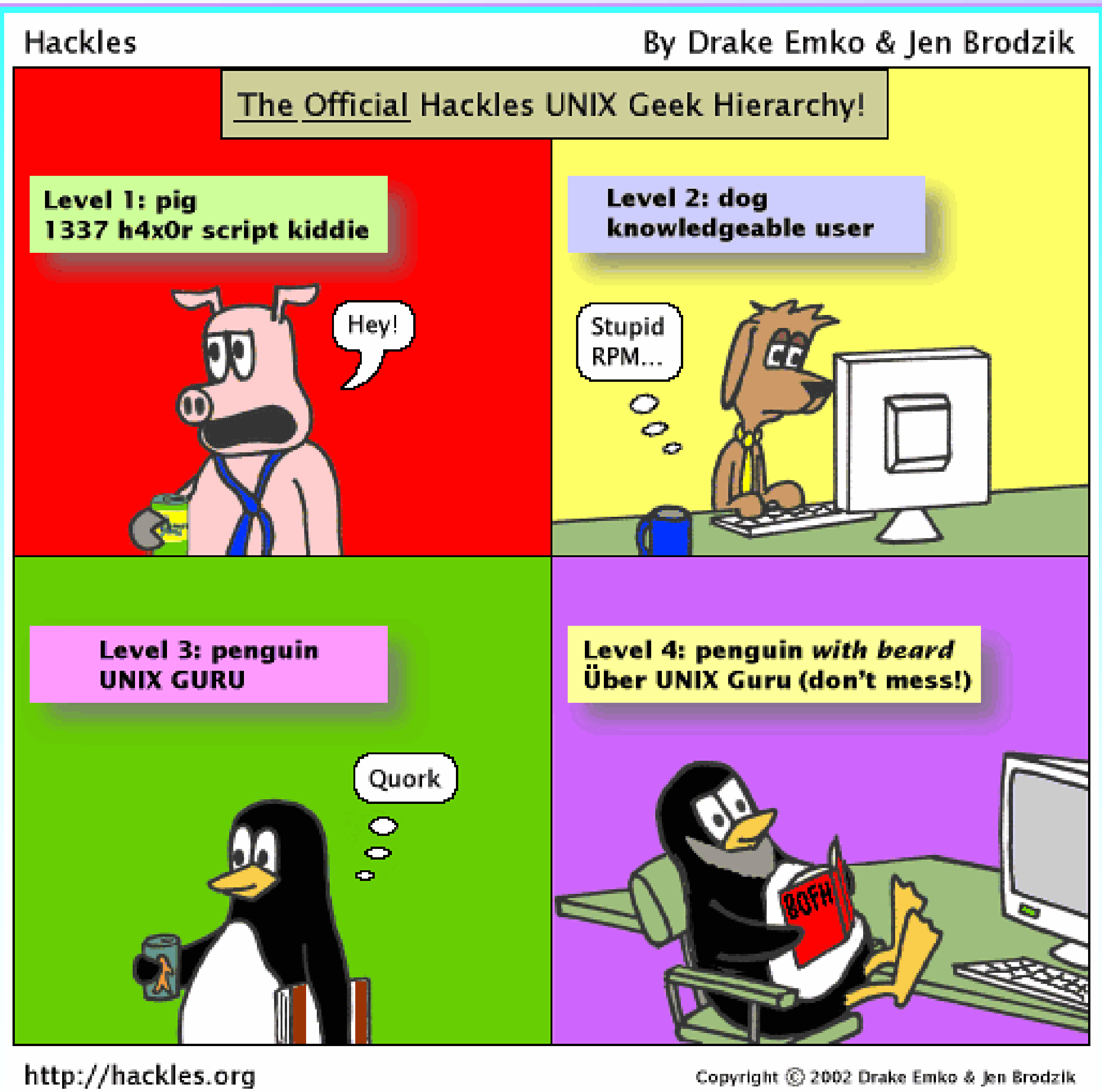
Програмиране в UNIX среда

Основи на системната администрация

System administration


Hackles
By Drake Emko & Jen Brodzik
The Official Hackles UNIX Geek Hierarchy!
Level 1: pig
1337 h4x0r script kiddie
Hey!
Level 2: dog
knowledgeable user
Stupid RPM...
Level 3: penguin
UNIX GURU
Quork
Level 4: penguin *with beard*
Über UNIX Guru (don't mess!)
BOFH
http://hackles.org
Copyright © 2002 Drake Emko & Jen Brodzik

SYS ADMIN TASKS

- Setting the Run Level
- System Services
- User Management
- Network Settings
- Scheduling Jobs
- Quota Management
- Backup and Restore
- Adding and Removing software/packages
- Setting a Printer
- Monitoring the system (general, logs)
- Monitoring any specific services running. Eg. DNS, DHCP, Web, NIS, NPT, Proxy etc.

Init Runlevels

- **The following runlevels are defined in Linux:**
  - 0 - halt (Do NOT set initdefault to this)
  - 1 - Single user mode
  - 2 - Multiuser, without Network (The same as 3, if
  - you do not have networking)
  - 3 – Text Mode
  - 4 - unused
  - 5 – Graphical Mode
  - 6 - reboot (Do NOT set initdefault to this)

Init Runlevels

- The default runlevel for a system to boot to is configured in /etc/inittab.

```
id:5:initdefault:
```

- In GUI: Applications à System Settings à Server Settings à Services
- Generally, Linux operates in runlevel 3 or 5.

Linux Services

There are 113 deamons, Out of them, the following are most widely used:

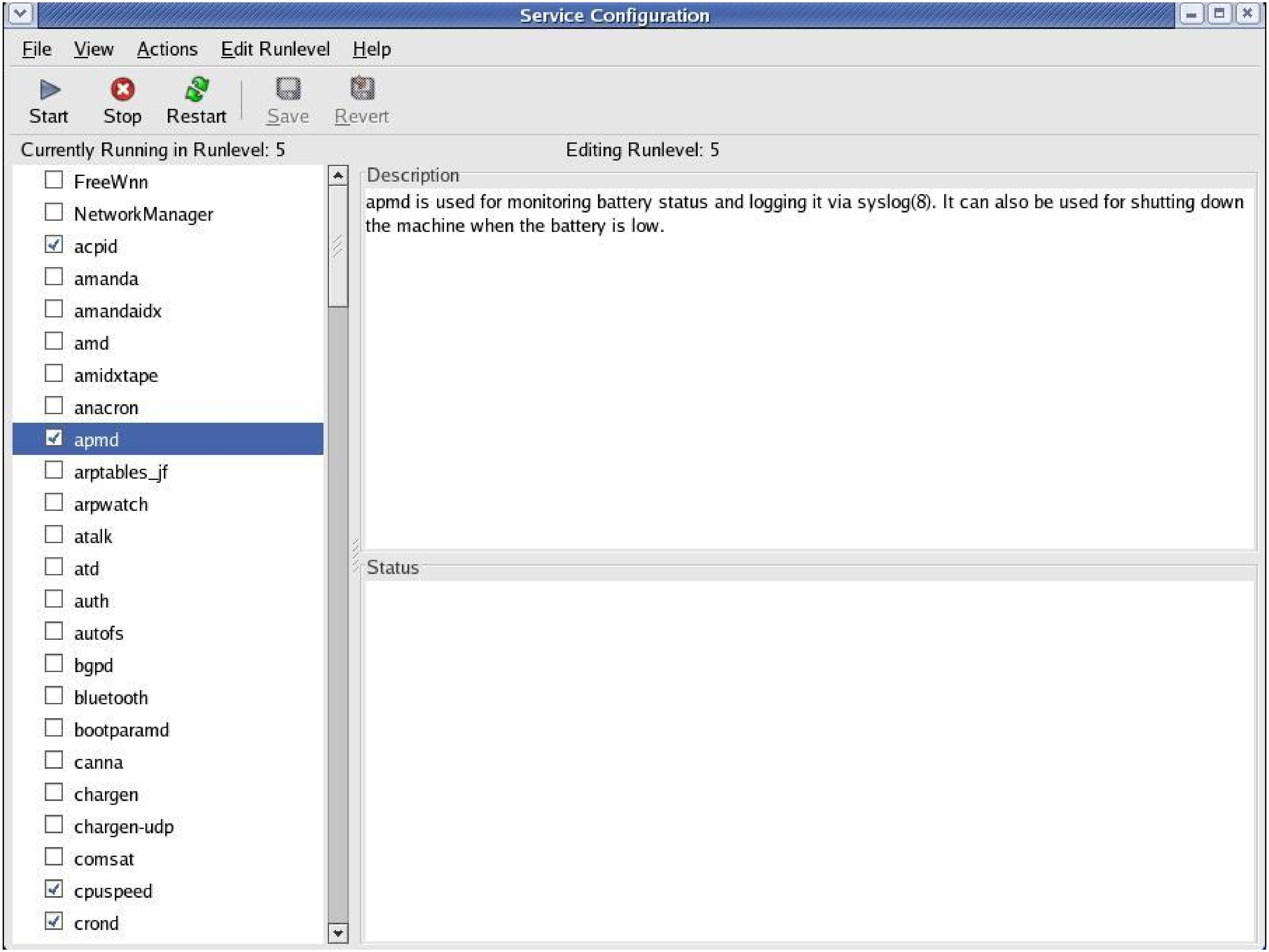
- **apmd** : Power Management
- **autofs** : Automount services
- **crond** : Periodic Command Scheduler
- **cups** : Common Unix Printing System
- **dhcpd** : The DHCP server
- **dovecot** : IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol) server
- **gpm** : Mouse
- **httpd** : Apache Web server

Linux Services

- **iptables** : Kernel based Packet Filtering firewall
- **kudzu:** Finds new Hardware
- **mysqld** : MySQL server
- **named** : BIND server
- **network** : Networking
- **nfs** : Network File Share
- **nfslock** : NFS file locking
- **ntpd** : NTP (Network Time Protocol) server
- **portmap** : RPC (Remote Procedure Call) support
- **postgresql** : The Postgresql Database Engine

Linux Services

- **sendmail** : Sendmail Mail Server
- **smb** : Samba Network Services
- **snmpd** : Simple Network Management Protocol
- **squid** : Squid Proxy Server
- **sshd** : Open SSH and SFTP server
- **syslog** : System Logging
- **xinetd** : Provides support for telnet, ftp, talk, tftp etc.
- **ypbind** : NIS Server



Currently Running in Runlevel: 5

Editing Runlevel: 5

- □ FreeWnn
- □ NetworkManager
- ☑ acpid
- □ amanda
- □ amandaidx
- □ amd
- □ amidxtape
- □ anacron
- ☑ apmd
- □ arptables_jf
- □ arpwatch
- □ atalk
- □ atd
- □ auth
- □ autofs
- □ bgpd
- □ bluetooth
- □ bootparamd
- □ canna
- □ chargen
- □ chargen-udp
- □ comsat
- ☑ cpuspeed
- ☑ crond

apmd is used for monitoring battery status and logging it via syslog(8). It can also be used for shutting down the machine when the battery is low.

Linux Services

- **Start/Stop boot time services in /etc/rc.d/rc3.d or /etc/rc.d/rc5.d**
- **All services startup scripts which start with S will start at boot time and all startup scripts which start with K will not start at boot time. The number after S or K is the priority.**

    K95kudzu

    K96pcmcia

    S56xinetd

    S60vsftpd

- **Use**

  service <service name> start/stop/restart

  to start, stop or restart a service from command line

Creating a new User Account

- Add an entry in /etc/passwd and /etc/shadow file (use next uid and suitable gid). You will have to create the user directory and assign a password to the user
- Use useradd or adduser command to create a new user (useradd –g <group> -d <home directory> -c <comment> -s <shell> login-name) and groupadd to create a new group (groupadd group-name). You will have to assign a password (passwd login-name)
- In GUI: Applications à System Settings à Users and Groups

/etc/passwd File

- ***/etc/passwd*** Holds user account info

  Included fields are:

  - Login name
  - User Id (uid)
  - Group Id (gid)
  - General Comment about the user
  - Home Directory
  - Shell

/etc/shadow File

- ***/etc/shadow*** Contains the encrypted password information for users' accounts and optionally the password aging information. Included fields are:
  - Login name
  - Encrypted password
  - Days since Jan 1, 1970 that password was last changed
  - Days before password may not be changed
  - Days after which password must be changed
  - Days before password is to expire that user is warned
  - Days after password expires that account is disabled
  - Days since Jan 1, 1970 that account is disabled

Suspending a User Account

- Put a * as start of Password field in /etc/shadow
- Change login shell to /sbin/nologin
- Use GUI to suspend the user

Removing a User Account

- Remove login id from /etc/passwd & /etc/shadow file and delete home directory
- userdel –r <username>
- Use GUI to Delete the user

Linux Network Configuration

- ***/etc/resolv.conf*** **Tells the kernel which name server should be queried when a program asks to "resolve" an IP Address.**

```
nameserver 172.31.1.1
search phys.uni-sofia.bg, cern.ch
```

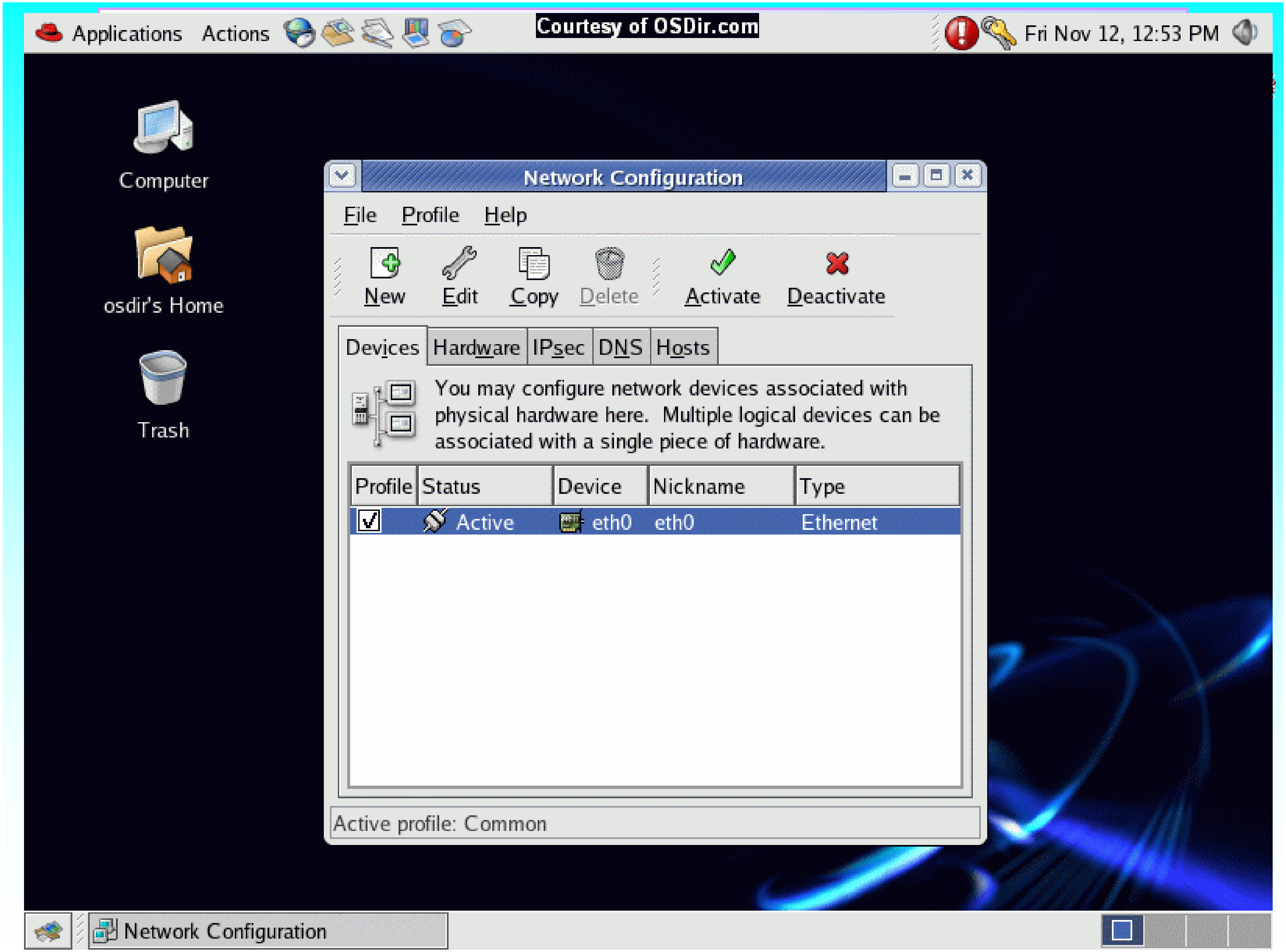
- ***/etc/sysconfig/network*** **Indicates networking is enabled (NETWORKING=yes) and provides information on hostname, gateway and nis domain.**

```
NETWORKING=yes
HOSTNAME=heph1.phys.uni-sofia.bg
NISDOMAIN=cc
GATEWAY=192.168.2.1
```

Linux Network Configuration

- */etc/sysconfig/network-scripts/ifcfg-eth0* **Network configurations like boot protocol (static/dhcp), ip address, netmask, network address, broadcast address etc.**

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.2.56
NETMASK=255.255.255.0
BROADCAST=192.168.255.255
NETWORK=192.168.2.0
GATEWAY=192.168.2.1
```



You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Active	eth0	eth0	Ethernet

Active profile: Common

Scheduling Jobs: Cron

- Cron is a program that enables you to execute a command, or a script with a sequence of commands, at a specified date, time or at set intervals.
- Add the job script in /etc/cron.hourly or /etc/cron.daily or /etc/cron.weekly or /etc/cron.monthly to schedule a job

Scheduling Jobs: Cron

- **Make an entry in /etc/crontab file to schedule a job (crontab -e) the format is**

  * * * * * command_to_execute

  each star denotes Minute Hour Day_of_Month Month Day_of_Week

  Minute = Minute of the hour, 00 to 59. * Will indicate every minute

  Hour = Hour of the day in 24-hour format, 00 to 23. * Will indicate every hour

  Day = Day of the month, 1 to 31. * Will indicate every day

  Month = Month of the year, 1 to 12. * Will indicate every month

  Day = Day of the week, 3 chars - sun, mon, tue, or numeric (0=sun, 1=mon etc).... * Will indicate every day

  Task = The command you want to execute

Backup & Restore

- Backup the user area or configuration file
- Use tar to take backup on a different disk or tape
- Backup can be scheduled using cron
- Backup: tar –zcvf <tar filename> <Directory Tree to be backedup>
- Restore: tar –zxvf <tar filename> <file to be recovered>
- Backup should be occasionally checked by restoring it
- Backup Policy: Full Backup every weekly/fortnightly and incremental backup every day

Adding & Removing Software

- Download a binary
- Download the source code and compile on the system (download, untar, configure, make, make install, make uninstall)
- Use **RPM - Redhat Package Manager** and install rpms
- www.rpmseek.com & www.rpmfind.net can be used to search and download rpms (i386 Binary RPMs or SRC RPMs)
- For Binary rpms: rpm [options] rpm-file

  (rpm –qa, rpm –ivh, rpm –Uvh, rpm -e)

  Where -q= query, -a= all, -i=install, -v=verbrose, -U= upgrade, -h= hash, -e= erase
- For Source rpms: rpmbuild –rebuild rpm-source-file

  Compiled binary rpms will be available at /usr/src/redhat/RPMS/i386 which can be installed

Configuring Disk Quotas

To implement disk quotas, use the following steps:

- **Enable quotas per file system by modifying /etc/fstab**
- **Remount the file system(s)**
- **Create the quota files and generate the disk usage table**
- **Assign quotas**

Configuring Disk Quotas

- **Enabling Quotas: Edit fstab to enable usrquota**

```
LABEL=/           /        ext3   defaults                     1 1
LABEL=/boot       /boot    ext3   defaults                     1 2
LABEL=/users      /users   ext3   exec,dev,suid,rw,usrquota    1 2
LABEL=/var        /var     ext3   defaults                     1 2
LABEL=SWAP-sda5   swap     swap   defaults                     0 0
```

Configuring Disk Quotas

- **Remounting the File Systems:** Issue the umount command followed by the mount command to remount the file system in which quota has been implemented (umount /users;mount /users)

- **Creating the Quota Database Files:** Use quotacheck command to create quota.user file

  ```
  quotacheck -cu /users
  ```

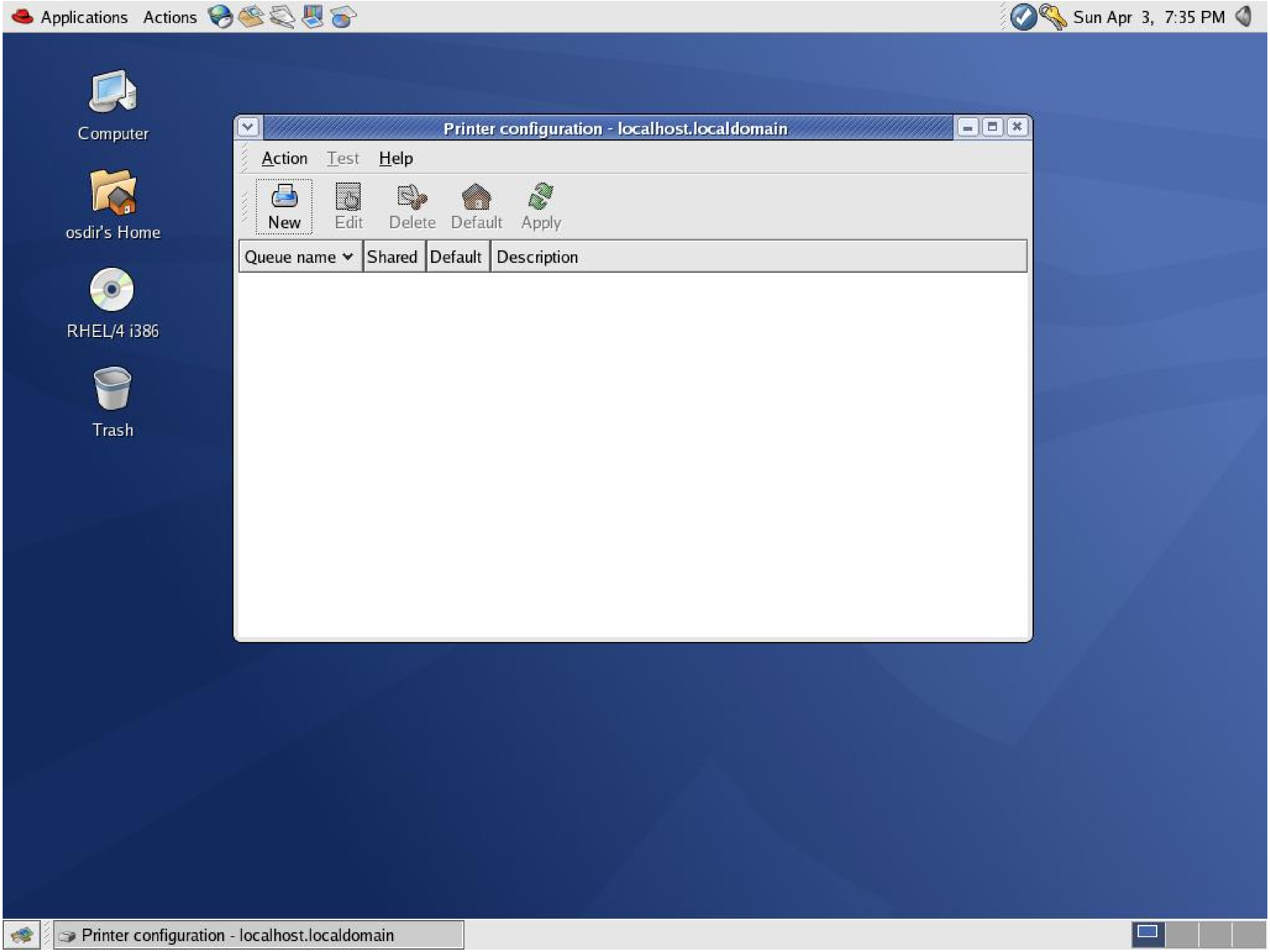
- **Assigning Quotas per User:** assigning the disk quotas with the edquota command (edquota <username>)

```
Disk quotas for user web_cc (uid 524):
 Filesystem          blocks     soft       hard      inodes   soft   hard
 /dev/sdb1           988612   1024000   1075200     7862      0      0
```

Setting Printer

- The Printer Configuration Tool allows users to configure a printer in Red Hat Linux. This tool helps maintain the printer configuration file, print spool directories, and print filters. Starting with version 9, Red Hat Linux defaults to the CUPS (Common Unix Printing System).

- To use the Printer Configuration Tool you must have root privileges. To start the application, select Applications => System Settings => Printing


Applications
Actions
Sun Apr 3, 7:35 PM
Computer
osdir's Home
RHEL/4 i386
Trash
Printer configuration - localhost.localdomain
Action
Test
Help
New
Edit
Delete
Default
Apply
Queue name
Shared
Default
Description
Printer configuration - localhost.localdomain

Setting Printer

The following types of print queues can be configured:

- **Locally-connected** — a printer attached directly to the computer through a parallel or USB port.
- **Networked CUPS (IPP)** — a printer that can be accessed over a TCP/IP network via the Internet Printing Protocol, also known as IPP (for example, a printer attached to another Red Hat Linux system running CUPS (Common Unix Printing System) on the network).
- **Networked UNIX (LPD)** — a printer attached to a different UNIX system that can be accessed over a TCP/IP network (for example, a printer attached to another Red Hat Linux system running LPD (Line Printer Daemon) on the network).
- **Networked Windows (SMB)** — a printer attached to a different system which is sharing a printer over a SMB network (for example, a printer attached to a Microsoft Windows™ machine).
- **Networked Novell (NCP)** — a printer attached to a different system which uses Novell's NetWare network technology.
- **Networked JetDirect** — a printer connected directly to the network through HP JetDirect instead of to a computer.

Monitoring the System

- Monitor Disk Usage (df)
- Monitor CPU and Memory utilization (top)
- Monitor process/services (ps, pgrep)
- Monitor logs (/var/log/messages)

- GUI Tool (Applications à System Tools à System Performance)

Linux Rescue

- Booting into Single User Mode
  - At the GRUB screen, press e
  - Select the kernel and type a
  - Write single at the end of the line (after leaving a space)
  - Boot by pressing b
- Booting into Rescue Mode
  - Boot the system using Installation CD #1
  - Type “linux rescue” at the installation boot prompt

▣ DHCP

DHCP

- DHCP (Dynamic Host Configuration Protocol) is a network service that enables clients to obtain network settings (IP Address, Subnet Mask, Default Gateway, DNS Server, Hostname and Domain) automatically from a central server
- The DHCP client sends a broadcast request to find the DHCP server and the DHCP server in the subnet responds with an IP address (and other common network parameters) from a pool of IP addresses
- The IP address can be bound to the MAC address of the client
- Daemon: dhcpd
  Lease file: /var/lib/dhcp/dhcpd.leases

DHCP Server Configuration

- **Configuration File: /etc/dhcpd.conf**

```
subnet 192.168.2.0 netmask 255.255.254.0 {

        authoritative;
         option routers                  192.168.2.1;
        option subnet-mask              255.255.254.0;
        option domain-name              “grid.uni-sofia.bg";
        option domain-name-servers      62.44.127.150;

        range  192.168.2.2 192.168.2.254;
        default-lease-time 7200;
        max-lease-time 10800;
        host tc1 {
                hardware ethernet 00:80:64:1A:E9:14;
                fixed-address  192.168.2.133;
        }
}
```

DHCP Client Configuration

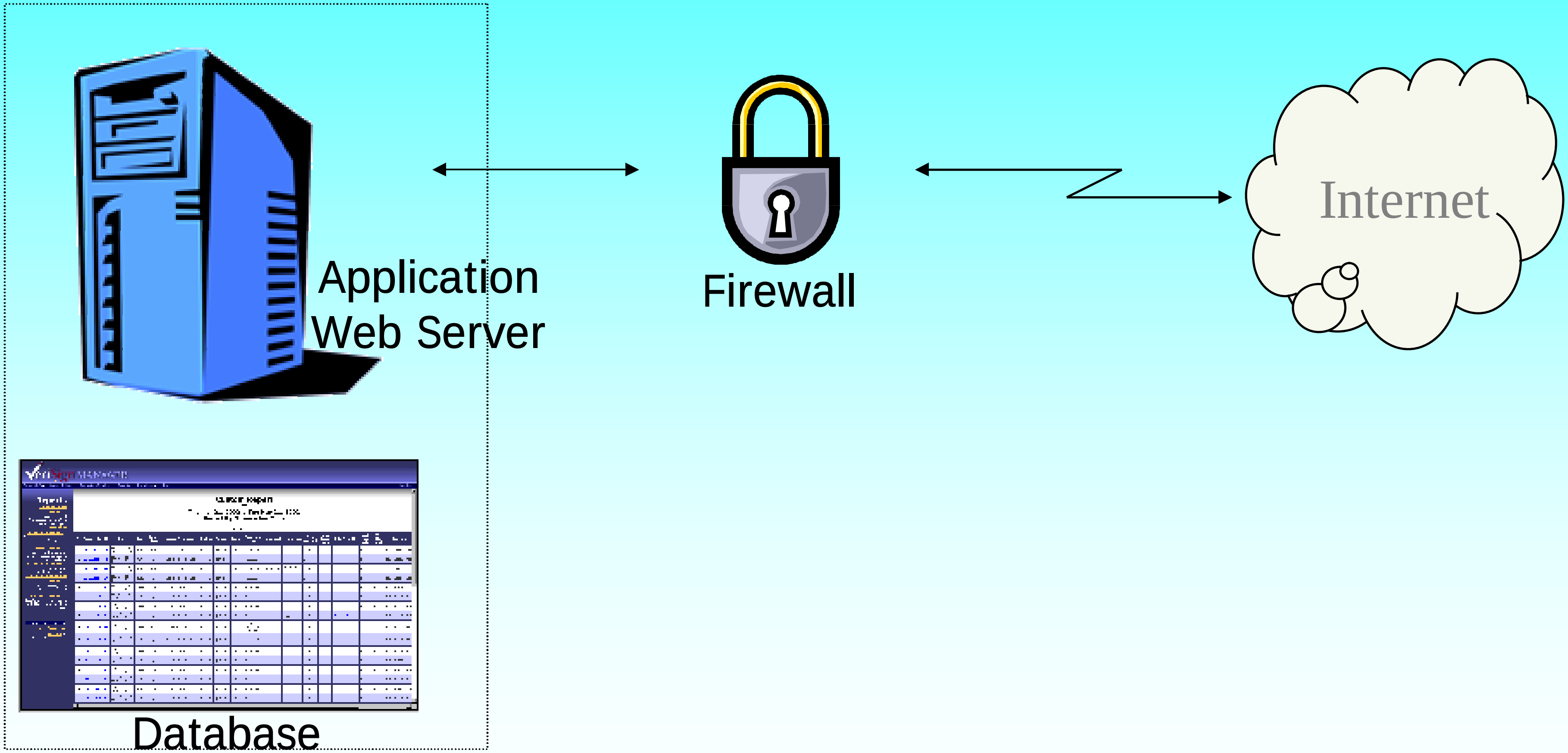
- **Configure the Network Configuration to pickup network settings from DHCP server**
- **/etc/sysconfig/network-scripts/ifcg-eth0**

```
BOOTPROTO=dhcp (static)
```

- **Applications à System Settings à Network**

▣LINUX SECURITY

Firewall



Application Web Server

Firewall

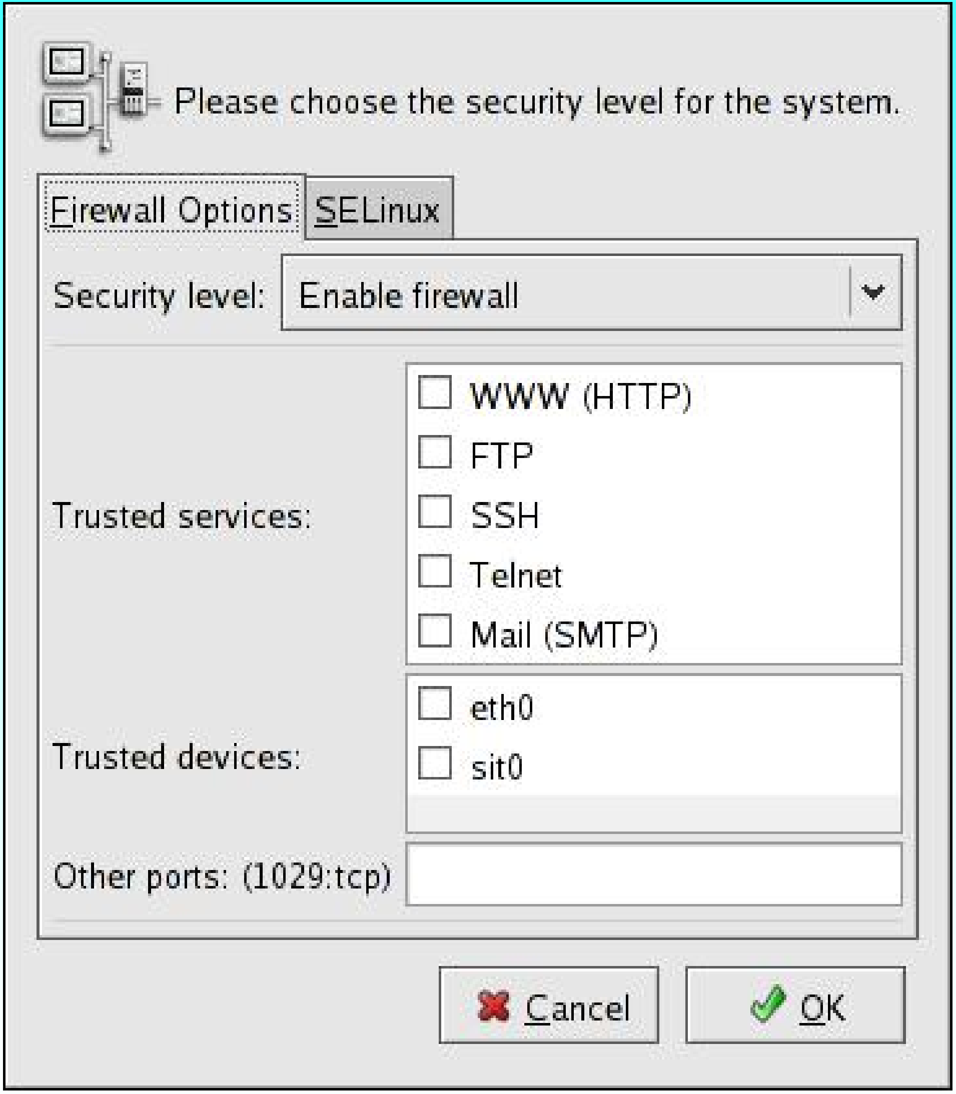
Internet

Database

LINUX Firewall

- Use GUI (Applications ->System Settings-> Security Level) to activate the firewall
- Allow standard services and any specific port based application
- All other services and ports are blocked

LINUX Firewall



Please choose the security level for the system.

Security level: Enable firewall

Trusted services:

- □ WWW (HTTP)
- □ FTP
- □ SSH
- □ Telnet
- □ Mail (SMTP)

Trusted devices:

- □ eth0
- □ sit0

Other ports: (1029:tcp)

SELinux

- Malicious or broken software can have root-level access to the entire system by running as a root process.
- SELinux (Security Enhanced Linux) provides enhanced security.
- Through SELinux policies, a process can be granted just the permissions it needs to be functional, thus reducing the risk

SELinux

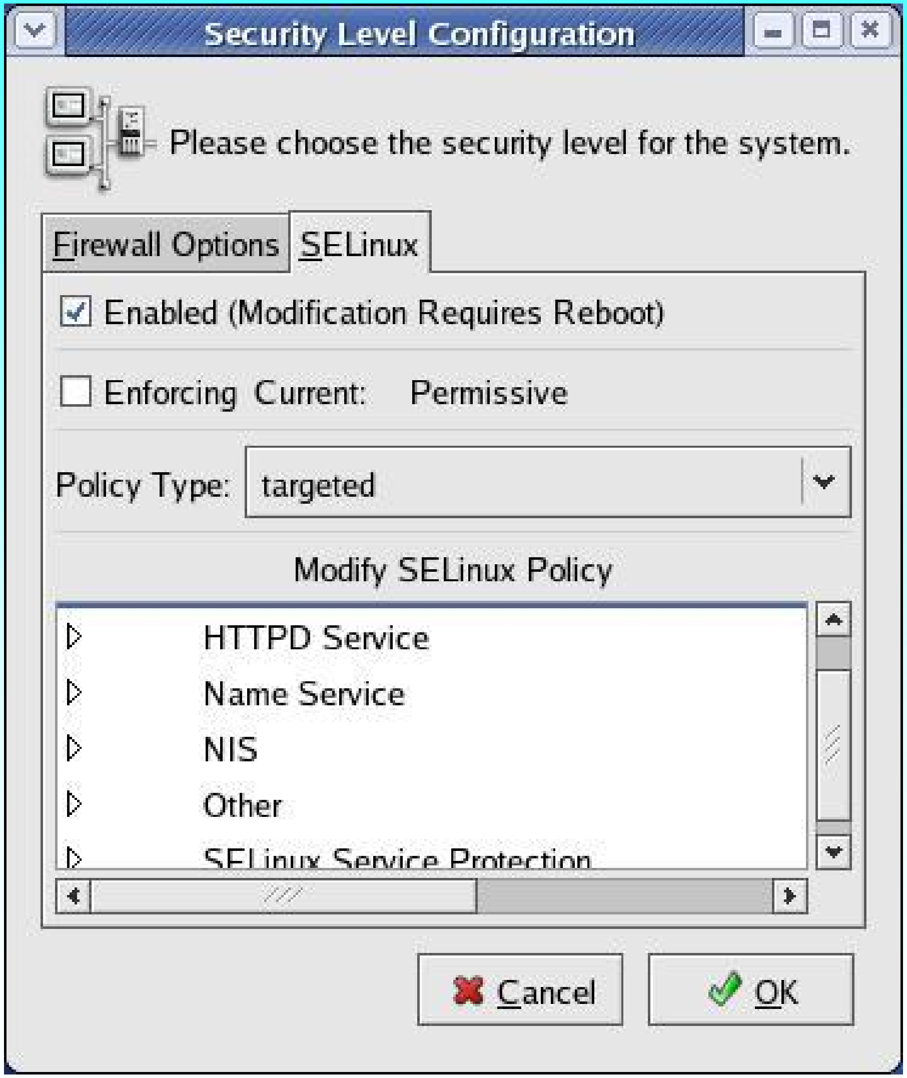
SELINUX can take one of these three values

- enforcing - SELinux security policy is enforced.
- permissive - SELinux prints warnings instead of enforcing.
- disabled - SELinux is fully disabled.

SELinux Configuration

- **Use GUI (Applications ->System Settings-> Security Level) to activate SELinux**
- **Enable/Disable SELinux**
- **Allow standard features in various services (http,nis,nfs,dns etc.)**
- **All other services and features are blocked**

SELinux Configuration



Security Level Configuration

Please choose the security level for the system.

☑ Enabled (Modification Requires Reboot)

☐ Enforcing Current: Permissive

Policy Type: targeted

Modify SELinux Policy

- HTTPD Service
- Name Service
- NIS
- Other
- SELinux Service Protection

Литература:

- http://www.wylug.org.uk/talks/2003/04/unix.pdf
- http://ce.sharif.edu/courses/ssc/unix/resources/root/Slides/unixhistory.pdf
- http://www.cs.uga.edu/~eileen/1730/Notes/intro-UNIX.ppt
- http://remus.rutgers.edu/cs416/F01
- http://www.cs.virginia.edu/~cs458/
- http://www.bobbooth.staff.shef.ac.uk/hpcs/materials/material.html
- http://www.comm.utoronto.ca/~jorg/teaching/ece461
- http://home.iitk.ac.in/~navi/sidbilinuxcourse/
- http://www.cs.washington.edu/homes/bershad/Mac/ssh/practicalmagic.pdf
- http://www.cs.cf.ac.uk/Dave/C/CE.html
- http://www.le.ac.uk/cc/tutorials/c/ccccintr.html
- http://www.shef.ac.uk/uni/academic/N-Q/phys/teaching/phy225/index.html