information technology & management

viabiliitijt

ITMO456

INTRO TO OPEN SOURCE OPERATING SYSTEMS

ILLINOIS INSTITUTE OF TECHNOLOGY

Linux System Administration

Sean Hughes-Durkin

ITMO/IT-O 456 Fall 2017

Information Technology & Management Programs

School of Applied Technology

1

Objectives

At the end of this lesson students should be able to:

- Use the set user (`su`) and set user do (`sudo`) commands

- Manage time and date settings

- Understand the purpose of log files and how they are administered

- Create, modify, manage, and delete user and group accounts using command-line utilities and the Red Hat User Manager

ITM0456

Becoming **root**

◆ The Linux system administrator or is a user named "root"

- It is very bad practice security-wise to log in as **root**; some distros preclude it

- Users should login as themselves and become root using the **su** command

- When root, prompt changes from **$** to **#**

◆ Use of **su** not allowed in Ubuntu

- Use **sudo** instead

ITMO456

Using set user - `su`

◆ The su command is used to "set a user"

- Syntax: `su - username`

- Allows you to "become" the user specified by *username*

◆ If no name is specified, `su -` sets the user to the default user: `root`

- Then you can become another user

- The `-` option allows you to use root's environment

ITMO456

Using set user - `su`

```
[sean@itmo456 ~]$ echo -e "$USER\n$PWD\n$MAIL\n$PATH"
sean
/home/sean
/var/spool/mail/sean
/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/home/sean/.local/bin:/home/sean/bin
[sean@itmo456 ~]$ su
Password:
[root@itmo456 sean]# echo -e "$USER\n$PWD\n$MAIL\n$PATH"
sean
/home/sean
/var/spool/mail/sean
/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/home/sean/.local/bin:/home/sean/bin
[root@itmo456 sean]# exit
exit
[sean@itmo456 ~]$ su -
Password:
Last login: Sat Oct 24 15:51:29 CDT 2015 on pts/0
[root@itmo456 ~ ]# echo -e "$USER\n$PWD\n$MAIL\n$PATH"
root
/root
/var/spool/mail/root
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
```

ITMO456

Using **sudo**

◆ **sudo** *command*

allows users to run a command as root

- Commands limited or allowed based on group

- Requires user added to appropriate group(s)

- Requires user's password

- Configured in /etc/sudoers file
  - Use command **visudo** (checks syntax)

ITMO456

Using `sudo`

◆ Security model of Ubuntu does not allow users to log in as **root**

- Issue root commandes using **sudo**
- Launch root session using **sudo su –**
- Can enable root using **sudo passwd root**

◆ Default allows use of **sudo** by user created during installation

- Additional users must be added to **admin** group to gain sudoer access

ITMO456

7

Using **sudo**

◆ Can add user to wheel group to gain root privileges

- `user_list host_list=(runas_list)] command_list`
- `%wheel  ALL=(ALL)       ALL`

◆ Can also allow/deny certain commands and options

- `sam ALL=(root) /bin/mount, /bin/umount, !/bin/umount /p03`

ITMO456

8

Printer Administration: Print Process

ITM0456

◆ Print job

- ▪ A set of information that is sent to a printer at the same time

- ▪ To send a print job to a printer, you must first use the `lp` or `lpr command` and specify what to print

Printer Administration: Print Process

◆ Spooling or queuing

- Accepting print jobs into a print queue

◆ If the printer is **started**, the printer command (`lp` or `lpr`) sends the print job from the print queue to the printer

- Conversely, if the printer is **stopped**, the print job remains in the print queue

◆ Printing

- Sending print jobs from print queue to a printer

ITMO456

Printer Administration: CUPS

◆ Common Unix Printing System (CUPS)

  ▪ Most common printing system used on Linux

◆ **lp** command

  ▪ Sends a print job to a printer

◆ cups daemon (**cupsd**)

  ▪ Responsible for printing in CUPS printing system

ITMO456

Printer Administration: CUPS

ITMO456

◆ Print job ID

- Print job's unique identifier

◆ Print queue

- Directory holding print jobs waiting to be printed

- Typically `/var/spool/cups`

◆ Printer can accept or reject request to print

- If rejected, CUPS gives an error message

Printer Administration: CUPS

ITM0456

cupsd

accept   enable

lp   reject   Print Queue   disable

/var/spool/cups

printer1

"spooling"   **"printing"**
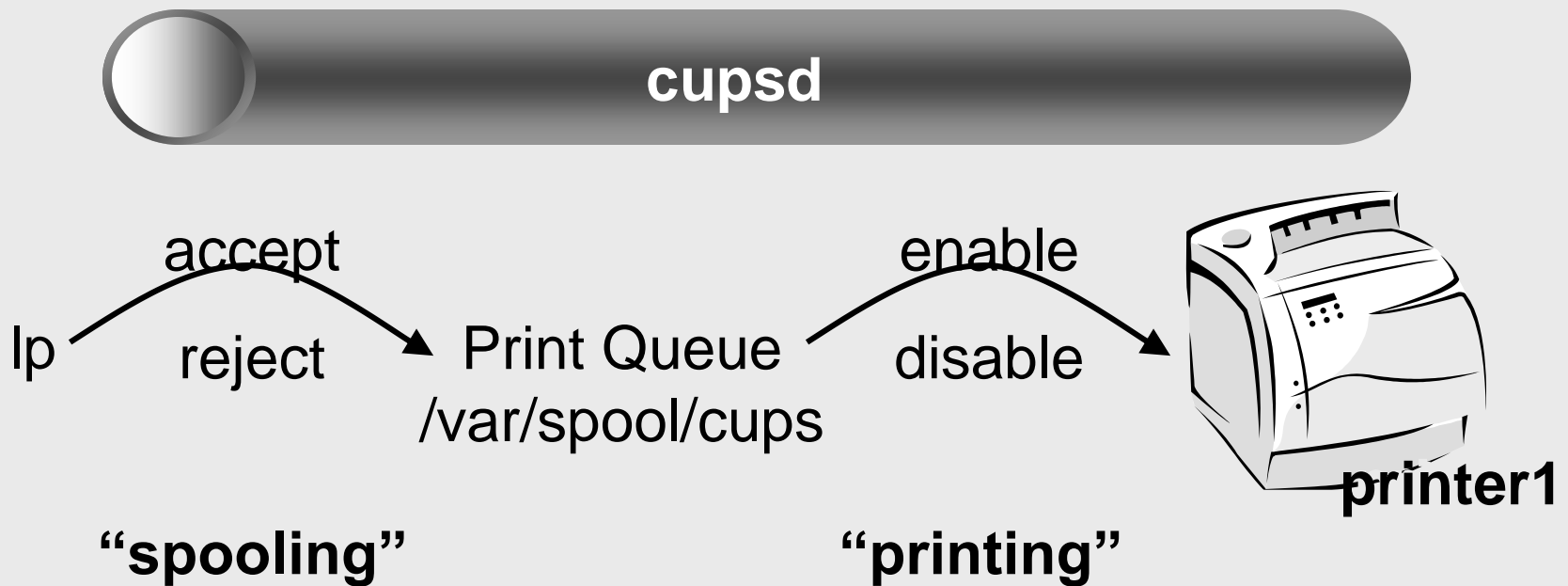
Figure 10-1: The CUPS print process

Printer Administration: CUPS

◆ **lpstat** command

- With **-t** (total) option, lists all printers and their status

◆ **cupsaccept**, **cupsreject**, **cupsenable**, and **cupsdisable** commands

- Manipulate status of a printer
- **-r** option: used to specify reason for **cupsdisable**/**cupsreject** commands

ITMO456

Printer Administration: Managing Print Jobs

◆ **`lp -d`** command

- Print to a specified printer
- If **`-d`** option omitted, prints to default printer

◆ **`lpoptions -d`** command

- Set default printer

◆ Users can set own default printer

- Add to **`.lpoptions`** file in home directory
- Use PRINTER or LPDEST variable

ITMO456

Printer Administration: Managing Print Jobs

Option	Description
-d *printername*	Specifies the name of the printer to send the print job
-l *print job ID*	Specifies a certain print job ID to modify
-n *number*	Prints a certain *number* of copies
-m	Mails you confirmation of print job completion
-o *option*	Specifies certain printing options. Common printing options include the following: cpl = *number*—Sets the characters per inch to *number* landscape—Prints in landscape orientation number-up = *number*—Prints *number* pages on a single page, where *number* is 1, 2 or 4 sides = *string*—Sets double-sided printing, where *string* is either 'two-sided-short-edge' or 'two-sided-long-edge'
-q *priority*	Specifies a print job priority from 1 (low priority) to 100 (high priority). By default, all print jobs have a priority of 50

Table 10-1: Common options to the `lp` command

ITMO456

Printer Administration: Managing Print Jobs

ITMO456

◆ **lp** command

- Accepts information from stdin

◆ **lpstat** command

- Can list print jobs in queue for a printer

◆ **cancel** command

- Remove print jobs from print queue

- Receives print job IDs as arguments

- **-u** option removes all jobs sent by a specified user

Printer Administration: Managing Print Jobs

ITMO456

◆ **`lpadmin`** command

- Perform printer administration
- e.g., restrict who can print to specific printers

Printer Administration: Managing Print Jobs

ITMO456

Option	Description
-a	Displays a list of printers accepting print jobs
-d	Displays the default destination printer
-o *printername*	Displays the print jobs in the queue for *printername* only
-r	Shows whether the cups daemon (scheduler) is running
-t	Shows all information about printers and their print jobs

Table 10-2: Common options to the `lpstat` command

Configuring Printers

◆ On Fedora 25 systems, GNOME desktop Printers tool can create new printers and manage them

- Access the Printers tool by navigating to the `Activities menu` → `Show Applications` → `Settings` → `Printers`

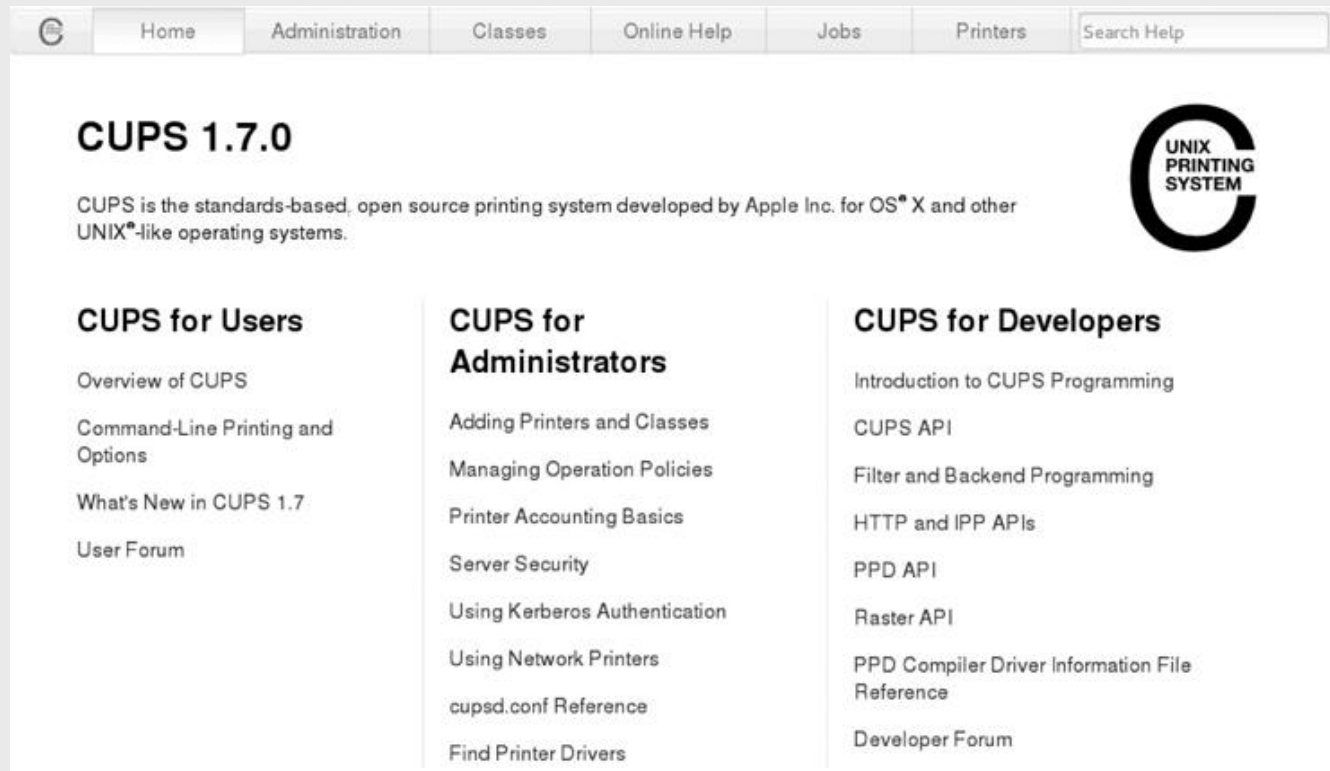◆ Most comprehensive way to create and manage CUPS printers is the CUPS Web administration tool

ITMO456

Printer Administration: CUPS

◆ CUPS is also Web configurable & manageable

- Configurations entered with Web interface are found in **/etc/cups/printers.conf**

- Access through **http://localhost:631**

◆ CUPS server configuration in **/etc/cups/cupsd.conf**

- Very similar to Apache configuration

ITMO456

Configuring Printers

ITMO456

Configuring Printers

ITMO456

Configuring Printers

◆ To create a new printer using CUPS Web tool:

- Select the **Administration** tab, click **Add Printer**, and log in using the root username and password
- You will need to select type of printer

ITMO456

24

Configuring Printers

ITM0456

Configuring Printers

◆ After selecting printer type, you need to specify the following information:

- Printer name

- Description

- Manufacturer and model

- Default printer options

- Whether to share the printer using IPP

◆ After that, you can use other options on the Administration tab to configure and manage the CUPS printing service

ITM0456

26

Configuring Printers

Configuring Printers

◆ CUPS allows configuration of collections of printers to be used as a single unit

- ▪ Called printer classes
- ▪ Often used in larger organizations, where multiple printers are stored in a print room

◆ When you print to a printer class, the print job is sent to the first available printer

◆ To create a printer class, select the Add Class button (see Figure 10-5 above)

ITMO456

28

Configuring Printers

◆ Clicking Manage Job allows you to view, modify, and delete print jobs that have submitted to the queue

- Regular users can use the CUPS Web administration tool and select the Jobs tab to manage their own jobs

◆ Server section allows editing of CUPS configuration file and log file access

- Also allows advanced function management

ITMO456

29

The LPD Printing System

◆ Line Printer Daemon (LPD)

- Printing system used on older Linux systems

- Places a copy of the print job into a temporary directory on the filesystem called the **print queue**, provided the printer is **enabled**

- If the printer is **disabled**, then the lpd prints an error message stating the printer is not accepting print jobs

ITMO456

Printer Administration: LPD System

◆ **`lpr`** command

- Create print jobs in print queue

◆ **`lpc`** command

- View status of printers

◆ **`lpq`** command

- View print jobs in print queue

◆ **`lprm`** command

- Remove print jobs
- Assigns the print job a unique **print job ID**

ITMO456

Printer Administration: LPD System

◆ CUPS contains versions of (aliases to) the `lpr`, `lpc`, `lpq`, and `lprm` commands

ITMO456

Printer Administration: Managing Print Jobs

◆ Postscript

- Non-text file format commonly used in documents

◆ `enscript` command

- Command used to print Postscript formatted files

◆ `a2ps` command

- Other command also used to print Postscript formatted files

ITMO456

Printer Administration: Configuring Printers

ITMO456

◆ **`/etc/cups/cupsd.conf`**

- Contains cupsd settings

◆ **`/etc/cups/printers.conf`**

- Contains each printer's configuration information

◆ **`/etc/printcap`**

- File holding configuration information for each printer installed on the system (pre-CUPS)

◆ Printer Configuration tool

- Used to configure printers e.g., add new printers
- Activated using the **`system-config-printer`** command in a desktop environment

Printer Administration: Configuring Printers

◆ For local printers, must choose printer port

- Such as `/dev/lp0`

◆ For remote printers, specify name or IP address of remote server, printer name, or printer port

◆ Enable sharing as needed

- CUPS can automatically search for other shared CUPS printers
  - Allow remote computers to print using the LPD protocol

ITMO456

Printer Administration: Configuring Printers

ITMO456

◆ For local printers that do not support PnP, must specify the Uniform Resource Identifier (URI) for the device

◆ Within Printer Configuration tool you can:

- Give a printer a name to identify it within programs and commands

- Specify printer location and description

- Modify printer properties

- Manage the status of the printer, share it using IPP, choose an error action, and configure banner pages

Printer Administration: Configuring Printers

◆ **`/etc/printcap.local`**

- ▪ A file that holds printer configuration information for each printer installed on the system

◆ Although the Printer Configuration Tool or the CUPS Web interface are the easiest methods for creating printers, you may also add printers by editing the **`/etc/printcap.local`** file

ITMO456

Adding PDF Printing to Linux

◆ Install `cups-pdf`

- Fedora (as root): `yum install cups-pdf`
- Ubuntu: `sudo apt-get install cups-pdf`

◆ This will add a new printer named **Cups-PDF** (Fedora) or **PDF** (Ubuntu)

- If no printer is installed, it will become your default printer
- Output goes to your home directory (Fedora) or to a directory named "PDF" in your home directory (Ubuntu)

ITM0456

38

Time & Date

◆ Hardware clock keeps time when system is powered down

- Not used by most programs while the system is running

◆ Most programs refer to the software clock

- Set from the hardware clock when the computer boots or using Network Time Protocol (NTP)

ITMO456

Time & Date

◆ Linux sets clock to Coordinated Universal Time (UTC)

- For most purposes identical to Greenwich Mean Time (GMT)
- Settings in **/usr/share/zoneinfo**, **/etc/localtime, /etc/timezone**
- **date** displays or sets date & time

◆ **hwclock** displays or sets the system hardware clock

ITMO456

40

Time & Date

ITMO456

```
[root@localhost ~]# ll /etc/localtime
lrwxrwxrwx. 1 root root 37 Sep 27 21:05 /etc/localtime -> ../usr/share/zoneinfo/America/Chicago
[root@localhost ~]# date
Tue Oct 25 12:46:47 CDT 2016
[root@localhost ~]# hwclock
2016-10-25 12:46:52.821923-6:00
[root@localhost ~]#
```

```
root@itmo-456-ubuntu-server:~# ll /etc/localtime
-rw-r--r-- 1 root root 3559 Nov 30 12:16 /etc/localtime
root@itmo-456-ubuntu-server:~# cat /etc/timezone
America/Chicago
root@itmo-456-ubuntu-server:~# date
Tue Mar  1 15:24:26 CST 2016
root@itmo-456-ubuntu-server:~# hwclock
Tue 25 Oct 2016 02:49:11 AM CDT  -0.255637 seconds
root@itmo-456-ubuntu-server:~# _
```

41

Time & Date

◆ NTP – Network Time Protocol – allows clocks to be set to a distributed standard

- Selected at installation for Fedora 24

- Runs **chronyd**

- Use **timedatectl** to view time/date settings. NTP Settings in /etc/chrony.conf

- system-config-date for GUI tool

- For datacenter use may want to create local NTP server

ITMO456

Time & Date

ITMO456

```
[root@itmo456 ~ ]# timedatectl status
      Local time: Sun 2015-10-25 20:23:46 CDT
  Universal time: Mon 2015-10-26 01:23:46 UTC
        RTC time: Mon 2015-10-26 01:23:46
       Timezone: America/Chicago (CDT, -0500)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: yes
 Last DST change: DST began at
                  Sun 2015-03-08 01:59:59 CST
                  Sun 2015-03-08 03:00:00 CDT
 Next DST change: DST ends (the clock jumps one hour backwards) at
                  Sun 2015-11-01 01:59:59 CDT
                  Sun 2015-11-01 01:00:00 CST
[root@itmo456 ~ ]# systemctl status chronyd
chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled)
   Active: active (running) since Sat 2015-10-24 15:07:20 CDT; 1 day 5h ago
  Process: 704 ExecStartPost=/usr/libexec/chrony-helper add-dhclient-servers (code=exited, status=0/SUCCESS)
  Process: 668 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 683 (chronyd)
   CGroup: /system.slice/chronyd.service
           └─683 /usr/sbin/chronyd

Oct 24 15:07:17 itmo456.iit.edu chronyd[683]: chronyd version 1.31.1 starting
Oct 24 15:07:19 itmo456.iit.edu chronyd[683]: Frequency -17.538 +/- 0.015 ppm read from /var/lib/chrony/drift
Oct 24 15:07:20 itmo456.iit.edu systemd[1]: Started NTP client/server.
Oct 24 15:07:43 itmo456.iit.edu chronyd[683]: Selected source 38.229.71.1
Oct 24 15:07:43 itmo456.iit.edu chronyd[683]: System clock wrong by 1.402094 seconds, adjustment started
Oct 24 15:07:45 itmo456.iit.edu chronyd[683]: Selected source 132.163.4.101
```

Time & Date

◆ NTP – Network Time Protocol – allows clocks to be set to a distributed standard

- Ubuntu 14.04 comes with **ntpdate**
  - Ran once at boot to sync system clock
- To install **ntpd**:
  - **sudo apt-get install ntp**
- Configuration located in /etc/ntp.conf
- Use **ntpq** to query more time information

ITMO456

44

Time & Date

ITMO456

```
root@itmo456-server:~# grep ^server /etc/ntp.conf
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org
server ntp.ubuntu.com
root@itmo456-server:~# service ntp reload
root@itmo456-server:~# service ntp status
 * NTP server is running
root@itmo456-server:~# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 nisttime.carson  .ACTS.           1 u    6   64    7   20.951  -10.290   1.634
 gopher.fart.web  106.61.18.129    3 u    5   64    7   76.068  -10.883  13.591
 clock.trit.net   69.36.224.15     2 u   10   64    7   74.980  -16.046   4.439
 leeloo.scurvyne  173.162.192.156  2 u   10   64    7   75.977   -8.491   3.316
 golem.canonical  193.79.237.14    2 u   13   64    7  103.466   -9.459   1.658
root@itmo456-server:~# _
```

Log Files

ITM0456

◆ Linux log files record key details about system operation

- Typically recorded during daemon activity

- Information includes error messages

◆ Most system logs are in `/var/log`

- Many programs store log files in subdirectories

46

Log Files

◆ Traditional Linux system log daemon is `rsyslogd`

◆ New daemon is Systemd Journal Daemon (`journald`)

Log File Administration

Log File	Description
boot.log	Contains information regarding daemon startup obtained during system initialization
cron	Contains information and error messages generated by the cron and at daemons
dmesg	Contains detected hardware information obtained during system startup
maillog	Contains information and error messages generated by the sendmail daemon
secure	Contains information and error messages regarding network access generated by the sshd and xinetd daemons
wtmp	Contains a history of all login sessions
rpmpkgs yum.log	Contains a list of packages installed by the Red Hat Package Manager and related error messages

Table 10-3: Common Linux log files found in **/var/log**

ITMO456

Log File Administration

Log File	Description
xferlog	Contains info & error messages generated by the FTP daemon
Xorg.0.log	Contains info and error messages generated by X Windows
lastlog	Contains a list of users and their last login time; must be viewed using the `lastlog` command
messages	Contains info regarding daemon startup obtained at system initialization as well as important system messages produced after system initialization
uucp	Contains information and error messages generated by the uucp (UNIX to UNIX copy) daemon; these messages typically involve modem communication

Table 10-3: Common Linux log files found in `/var/log`

ITMO456

Log Rotation

◆ **`logrotate`** command

- Back up and clear log files
- Compress old log files and save under new name

◆ Controlled via **`/etc/logrotate.conf`**

- Normally refers to files in **`/etc/logrotate.d`**
- Tells system whether to rotate logs at fixed intervals or when they reach particular sizes

ITMO456

Log Rotation

◆ When a log rotates, it's renamed, possibly compressed, a new log file is created, and the oldest archived log file may be deleted

ITMO456

Log Rotation

```
[root@itm456 ~]# ll /var/log/*-*
-rw-------. 1 root utmp      768 Sep 27 19:53 /var/log/btmp-20131001
-rw-r--r--. 1 root root    47806 Oct  6 03:36 /var/log/cron-20131006
-rw-r--r--. 1 root root    35528 Oct 13 03:42 /var/log/cron-20131013
-rw-r--r--. 1 root root    70587 Oct 20 03:18 /var/log/cron-20131020
-rw-r--r--. 1 root root    48061 Oct 27 03:48 /var/log/cron-20131027
-rw-------. 1 root root      173 Oct  5 23:14 /var/log/maillog-20131006
-rw-------. 1 root root     1040 Oct 12 19:47 /var/log/maillog-20131013
-rw-------. 1 root root     2358 Oct 16 12:13 /var/log/maillog-20131020
-rw-------. 1 root root      784 Oct 23 14:52 /var/log/maillog-20131027
-rw-------. 1 root root  1161767 Oct  6 03:36 /var/log/messages-20131006
-rw-------. 1 root root  1566901 Oct 13 03:37 /var/log/messages-20131013
-rw-------. 1 root root 18867940 Oct 20 03:15 /var/log/messages-20131020
-rw-------. 1 root root     4318 Oct  5 23:15 /var/log/secure-20131006
-rw-------. 1 root root    11791 Oct 12 20:26 /var/log/secure-20131013
-rw-------. 1 root root    31004 Oct 16 19:16 /var/log/secure-20131020
-rw-------. 1 root root        0 Sep 29 20:18 /var/log/spooler-20131006
-rw-------. 1 root root        0 Oct  6 03:36 /var/log/spooler-20131013
-rw-------. 1 root root        0 Oct 13 03:42 /var/log/spooler-20131020
-rw-------. 1 root root        0 Oct 20 03:18 /var/log/spooler-20131027
```

ITM456

The System Log Daemon

ITMO456

◆ Systemlog daemon (`rsyslog`)

- Logs system events to various log files
- Creates `/dev/log` socket for system processes to write to
- Uses `/etc/rsyslog.conf`
  - Entries indicate facility and priority

◆ Facility

- Area of system that information is gathered from

◆ Priority

- Importance of system information

The System Log Daemon

Facility	Description
auth or **security**	Specifies messages from the login system such as the login program, the getty program, and the su command
authpriv	Specifies messages from the login system when authenticating users across the network or to system databases
cron	Specifies messages from the cron and at daemons
daemon	Specifies messages from system daemons such as the FTP daemon
kern	Specifies messages from the Linux kernel
lpr	Specifies messages from the printing system (lpd)
mail	Specifies messages from the e-mail system (sendmail)
mark	Used internally only; specifies timestamps used by syslogd
news	Specifies messages from the Inter Network News daemon and other USENET daemons
syslog	Specifies messages from syslogd
user	Specifies messages from user processes
uucp	Specifies messages from the uucp (UNIX to UNIX copy) daemon
local0-7	Specifies local messages; these are not used by default but may be defined for custom use

Table 10-4: Facilities used by the system log daemon

ITM0456

The System Log Daemon

ITM0456

Priority	Description
debug	Indicates all information from a certain facility
info	Indicates normal information messages as a result of system operations
notice	Indicates information that should be noted for future reference, yet does not indicate a problem
warning or **warn**	Indicates messages that may be the result of an error but are not critical to system operations
error or **err**	Indicates all other error messages not described by other priorities
crit	Indicates critical system errors such as hard disk failure
alert	Indicates an error that should be rectified immediately, such as a corrupt system database
emerg or **panic**	Indicates very serious system conditions that would normally be broadcast to all users

Table 10-5: Priorities used by the log daemon

Using the Systemd Journal Daemon

ITMO456

◆ The Systemd Journal Daemon replaces the System Log Daemon on Linux distributions that use Systemd

- Fedora

◆ Similar to System Log Daemon

- Events logged are not controlled by specific rules

56

Using the Systemd Journal Daemon

◆ **journald** logs all info to a database under the **/var/log/journal** directory structure

- Events are tagged with same facility and priority information as the **rsyslogd** daemon

ITMO456

Using the Systemd Journal Daemon

ITMO456

◆ **`journalctl`** command: use to view events within the journald database

◆ Type **`journalctl`** and press the Tab key to see a list of areas and criteria that can be queried

◆ You can query events related to a specific process or daemon

- ▪ If you specify the path name to the executable file or PID

Managing Log Files and the Journald Database

◆ For systems using Systemd

- Limit the size of the **journald** database by uncommenting and configuring the **SystemMaxUse** line in **/etc/systemd/journald.conf**

◆ To prevent key older events from being overwritten, create a shell script that executes necessary **journalctl** commands to either print or save them to a text file

ITMO456

Administering Users and Groups

◆ User account

- Information regarding a user that is stored in a system database

◆ Authentication

- Act of verifying a user's identity

- Compare username and password to a system database

◆ Database containing user account information typically consists of two files:

- `/etc/passwd` – user account information

- `/etc/shadow` – encrypted password information

ITMO456

Administering Users and Groups

ITMO456

◆ **pwconv** command

- Convert system to use an **/etc/shadow** file for encrypted password storage

◆ **pwunconv** command

- Revert back to using an **/etc/passwd** file only
  - You would never want to do this in a production environment

Administering Users and Groups

◆ User Identifier (UID)

- Specifies the unique user ID assigned to each user

◆ Group Identifier (GID)

- Primary group ID for each user

◆ Primary group

- Group owner for all files created by a user

- Specified in **/etc/passwd** file

ITMO456

Administering Users and Groups

◆ General Electric Comprehensive Operating System (GECOS)

- Field in `/etc/passwd` file containing user account description

◆ Root user usually listed at top of `/etc/passwd` file

- Next are listed system daemons then users

◆ `/etc/shadow`

- Password field contains encrypted password

◆ `/etc/passwd`

- Password field contains an x (not used)

ITMO456

Administering Users and Groups

◆ **`lastchange`** field

- ▪ Date of most recent password change
  - ● Located in /etc/shadow

- ▪ Number represents number of days since January 1, 1970
  - ● Called Unix Time

ITMO456

passwd File Contents

ITMO456

user1:x:1000:1000:Sean Hughes-Durkin,,,:/home/user1:/bin/bash

passwd File Contents

◆ Username ■

◆ x in lieu of password ■

◆ User ID (UID) ■

◆ Default group ID (GID) ■

◆ GECOS ■

◆ Home directory path ■

◆ Login shell ■

ITMO456

66

`shadow` File Contents

user1:6VbsIeV7p$01sL6ZKB2tZFGgnVqg7g8CwX0BmDn1cies13up5aKG4FcwfrZqYy28pOsdxQX08mGfQUzHbufFJ4xQ5.1XvDU.:17099:0:99999:7:::

ITMO456

`shadow` File Contents

◆ User login name ■

◆ Hashed password ■

◆ Date of last password change ■

◆ Minimum password age ■

◆ Maximum password age ■

◆ Days warning for password expiration ■

◆ Days before account inactive

◆ Days since epoch when account expires

ITMO456

Administering Users and Groups

◆ Passwords often set to expire at certain intervals

- Intervals specified in **/etc/shadow**

◆ **/etc/group** file

- Lists all groups and their members
- Allows users to belong to multiple groups
- Password field usually contains an x

ITMO456

Creating User Accounts

◆ **useradd** command

- ▪ Add new user accounts
- ▪ Normally **/usr/sbin/useradd**

◆ Most new user information comes from two files

- ▪ **/etc/login.defs**
  - ● E-mail location, password expiration, minimum password length, range of UIDs and GIDs
- ▪ **/etc/default/useradd**
  - ● default primary group, home directory location, password expiration info, shell, skeleton directory

ITMO456

Creating User Accounts

◆ Skeleton directory

▪ Contains files copied to all new users' home directories upon creation

▪ **`/etc/skel`** is Fedora default

▪ Override these defaults by specifying options to **`useradd`** command

◆ **`passwd`** command

▪ Set a user's password

▪ If no arguments, sets current user's password

▪ User accounts must have password set to log on

▪ Root user can change any user's password

ITMO456

Creating User Accounts

◆ Using **useradd**

```
# /usr/sbin/useradd -g 200
-c "Walter T. Door" -s /bin/bash
-d /home/door/wtdoor wtdoor
```

◆ After adding user, set password with **passwd** command

```
# passwd wtdoor
changing password for user wtdoor
New password:
Retype new password:
passwd: all authentication tokens updated
successfully
```

ITM0456

Creating User Accounts

ITMO456

Option	Description
-c *"description"*	Adds a description for the user to the GECOS field of /etc/passwd
-d *homedirectory*	Specifies the absolute pathname to the user's home directory
-e *expirydate*	Specifies a date to disable the account from logging in
-f *days*	Specifies the number of days after a user account with an expired password is disabled
-g *group*	Specifies the primary group for the user account; by default in Red Hat Linux, a group is created with the same name as the user and made the primary group for that user
-C *group1, group2, etc.*	Specifies all other group memberships for the user account
-m	Specifies that a home directory should be created for the user account; by default in Red Hat Linux, home directories are created for all users via an entry in the /etc/login.defs file
-k *directory*	Specifies the skeleton directory used when copying files to a new home directory
-s *shell*	Specifies the absolute pathname to the shell used for the user account
-u *UID*	Specifies the UID of the user account

Table 10-6: Common options to the `usradd` command

Modifying User Accounts

ITMO456

◆ `usermod` command

  ▪ Modify user account information

◆ `chage` command

  ▪ Modify password expiration information

◆ Locking an account

  ▪ Make an account temporarily unusable

  ▪ Alter password information

  ▪ Use `-l` with `passwd` command to lock account

  ▪ Use `chsh` command to change a valid shell to an invalid shell

Modifying User Accounts

ITM0456

Option	Description
-c *"description"*	Specifies a new description for the user in the GECOS field of /etc/passwd
-d *homedirectory*	Specifies the absolute pathname to a new home directory
-e *expirydate*	Specifies a date to disable the account from logging in
-f *days*	Specifies the number of days after a user account with an expired password is disabled
-g *group*	Specifies a new primary group for the user account
-G *group1, group2, etc.*	Specifies all other group memberships for the user account
-l *name*	Specifies a new login name
-s *shell*	Specifies the absolute pathname to a new shell used for the user account
-u *UID*	Specifies a new UID for the user account

Table 10-7: Common options to the `usrmod` command

Deleting User Accounts

◆ **`userdel`** command

- Remove a user account from the system
- Specify user name as argument

◆ When a user account is deleted, files previously owned by the user become owned by a number representing the UID of the deleted user

- Next user with that UID will own the files

ITM0456

Managing Groups

◆ Can add groups by editing **/etc/group**

◆ **groupadd** command

- Add a group to the system

◆ **groupmod** command

- Modify the name of GID of a group on the system

◆ **groupdel** command

- Remove a group from the system

ITMO456

Managing Groups

◆ **`groups`** command
- List groups that a user belongs to

◆ **`id`** command
- List GIDs of groups that a user belongs to

◆ **`newgrp`** command
- Temporarily change user's primary group

◆ Graphical utilities exist to create, modify, and delete user and group accounts

ITMO456

Using User Manager

ITMO456
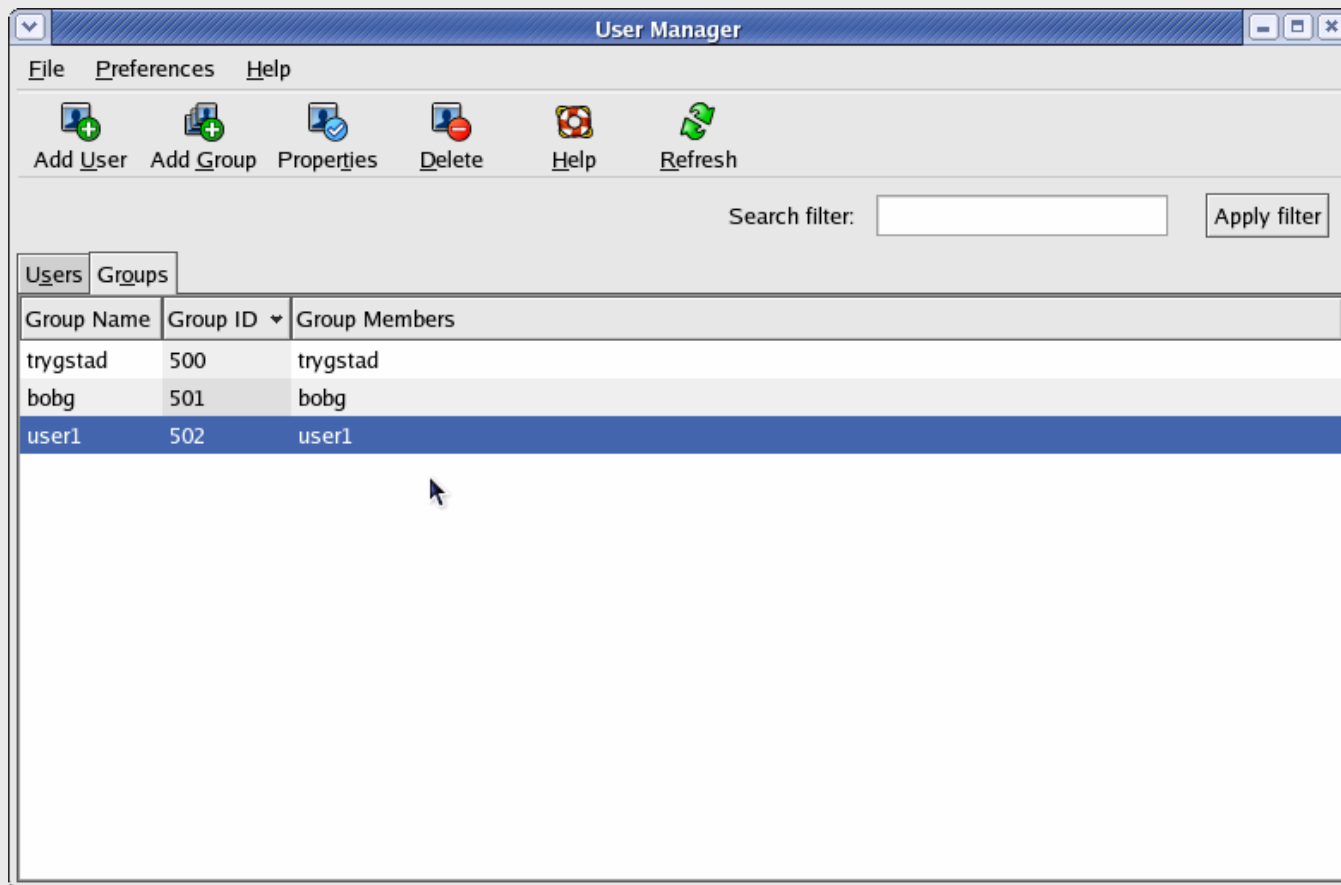
Figure 10-13: Configure users and groups with a desktop environment

Using User Manager

ITM456

Configure users and groups with a desktop environment
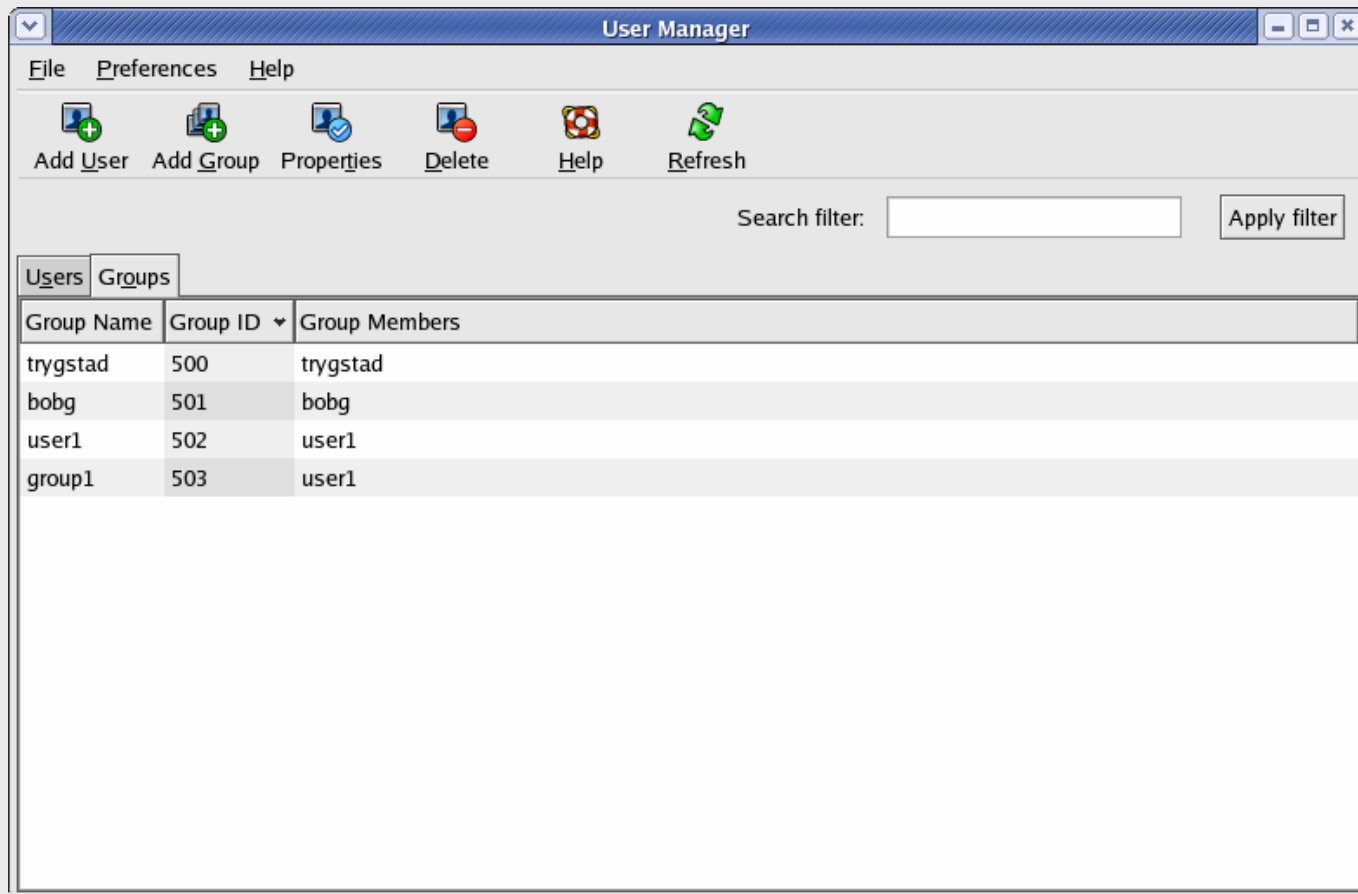
Using User Manager

Viewing groups in the User Manager

Using User Manager
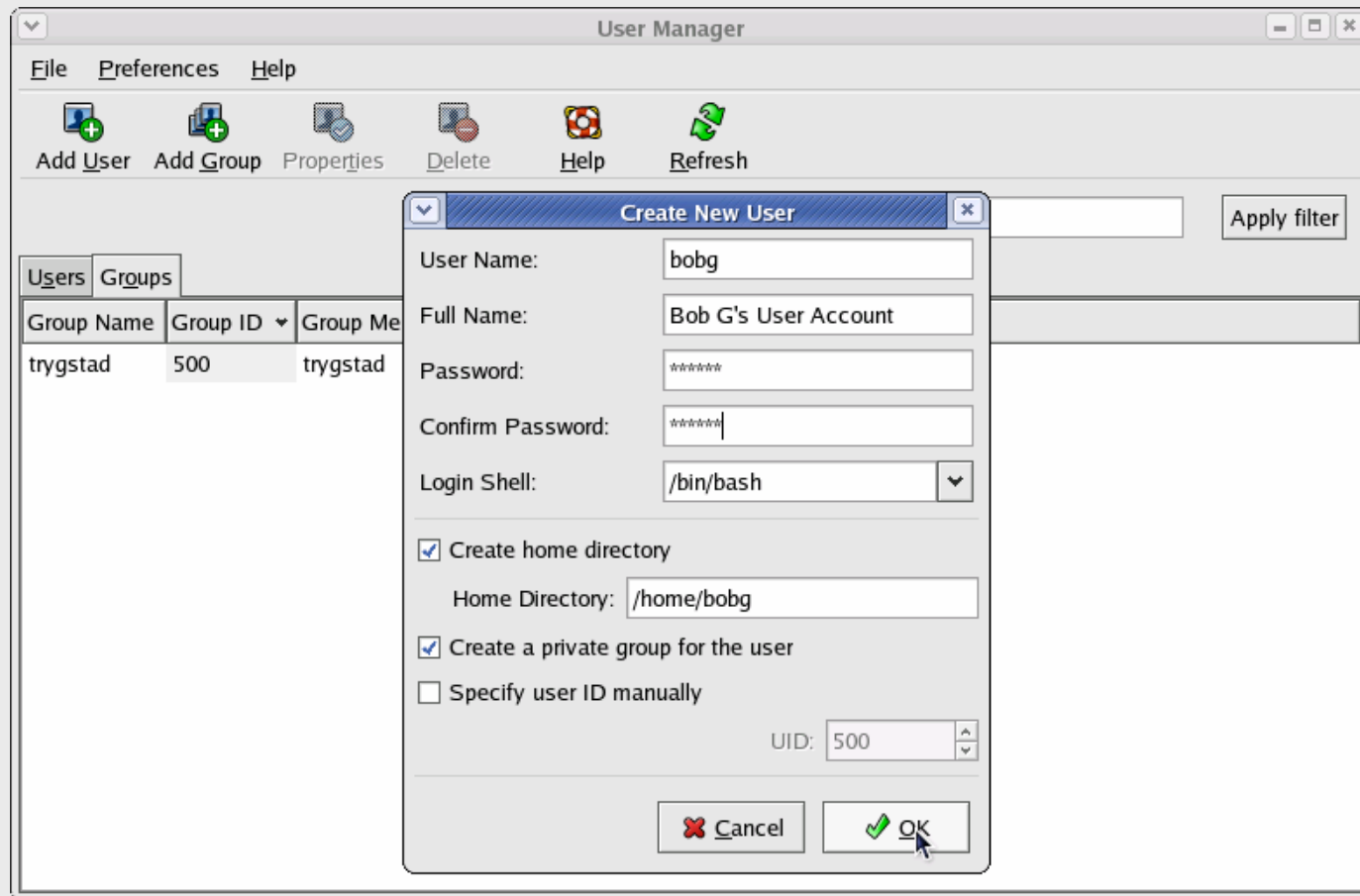
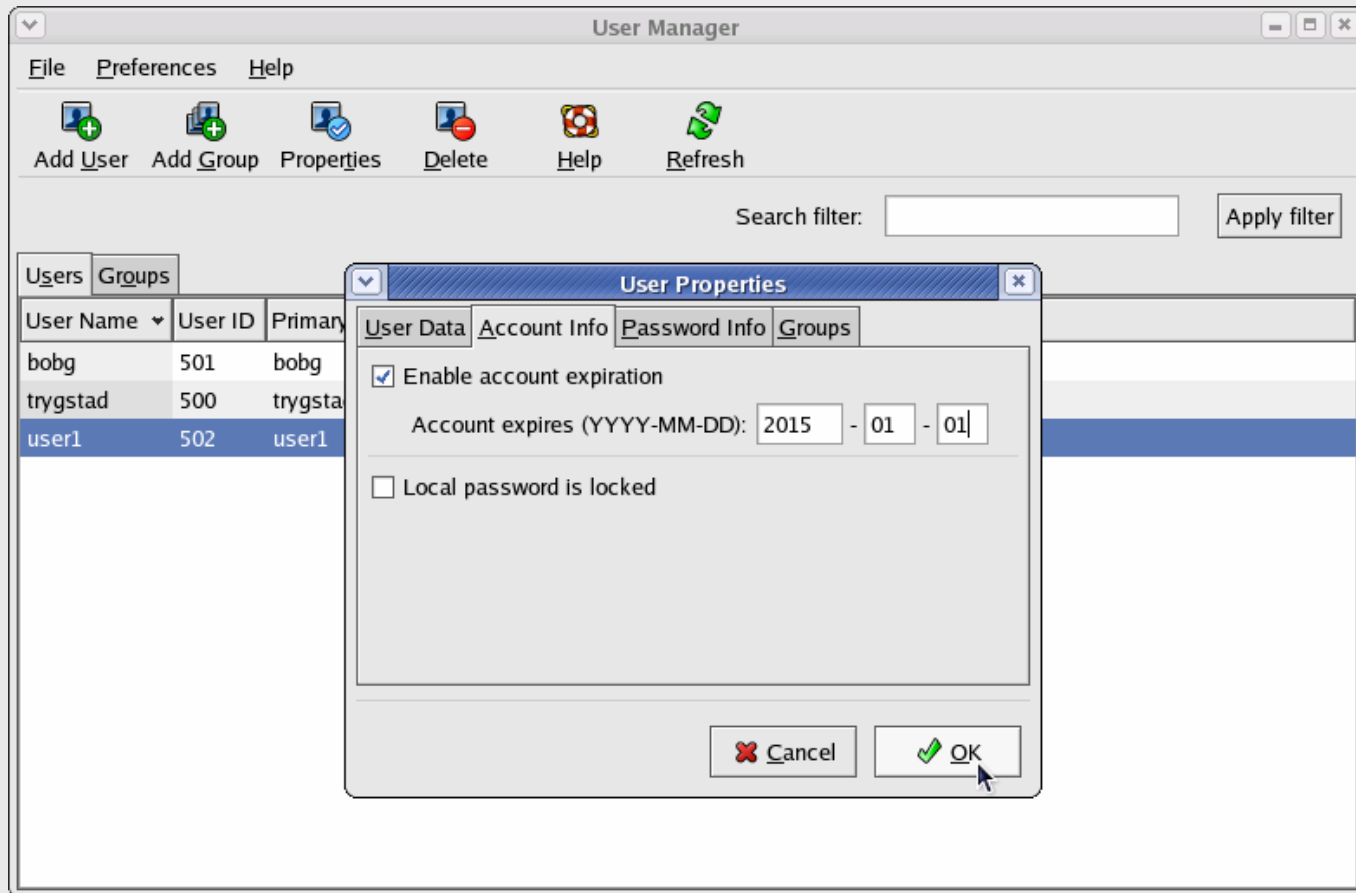Creating a new account with User Manager

Using User Manager
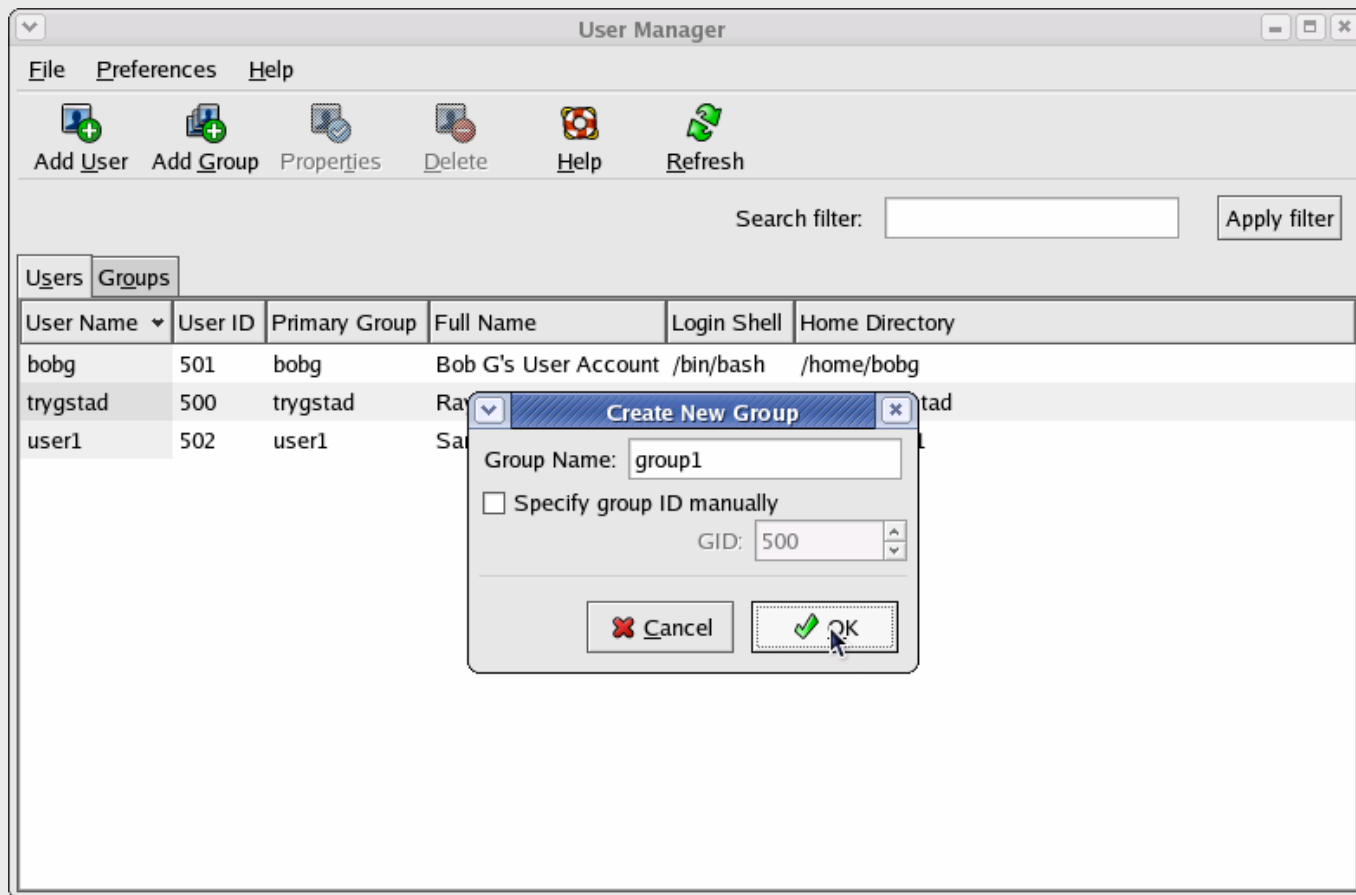
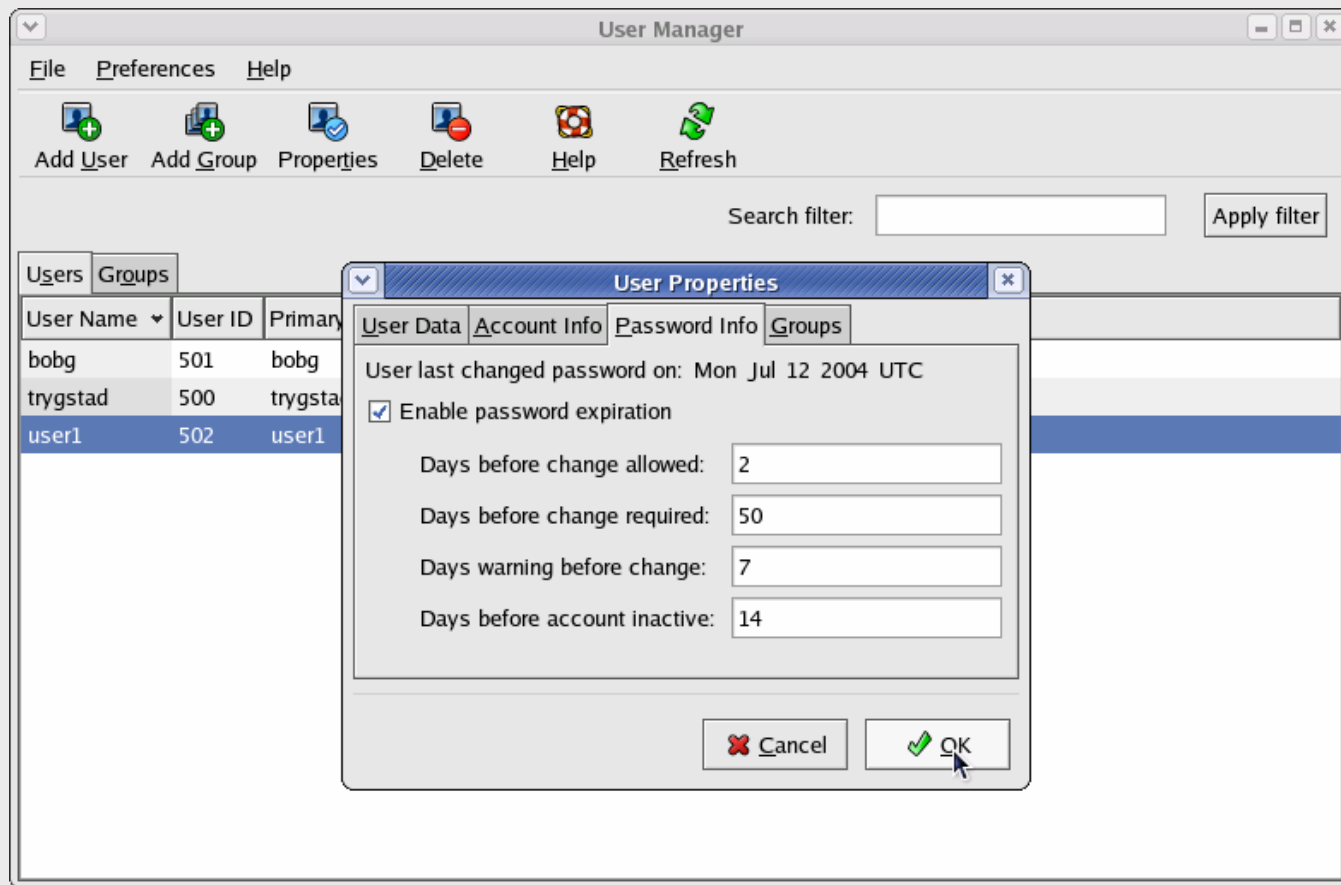Creating a new group account

ITM0456

Using User Manager

ITMO456
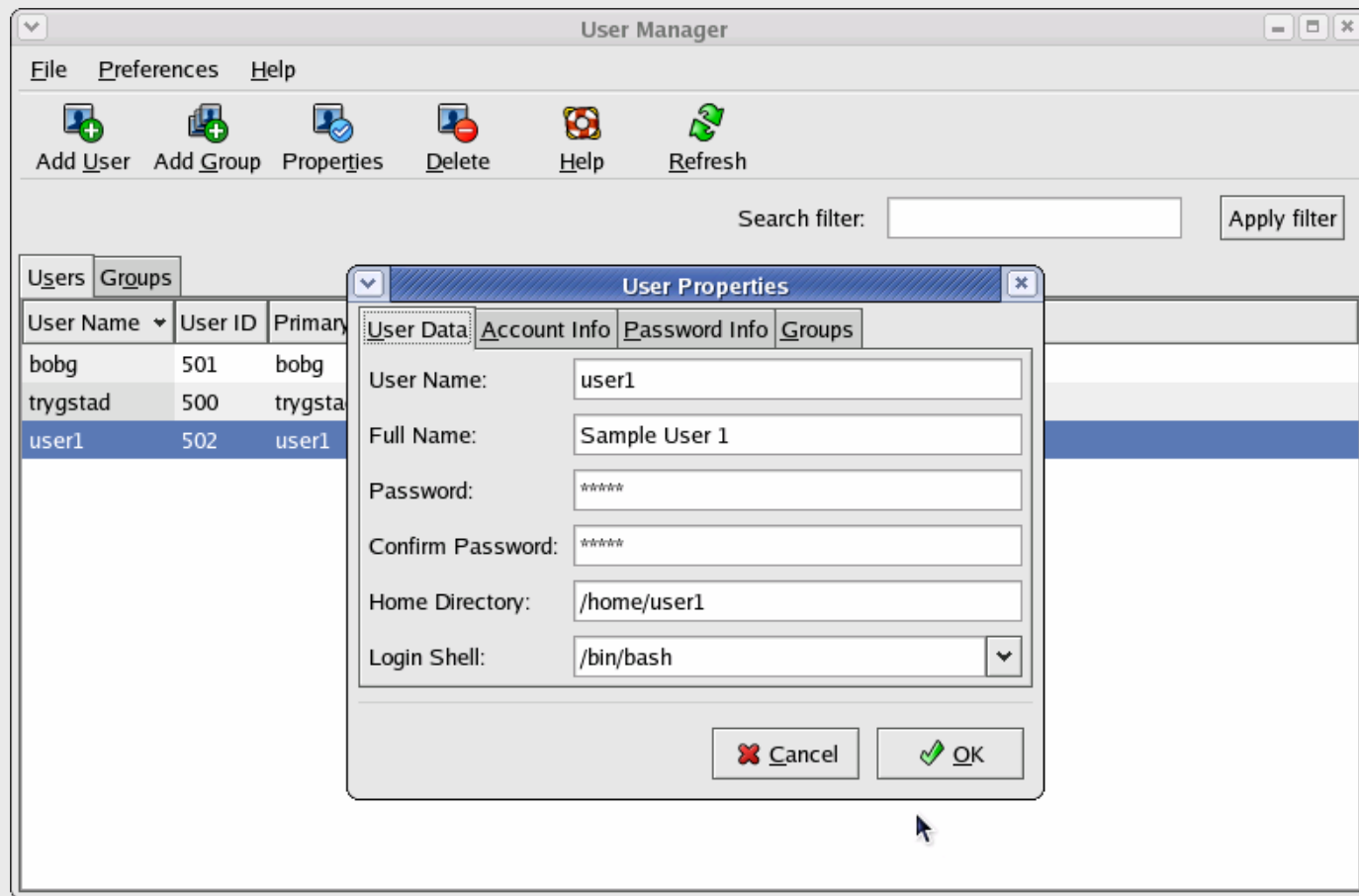
Editing the properties of a user account
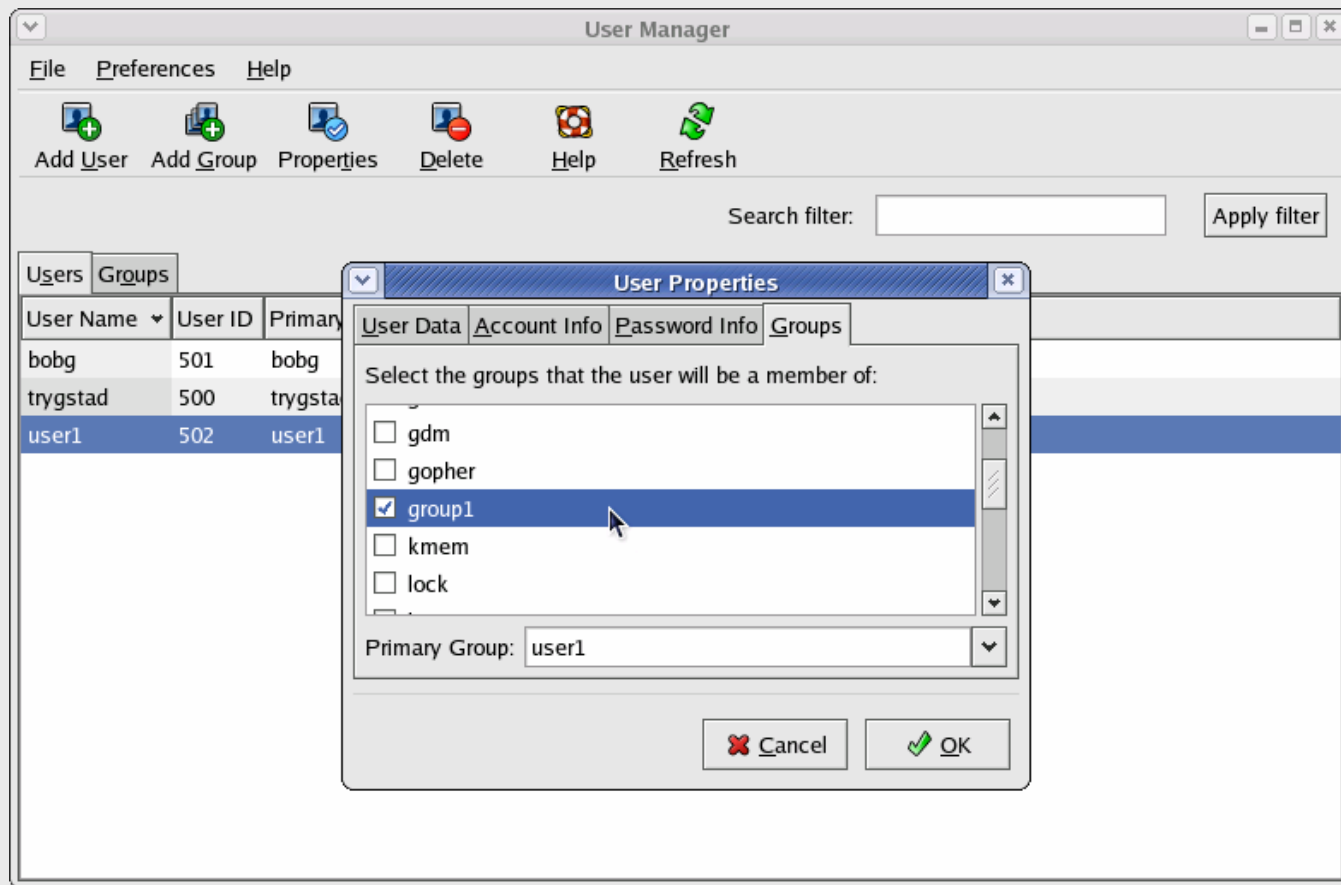
Using the Red Hat User Manager

ITMO456

Editing the disable date & lockout of a user account
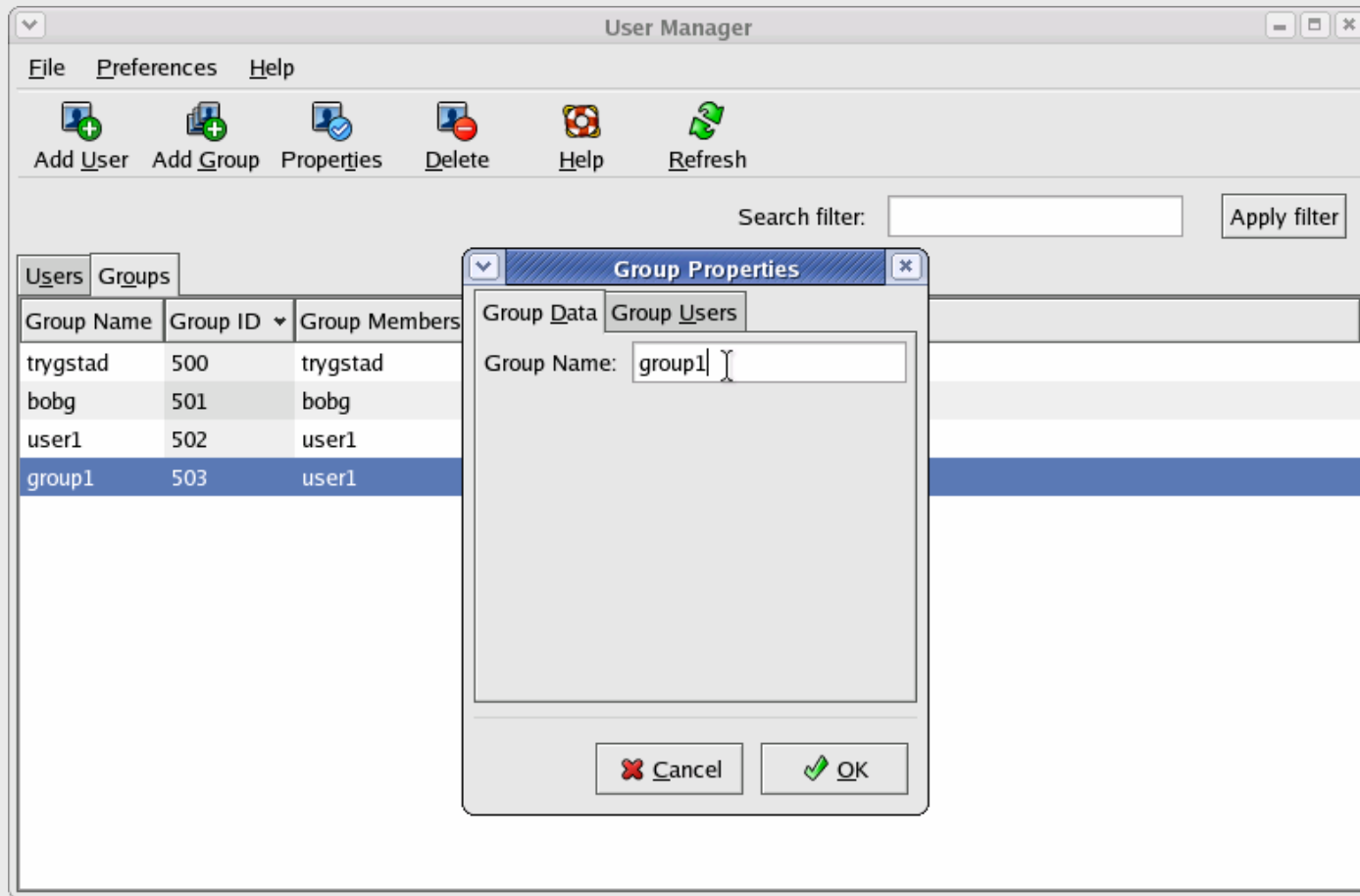
Using User Manager

ITMO456

Editing the password expiration parameters of a user account

Using User Manager

ITMO456

Editing the group membership of a user account

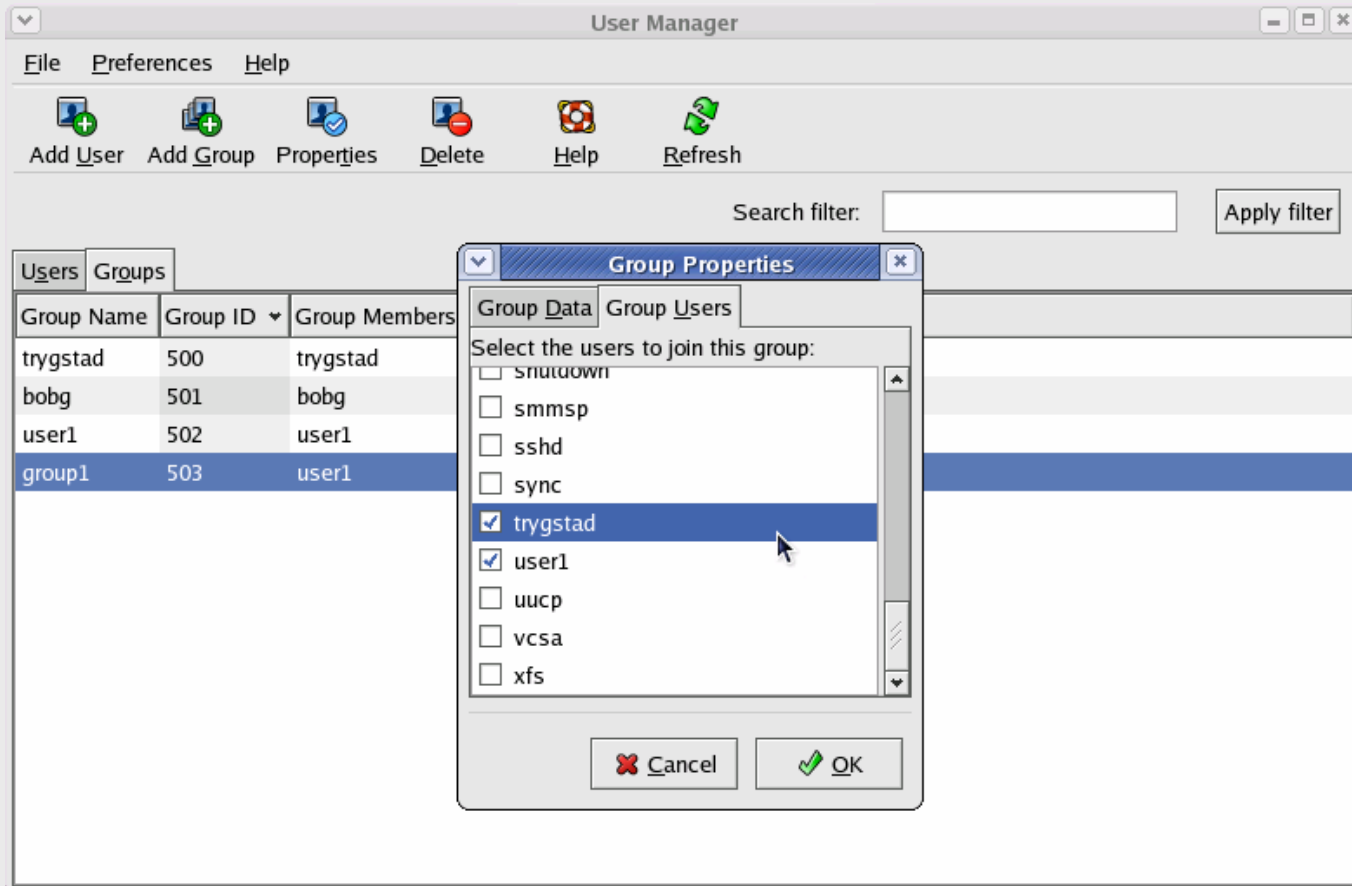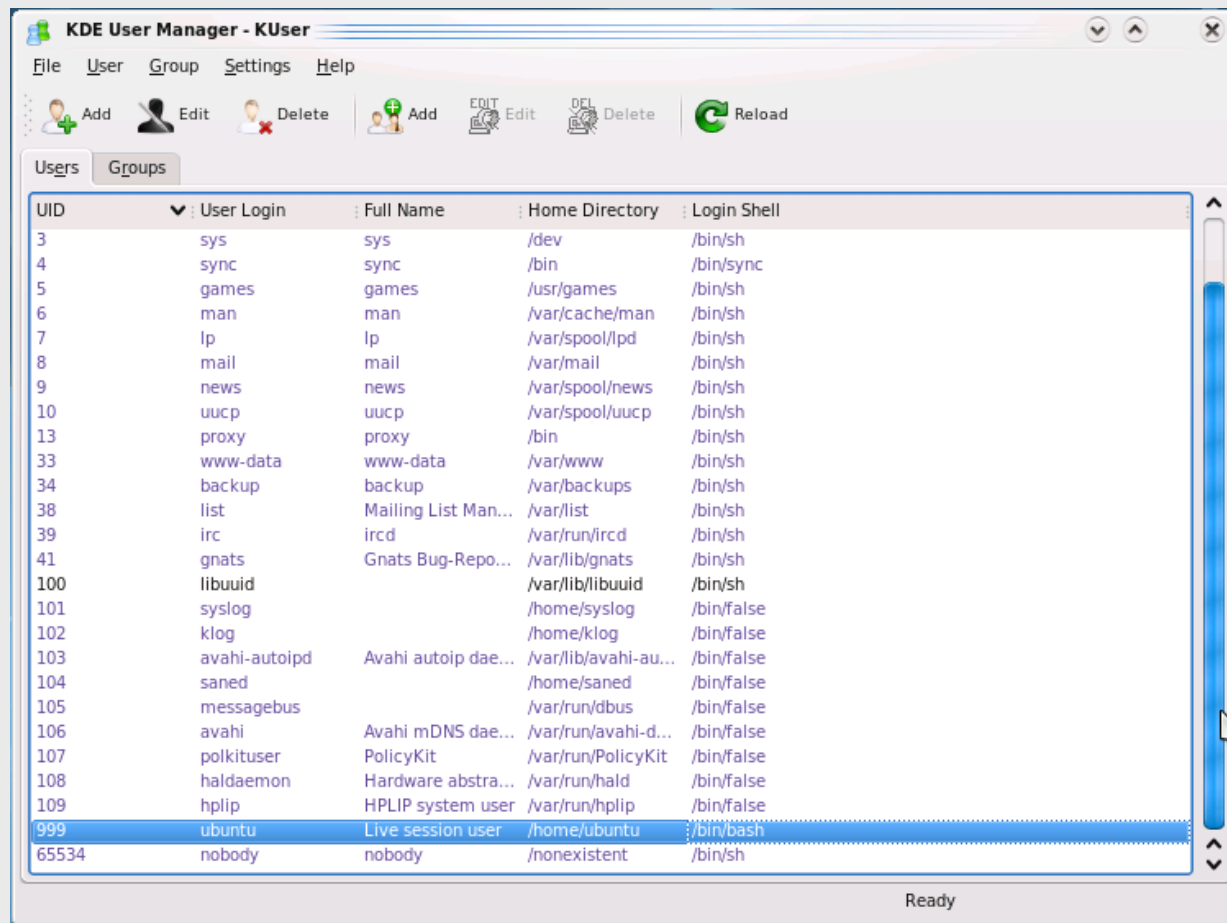# Using User Manager

Editing a group name

Using User Manager

Editing the members of a group

Using User Manager

KDE User Manager (from Kubuntu)

ITMO456

Summary

◆ Print jobs are spooled to a print queue

◆ Can configure spooling or printing by using the **accept**, **reject**, **enable**, and **disable** commands

◆ Print jobs are created using **lp**, can be viewed in the queue using **lpstat**, and are removed from the queue using **cancel**

◆ Create local and remote printers using Printer Configuration, the KDE Wizard or **/etc/cups/printers.conf**

ITMO456

Summary

◆ Clocks in Linux are set to UTC and have files to support local time

◆ Often system clock is set using NTP

◆ Most log files in Linux are stored in `/var/log`

◆ System events are typically logged to files by the System Log Daemon or to a database by the Systemd Journal Daemon

ITMO456

Summary

ITMO456

◆ You can use the `journalctl` command to view the contents of the journald database

◆ Log files should be cleared or rotated over time to save disk space

◆ User and group account information is typically in `/etc/passwd`, `/etc/shadow`, and `/etc/group`

Summary

ITMO456

◆ Use the **`useradd`** command to create users and the **`groupadd`** command to create groups

◆ All users must have a valid password before logging into a Linux system

◆ Users may be modified with **`usermod`**, **`chage`**, **`chsh`**, and **`passwd`** commands, and groups may be modified using **`groupmod`** command

Summary

ITMO456

◆ The **userdel** and **groupdel** commands may be used to remove users and groups from the system, respectively

◆ User Manager is a graphical utility that can manage users and groups on the system from a desktop environment

The End…

◆Questions?

ITMO456