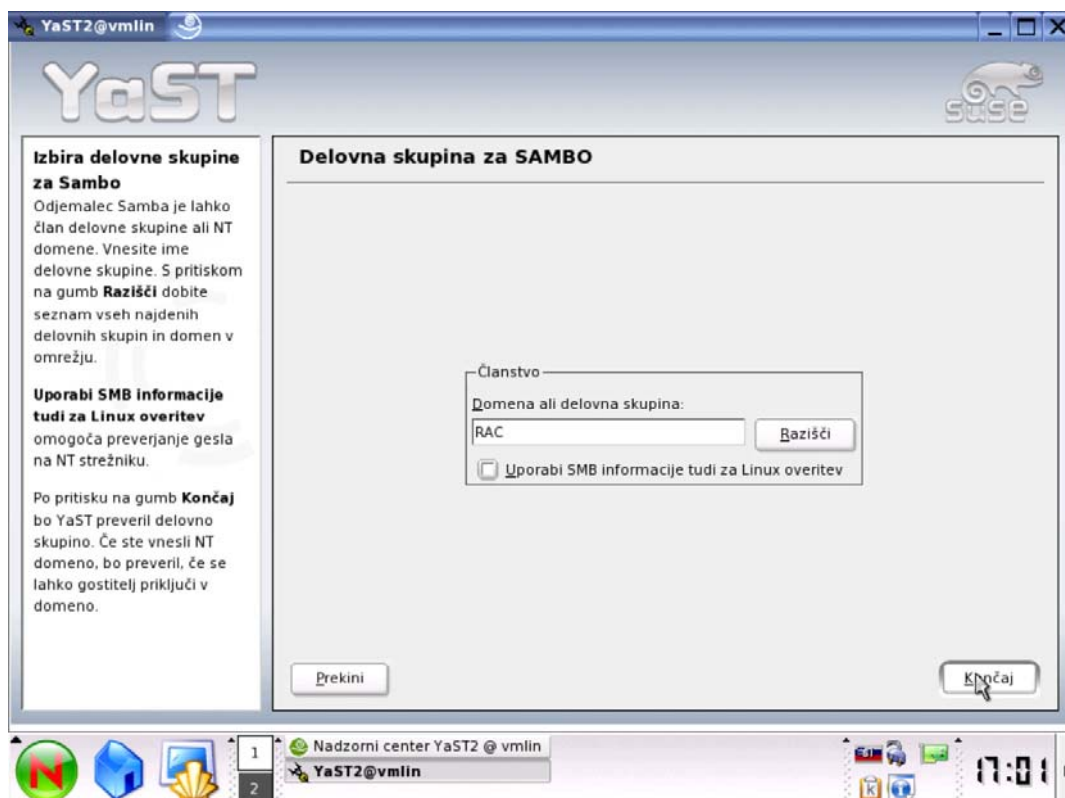
```
ldapsearch -b ou=people,dc=p-ng,dc=si '(uid=bojan) '
SASL/GSSAPI authentication started
SASL SSF: 56
SASL installing layers
...
# bojan, people, p-ng, si
```

```
dn: uid=bojan,ou=people,dc=p-ng,dc=si
uid: Bojan
cn: Bojan Korečič
...
```

Kot je razvidno iz zgornjega izpisa, ukaz `ldapsearch` izpiše sporočilo, da je začel SASL/GSSAPI avtentikacijo in v nadaljevanju izpiše podatke iz imenika. Tako vidimo, da je pri iskanju po imeniku LDAP, ki ga je zahteval LDAP odjemalec, v postopek stopil tudi Kerberos.

#### 4.2.4 Konfiguracija strežnika Samba

Strežnik Samba nastavimo tako, da najprej nastavimo odjemalec Samba, ki je v nadzornem središču YaST, pri tem se odpre okno, v katerega vpišemo domeno ali delovno skupino (slika 9) (Samba documentation collection, 2005).

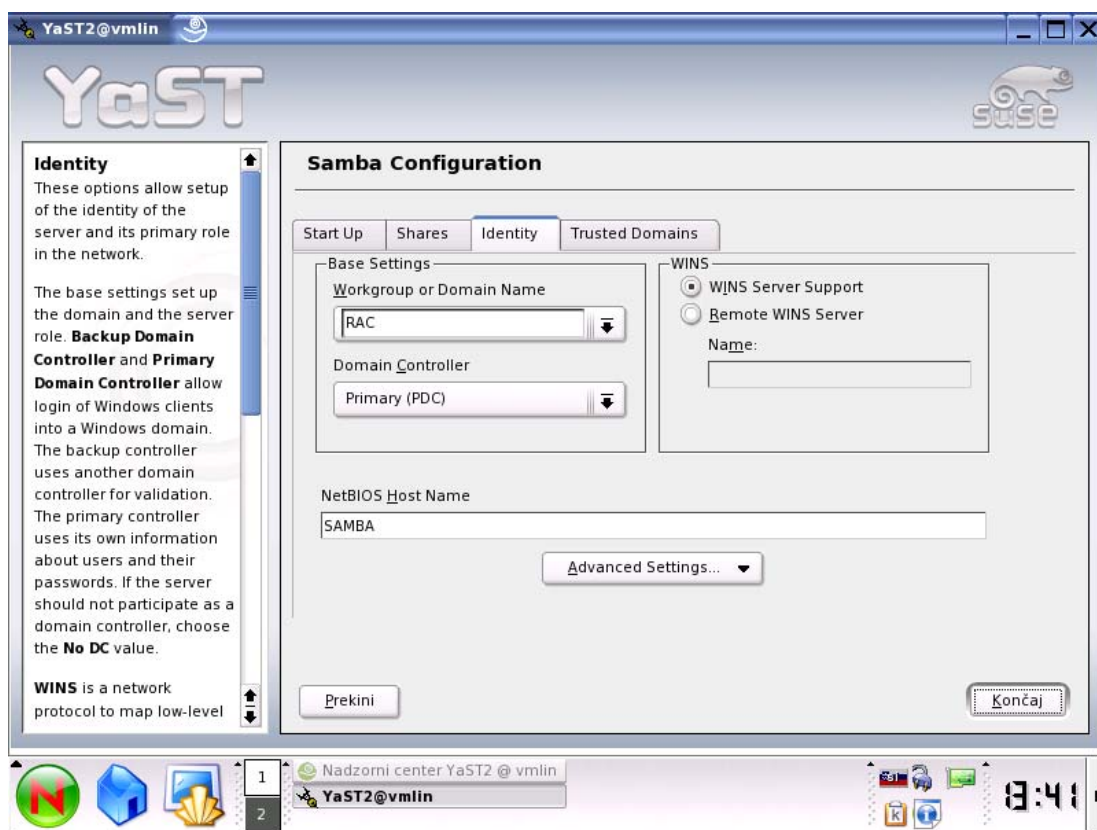


Slika 9: Izbira delovne skupine za odjemalec Samba

Sedaj v nadzornem središču YaST zaženemo strežnik Samba in odpre se nam okno, ki nas povpraša po namestitvi programa Samba, prav tako kot v prejšnjem primeru to

dovolimo. Čez nekaj trenutkov smo pred štirimi zavihki z nastavitvami za strežnik Samba (slika 10).

- S prvim zavihkom, Zagon (angl. Start-up), vključimo avtomatski zagon strežnika Samba ob zagonu računalnika.
- Z drugim zavihkom, Souporabljeni viri (angl. shares), spremenimo nastavitve souporabljenih virov. Onemogočimo, dodamo oziroma spremenimo vire glede na potrebe.
- S tretjim zavihkom, Identiteta (angl. Identity), spremenimo vrsto domenskega nadzornika. Kot glavni domenski nadzornik nastavimo PDC (angl. Primary Domain Controller). Prav tako je potrebno omogočiti podporo za WINS strežnik (angl. wins server support). V okno pod NetBIOS gostiteljsko ime pa vpišemo ime, pod katerim NetBIOS protokol prepozna ta računalnik.
- S četrtem zavihkom, Zaupanja vredne domene (angl. Trusted Domains), lahko dodajamo domene, ki jim lahko strežnik Samba zaupa.

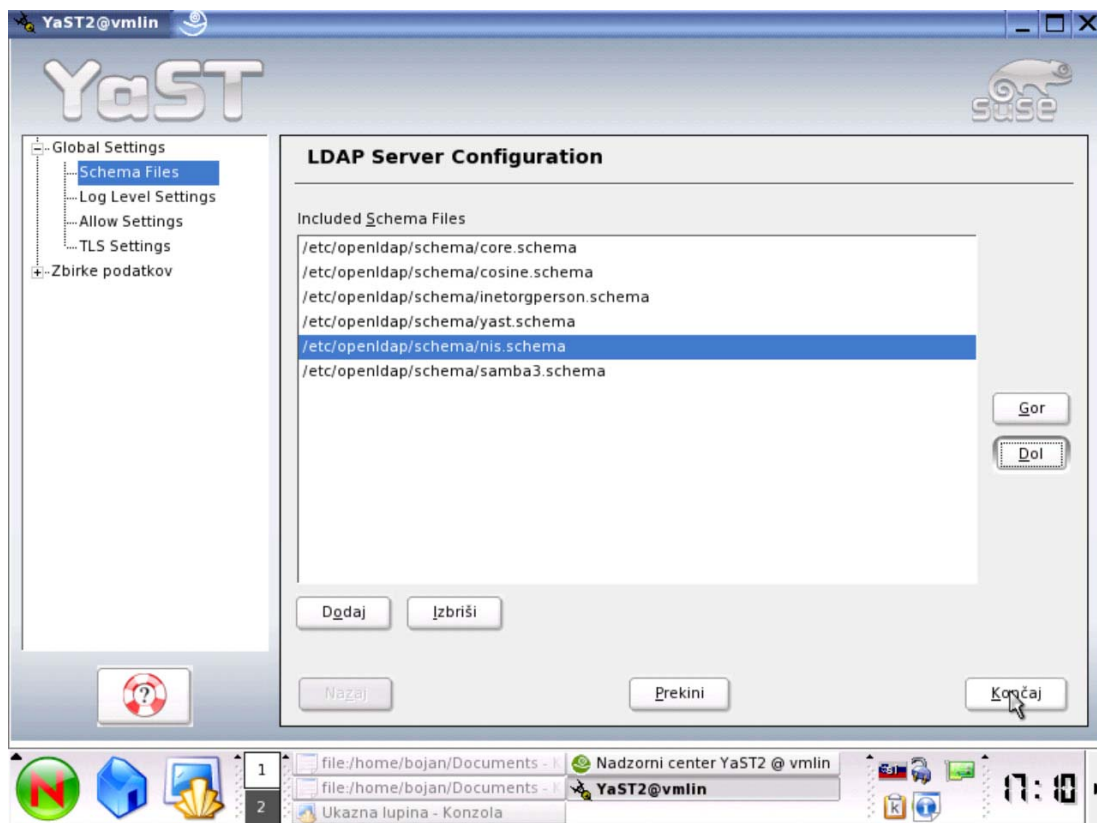


Slika 10: Nastavitve strežnika Samba

Sedaj je potrebno še nastaviti strežnik Samba tako, da bo komuniciral s strežnikom LDAP, tako da dodamo LDAP avtentikatorja.

Datoteko smb.conf, ki je nastavitvena datoteka za strežnik Samba, lahko uredimo iz nadzornega središča YaST, kot je bilo nakazano zgoraj, ali pa z urejevalnikom besedila (kate, kwrite, vi, vim, emacs ipd.).

Sedaj je potrebno še dodatno nastaviti strežnik LDAP oziroma razširiti strukturo imenika tako, da bosta strežnik Samba in strežnik LDAP lahko sodelovala. V nadzornem središču YaST zaženemo strežnik LDAP in preuredimo sheme imenika kot je prikazano na sliki 11. Nepotrebne sheme zberemo, tiste sheme, ki manjkajo, pa dodamo.



Slika 11: Nastavitev shem strežnika LDAP

Ko so sheme urejene, ponovno zaženemo strežnik LDAP in pogledamo, če strežnik Samba deluje:

```
rclldap restart  
smbclisment -L localhost -U%  
Domain=[RAC] OS=[Unix] Server=[Samba 3.0.4-SUSE]
```



```

Sharename Type      Comment
-----
IPC$      IPC      IPC Service (Samba 3.0.4-SUSE)
ADMIN$    IPC      IPC Service (Samba 3.0.4-SUSE)

```

```

Domain=[RAC] OS=[Unix] Server=[Samba 3.0.4-SUSE]

```

```

Server      Comment
-----
SAMBA      Samba 3.0.4-SUSE

```

```

Workgroup      Master
-----
MDKGROUP      SLOKARJI
P-NG          BOVEC
RAC           SAMBA
SES-NG        DHRV511J
WORKGROUP     LAVERDA

```

Če je izpis podoben zgornjemu, potem strežnik Samba deluje. Izpiše nam, kateri viri so na voljo na našem strežniku Samba in katere delovne skupine so še v omrežju.

Sedaj še pogledajmo, ali nam ukaz `net getlocalsid` vrne vrednost SID (angl. Security Identifier):

```

net getlocalsid
SID for domain SAMBA is: S-1-5-21-3434155592-
184838261-2880432530

```

Pomembno je, da pri izpisu dobimo SID. Če je izpis podoben zgornjemu, pomeni, da lahko strežnik Samba komunicira z operacijskim sistemom Windows ter da lahko nadaljujemo z nastavitvami.

#### 4.2.5 Namestitev in konfiguracija skript Idealx smbldap-tools

Da strežnik Samba shranjuje nastavitve v imenik LDAP, je potrebo imenik pravilno sestaviti. V ta namen so nam v veliko pomoč že pripravljene skripte z imenom smbldap-tools, ki jih je sestavilo podjetje Idealx.

Skripte smbldap-tools (smbldap-tools-0.9.1.rpm) namestimo in preden jih uporabimo, jih je potrebno še nastaviti, tako da se ujemajo z nastavitvami strežnikov Samba in LDAP. Nastavitev skript smbldap-tools izvedemo tako, da poženemo nastavitveno skripto ter sledimo navodilom in vprašanjem, ki se izpisujejo na zaslon in nanje odgovarjamo. Ko je nastavitev končana, so skripte smbldap-tools pripravljene za uporabo in popolnitev imenika LDAP.

#### 4.2.6 Popolnitev LDAP strežnika

Za popolnitev LDAP strežnika izvedemo skripto smbldap-populate, ki je del smbldap-tools skript.

```
./smbldap-populate
Populating LDAP directory for domain RAC (S-1-5-21-
2617803238-1940587940-114769750)
(using builtin directory structure)

entry cn=p-ng,cn=si already exist.
entry ou=people,cn=p-ng,cn=si already exist.
entry ou=group,cn=p-ng,cn=si already exist.
adding new entry: ou=Computers,cn=p-ng,cn=si
adding new entry: ou=Idmap,cn=p-ng,cn=si
adding new entry: uid=root,ou=people,cn=p-ng,cn=si
...
```

Iz zgornjega izpisa je razvidno, da skripta smbldap-populate vpiše nove objekte v imenik LDAP tako, da lahko objekt, ki je v našem primeru uporabniški račun, uporablja tudi strežnik Samba. Po popolnitvi ponovno zaženemo strežnik LDAP in preverimo, ali se lahko vključimo v domeno.

```
rclldap restart
Shutting down ldap-server           done
Starting ldap-server                 done
net rpc join -S SAMBA -U root%geslo
Joined domain RAC.
```

Sedaj je strežnik Samba nastavljen in lahko nadaljujemo z naslednjo nalogo, konfiguracijo uporabniškega profila.

#### 4.2.7 Konfiguracija prenosljivosti uporabniškega profila

Da vzpostavimo komunikacijo med Sambo in računalnikom z operacijskim sistemom Windows do take mere, da bo Samba shranjevala profil in da bodo nekateri imeniki gostovali na strežniku, je potrebno glede na potrebe uporabniškega profila oziroma datoteke `smb.conf` ustvariti potrebne imenike in urediti njihovo lastništvo.

Potrebni imeniki za vsakega uporabnika so:

- `profdata` – v tem imeniku so imeniki `AppData`, `MyPictures`, `MyDocuments`, ki gostujejo na strežniku,
- `profiles` – v tem imeniku so imeniki uporabniškega profila.

Za te vse te nastavitve sem sestavil skripto, ki nam olajša delo, saj le vpišemo `./profil »uporabnik«` in se avtomatsko kreirajo vse potrebne mape in določi njihovo lastništvo.

#### 4.2.8 Urejanje privzetega profila

Ko se nov uporabnik prvič prijavi v sistem in še nima svojega profila, ustvari strežnik njegov profil s pomočjo privzetega profila. Trenutni privzeti profil ne omogoča gostovanja map na strežniku, zato ga je potrebno preurediti.

Profil uredimo tako, da bodo tisti imeniki, ki postanejo v kratkem času veliki, domovali na strežniku in se ne bodo prenašali po omrežju ter ga po nepotrebem dodatno obremenjevali. Ti imeniki so:

- AppData,
- MyPictures,
- MyDocuments.

V operacijski sistem Windows se prijavimo kot lokalni administrator in pridemo do registra privzetega profila. To storimo tako, da zaženemo urejevalnik registra in uvozimo register.

Nato se premaknemo v del registra User Shell Folders, ki se nahaja v HKEY\_LOCAL\_MACHINE\Default\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\ in v desnem delu okna urejevalnika registra mora biti vsebina enaka, kot jo prikazuje slika 12.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AppData	REG_EXPAND_SZ	%USERPROFILE%\Application Data
Cache	REG_EXPAND_SZ	%USERPROFILE%\Internet Files
Cookies	REG_EXPAND_SZ	%USERPROFILE%\Cookies
Desktop	REG_EXPAND_SZ	%USERPROFILE%\Desktop
Favorites	REG_EXPAND_SZ	%USERPROFILE%\Favorites
History	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\History
Local AppData	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Application Data
Local Settings	REG_EXPAND_SZ	%USERPROFILE%\Local Settings
My Pictures	REG_EXPAND_SZ	%USERPROFILE%\My Documents\My Pictures
NetHood	REG_EXPAND_SZ	%USERPROFILE%\NetHood
Personal	REG_EXPAND_SZ	%USERPROFILE%\My Documents
PrintHood	REG_EXPAND_SZ	%USERPROFILE%\PrintHood
Programs	REG_EXPAND_SZ	%USERPROFILE%\Start Menu\Programs
Recent	REG_EXPAND_SZ	%USERPROFILE%\Recent
SendTo	REG_EXPAND_SZ	%USERPROFILE%\SendTo
Start Menu	REG_EXPAND_SZ	%USERPROFILE%\Start Menu
Startup	REG_EXPAND_SZ	%USERPROFILE%\Start Menu\Programs\Startup
Templates	REG_EXPAND_SZ	%USERPROFILE%\Templates

Slika 12: Register operacijskega sistema Windows

Sedaj spremenimo vrednosti ključev, kot je prikazano v tabeli 2.

**Tabela 2: Spremembe v registru operacijskega sistema Windows**

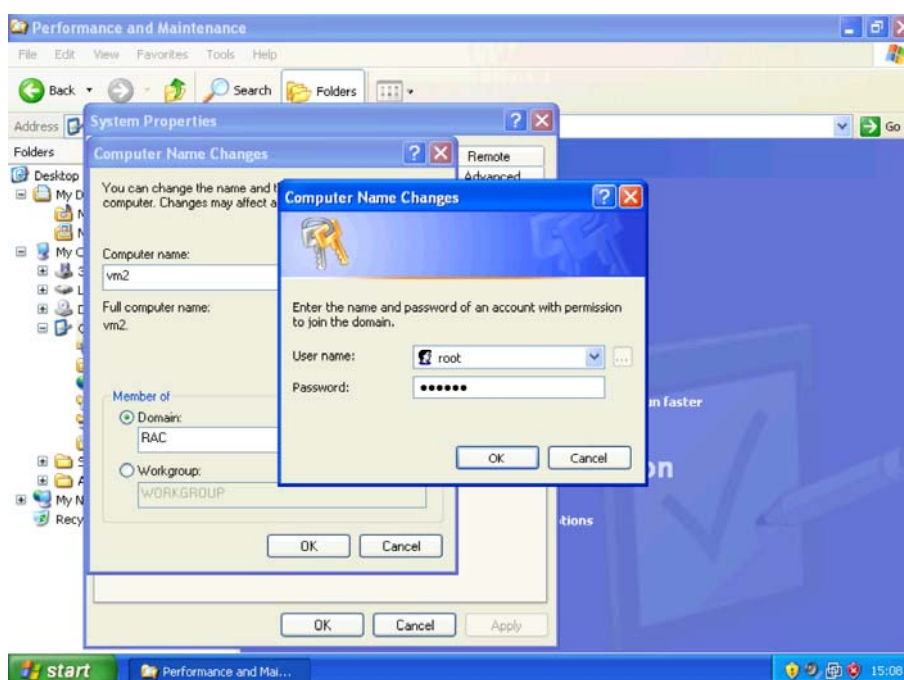
Ključ	Vrednost
Local AppData	%LOGONSERVER%\profdata\%USERNAME%\AppData
My Pictures	%LOGONSERVER%\profdata\%USERNAME%\MyPictures
Personal	%LOGONSERVER%\profdata\%USERNAME%\MyDocuments

Ko smo spremenili vse potrebne ključe, izvozimo register in privzeti profil skopiramo iz operacijskega sistema Windows na strežnik Samba v imenik /var/lib/samba/netlogon. S tem je privzeti profil nastavljen glede na naše potrebe.

#### 4.2.9 Vključitev računalnika v domeno

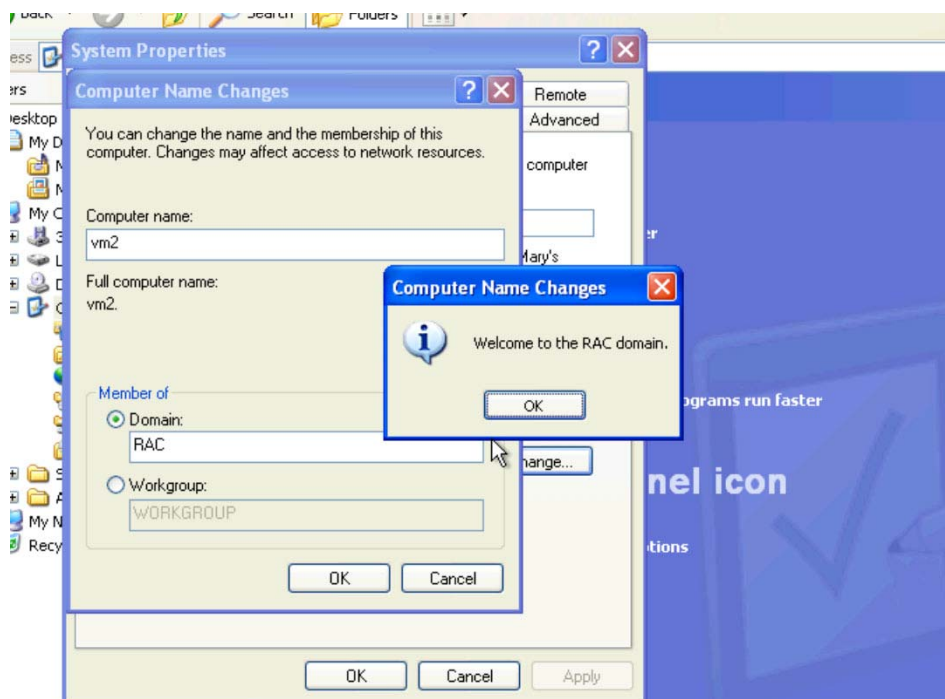
Zadnje dejanje postavitve sistema je, da vključimo vse odjemalce z operacijskim sistemom Windows v domeno.

Vključitev v domeno izvedemo na naslednji način Start -> My Computer -> Folders -> Control Panel -> Performance and Maintenance -> System -> Computer name -> Change... Vpišemo domeno, v katero se vključujemo, in v oknu, ki se pojavi, vpišemo korenskega uporabnika in njegovo geslo (slika 13).



**Slika 13: Vključevanje računalnika v domeno**

Ko se računalnik poveže v domeno, se na zaslonu pojavi sporočilo (slika 14).



Slika 14: Sporočilo ob vključitvi računalnika v domeno

S tem je računalnik vključen v domeno in naš sistem je postavljen.

### 4.3 Vzdrževanje sistema

Vzdrževanje takega sistema bi lahko razdelili na dva dela:

- vzdrževanje strežnika,
- vzdrževanje odjemalcev.

#### 4.3.1 Vzdrževanje strežnika

Tak sistem potrebuje zelo malo vzdrževanja. Edino, na kar moramo biti pozorni, je, da posodabljam vse strežnike in operacijski sistem s kritičnimi popravki ter skrbimo za varnost pred internetnimi napadi. Poleg tega pa je potrebno postoriti še ostala administrativno vzdrževalna dela kot so administracija prostora na disku, varnostno kopiranje (angl. backup), ipd.

Vzdrževalna dela in spremembe na strežnikih in operacijskem sistemu Linux lahko izvajamo prek treh poti:

- nadzornega središča YaST (angl. YaST Control Center),
- nadzornega središča KDE (angl. KDE Control Center),
- z ročnim spreminjanjem konfiguracijskih datotek.

#### 4.3.2 Vzdrževanje odjemalcev

Še največ napora zahteva posodabljanje operacijskega sistema Windows s kritičnimi in ostalimi nujnimi popravki. Deloma se da posodabljanje operacijskega sistema Windows rešiti z avtomatsko posodobitvijo, a kljub temu je potrebno, da vzdrževalec občasno pregleda vsakega odjemalca/računalnik posebej. Glede na to, da ima operacijski sistem Windows velike težave z virusi, črvi in ostalimi zlonamernimi programi, priporočamo, da se v sistem vključi antivirni program, ki bo vsaj deloma omilil težave, ki jih povzročajo zlonamerni programi. Prav tako je potrebno občasno posodobiti operacijski sistem Linux s kritičnimi popravki.

#### 4.4 Upravljanje sistema

Z upravljanjem sistema imamo v mislih manipulacijo z uporabniškimi računi in njihovih podatki. Ta obsega:

- dodajanje uporabniških računov,
- brisanje uporabniških računov,
- spreminjanje podatkov o uporabniku.

##### 4.4.1 Dodajanje uporabniškega računa

Za vsakega uporabnika, za katerega želimo, da ima dostop do operacijskega sistema Windows, je najprej potrebno narediti vse potrebno za gostovanje profila na strežniku in dodati uporabnika in njegovo geslo v imenik LDAP. Da bo ta uporabnik imel dostop tudi do operacijskega sistema Linux, ga je potrebno dodati še v Kerberos bazo:

```
./profil jan
./smbldap-useradd -m -a jan
```

```

./smbldap-passwd jan
Changing password for jan
New password : »vpiši geslo«
Retype new password : »ponovno vpiši geslo«
kadmin -l
kadmin> add jan
Max ticket life [1 day]: »pritisni enter«
Max renewable life [1 week]: »pritisni enter«
Principal expiration time [never]: »pritisni enter«
Password expiration time [never]: »pritisni enter«
Attributes []: »pritisni enter«
jan@P-NG.SI's Password: »vpiši geslo«
Verifying password: »ponovno vpiši geslo«

```

Sedaj ima uporabnik ne glede na to, na kateri operacijski sistem je naletel, možnost, da se vanj prijavi.

#### 4.4.2 Brisanje uporabniškega računa

Uporabnika in njegov profil je potrebno zbrisati iz imenika LDAP in iz Kerberos baze. To pa storimo na naslednji način:

```

./smbldap-userdel jan
kadmin -l
kadmin> del jan

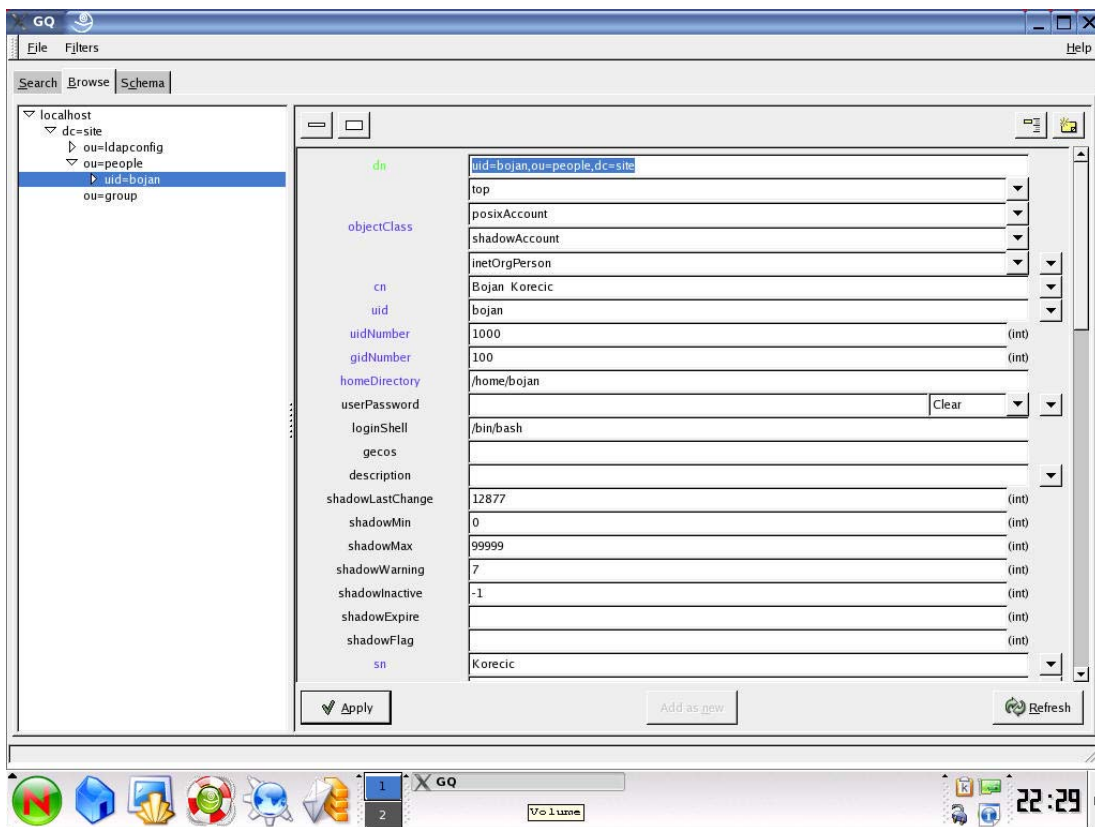
```

S prvim ukazom s pomočjo smbldap skripte zberšemo uporabniški profil in uporabniški račun iz imenika LDAP. Z drugim ukazom dostopamo do Kerberosa ter s tretjim ukazom zberšemo račun iz Kerberos baze.

#### 4.4.3 Spreminjanje podatkov o uporabniku

Osnovne podatke o uporabniku (naslov, ime, priimek ipd.) lahko spreminjamo v imeniku LDAP z različnimi LDAP odjemalci. Eden izmed njih z imenom GQ (slika 15) se nahaja že v sami SUSE distribuciji, le namestiti ga je potrebno.





Slika 15: Program GQ za urejanje podatkov o uporabnikih

Pri vpisu uporabnika v imenik LDAP s pomočjo smbldap skripte se vpišejo samo osnovni podatki o računu, kot so domači imenik, uporabniško ime in ostale nastavitve, ki jih potrebuje Samba. Vse ostale informacije o uporabniku (ime, priimek, naslov, kontakti, itd.) pa je potrebno dodatno vpisati v imenik LDAP.

Geslo uporabnika lahko spreminjamo na naslednji način:

```
./smbldap-passwd jan
Changing password for jan
New password : »vpiši geslo«
Retype new password : »ponovno vpiši geslo«
```

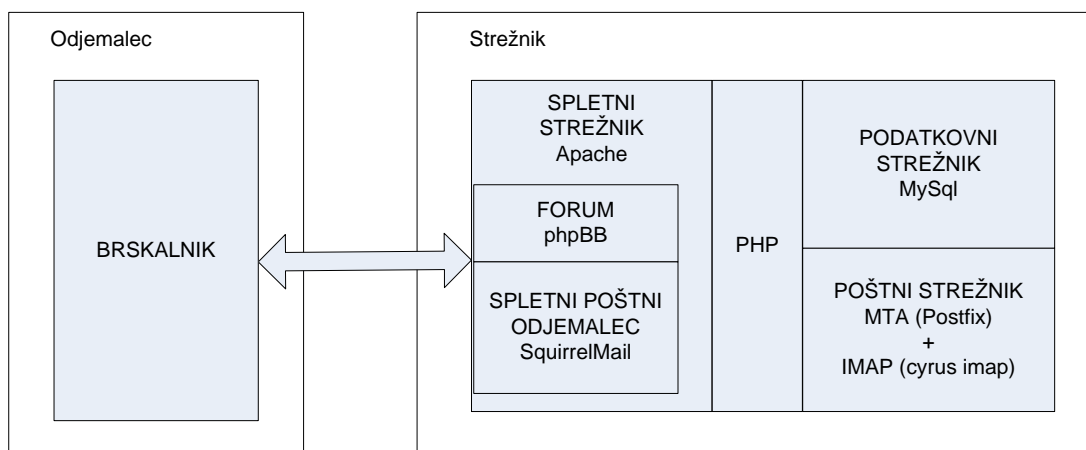
Spremembe gesla v Kerberos bazi naredimo na naslednji način:

```
kadmin -l
kadmin> passwd jan
jan@P-NG.SI's Password: »vpiši geslo«
Verifying password: »ponovno vpiši geslo«
```

## 5 DODATNI STREŽNIKI IN APLIKACIJE

V tem poglavju bomo predstavili nekatere dodatne strežnike in aplikacije, ki bi jih lahko ponudili študentom ter jim s tem omogočili boljše delo, učenje ter druženje. Dodatni strežniki in aplikacije so le predstavljeni in še niso bili postavljeni in testirani.

Politehnika Nova Gorica bi tako lahko ponudila vsakemu študentu elektronsko pošto, spletni prostor in forum za izmenjavo mnenj in sporočil. S tem bi se približala študentom in jim ponudila možnost za povečanje elektronskega opismenjevanja. Z brskalnikom (Internet Explorer, Mozilla FireFox, Opera, Konqueror ipd.) bi študenti dostopali do elektronske pošte s pomočjo spletnega poštnega odjemalca, izmenjevali mnenja preko foruma in imeli svoj spletni prostor za dokumente in interaktivne spletne strani. Shema take postavitve je predstavljena na sliki 16.



Slika 16: Shema postavitve dodatnih strežnikov in aplikacij

Strežniki in aplikacije so izbrane glede na popularnost, dostopnost in/ali so del distribucije Linux SuSE. Pri vsakem elementu sistema so navedene tudi alternative.

Preko spletnih strani lahko dosežemo, da so vse pomembne informacije vedno na voljo vsem, ki jih potrebujejo. V ta namen se uporabljajo spletni strežniki. Eden najboljših spletnih strežnikov je Apache HTTP Server, ki s podporo PHP omogoča gostovanje dinamičnih spletnih strani vsakemu uporabniku.

Uporaba baz podatkov je v današnjem informacijskem svetu zelo pogosta. Bazo marsikatera aplikacija, kot so forumi in spletni poštni odjemalci, potrebuje za svoje

delovanje. Linux SuSE tako nudi možnost uporabe bolj poznanih in prosto dostopnih baz, kot sta PostgreSQL in MySQL.

Elektronska pošta je v današnjih časih zelo razširjena in najbolj uporabljena internetna storitev. Da bi študentje imeli elektronsko pošto tudi na šolskem strežniku, je potrebno postaviti poštni strežnik in spletni poštni odjemalec. Tako je na Linuxu možno postaviti poštni strežnik z namestitvijo poštne posrednika (angl. mail transfer agent – MTA), ki usmerja in dostavlja elektronsko pošto. Poleg Postfixa je zelo razširjen tudi poštni posrednik Sendmail. IMAP (courier-imap, cyrus-imap, MS Exchange Server, MercuryMail 32 itd.) internetni protokol pa omogoča dostop do elektronske pošte.

## **5.1 Spletni strežnik**

### **5.1.1 Strežnik Apache**

Apache HTTP Server je odprtokodni HTTP spletni strežnik za sisteme, temelječe na Unixu (BSD, Linux, in UNIX), Microsoft Windows, Novell Netware in ostale platforme. Apache HTTP strežnik razvija in vzdržuje odprtokodna skupnost pod okriljem Apache Software Foundation. Pred desetimi leti je bil strežnik Apache edina odprtokodna alternativa spletnemu strežniku Netscape (sedaj poznan kot Sun Java Web Server).

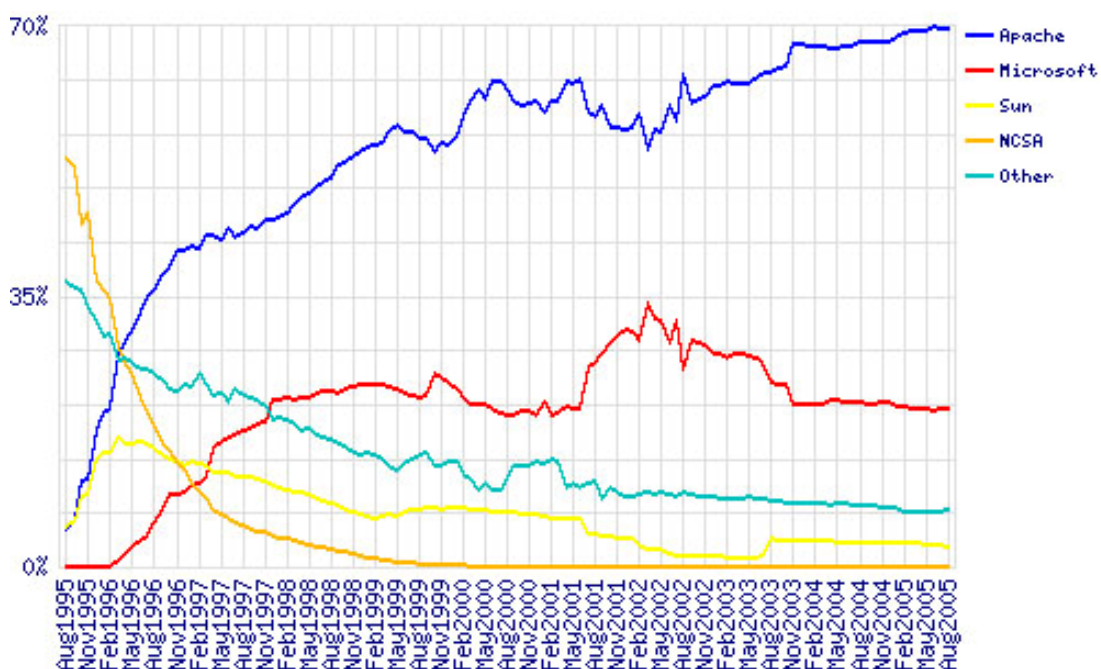
Strežnik Apache je izredno stabilen, zanesljiv in zmogljiv strežnik, ki se nahaja v vsaki distribuciji sistema Linux. Je visoko nastavljiv in modularen strežnik z veliko možnostmi. Od konkurenčnih spletnih strežnikov je predvsem hitrejši, učinkovitejši in manj obremenjuje celoten sistem. Nudi tudi virtualne strežnike za več 1000 domen ter odlično podporo novejšim aplikacijskim protokolom, ki jih nudijo vsi današnji aplikacijski strežniki.

Za strežnik Apache je napisanih niz različnih modulov, ki omogočajo integracijo aplikacije s strežnikom, od takih, ki omogočajo integracijo visokonivojskih programskih jezikov, kot so Perl, PHP, Python, Tcl, .Net, ASP, ISAPI, Java, do avtentikacijskih in varnostnih. Vse nastavitve in razširitve z moduli so izvedene s spremembami v datoteki httpd.conf ali v vključenih datotekah.

Podjetja in ustanove, kot so Amazon.com, Yahoo!, W3 Consortium, Financial Times, Apple, MP3.com, Stanford itd., uporabljajo strežnik Apache za svoje spletne storitve (Apache Overview HOWTO, 2005).

### 5.1.2 Konkurenca

Po podatkih podjetja Netcraft je Apache najbolj razširjen spletni strežnik na svetu (slika 17), saj 70% spletnih strežnikov uporablja strežnik Apache. Njegov največji konkurent je Microsoftov Internet Information Services (IIS) z 20%-deležem, sledi Sun Microsystems Sun Java Web Server z 2% ter ostali (October 2005 Web Server Survey, 2005).



Slika 17: Časovni pregled deležev nameščenih spletnih strežnikov

Nekaj ključnih faktorjev, ki so pripomogli, da je Apache tako uspešen:

- Apache licenca omogoča komercialno in nekomercialno uporabo strežnika,
- brezplačnost,
- modularna arhitektura: funkcionalnost strežnika Apache se brez večjih težav poveča ali zmanjša ter oblikuje strežnik glede na potrebe z moduli,
- prenosljivost: strežnik Apache teče na skoraj vseh operacijskih sistemih,

- ponaša se z veliko robustnostjo, varnostjo, stabilnostjo in hitrostjo.

### 5.1.3 Spletni imenik uporabnika

Na sistemih z več uporabniki je vsakemu uporabniku omogočeno, da ima svojo spletno stran. Uporabnik, ki bi rad spletno stran objavil na internetu, jo shrani v imenik `public_html`, ki je v njegovem domačem imeniku. Strežnik Apache pa poskrbi, da ko obiskovalec vpiše spletni naslov, npr. `http://example.com/~username/`, dostopa do uporabnikovih spletnih strani, ki niso v korenskem imeniku strežnika, ampak zunaj njega.

To je v strežniku Apache omogočeno z modulom `mod_userdir` in nastavitvijo usmerjevalnika `UserDir` na imenik `public_html`, kot je razvidno iz spodnjih vrstic.

```
<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>
```

To omogoča, da se spletni naslov `http://example.com/~bojan/file.html` pretvori v `/home/bojan/public_html/file.html`, kar pomeni, da se strani berejo in strežejo iz uporabniškega imenika.

Uporabniku je tudi omogočeno, da omeji dostop do svojih strani z geslom tako, da to nastavi v datoteki `.htaccess` (HTTP Server Documentation, 2005).

## 5.2 Programski jezik PHP

Strežnik Apache brez dodatnih nastavitvev ne omogoča serviranja dinamičnih strani, ki so v zadnjem času postale nujne pri vsaki internetni strani, saj omogočajo večjo prilagodljivost vsebine. Po podatkih podjetja Netcraft je PHP najbolj popularen skriptni jezik za dinamične strani (April 2002 Web Server Survey, 2005).

PHP (Hypertext Preprocessor) je široko razširjen odprtokodni skriptni jezik, ki je še posebej primeren za razvoj spletnih strani, saj ga lahko uporabljamo znotraj HTML strani. Lahko ga primerjamo z Microsoftovim ASP/VBScript/JScript sistemom, Sun Mycrosystemovim JSP/Java sistemom in CGI/Perl sistemom. Sintaksa PHP-ja je podobna tisti iz jezikov C, Java in Perl in se ga je preprosto naučiti. Glavni cilj jezika

je omogočiti hiter razvoj dinamičnih spletnih strani, z njim pa je mogoče opraviti še mnogo drugih stvari (PHP, 2005).

PHP teče na večini operacijskih sistemov, kot so UNIX, Linux, Windows in Mac OS X, in lahko vzajemno deluje z večjimi spletnimi strežniki, kot sta Apache in IIS.

PHP je zgrajen modularno. Med mnogimi drugimi moduli so podprti tudi naslednji:

- podatkovne baze, kot so Oracle, MS-SQL server, ODBC interface, MySQL, mSQL, PostgreSQL itd.,
- XML podpora,
- prenos datotek: FTP,
- http,
- podpora imenikom: LDAP,
- pošta: IMAP, POP3, NNTP,
- kreator PDF dokumentov.

### **5.3 Spletni poštni odjemalec**

Spletni poštni odjemalec (angl. webmail) je spletna aplikacija, ki omogoča branje in pisanje elektronske pošte z uporabo spletnega brskalnika. Elektronsko pošto največkrat ponujajo internetni ponudniki in podjetja, ki se ukvarjajo z računalništvom oziroma internetom. Večji ponudniki elektronske pošte s spletnim poštnim odjemalcem so Hotmail, Yahoo! in Gmail, na Slovenskem pa Email.si.

Prednosti spletnega poštnega odjemalca so:

- ni potreben poštni odjemalec (Outlook Express, Mozilla Thunderbird itd.),
- sporočil ni potrebno prenašati na računalnik,
- ni potrebno spremeniti elektronskega naslova ob spremembi internetnega ponudnika,

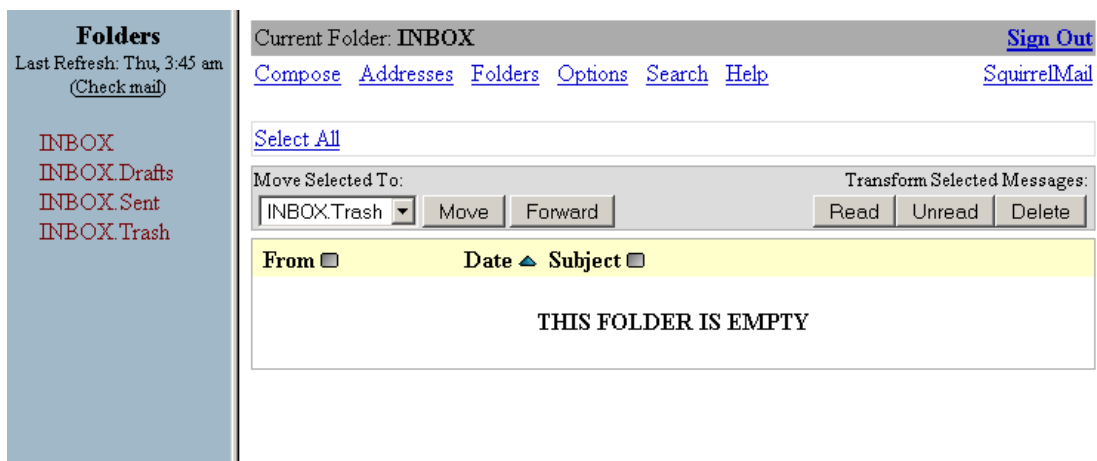
- dostop od kjerkoli itd.

### 5.3.1 Poštni odjemalec SquirrelMail

SquirrelMail je standardiziran spletni poštni odjemalec napisan v PHP4. Vsebuje PHP podporo za protokola IMAP in SMTP in vse strani so napisane v čisti HTML 4.0 kodi. Ima malo zahtev in ga je zelo lahko namestiti in nastaviti. SquirrelMail ima vse funkcije, ki jih mora imeti odjemalec elektronske pošte, vključno z MIME (angl. Multipurpose Internet Mail Extension) podporo, imenikom, filtrom nezaželene pošte, posredovanjem pošte, upravljanjem z mapami itd. (SquirrelMail, 2005). Njegov uporabniški vmesnik vidimo na sliki 18.

Zahteve za postavitev SquirrelMail so:

- UNIX/Linux ali Windows,
- IMAP4 rev1,
- PHP4,
- spletni strežnik z integracijo PHP4 (zaželen Apache).



Slika 18: Uporabniški vmesnik spletnega poštnega odjemalca SquirrelMail

## 5.4 Internetni forum

Internetni forum je spletna aplikacija, namenjena diskusijam, razpravam, sporočilom, podajanju mnenj itd. Prvi forumi so nastali okoli leta 1996, sledile so novičarske

skupine in oglasne deske, ki so se razširile v 80-ih in 90-ih letih. V zadnjem času pa je najbolj razširjen forum oziroma oglasna deska phpBB (Internet forum, 2005).

#### 5.4.1 Forum phpBB

Forum phpBB je odprtokodna oglasna deska oziroma forum, ki ima uporabniku prijazen vmesnik ter enostavno administratorsko ploščo. Temelji na jeziku PHP in na eni izmed podatkovnih baz MySQL, MS-SQL, PostgreSQL ali Access/ODBC (phpBB, 2005).

Nekatere značilnosti foruma phpBB:

- podpira popularne podatkovne baze,
- neskončno tem,
- večjezikovni vmesnik,
- privatni in javni forumi,
- zmogljiv iskalnik,
- sistem zasebnih sporočil itd.

Primer uporabe foruma phpBB vidimo na sliki 19.

Forum	Teme	Prispevkov	Zadnja objava
<b>Klub Kanalske Mladine</b>			
 <b>Kanalčan</b> Edini časnik, ki se ga pije Moderator <a href="#">editor</a>	12	207	11.10.05 9:00 <a href="#">editor</a> ➡
 <b>O klubu</b> Povejte kaj vas moti in kaj veseli pri KKM Moderator <a href="#">editor</a>	12	502	06.10.05 13:20 <a href="#">Ernesto Sanchez</a> ➡
 <b>O forumu</b> Novosti na forumu, predlogi kaj izboljšati Moderator <a href="#">editor</a>	8	157	02.04.05 18:26 <a href="#">editor</a> ➡
 <b>O strani</b> Vse o internetni strani KKM-a Moderator <a href="#">webmaster</a>	5	72	26.09.05 11:31 <a href="#">editor</a> ➡
 <b>Upravni odbor</b> Forum namenjen članom upravnega odbora. POZOR: Forum vidite samo člani UO! Moderator <a href="#">predsednik</a>	36	661	17.10.05 12:55 <a href="#">editor</a> ➡
 <b>Moderatorji</b> Forum namenjen moderatorjem na KKM forumu! POZOR: Forum vidite le moderatorji!	6	59	06.04.05 21:31 <a href="#">editor</a> ➡

Slika 19: Primer uporabe foruma phpBB



## 6 ZAKLJUČEK

Opisani strežniški sistem je bil poskusno postavljen in testiran na enem izmed računalnikov na Politehniko Nova Gorica, tako da je nadaljnji korak namestitev, testiranje, uporaba, upravljanje in vzdrževanje strežniškega sistema v računalniški učilnici ter morebitna nadgradnja.

Predlagani sistem omogoča avtentikacijo in prijavo odjemalcev oziroma računalnikov v sistem. Avtentikacija in prijava sta izvedeni s pomočjo imenika LDAP in strežnika Kerberos za odjemalce z operacijskim sistemom Linux. Avtentikacija in prijava za odjemalce z operacijskim sistemom Windows sta izvedeni s pomočjo imenika LDAP in strežnika Samba. Pomanjkljivost tega sistema je, da imamo dve bazi z gesli, eno v Kerberos bazi za potrebe odjemalcev z operacijskim sistemom Linux in drugo v imeniku LDAP za potrebe odjemalcev z operacijskim sistemom Windows. Vsekakor je priporočljivo, da se to v prihodnje reši tako, da bo zadoščala ena sama baza z gesli. S prijavo odjemalca z operacijskim sistemom Linux pridobimo to, da lahko uporabnik dostopa do svojih map, ki so na strežniku. S prijavo v sistem odjemalca z operacijskim sistemom Windows pa pridobimo to, da se uporabniški profil prenese na delovni računalnik in tam ima uporabnik svoje delovno okolje. Nekateri imeniki pa so še vedno na strežniku in se ne prenašajo z uporabniškim profilom. Pri odjavi iz sistema se uporabniški profil prenese nazaj na strežnik in s tem smo dosegli, da ima vsak študent svoje delovno okolje ne glede na to, na katerem računalniku dela.

Tak sistem tudi omogoča ugotavljanje lastništva datotek in imenikov, kar do sedaj ni bilo mogoče, ter s tem opominjanje študentov ob nenamenski uporabi računalnika, saj se je pri pregledu računalnikov izkazalo, da je na računalnikih veliko datotek, ki niso namenjene izvajanju študijskega programa, ampak izključno zabavi med poukom.

### 6.1 Nadgradnja sistema

Zgrajeni sistem bi bilo potrebno še izpopolniti, tako da bi pridobili večjo preglednost nad njim ter lažje upravljanje. Pri tem imamo v mislih predvsem oblikovno ureditev nekaterih nastavitvenih datotek, kot so `smb.conf`, `sldap.conf` itd.

Nadgradnja sistema, ki sem jo tudi sam pogrešal že med študijem, je v tem, da bi bil omogočen dostop do sistema oziroma vsaj do datotek tudi prek interneta oziroma od doma. S predstavljenimi strežniki in aplikacijami smo nakazali, kako bi lahko sistem razširili in povečali njegove zmožnosti. Tak sistem bi bilo potrebno še pred tem namestiti in testirati. S tem bi se Politehnika Nova Gorica še bolj približala svojim študentom.

## **6.2 Sklep**

Dosedanji sistem v računalniški učilnici Politehnike Nova Gorica ni omogočal osebnega profila uporabnika, kar je pomenilo, da je do mojih podatkov oziroma datotek lahko dostopal vsak in z njimi počel vse, kar je želel. Sedaj je pred nami strežniški sistem, ki na enem mestu shranjuje podatke o vseh študentih ter jim dovoli vstop v sistem in dostop do njihovih datotek ne glede na to, za kateri računalnik sedejo, ko pridejo v računalniško učilnico. S postavitvijo dodatnih strežnikov in aplikacij pa bi zmožnosti sistema še povečali.

Če bi tak sistem imela računalniška učilnica Politehnike že takrat, ko sem jaz vstopil vanjo, bi bilo delo na računalnikih prijetnejše, saj bi imel eno skrb manj in po moji meri prilagojeno ter prijaznejše delovno okolje.

V prihodnosti pa bo morda operacijski sistem GoogleOS omogočal, da bomo kjerkoli na svetu na vsakemu računalniku, s katerim bomo prišli v stik, imeli enako delovno okolje.

## 7 LITERATURA

**Apache Overview HOWTO.** Pridobljeno 11.10.2005 s svetovnega spleta:

<http://www.tldp.org/HOWTO/Apache-Overview-HOWTO.html>

**April 2002 Web Server Survey.** Pridobljeno 11.10.2005 s svetovnega spleta:

[http://news.netcraft.com/archives/2002/04/april\\_2002\\_web\\_server\\_survey.html](http://news.netcraft.com/archives/2002/04/april_2002_web_server_survey.html)

**Anderson, P., Barnes, D., Van Dijk, D., Griffa, M., Gonzato, G., Haible, B., Johnson, M., Kerr, P., Kiesling, R., Komarinski, M., Langfeldt, N., Martin, P., Merrill, D., Meunier, F., Peterlin, P., Raymond, E., Schoen, S., Taylor, G., Trümper, W., Ward, B., Zawodny, J., Zhang, Y. (2002).** Kako v Linuxu? : priročnik za delo z operacijskim sistemom Linux. Ljubljana: Pasadena.

**AOL/National Cyber Security Alliance (2004).** Online Safety Study. Pridobljeno 7.8.2005 s svetovnega spleta:

[http://www.staysafeonline.info/news/safety\\_study\\_v04.pdf](http://www.staysafeonline.info/news/safety_study_v04.pdf)

**Cvjetović, S., Košir, A., Maurer, R., Peterlin, P., Samastur, M. (2000).** LINUX z namizjem KDE: priročnik za delo z operacijskim sistemom Linux. Ljubljana: Pasadena.

**Garman, J. (2003).** Kerberos: The Definitive Guide. Sebastopol: O'Reilly & Associates.

**HTTP Server Documentation.** Pridobljeno 11.10.2005 s svetovnega spleta:

[http://httpd.apache.org/docs/2.0/howto/public\\_html.html](http://httpd.apache.org/docs/2.0/howto/public_html.html)

**Internet forum.** Wikipedia, the free encyclopedia. Pridobljeno 11.10.2005 s svetovnega spleta: [http://en.wikipedia.org/wiki/Internet\\_forum.html](http://en.wikipedia.org/wiki/Internet_forum.html)

**Jay Ts, J., Eckstein, R., Collier-Brown, D. (2003).** Using Samba. Druga izdaja.

Pridobljeno 7.8.2005 s svetovnega spleta:

[http://www.samba.org/samba/docs/man/using\\_samba/ch01.html](http://www.samba.org/samba/docs/man/using_samba/ch01.html)

**Korečič, B. (2005).** Postavitev mrežnega sistema v računalniški učilnici, Končno poročilo praktičnega usposabljanja. Nova Gorica: Politehnika Nova Gorica, Visoka poslovno-tehniška šola.

**Linux.** Wikipedija, prosta enciklopedija. Pridobljeno 11.4.2005 s svetovnega spleta:  
<http://sl.wikipedia.org/wiki/Linux>

**Lugos - Kaj je Linux.** Pridobljeno 11.4.2005 s svetovnega spleta:  
<http://www.lugos.si/linux>

**Microsoft Windows.** Wikipedia, the free encyclopedia. Pridobljeno 7.8.2005 s svetovnega spleta: [http://en.wikipedia.org/wiki/Microsoft\\_Windows](http://en.wikipedia.org/wiki/Microsoft_Windows)

**Mitnick, K. (2004).** Time to live on the network. Pridobljeno 7.8.2005 s svetovnega spleta: <http://www.avantgarde.com/xxxxttl.pdf>

**Network Authentication - Kerberos.** SuSE help - center. Integrirana pomoč v SUSE Linuxu.

**October 2005 Web Server Survey.** Pridobljeno 11.10.2005 s svetovnega spleta:  
[http://news.netcraft.com/archives/2005/10/04/october\\_2005\\_web\\_server\\_survey.htm](http://news.netcraft.com/archives/2005/10/04/october_2005_web_server_survey.htm)

**Peeling, N., Satchell, J. (2001).** Analysis of the Impact of Open Source Software. Pridobljeno 7.8.2005 s svetovnega spleta:  
[http://www.govtalk.gov.uk/documents/QinetiQ\\_OSS\\_rep.pdf](http://www.govtalk.gov.uk/documents/QinetiQ_OSS_rep.pdf)

**PHP.** Wikipedija, prosta enciklopedija. Pridobljeno 11. 10. 2005 s svetovnega spleta:  
<http://sl.wikipedia.org/wiki/PHP.html>

**phpBB.** Pridobljeno 11. 10. 2005 s svetovnega spleta: <http://www.phpbb.org/>

**Samba documentation collection.** Pridobljeno 11. 4. 2005 s svetovnega spleta:  
<http://us2.samba.org/samba/docs/man>

**Sodnik, J. (2002).** Preprost protokol za dostop do imenika LDAP. Diplomsko delo. Ljubljana: Univerza v Ljubljani, Fakulteta za elektrotehniko.

**SquirrelMail - Webmail for Nuts!** Pridobljeno 11.10.2005 s svetovnega spleta:  
<http://www.squirrelmail.org/about.php>

**Unix.** Wikipedija, prosta enciklopedija. Pridobljeno 7.8.2005 s svetovnega spleta:  
<http://sl.wikipedia.org/wiki/UNIX>

**Welsh, M., Hughes, P., Bandel, D., Beletsky, B., Dreilinger, S., Kiesling, R.,  
Liebovitch, E., Pierce H.** (1999). Namestitev in začetek dela z Linuxom. Prevod in  
priredba: R. Maurer. Pridobljeno 7.8.2005 s svetovnega spleta:  
<ftp://ftp.lugos.si/doc/install-guide-sl/install-guide-3.2-sl.pdf>