Verificarea clientului NIS

1.) ypcat passwd - tipăreste baza de date cu parola NIS; se poate lansa pe client pentru a verifica dacă baza de date este actualizată (contine si noii utilizatori creati pe server).

2.) ypmatch nume_utilizator passwd - afisează doar parola lui nume_utilizator; bineinteles, aceasta e criptată.

3.) ypmatch nume_utilizator group - afisează numele grupului din care fac parte nume_utilizator, parola de grup si identificatorul de grup.

4.) ypcat -x - afisează lista hărtilor NIS pe care serverul le pune in comun.

Configurarea si recompilarea nucleului S.O. (kernel)

Kernel-ul este nucleul sistemului de operare si conduce functionarea unitătii centrale, gestionează memoria sistemului, controlează accesul la unitatea de disc si contine drivere care ne ajută să interactionăm cu sistemul si să folosim hardware-ul si perifericele atasate calculatorului.

De cele mai multe ori recompilarea kernel-ului este necesară:

1.) Din cauza aparitiei de hardware nou care nu este suportat sau este suportat slab de către kernel-ul deja existent pe sistem.

2.) De asemenea se poate ca o versiune mai nouă a kernel-ului să repare un bug existent sau să repare o gaură de securitate.

3.) Pentru a configura kernel-ul să suporte un anumit procesor (mărind astfel performanta sistemului). Kernel-ul implicit rezultat la instalarea Linux, de obicei e făcut să meargă pe mai multe tipuri de procesoare, nefiind configurat specific pentru procesorul pe care il avem, deci nu beneficiază de avantajele pe care un anumit procesor mai nou le are. Deci o configuratie specifică CPU-ului nou poate creste performantele sistemului sau nu.

4.) Kernel-ul implicit de asemenea contine optiuni pe care le dorim (de exemplu suport pentru Samba) sau contine optiuni de care nu avem nevoie si care se pot elimina. Configurarea si recompilarea nucleului ne permit să eliminăm caracteristicile nedorite si să adăugăm caracteristicile dorite si folositoare.

5.) Kernel-ul implicit contine suport pentru o varietate largă de hardware. Pentru a-l face mai mic ca dimensiune putem elimina suportul

pentru hardware-ul pe care nu il am. Vom obtine din nou o crestere a performantei sistemului.

6.) Dacă la instalare aveam hardware pentru care nu exista suport (nu era recunoscut de kernel) sau era suportat partial, atunci vom dori, in momentul in care apar driver-ele noi, să le includem in kernel.

Actualizarea kernel-ului se referă la obtinerea unei versiuni mai noi de kernel (> 20 MB) sau doar a unor patch-uri (petice), urmată de reconfigurare, recompilare, instalare si rebootarea sistemului.

Configurarea sistemului se referă la configurarea unui kernel existent, recompilarea lui, instalarea noului kernel si rebootarea sistemului.

Comenzi utile *uname* :

1.) *uname* -r - afisează versiunea kernel-ului
uname -a - afisează toate informatiile
uname -m - afisează numele hardware al maşinii
uname -n - afisează numele calculatorului
uname -s - afisează sistemul de operare (linux)
uname -p - afisează tipul procesorului
uname -v - afisează versiunea Linux

2.) *rpm - qa | egrep kernel* - afisează toate pachetele RPM instalate care nu au legături (dependente) cu kernel-ul

3.) Numerotarea versiunii de kernel respectă sablonul
versmajora.versminora.nrpatch

Un nr. de versiune minoră par indică o versiune stabilă, iar unul impar, o versiune "in lucru". Ex: avem versiunea 2.4.9 stabilă, iar versiunea in lucru 2.5; cand schimbările din 2.5 sunt considerate stabile, preferabil se va trece la versiunea 2.6 sau la versiunea 3.0 (dacă schimbările sunt mai mari).

CURS 14

Recompilarea kernel-ului (continuare)

Recompilarea kernel-ului presupune următoarele etape:

1) Descărcarea şi instalarea sursei noului kernel
2) Configurarea kernel-ului (K)
3) Compilarea K
4) Construirea si instalarea modulelor de K (dacă există)
5) Instalarea K si setarea progr. incărcător (boot loader) GRUB

Etapele mai detaliat:

1) Descărcarea şi instalarea sursei noului kernel

a) se poate descărca o nouă versiune de kernel de la http://www.kernel.org/mirrors

Dacă avem deja descărcat kernel-ul, putem descărca patch-urile la acesta (numărul patch-ului este al 3-lea din numărul de versiune al kernel-ului, de ex. pentru 2.4.18 nr. patch-ului este 18 si este suficient); dacă apare patch-ul 19 sau unul ulterior, descărcăm patch-ul, nu tot kernel-ul.

b) despachetăm kernel-ul respectiv patch-ul cu comanda
gunzip -c linux-2.4.8.tar.gz | tar-xf-
dezarhivează kernel-ul vers. 2.4.8 intr-un subdirector al directorului curent, numit linux-2.4.8
comanda

bunzip2 -c patch-2.4.09.bz2 | patch –p0

dezarhivează arhiva bz si aplică patch-ul. Pentru a doua comandă, trebuie să avem programul bunzip2 instalat.

2) Configurarea kernel-ului se poate face in mod text sau în mod grafic.

Prima variantă **make menuconfig**
A doua variantă **make xconfig**
A treia variantă de configurare este tot in mod text, in stilul wizard, la fiecare etapă trebuie să selectăm optiunea pe care dorim să o configurăm. Se face cu

make config

3) Compilarea si instalarea unui nou kernel

a) in directorul in care s-a dezarhivat kernel-ul in ex. nostru
$ HOME | linux_2.4.8
dăm comenzile

make dep
make bzImage

b) dacă s-a optat pentru un kernel modular sau hibrid, se dă comanda

make modules

c) facem o copie de sigurantă a kernel-ului vechi

d) copiem noul kernel la locul său

cp linux-2.4.8/arch/i386/boot/bzImage /boot/vmlinuz-2.4.9

e) in cazul in care am optat pentru un kernel modular, instalăm si modulele cu

make modules_install

f) dacă avem nevoie de un disc RAM (de obicei in cazul in cazul harddisk-urilor SCSI) il scriem cu

mkinitrd –v /boot/initrd-2.4.9.img 2.4.9

g) configurarea programelor incărcător GRUB (boot loader)

In fisierul /boot/grub/grub.conf

scriem liniile

title Test kernel (2.4.9)

root (hda2)

kernel /vmlinuz-2.4.9 ro root=/dev/hda2

initrd /initrd-2.4.9.img

bineinteles in loc de /dev/hda2 trebuie pusă pozitia de pe care bootează S.O., iar in loc de 2.4.9, nr. de versiune al kernel-ului instalat. La fel si la punctele 3.) si 4.)

h) Rebootarea sistemului

La repornirea sistemului vom avea o nouă linie cu numele

Test kernel (2.4.9), pe care trebuie s-o selectăm pentru a boota sistemul cu noul kernel.

LDAP (Lightweight Directory Access Protocol)

LDAP este un set de protocoale "open source", folosite pentru a accesa informatii stocate centralizat prin intermediul unei retele. Este baza pentru standardul X.500 de "directory sharing", dar e mai putin complex si consumă mai putine resurse.

Informatiile stocate de LDAP sunt organizate ierarhic folosind directoare. Aceste directoare pot stoca o mare varietate de informatii si pot fi chiar folosite intr-o manieră similară cu NIS, pentru a permite oricui accesul la contul propriu de pe orice masină din reteaua LDAP.

LDAP e folosit de multe ori doar pentru a stoca informatii de tipul unui director virtual cu numere de telefon, permitând utilizatorilor să afle informatii despre alti utilizatori. Faptul că LDAP contine mecanisme de

replicare a acestor "cărti de telefon" cu alte servere răspândite prin lume face ca informatia să poată fi global distribuită.

LDAP este un sistem client-server. Partea de server stochează diverse baze de date in formate diferite, fiecare optimizată pentru operatiile care se pot efectua asupra ei.

Clientul LDAP poate să chestioneze (query) serverul care, dacă nu contine răspunsul local, il poate trimite la un server de pe un nivel superior in ierarhia LDAP, care are răspunsul.

Dacă aplicatia client LDAP incearcă să modifice bazele de date, atunci serverul verifică dacă are aceste drepturi si in cazul că da, efectuează modificarea.

LDAP contine suport pentru SSL (Secure Socket Layer) si TLS (Transport Layer Security), IP6, protocolul IPC (Inter Process Comunication), are o interfată de programare a aplicatiilor (API-Application Programming Interface) bine definită, suport pentru LDIF (LDAP Data Interchange Format), suport pentru NSS (Name Service Switch), suport pentru autentificare PAM, suport pentru limbajul PHP, suport pentru sistemul de autentificare Kerberos.

Utilitare si demoni LDAP

Pachete necesare :

- openldap - contine bibliotecile necesare pentru rularea serverului openldap si a aplicatiilor client
- openldap-clients - contine utilitare din linia de comandă, pentru accesarea si modificarea directoarelor LDAP
- openldap-server - contine serverele si alte utilitare necesare pentru configurarea serverului LDAP

Există 2 servere in pachetul openldap-server :

- Standalone LDAP Daemon (/usr/sbin/slapd)
- Standalone Update Replication Daemon (/usr/sbin/slurpd)

Primul este serverul LDAP, al doilea e folosit pentru sincronizarea modificărilor intervenite pe serverul LDAP cu alte servere LDAP din retea.

Utilitare (toate se găsesc in directorul /usr/sbin) :

- slapadd - adaugă intrări dntr-un fisier LDIF in directorul LDAP, de ex. /usr/sbin/slapadd -l ex.ldif va citi fisierul in format LDIF "ex.ldif" si va incărca in bazele de date LDAP modificările continute in acesta.

- slapcat - extrage intrări din directorul LDAP si le salvează in formatul LDIF (ex. /usr/sbin/slapcat –l out.ldif va crea fisierul out.ldif continând toate datele din directorul LDAP)

- slapindex - reindexează directorul LDAP

- slappasswd – generează parole criptate care pot fi folosite apoi cu slapmodify sau valoarea lui rootpw. Acestea se vor găsi in fisierul de configuratie /etc/openldap/slapd.conf

Se recomandă ca demonul slapd să fie oprit când folosim comenzile slapadd, slapcat sau slapindex, altfel s-ar putea ca să se producă erori in directorul LPAD. Oprirea demonului slapd se face cu "usr/sbin/service slapd stop"

Pachetul ldap-clients contine si el utilitare pe care le instalează in /usr/bin :

- ldapmodify – modifică directorul LDAP, acceptând intrări de la intrarea standard (tastatură) sau dintr-un fisier

- ldapadd – adaugă intrări in director de la intrarea standard sau dintr-un fisier; de fapt ldapadd este un shortcut la ldapmodify –a

- ldapsearch – caută intrări in directorul LDAP folosind un prompter shell

- ldapdelete – sterge intrări din directorul LDAP, acceptând comenzi de la intrarea standard sau dintr-un fisier

Cel mai usor mod de a folosi comenzile de mai sus este ca schimbările pe care acestea trebuie să le facă să fie indicate in câte un fisier.

Pe lângă pachetele OpenLDAP, Red Hat Linux contine un pachet numit nss-ldap, care măreste capacitatea LDAP să se integreze in medii Linux sau Unix. Acest pachet contine următoarele module :

/lib/libnss_ldap-<glibc-version>.so

/lib/security/pam_ldap.so

Primul permite aplicatiilor să caute utilizatori, grupuri, calculatoare sau alte informatii folosind un director LDAP, cu ajutorul interfetei NSS (Nameservice Switch) a lui glibc. NSS permite aplicatiilor să se autentifice folosind LDAP, impreună cu NIS si fisiere de autentificare.

Modulul pam_ldap permite aplicatiilor "PAM-aware" (compatibile PAM) să autentifice utilizatori folosind informatii stocate intr-un director LDAP. Aplicatiile compatibile PAM sunt :

- conectarea de la consolă
- servere POP si IMAP (de mail)
- samba

Modulul php-ldap permite suport pentru PHP.

Aplicatii client LDAP

Există clienti grafici pentru modificarea directorului LDAP. Acestia nu sunt distribuiti in distributia Red Hat. Un exemplu de asemenea client este LDAP Browser/Editor, o aplicatie Java disponibilă la adresa

http:/www.iit.edu/~gawojar/ldap

Cei mai multi clienti LDAP accesează directorul LDAP in mod read-only. Exemple de asemenea aplicatii pot fi Mozzila, sendmail Balsa, Pine, Evolution, Gnome Meeting.

Terminologie LDAP

O "*intrare*" este o entitate din directorul LDAP. Fiecare intrare este identificată printr-un "Distinguished Name" (*DN*). Fiecare intrare are *atribute*, care sunt informatii asociate acelei intrări, caracteristici ale acelei intrări.

Ex. Dacă o intrare in directorul LDAP este o organizatie, atribute ale organizatiei ar putea fi numărul ei de fax, adresa sa si asa mai departe.

Unele atribute sunt obligatorii, altele sunt optionale. O definitie *objectclass* stabileste care atribute sunt obligatorii pentru o intrare si care nu. Definitiile objectclass se găsesc in diverse fisiere "*schema*", care se găsesc in directorul /etc/openldap/schema.

Formatul LDIF (LDAP Interchange Format) este un format text ASCII pentru intrări LDAP. Toate aplicatiile care modifică directorul LDAP sau care extrag date din acesta necesită formatul LDIF. Un exemplu de intrare intr-un fisier LDIF ar fi [<id>]

dn: <distinguished-name>

<attrtype>: <attrvalue>

<attrtype>: <attrvalue>

O intrare poate contine oricâte perechi <attrname>: <attrvalue>.

O linie liberă indică sfârsitul unei intrări.

Nu este necesar să editäm fisierele LDIF, ci putem folosi clientii LDAP amintiti anterior.

Fisierele de configurare LDAP

/etc/openldap/schema/ - este un director care contine fisiere "schema" folosite de demonul slapd
/etc/openldap/ldap.conf – fisier de configuratie pentru toate aplicatiile client care folosesc directoarele LDAP
/etc/openldap/slapd.conf – fisier de configuratie pentru demonul slapd

Fisierul de configuratie slapd.conf

Se găseste in directorul /etc/openldap/slapd.conf si trebuie neapărat editat, pentru a-l configura cu configurari specifice domeniului si serverului propriu. Linia

suffix "dc=your_domain, dc=com"

Va deveni

suffix "dc=info,dc=not,dc=ro"

deoarece indică pentru care domeniu va furniza informatii serverul LDAP.

rootdn este intrarea care indică "distinguished name" pentru utilizatorul a cărui acces la operatiile asupra LDAP este nerestrictionat (administratorul LDAP).

rootdn "cn=root,dc=info,dc=uvt,dc=ro"

Intrarea rootpw contine parola utilizatorului specificat de rootdn. Această parolă se generează cu comanda slappasswd, după care se copiază in locul celei din exemplul de mai jos :

rootpw {SHA}vv2yti6V6esazrJv……..

Această linie este necesară doar dacă dorim să modificăm directorul LDAP de la distanta. Dacă folosim slapd pentru a popula LDAP nu avem nevoie de parolă pentru utiliyatorul root, deci rootpw nu este necesar şi linia poate fi comentată, scriind la inceputul ei un #.

Directorul /etc/openldap/schema contine definitiile LDAP, care la versiuni anterioare se găseau in fisierul *slapd.at.conf* si *slapd.oc.conf*. Toate definitiile de atribute sau definitiile *objectclass* sunt acum in fisiere "schema" diferite. Acestea trebuiesc incluse prin directiva *include* in fisierul /etc/openldap/slapd.conf.

Ex.: include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/kerberosobject.schema

Obs. Fisierele din directorul schema nu este recomandat să fie modificate. Dacă dorim să creem alte tipuri aditionale de atribut cu clase de

obiecte, atunci este indicat să creem un fisier numit local.schema in care să facem aceste definitii. Apoi vom include acest fisier printr-o directivă *include* in fisierul slapd.conf si anume

include /etc/openldap/schema/local.schema

Crearea serverului LDAP

La adresele http://www.openldap.org/doc/admin/quickstart.html
si
http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html
se găsesc informatii utile despre instalarea si configurarea unui server LDAP. De asemenea si in cartea Red Hat Linux 8 – The official Red Hat Linux Reference Guide, capitolul 18, pag. 257.

Etape :

1.) Se instalează openldap, openldap-servers si openldap-clients.
2.) Se editează fisierul /etc/openldap/slapd.conf conform celor spuse anterior.
3.) Se porneste demonul slapd cu comanda /sbin/service/ldap start. Dacă dorim să pornească automat folosim chkconfig ldap on.
4.) Adăugăm intrări in directorul LDAP cu ldapadd.
5.) Folosind ldapsearch putem vedea dacă slapd accesează inf. correct.
6.) Configurăm aplicatiile comenzilor LDAP cu ajutorul fisierului de configuratie /etc/ldap.conf

Configurarea sistemului ca să folosească openldap pentru autentificare

1.) Se instalează pachetele necesare pe masinile server si pe masinile client. Pe server trebuie instalat openldap-servers. Pe masinile client trebuie instalate openldap-clients, openldap, nss_ldap.
2.) Se configurează (editează) fisierul /etc/openldap/slapd.conf de pe server ca să aibă informatiile specifice organizatiei proprii.
Sunt suficiente liniile
suffix
rootdn
si
rootpw
conform celor spuse mai devreme.
3.) Pe masinile client se editează fisierele
/etc/ldap.conf

/etc/openldap/ldap.conf
Astfel incat să conțină informatii corecte despre server.
Cel mai usor se poate face acest lucru cu aplicatia
authconfig
in care selectăm "Use LDAP" din ecranul "User Information Configuration".

4.) Pe masinile client se editează /etc/nsswitch.conf pentru a folosi LDAP. Se poate face acest lucru cu
Authconfig -> Use LDAP -> "User Information Configuration"
sau manual scriind ldap la sfârşitul liniilor
sau

passwd: files ldap
shadow: files ldap
group: files ldap

5.) Pentru autentificare folosind PAM
anthconfig -> Use LDAP Autentification din ecranul "Autentification Configuration"

Migrarea vechilor informatii de autentificare in format LDAP

Directorul /usr/share/openldap/migration/ contine o serie de scripturi Perl pentru a migra informatia de autentificare in format LDAP. Trebuie să avem Perl instalat pentru a putea rula aceste scripturi.

a.) trebuie modificat fisierul
migrate_common.sh
in asa fel incât să reflecte domeniul propriu
Trebuie modificate liniile
$ DEFAULT_MAIL_DOMAIN="your_company";
si
$ DEFAULT_BASE="dc=your_company;dc=com";
Tabelul de mai jos indică ce utilitar vom folosi pentru migrare:

Serviciu existent	Rulează LDAP ?	Ce script trebuie folosit
Fisierele /etc	Da	migrate_all_online.sh
Fisierele /etc	Nu	migrate_all_offline.sh
NetInfo	Da	migrate_all_netinfo_online.sh
NetInfo	Nu	migrate_all_netinfo_offline.sh
NIS (YP)	Da	migrate_all_nis_online.sh

NIS (YP)	Nu	migrate_all_nis_offline.sh

Informatii suplimentare se găsesc in fisierul :
/usr/share/openldap/migration/README