RH124

Copyright © 2011 Red Hat, Inc.

RH124-RHEL6-EN-20110211

Red Hat System Administration I
Student Workbook
Red Hat Enterprise Linux 6
Release en-2-20110211

RED HAT SYSTEM ADMINISTRATION I

Red Hat Enterprise Linux 6 RH124
Red Hat System Administration I
Edition 2

Author	George Hacker
Author	Forrest Taylor
Editor	Steven Bonneville
Editor	Mark Howson

Copyright © 2011 Red Hat, Inc.

The contents of this course and all its modules and related materials, including handouts to audience members, are Copyright © 2011 Red Hat, Inc.

No part of this publication may be stored in a retrieval system, transmitted or reproduced in any way, including, but not limited to, photocopy, photograph, magnetic, electronic or other record, without the prior written permission of Red Hat, Inc.

This instructional program, including all material provided herein, is supplied without any guarantees from Red Hat, Inc. Red Hat, Inc. assumes no liability for damages or legal action arising from the use or misuse of contents or details contained herein.

If you believe Red Hat training materials are being used, copied, or otherwise improperly distributed please e-mail training@redhat.com or phone toll-free (USA) +1 (866) 626-2994 or +1 (919) 754-3700.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, Hibernate, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a registered trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Contributors: Rob Locke, Bowe Strickland, Joshua Hoffman, Chris Negus, Andrew Dingman

Document Conventions vii
Notes and Warnings ... vii

Introduction ix
Welcome to class! ... ix
About Red Hat Enterprise Linux ... ix
Additional Red Hat Enterprise Linux Software ... x
Contacting Red Hat Technical Support ... xii

About This Course xv
Red Hat System Administration I ... xv
Structure of the Course ... xv
Orientation to the Classroom Network ... xvi

Internationalization xvii
Language Support ... xvii
System-wide Default Language ... xvii
Per-user Language Selection ... xvii
Input Methods ... xviii
Language Codes Reference ... xviii

1. Get Started with the GNOME Graphical Desktop 1
Using the GNOME Desktop ... 2
Editing Files with **gedit** ... 5
Criterion Test ... 7

2. Manage Files Graphically with Nautilus 11
Using Nautilus ... 12
Accessing Remote File Systems in Nautilus ... 15
Criterion Test ... 17

3. Get Help in a Graphical Environment 21
Research Local Documentation ... 22
Research On-line Documentation ... 25
Getting the Most from Red Hat Global Support Services ... 27
Criterion Test ... 29

4. Configure Local Services 33
Understand the Role of the root User ... 34
Manage the System Clock ... 37
Configure Printers ... 39
Manage Print Jobs ... 42
Criterion Test ... 44

5. Get Started with Bash 47
Introduction to Bash ... 48
Using Bash ... 51
Launching Graphical Tools from Bash ... 55
Criterion Test ... 58

6. Manage Physical Storage I 61
Describe MBR, Primary, Extended, and Logical Partitions ... 62
List Available Disk Devices ... 65
Introduce Classroom Virtual Machines ... 67
Create a New Disk Partition, Format It with a File System and Use It ... 69

Criterion Test 71

7. Manage Logical Volumes 75
General LVM Concepts and Terms 76
Displaying Current LVM Usage 79
Initial LVM Deployment 81
Extending a Volume Group 84
Extending a Logical Volume 86
Removing a Physical Volume 88
Criterion Test 90

8. Monitor System Resources 93
Understand Process, Priority, and Signal Concepts 94
Monitor Processes by CPU or Memory Consumption 96
Manage Running Processes 98
Monitor Disk Usage 101
Criterion Test 103

9. Manage System Software 107
Identify Installed Packages 108
Register with Red Hat Network (RHN) 110
Install, Remove and Update Packages 114
Criterion Test 117

10. Get Help in a Textual Environment 121
Read Documentation Using **man** 122
Identify Relevant Man Pages by Keyword 125
Read Documentation Using **pinfo** 127
Documentation in **/usr/share/doc** 129

11. Establish Network Connectivity 133
Essential Network Concepts 134
Linux Network Configuration 139
Confirming Network Functionality 141
Criterion Test 143

12. Administer Users and Groups 147
User and Group Administration 148
Criterion Test 152

13. Manage Files from the Command Line 155
The Linux File System Hierarchy 156
Navigate with Absolute Path Names 159
Command Line File Management 163
Save Typing with Relative Path Names 165
Criterion Test 168

14. Secure Linux File Access 171
User, Group, Other (UGO) Concepts 172
Manage Permissions Using GUI Tools 178
Manage Permissions from the Command Line 182
Criterion Test 188

15. Administer Remote Systems 191
Remote Shell Access 192

Remote File Transfers 194
Archives and File Compression 196
Using SSH Keys 199
Criterion Test 202

16. Configure General Services **205**
Deploy a Generic Network Service 206
Securing SSH Access 207
Configuring a VNC Server 209
Secure Access to a Remote GNOME Desktop 211
Criterion Test 213

17. Manage Physical Storage II **217**
Examine Filesystem Parameters 218
Modify File System Parameters 221
Delete an Existing Partition 223
Swap Space Concepts 225
Managing Swap Space 228
Criterion Test 230

18. Install Linux Graphically **233**
Graphical Installation with Anaconda 234
Post-install Configuration with Firstboot 238
Criterion Test 240

19. Manage Virtual Machines **245**
Introduction to KVM Virtualization 246
Virtual Guest Installation 248
Configuring Guests to Start at Boot Time 250
Criterion Test 252

20. Control the Boot Process **255**
Booting an Alternate Kernel 256
Booting into a Different Runlevel 259
Resolve GRUB Issues 261
Making Persistent GRUB Changes 264
Passing Kernel Arguments 266
Changing the Default Runlevel 268
Criterion Test 270

21. Deploy File Sharing Services **273**
Deploy an FTP Server 274
FTP Server Configuration 276
Deploy a Web Server 278
Criterion Test 280

22. Secure Network Services **283**
Activate and Deactivate Firewall Protection 284
Modify the Firewall to Allow Access to Trusted Services 287
Basic SELinux Security Concepts 289
SELinux Modes 293
Use the SELinux Management Tool to Change SELinux Modes 296
Display the SELinux Contexts of Processes and Files 298
Criterion Test 300

23. Comprehensive Review 303
Do You Still Have Questions? 304

A. Solutions 307
Get Started with the GNOME Graphical Desktop 307
Manage Files Graphically with Nautilus 312
Get Help in a Graphical Environment 317
Configure Local Services 319
Get Started with Bash 323
Manage Physical Storage I 327
Manage Logical Volumes 331
Monitor System Resources 341
Manage System Software 346
Get Help in a Textual Environment 349
Establish Network Connectivity 352
Administer Users and Groups 357
Manage Files from the Command Line 361
Secure Linux File Access 368
Administer Remote Systems 378
Configure General Services 384
Manage Physical Storage II 389
Install Linux Graphically 395
Manage Virtual Machines 398
Control the Boot Process 407
Deploy File Sharing Services 414
Secure Network Services 419
Comprehensive Review 426

Document Conventions

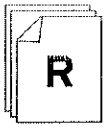
Notes and Warnings

Note

"Notes" are tips, shortcuts or alternative approaches to the task at hand. Ignoring a note should have no negative consequences, but you might miss out on a trick that makes your life easier.

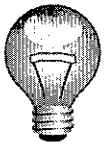
Comparison

"Comparisons" look at similarities and differences between the technology or topic being discussed and similar technologies or topics in other operating systems or environments.



References

"References" describe where to find external documentation relevant to a subject.



Important

"Important" boxes detail things that are easily missed: configuration changes that only apply to the current session, or services that need restarting before an update will apply. Ignoring a box labeled "Important" will not cause data loss, but may cause irritation and frustration.

Warning

"Warnings" should not be ignored. Ignoring warnings will most likely cause data loss.

Introduction

Welcome to class!

Thank you for attending this Red Hat training class. Please let us know if you have any special needs while at our training facility.

Please ask the instructor if you have any questions about the facility, such as operating hours of the facility and when you will have access to the classroom, locations of restrooms and break rooms, availability of telephones and network connectivity, and information about the local area.

As a courtesy to other students, please place your pager or cell phone's ringer on vibrate or mute, or turn off your devices during class. We ask that you only make calls during break periods.

If you have a personal emergency and are unable to attend or complete the class, please let us know. Thank you!

About Red Hat Enterprise Linux

This course is taught using Red Hat Enterprise Linux, an enterprise-targeted Linux distribution focused on mature open source software designed specifically for organizations using Linux in production settings.

Red Hat Enterprise Linux is sold on a subscription basis, where the subscription gives you continues access to all supported versions of the operating system in binary and source form, not just the latest one, including all updates and bug fixes. Extensive support services are included: a support contract and Update Module entitlement to Red Hat Network are included for the subscription period. Various Service Level Agreements are available that may provide up to 24x7 coverage with a guaranteed one hour response time for Severity 1 issues. Support will be available for up to seven years after a particular major release (ten years with the optional "Extended Update Support" Add-On).

Red Hat Enterprise Linux is released on a multi-year cycle between major releases. Minor updates to major releases are released roughly every six months during the lifecycle of the product. Systems certified on one minor update of a major release continue to be certified for future minor updates of the major release. A core set of shared libraries have APIs and ABIs which will be preserved between major releases. Many other shared libraries are provided, which have APIs and ABIs which are guaranteed within a major release (for all minor updates) but which are not guaranteed to be stable across major releases.

Red Hat Enterprise Linux is based on code developed by the open source community, which is often first packaged through the Red Hat sponsored, freely-available Fedora distribution (`http://fedoraproject.org/`). Red Hat then adds performance enhancements, intensive testing, and certification on products produced by top independent software and hardware vendors. Red Hat Enterprise Linux provides a high degree of standardization through its support for four processor architectures (32-bit Intel x86-compatible, AMD64/Intel 64 (x86-64), IBM POWER, and IBM mainframe on System z). Furthermore, we support the 4000+ ISV certifications on Red Hat Enterprise Linux whether the RHEL operating system those applications are using

is running on "bare metal", in a virtual machine, as a software appliance, or in the cloud using technologies such as Amazon EC2.

Currently, the Red Hat Enterprise Linux product family includes:

- *Red Hat Enterprise Linux for Servers*: the datacenter platform for mission-critical servers running Red Hat Enterprise Linux. This product includes support for the largest x86-64 and x86-compatible servers and the highest levels of technical support, deployable on bare metal, as a guest on the major hypervisors, or in the cloud. Subscriptions are available with flexible guest entitlements of one, four, or unlimited guests per physical host. Pricing is based on the basis of the number of socket-pairs populated on the system motherboard, the number of guests supported, the level of support desired, and the length of subscription desired.

  Red Hat Enterprise Linux for IBM POWER and *Red Hat Enterprise Linux for IBM System z* are similar variants intended for those system architectures.

- *Red Hat Enterprise Linux Desktop*: built for the administrator and end-user, Red Hat Enterprise Linux Desktop provides an attractive and highly productive environment for knowledge workers on desktops and laptops. Client installations can be finely tailored and locked down for simplicity and security for any workstation task.

  The basic *Desktop* variant is designed for task workers who have a limited amount of administrative control over the system, who primarily use productivity applications like Firefox Evolution/Thunderbird, OpenOffice.org, and Planner/TaskJuggler. The more sophisticated *Workstation* variant is designed for advanced Linux users who need a stand-alone development environment, and who are expected to have local super-user privileges or selected super-user privileges.

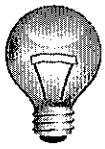
In addition, other variants exist such as *Red Hat Enterprise Linux for HPC Head Node* and *Red Hat Enterprise Linux for HPC Compute Node* (targeted at high-performance computing clusters), and *Red Hat Enterprise Linux for SAP Business Applications*. For more information please visit `http://www.redhat.com/`.

Additional Red Hat Enterprise Linux Software

Two additional software update channels are provided with Red Hat Enterprise Linux beyond the core software packages shipped:

- *Supplementary*: the "Supplementary" channel provides selected closed source packages, built for Red Hat Enterprise Linux as a convenience to the customer. These include things like Adobe Flash or proprietary Java JVMs.

- *Optional*: the "Optional" channel provides selected open source packages, as a convenience only. They are generally included in another Red Hat Enterprise Linux variant as a fully-supported package, or are a build requirement for the distribution. These packages are only available through a Red Hat Network child channel.



Important

Supplementary and *Optional* packages are provided with limited support, as a customer convenience only.

Red Hat also offers a portfolio of fully-supported *Add-Ons for Red Hat Enterprise Linux* which extend the features of your Red Hat Enterprise Linux subscription. These add-ons allow you to add capabilities and tailor your computing environment to your particular needs. These Add-Ons include support for high availability application clustering, cluster file systems and very large file systems, enhanced system management with Red Hat Network, extended update support, and more.

Note

Please visit `http://www.redhat.com/rhel/add-ons/` for more information about available *Add-Ons for Red Hat Enterprise Linux*.

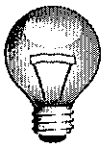
For information about other products which are provided by Red Hat, such as Red Hat Enterprise Virtualization, JBoss Enterprise Middleware, Red Hat Enterprise MRG, and various custom consulting and engineering services, `http://www.redhat.com/products/` also has useful information.

The Fedora Project also provides additional packages for Red Hat Enterprise Linux through *EPEL (Extra Packages for Enterprise Linux)*. EPEL is a volunteer-based community effort to create a repository of high-quality add-on packages which can be used with Red Hat Enterprise Linux and compatible derivatives. It accepts legally-unencumbered free and open source software which does not conflict with packages in Red Hat Enterprise Linux or Red Hat add-on products. EPEL packages are built for a particular major release of Red Hat Enterprise Linux and will be updated by EPEL for the standard support lifetime of that major release.

Red Hat does not provide commercial support or service level agreements for EPEL packages. While not supported officially by Red Hat, EPEL provides a useful way to reduce support costs for unsupported packages which your enterprise wishes to use with Red Hat Enterprise Linux. EPEL allows you to distribute support work you would need to do by yourself across other organizations which share your desire to use this open source software in RHEL. The software packages themselves go through the same review process as Fedora packages, meaning that experienced Linux developers have examined the packages for issues. As EPEL does not replace or conflict with software packages shipped in RHEL, you can use EPEL with confidence that it will not cause problems with your normal software packages.

For developers who wish to see their open source software become part of Red Hat Enterprise Linux, often a first stage is to sponsor it in EPEL so that RHEL users have the opportunity to use it, and so experience is gained with managing the package for a Red Hat distribution.

Visit `http://fedoraproject.org/wiki/EPEL/` for more information about EPEL.



Important

EPEL is supported by the community-managed Fedora Project and not by Red Hat Support.

Contacting Red Hat Technical Support

One of the benefits of your subscription to Red Hat Enterprise Linux is access to technical support through Red Hat's customer portal at `http://access.redhat.com/`. If you do not have a Red Hat account on the customer portal or are not able to log in, you can go to `https://access.redhat.com/support/faq/LoginAssistance.html` or contact Customer Service for assistance.

You may be able to resolve your problem without formal technical support by searching Knowledgebase (`https://access.redhat.com/kb/knowledgebase/`). Otherwise, Red Hat Support may be contacted through a web form or by phone depending on your support level. Phone numbers and business hours for different regions vary; see `https://access.redhat.com/support/contact/technicalSupport.html` for current information. Information about the support process is available at `https://access.redhat.com/support/policy/support_process.html`.

Some tips on preparing your bug report to most effectively engage Red Hat Support:

- *Define the problem.* Make certain that you can articulate the problem and its symptoms before you contact Red Hat. Be as specific as possible, and detail the steps you can use (if any) to reproduce the problem.
- *Gather background information.* What version of our software are you running? Are you using the latest update? What steps led to the failure? Can the problem be recreated and what steps are required? Have any recent changes been made that could have triggered the issue? Were messages or other diagnostic messages issued? What *exactly* were they (exact wording may be critical)?
- *Gather relevant diagnostic information.* Be ready to provide as much relevant information as possible; logs, core dumps, traces, the output of **`sosreport`**, etc. Technical Support can assist you in determining what is relevant.
- *Determine the Severity Level of your issue.* Red Hat uses a four-level scale to indicate the criticality of issues; criteria may be found at `https://access.redhat.com/support/policy/GSS_severity.html`.

Warning

Bugzilla is not a support tool! For support issues affecting Red Hat Enterprise Linux, customers should file their bugs through the support channels discussed above in order to ensure that Red Hat is fully aware of your issue and can respond under the terms of your Service Level Agreement. Customers should *not* file bugs directly in the `http://bugzilla.redhat.com/` web interface.

For Red Hat Enterprise Linux, Bugzilla is used by engineering to track issues and changes, and to communicate on a technical level with Engineering partners and other external parties. Anyone, even non-customers, can file issues against Bugzilla, and Red Hat does monitor them and review them for inclusion in errata.

However, Red Hat does not guarantee any SLA for bugs filed directly in Bugzilla (bypassing normal support channels). A review might happen immediately, or after a time span of any length. Issues coming through Support are always prioritized above issues of similar impact and severity filed against Bugzilla. Also, work arounds and hotfixes if possible and appropriate may be provided to customers by Support even before a permanent fix is issued through Red Hat Network.

Red Hat considers issues directly entered into Bugzilla important feedback, and it allows us to provide efficient interaction with the open source development community and as much transparency as possible to customers as issues are processed. Nevertheless, for customers encountering production issues in Red Hat Enterprise Linux, Bugzilla is not the right channel.

About This Course

Red Hat System Administration I

Red Hat System Administration I (RH124) is designed for IT professionals without previous Linux system administration experience. The course focuses on enabling students to rapidly become capable of performing core administrative tasks. Students are introduced to the graphical environment and tools first, but *Red Hat System Administration I* also provides a foundation for students planning to become full-time Linux system administrators by introducing key command-line concepts and enterprise-level tools. These concepts will be further expanded upon in the follow-on course, *Red Hat System Administration II* (RH135).

Objectives

- Gain sufficient skill to perform core system administrator tasks on Red Hat Enterprise Linux
- Start building the skills needed by an RHCSA-certified Red Hat Enterprise Linux system administrator

Audience and Prerequisites

- Students who are IT professionals, including Microsoft Windows and network administrators, who need to perform essential Linux system administration tasks including installation, establishing network connectivity, managing physical storage, and basic security administration
- There are no formal prerequisites for this course; however, previous system administration experience on other operating systems will be very beneficial

Structure of the Course

Red Hat training courses are interactive, hands-on, performance-based, real world classes meant to engage your mind and give you an opportunity to use real systems to develop real skills. We encourage students to participate in class and ask questions in order to get the most out of their training sessions.

This course is divided up into a number of *Units* organized around a particular topic area. Each Unit is divided up into multiple *Sections* which focus on a specific skill or task. The unit will start with an introduction to the material, then move on to the first section.

In each section, there will be a *presentation* led by the instructor. During the presentation, it may be a good idea to take notes in your student workbook (this book), and the instructor may remind you to do so. The presentation is followed by a short activity or *assessment* to give you the opportunity to practice with the material or review procedures. After a review of the assessment, the instructor will move on to the next section. At the end of the unit, there will normally be a hands-on lab exercise of some sort (a "*criterion test*") which will give you an opportunity to learn by doing and review your understanding of the unit's content. Please feel free ask questions in class, or asking the instructor for advice and help during the end-of-unit exercise. We want the

classroom environment to be a "low risk" place where you feel comfortable asking questions and learning from things that work and things that do not at first.

Orientation to the Classroom Network

Two subnets may be used in this course. The primary classroom network is 192.168.0.0/24, and belongs to hosts in the DNS domain "example.com". This network will be used for most classroom activities. Some courses use a second subnet, 192.168.1.0/24, belonging to hosts in the DNS domain "remote.test". This network can be reached from hosts in example.com, and is used in lab exercises which require testing services or security settings from machines (theoretically) outside your administrative control.

Students are each assigned a physical machine (desktop*X*.example.com on 192.168.0.*X*) which may host two or more virtual machines for lab activities, server*X*.example.com and host*X*.example.com.

In some courses, students may also use a non-root account on a test machine in the remote.test domain, remote*X*.example.com (192.168.1.*X*) to test access to network services on their example.com machines in lab activities.

The instructor controls a number of machines which students may see as well. The machine instructor.example.com (also known as instructor.remote.test) is the classroom utility server, providing default routing services, DHCP, DNS name service, one or more YUM repositories of software used by the class, and other network services. It is also connected to the classroom video projector to allow the instructor to display slides and demonstrations. It provides a virtual machine for the instructor, demo.example.com, which the instructor will use for in-class demonstrations.

Machine name	IP addresses	Role
desktop*X*.example.com	192.168.0.*X*	Physical student workstation
server*X*.example.com	192.168.0.*(X+100)*	Main student virtual machine
host*X*.example.com	192.168.0.*(X+200)*	Secondary student virtual machine
remote*X*.remote.test	192.168.1.*X*	Student test machine in remote.test domain (shared)
instructor.example.com	192.168.0.254	Physical instructor machine and utility server
instructor.remote.test	192.168.1.254	Identity of instructor.example.com on remote.test network
demo.example.com	192.168.0.250	Instructor virtual demonstration machine

Table 1. Classroom Machines

Internationalization

Language Support

Red Hat Enterprise Linux 6 officially supports twenty-two languages: English, Assamese, Bengali, Chinese (Simplified), Chinese (Traditional), French, German, Gujarati, Hindi, Italian, Japanese, Kannada, Korean, Malayalam, Marathi, Oriya, Portuguese (Brazilian), Punjabi, Russian, Spanish, Tamil, and Telugu. Support for Maithili, Nepalese, and Sinhala are provided as Technology Previews.

System-wide Default Language

The operating system's default language is normally set to US English (en_US.UTF-8), but this can be changed during or after installation.

To use other languages, you may need to install additional package groups to provide the appropriate fonts, translations, dictionaries, and so forth. By convention, these package groups are always named ***language*-support**. These package groups can be selected during installation, or after installation with PackageKit (**System** → **Administration** → **Add/Remove Software**) or **yum**.

A system's default language can be changed with **system-config-language** (**System** → **Administration** → **Language**), which affects the **/etc/sysconfig/i18n** file.

Per-user Language Selection

Users may prefer to use a different language for their own desktop environment or interactive shells than is set as the system default. This is indicated to the system through the **LANG** environment variable.

This may be set automatically for the GNOME desktop environment by selecting a language from the graphical login screen by clicking on the **Language** item at the bottom left corner of the graphical login screen immediately prior to login. The user will be prompted about whether the language selected should be used just for this one login session or as a default for the user from now on. The setting is saved in the user's **~/.dmrc** file by GDM.

If a user wants to make their shell environment use the same **LANG** setting as their graphical environment even when they login through a text console or over **ssh**, they can set code similar to the following in their **~/.bashrc** file. This code will set their preferred language if one is saved in **~/.dmrc** or will use the system default if one is not:

```
i=$(grep 'Language=' ${HOME}/.dmrc | sed 's/Language=//')
if [ "$i" != "" ]; then
    export LANG=$i
fi
```

Languages with non-ASCII characters may have problems displaying in some environments. Kanji characters, for example, may not display as expected on a virtual console. Individual commands can be made to use another language by setting **LANG** on the command-line:

```
[user@host ~]$ LANG=fr_FR.UTF-8 date
lun. oct. 24 10:37:53 CDT 2011
```

Subsequent commands will revert to using the system's default language for output. The **locale** command can be used to check the current value of **LANG** and other related environment variables.

Input Methods

IBus (Intelligent Input Bus) can be used to input text in various languages under X if the appropriate language support packages are installed. You can enable IBus with the **im-chooser** command (**System** → **Preferences** → **Input Method**).

Language Codes Reference

Language	$LANG value	Language package group
English (US)	en_US.UTF-8	*(default)*
Assamese	as_IN.UTF-8	assamese-support
Bengali	bn_IN.UTF-8	bengali-support
Chinese (Simplified)	zh_CN.UTF-8	chinese-support
Chinese (Traditional)	zh_TW.UTF-8	chinese-support
French	fr_FR.UTF-8	french-support
German	de_DE.UTF-8	german-support
Gujarati	gu_IN.UTF-8	gujarati-support
Hindi	hi_IN.UTF-8	hindi-support
Italian	it_IT.UTF-8	italian-support
Japanese	ja_JP.UTF-8	japanese-support
Kannada	kn_IN.UTF-8	kannada-support
Korean	ko_KR.UTF-8	korean-support
Malayalam	ml_IN.UTF-8	malayalam-support
Marathi	mr_IN.UTF-8	marathi-support
Oriya	or_IN.UTF-8	oriya-support
Portuguese (Brazilian)	pt_BR.UTF-8	brazilian-support
Punjabi	pa_IN.UTF-8	punjabi-support
Russian	ru_RU.UTF-8	russian-support

Language	$LANG value	Language package group
Spanish	es_ES.UTF-8	spanish-support
Tamil	ta_IN.UTF-8	tamil-support
Telugu	te_IN.UTF-8	telugu-support
Technology Previews		
Maithili	mai_IN.UTF-8	maithili-support
Nepali	ne_NP.UTF-8	nepali-support
Sinhala	si_LK.UTF-8	sinhala-support

Table 2. Language Codes

UNIT ONE

GET STARTED WITH THE GNOME GRAPHICAL DESKTOP

Introduction

Topics covered in this unit:

- GNOME Desktop
- `gedit` Text Editor

Using the GNOME Desktop

GNOME is the default graphical *desktop environment* for Red Hat Enterprise Linux. It provides an integrated, attractive desktop for users and a unified development platform on top of the graphical framework provided by the **X Window System**.

The GNOME desktop environment includes integrated applications, such as the **Nautilus** file manager and **gedit** text editor, that let you use mouse and keyboard combinations to cut, paste, copy, move and remove files, folders and and other items on the desktop. Graphical administration tools on GNOME menus let you monitor processes, configure services, and contact remote systems.

Important terms used in GNOME documentation (from the *GNOME Desktop User Guide*):

- *panel* - area in the GNOME Desktop where you have access to certain actions or information, no matter what the state of your application windows.
- *applet* - a small, interactive application that resides within a panel, for example the **Volume Control**. Each applet has a simple user interface that you can operate with the mouse or keyboard.
- *workspace* - a discrete area in the GNOME Desktop in which you can work.

Workspaces are essentially separate desktop screens which have the same background, panels, panel menus, and applets, but which may have different application windows. These can be used to organize your working environment by grouping open application windows by task. For example, you could group windows being used to perform a particular system maintenance activity (such as setting up a new remote server) in one workspace, while putting your e-mail and other communication applications in another workspace. This is a particulary powerful feature.

You can switch between workspaces at any time, either by clicking on a workspace icon using the **Workspace Switcher** applet on the right side of the bottom panel, or by typing **`Ctrl`**+**`Alt`**+**`LeftArrow`** or **`Ctrl`**+**`Alt`**+**`RightArrow`**. You can also use **Workspace Switcher** to click and drag windows from one workspace to another, and by right-clicking on it and selecting **Preferences**, increase or decrease the number of available workspaces.

Linux system administration is known for the power and flexibility of its command line interface. So why do we start this class by looking at a graphical desktop environment? One reason is that some things *are* easier to do with graphical tools, and it is useful to understand the differences in the Linux graphical environment so sysadmins can be fully effective. Also, some sysadmins may need to support users in the graphical environment, and therefore being able to work in this environment may be important. If you are new to Linux, the graphical file manager can be a useful way to explore the system. Also, some students coming from a non-Linux background may find it helpful to start by using graphical administration tools while getting familiar with the way Linux presents certain concepts. So, for a number of reasons, it is useful to start by working with the graphical environment.

Does that mean that learning the command line is unimportant? No! We will be looking at the shell and begin introducing command line tools as we get further into this class. Also, keep your eyes open for *Looking Ahead* notes which point more experienced students toward additional information of interest.

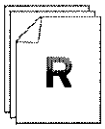
Changing Your Password

As on any other system, it is a good practice to change the password to any new user account which you are given. When changing your password as a regular user, it must meet the following requirements:

- It must have at least six characters
- It must not be based on a dictionary word
- It must not be too "simple". Use a combination of letters, capitalization, and other characters (numbers, punctuation, etc.) for the best results.

As the system administrator (the *superuser* or **root** user), you may set any user's password to anything you like. You will be warned if you do not meet normal password complexity requirements.

Use this space for notes



References

GNOME Desktop User Guide

- Available locally - **System** → **Help** then click **Desktop User Guide** link
- Available via the Internet -
  http://library.gnome.org/users/user-guide/2.28/

GNOME Desktop User Guide

- Chapter 2: Desktop Overview

GNOME Desktop User Guide

- Chapter 3: Desktop Sessions

Note

Looking Ahead: Later in this course we will look at how the command line shell (in the "Get Started with Bash" unit), and at how the **passwd** command can also be used to change user passwords.

Practice Performance Checklist

Using the GNOME Desktop

Do each of the following tasks on your desktop machine. Mark each task as you complete it.

- ☐ Log in as **visitor** with the original password of **password**.
- ☐ Change the **visitor** password from **password** to **55TurnK3y**.
- ☐ Log out.
- ☐ Log back in as **visitor** with the new password of **55TurnK3y**.
- ☐ Lock the screen.
- ☐ Unlock the screen.
- ☐ Without logging out, switch to the user **student** with a password of **student**.
- ☐ Log out from the **student** account. Provide visitor's password when the screensaver appears to get back to the GNOME desktop.
- ☐ Shut down your machine.
- ☐ Power on your machine to be ready for future lab work.

Note

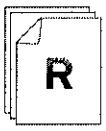
If your hardware is configured to PXE boot by default, a boot menu may appear when you power on your workstation. Select the fourth boot option, **Boot from local drive**, in this situation.

Editing Files with gedit

One of the basic design principles of Linux is that configuration files should be text based. There are a number of reasons for this. Text files are easier for humans to comprehend. If most programs use text files to store their settings, then even if they break a simple text editor can be used to repair any of them, rather than requiring a complex unique tool for each. Therefore, knowing how to edit text files in Linux is important.

The **gedit** text editor is a graphical tool for editing text files. If your Linux system has a graphical desktop interface available, **gedit** provides an intuitive, point-and-click way of editing files that is similar to Windows Notepad. The **gedit** window is launched by selecting **Applications** → **Accessories** → **gedit Text Editor** from GNOME.

Use this space for notes



References

To access the *Gedit Manual*:

- **System** → **Help** then click **Utilities** at left, then **Gedit Manual**
- From within **gedit**: **Help** → **Contents** or simply **F1**

Note

Looking Ahead: We will focus on **gedit** as our text editor in this class. Command line editors are also available, such as **vim** and **nano**. While **vim** is very powerful, it is also designed more for power than for ease of use. The next course, *Red Hat System Administration II*, covers **vim** in detail. In the meantime, you may wish to investigate the **vimtutor** tutorial from the command line if you are interested in learning more about **vim**.

Practice Performance Checklist

Using gedit

- ☐ Log into your desktop machine as **student**.
- ☐ Launch the **gedit** text editor.
- ☐ Open the **gedit-fix-practice.txt** file in the **student** folder and follow the directions contained therein.

Test

Criterion Test

Performance Checklist

GNOME Skills

Before you begin...

Close **gedit** and logout **student** from the previous exercise.

- ☐ Successfully log in as **visitor** with the password of **55TurnK3y**.
- ☐ Change **visitor** password from **55TurnK3y** to **Test123Time**.
- ☐ Without logging out, switch to the user **student** with a password of **student**.
- ☐ Lock the screen.
- ☐ Unlock the screen.
- ☐ Log out from the **student** account. You will probably have to provide the **visitor** password to continue.
- ☐ Reboot your machine.

Exercise

Editing Files with gedit

Carefully perform the following steps. Ask your instructor if you have problems or questions.

1. Log into your desktop machine as **student**.
2. Launch the **gedit** text editor.
3. Open the **gedit-fix-test.txt** file in the **student** folder.
4. Save a copy of that file to **gedit-fix-test-solution.txt** in the **student** folder.
5. Edit **gedit-fix-test-solution.txt** as described in that file. The resulting file should appear similar to the following:

```
This is the document that needs to be fixed for the GNOME Desktop/
gedit test.
```

```
Insert your name at the end of this line: John Doe
This paragraph needs to be copied later in the document.

Delete the extra word that does not belong in this sentence.

Copy the paragraph above below this paragraph. Make sure there is a
 blank line between the two paragraphs.

This paragraph needs to be copied later in the document.

This should be the last paragraph of the document. Save your corrected
 version of this document under its original name.
```

6. Save your changes to the document.

7. Create a new text file in the **student** folder called **gedit-new-test.txt** with the following single line of content:

```
I can create new text files with gedit.
```

Personal Notes

Unit Summary

Using the GNOME Desktop

In this section you learned how to:

- Log in and out from the GNOME desktop
- Change your account password
- Reboot and shutdown the server gracefully
- Lock and unlock your screen
- Switch to another user's account without logging out

Editing Files with **gedit**

In this section you learned how to:

- Edit existing files with **gedit**
- Create new files with **gedit**

UNIT TWO

MANAGE FILES GRAPHICALLY WITH NAUTILUS

Introduction

Topics covered in this unit:

- Nautilus file manager
- Using remote storage

Using Nautilus

Nautilus is the *file manager* that comes with the GNOME desktop. With Nautilus you can explore the file system, create files and folders, view file properties, and manipulate files and folders (copy, delete, move, cut, paste, and so on).

By default, Nautilus operates in *spatial mode*, in which a new window opens each time you open a folder. It may be changed to operate in *browser mode*, in which the contents displayed in the window changes each time you change to a new folder. To use browser mode for the current user, select **System** → **Preferences** → **File Management**. In the **File Management Preferences** window, on the **Behavior** tab, make sure **Always open in browser windows** is checked, and **Close** the window.

Comparison

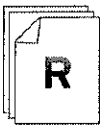
Nautilus is similar to the Finder in Apple Mac OS X or to Windows Explorer (**`explorer.exe`**) in Microsoft Windows. While the file manager is not as critical a tool for system administration in Linux as it is in Mac OS X or Windows it is still important to understand how it works, both for your own use and so that you can help users of the desktop environment.

Spatial mode operates like the Finder did in Mac OS 9; browser mode is similar to current versions of the Finder or Windows Explorer. Unlike Red Hat Enterprise Linux, Fedora 14 uses browser mode by default.

Besides working with local files and folders, Nautilus also lets you access files and folders on remote systems. You can connect to (and browse files on) FTP servers, Windows shares, SSH (remote login) servers, and other network servers.

Tips for working with files and folders in Nautilus:

- Files and folders are represented by icons and file names by default (icon view). Select the **View** pull-down menu to change the display to **List** (to see name, size, type and date modified) or **Compact** (to display small icons). Select the **Arrange Items** menu item, to list files by name, size, time, date or emblem.
- File names beginning with a period (.) are referred to as hidden files. To see files or folders beginning with a period in your current folder, select **View** → **Show Hidden Files**. Uncheck the checkbox to stop showing hidden files and folders.
- When copying a file or folder in Nautilus, if the source and destination folders are on different physical disk partitions, the default drag-and-drop action between those folders will be a copy instead of a move. This is also the case when copying a file to or from a folder on a remote file server.



References

GNOME Desktop User Guide

- Chapter 6: Working With Files

(See Section 6.6 "Managing Your Files and Folders" in particular.)

Note

Looking Ahead: Later in this course, we will also look at how to work with files using command line tools such as **`ls`**, **`mv`**, **`cp`**, **`mkdir`**, and **`rm`** in the **`bash`** shell.

Practice Performance Checklist

Managing Local Files with Nautilus

In this lab you will use the Nautilus file manager to manipulate sample files as **student**.

- ☐ Log into the GNOME desktop as the user **student**.
- ☐ Once the GNOME desktop appears, open the folder called Labs. Double-click the Nautilus Lab Setup launcher. It will ask for confirmation then create several files you will manipulate in this practice exercise.
- ☐ Open **student**'s home folder.
- ☐ Create a folder called **targetdir** under student's home folder.
- ☐ Copy the file **original1.txt** from student's home folder into **targetdir** without changing the name of the file.
- ☐ Create a link from **original2.txt** in student's home folder into **targetdir** with the same name.
- ☐ Move the file **original3.txt** from student's home folder into **targetdir**.
- ☐ Change the name of **original9.txt** to **original4.txt**. It should remain in student's home folder.
- ☐ Delete the file called **original5.txt** from student's home folder.
- ☐ Delete the folder called **originaldir** from student's home folder.
- ☐ Reclaim the disk space used by the file and folder you just deleted in the previous two steps.

Accessing Remote File Systems in Nautilus

Given network connectivity, Nautilus can display files and folders from remotely accessible FTP, SSH, Windows, and other server types. The easiest way to launch Nautilus to connect to a remote file service is to open a **Connect to Server** window. The tasks described in this unit show how to open a **Connect to Server** window to access remote files and folders from several different types of servers.

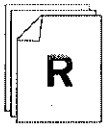
Using the **Connect to Server** window, you can also have Nautilus connect to other types of network file services. Here are some other **Server type** entries you can choose:

- **Public FTP** - Enter the name of the server (**Server**) and optionally a folder to open (**Folder**) and select **Connect**. When prompted, enter the user's password. Try **`instructor.example.com`** as the server. By default, you are logged in as the anonymous user.
- **FTP (with login)** - Use this selection to login as a specific user to the FTP server. Keep in mind that passwords and data are sent in clear text.
- **Windows share** - In the **Server** box, enter the name of the Microsoft Windows files server or Linux Samba server you want to connect to. Type the name of the **Share** and **User Name** needed to connect to the server and click **Connect**. When prompted, enter the user's password.

Other **Server types** are available as well. Given permission from the server, you can copy, move, remove, and rename files and folders using your mouse and keyboard as you would from the local system.

Connecting to an NFS server can be done through an **autofs** service running on the client, by accessing the directory **`/net/`*`host`*** where ***`host`*** is either the hostname or IP address of the remote NFS server. In **Nautilus** choose **File** → **Open Location...**.

Use this space for notes



References

GNOME Desktop User Guide

- Section 6.11: Navigating Remote Servers

Practice Performance Checklist

Managing Remote Files with Nautilus

Start the **Connect to Server** window to select a remote server. Using the Nautilus window that appears, you can access remote files and copy files to and from the server.

- ☐ Log into the GNOME desktop as the user **student**.
- ☑ Select **Places → Connect to Server...** from the top panel.
- ☐ From the **Connect to Server** window, choose the following:
  - **Server type** - Choose **SSH**
  - **Server** - Enter serverX where *X* is replaced by your desktop number (for example, server12 if your desktop were desktop12)
  - **Folder** - Enter **/home/student**
  - **User Name** - Enter **student**
- ☐ Select **Connect**. If this is the first time this user has connected, you will be prompted to accept the SSH key. Click the **Log In Anyway** button to continue.
- ☐ Enter **student** as the password and check the **Forget password immediately** button. A Nautilus window opens, displaying the contents of the selected remote folder (it may be empty).
- ☐ Disconnect the folder from the remote system, serverX.

smb : share of windows
FTP :

Test

Criterion Test

Performance Checklist

Copy, Move, and Remove Remote Files

Once you have opened a connection to a remote folder, use your mouse and keyboard to work with the files and folders available from the remote server.

- ☐ From your desktopX machine, open **student**'s home folder on serverX using SSH. The password for **student** is **student**.
- ☐ Open the desktopX **student**'s home folder.
- ☐ Create a folder called **nautilus-test** in the serverX student's home folder.
- ☐ Copy the file **original1.txt** from student's desktopX home folder into the serverX **nautilus-test** folder without changing the name of the file.
- ☐ From **student**'s desktopX home folder, open the **targetdir** folder and move the file **original3.txt** to the serverX **student**'s home folder.
- ☐ Change the name of **original3.txt** to **original9test.txt**. It should remain in **student**'s home folder on serverX.
- ☐ Delete the file called **original8.txt** from the serverX **student**'s home folder.
- ☐ Close both windows when you are done.

lama baz mel drag ddop
by default bey3mel lessin

Warning

If you are using the Red Hat Virtual Training environment, be careful not to use the **Ctrl+q** hotkey to close Nautilus windows. While convenient, it may also close your client application.

Notice that an icon representing the connection to the remote folder stays on the desktop (named **sftp for student on serverX**). Double-click that icon if you want to open the remote folder again. Right-click and select Unmount if you want to remove the icon from your desktop.

- ☐ Connect to the **ftp** windows share on **instructor.example.com** as **guest20XX** where *XX* is your desktop number. The password is **password**.
- ☐ Copy the file **example-ca.crt** from the share to the desktop on your local machine.

- ☐ Right-click the **ftp on instructor** folder on your desktop and select **Unmount** to disconnect from the share.

Personal Notes

search in google
site: docs.redhat.com/docs

sos report

Unit Summary

Using Nautilus

In this section you learned how to:

- Copy and link files using Nautilus
- Rename files using Nautilus
- Move files from one directory into another using Nautilus
- Delete files and reclaim disk storage using Nautilus
- Create a new directory/folder using Nautilus
- Collect related files into a common folder
- Delete a directory with the files it contains to reclaim disk space

Accessing Remote File Systems in Nautilus

In this section you learned how to:

- Mount a network share to your system for temporary use

UNIT THREE

GET HELP IN A GRAPHICAL ENVIRONMENT

Introduction

Topics covered in this unit:

- Local documentation
- On-line Red Hat documentation
- Contacting Red Hat

Research Local Documentation

A number of standardized help systems are available on the local system in Red Hat Enterprise Linux. One of the most commonly used is the built-in *Linux System Manual*, made up of individual manual pages, or *man pages*, documenting individual commands, configuration files, and programming calls. These each follow a fairly strict set of structural conventions in terms of how they are written, and are divided up into numbered "chapters" by category.

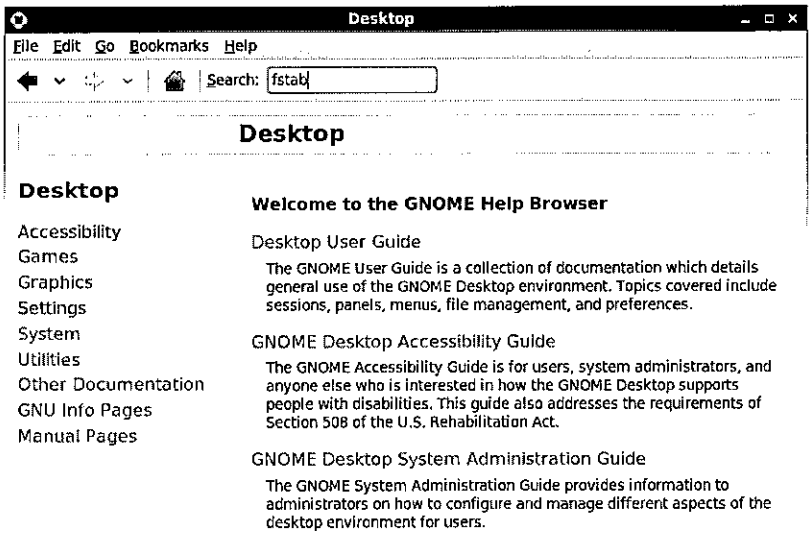
A second help system is *GNU Info*, which is used heavily by software developed by the GNU Project. This help system is organized as a set of hypertext books about various software components.

GNOME also has its own help system on various components of the desktop environment, also written as a collection of graphical hypertext books.

Note

Why three different help systems? The original online system manual is relatively inflexible in format but comprehensive. GNU Info was designed to be more flexible in style and to work on a variety of operating systems, not just Linux or even UNIX-like systems. The GNOME documentation system can display graphics and diagrams, while the older GNU Info system is text-only.

One handy way to access all these help systems with one tool is through the graphical **GNOME Help Browser**. Whether you are viewing the GNOME desktop or a selected GNOME application, pressing the **F1** function key will open the **GNOME Help Browser**. From the GNOME desktop, you can also select **System** → **Help** to open it. (*Advanced Students:* From the command line, you can also start it by typing **`yelp`**.)



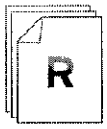
Once the **GNOME Help Browser** is open, here are a few ways to use it:

- Select one of the main GNOME guides (the *GNOME Desktop User Guide*, *GNOME Desktop Accessibility Guide*, or *GNOME System Administration Guide*) and browse its table of contents.
- Select a GNOME guide by application category from the menu on the left-hand side of the window.
- Type a term into the **Search** box.

There are two ways to access GNU Info documentation with the **GNOME Help Browser**. From its home screen, you can select the **GNU Info Pages** item and browse for documentation by category. Otherwise, if you know the name of the info node, you can type that into the **Search** box from the home screen. For example, **`info:GRUB`** will look for an info node named **GRUB**.

To access man pages with the **GNOME Help Browser**, simply enter **`man:`*`man-page`*** into the **Search** box. For example, to look in the manual for the **`ls`** man page, enter **`man:ls`**. Sometimes two pages in different chapters of the manual have the same name. For example, **passwd** in Chapter 1 ("User Commands") is not the same as the **passwd** man page in Chapter 5 ("File Formats"). By convention, when writing about man pages we can specify the exact chapter of interest in parentheses after the name of the man page: **passwd**(1) is not the same as **passwd**(5). You can specify exactly which chapter of the manual to search for your page in the **Search** box: **`man:passwd(5)`**, for example.

Use this space for notes



References

GNOME Desktop User Guide

- Section 7.3: Yelp Help Browser

man-pages(7) man page

- *(Discusses format and organization of man pages; use **`man:man-pages(7)`** in the Search box of the GNOME Help Browser to view)*

Note

Looking Ahead: Man and GNU Info pages, being pure text in format, can be viewed without a graphical interface through command line tools. We will look at how to use the **man**(1) and **`info`**(1) commands to do this later in the class, in the unit "Get Help in a Textual Environment".

Practice Quiz

Researching Local Documentation

1. Which document, with section reference, describes in detail what panel applets are in the GNOME desktop?

_____

2. Which document, with section reference, describes how to copy and paste in the graphical text editor?

gedit man u.1

_____

3. Which document, with section reference, describes the various ways to add a launcher to a GNOME panel.

_____

4. Which document, with section reference, describes the shortcut keys for the Gedit text editor?

_____

5. Which document, with section reference, describes what each mouse buttons does when using GNOME?

_____

6. Which document, with section reference, describes how to get started writing notes using the panel applet?

_____

Research On-line Documentation

As we have seen, quite a bit of documentation is included on a normal Red Hat Enterprise Linux system with the software you have installed, in the form of man pages, info nodes, and GNOME documents.

Additional documentation is stored in the **/usr/share/doc** directory. If you use **Nautilus** to look in that directory (Under the **Computer** icon, select **File System** → **usr** → **share** → **doc**), you should see folders (subdirectories) with names matching software packages installed on the system. Look for a subdirectory named after a software package that interests you, and in that subdirectory you should see documentation for that package. Typically, that documentation may include the license of the software package, **README** files included with the source code, sample configuration files, or other documentation not in the form of a man page, set of info nodes, or GNOME documents.

Beyond local resources, there are also sources of official documentation for your Red Hat Enterprise Linux system available on the Internet. These include formal manuals produced by Red Hat, and the Knowledgebase articles at the Red Hat Customer Portal.

1. Documentation

   Red Hat produces its own set of manuals to go with each release of Red Hat Enterprise Linux. Those manuals are available from **http://access.redhat.com/docs**. Manuals include:

   - Release Notes - Describes features and issues associated with the Red Hat Enterprise Linux release.
   - Migration Planning Guide - Describes how to migrate from earlier Red Hat Enterprise Linux releases.
   - Installation Guide - Covers installation issues, including how to do bare-metal and unattended installs.
   - Deployment Guide - Includes topics for configuring your Red Hat Enterprise Linux systems.

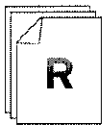
   Other online guides cover topics such as security, resource management, clustering and virtualization.

2. Red Hat Customer Portal

   The Red Hat Customer Portal (**http://access.redhat.com/**) consolidates information you need to manage your Red Hat Enterprise Linux system. The site tells how to manage subscriptions and get telephone and online support. Full site access is provided through the same Red Hat login you may already use for hosted Red Hat Network access, and is one of the benefits of your software subscription.

   On the **Knowledge** tab, you can select the **Knowledgebase** item to search the Red Hat Knowledgebase to find articles on hardware and software questions and issues.

   Portions of the Red Hat Customer Portal are accessible without a current Red Hat login.



References

Red Hat documentation

http://access.redhat.com/docs/
http://www.redhat.com/docs/

Knowledgebase

http://access.redhat.com/kb/knowledgebase/

Red Hat Customer Portal

http://access.redhat.com/

Linux-related searches

http://www.google.com/linux/

To limit your Google search to the Red Hat documentation site, enter your search terms followed by **`site:www.redhat.com/docs`**

Getting the Most from Red Hat Global Support Services

There are many ways of getting technical support for Red Hat Enterprise Linux. As a subscriber to Red Hat Enterprise Linux, one of your best resources is official Red Hat technical support. To get the best result when you contact Red Hat Global Support Services, you should understand a bit about how the process works and what information you need to bring with you.

The following are seven steps to take when interacting with Red Hat Global Support Services:

1. *Define the problem*

   Explain the issue. Reproduce the problem and list the steps taken to do so.

2. *Search documentation and kbase articles*

   Do your homework. Search for documentation from others who have dealt with similar issues.

3. *Gather background information*

   What versions of relevant software are you running? Are there updates that may fix your issue? What error messages and symptoms are produced? Be as specific as possible.

4. *Gather relevant diagnostic information (**`sosreport`**)*

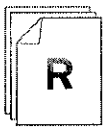
   Gather log files, core dumps, output from commands and anything else you may think is relevant. Run **`sosreport`** to gather information.

5. *Determine the severity level*

   Try to accurately determine the severity level. The severity levels (1 to 4) are described at *https://access.redhat.com/support/policy/GSS_severity.html*

6. *Contact Red Hat by web form or telephone*

   Make sure you have your Red Hat account number available. Contact information is available from *https://access.redhat.com/support/policy/support_process.html* by clicking on either the **submit a support case online** link or the **contact us by phone** link.



References

Overview of Red Hat support process
https://www.redhat.com/support/process/

Netiquette
http://www.catb.org/~esr/faqs/smart-questions.html

Contacting Red Hat Technical Support in this book's "Introduction" unit.

Practice Resequencing Exercise

Working with Red Hat Global Support Services

Below are the steps taken when interacting with Red Hat Global Support Services. Mark the order the steps should be taken:

__ Gather relevant diagnostic info (log information, core dumps, etc.)

__ Define the problem

__ Contact Red Hat via phone or web

__ Determine the severity level

__ Gather background information

__ Search documentation and kbase articles

Test

Criterion Test

Consult local documentation (not the Internet) to answer the following questions.

Quiz

Get Help in a Graphical Environment

1. What is "browser mode" in the graphical file manager (Nautilus)?

   _____

   How do you start "browser mode"?

   _____

   Where did you find the answer?

   _____

2. How can Nautilus be configured to always open folders in browser mode?

   _____

   Where did you find the answer?

   _____

3. Which document provides more information on how to use the **`gedit`** text editor? Use the search function to answer this question.

   _____

4. What are the two default key shortcuts for taking screen shots?

   _____

   Where did you find the answer?

   _____

5. What are workspaces?

_____

What are the keyboard shortcuts used to switch between workspaces?

_____

Where did you find the answers?

_____

Personal Notes

Unit Summary

Research Local Documentation

In this section you learned how to:

- Research local documentation using the GNOME documentation tool to answer questions

Research On-line Documentation

In this section you learned how to:

- Use Red Hat online documentation to answer questions

Getting the Most from Red Hat Global Support Services

In this section you learned how to:

- Describe the process for getting additional help from Red Hat Global Support Services

UNIT FOUR

CONFIGURE LOCAL SERVICES

Introduction

Topics covered in this unit:

- The `root` user
- System clock management
- Print queue management
- Print job management

Understand the Role of the root User

Most operating systems have some sort of *superuser*; a user that has all power over the system. This user in Red Hat Enterprise Linux is the **root** user. This user has the power to override normal privileges on the file system and is used to manage and administer the system. In order to perform tasks such as installing or removing software and to managing system files and directories, you must escalate privileges to the **root** user.

Most devices can only be controlled by **root**, but there are a few exceptions. For instance, removable devices, such as USB devices, are allowed to be controlled by a normal user. Thus a non-root user is allowed to add and remove files and otherwise manage a removable device, but only root is allowed to manage "fixed" hard drives by default.

This unlimited privilege, however, comes with responsibility. **root** has unlimited power to damage the system: remove files and directories, remove user accounts, add backdoors, etc. If the **root** account is compromised, someone else would have administrative control of your system. Throughout this course, you will be encouraged to log in as a normal user and escalate privileges to **root** only when needed.

Comparison

The **root** account on Linux is roughly equivalent to the local Administrator account on Windows. In Linux, most system administrators log in to an unprivileged user account and use various tools to temporarily gain root privileges.

Warning

The traditional practice on Windows is that either a user with Administrator privileges or Administrator logs in directly to perform system administrator duties. However, on Linux it is recommended that system administrators *should not* log in directly as **root**. Instead, system administrators should log in as a non-root user, and use other mechanisms (**su**, **sudo**, or **PolicyKit**, for example) to temporarily gain root privileges.

One reason for this is that by logging in as the administrative user, the entire desktop environment runs unnecessarily with administrative privileges, and any security vulnerability which would normally only compromise the user account has the potential to compromise the entire system.

Note that in recent versions of Windows, Administrator is disabled out of the box and features such as User Account Control (UAC) are used to limit administrative privileges for users with Administrator privileges until actually needed for this reason. In Linux, the **PolicyKit** system is the nearest thing to UAC.

Use this space for notes

References

`info libc` (*GNU C Library Reference Manual*)

- Section 29.2: "The Persona of a Processs"

Note

Looking Ahead: Most of the graphical administrative applications we will look at use **PolicyKit** to prompt users for authentication and manage root access. Very advanced students may be interested in the **pkexec**(1) and **`polkit`**(8) man pages for details on how this system works, but it is beyond the scope of this course.

Later in this class in the unit "Get Started with Bash", we will look at the **su** command, which is used to get a shell prompt as root. We discuss how to configure and use **sudo** in *Red Hat System Administration III*.

Practice Quiz

The Role of the root User

Complete the chart below with the similarities and differences between the Linux **root** user and the Windows Administrator user.

Linux **root** user	Windows **Administrator** user

Table 4.1. T-chart

Manage the System Clock

The PC hardware clock is not accurate enough for many applications. It tends to drift over time. Many applications require exact timing and may react poorly if the clock is reset suddenly to a new time.

Network Time Protocol (NTP) counters the drift by dynamically modifying the length of a second, much like tuning the pendulum of an old fashioned clock. If the system's time is behind the combined reference time of the time servers the second is made shorter so that the system clock races towards the correct time. Thus the time difference is reduced gently without disturbing other applications. However if the time differs too greatly, NTP ceases to work.

Having three central time servers allows clients to reject bogus synchronization messages if one of the servers' NTP daemons or clocks malfunctions. It is possible for a client to synchronize with fewer time servers if necessary but it is less reliable and secure.

Configure NTP Service

1. From the **System** → **Administration** menu, launch the **Date & Time** management tool.
2. If prompted, enter the root password so **`system-config-date`** can run with administrative privileges.
3. Click the **Time Zone** tab.
4. Set the timezone for your locale.
5. Select **UTC**.
6. Click the **Date and Time** tab.
7. Check **Synchronize date and time over the network** to turn on NTP support.
8. Click the **Add** button to add an NTP server to synchronize from.

   *In the classroom, **`instructor.example.com`** will work. On the Internet, **`0.pool.ntp.org`** is a public service which will work, see the References below.*
9. Under **Advanced Options**, select **Speed up initial syncrhonization.**

References

Red Hat Enterprise Linux Deployment Guide
- Chapter 13: Date and Time Configuration

NTP: Network Time Protocol
http://www.ntp.org/

NTP Pool Project: How do I use pool.ntp.org?
http://www.pool.ntp.org/en/use.html

Practice Performance Checklist

Manage the System Clock

Perform the following steps on serverX unless directed otherwise.

- ☐ Configure serverX to synchronize with instructor.example.com using NTP.
- ☐ Set the timezone to the appropriate setting for your locale.
- ☐ Make the hardware clock store UTC time.

Configure Printers

Printing on a Red Hat Enterprise Linux system is handled by the **Common Unix Printing System**, or **CUPS**. The default **CUPS** installation supports thousands of different printer models, which can be attached to the system locally or over the network. Supported network printer connections include other IPP servers, older Unix style LPD servers, JetDirect printers and printers shared by Microsoft Windows (SMB) servers.

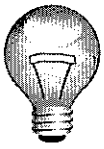
One or more *queues* are associated with each printer. Print jobs are sent to a queue, not to a printer. Different queues for the same printer may have different priority or output options. Setting up print queues is the responsibility of the system administrator; individual users do not create print queues.

A graphical configuration tool is provided to make adding new printers to your system easy. To run this tool, **`system-config-printers`**, select **System** → **Administration** → **Printing** and follow the instructions to specify your printer's name, manufacturer, model and connection type. Once the printer has been created, it can be selected from the list of printers for further configuration. This interface can also be used to print test pages and set the printer as your system's default. A private web interface on TCP port 631 that can only be contacted from the local system by default provides documentation and a separate administrative interface.

Example Printer Configuration

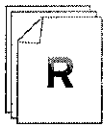
- Use **System** → **Administration** → **Printing** to start **`system-config-printer`**
- Click the **New** button to add a printer
- **Authenticate** with the root password if **Privileges are required to get devices**
- On the **Devices** sidebar, expand **Network Printer**. Select **Find Network Printer**, enter the hostname or IP of the printer or print server, and click **Find**. (Alternatively, select the type of network printer or local printer manually and fill in appropriate connection information by hand.)
- The system will attempt to autodetect drivers for the printer; if this fails, you will need to specify the driver from a list manually. Then you may be prompted to specify any special installable options for the printer that were not autodetected.
- Enter a unique **Printer Name**; this will be the name of the print queue. You may enter a **Description** and **Location** for the printer to make it easier for users to find.
- **Authenticate** as root if **Privileges are required to add/remove/edit a printer**. Print a test page if prompted to verify that the settings work.
- If you want the printer to be the system-wide default for all print jobs, right-click on its icon and select **Set As Default**.

Printers may also be shared by CUPS with other CUPS systems on the network. By default, the system is configured to autodetect printers advertised by a CUPS print server to the local network on UDP port 631.



Important

Sharing needs to be enabled at the printer level and at the print server level. To share any printer, go to **Server** → **Settings**. Check the **Publish shared printers connected to this system** checkbox. Once that is configured, each printer can be shared individually by right-clicking on the printer and choosing **Properties**. Highlight **Policies** in the left pane and check the **Shared** checkbox.



References

CUPS Online Help
http://localhost:631/help/

`system-config-printer`(1) man page

Practice Group Exercise

Manage Print Queues

Perform the following steps on serverX unless directed otherwise.

1. Create a local print queue and share it with other systems. Name the print queue **`local`** and make it a PostScript printer that points to either the serial or parallel port on your system.
2. After your partner has configured his or her printer, create a second print queue on your system that points to your partner's **`local`** print queue. Name the print queue **`remote`** and make it a raw print queue that forwards jobs to your partner's **`local`** print queue.
3. When you finish, print some text files to **`local`** and **`remote`** to verify.

Note

If you are using a serial port, the print jobs are sent to it almost immediately and cleared, so it may be difficult to verify that your print queues are working properly. If this is the case, use the "count" files (e.g., **`c00001`**, **`c00002`**, etc.) in **`/var/spool/cups/`** to verify. There will be a new count file created every time a print job goes through the queue.

Manage Print Jobs

Once a file has been sent to a queue for printing, it is called a *job*. Each job is numbered so that it may be monitored or canceled while it is in the queue printing or waiting to be printed.

Print queues may be *disabled* which allow jobs to queue but do not send them to the printer. This is useful if you are doing printer maintenance. Once you are finished, you must be sure to *enable* the print queue again.

Your instructor will perform a demonstration like the following to illustrate how to perform some of these tasks:

Manage Print Jobs Demonstration

- *Disable the print queue*: In the printer utility (**System** → **Administration** → **Printing**, **`system-config-printer`**), right-click on the printer and uncheck the **Enabled** checkbox.
- *Submit a print job*: In a GUI application such as **Firefox**, use **`Ctrl`**+**`P`** or select **File** → **Print...** to print a page.
- *View the queued jobs*: In the printer utility, double-click on the printer queue's icon.
- *Select the pending job and remove it*: In the printer utility, open the printer queue to view the queued jobs as above, right-click on the job and choose **Cancel**.
- *Enable the print queue*: In the printer utility, right-click on the printer and check the **Enabled** checkbox.

References

CUPS Online Help: "Command-Line Printing and Options"
http://localhost:631/help/options.html

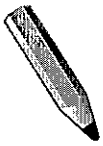
- *(Provides information on how to perform some of these tasks with command line tools)*

Practice Performance Checklist

Print Job Management

Perform the following steps on desktopX unless directed otherwise.

- ☐ Disable the default print queue on your system.
- ☐ Submit a print job to the print queue.
- ☐ List the jobs in the default print queue.
- ☐ Cancel the print job you just submitted.
- ☐ Enable the default print queue



Test

Criterion Test

Exercise

Configure and Manage a Printer

Carefully perform the following steps. Ask your instructor if you have problems or questions.

Perform the following steps on desktopX unless directed otherwise.

1. Configure a network printer to send print jobs to an IPP print queue on instructor.example.com called /printers/printer*X* where *X* is your desktop number.
2. Your print queue should be called **`remote-test`*`X`*** (where *X* is your station number) and should be the default print queue. Use **`PostScript Printer`** as the model.
3. Once you have completed your work, open the **Labs** folder on your GNOME desktop and double click the Printer Management Grading icon.

Personal Notes

Unit Summary

Understand the Role of the root User

In this section you learned how to:

- Use root privileges

Manage the System Clock

In this section you learned how to:

- Set the system time and time zone using a graphical tool
- Configure the system to use NTP to synchronize its clock

Configure Printers

In this section you learned how to:

- Configure a printer
- Share a printer

Manage Print Jobs

In this section you learned how to:

- Manage jobs in a print queue
- Enable and disable print queues
- Cancel print jobs

UNIT FIVE

GET STARTED WITH BASH

Introduction

Topics covered in this unit:

- Bash syntax
- Using Bash
- Launching graphical commands as root

Introduction to Bash

In this unit we will start looking at how to use the command line in Linux. Command line interfaces can be very powerful, and when supported by a scripting language can support automation of tasks and can simplify or make possible operations that are hard to accomplish efficiently with graphical tools.

The command line is provided by a program called the *shell*. Over the long history of UNIX-like systems, many shells have been developed. The default shell for users in Red Hat Enterprise Linux is **bash**, the **GNU Bourne-Again Shell**. The **bash** shell is an improved version of one of the most successful shells used on UNIX-like systems, the **Bourne Shell (sh)**.

Comparison

The **bash** shell is similar in concept to the command line interpreter found in recent versions of Microsoft Windows, **`cmd.exe`**, (although **bash** has a much more sophisticated scripting language and is generally more capable), or to Windows PowerShell in Windows 7 and Windows Server 2008 R2. Mac OS X administrators who use the Macintosh's **Terminal** utility will be pleased to note that **bash** is also the default in Mac OS X.

Using the Command Line

Commands are entered in a terminal at the *shell prompt*. The standard prompt lists the login name of the current user, the short hostname of the machine, the name of the current directory in square brackets, followed by a **$** prompt:

```
[student@host ~]$
```

The **$** is replaced by a # if the shell is running as the superuser, **`root`**, to make it more obvious that it is a superuser shell (which helps to avoid accidents and mistakes in that very powerful account).

```
[root@host ~]#
```

Commands entered at the shell prompt have three basic parts:

- Command
- Options
- Arguments

The *Command* is the name of the program to run. It may be followed by one or more *Options* which adjust the behavior of the command or what it will do. Options normally start with one or two dashes (**`-a`** or **`--all`**, for example) to distinguish them from arguments. Commands may also be followed by one or more *Arguments* which often indicate a target that the command should operate on.

For example, the command line **usermod -l morgan** has a command (**usermod**), an option (**-l**), and an argument (**morgan**). The effect of this command is to lock the password on user morgan's account.

Just knowing what a command does is not always enough. In order to use a command effectively you need to know what options and arguments it accepts and what order it expects them in (the *syntax* of the command). Most commands have a **--help** option. This causes the command to print a description of what it does, a "usage statement" that describes the command's syntax and a list of the options it accepts and what they do.

At first glance, usage statements may seem complicated and difficult to read. However, they become much simpler to understand once one is familiar with a few basic conventions:

- Anything in square braces (**[]**) is optional
- Anything followed by **...** represents an arbitrary-length list of that thing
- If you see multiple options separated by pipes (**|**) it means you can choose any *one* of them
- Text in angle brackets (**<>**) represents variable data. So **<filename>** means "insert the filename you wish to use here". Sometimes such variables are simply written in all caps (e.g., FILENAME).

So, looking at the first usage statement for the **date** command:

```
date --help
date [OPTION]... [+FORMAT]
```

we see that **date** can take an optional list of options (**[OPTION]...**) followed by an optional format string, prefixed with a **+**, that defines what you want the date to look like (**[+FORMAT]**). Since both of these are optional, you will note that **date** will work even if it is not given options or arguments (it will print the current date and time using its default format).

Note

If you look at the **man** page for a command, the SYNOPSIS section will also provide information about the command's syntax. You may also find it useful to look in **man-pages**(7) to remind yourself about how to interpret all the square brackets, vertical bars, and so forth that you see in SYNOPSIS or a usage message.

References

intro(1), **man-pages**(7), and **bash**(1) man pages

Practice Quiz

Bash Syntax

1. Options modify how a command will work and begin with - or --.

2. Optional, additional parameters are called arguments and are enclosed by [ ] in Linux documentation.

3. The following usage notation,

   `--create|--list|--extract`

   indicates what about the options?

   _____

   * Feh option nie zerwa3 odaj 2 opcje
   & one time łączem wszed bas

   Command [options] [arguments]

Using Bash

In the desktop environment, you need to run a graphical *terminal emulator* in order to access a shell prompt. This is a program that opens a window that pretends to be an old-style text-only terminal such as a DEC VT102 or VT220.

The default terminal emulator in GNOME is **gnome-terminal**. It can be started by selecting **Applications** → **System Tools** → **Terminal** from the top panel, or by right-clicking on an empty area of the desktop or an open **Nautilus** window and selecting **Open in Terminal** from the pop-up menu.

Your instructor will demonstrate the following shell commands. What do they do? (See also the *References* at the end of this section.)

- **passwd [*username*]**
- **id**
- **su [-] *username***
- **exit**

Note

The command **su *username*** starts a *non-login shell*, while the command **su - *username*** starts a *login* shell. The main distinction is **su -** sets up the shell environment as if you cleanly logged in as that user, which **su** just starts a shell as that user with your current environment settings.

In most cases, you probably want to run **su -** to get the user's normal settings. For more information, see the **bash**(1) man page.

Comparison

The **su** command is most frequently used to get a command-line interface (shell prompt) which is running as another user, typically **root**. However, with the **-c** option it can be used like the Windows utility **runas**, to run an arbitrary program as another user. See **info su** for details.

Useful Bash Features

What are two useful shell features demonstrated by your instructor?

1. _____

2. _____

Tab completion allows you to quickly complete commands and file names once you have typed enough at the prompt to make it unique. If the characters you typed are not unique, use two **Tab** presses to display all commands that begin with the characters already typed. For example, type **pas** and hit the **Tab** key twice. Add another **s** (**pass**) and hit the **Tab** key to complete the **passwd** command.

```
[root@serverX ~]# pas<Tab><Tab>
passwd        paste         pasuspender
[root@serverX ~]# pass<Tab>
[root@serverX ~]# passwd
```

Shell history allows you to view commands previously run and edit or execute them. Use the **history** command to view all previous commands, or use the up and down arrow keys to scroll through the history one command at a time. The output from the history command includes a numeric value. Use this numeric value after the exclamation point (**!**) to run the command again. Using non-numeric characters after the **!** will run the last command that began with those characters.

```
[root@serverX ~]# history
    1  su --help
    2  date --help
    3  man 1 intro
    4  id
    5  su -
    6  su -
    7  exit
    8  passwd
    9  passwd student
   10  man passwd
   11  history
[root@serverX ~]# !4
id
uid=0(root) gid=0(root) groups=0(root),...
[root@serverX ~]# !pa
passwd student
...
```

يعمل find
run يعمل and لأنه

Use this space for notes

References

GNOME Terminal Manual

- (Select **Help** → **Contents** in any **`gnome-terminal`** window.)

`info su` or **`info coreutils`** (*GNU Coreutils*)

- Section 23.6: "**su**: Run a command with substitute user and group ID"

passwd(1), **id**(1), **su**(1), **bash_builtins**(1), and **bash**(1) man pages

Practice Performance Checklist

Using Bash

- ☐ Log in graphically to your serverX host as **student**.
- ☐ Open a terminal window.
- ☐ Switch your shell prompt to run as the **root** user.
- ☐ Change the password of the **visitor** account to **visitor**.
- ☐ Exit the **root** shell.

Launching Graphical Tools from Bash

Commands that have graphical interfaces can be started from the command line just like any other program. For example, instead of selecting **Applications** → **Internet** → **Firefox** to start **Firefox**, you can type **firefox** at a shell prompt in one of your graphical terminal windows.

However, the downside of this is that as long as the graphical program is still running, the shell prompt that you used to start it will be unavailable. To avoid this inconvenience, you can take advantage of a feature of the shell called *job control*. Job control can be used to launch a program into the *background*, detaching it from the shell prompt and allowing the prompt to return while the graphical program is still running.

When you start a program normally at the shell prompt, we say it runs in the *foreground*, tying up the prompt. To start a program in the background, simply add an **&** to the end of the command line at the prompt.

This can be useful if for some reason you need to run a graphical program as **root** (generally not a preferred practice), most likely because it does not have proper support from **PolicyKit** to run as a regular user and escalate to root only when necessary.

How to run graphical commands as **root**:

1. Open a terminal window
2. Use **su -** to become root (you must use the **-**)
3. Run ***command* &**

   Example:

   ```
   [student@serverX ~]$ su -
   Password: redhat
   [root@serverX ~]# nautilus &
   ```

The **bash** shell also provides ways for you to change whether a process is running in the foreground, the background, or at all, from the shell prompt. Some additional job control related shell commands are:

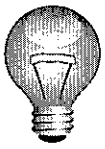
- **Ctrl+c** (often written ^C): *Terminate* the foreground process. This causes the foreground process to exit completely.
- **Ctrl+z** (often written ^Z): *Suspend* the foreground process. This causes the foreground process to stop executing and returns you to the shell prompt. The program will stay in memory, hanging. From here the process can be backgrounded or killed, but if you do nothing it will just wait, detached from the shell, until the shell exits.
- **jobs**: List backgrounded and stopped processes associated with this shell prompt.
- **fg**: Send a job to the foreground. Only one process can run in the foreground in a shell. If no argument is given, it will foreground the current job (shown with a **+** in the output of **jobs**). Pass **fg** the job ID to manage jobs other than the current job:

  ```
  [student@serverX ~]$ sleep 3000 &
  ```

Ctrl c → end
Ctrl z → Pause

```
[1] 22252
[student@serverX ~]$ sleep 4000 &
[2] 22253
[student@serverX ~]$ sleep 5000 &
[3] 22254
[student@serverX ~]$ jobs
[1]   Running                 sleep 3000 &
[2]-  Running                 sleep 4000 &
[3]+  Running                 sleep 5000 &
[student@serverX ~]$ fg → for grand ▽ job no.
sleep 5000
 Ctrl+c
[student@serverX ~]$ jobs
[1]-  Running                 sleep 3000 &
[2]+  Running                 sleep 4000 &
[student@serverX ~]$ fg 1
sleep 3000
```

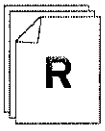
- **bg**: Send a job to the background. Many jobs can run in the background in a single shell. If no argument is given, **bg** will background the current job (just like **fg** foregrounds the current job) as though the job had been started with **&**.



Important

Note that even if a job is backgrounded, if it issues output or error messages to the terminal window, those messages will still be printed in the terminal. This can be confusing when multiple jobs are running at the same prompt and may be issuing output.

Kill %1



References

GNU Bash Reference Manual

- Chapter 7: Job Control

> http://www.gnu.org/software/bash/manual
> If ***bash-doc*** is installed from the ***Optional*** RHN channel:
> file:///usr/share/doc/bash-4.1.2/doc/bashref.pdf

jobs(1), **fg**(1) and **bg**(1) man pages

System-config-tab tab

Su - user profile "yonkal be kol Fasa lcha el-Profile"

su yonkal be nafs elmakan elle leh variable zay ma hoza

Practice Performance Checklist

Launching Graphical Tools from Bash

- ☐ Log in to your serverX host graphically as **student**.
- ☐ Open a terminal window.
- ☐ Within the window switch to a **root** shell. su -
- ☐ Launch **nautilus** in the foreground from the command line. fg
- ☐ Use the keyboard shortcut to get your shell prompt back without terminating the process.
- ☐ Put **nautilus** in the background. Ctrl z → bg
- ☐ List your current shell jobs. jobs
- ☐ Exit the root shell. exit

Test

Criterion Test

Performance Checklist

Get Started with Bash

From a Terminal window, use the bash shell to launch a Nautilus file manager as root user. Copy a file and create a folder in Nautilus.

- ☐ Log in to your serverX host as **student**.
- ☐ Open a Terminal window and become **root**.
- ☐ Launch **nautilus** from the command line.
- ☐ Navigate to the **/etc** folder and copy **issue** to **issue.backup**.
- ☐ Create a new folder called **/usr/local/music**.

Personal Notes

Unit Summary

Introduction to Bash

In this section you learned how to:

- List the benefits and services provided by Bash
- Execute shell commands with correct syntax

Using Bash

In this section you learned how to:

- Access a Bash prompt from a GNOME session
- List previous shell commands and execute them using Bash history
- Complete partial commands using the [tab] key
- Complete partial file and path names using the [tab] key
- Change their account password from Bash
- Display their current user and list of groups from Bash
- Logout from Bash

Launching Graphical Tools from Bash

In this section you learned how to:

- Temporarily switch to another account from Bash without logging out
- Describe the role and privileges of the root user
- Launch graphical commands from Bash as root

UNIT SIX

MANAGE PHYSICAL STORAGE I

Introduction

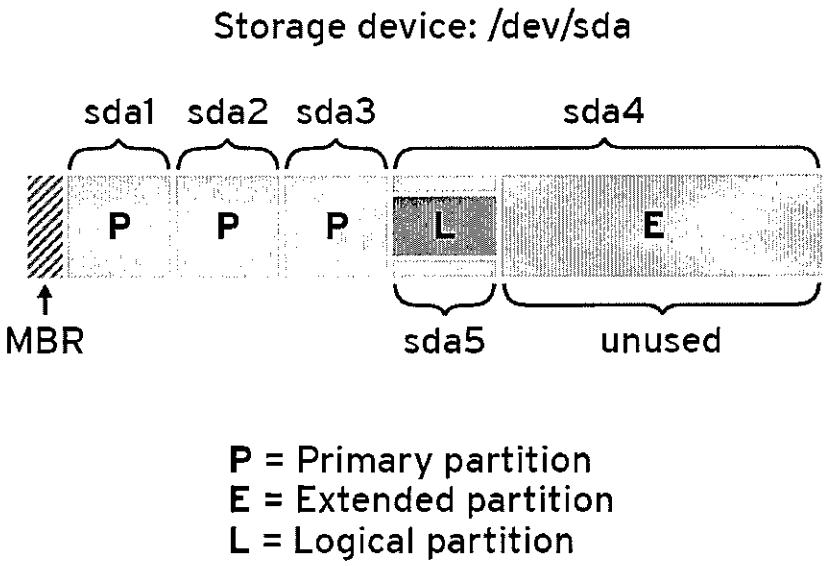
Topics covered in this unit:

- IBM PC storage model
- Determine disk usage
- Manage virtual guests
- Create a new file system

Describe MBR, Primary, Extended, and Logical Partitions

Hard disks and storage devices are normally divided up into smaller chunks called *partitions*. A partition is a way to compartmentalize a disk, so that different parts of it can be formatted with different file systems or used for different purposes. For example, one partition could contain user home directories while another could contain system data and logs; by placing the data in two separate file systems on two separate partitions, even if a user fills up the home directory partition with data, the system data partition may have space.

Most Red Hat Enterprise Linux systems on the x86 and x86-64 processor architectures use the *MBR partitioning format* for their hard disks. This is the same format that is used by most Microsoft Windows systems, and dates back to the IBM PC.



In this format, the first sector of the disk is reserved for the *Master Boot Record*, or MBR. The first 446 bytes contain the first part of the bootloader that starts the system, followed by 64 bytes that contains the *partition table*. There is room for information about four *primary partitions* in the partition table; where they start, where they end, and a code that indicates what sort of information is stored in them. The partitions must then be formatted with a file system before they can be used.

If more partitions are needed, one of the primary partitions can be converted into an *extended partition* which, rather than having a file system itself, is divided into multiple *logical partitions*. For various reasons, typically you are limited to no more than 15 partitions in total; fourteen are usable for file systems, counting three primaries, the extended, and eleven logical.

Important

Do not confuse *logical partitions* with *logical volumes*. Logical volumes will be discussed in the next unit.

Storage devices are represented by *device files* in **/dev**. In Red Hat Enterprise Linux 6, the first SCSI, PATA/SATA, or USB hard drive detected is **/dev/sda**, the second is **/dev/sdb**, and so on. This name represents the whole drive. The first primary partition on **/dev/sda** is **/dev/sda1**, the second partition is **/dev/sda2**, and so on. Partitions 1 through 4 are the primary partitions; 4 is usually used as the extended partition if one is used; 5 and higher are always logical partitions.

Note

One exception are paravirtualized hard drives in guest virtual machines, which instead show up as **/dev/vd?**. Also, in earlier versions of Red Hat Enterprise Linux, some PATA and SATA drives may appear as **/dev/hd?** instead.

Use this space for notes

References

Red Hat Enterprise Linux Installation Guide

- Appendix A: An Introduction to Disk Partitions

Ch. 6 why:

2 Controller (Socket) in motherboard
& each one master & slave
IDE = 4

Practice Quiz

Physical Storage Concepts

1. The IBM PC disk architecture supports how many primary partitions maximum?

   (select one of the following...)

   a. 2
   b. 4
   c. 15
   d. 32

2. Which of the following ***cannot*** be formatted and used as a file system?

   (select one of the following...)

   a. Primary partition
   b. Extended partition
   c. Logical partition
   d. All of the above
   e. None of the above

List Available Disk Devices

The **Palimpsest Disk Utility** application (**`gnome-disk-utility`**) is a very recent addition to Red Hat Enterprise Linux, and provides an improved graphical interface for easily managing disk partitions. It will list the devices available to the system, information about the characteristics and health of the hardware, how the disks are partitioned, and allow you to re-partition the disk and format partitions with file systems.

- Launch **Disk Utility** by selecting **Applications** → **System Tools** → **Disk Utility**.
- Select the hard disk to manage in the left pane.
- Information about the selected disk displays in the right pane.

Note that this information includes a diagram of the partition table on the disk along with a host of other useful information.

Comparison

Palimpsest Disk Utility is similar to the Windows **Disk Management** tool.

Use this space for notes

Practice Quiz

List Available Disk Devices

Use **Disk Utility** on your desktopX workstation to answer the following questions:

1. _____ is the Linux device name for the first hard drive on your desktopX.example.com machine.

2. Is there free space available on that device? If so, how much?

   _____

Introduce Classroom Virtual Machines

Note

The instructor has configured your machine as a host for *virtual machines* that will be used in a number of labs from this point forward in the class. At this point we will pause the discussion briefly so that you can learn about how to access and manage these existing virtual machines on your system.

Looking Ahead: You will learn more about virtualization in Red Hat Enterprise Linux and about how to set up your own virtual machines in Unit 19 of this course, "Manage Virtual Machines".

Launch Virtual Machine Manager

1. Select **Applications** → **System Tools** → **Virtual Machine Manager** to launch the Virtual Machine Manager utility.

Start a Virtual Machine

1. Right click on the virtual guest's icon.
2. Select **Run**.

Connect to a Virtual Machine's Console

1. Right click on the virtual guest's icon.
2. Select **Open**.

Resize the Screen

- In the console for the virtual guest, select **View** → **Resize to VM**.

Release the Mouse Caught in the Guest Window

- Hit the left **`Ctrl`** and **`Alt`** keys simultaneously.

References

Red Hat Enterprise Linux Virtualization

- Chapter 31: Managing Guests with the Virtual Machine Manager (virt-manager)

Practice Quiz

List Available Disk Devices (Redux)

Before you begin, reset the serverX virtual machine. Log into your desktopX workstation as **student** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reset your virtual server's storage and boot it after a fresh installation.

Use **Disk Utility** on your serverX virtual server to answer the following questions:

1. _____ is the Linux device name for the first hard drive on your serverX.example.com machine.

2. Is there free space available on that device? If so, how much?

   _____

Create a New Disk Partition, Format It with a File System and Use It

Disk Utility can also be used to create new partitions and prepare them for use. Once a partition has been created, it must be *formatted* with a file system before it can be used. The standard file system used in Red Hat Enterprise Linux is *ext4*, the *Fourth Extended File System*.

In order to use the file system, we need to associate it with a *mount point*, and empty directory on a file system that is already available. Then the contents of that file system can be browsed as if they are the contents of the mount point directory. This is called *mounting* the file system on the mount point.

A file which only root can edit, **/etc/fstab**, lists what partitions should have their file systems mounted on what mount points with which options, one partition per line. A typical line might look like this:

```
/dev/sda6  /data  ext4  defaults  1  2
```

This indicates that the **ext4** file system on the **/dev/sda6** partition should be mounted on the directory **/data** automatically using default options at boot time, and it should be backed up and checked for errors normally.

Once this is set, root can run **mount /data** to mount the file system above, and **umount /data** to un-mount it.

Note

There are two special contingencies that need to be handled when using **Disk Utility** to format and manage new drives:

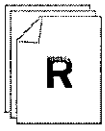
1. With new, uninitialized disks, you will be prompted to format the drive before you can create partitions.
2. When there are three existing primary partitions, you should allocate all remaining space as an extended partition so you are able to create logical partitions for additional file systems.

Use this space for notes

High-level Steps for Creating Persistent Storage

1. Log into GNOME as a regular user.
2. Use **Disk Utility** to create a partition. Enter the root password when prompted by the **Authentication is required to create a partition** dialog.
3. Format the file system and assign it a label.
4. Test the file system by mounting it with **Disk Utility**.

   (It will be mounted on the directory **/media/*your-label***.)
5. Open a shell prompt with **Applications** → **System Tools** → **Terminal**.
6. At the shell prompt, type **su -** to switch to a root shell.
7. As root, type the shell command **mkdir /data** to make an empty directory, **/data**, for the file system.
8. Use **gedit** to add a line to **/etc/fstab** which will mount the ext4 file system in your new partition on your mount point (**/data** in this example), using default options as in the example above. Save **/etc/fstab**.
9. As root, run **umount /media/*your-label***, then **mount /data**. Verify that your partition is mounted on **/data** by highlighting the partition in **Disk Utility**.
10. Reboot to confirm that the file system mounts automatically on the desired mount point.



References

mkdir(1), **mount**(8), and **umount**(8) man pages

Note

Looking Ahead: The general steps outlined above must also be followed when using command line tools. The command line approach, using tools such as **fdisk**(8) and **mkfs**(8), is introduced in the *Red Hat System Administration II* course.

Test

Criterion Test

Case Study

Configure Partitions and File Systems Persistently

Before you begin...

Login as **student** on desktopX. When the GNOME desktop appears, open the folder called **Labs**. Double-click on the **Physical Storage Lab Setup** launcher. A window will appear confirming you want to reset your virtual machine. Type **y**.

When a colleague built your server - serverX, they didn't use all of the available disk space to permit future growth. A persistent area for storage needs to be created separate from your existing Linux file system hierarchy.

Create a new partition on your hard disk that is 1 GB in size and leave at least a small amount of disk space unused. It should *not* be encrypted and it should contain an ext4 file system that mounts under the **/extras** mount point persistently when the system boots.

Once you have completed your work, reboot serverX. Log into it as **student**, open the **Labs** folder and double click the **Physical Storage Grading** icon to confirm that you have completed the lab correctly.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

① disk utility
↳ new partition

② /etc/fstab
↳ last line
⇓
LABEL=Sample /extras ext4 defaults 0 0
or /dev/sda3

dump 0 or no
fsck 0 filesystem check

Personal Notes

Unit Summary

Describe MBR, Primary, Extended, and Logical Partitions

In this section you learned how to:

- Describe the MBR, primary, extended, and logical partitions

List Available Disk Devices

In this section you learned how to:

- List current disk usage and availability

Introduce Classroom Virtual Machines

In this section you learned how to:

- Connect to virtual machines

Create a New Disk Partition, Format It with a File System and Use It

In this section you learned how to:

- Create a new partition and format it with a specified file system
- Format an encrypted partition
- Mount a locally connected file system to their system for temporary use
- Unmount a mounted file system
- Configure your system so a file system is mounted when the system boots

UNIT SEVEN

MANAGE LOGICAL VOLUMES

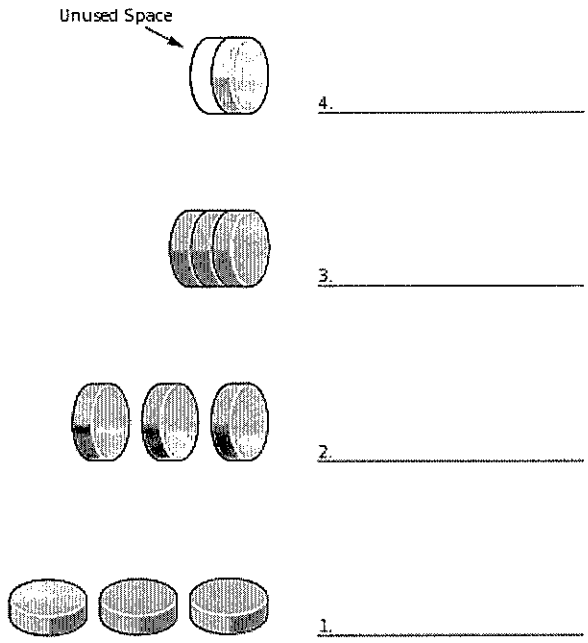
Introduction

Topics covered in this unit:

- LVM (logical volume management) concepts and terms
- Displaying LVM usage
- Deploying LVM
- Extending LVM storage
- Extending a file system on LVM
- Removing a disk from LVM

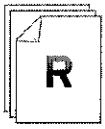
General LVM Concepts and Terms

Logical Volume Management provides a more flexible way to manage disk space than physical disk partitions. Raw disk space in physical disk partitions can be pooled together or divided up into virtual partitions called *logical volumes*. This allows a number of powerful features, such as the ability to create file systems larger than any one disk, the ability to divide up a single disk into more than fourteen file systems, and the ability to easily extend an existing file system with more space without the need to reformat it.



LVM Definitions

- *physical volume*: a partition marked as usable space for LVM. On an MBR disk, marked with partition type 0x8e.
- *volume group*: a collection of one or more physical volumes. Can be thought of as a virtual disk drive.
- *logical volume*: Can be thought of as a virtual partition of the volume group. This is formatted with a file system and used like a partition.
- *physical extent*: disk space is allocated from physical volumes by the volume group to logical volumes in large chunks called *physical extents*. Logical volumes are collections of physical extents from one or more physical volumes.



References

Red Hat Enterprise Linux Logical Volume Manager Administration
- Section 1.2: Logical Volumes

Red Hat Enterprise Linux Logical Volume Manager Administration
- Section 1.3: LVM Architecture Overview

Practice Resequencing Exercise

General LVM Concepts and Terms

__ Create physical volume(s)

__ Create physical partition(s)

__ Create logical volume(s)

__ Create volume group

Displaying Current LVM Usage

Search & Learn: LVM

In this section, we will have a short activity that will give you a chance to explore the graphical **Logical Volume Management** utility, **`system-config-lvm`**. You will have about five minutes to explore the utility before working on the quiz on the next page.

Note

Do not make any changes to your configuration at this point.

The following steps are to be performed on your serverX machine.

1. Open the Logical Volume Management tool: **System** → **Administration** → **Logical Volume Management**.
2. Examine the physical volumes and how they are used.
3. Examine the volume group that is defined and its logical volumes.

References

Red Hat Enterprise Linux Storage Administration Guide

- Section 3.2: Using system-config-lvm

Practice Quiz

Displaying Current LVM Usage

Perform the following steps on serverX unless directed otherwise.

1. What is the name of your volume group?

   _____

2. What is the total size of the volume group?

   _____

3. How much, if any, unused space is in the volume group?

   _____

4. How many total and free physical extents does the volume group have? 143 12 1

5. How big is each physical extent in the volume group?

   _____

Initial LVM Deployment

Steps to Deploy Logical Volumes

Work as a class to complete the following list of steps required to create logical volume storage. Some of the steps have been provided, but you will need to write in the missing steps. The completed list of steps is available in the Solutions appendix of this student guide.

1. ### Create a New Partition (Review)

   a.

   b. Edit the new partition and change its type to Linux LVM (0x8e)

   c.

2. ### Initialize the New Partition As an LVM Physical Volume

   a. Select **System** → **Administration** → **Logical Volume Management** from the GNOME desktop menus.

   b. Expand the **Uninitialized Entities** in the left pane.

   c.

   d. Select the new partition (make sure the partition type is 0x8e in the right pane).

   e.

   f.

3. ### Create a Volume Group Using the New Physical Volume

   a.

   b. Specify the **Volume Group Name**.

   c. Click **OK**.

4. ### Create a Logical Volume within the New Volume Group

   a. Expand the new volume group.

   b. Select **Logical View**.

   c.

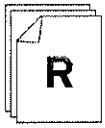
   d.

   e.

   f. Specify file system properties such as file system type, mount point, etc.

   g.

   h. Confirm to create the mount point when necessary.



References

Red Hat Enterprise Linux Storage Administration Guide

- Section 3.2: Using system-config-lvm

Practice Performance Checklist

Initial LVM Deployment

Before you begin...

Reset the serverX virtual machine. Log into your desktopX workstation as **student** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reset your virtual server's storage and boot it after a fresh installation.

Perform the following steps on serverX unless directed otherwise. Perform all physical partitioning so additional partitions can be created if needed.

- ☐ Create a new partition of type Linux LVM (0x8e) that is approximately 400 MB in size.

  * fdisk
  * edit partition → 0x8e
  * logical volume manager

- ☐ Initialize the new partition as a physical volume.

  initialize → convert physical volume

- ☐ Use the physical volume to create a new volume group called **vg.learn**.

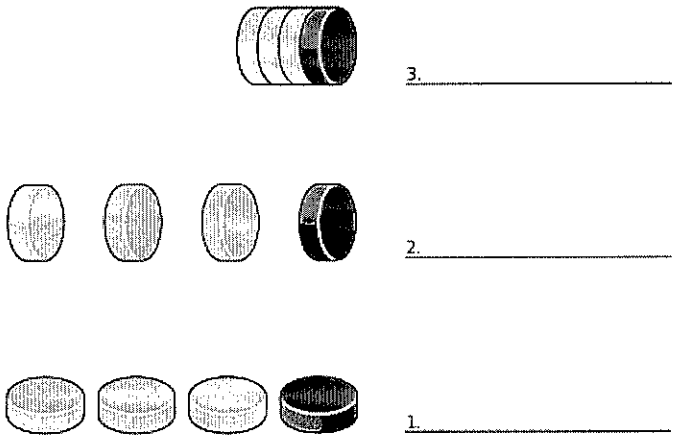
  * create New volume group

  → Create new logical volume

- ☐ Create a logical volume called **data** within **vg.learn** that consumes all physical extents. It should contain an ext4 file system that mounts as **/data** persistently.

- ☐ Use Nautilus to browse to **/data** and confirm it exists with a **lost+found** folder as its only contents.

Extending a Volume Group



Volume groups can be *extended* by assigning them additional physical volumes. These PVs may be additional partitions on the same hard drive or may be provided by partitions on different hard drives. This space can then be used to create more logical volumes (or, as will be discussed in the next section, to *extend* existing logical volumes).

Steps to Extend a Volume Group

1. Click the **Add to existing Volume Group** button.
2.
3.

References

Red Hat Enterprise Linux Storage Administration Guide

- Section 3.2.6: Extending a Volume Group

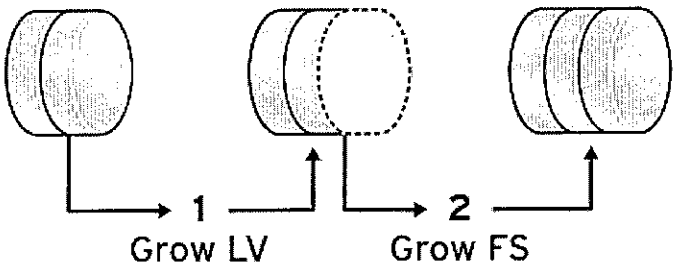
Practice Performance Checklist

Extending a Volume Group

Perform the following steps on serverX unless directed otherwise.

- ☐ Create a new partition of type Linux LVM (0x8e) that consumes all remaining disk space.
- ☐ Initialize the new partition as a physical volume.
- ☐ Add the physical volume to the **`vg.learn`** volume group.

Extending a Logical Volume

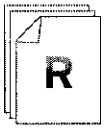


A logical volume can be extended if there are free extents left in its volume group. The extents are allocated to the logical volume, making it larger. To be of use, once the logical volume is extended any file system on the logical volume must then be extended to fill the new space.

One way to think of this is to imagine that the logical volume is a box containing a file system. First you extend the logical volume, making the box bigger. Then you grow the file system to fill the larger box.

Steps to Extend a Logical Volume and Its File System

1. Open the Logical Volume Management tool: **System → Administration → Logical Volume Management.**
2. Browse the logical devices in the left pane and select the logical volume you want to extend.
3.
4.
5.



References

Red Hat Enterprise Linux Storage Administration Guide

- Section 3.2.7: Editing a Logical Volume

Practice Performance Checklist

Extending a Logical Volume

Perform the following steps on serverX unless directed otherwise.

- ☐ Open a Nautilus browser window, and navigate to the **/data** directory. Note the "available space" in the lower lefthand corner.
- ☐ Grow the data logical volume and its file system (**/data**) by 200 MB so it is a total size of about 600 MB.
- ☐ Re-examine the "available space" in the Nautilus browser window for the **/data** directory. Confirm that more space is now available.

Removing a Physical Volume

Physical volumes sometimes are removed from volume groups. This may need to be done because the disk the PV is on needs to be replaced with a newer or larger hard drive.

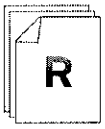
It is possible to migrate data stored on a physical volume to another physical volume in the volume group so that the old physical volume can be removed. This can be done without disturbing the logical volumes in the volume group.

Read the following reference about removing a physical volume and take notes below. What are the steps required to remove a physical volume?

The site **`http://instructor.example.com/pub/docs/`** has a copy of the documentation referenced below.

Steps to Remove a Physical Volume

1. Open the Logical Volume Management tool: **System** → **Administration** → **Logical Volume Management**.
2.
3.
4. Click the **Migrate Selected Extent(s) From Volume** button.
5.



References

Red Hat Enterprise Linux Storage Administration Guide

- Section 3.2.3: Migrating Extents

Practice Performance Checklist

Removing a Physical Volume

Perform the following steps on serverX unless directed otherwise.

- ☐ Migrate all physical extents from the original partition that was used to create the **`vg.learn`** volume group.
- ☐ Remove the original partition from the **`vg.learn`** volume group.
- ☐ Remove the physical volume from LVM.

Test

Criterion Test

Case Study

Manage Logical Volumes

Before you begin...

Login as **student** on desktopX. When the GNOME desktop appears, open the folder called **Labs**. Double-click on the **Logical Volume Lab Setup** launcher. A window will appear confirming you want to reset your virtual machine. Type **y**.

You have just been assigned to administer a freshly installed server - serverX. Management would like some adjustments made to the disk allocation according to the following specifications:

- The **/home** file system is too small and should be expanded to take 500 MB total space.
- Use the remaining disk space to create a volume group called **extra** with a logical volume called **iso** that contains an ext4 file system that will be mounted as **/iso**. Allocate the file system so it can be migrated to a larger device and grown without down time.

When you have completed the tasks, reboot serverX and run the **Logical Volume Grading** grading script.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

General LVM Concepts and Terms

In this section you learned how to:

- Define physical volume, volume group, logical volume, physical extent, and general Logical Volume Manager (LVM) architecture

Displaying Current LVM Usage

In this section you learned how to:

- Display all current volume group usage and availability

Initial LVM Deployment

In this section you learned how to:

- Create a partition as an LVM physical volume
- Create an LVM volume group with a specified name
- Create a logical volume of a specified size with a specified name

Extending a Volume Group

In this section you learned how to:

- Extend a volume using a subset of available free space

Extending a Logical Volume

In this section you learned how to:

- Extend the logical volume to use a subset of free volume group space and non-destructively extend the file system

Removing a Physical Volume

In this section you learned how to:

- Evacuate the data from and remove the physical volume from a volume group

UNIT EIGHT

MONITOR SYSTEM RESOURCES

Introduction

Topics covered in this unit:

- Processes, priorities, and signals
- System Monitor
- Process management
- Disk Usage Analyzer

Understand Process, Priority, and Signal Concepts

A process is an instance of a running program. Processes have their own address space in memory, thread of execution, and characteristics such as security context, environment and current priority. The Linux kernel tracks every aspect of a process by its process ID number (or PID). Information about each process is advertised by the kernel to user programs through the **/proc/*PID*** directories.

When a process starts another program, the new process is called its *child process*. The original process is the *parent process* of its child process. Child processes inherit characteristics from its parent, such as its environment and the user and groups it as which it runs.

Child processes can have their own children, and so on. When a parent process exits, all of its descendant processes also exit.

Signals

The operating system communicates to processes through *signals*. These signals report events or error situations to processes. In many cases, these signals will result in the process exiting. One typical signal is **SIGTERM**, which *terminates* the process; it asks it to exit cleanly. Another is **SIGKILL**, which *kills* the process; the process is required to exit immediately.

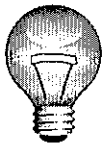
Process Scheduling

Only one process at a time may be executing per logical processing unit on its CPUs. Therefore, every process which is ready to run has a scheduling priority: a ranking among ready processes determining which should get to run next.

The Linux process scheduler divides CPU time into time slices, in which each process will get a turn to run on a logical processing unit, higher priority processes first. The formula for calculating this priority is complex, but users can affect the priority by setting the *niceness* value for a process.

Niceness values range from -20 to +19, which indicates how much of a bonus or penalty to assign to the priority of the process. Most processes run with a niceness value of 0 (no change). Smaller numbers are higher priority. Processes with a higher priority will run first in each time slice, and will run longer before its turn to run ends.

Users can adjust this value down as far as +19, but can not increase it. (This is why this is called the "nice" value.) The root user can increase the priority of a process as high as -20.



Important

Note carefully the effect of niceness. If all ready processes have the same priority, they will share the processor equally. Priority only has an effect when two processes at different priority levels are competing for CPU time, in which case the lower priority process will get less time and appear to run more slowly.

Use this space for notes

References

Red Hat Enterprise Linux Deployment Guide
- Section 20.1: System Processes

info libc (*GNU C Library Reference Manual*)
- Section 24: Signal Handling

info libc (*GNU C Library Reference Manual*)
- Section 26: Processes

(Note that *glibc-devel* must be installed for these Info nodes to be available.)

signal(7) man page

Why monitor CPU, Memory, ~~process~~ disk space
- to know

Process: unique process id to data
- Signal:
- ↓ Nice Value: high priority ↑ cubs cubs
- process like as parent & child ⇒ tree

MPR: Boot loader
process no. (init)

(System Monitor)

Monitor Processes by CPU or Memory Consumption

The GNOME **System Monitor** (**`gnome-system-monitor`**) is a utility which makes it easy to observe which processes are running on the system and what resources they are currently using. It also provides a means to terminate or kill processes and to adjust their current niceness values.

In this section the instructor will perform a short demonstration to show you how the **System Monitor** utility works.

Comparison

System Monitor is similar to the **Task Manager** utility in Microsoft Windows.

Steps for viewing processes by priority or memory consumption:

1. Launch **System Monitor** by selecting **Applications** → **System Tools** → **System Monitor**.
2. Select the **Processes** tab.
3. Click on any process displayed.
4. Go to **View** → **All Processes** to view all processes or you can view active processes.
5. Click the **%CPU** column in the center pane so the arrow points upward.
6. Click the **Memory** column in the center pane so the arrow points upward.

Use this space for notes

References

System Monitor Manual

- Launch the tool, then select **Help** → **Contents**

Practice Quiz

Monitor Running Processes

Before you begin, login to serverX as student, open the **Labs** folder and double-click the **Process Management Setup** launcher. It will create processes that you will examine and manipulate throughout this unit.

Perform the following steps on serverX unless directed otherwise.

1. Which process running on your serverX machine is currently consuming the most CPU?

   _____

2. Which process on your serverX machine is currently consuming the most memory?

   _____

Manage Running Processes

Search & Learn: process101

In this section, we will divide up into small groups and have a short classroom activity to familiarize you with **System Monitor**. There is a process running on your system with the name **`process101`**. You will first adjust its nice value, then terminate the process, using **System Monitor**. Complete solutions are available in the appendix.

1. Change the **`nice`** value of **`process101`** to **`7`**. Write down the steps you took to make that happen:

   a. Launch System Monitor by selecting **Applications** → **System Tools** → **System Monitor**.

   b.

   c.

   d.

   e.

   f.

2. Terminate the **`process101`** process. Write down the steps you took to terminate the process:

   a. Launch System Monitor by selecting **Applications** → **System Tools** → **System Monitor**.

   b.

   c.

   d.

   e. If the process does not terminate:

      a. Highlight the process.

      b.

      c.

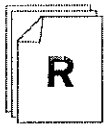
Note

Root authentication is required when manipulating processes you don't own or when you try to increase a process' priority.

Important

In **System Monitor**, **End Process** sends the process a **SIGTERM** signal, allowing it to gracefully terminate. (This is similar to **End Task** in the Windows **Task Manager**.)

Kill Process instead sends the process a **SIGKILL** signal, forcing it to die immediately. (This is similar to **End Process** in the Windows **Task Manager**.)



References

System Monitor Manual

- Launch the tool, then select **Help** → **Contents**

Practice Performance Checklist

Terminate and Change Process Priority

Change the priority of a CPU hog and terminate a memory hog on serverX.

Perform the following steps on serverX unless directed otherwise.

- ☐ Change the priority of the process called **hippo** that is using a lot of CPU resources to 5.
- ☐ Terminate the process called **elephant** that is using a lot of memory resources.
- ☐ When you have completed the tasks, double-click the **Process Management Grading** launcher icon in the **Labs** folder on student's GNOME desktop. This will confirm if you identified and managed the correct processes.

Monitor Disk Usage

While **System Monitor** provides some information on disk space usage, a much more useful tool is **Disk Usage Analyzer.** It provides detailed information on disk usage, as well as visualizing the data as a browsable rings chart or treemap chart to help you understand it better.

In this section the instructor will demonstrate and discuss the following procedures for getting information about file system usage.

Steps for Performing File System-Level Disk Usage Analysis

1. Launch the Disk Analysis tool by selecting **Applications** → **System Tools** → **Disk Usage Analyzer.**
2. Select **Edit** → **Preferences** to display device, mount point, file system type, total size, and available space information.

Steps for Performing Directory-level Disk Usage Analysis

1. Launch the Disk Analysis tool by selecting **Applications** → **System Tools** → **Disk Usage Analyzer.**
2. Select **Analyzer** → **Scan Filesystem** to scan the entire root file system.
3. To view directory usage, click on the name of the directory in the left pane, or the directory ring in the right pane.
4. Recurse into deeper subdirectories as desired.

References

Disk Usage Analyzer Manual

- Launch the tool, then select **Help** → **Contents**

Red Hat Enterprise Linux Deployment Guide

- Section 20.3: File Systems

filesystem
df -h
du -h /etc
du -sh /etc

Practice Exercise

Monitor Disk Usage

Carefully perform the following steps. Ask your instructor if you have problems or questions.

Perform the following steps on serverX unless directed otherwise.

Disk usage Analyzer

1. Which file system has the most free disk space on serverX? /
2. Which top level directory in / uses the most space on serverX? /usr
3. Which top level directory in **/home** uses the least space on serverX? student

Test

Criterion Test

Exercise

Monitoring Processes and Filesystems

Before you begin...

Login as **`student`** on desktopX. When the GNOME desktop appears, open the folder called **Labs**. Double-click the **`Process Management Test Setup`** launcher. A window will appear confirming you want to reset your virtual machine. Type **y**. Be patient and wait a couple minutes for serverX to be prepared for this lab.

Carefully perform the following steps. Ask your instructor if you have problems or questions.

Perform the following steps on serverX unless directed otherwise.

1. Identify the process that consumes the most memory on serverX and terminate it.
2. Identify the process that consumes the most CPU on serverX and change the priority to 10.
3. Determine which file system has the least amount of available free space.
4. Open the **`/home/student/Desktop/least-free-space-filesystem.txt`** file on serverX, then edit it so that only the directory that matches what you found in the previous step appears in the file.
5. Determine which top level directory in **`/usr`** consumes the most disk space?
6. Open the **`/home/student/Desktop/usr-directory.txt`** file on serverX, then edit it so that only the directory that matches what you found in the previous step appears in the file?
7. When you finish, double-click the **Process Management Test Grading** icon in the **Labs** folder on the GNOME desktop to confirm that you have completed the lab correctly.

Personal Notes

Unit Summary

Understand Process, Priority, and Signal Concepts

In this section you learned how to:

- Define concepts such as process, parent/child process relationships, process ID (PID), signals, and nice/priority value

Monitor Processes by CPU or Memory Consumption

In this section you learned how to:

- Use GUI tools to identify the process consuming the most CPU resources on the system
- Use GUI tools to identify the process using the most memory resources on the system

Manage Running Processes

In this section you learned how to:

- Terminate a specific process using GUI tools
- Change the priority of a specific process using GUI tools

Monitor Disk Usage

In this section you learned how to:

- Identify current file system usage and availability
- Identify which subdirectory of a given directory consumes the most disk resources

UNIT NINE

MANAGE SYSTEM SOFTWARE

Introduction

Topics covered in this unit:

- Software inventory
- Red Hat Network (RHN) registration
- Manage packages

Identify Installed Packages

One of the fundamental problems in system administration is how to manage and update software installed on a system. One way to install software is simply to expand an archive of executables, libraries, and other support files and copy the contents into place on the system. The problem with this approach is then it is very difficult to determine why a file was installed on the system in the first place, what needs it, and therefore whether it can be safely removed or updated to a newer version as software is removed or updated on a production system.

Many years ago, Red Hat developed the **RPM Package Manager**, which provides a standard way to package software for distribution, cleanly install, update, and remove software from the system, and to ensure that all support libraries needed by an application are installed on the system properly.

All software provided by Red Hat for Red Hat Enterprise Linux is provided as an *RPM package*. These are archives that contain all the files and programs needed for the software package, as well as information about the package, its dependencies on other packages (such as shared libraries or supporting software), and scripts which should be run when it is installed or uninstalled.

Once a system is installed, additional software packages and updates are normally installed from a network *package repository*, most frequently the Red Hat Network service which will be discussed in the next section. Tools such as **PackageKit** and **yum** can be used to install individual packages or *package collections* (sometimes called *package groups*).

Use this space for notes

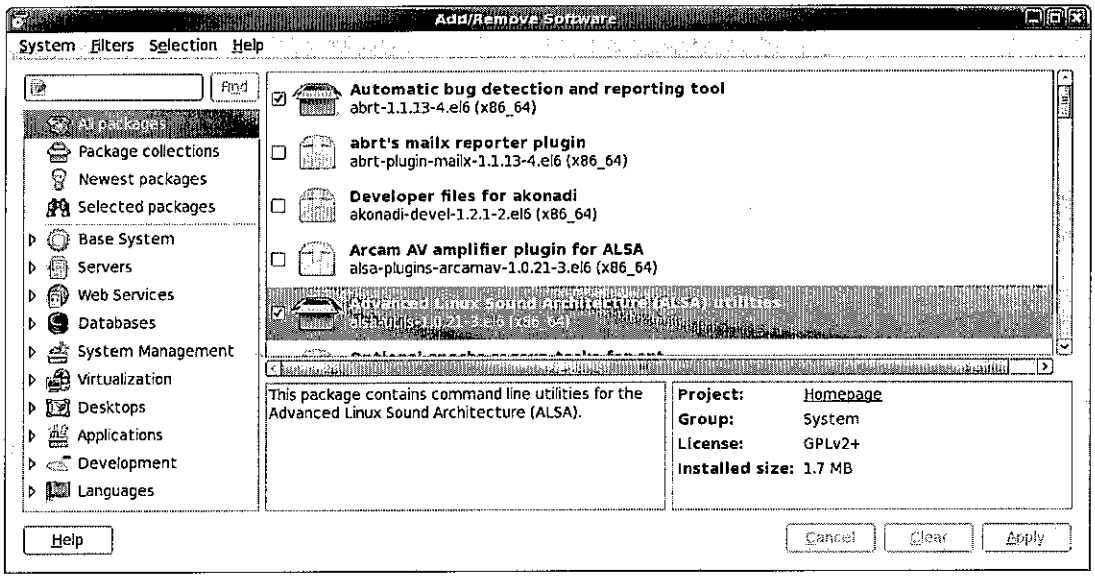
Using PackageKit

To identify what software is currently installed, open the **Add/Remove Software** application (also known as **`gpk-application`**) by clicking on **System** → **Administration** → **Add/Remove Software**.

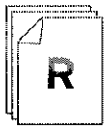
To view individual packages which are installed or which are available, select **All packages** in the left pane and browse the list in the right pane. Those packages with a check in the checkbox (and an open box icon) are installed. Those packages with no check in the checkbox (and a closed box icon) are available to be installed.

To view package groups that are installed or available, select **Package collections** in the left pane and browse the list in the right pane. Those groups with a check in the checkbox are installed; those which do not have a check in the checkbox are available to be installed.

The screenshot below shows a list of individual packages.



The search field, which matches arbitrary text against package names, summaries, and descriptions, allows administrators to quickly find appropriate packages.



References

Red Hat Enterprise Linux Deployment Guide

- Chapter 2: PackageKit

gnome-packagekit Manual

- (**System** → **Help**, under the **System** category of **GNOME Help Browser**)

Register with Red Hat Network (RHN)

What is Red Hat Network?

Red Hat Network is a centrally-managed service that makes it easy to deploy software and software updates to Red Hat Enterprise Linux systems and to remotely manage and monitor those systems. You can use the "hosted" RHN service managed by Red Hat, or you can set up and manage your own RHN Satellite in your organization. Either way, to get package updates for your clients from RHN and to have them show up in your web management interface, you need to start by registering those systems with the RHN server of your choice.

Using rhn_register

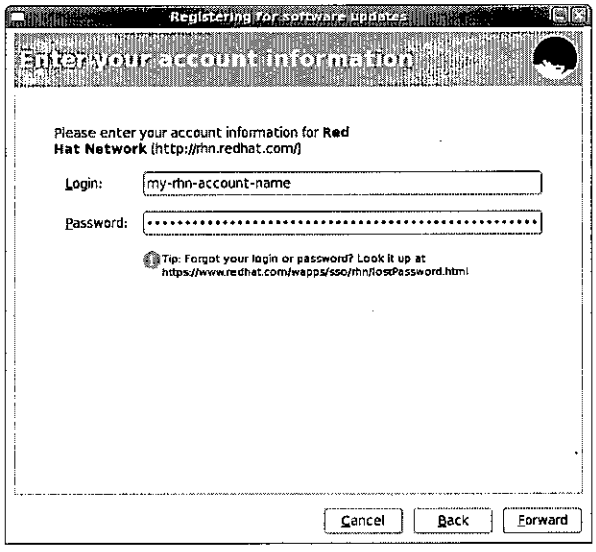
Start the Red Hat Network (RHN) registration process by running the **`rhn_register`** command from the command-line or choosing it from the GUI menu: **System** → **Administration** → **RHN Registration**

If you have a RHN Satellite or RHN Proxy server, choose the **I have access to a Red Hat Network Satellite...** button in the GUI. Fill in the DNS name of the RHN Satellite server or RHN Proxy server.

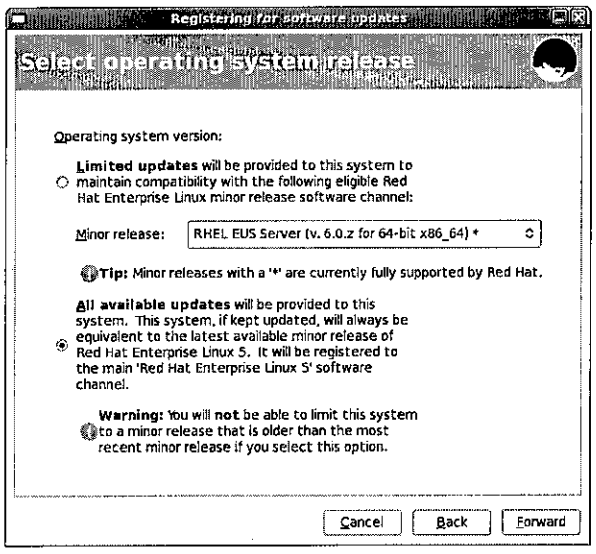
If you do not have a RHN Satellite or RHN Proxy server, or you want to register with Hosted RHN, choose the **I'd like to receive updates from Red Hat Network** button.

If you need to set proxy setting for the connection, click on the **Advanced Network Configuration...** button and fill in the appropriate fields.

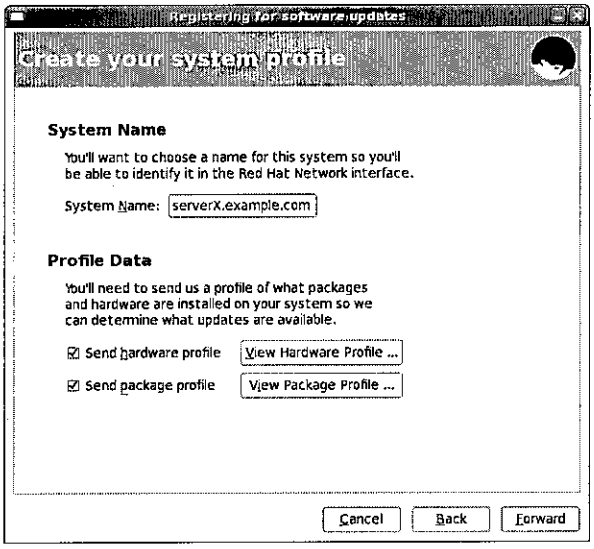
Fill in your Red Hat Network account information. If you have forgotten your account name or password, or you need to create a new account, go to `https://www.redhat.com/wapps/sso/login.html`



The next screen allows you to limit updates to maintain compatibility with Red Hat Enterprise Linux minor releases. If you want this ability choose **Limited updates.** If you want all the current updates, choose **All available updates.**

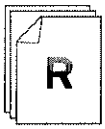


Enter the name for your system (it will use the current hostname by default), and optionally send the hardware and package profile to RHN.



Note

The **rhn_register** command works equally well in a graphical environment or a text environment. If you run **rhn_register** in a text-only environment, it will prompt for information much as the GUI does.



References

rhn_register(8) and **rhnplugin**(8) man pages

Knowledgebase: "What is the command rhn_register used for in Red Hat Enterprise Linux?"
https://access.redhat.com/kb/docs/DOC-11217

Knowledgebase: "I had to re-install my system. How do I re-register my system with Red Hat Network (RHN)?"
https://access.redhat.com/kb/docs/DOC-8037

Practice Quiz

Red Hat Network Registration

1. The graphical tool that begins the registration with the Red Hat Network is SYS Admin RHN.

2. The first registration choice determines whether a system registers with _____ or _____.

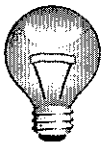
3. Optionally additional web proxy server and authentication information may need to be be provided.

4. An RHN username and its matching password must be provided for successful Red Hat Network registration.

5. The last questions to be answered during the registration process are _____ and whether to upload _____ and _____ profile information.

Install, Remove and Update Packages

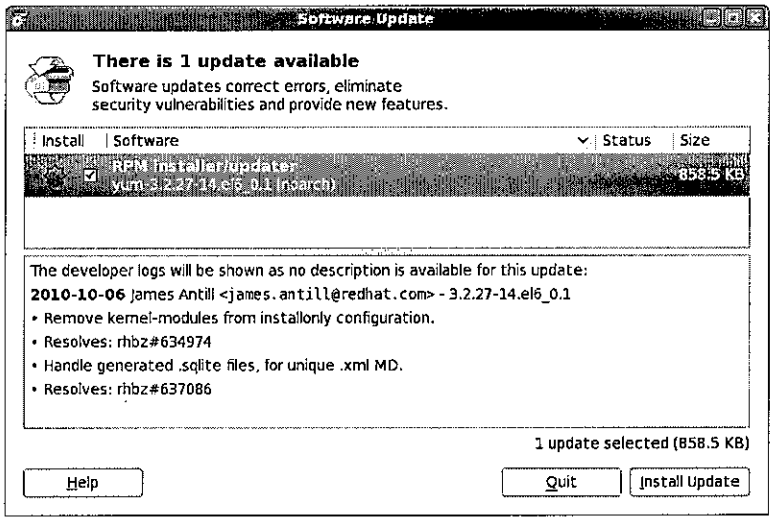
To install or remove system software, open the **Add/Remove Software** application (**System** → **Administration** → **Add/Remove Software**). Select **All packages** to manage individual packages, or select **Package collections** to manage package groups. Check the checkbox next to the package or group to install it. Uncheck the checkbox next to the package or group to remove it. Once you have made your selection(s), click the Apply button. If the package or groups requires other packages as a dependency, click the Install button to install the required dependencies.



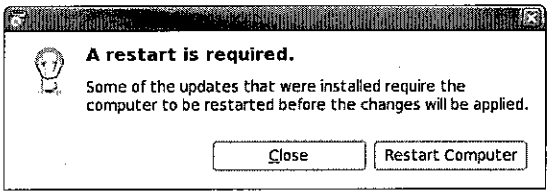
Important

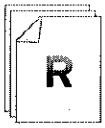
You cannot install and remove packages at the same time. As soon as you select a package to be installed, the checkboxes for installed packages will no longer be available for removal. If you want to install and remove packages, select all packages to be installed, then click Apply. Once that transaction has completed, deselect the packages to be removed and click Apply.

To update system software, launch the **Software Update** application (also known as **gpk-update-viewer**) by clicking on **System** → **Administration** → **Software Update**. All packages are marked to be updated, so deselect any updates that you do not want to install immediately and click the Install Update(s) button. Normally, the **Software Update** application will first install packages related to the application used to install packages (**yum**), so you may have to run the **Software Update** application several times in a row to apply all updates.



The system should be rebooted when the kernel has been updated or when certain major libraries have been updated (such as *glibc*). The **Software Update** application will ask you to reboot when this is the case.





References

Red Hat Enterprise Linux Deployment Guide

- Chapter 2: PackageKit

Note

Looking Ahead: The best command line tool to install, update, and remove software packages is **yum**(8). This course will look at **yum** in passing, with a detailed look at the tool in the next course, *Red Hat System Administration II*.

Practice Case Study

Software Management

Before you begin...

Reset the serverX virtual machine. Log into your desktopX workstation as **student** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reboot your virtual server and reset its storage back to the original state when it was first installed.

Perform the following steps on serverX unless directed otherwise.

You have a new server to administrate that has very specific software requirements. It must have the latest version of the following packages installed (including any dependencies):

xsane (new package)

gimp (new package)

yum (updated package)

samba-client (updated package)

For security reasons it should not have the **vsftpd** package installed. Delete

Do not install all updates. Only install updates for the packages listed above if they are available.

When you are ready to check your work, run the **Software Management Grading** script in the **Labs** folder on serverX.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Test

Criterion Test

Case Study

Update and Install Software

Before you begin...

Reset the serverX virtual machine. Log into your desktopX workstation as **student** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reboot your virtual server and reset its storage back to the original state when it was first installed.

Perform the following steps on serverX unless directed otherwise.

You have a new server, serverX, to administrate that has very specific software requirements. It must have the latest version of the following packages installed (including any dependencies):

kernel (existing package with an update)

xsane-gimp (new package)

yum (updated package)

bzip2 (updated package)

For security reasons it should not have the **festival** package installed.

Do not install all updates. Only install updates for the packages listed above if they are available.

When you are ready to check your work, run the **Software Management Test Grading** script in the **Labs** folder on serverX.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

Identify Installed Packages

In this section you learned how to:

- Identify individual packages installed on the system
- List all of the packages installed on the system

Register with Red Hat Network (RHN)

In this section you learned how to:

- Register a system with Red Hat Network

Install, Remove and Update Packages

In this section you learned how to:

- Install packages using a GUI tool
- Update packages on the system using a GUI tool
- Remove packages using a GUI tool

UNIT TEN

GET HELP IN A TEXTUAL ENVIRONMENT

Introduction

Topics covered in this unit:

- man reader
- Searching for keywords
- pinfo reader
- Additional package documentation

① local help : System → help
or we enter the App. ⇒ F1

Read Documentation Using man

Earlier in class we looked at various sources of documentation which are available to **yelp**, the **GNOME Help Browser**. We saw three; the Linux System Manual (man pages), GNU Info nodes, and GNOME graphical documentation. In a text-only environment, GNOME graphical documents are not easily available, but man pages and GNU Info nodes are. In this section, we will start by looking more closely at man pages.

As we mentioned earlier, the Linux Manual can be thought of as a single large book which is divided into sections or chapters. Each section contains man pages relevant to a particular type of information:

man 5 Passwd

Section	Types of man pages
1	User commands
2	Kernel system calls (entry points to the kernel from userspace)
3	Library functions
4	Special files and devices
5	File formats and conventions
6	Games
7	Conventions, standards, and miscellaneous pages
8	System administration commands
9	Linux kernel API (internal kernel calls)

Table 10.1. Sections of the *Linux Manual*

man 7 man

Note that section 9 of the manual is a relatively recent addition to Linux and not all the documentation on man sections discusses it.

As we mentioned earlier in this course, two sections of the manual may contain man pages that have the same name. In order to distinguish between the pages, written references to a man page usually add the section of the manual in parentheses after the name of the man page. The first example most system administrators run into is the difference between **passwd**(1) (on the command used to change passwords) and **passwd**(5) (on the format of the **/etc/passwd** file that stores local user information).

The command line tool to read man pages is **man *manpage***. The contents are displayed on the terminal a screen at a time, and can be scrolled through with arrow keys or the next screen displayed by typing **Space**. The **man** command searches through the manual sections in a specific order and displays the first match it finds; for example, **man passwd** will display **passwd**(1) by default. To ask for a man page from a specific section, you must give the section number as an argument on the command line: **man 5 passwd** will display **passwd**(5).

Navigating Man Pages

Knowing how to efficiently navigate and search a **man** page will save you enormous amounts of frustration and make you a much more effective Linux user. The following table lists some basic navigation commands for **man**:

Command	Result
Space	Scroll forward one screen
DnArrow	Scroll forward one line
UpArrow	Scroll back one line
/string	Search forward for *string* in the man page
n	Repeat previous search forward in the man page
N	Repeat previous search backward in the man page
q	Exit **man** and return to the prompt

Table 10.2. Navigating **man** Pages

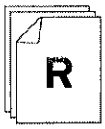
Warning

When performing searches, the string uses *regular expression* syntax. While simple text (such as *passwd*) works as expected, regular expresssions use metacharacters (such as *$*, *, ., and ^) for more sophistacated pattern matching. A search for *make $$$* might yield unexpected results.

Regular expressions are discussed in *Red Hat System Administration II*, and in **regex**(7).

Later in this class you will learn about a command called **less**, which is used for displaying and navigating large amounts of text one screen at a time and uses the same commands for moving and searching. This similarity is not coincidental. In fact, when you view a man page with **man**, it uses **less** to display the page.

Use this space for notes



References

man(1), **intro**(1), **man-pages**(7), and **less**(1) man pages

Practice Performance Checklist

Using man

- ☐ Consult the **man** page for **gedit**(1).
- ☐ Identify how to edit a specific file using **gedit** from the command line.
- ☐ Determine the option you specify to cause **gedit** to begin the editing session with the cursor at the end of the file.
- ☐ Consult the **man** page for **su**(1).
- ☐ Determine what **su** does when the username argument is omitted.
- ☐ Identify how **su** behaves when a dash option by itself is specified.
- ☐ Consult the **man** page for **passwd**(1). Determine the options that will lock and unlock a user account when this command is used by **root**.
- ☐ Locate the two principles to remember according to the **passwd man** page authors. Search for the word **principle**.
- ☐ Consult the man-page documenting the syntax of the **/etc/passwd** file. What is stored in the third field of each line?

Identify Relevant Man Pages by Keyword

A keyword search of man pages can be performed using **man -k** ***keyword***, which results in a list of relevant man pages, including chapters.

```
[student@stationX ~]$ man -k passwd
checkPasswdAccess (3) - query the SELinux policy database in the kernel.
chpasswd (8)          - update passwords in batch mode
ckpasswd (8)          - nnrpd password authenticator
fgetpwent_r (3)       - get passwd file entry reentrantly
getpwent_r (3)        - get passwd file entry reentrantly
...
passwd (1)            - update user's authentication tokens
sslpasswd (1ssl)      - compute password hashes
passwd (5)            - password file
passwd.nntp (5)       - Passwords for connecting to remote NNTP servers
passwd2des (3)        - RFS password encryption
...
```

Remember that programmers also use man pages, so system administrators generally focus on entries from sections 1 (user commands), 5 (file formats), and 8 (administrative commands).

makewhat is => to update in another time, year el matlub beta3o
whatis = <- man -f passwd
man -k enter ->

Passwd فيها كلمة
Keyword بيدور على
& description

Note

Keyword searches rely on a database generated with the **makewhatis** command, which must be run as root. Generally, this command runs automatically about an hour after the first boot and is updated daily thereafter. Newly installed documentation may not be immediately accessible until **makewhatis** is run either automatically or manually.

Use this space for notes

References

man(1) man page

Practice Quiz

1. Which command will list detailed information about a zip archive? zipinfo

2. Which man page contains a list of parameters that can be passed to the kernel at boot time? bootparam

3. Which command is used to tune ext4 file system parameters? tune2fs

Read Documentation Using pinfo

Software developed as part of the GNU Project uses the Info system for much of its documentation, as we have previously seen. Remember that Info documentation is generally provided in the form of books which are made up of hyperlinked *Info nodes*. This format is more flexible than man pages, allowing more thorough discussion of complex commands and concepts. In some cases, both a man page and Info documentation exist for a command; most of the time, the Info documentation will be more in-depth in this case. For example, compare **man tar** with **pinfo tar**.

Like man pages, Info nodes can also be read from a text-only terminal. The **pinfo** command is an Info reader that is relatively easy to use. The Info nodes for a particular topic can be browsed with **pinfo *topic***, and just running **pinfo** provides an index to all Info topics. (Another Info reader on the system is **info**, which has a slightly different interface.)

Man Page vs. Info Page Navigation

Fill in the table below as your instructor presents this material. (Also see the Info nodes for **info** for review.)

Key Binding	**man** Navigation	**pinfo** Navigation
PgDn / PgUp	Read the next/previous page	
/	Search for a pattern	
q	Quit reading the documentation	
DownArrow / UpArrow	Scroll one line at a time	
n	Find the next occurrence of an earlier search	
p	N/A	
u	N/A	

Table 10.3. **man/pinfo** Comparison

References

info info (*Info: An Introduction*)

info pinfo (*pinfo*)

pinfo(1) and **info**(1) man pages

Practice Performance Checklist

Read Documentation Using pinfo

- ☐ Invoke **pinfo** without any arguments.
- ☐ Navigate to the topic **Common options** and go to that **info** page.
- ☐ Skim through this **info** page and find out if long options can be abbreviated.
- ☐ Determine what **--** by itself means as an argument to a command.
- ☐ Without exiting **pinfo**, go up a level to the **GNU Coreutils** page.
- ☐ Go up another level to the top level page.
- ☐ Search for the pattern **nano** and enter that topic.
- ☐ Locate the topic in the **Introduction** entitled **Command line options** and skim it very quickly.
- ☐ Go up to the **Introduction** level then skip to the next topic.
- ☐ Exit **pinfo**.
- ☐ Invoke **pinfo** and specify **nano** as your topic/command of interest on the command line.
- ☐ Select the **Editor Basics** topic.
- ☐ Read the **Entering Text** and **Special Functions** subtopics.

Documentation in /usr/share/doc

By convention, most other documentation is found in the **/usr/share/doc** directory, in subdirectories named by RPM package. The **/usr/share/doc** directory is used to collect "everything else": If it's not a **man** page, not an **info** page, not part of the GNOME help utility, it's found here.

The documentation directory for the *zip* utility, for example, tells you the compression algorithm, and little else. Not much help to the administrator. The *samba-doc* directory, however, includes three large texts, including the complete text of *Samba-3 by Example*.

Note

Many applications have their documentation packaged in a separate RPM package, which may or may not be installed. Examples include the *bash-doc* and *samba-doc* packages. Often, these packages are found in Red Hat Enterprise Linux 6's *Optional* tree.

Use this space for notes

References

hier(7) man page

- Discusses what certain directories are used for, including **/usr/share/doc**

Practice Quiz

1. Where can you find the latest news about the vim package?

   Readme.txt → /usr/share/doc

   Which file contained this information?

2. What is the URI for the wiki for the yum package?

   wiki: http://yum.baseurl.org/wiki

   Which file contained this information?

   Readme.txt

3. What are the commands or utilities provided by the diffutils package?

   diff, diff3, sdiff, cmp.

Personal Notes

Unit Summary

Read Documentation Using **man**

In this section you learned how to:

- Answer questions about commands based on reading man pages

Identify Relevant Man Pages by Keyword

In this section you learned how to:

- Identify relevant man page articles based on **man -k** keyword searches

Read Documentation Using **pinfo**

In this section you learned how to:

- Answer questions from info page documentation

Documentation in **/usr/share/doc**

In this section you learned how to:

- Answer questions based on answers found in **/usr/share/doc** documentation

UNIT ELEVEN

ESTABLISH NETWORK CONNECTIVITY

Introduction

Topics covered in this unit:

① → Intro
② → Config
③ → test

- IPv4 concepts
- Linux network configuration
- Confirming network functionality

Essential Network Concepts

The *Internet Protocol*, or *IP*, is the protocol used to send network traffic between hosts across the Internet. It comes in two versions. *IPv4* is what most system administrators think of as "IP", in which 32-bit network addresses on variable sized networks are used to address hosts. The second version, *IPv6*, uses 128-bit network addresses to address hosts, and provides some other changes to the protocol. It is expected to see increasing use as it becomes harder to obtain new IPv4 networks.

IPv4 Networking Concepts

IP Address:

```
   172.17.5.3 = 10101100.00010001.00000101.00000011
```

Netmask:

```
  255.255.0.0 = 11111111.11111111.00000000.00000000

                10101100.00010001.00000101.00000011
                \_____________/   \_____________/
                   Network            Host
```

IP Address:

```
  192.168.5.3 = 11000000.10101000.00000101.00000011
```

Netmask:

```
255.255.255.0 = 11111111.11111111.11111111.00000000

                10101100.00010001.00000101.00000011
                \_____________________/   \_____/
                         Network            Host
```

An IPv4 address is a 32-bit number, normally expressed in decimal as four *octets* ranging in value from 0 to 255, separated by dots. The address is divided into two parts; the *network part* and the *host part*. All hosts on the same subnet, which can talk to each other directly without a router, have the same network part; the network part identifies the subnet. No two hosts on the same subnet can have the same host part; the host part identifies a particular host on a subnet.

In the modern Internet, the size of a subnet is variable. To know which part of an IPv4 address is the network part and which the host part, you must know the *netmask* which the network administrator has assigned to the subnet. The netmask indicates how many bits of the IPv4 address belong to the subnet. The more bits that are available for the host part, the more hosts can be on the subnet.

The lowest possible address on a subnet (host part is all zeros in binary) is sometimes called the *network address*. The highest possible address on a subnet (host part is all ones in binary) is used for broadcast messages in IPv4, and is called the *broadcast address*.

Network masks are expressed in two forms. The older syntax for a netmask which uses 24 bits for the network part would read *255.255.255.0*. A newer syntax called CIDR notation, would specify a *network prefix* of */24*. Both syntaxes convey the same information, namely, how many leading bits in the IP address contribute to its network address.

The examples below illustrate how the IP address, netmask (or prefix), network part, and host part are related.

Host Addr	192.168.1.107	**11000000.10101000.00000001.01101011**
Network Mask	255.255.255.0 ("/24")	**11111111.11111111.11111111.00000000**
Network Addr	192.168.1.0	**11000000.10101000.00000001.00000000**
Broadcast Addr	192.168.1.255	**11000000.10101000.00000001.11111111**

Table 11.1. Calculating the network address for 192.168.1.107/255.255.255.0

Host Addr	10.1.1.18	**00001010.00000001.00000001.00010010**
Network Mask	255.0.0.0 ("/8")	**11111111.00000000.00000000.00000000**
Network Addr	10.0.0.0	**00001010.00000000.00000000.00000000**
Broadcast Addr	10.255.255.255	**00001010.11111111.11111111.11111111**

Table 11.2. Calculating the network address for 10.1.1.18/255.0.0.0

Host Addr	172.168.181.23	**10101100.10101000.10110101.00010111**
Network Mask	255.255.224.0 ("/19")	**11111111.11111111.11100000.00000000**
Network Addr	172.168.160.0	**10101100.10101000.10100000.00000000**
Broadcast Addr	172.168.191.255	**10101100.10101000.10111111.11111111**

Table 11.3. Calculating the network address for 172.16.181.23/255.255.224.0

The special address 127.0.0.1 with the 255.0.0.0 netmask always points to the local system ("localhost"), so that it can talk to itself using network protocols.

Use this space for notes

IPv6 Networking Concepts

IPv6 Address:

```
2001:0db8:0000:0000:0215:58ff:fec4:c6fe =

0010000000000001:0000110110111000:0000000000000000:0000000000000000:
0000001000010101:0101100011111111:1111111011000100:1100011011111110

= 2001:0db8::215:58ff:fec4:c6fe (abbreviated form)
```

Netmask:

Normally 64 bits long (**/64**). Host part is therefore 64 bits long (128 - 64 = 64).
Usually not written as `ffff:ffff:ffff:ffff:0000:0000:0000:0000`

Network:

```
2001:0db8:0000:0000:: =
0010000000000001:0000110110111000:0000000000000000:0000000000000000
```

Host:

```
::0215:58ff:fec4:c6fe =
0000001000010101:0101100011111111:1111111011000100:1100011011111110
```

An IPv6 address is a 128-bit number, expressed as eight colon-separated groups of four hexadecimal digits (ranging from 0000 to ffff). The address is divided into a network part and a host part, but the prefix is *always* assumed to be **/64**; therefore the network part is the first four groups and the host part is the last four groups. (An organization might be assigned a "/48" network, giving it the ability to have up to 65535 subnets, for example.)

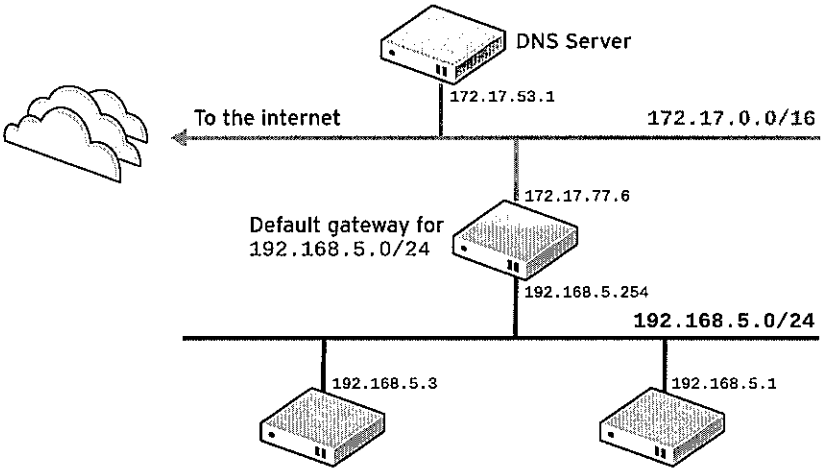
Because IPv6 addresses can be long, there are a couple of rules that can be used to condense them in use:

- In any group, leading zeros can be suppressed: **`:0db8:`** can be written **`:db8:`** and **`:0000:`** can be written **`:0:`**.
- Only once in the address, one run of consecutive zeros can be replaced with **`::`**. For example, **`2001:db8:0:0:0:0:0:1`** is better written as **`2001:db8::1`** and **`0:0:0:0:0:0:0:1`** is better written as **`::1`**

IPv6 does not have a broadcast address, but machines normally have a number of special multicast addresses that are used only to talk to hosts on the local link. The special unicast address ::1 is the IPv6 version of the 127.0.0.1 "localhost" address.

Use this space for notes

Network Routing and DNS Concepts



Whether using IPv4 or IPv6, network traffic needs to move from host to host and network to network. Each host has a *routing table* which tells it which network interfaces to use to communicate to the subnets to which it is attached directly. If the network traffic is not addressed to one of these subnets, the routing table usually has an entry for all other networks that points to a *router* or *gateway* on a reachable subnet.

If a router recieves traffic which is not addressed to it, instead of ignoring it, it *forwards* the traffic based on its own routing table. This may send the traffic directly to the destination host (if the router happens to be on the destination's subnet), or it may be forwarded on to another router. This process of forwarding continues until the traffic reaches its final destination.

The IP protocol uses addresses to communicate, but human beings would rather work with names than long and hard to remember strings of numbers. *DNS*, the Domain Name System, is a distributed network of servers that map hostnames to IP addresses. In order for name service to work, the host needs to be pointed at a *nameserver*. This nameserver does not need to be on the same subnet, it just needs to be reachable by the host.

Use this space for notes

References

Red Hat Enterprise Linux Deployment Guide

- Chapter 5: Network Configuration

Practice Group Exercise

Essential Network Concepts

Are the following network configurations feasible? If not, what is wrong with them?

1. Scenario 1

```
IP address: 192.168.7.351
Netmask: 255.255.255.0
Gateway: 192.168.7.1
```

2. Scenario 2

```
IP address: 10.1.2.3
Netmask: 255.255.255.0
Gateway: 10.1.2.1
DNS server: 172.17.4.53
```

3. Scenario 3

```
IP address: 192.168.7.0
Netmask: 255.255.255.0
Gateway: 192.168.7.1
DNS server: 192.168.0.254
```

4. Scenario 4

```
IP address: 10.4.5.6
Netmask: 255.255.255.0
Gateway: 10.4.6.1
DNS server: 192.168.0.254
```

5. Scenario 5

```
IP address: 172.17.23.5
Netmask: 255.255.0.0
Gateway: 172.17.0.1
DNS server: 192.168.0.254
```

6. Scenario 6

```
IP address: 2001:db8::219:a0ff:fe26:a221
Prefix: /64
Gateway: 2001:db8::fe
DNS server: 2001:db8:0:1::1
```

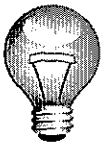
Linux Network Configuration

The easiest way to configure networking in Red Hat Enterprise Linux is to use the **NetworkManager** application. It can set system-wide defaults that affect all users, or it can be configured to activate certain network interfaces (perhaps connected to VPN tunnels) only when particular users are logged in.

Steps for configuring an IPv4 network interface:

1. Right click the **NetworkManager** applet and select **Edit Connections...**
2. Click **Add** or select a profile and click **Edit...** button
3. Make sure **Connect automatically** is checked so that the interface comes up immediately
4. Also make sure **Available to all users** is checked so that the interface comes up for all users at boot and is not just up when the current user is logged in
5. Select **IPv4 Settings** tab
6. Select method as **Automatic (DHCP)** or **Manual**
7. With **Manual**, click **Add** and specify the IPv4 address, netmask, gateway, and DNS servers
8. Click **Apply**

Configuring IPv6 is similar, except that for step 6 there are three main options: **Automatic, DHCP only**; **Automatic**; and **Manual**. The difference between the two automatic modes is that the first only uses DHCPv6 to get IPv6 addresses, while the second will try DHCPv6 or will find out what network it is on from the router and autoconfigure the host part of its address from the MAC address of its Ethernet card.



Important

Advanced Students: If **Available to all users** is checked for a network interface in **NetworkManager**, the normal network configuration files in **`/etc/sysconfig/network-scripts`** are updated and store the configuration settings.

References

Red Hat Enterprise Linux Deployment Guide

- Chapter 5: Network Configuration

Practice Performance Checklist

Linux Network Configuration

Use **`NetworkManager`** to create a static network configuration profile for your serverX machine:

- ☐ Create a network connection called **`Wired static`**.
- ☐ Ensure that the connection will start automatically at boot.
- ☐ Define static IPv4 settings with an IP address of 192.168.0.X+100.
- ☐ Defined the netmask as 255.255.255.0.
- ☐ Set the default gateway to 192.168.0.254.
- ☐ Define the DNS server as 192.168.0.254.

Confirming Network Functionality

In this section, the instructor will discuss and demonstrate a number of commands that are useful for troubleshooting networking issues: **ip route** for viewing the routing table, **host** for testing DNS name resolution, and **ping** for testing network connectivity.

Display current routing table:

```
[student@serverX ~]$ ip route
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.1  metric 1
default via 192.168.0.1 dev eth0  proto static
```

This shows us that we have a direct route to hosts on 192.168.0.0/24 out eth0, and our source IP address is 192.168.0.1. Packets to hosts on other networks will be sent to the router at 192.168.0.1 which can be reached through eth0.

dig = host

mtr → my traceroute

Confirm DNS operation:

```
[student@serverX ~]$ host instructor
instructor.example.com has address 192.168.0.254
[student@serverX ~]$ host instructor.example.com
instructor.example.com has address 192.168.0.254
[student@serverX ~]$ host 192.168.0.254
254.0.168.192.in-addr.arpa domain name pointer instructor.example.com.
```

Confirm connectivity:

```
[student@serverX ~]$ ping instructor.example.com
[student@serverX ~]$ ping 192.168.0.254
```

Use this space for notes

References

Red Hat Enterprise Linux Deployment Guide

- Section 5.2: Interacting with NetworkManager

Practice Performance Checklist

Confirming Network Functionality

- ☐ Switch workstations with another student.
- ☐ Evaluate their serverX machine to make sure it is functioning correctly on the network.

Test

Criterion Test

Case Study

Weekend Network Adjustment

Before you begin...

Although most of the work is done on your serverX machine, execute the **`lab-setup-netconfig`** script on desktopX before beginning the criterion test.

The network administrator spent last weekend making changes to the office network. Somehow the memorandum notifying the network users of the changes didn't get published before the changes were made.

Configure your Linux server to communicate with the new network configuration.

When you have fulfilled the requirements, run **`lab-grade-netconfig`** on serverX to check your work.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

Essential Network Concepts

In this section you learned how to:

- Identify valid IPv4 and IPv6 addresses
- Identify the host and network part of a specified IP address
- Describe the process of packet transmission within the local network and through the default gateway

Linux Network Configuration

In this section you learned how to:

- Configure the NIC statically and dynamically using NetworkManager
- Configure the server to use DNS to resolve host names

Confirming Network Functionality

In this section you learned how to:

- Determine if the system is connected to the network and what its IP address and network mask are
- Examine the server's route table
- Confirm the server is resolving host names using DNS
- Confirm the server is communicating with a remote host using ping

UNIT TWELVE

ADMINISTER USERS AND GROUPS

Introduction

Topics covered in this unit:

- Creating, and Deleting Users
- Disabling User Accounts
- Creating and Deleting Groups
- Changing Group Memberships
- Managing Password Aging Policies

User and Group Administration

Management of user and group accounts is an important system administration task. In this section we will look at a graphical tool, **User Manager** (also known as **`system-config-users`**) which can be used to manually administer local user accounts.

Among the tasks that the class will investigate will be how to

- Create and delete local user and group accounts
- Assign local users to local groups
- Lock and unlock access to a local user account
- Require a password change after a set number of days
- Have a local user account expire on a certain date

In a standard classroom, this will be explored as a group activity. One student in each group will work through these tasks at a computer while the other members observe and take notes on the correct procedure. (In a virtual training classroom, this will be an individual activity.) At the end of the section, the instructor will review the answers. (Note also that correct answers are included in the Solutions appendix at the back of your book.)

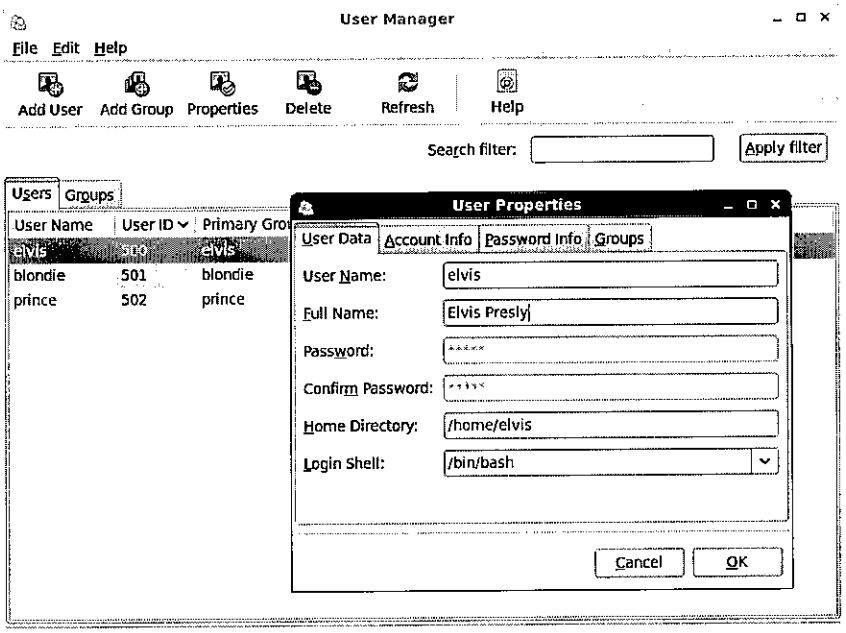


Figure 12.1. The "Users and Groups" adminstration tool

User and Group Administration Group Project

Write down the steps to complete the following tasks.

1. Example: How do you access the Users and Groups management utility?

   - Select the **System** → **Administration** → **Users and Groups** menu item from the GNOME desktop menus.

2. Example: How do you create a new user account?
   - Open the **Users and Groups** management utility.
   - Click on the **Add User** button.
   - Fill in the **User Name**, **Full Name**, and **Password** fields, then click **OK**
3. How do you change a user's password?

   Use this space for notes

4. How do you adjust a user's password aging attributes?

   Use this space for notes

5. How do you lock and unlock a user account?

   Use this space for notes

6. How do you change a user's group affiliation?

   Use this space for notes

7. How do you delete a user account?

   Use this space for notes

8. How do you create a new group?

   Use this space for notes

9. How do you delete a group?

   Use this space for notes

References

Red Hat Enterprise Linux Deployment Guide

- Chapter 15: Users and Groups

Note

Looking Ahead: Users and groups can be managed from the command line using a suite of commands called **useradd**(8), **usermod**(8), and **userdel**(8), and **groupadd**(8), **groupmod**(8), and **groupdel**(8), among others. These commands are covered in detail in the *Red Hat System Administration II* course.

Practice Performance Checklist

User and Group Administration

Perform the following steps on serverX unless directed otherwise.

- ☐ Create a user account with the following attributes:

  User name = **`practice`**

  Full name = **`Joe Practice`**

  Password = **`practice`**

- ☐ Create a user account with the following attributes:

  User name = **`baduser`**

  Full name = **`Bad User`**

  Password = **`baduser`**

- ☐ Create a supplementary group called **`pgroup`** with a group ID of **`30000`**.

- ☐ Create a supplementary group called **`badgroup`**.

- ☐ Add the **`practice`** user to the **`pgroup`** group as a supplementary group.

- ☐ Modify the password for student to **`password`**.

- ☐ Modify student's account so the password expires after 30 days.

- ☐ Lock the **`practice`** user account so they cannot log in.

- ☐ Delete the user called **`baduser`**.

- ☐ Delete the supplementary group called **`badgroup`**.

Test

Criterion Test

Case Study

Administer Users and Groups

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise.

Perform the following steps on serverX unless directed otherwise.

A team of consultants have been hired to work on a project. Create user accounts for each consultant and add them to a group called **`consultants`** as a supplementary group with a group ID of **`40000`**.

Their accounts should expire when their contract ends in 90 days and their passwords should have to be changed every month.

The following is the list of consultants with their user names (and they should all have an initial password of **`default`**):

- Sam Spade = sspade
- Betty Boop = bboop
- Dick Tracy = dtracy

When you finish, run the **`lab-grade-newusers`** evaluation script to confirm you have done everything correctly.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

User and Group Administration

In this section you learned how to:

- Create a new student account according to predefined specifications
- Grant or deny access to a specified user account
- Delete an existing user account
- Create a new supplementary group with a specific group ID
- Delete an existing group
- Change the supplementary group assignment for a user account
- Change a user's password to a specified string
- Change the password expiration of a user account to a fixed age in days or have the account expire on a set date

UNIT THIRTEEN

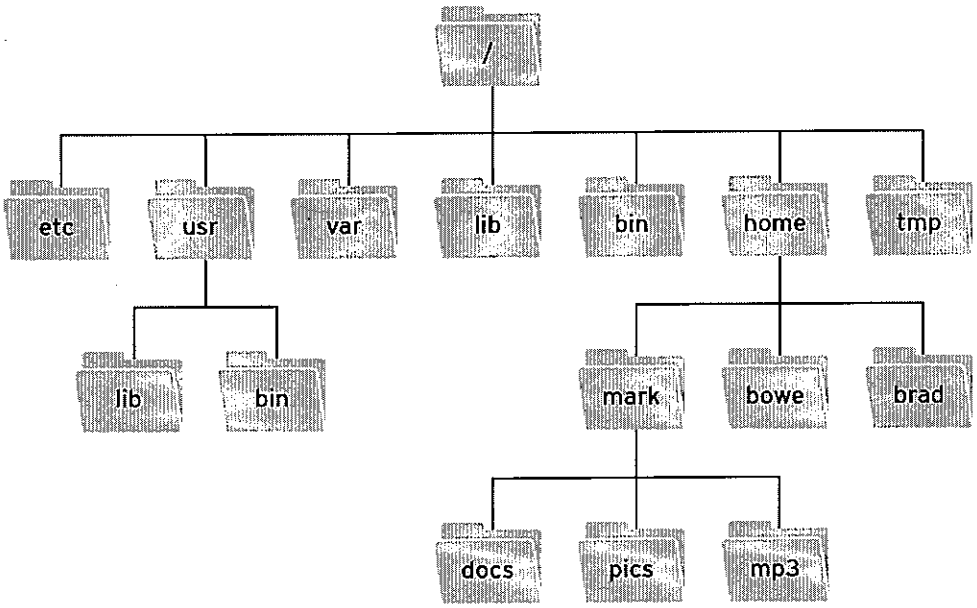
MANAGE FILES FROM THE COMMAND LINE

Introduction

Topics covered in this unit:

- Linux file system hierarchy
- Absolute path names
- File/directory management commands
- Relative path names

The Linux File System Hierarchy



In Linux and UNIX-like operating systems, file systems are organized into a *hierarchy*, organized like an inverted tree. The root of the tree is the / directory. As we saw in an earlier unit, file systems are *mounted* on an empty directory. That means that the top level of a file system is treated as if it were the contents of some directory in the file system hierarchy.

To specify the location of a file on the system, we can specify the *absolute path* to that file from the root of the tree through its subdirectories to the file. On Linux, the / character is the directory separator in the path. So, for example, **/bin** is the **bin** file or directory in /. Or, for another example, the file **/home/bowe/file.txt** is the **file.txt** file in the **bowe** subdirectory of the **home** directory, which is in /.

Comparison

Linux uses the forward slash (/) to separate directories in the path name, as opposed to the back slash (\) used in DOS and Windows.

Remember that a directory in Linux is equivalent to a folder in Windows.

Each directory in the file system has a standardized use specified, which is documented by the **hier**(7) man page and by the *Filesystem Hierarchy Standard* (see the References below).

Most configuration files are stored in the **/etc** directory and its subdirectories.

The **/var** directory contains regularly-changing system files such as logs, print spools and email spools.

Executables, or commands, are kept in **/usr/bin** or **/bin** to be accessible by all users. Some administrative commands may be kept in **/usr/sbin** or **/sbin**.

Every user has a home directory. All of the user's personal files (configuration, data, or even applications) go here. Root's home directory is **/root**. Most non-root home directories are in the **/home** tree, usually named after the user.

Note

The root user's home directory is called **/root**, yet the / directory is called the "root directory" since it is at the root of the file system hierarchy. This is a possible source of confusion. (At one time, some UNIX-like systems actually used / as the root user's home directory, further confusing matters.)

/tmp is usually used by applications for storing temporary data. Once a day the system automatically deletes any files over ten days old in **/tmp**.

The boot loader is in charge of loading the core of Red Hat Enterprise Linux, called the kernel, into memory. The boot loader, kernel and loader's configuration files, are stored in **/boot**.

One fundamental principle of Linux and UNIX-like systems is that "everything is a file", including hardware devices. This enables some very powerful things to be done with simple tools. In any case, there are special files and the system which represent hardware devices, which are kept in the **/dev** directory and its subdirectories.

When removable media is loaded the file system on the media is mounted into a subdirectory of **/media**. For example, a CD-ROM might be mounted on **/media/CDROM**, and you could access that directory whenever you wanted to read a file from the CD-ROM. If the removable media has a file system label, that label is often used as the name of the mount point in **/media**.

References

hier(7) man page

Filesystem Hierarchy Standard
http://www.pathname.com/fhs

cd ../../var = cd /var

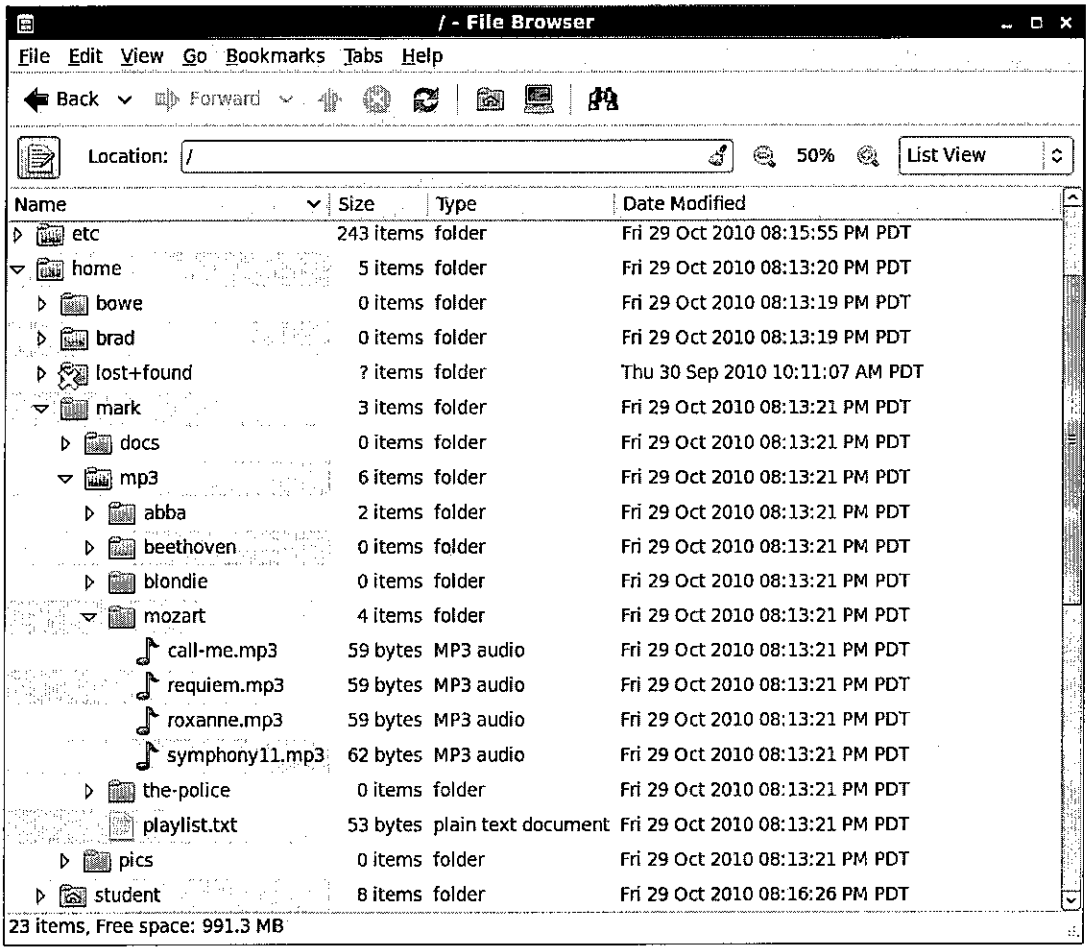
Practice Quiz

Linux File System Hierarchy

1. /etc contains most of the system configuration files.
2. / is the root directory.
3. User home directories are found below /home but root's home directory is /root.
4. The /var directory contains variable data like web sites and FTP sites.
5. Temporary files are stored in /tmp and /var/tmp.
6. Removable devices are normally mounted on /media.
7. Device files are kept in /dev.
8. Files used during the boot process are stored in /boot.

Navigate with Absolute Path Names

The screenshot below shows a partial view of the file system hierarchy, starting from /, in **Nautilus**. Look in particular at the MP3 files in the home directory of user **mark**.



An absolute path name always begins with a forward slash (/), identifying the complete file name starting from the root directory, through any intervening directories, to the name of the file. An absolute path name represents a unique name for a file on the file system. Path names can be used as arguments to any command that takes a file name argument.

So, in the screenshot above, the absolute path to the **`call-me.mp3`** file in the home directory of user **`mark`** is **`/home/mark/mozart/call-me.mp3`**.

Use this space for notes

Two special path names are ~, which is an abbreviation for the absolute path name for the current user's home directory; and **~user**, which abbreviates the absolute path name for the home directory of **user**.

Note

Both special path names are interpreted by the shell through a mechanism called *tilde expansion*.

When working from the command line, the shell keeps track of your *current working directory*. This affects which folder it thinks you are currently working in. The **ls** command with no arguments lists the files in your current working directory, which **pwd** prints the absolute path to your current working directory. You can change your current working directory with **cd**.

The following table compares and contrasts these shell commands with operations in the graphical **Nautilus** file manager:

Graphical Navigation	Command Line Equivalent
Click from folder to folder to move around.	**cd** [*directory*] When *directory* is omitted, **cd** returns to the home directory.
Open a folder to view its contents.	**ls** [*directory*] When *directory* is omitted, **ls** lists the current directory you are in.
List of folders in the **Location** bar.	**pwd** This command displays the current working directory.
Have a window in focus.	Current working directory.

Table 13.1. Graphical Versus Command Line Navigation Comparison

References

info libc (*GNU C Library Reference Manual*)

- Section 11.2.2: File Name Resolution

pwd(1), **cd**(1), **ls**(1), and **bash**(1) man pages

Practice Quiz

Navigating with Absolute Path Names

Use the **nautilus** screenshot from this section to answer the following questions.

1. What command would make Brad's home directory your current directory?

   cd

2. What command would change your current directory back to your (student's) home directory?

   cd ~

3. How would you display the list of files in the current directory?

   ls

4. What command would you use to list the pictures in Mark's **pics** folder?

   ls ~/home/pics

5. You are in Brad's home directory. How would you list the files in your own home directory with the fewest keystrokes?

   ls

6. You are not sure where your current directory is. What command would display your current location?

7. What single command would you use to list the files in both the **abba** and **blondie** directories?

   ls /home/abba /home/blondie

8. What is the absolute path name to the **playlist.txt** file?

9. There is a file called **`requiem.mp3`** inside the **`mozart`** folder. What is that file's absolute path name?

_____

10. BONUS: There is a directory called **`Desktop`** inside student's home directory. What is the absolute path name to **`Desktop`**?

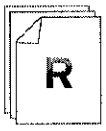
_____

Command Line File Management

In this section, the class will break into small groups and investigate the following shell file management commands. After five minutes, the groups will reassemble and each group will explain what the commands do and how to use them from the command line.

Command Reading Exercise

1. Team 1:
   - **cp**
   - **ln -s**
   - **mv**
2. Team 2:
   - **rm [-rf]**
   - **touch**
3. Team 3:
   - **mkdir**
   - **rmdir**



References

cp(1), **ln**(1), **mv**(1), **rm**(1), **touch**(1), **mkdir**(1), and **rmdir**(1) man pages

Practice Performance Checklist

Manage Files with Absolute Path Names

Before you begin...

These tasks require some existing files.

Log in as **root** on serverX and run **lab-setup-filemgmt**.

Do all of your work from the command line, do not use Nautilus to manage your files.

Note

Use absolute path names for every filename argument when performing the following tasks.

Perform the following steps on serverX unless directed otherwise.

- ☐ Log in as **student** on serverX.
- ☐ Create a folder called **bowe-labs** in your home directory.
- ☐ Copy all of the files from the chemistry folder in Bowe's home directory to your **bowe-labs** directory.
- ☐ Log in as **mark** on serverX (password is **password**).
- ☐ Sort some of his music collection. Move the **call-me.mp3** and the **roxanne.mp3** files from the **mozart** folder into the **blondie** and the **the-police** folders respectively.
- ☐ Remove his **playlist.txt** file from the **mp3** folder.
- ☐ When you have completed all of the tasks, login as **root** on serverX and run the **lab-grade-filemgmt-1** script.

Save Typing with Relative Path Names

Absolute vs. Relative Path Names

Fill in the below table as discussed with your instructor:

Absolute Path Names	Relative Path Names
Path name begins with a slash (/).	
Uses slashes to separate directories in the path name.	Same as absolute path name.
Linux begins searching at the root (/) directory for the file.	
Does not change unless the file is moved.	
Special absolute path names: • ~ = your home directory • ~*user* = *user*'s home directory	Special relative path names: • . = your current working directory • .. = the parent of your current working directory (../.. is two levels left, or up)

Table 13.2. Absolute Versus Relative Path Name Comparison

Example Path Names

1. How would you move the **call-me.mp3** file from the **mozart** folder to the **blondie** folder using absolute path names?

2. How would this command look if Mark used relative path names if he was in his home directory?

3. If Mark was going to do a lot of organizing, it might be easier to move to where the files are before moving them. What commands would Mark use in this case?

Relative Path Name Applications: Gather vs. Scatter

The goal of gathering is to collect files from different locations into a single place. When the source files are in close proximity, you could **cd** in to a directory close to them and use relative path names to copy them in to the target directory. When the source files are all over the file system, you could **cd** in to the target directory and use absolute and relative path names to copy them in to the current directory (.).

The goal of scattering is to distribute files in a single directory to various locations throughout the file system. You could **cd** to the directory with all of the files and copy or move them to their final destinations.

Wildcards

Wildcards can be used in directory or file name references. The asterisk (*) is used to match zero or more characters. Thus **ls d*** would match all of the following names:

```
d
d.txt
desktop
driver
...
```

...but it would not match **ad.txt** or **Desktop**.

ls h*t.txt would match:

```
hat.txt
hot.txt
history-text.txt
...
```

Which of the following would **ls *txt*** match?

```
my-files.txt
I-love-to-txt.doc
textingisfun.html
asdftxtasdf.jpg
```

All but **textingisfun.html** would match.

References

info libc (*GNU C Library Reference Manual*)

- Section 11.2.2: File Name Resolution

path_resolution(7), **pwd**(1), **cd**(1), **ls**(1), and **bash**(1) man pages

Practice Performance Checklist

Save Typing with Relative Path Names

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise. Subsequently, run **`lab-setup-filemgmt`** on serverX to create user accounts and files needed for the lab.

- ☐ Log in as **`student`** on serverX.
- ☐ Create a folder called **`bowe-labs`** in your home directory.
- ☐ Copy all of the files from the chemistry folder in Bowe's home directory to your **`bowe-labs`** directory.
- ☐ Log in as **`mark`** on serverX (password is **`password`**).
- ☐ Sort some of his music collection. Move the **`call-me.mp3`** and the **`roxanne.mp3`** files from the **`mozart`** folder into the **`blondie`** and the **`the-police`** folders respectively.
- ☐ Change into Mark's home directory.
- ☐ Use a relative path name to remove his **`playlist.txt`** file from the **`mp3`** folder.
- ☐ When you have completed all of the tasks, login as **`root`** on serverX and run the **`lab-grade-filemgmt-2`** script.
- ☐ Bonus:

  Log in as **`student`** on serverX and create a directory called **`marks-music`**.
- ☐ With a single command, copy all of Mark's individual mp3 files into the **`marks-music`** folder.

  Hint: Shell wildcards can help you accomplish this task.

Test

Criterion Test

Case Study

Organizing Brad's Photo Collection

Before you begin...

If you have not previously done so, run **lab-setup-filemgmt** on serverX to create user accounts and files needed for the criterion test.

Brad has been busy taking digital pictures. He works at Red Hat and has pictures from work He has pictures of his wife Jenny. He also has pictures of some famous cities he has visited.

He downloaded all of his pictures into a folder called **camera** below his home directory, but he needs your help sorting through them and organizing them into the appropriate folders below the **photos** directory below his home directory.

Login as **brad** on serverX (password is **password**) and organize his photos into the following subdirectories below **photos**:

- **family** - this folder is reserved for pictures of Jenny
- **places** - Brad's tourist photos belong here
- **work** - his Red Hat photos should go here

Some of the photos Brad took have **bad** in their name. Delete these pictures from the collection.

Finally, create a symbolic link to the **family** folder called **jenny**. This link should exist in Brad's **photos** folder.

When you finish, login as **root** on serverX and run the **lab-grade-filemgmt-3** script.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

The Linux File System Hierarchy

In this section you learned how to:

- Identify the purpose for the top level directories in the Linux hierarchy

Navigate with Absolute Path Names

In this section you learned how to:

- Use absolute path names to correctly select files and directories
- Change your current working directory
- Use **pwd** to identify the path name of their current working directory
- Use **ls** to list files in various directories

Command Line File Management

In this section you learned how to:

- Copy files using the **cp** command
- Link files using the **ln -s** command.
- Use **mv** to rename and move files in various directories
- Delete files using **rm**
- Create directories using **mkdir**
- Delete empty directories using **rmdir**
- Update file timestamps using the **touch** utility

Save Typing with Relative Path Names

In this section you learned how to:

- Use relative path names to correctly select files and directories

UNIT FOURTEEN

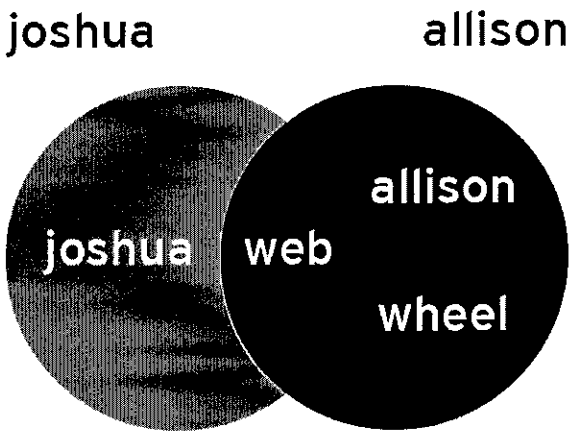
SECURE LINUX FILE ACCESS

Introduction

Topics covered in this unit:

- User/Group/Other (UGO) security scheme
- Nautilus file security
- Command line file security

User, Group, Other (UGO) Concepts



Access to files by users are controlled by *file permissions*. The Linux file permissions system is simple but flexible, which makes it easy to understand and apply yet able to handle most normal permission cases easily.

Files have just three categories of user to which permissions apply. The file is owned by a *user*, normally the one who created the file. The file is also owned by a single *group*, usually the primary group of the user who created the file, but this can be changed. Different permissions can be set for the owning user, the owning group, and for all *other* users on the system that are not the user or a member of the owning group.

The most specific permissions apply. So, *user* permissions override *group* permissions, which override *other* permissions.

There are also just three categories of permissions which apply: *read*, *write*, and *executable*. These permissions affect access to files and directories as follows:

Permission	Effect on Files	Effect on Directories
r (read)	Contents of the file can be read	Contents of the directory (file names) can be listed
w (write)	Contents of the file can be changed	Any file in the directory may be created or deleted
x (exec)	Files can be executed as commands	Contents of the directory can be accessed (dependent on the permissions of the files in the directory)

Table 14.1. Effects of permissions on files and directories

Note that users normally have both **read** and **exec** on read-only directories, so that they can list the directory and access its contents. If a user only has **read** access on a directory, the names of the files in it can be listed, but no other information including permissions or time stamps are available, nor can they be accessed. If a user only has **exec** access on a directory, they can not list the names of the files in the directory, but if they already know the name of a file which they have permission to read, then they can access the contents of that file by specifying the file name explicitly.

A file may be removed by anyone who has write permission to the directory in which the file resides regardless of the ownership or permissions on the file itself. (This can be overridden with a special permission, the *sticky bit*, which we will discuss at the end of the unit.

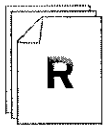
Comparison

Unlike NTFS permissions, Linux permissions only apply to the directory or file that they are set on. Permissions on a directory are not inherited automatically by the subdirectories and files within it. (The permissions on a directory *may* effectively block access to its contents, however.) All permissions in Linux are set directly on each file or directory.

The **read** permission on a directory in Linux is roughly equivalent to **List folder contents** in Windows.

The **write** permission on a directory in Linux is equivalent to **Modify** in Windows; it implies the ability to delete files and subdirectories. In Linux, if **write** and the **sticky bit** are both set on a directory, then only the user that owns a file or subdirectory in the directory may delete it, which is close to the behavior of the Windows **Write** permission.

Root has the equivalent of the Windows **Full Control** permission on all files in Linux. However, root may still have access restricted by the system's SELinux policy and the security context of the process and files in question. SELinux will be discussed at the end of this course.



References

`info coreutils` (*GNU Coreutils*)

- Section 13: Changing file attributes

Practice Quiz

Linux User, Group, Other Concepts

Answer the True/False questions based on the following user and file configurations.

```
Users and their groups:
    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   .rfile2
```

Questions regarding the **lfile1** file.

1. **lucy** can change the contents of **lfile1**.

   (select one of the following...)
   a. True
   b. False

2. **fred** can change the contents of **lfile1**.

   (select one of the following...)
   a. True
   b. False ✓

3. **fred** can delete **lfile1**.

   (select one of the following...)
   a. True
   b. False ✓

4. **ricky** can change the contents of **lfile1**.

   (select one of the following...)
   a. True
   b. False ✓

5. **ricky** can delete **lfile1**.

   (select one of the following...)
   a. True ✓
   b. False

```
Users and their groups:
    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **`lfile2`** file.

1. **`ricky`** can view the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

2. **`ricky`** can change the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

3. **`ricky`** can delete **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

4. **`ethel`** can view the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

5. **`ethel`** can change the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

```
Users and their groups:

    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **rfile1** file.

1. **lucy** can view the contents of **rfile1**.

   (select one of the following...)
   a. True ✓
   b. False

2. **lucy** can change the contents of **rfile1**.

   (select one of the following...)
   a. True ✓
   b. False

3. **fred** can view the contents of **rfile1**.

   (select one of the following...)
   a. True
   b. False

4. **fred** can change the contents of **rfile1**.

   (select one of the following...)
   a. True
   b. False

```
Users and their groups:

    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **rfile2** file.

1. **lucy** can view the contents of **rfile2**. lucy member the grp ricardo so false real

   (select one of the following...)
   a. True ✓
   b. False

2. **lucy** can change the contents of **rfile2**.

   (select one of the following...)
   a. True
   b. False ✓

3. **fred** can view the contents of **rfile2**.

   (select one of the following...)
   a. True
   b. False

4. **fred** can change the contents of **rfile2**.

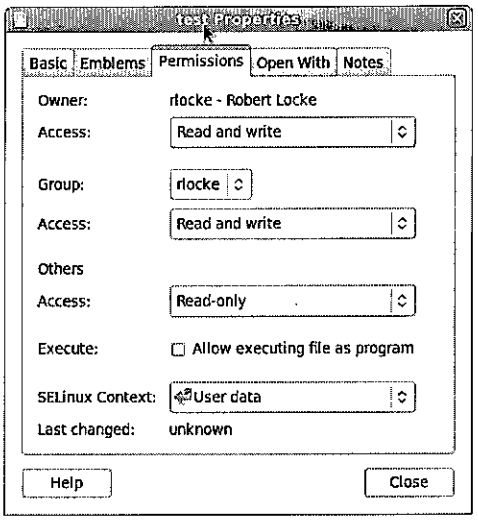
   (select one of the following...)
   a. True
   b. False

Manage Permissions Using GUI Tools

The **Nautilus** file manager allows you to have a limited ability to set or change the basic permissions on a file using the most common configuration settings.

View the Security Properties of a File or Folder

1. Right-click on the file or folder in Nautilus.
2. Select **Properties.**
3. Click on the **Permissions** tab.



Modify Ownership or Group Ownership

Note that there is a pull-down box that allows you to change the group that owns a file to any group of which the current user is a member.

Note

Ownership will have a pull-down selection only if running Nautilus as **`root`**. Group ownership is available to both file owner and **`root`**. As **`root`**, these lists can get quite long.

Use this space for notes

Modify Permissions

Note that the combinations of permissions whch can be set are the main ones that you would normally use on a file. However, the default permissions interface in **Nautilus** will have trouble expressing certain combinations of permissions, and you may not be able to set unusual permissions combinations.

Use this space for notes

Note

Advanced Students: **Nautilus** has a hidden preference that allows you to get a more sophisticated interface for adjusting permissions. To switch to that interface permanently for a particular user account, at a shell prompt as that user, run the command

```
gconftool-2 -t bool --set /apps/nautilus/preferences/show_advanced_permissions true
```

To switch back, just use the keyword **`false`** instead of true at the end of the previous command.

References

GNOME Desktop User Guide

- Section 6.6.16: Changing Permissions

Practice Performance Checklist

Manage File Security Using GUI Tools

Before you begin...

Run **lab-setup-users-2** on serverX to prepare for the exercise by creating the needed users and groups.

Perform the following steps on serverX unless directed otherwise.

- ☐ Log out of the GNOME desktop on serverX
- ☐ Log into the GNOME desktop on serverX as **alice** with a password of **password**.
- ☐ Open a window with a Bash prompt.
- ☐ Become the **root** user at the shell prompt.
- ☐ Launch **nautilus** from the root shell.
- ☐ Create a folder in **/home** called **ateam**.
- ☐ Change the group ownership of the **ateam** folder to **ateam**.
- ☐ Ensure the folder access of **ateam** allows group members to create and delete files.
- ☐ Ensure the folder access of ateam forbids others from accessing its files.
- ☐ Create a folder in **/home** called **bteam**.
- ☐ Change the group ownership of the **bteam** folder to **bteam**.
- ☐ Ensure the folder access of **bteam** allows group members to create and delete files.
- ☐ Ensure the folder access of bteam allows others to access its files.
- ☐ Log out from the GNOME desktop as **alice**.
- ☐ Log into the GNOME desktop as **andy** with a password of **password**.

- ☐ Navigate to the **/home/ateam** folder.
- ☐ Create an empty file called **andyfile1**.
- ☐ Record the default user and group ownership of the new file and its permissions.
- ☐ Create an empty file called **andyfile2**.
- ☐ Change the group ownership of **andyfile2** to **ateam**.
- ☐ Switch GNOME users to **alice**.
- ☐ Navigate to the **/home/ateam** folder.
- ☐ Note the difference in appearance between **andyfile1** and **andyfile2**.
- ☐ Switch GNOME users to **betty** with a password of **password**.
- ☐ Navigate to the **/home** folder.
- ☐ Note the difference in appearance between the **ateam** and **bteam** folders.

Manage Permissions from the Command Line

Viewing File/Directory Permissions and Ownership

The **-l** option of the **ls** command will expand the file listing to include both the permissions of a file and the ownership:

```
[student@desktopX ~]$ ls -l test
-rw-rw-r--. 1 student student 0 Feb  8 17:36 test
```

If you were to run **ls -l directoryname**, you would see the expanded listing of all of the files that reside inside that directory. If you would like to prevent the descent in to the directory and see the expanded listing of the directory itself, add the **-d** option to ls:

```
[student@desktopX ~]$ ls -ld /home
drwxr-xr-x. 5 root root 4096 Jan 31 22:00 /home
```

Changing File/Directory Permissions

The **chmod** command changes access mode for files and directories. The **chmod** command takes a permission instruction followed by a list of files or directories to change. The permission instruction can be issued either symbolically (the symbolic method) or numerically (the numeric method).

Read the **DESCRIPTION** section of the **chmod** man page. Take notes below about the two methods of changing permissions.

Changing permissions with symbols:

Use this space for notes

Changing permissions with numbers:

Use this space for notes

Symbolic Method Keywords:

```
chmod WhoWhatWhich file|directory
```

- *Who* is u, g, o, a *(for user, group, other, all)*
- *What* is +, -, = *(for add, remove, set exactly)*
- *Which* is r, w, x *(for read, write, executable)*

Numeric Method:

```
chmod ### file|directory
```

- Each digit represents an access level: user, group, other
- # is sum of r=4, w=2, and x=1

Examples

- `[student@desktopX ~]$ chmod go-rw file1`
- `[student@desktopX ~]$ chmod a+x file2`
- `[student@desktopX ~]$ chmod 750 sampledir`

Changing File/Directory User or Group Ownership

File ownership can be changed with the **chown** command. For example, to grant ownership of the file **foofile** to **student**, the following command could be used:

```
[root@desktopX ~]# chown student foofile
```

chown can be used with the **-R** option to recursively change the ownership of an entire directory tree. The following command would grant ownership of **foodir** and all files and subdirectories within it to **student**:

```
[root@desktopX ~]# chown -R student foodir
```

Only **root** can change the ownership of a file. Group ownership, however, can be set by **root** or the file's owner. **root** can grant ownership to any group, while non-**root** users can grant ownership only to groups they belong to. Changing the group ownership of a file is done with the **chgrp** command. The syntax is identical to that of **chown**, including the use of **-R** to affect entire directory trees.

Special Permissions

The **setuid** (or **setgid**) permission on an executable means that the command will run as the **user** (or **group**) of the file, no as the user that ran it. An example is the **passwd** command:

```
[student@desktopX ~]$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 35504 Jul 16  2010 /usr/bin/passwd
```

The **sticky bit** for a directory sets a special restriction on deletion of files: only the owner of the file (and **root**) can delete files within the directory. An example is **/tmp**:

```
[student@desktopX ~]$ ls -ld /tmp
drwxrwxrwt. 39 root root 4096 Feb  8 20:52 /tmp
```

Lastly, **setgid** on a directory means that files created in the directory will inherit the group affiliation from the directory, rather than inheriting it from the creating user. This is commonly used on group collaborative directories.

Special Permission	Effect on Files	Effect on Directories
u+s (suid)	File executes as the user that owns the file, not the user that ran the file	No effect
g+s (sgid)	File executes as the group that owns the file	Files newly created in the directory have their group owner set to match the group owner of the directory
o+t (sticky)	No effect	Users with **write** on the directory can only remove files that they own, they can not remove files owned by other users

Table 14.2. Effects of special permissions on files and directories

Setting Special Permissions

- Symbolically: setuid = **u+s** ; setgid = **g+s** ; sticky = **o+t**
- Numerically (fourth preceding digit): setuid = 4 ; setgid = 2 ; sticky = 1

Examples

- `[root@desktopX ~]# chmod g+s directory`
- `[root@desktopX ~]# chmod 2770 directory`

References

`ls`(1), **chmod**(1), **chown**(1), and **chgrp**(1) man pages

Practice Performance Checklist

Manage File Security from the Command Line

Perform the following steps on serverX unless directed otherwise.

- ☐ Log into the GNOME desktop on serverX as **alice** with a password of **password**.
- ☐ Open a window with a Bash prompt.
- ☐ Become the **root** user at the shell prompt.
- ☐ Create a directory in **/home** called **ateam-text**.
- ☐ Change the group ownership of the **ateam-text** directory to **ateam**.
- ☐ Ensure the permissions of **ateam-text** allows group members to create and delete files.
- ☐ Ensure the permissions of **ateam-text** forbids others from accessing its files.
- ☐ Ensure the permissions of **ateam-text** causes files created in that directory to inherit the group ownership of **ateam**.
- ☐ Log out from the GNOME desktop as **alice**.
- ☐ Log into the GNOME desktop as **andy** with a password of **password**.
- ☐ Navigate to the **/home/ateam-text** folder (remember to open a terminal window first).
- ☐ Create an empty file called **andyfile3**.
- ☐ Record the default user and group ownership of the new file and its permissions.
- ☐ Switch GNOME users to **alice**.
- ☐ Navigate to the **/home/ateam-text** folder.

- ☐ Determine **alice**'s privileges to access and/or modify **andyfile3**.

Test

Criterion Test

Case Study

Securing the Stooges

Before you begin...

Run **lab-setup-stooges** as root from desktopX to reset your virtual server, serverX, and have the necessary users and groups created for you.

Your serverX machine has three accounts, **curly**, **larry**, and **moe**, who are members of a group called **stooges**.

Create a directory called **/home/stooges** where these three users can work collaboratively on files. Modify the permissions on this directory so only the user and group access, create, and delete files in that directory. Files created in this directory should automatically be assigned a group ownership of **stooges**. ug=rwx g+s on dir

When you finish, run the evaluation script **lab-grade-stooges** from serverX to make sure that you have done everything correctly.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

User, Group, Other (UGO) Concepts

In this section you learned how to:

- Identify which permissions are applicable when a user accesses a given file based on user, group, or other relationship
- Restrict a file based on a set of specified restrictions that can be implemented using the UGO permission scheme

Manage Permissions Using GUI Tools

In this section you learned how to:

- Display file and directory permissions with Nautilus
- Modify file and directory permissions using Nautilus

Manage Permissions from the Command Line

In this section you learned how to:

- Display file and directory permissions with ls
- Modify file and directory permissions using chmod
- Modify file ownership using chown and chgrp

UNIT FIFTEEN

ADMINISTER REMOTE SYSTEMS

Introduction

Topics covered in this unit:

- Remote shell access
- Remote file transfers
- Archives and compression
- SSH keys

Remote Shell Access

The Secure Shell (SSH) is one of the most versatile system administration tools. It allows login and execution of commands on remote systems. It uses strong encryption and host keys as a protection against network sniffing. It is the only network service which is enabled by default and is remotely accessible. The OpenSSH server configuration usually does not require modification.

SSH Basics

Fill in the blanks as your instructor demonstrates the use of **ssh** and covers these key points.

1. SSH is more secure than telnet because all communication between hosts is _____.
2. **`ssh -X user@host.fqdn`** initiates a remote connection to _____ as **`user`**.
3. The first time an SSH connection is made to a system, the ___public key___ of the remote system is stored locally so its identity can be verified each time a future connection is started.
4. The ___exit___ command is used to finish an SSH session and return to the local shell.

Warning

The **-X** option to **ssh** allows programs on the remote host to display graphical interfaces on your local desktop environment. This can be convenient, and the communication channel itself is secure between the local host and the remote host. However, if your account has been compromised on the remote system, remote users can use your SSH connection to connect to your local desktop environment and eavesdrop on what you are doing or otherwise attempt to compromise your local system.

You should only use **-X** when connecting to systems when you are confident that their security has not been compromised.

References

Red Hat Enterprise Linux Deployment Guide

- Section 9.3.1: Using the ssh Utility

Practice Quiz

Remote Shell Access

Connect to serverX from desktopX using a remote shell. Answer the following questions running commands from that remote shell:

1. The Disk Utility command is **palimpsest**.
   /dev/vda1 is the name of the hard drive on serverX.

2. Redhat Santiago is the name of the OS release according to **/etc/redhat-release**.

3. Run **nautilus** or use the command-line in the remote shell on serverX to perform the following:

   - Create a file named **a1.txt** in **/root**
   - Create a directory named **b2** in **/home/student** which is owned by the **student** user and the **student** group.

Remote File Transfers

The **ssh** command is useful for securely running shell commands on remote systems. However, **ssh** can also be used to securely copy files from one machine to another. There are several utilities that use SSH to do this, but in this section we will look at the **rsync** command.

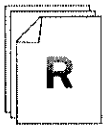
One of the key advantages to **rsync** is not just that it can securely copy files between a local system and a remote system, but that it does so *efficiently*. When copying one directory to a similar directory, only the differences are copied over the network to synchronize them.

Compare and Contrast: Local vs. Remote File Copy

Fill in the open fields.

	Local File Copy	Remote File Copy
Command	**cp**	
Syntax	**cp** ***original-file new-file***	
Arguments	Can use pathnames for arguments	In addition to pathnames, the files can have the following syntax: **target:pathname**, where **target** = **[user@]host.fqdn**. Specify **user@** when the remote username is different than the current username.
Scope of operation	Only works with local files	
How handle directories?	**-r** or **-a** command line switch.	

Table 15.1. Local vs. Remote File Copy Comparison



References

cp(1) and **rsync**(1) man pages

Practice Performance Checklist

Remote File Transfers

Perform the following steps on desktopX unless directed otherwise.

- ☐ Use **rsync** to backup **student**'s home directory on desktopX to the **/tmp** directory on serverX.
- ☐ Create a new file named **z.txt** in **student**'s home directory.
- ☐ Use the same **rsync** command to backup **student**'s home directory on desktopX to the **/tmp** directory on serverX.
- ☐ Remove the **Desktop** directory from the backup on serverX. Run the same **rsync** command.

Archives and File Compression

In the previous section we looked at how files can be copied from one machine to another. In this section we will look at how to create an *archive*, a file which is a bundled collection of files and directories so that it can be stored and transferred more easily. Red Hat Enterprise Linux includes a convenient graphical tools for managing archives, Archive Manager, which can create and handle many different archive formats, including ZIP and TAR archives. cmd ⇒ file-roller

The instructor will demonstrate **Archive Manager** for you. Write down the steps below to perform various activities with **Archive Manager** as your instructor demonstrates them. (If you fall behind, a complete list of steps is included in the Solutions appendix in the back of the book.)

Create an Archive

1. Launch Archive Manager: **Applications** → **Accessories** → **Archive Manager**

2.

3.

4.

5.

Browse and Extract from an Archive

1.

2.

3.

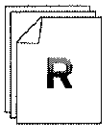
Compress/Decompress a File

1.

2.

3.

4.



References

Archive Manager Manual

- (Open **GNOME Help Browser** with **System** → **Help**, then look under **Utilities**)

Practice Performance Checklist

File Roller Archive

- ☐ Archive **student**'s home directory on desktopX into **/tmp/student.tar.gz**.
- ☐ Send **/tmp/student.tar.gz** to **/tmp** on serverX.
  scp /tmp/student.tar.gz [illegible]@[illegible]:/tmp
- ☐ Extract the **Desktop** folder from the archive to **/home/student** on serverX.

Using SSH Keys

The Secure Shell, **ssh**, allows you to authenticate using a private-public key scheme. This means that you generate two keys, called your private key and your public key. The private key should, as the name implies, be kept private. The public key can be given to anyone. An ssh server that has your public key can issue a challenge that can only be answered by a system holding your private key. As a result, you can authenticate using the presence of your key. This allows you to access systems in a way that does not require typing a password every time but is still secure.

Key generation is done using the **ssh-keygen** command. You can use a key type of DSA or RSA with SSH version 2. SSH protocol version 1 is known to have a security flaw, and therefore its use is not recommended unless you need to connect to legacy ssh servers.

During key generation, you will be given the option to specify a passphrase, which must be provided in order to access your private key. This way, even if the key is stolen, it is very difficult for someone other than you to use it. This gives you time to make a new key pair and remove all references to the old ones, before the private key can be used by an attacker who has cracked it.

It is always wise to passphrase-protect your private key since the key allows you to access other machines. However, this means that you must type your passphrase whenever the key is used, making the authentication process no longer password-less. This can be avoided using **ssh-agent**, which can be given your passphrase once at the start of your session (using **ssh-add**) so it can provide it as necessary while you stay logged in.

Once your SSH keys have been generated, they are stored by default in the **.ssh/** directory of your home directory. Permissions should be 600 on your private key and 644 on your public key.

Before you can use key-based authentication, you will need to copy your public key to the destination system. This can be done with **ssh-copy-id**.

```
[student@desktopX ~]$ ssh-copy-id -i .ssh/id_rsa.pub root@desktopY
```

When you copy your key to another system via **ssh-copy-id**, it uses the **~/.ssh/id_rsa.pub** file by default. Use a the **-i** option to copy a different key with **ssh-copy-id**.

SSH Key Demonstration

ssh-copy-id root@desk

- Use **ssh-keygen** to create a public-private keypair.
- Use **ssh-copy-id** to copy the public key to the correct location on a remote system. For example:

```
[root@serverX]# ssh-copy-id root@serverY.example.com
```

ssh-copy-id -i /root/.ssh/id_rsa.pu
root@desktop

References

Red Hat Enterprise Linux Deployment Guide

- Section 9.2.4: Using a Key-Based Authentication

ssh-keygen(1), **ssh-copy-id**(1), **ssh-agent**(1), **ssh-add**(1) man pages

Practice Performance Checklist

Securely Transferring Backups

- ☐ Create an SSH key-pair as **student** on desktopX using no passphrase.

  ssh-keygen

- ☐ Send the SSH public key to the **student** account on serverX.

  ssh-copy-id

- ☐ Run the **rsync** command used before to backup **student**'s home directory on desktopX to the **/tmp** directory on serverX.

Test

Criterion Test

Exercise

SSH Keys and File Archives

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise.

In the instructions that follow, pay particular attention to the contexts of the two different hosts.

Carefully perform the following steps. Ask your instructor if you have problems or questions.

1. Install the SSH public key generated previously on desktopX to the **`student`** account on serverX.
2. Archive **`student`**'s home directory on desktopX into **`/tmp/student.tar.bz2`**.
3. Copy the **`/tmp/student.tar.bz2`** file on desktopX to **`/tmp`** on serverX.
4. Remove **`student`**'s home directory on serverX.
5. Login to serverX as root using a secure connection from desktopX. Restore **`student`**'s home directory from the **`/tmp/student.tar.bz2`** archive. Hint: the command to launch the Archive Manager is **`file-roller`**.
6. As student, install the SSH public key from the backup you just restored on serverX to desktopX. Verify you can use the SSH keys to get from serverX to desktopX without typing a password.
7. When you are ready to check your work, run **`lab-grade-remote`** on serverX.

Personal Notes

Unit Summary

Remote Shell Access

In this section you learned how to:

- Describe the steps taken by SSH to initiate a secure link
- Use SSH to access a remote shell prompt

Remote File Transfers

In this section you learned how to:

- Copy files securely to/from a remote server

Archives and File Compression

In this section you learned how to:

- Combine files/directories into a tar archive and extract them
- Compress and decompress gzip and bzip2 files

Using SSH Keys

In this section you learned how to:

- Create a user SSH key pair and will deploy the public key on a remote system

UNIT SIXTEEN

CONFIGURE GENERAL SERVICES

Introduction

Topics covered in this unit:

- Managing network services
- SSH hardening
- Desktop server (VNC) configuration
- Secure remote desktop access

Deploy a Generic Network Service

Four Steps to Deploy a Service

1. I Install
2. S Setup
3. E Enable
4. T Test

خطوات
لنشر
Deploy a Service

The four steps above can be used to deploy any network service (such as a web server or an FTP server). First, you must install the software necessary to run the service. Launch the software manager: **System** → **Administration** → **Add/Remove Software**. Search for the package(s) needed for the service and install them.

Next, start the service. Launch the **Services** application: **System** → **Administration** → **Services**. Select the service and click the Start button.

Once it is running, enable the service. This configures the service to start at boot time. Launch the **Services** tool as above. Select the service and click the Enable button.

Lastly, test the service. For instance, to test a web server, connect to the server using a web browser like **Firefox**.

References

Red Hat Enterprise Linux Deployment Guide

- Section 7.2.1: Using the Service Configuration Utility

Securing SSH Access

While OpenSSH server configuration usually does not require modification, additional security measures are available.

In this activity, we are going to discover how to disable remote root logins and the use of passwords (require use of SSH keys).

Securing SSH Search & Learn

1. Use the **Add/Remove Software** application to determine which package provides the SSH service (search for **ssh server**).

2. Use the file listing of the package discovered in the previous question to determine the primary configuration file for the service.

3. Reviewing the man page for the configuration file, which directive disables root login?

4. Which directive in that configuration file disables password login?

References

Red Hat Enterprise Linux Deployment Guide

- Section 9.2.4: Using a Key-Based Authentication

Practice Performance Checklist

Securing SSH

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise.

- ☐ If not done earlier, generate SSH keys on desktopX.

  Copy the public key to the **`student`** account on serverX and verify that the keys are working.

- ☐ Configure SSH on serverX to prevent root logins.

- ☐ Restart the SSH service.

- ☐ Confirm that **`root`** cannot log in with SSH, but **`student`** is permitted to log in.

- ☐ Configure SSH on serverX to prevent password authentication.

- ☐ Restart the SSH service.

- ☐ Confirm that **`visitor`** cannot log in using a password, but **`student`** is permitted to log in using the SSH keys created earlier.

Configuring a VNC Server

While many data centers will standardize on **ssh** for remote administration of Unix and Linux systems, some will use Virtual Network Computing (VNC) for remote administration of Windows servers. Red Hat Enterprise Linux 6 supports the implementation of a VNC server that can allow one or more remote graphical desktops.

Configure a VNC Server Demonstration

1. Install the VNC server package: *tigervnc-server*. package vncserver
2. Edit the **/etc/sysconfig/vncservers** file and add the following line:

```
VNCSERVERS="1:visitor 2:student"
```

3. Set the VNC passwords.

Warning

The **vncpasswd** command must be run by the user whose VNC password is being set. Unlike the **passwd** ***username*** command, **root** cannot configure a VNC password for another user with the **vncpasswd** command.

```
[student@demo ~]$ vncpasswd
Password:  password
Verify:  password
[student@demo ~]$ su - visitor
Password: password
[visitor@demo ~]$ vncpasswd
Password:  password
Verify:  password
```

4. Start and enable the **vncserver** service. ← restart vncserver

chkconfig vncserver on

References

Red Hat Enterprise Linux Deployment Guide

- Section 18.1.23: /etc/sysconfig/vncservers

vncviewer(1), **vncpasswd**(1) man pages

/etc/init.d/vncserver restart

Practice Exercise

Deploy a VNC Server

Carefully perform the following steps. Ask your instructor if you have problems or questions.

Perform the following steps on serverX unless directed otherwise.

1. Install the *tigervnc-server* package on serverX.
2. Configure VNC display 1 for student and display 2 for visitor.
3. Set **redhat** as the VNC password for both student and visitor.
4. Start and enable the **vncserver** service.

Note

When starting the **vncserver** service, the status may not get updated. If this happens, close down the **Services** application and restart it to check the status.

5. You will test the connection in the next section.

Secure Access to a Remote GNOME Desktop

The **vncviewer** command is a viewer (client) used to connect to a VNC server running on a remote system. This can also be found by going to **Applications** → **Internet** → **TigerVNC Viewer**. Both of these are provided by the *tigervnc* package.

VNC is a clear text network protocol; there is no security against eavesdropping, interference, or hijacking of the communication. Therefore, a more secure way to use VNC is to wrap all VNC traffic in a layer of encryption. The easiest way to do this is to tunnel the traffic over an SSH tunnel, assuming **sshd** is running on the remote system. Once the remote **sshd** service decrypts the VNC traffic, it can be passed clear text over its local loopback interface to the machine's VNC service without exposing the clear text traffic over the network.

This is such a useful approach that the **vncviewer** command has an option, **-via** ***user@host***, which connects to the SSH server on *host* as *user* before attempting to connect to the VNC server from there. Note that the hostname given for *host* is resolved by the remote side of the connection, so if you specify *localhost* it will point at *host*, not the local client machine.

On the VNC server, use a line similar to the following to only allow local connections:

```
VNCSERVERARGS[2❶]="-localhost"
```

❶ This number is in reference to the VNC display number (**VNCSERVERS="2:root"**).

VNC viewer -via visitor

Warning

Use the **-via** option to tunnel VNC traffic over an SSH tunnel whenever possible. VNC is a cleartext protocol and your passwords and desktop session will be vulnerable to eavesdropping and interference if you do not tunnel it over a secure connection.

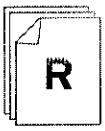
Connect to VNC Server Securely Demonstration

1. Only allow local connections on the server. Add the following to the **/etc/sysconfig/vncservers** file and restart the service:

   ```
   VNCSERVERARGS[2]="-localhost"
   ```

2. Connect to a VNC server using SSH:

   ```
   [instructor@instructor ~]# vncviewer -via visitor@demo localhost:2
   ```



References

vncviewer(1) man page

Practice Exercise

Connect to VNC Securely

Carefully perform the following steps. Ask your instructor if you have problems or questions.

1. Configure the VNC server on serverX to allow local connections only (unless you already did this in the previous exercise).
2. Connect to the VNC server on serverX securely from desktopX using an SSH tunnel.

Test

Criterion Test

Exercise

Secure Remote Administration

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise.

Carefully perform the following steps. Ask your instructor if you have problems or questions.

1. Create SSH keys for **`student`** on desktopX (if necessary).
2. Copy **`student`**'s public key to the **`student`** account on serverX.
3. Configure SSH on serverX to prevent root logins and password authentication.
4. Configure VNC for **`student`** using a password of **`redhat`** on display 1.
5. Allow connections to VNC only from localhost.
6. When you are ready to check your work, run **`lab-grade-securevnc`** on desktopX.

Personal Notes

Unit Summary

Deploy a Generic Network Service

In this section you learned how to:

- Start or stop a specified service temporarily
- List which services are started when the system boots
- Enable or disable a specified service persistently

Securing SSH Access

In this section you learned how to:

- Configure SSH to prohibit root login
- Configure SSH to prohibit password login, but allow access with ssh keys

Configuring a VNC Server

In this section you learned how to:

- Configure a VNC server

Secure Access to a Remote GNOME Desktop

In this section you learned how to:

- Connect securely to a VNC server

UNIT SEVENTEEN

MANAGE PHYSICAL STORAGE II

Introduction

Topics covered in this unit:

- File system parameters
- Modify file system parameters
- Partition removal
- Swap space concepts
- Swap space management

Examine Filesystem Parameters

Previously, this course introduced the **Disk Utility** application, which was used to create new disk partitions and file systems. We now revisit file systems, this time looking "under the hood" at some file system features which are not exposed by the graphical application.

As discussed earlier, the default file system in Red Hat Enterprise Linux 6 is the *Fourth Extended File System*, abbreviated *ext4*. The *ext4* file system is a further improved version of its predecessors, the *ext3* and *ext2* file systems.

The *ext4* file system and its predecessors have tunable settings which are stored internally, here referred to as file system parameters. The parameters can be examined with **`tune2fs -l`**.

The following table highlights some commonly adjusted parameters, along with the relevant **`tune2fs`**(8) command line switch to adjust them (as discussed in the next section).

Attribute	Switch	Comments
Label	**`-L`**	An optional identifying label, similar to disk labels in Windows. In graphical environments, removable media will often be automatically mounted to **`/media/`***`label`*.
UUID	(**`-U`**)	A universally unique identifier, such as *60ab619d-0db0-4d74-9951-c7bd3f67ed85*. The UUID is usually generated when the file system is created, and never changed.
Journal	(**`-j`**)	The *ext3* and *ext4* file systems are *journaling* file systems, which allows them to recover more quickly from irregular unmounts. Usually, journaling file systems create their journal when the file system is created.
Default Mount Options	**`-o`**	Default mount options, such as **`user_xattr`** or **`acl`**. See below.

Table 17.1. Selected Filesystem Parameters

Mount Options

Mount options are applied when the file system is mounted, and default mount options can be specified either in the **`/etc/fstab`** file or embedded within the file system itself. When file systems are created by the **Anaconda** installer, the following default mount options are embedded in the file system.

- **`user_xattr`**: Use user specified extended file attributes.
- **`acl`**: Use POSIX access control list extended file permissions.

/swap → paging space
swap ↓ [illegible]

Note

The *ext4* file system and its predecessors support *attributes* which can be set on files to enable special features or track metadata, data about the data in the files. The most primitive form of attributes affects how files are accessed; see **chattr**(1) and **lsattr**(1) for details.

The *ext4* file system also allows flexible *extended attributes* to be associated with files. Attributes used by the Linux operating system are known as system attributes (such as access control lists (ACLs) and SELinux policy labels). When other applications make use of extended attributes, they are referred to as user attributes.

Often, in order to be useful, attributes need to be enabled at mount time, using, for example, the **user_xattr** or **acl** mount options.

See the **getfattr**(1), **setfattr**(1), and **attr**(5) man pages for more information.

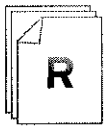
Attributes are beyond the scope of this course.

Examining File System Parameters

Filesystem parameters can be examined using **tune2fs -l** ***device_node***.

```
[root@serverX ~]# tune2fs -l /dev/vda1
tune2fs 1.41.12 (17-May-2010)
Filesystem volume name:   boot_partition
Last mounted on:          /boot
Filesystem UUID:          af796dd7-6455-4e0f-a29d-b9d5bd1575dd
...
Filesystem features:      has_journal ext_attr ...
Default mount options:    user_xattr acl
...
Journal size:             8M
Journal length:           8192
...
```

Use this space for notes



References

Red Hat Enterprise Linux Storage Administration Guide

- Section 7.4: Other Ext4 File System Utilities

Practice Quiz

File System Parameters

1. **/boot** has a journal

   (select one of the following...)
   a. True
   b. False

2. **/boot** does not have any default mount options

   (select one of the following...)
   a. True
   b. False

3. A newly formatted ext4 file system includes **acl** as a default mount option.

   (select one of the following...)
   a. True
   b. False

4. / includes **user_xattr** as a default mount option.

   (select one of the following...)
   a. True
   b. False

5. A file system created by **Disk Utility** has a file system label.

   (select one of the following...)
   a. True
   b. False

Modify File System Parameters

The **tune2fs** command can be used to adjust as well as to view file system parameters. Some example commands include

1. List file system parameters

   ```
   tune2fs -l /dev/fsdev
   ```

2. Create a file system journal

   ```
   tune2fs -j /dev/fsdev
   ```

3. Set the file system label

   ```
   tune2fs -L label /dev/fsdev
   ```

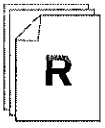
4. Set default mount options

   ```
   tune2fs -o user_xattr,acl /dev/fsdev
   ```

   Note that **-o ^*option*** clears the default mount option *option*.

Use this space for notes

tune2fs -o usr_xattr-acl /dev/vda ep



References

Red Hat Enterprise Linux Storage Administration Guide

- Section 7.4: Other Ext4 File System Utilities

tune2fs(8) man page

Practice Performance Checklist

Modifying File System Parameters

Perform the following steps on serverX unless directed otherwise directed.

- ☐ Create a new 256 MB partition on serverX and use ext4 as the file system type.
- ☐ Add a label of **/test** to the file system.
- ☐ Add **user_xattr** and **acl** as default mount options.
- ☐ Mount the file system on **/test**

Delete an Existing Partition

Freeing the disk space allocated to an existing partition is relatively straightforward.

1. Unmount the file system. If the partition is a physical volume, remove it from the volume group it is currently assigned to.
2. Remove **/etc/fstab** references (if any).
3. Launch **Disk Utility**.
4. Select, then delete the partition.

Use this space for notes

References

fstab(5), **umount**(8), and **vgreduce**(8) man pages

Practice Performance Checklist

Delete a File System

Perform the following steps on serverX unless directed otherwise.

- ☐ Delete the 256 MB partition you just created in the last lab.

Swap Space Concepts

Swap Partitions

Swap space is the general term for disk space which has been committed to extend a system's memory, usually as a special disk partition. Just as a partition needs to be formatted with a file system before it can be used to store files and directories, swap partitions initially must be formatted as such, using, for example, the **Disk Utility** application. Once a partition has been formatted as a *swap partition*, it may not be used for any other purpose.

Once formatted, swap partitions are activated using **swapon**, and deactivated with **swapoff**. Usually, swap partitions are registered in the **/etc/fstab** file, and swap activation happens automatically at boot time.

Activating a swap partition with **swapon** is comparable to mounting a file system with **mount**, though, of course, there is no mount point.

Comparison

Microsoft Windows usually uses a *paging file* which is dynamically allocated on disk by the operating system for the same purpose as Linux swap space. The paging file in Windows can be prone to performance issues due to fragmentation of the file on disk as it grows and shrinks. Linux usually uses a dedicated swap partition for paging, which can help avoid the fragmentation issue; it can also use a preallocated swap file on a file system.

To be completely accurate, like Windows, Linux sends individual pages to "swap" space, it does not swap out entire process memory images. However, older UNIX-like systems did swap processes, and the Linux paging spaces get their names from this historical quirk.

Registering Swap Partitions

Swap partitions can be registered in the **/etc/fstab** file, such that they are activated automatically at bootup. The syntax is similar to registering a file system, using *swap* as both the file system type and a placeholder for the unused mount point.

```
[root@serverX ~]# cat /etc/fstab
/dev/mapper/vg0-lv_root /                       ext4    defaults        1 1
UUID=af796dd7-6455-4e0f-a29d-b9d5bd1575dd /boot ext4    defaults        1 2
...
dev/mapper/vg0-lv_swap swap                     swap    defaults        0 0
...
```

Use this space for notes

Swap Utilization

Once activated with **swapon**, an administrator has no more control over swap space utilization. The Linux kernel will decide to use swap space if "real" memory (RAM) is in short supply. Swap space utilization can be monitored with the **System Monitor : Resources** panel.

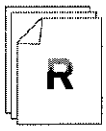
In general, using swap space is considered a bad thing, as accessing information from disk is many times slower than accessing information in RAM. However, swap utilization is considered better than running out of memory. Also some swap use is fine even in normal operation, as pages of anonymous memory which are not currently in use are being moved out of physical RAM to make room for data which is being used or I/O buffers to speed up disk access. When allocating resources, swap space should not be used as a replacement for physical memory for normal day to day use, but instead as a contingency to overcome peak memory demands.

Filesystems vs. Swap Partitions

Fill in the below table with comparable swap area information.

Standard File System	Swap Area
Purpose: Store various files and directories	
Stored on physical disk (Partition ID **0x83**)	
Can reside in an LVM logical volume	
Activated by **mount** and deactivated by **umount**	Activated by _____ and deactivated by _____
Persist a system crash	

Table 17.2. Standard File System/Swap Area Comparison



References

Red Hat Enterprise Linux Storage Administration Guide

- Section 14.1: What is Swap Space?

> Knowledgebase: "If I add several hundred GB of RAM to a system, do I really need several hundred GB of swap space ?"
> https://access.redhat.com/kb/docs/DOC-15252

mkswap(8) and **swapon**(8) man pages

Practice Quiz

Swap Space Concepts

1. Swap Space is used when the system begins to run out of RAM.

2. The Swap on command is used to activate a swap space.

3. The Swap off command is used to deactivate a swap space.

4. The physical ID for a swap partition is _____.

Swapon /dev/vdan
swapoff /dev/vdan
Swapon -s

يحتاج
كلام
Ram
swap
طالب
يكتب كل
swap

Managing Swap Space

Creating Filesystems vs. Creating Swap Partitions

Compare and contrast creating a swap space with creating a regular file system.

File System Creation	Swap Space Creation

Table 17.3. Compare file system/swap space creation

Use this space for notes

References

mkswap(8) and **swapon**(8) man pages

Practice Performance Checklist

Manage Swap Space

You added some additional RAM to serverX and you want to ensure you have enough swap space to support it. You need to create a new swap partition of 1 GB in size.

- ☐ Use all available physical extents in **`vgsrv`** up to 1 GB to create a new logical volume called **swap2**.
- ☐ In the **Disk Utility**, make this logical volume swap space.
- ☐ Make an entry in **`/etc/fstab`** for the swap device.
- ☐ Enable the swap space.

Test

Criterion Test

Performance Checklist

Physical Storage II

- ☐ Run **lab-setup-storage-2** on desktopX to prepare serverX for this exercise.
- ☐ Create two new physical partitions 512 MB in size each.
- ☐ With the first partition, create swap space and make it persistent.
- ☐ With the second partition, create an ext4 file system persistently mounted on **/opt** with **acl** as a default mount option.
- ☐ Reboot then run the **lab-grade-storage-2** grading script on serverX.

Personal Notes

Unit Summary

Examine Filesystem Parameters

In this section you learned how to:

- Get file system information such as volume label, file system type, and block size

Modify File System Parameters

In this section you learned how to:

- Modify file system parameters such as volume label and file system check frequency settings

Delete an Existing Partition

In this section you learned how to:

- Delete an existing partition from the hard disk

Swap Space Concepts

In this section you learned how to:

- Describe how Linux uses swap storage to extend memory

Managing Swap Space

In this section you learned how to:

- Create a swap partition on local storage and configure it for automatic use at boot time
- Activate or deactivate the swap area

UNIT EIGHTEEN

INSTALL LINUX GRAPHICALLY

Introduction

Topics covered in this unit:

- Anaconda: Red Hat Enterprise Linux's installer
- Firstboot customization

Graphical Installation with Anaconda

Getting Started with Anaconda

The Red Hat Enterprise Linux installation program, called **Anaconda**, supports a variety of installation methods. The installation DVD image available from Red Hat Network can be burned to physical DVD media, copied to a USB hard drive, or published by a network installation server.

A physical installation DVD is bootable, so it is the easiest method to use to install Red Hat Enterprise Linux. The other media require booting **Anaconda** from a CDROM, a USB device, or from the network with PXE. A minimal installation image is also available from Red Hat Network called the **`boot.iso`** image. It only provides the first stage of **Anaconda**, so it must be used with other installation media, most commonly a network install server.

Note

In this classroom, the instructor has set up the system so that you can boot the installer from the network using PXE, which gets the installation DVD image from a network installation server. You will perform an installation yourself shortly.

Stages of Anaconda

Anaconda presents an interactive wizard for installing your system. It is broken into two stages, prompting for different information in each stage:

Stage 1 of Anaconda

- The first stage of **Anaconda** uses text-based menus to get input from the user. The purpose of the first stage is to get enough information to locate and download the second stage of the installer.
- Language
- Keyboard
- Installation Method (or source): DVD, hard drive, URL (HTTP/FTP) or NFS
- Network

Stage 2 of Anaconda

- The second stage of **Anaconda** detects video hardware, launches a graphical environment, then interacts with the user graphically. It gets information about how the machine should be installed and configured.
- Select storage devices
- Hostname/network configuration
- Time zone, UTC
- Root password

- Disk partitioning specifics (LVM)
- Boot loader
- Packages

Troubleshooting Anaconda

The **Anaconda** installer prints debugging messages to different *virtual consoles* that are normally not seen. The table below shows the virtual consoles that are available and the key sequence needed to access them:

Key Sequence	Function
Ctrl+Alt+F1	Graphical installation screen
Ctrl+Alt+F2	A shell prompt (Only available during Stage 2 of the installation)
Ctrl+Alt+F3	Installer log messages
Ctrl+Alt+F4	Installer kernel messages
Ctrl+Alt+F5	Other messages (partitioning, file system formatting, etc.)

Table 18.1. Anaconda Virtual Consoles

Use this space for notes

References

Red Hat Enterprise Linux Installation Guide
- Chapter 7: Booting the Installer

Red Hat Enterprise Linux Installation Guide
- Chapter 9: Installing using Anaconda

Practice Performance Checklist

Graphical Installation

- ☐ Save any data you don't want to lose on your desktopX system. Reboot desktopX and initiate a PXE boot (ask your instructor for details).
- ☐ Select **Standard installation** from the GRUB menu that appears.
- ☐ Choose the appropriate language and keyboard.
- ☐ Choose URL as the installation method and configure the network using DHCP. Optionally select the appropriate network card.
- ☐ Enter http://instructor/pub/rhel6/dvd as the URL for the installation image.
- ☐ Click **Next** at the Welcome screen.
- ☐ Choose **Basic storage devices**, click **Next**.
- ☐ Choose **Fresh installation**, click **Next**.
- ☐ Enter desktopX.example.com as the hostname. Configure the network using DHCP and click **Next**.
- ☐ Ensure the date and time are correct and click **Next**.
- ☐ Enter **password** as the **root** password and click **Next**.
- ☐ Click **Use Anyway** when prompted that the root password is weak.
- ☐ Choose **Replace Existing Linux Systems**. Check the **Review & modify** button. Check the **Encrypt** button. Click **Next**.
- ☐ Make a note of the file systems. Encrypt the root file system.
- ☐ Enter a passphrase of **password** (it must be at least eight (8) characters), twice, and click **OK**.
- ☐ Click on **Write changes to disk** when asked.
- ☐ Leave the defaults for the boot loader and click **Next**

- ☐ Choose the **Desktop** software group and select **Customize now**, then click **Next**.

- ☐ In the **Remote Desktop Clients** group, choose the **`tigervnc`** package for installation. You can find this package group by selecting **Desktops** in the left pane, then choose **Remote Desktop Clients** in the right pane of the package selection screen.

Post-install Configuration with Firstboot

Firstboot performs some basic configuration of a newly installed server. When the system first boots up, the boot process is paused so that the system administrator can make some final configuration adjustments before initial logins are allowed.

Firstboot Dialogs

- Agree to Red Hat licensing terms
- Register with Red Hat Network for software updates
- Select appropriate keyboard
- Create a user account (or configure network authentication)
- Configure the date/time (or use NTP)
- Configure kdump for troubleshooting

Use this space for notes

References

Red Hat Enterprise Linux Installation Guide

- Chapter 34: Firstboot

Practice Performance Checklist

Firstboot

After the installation is complete, work through **`firstboot`**.

- ☐ Click **Forward** on the Welcome screen.
- ☐ If you agree to the license agreement, select **Yes, I agree to the License Agreement** and click **Forward**.
- ☐ Do *not* register with Red Hat Network.
- ☐ Create a user named **`visitor`**. Enter a password of **`visitor`** for the **`visitor`** account, twice. Click Forward.
- ☐ Configure instructor.example.com as the NTP server, then click Forward.
- ☐ Leave **kdump** disabled and click **Forward**.

Test

Criterion Test

Exercise

Install Linux Graphically

Before you begin...

This task completely reinstalls your desktopX.example.com system. All data on your system are destroyed, so be sure to copy off any data you want to keep before starting this task.

Carefully perform the following steps. Ask your instructor if you have problems or questions.

1. Reboot your desktop system, interrupting the boot process to boot off your network interface card.
2. Select **Install or upgrade an existing system** from the boot screen.
3. Choose your Language and Keyboard, when prompted.
4. Choose URL as the install type and select **`http://instructor/pub/rhel6/dvd`** as the installation source.
5. Choose Basic Storage Devices, Fresh Installation, and set desktopX.example.com as the hostname. (Use the same desktop name the system had when you started the install.)
6. Choose your timezone and set the **`root`** password to **`redhat`**.
7. Configure the partitions as follows:
   - **`/boot`** 200 MB physical partition
   - **`/home`** 1024 MB physical partition, encrypted using a passphrase of **`password`**
   - 50 GB physical volume for use with a volume group
     - 20 GB logical volume for /
     - 2 GB logical volume for swap
8. No changes are required for the bootloader, so click Next.
9. Select **Desktop** to set the basic install type. Select the **`Customize now`** button, then click **`Next`**. Besides those packages already selected, select the **FTP server** package group. Click Next and the packages begin installing.
10. When installation is complete, press **`Enter`** to reboot as prompted.
11. During boot-up, enter the passphrase (password) to unlock the /home partition when prompted.

12. When you see the welcome screen (**`firstboot`**), answer the questions as appropriate. Do not register with RHN. When prompted, create a user account called student with the password student. You can turn off or disregard Kdump, when you get to it.

13. Once the installation and **`firstboot`** have completed, download and run the grading script. It can be found at the following URL: *http://instructor/pub/gls/ulbin/lab-grade-installation*

14. After you have completed the criterion test, reinstall the standard classroom desktop system. To do this, reboot your desktop system, interrupting the boot process to boot off your network interface card. Select **Install GLS Workstation** from the GRUB menu that appears.

Personal Notes

Unit Summary

Graphical Installation with Anaconda

In this section you learned how to:

- Initiate a graphical installation and will be able to choose available network install media
- Partition the hard disk according to a custom specification
- Use the installer to configure the new system's network interface
- Choose specified package groups and individual packages

Post-install Configuration with Firstboot

In this section you learned how to:

- Perform additional customization using **`firstboot`**

UNIT NINETEEN

MANAGE VIRTUAL MACHINES

Introduction

Topics covered in this unit:

- KVM virtualization
- Virtual guest installation
- Autostart at boot

- Costing

Introduction to KVM Virtualization

Virtualizaton is a feature that allows a single physical machine to be divided into multiple *virtual* machines, which can each run an independent operating system. Red Hat Enterprise Linux 6 for x86-64 supports *KVM*, which allows the kernel to function as a hypervisor supporting guest virtual machines, as long as certain requirements are met.

Facts about KVM virtualization:

- *Kernel-based Virtual Machine*: the virtualization system in Red Hat Enterprise Linux, built into the kernel as a module
- *VirtIO*: KVM supports *paravirtualized drivers* which can be used by KVM guests to obtain better IO performance

KVM benefits include:

- *Fast*: KVM is able to achieve high performance by taking advantage of x86-64 hardware virtualization support and by being closely integrated into the Linux kernel
- *Simple*: the design of KVM is simple, which makes it more robust, easier to support and optimize, and easier to use
- *Standard*: the KVM hypervisor is provided as a capability of the unmodified Linux kernel by the official "upstream" kernel team, which includes Red Hat engineers

KVM support requirements:

- *64-bit*: Red Hat supports KVM on 64-bit AMD or Intel processors running the x86-64 processor architecture
- *Extensions*: the 64-bit CPU, BIOS, and system hardware must also support the AMD Virtualization or Intel VT-x hardware-based virtualization extensions

To check whether a CPU claims to support hardware-assisted virtualization extensions, you can examine its *feature flags*. For example:

```
[user@host ~]$ grep flags /proc/cpuinfo
flags  : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
 dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon
 pebs bts rep_good xtopology nonstop_tsc aperfmperf pni pclmulqdq dtes64 monitor ds_cpl
 vmx smx est tm2 ssse3 cx16 xtpr pdcm sse4_1 sse4_2 popcnt aes lahf_lm ida arat tpr_shadow
 vnmi flexpriority ept vpid
```

Relevant CPU feature flags include:

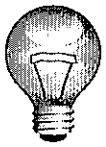
- **lm** = Long Mode (indicates 64-bit support)
- **svm** = Secure Virtual Machine (AMD basic virtualization support)
- **vmx** = Virtual Machine x86 (Intel basic virtualization support)

Only one of **svm** or **vmx** needs to (or is likely to) be present. Note the example above has the **lm** and **vmx** flags, so the CPU should support KVM.

Note

Red Hat Enterprise Linux 6 can not act as a Xen hypervisor, although it can run as a para-virtualized or fully-virtualized Xen guest on a RHEL 5 Xen host. See *Red Hat Enterprise Linux Virtualization* chapter 8, "Installing Red Hat Enterprise Linux 6 as a para-virtualized guest on Red Hat Enterprise Linux 5", for details.

Existing Xen guest machines from a Red Hat Enterprise Linux 5 host can be migrated to run as KVM guest machines on a Red Hat Enterprise Linux 6 host. See *Red Hat Enterprise Linux Virtualization* chapter 23, "Migrating to KVM from other hypervisors using virt-v2v", for details.

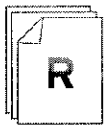


Important

There are two ways that the term *paravirtualization* is used in Linux virtualization which may lead to confusion.

In Red Hat Enterprise Linux 5, the Xen hypervisor supported *paravirtualized guests*. In this scenario, the drivers and kernel of the guests were modified to allow it to run on a Xen hypervisor running on a system that did not support full hardware virtualization extensions. This required that the operating system itself be modified to support Xen paravirtualized virtualization. KVM does not support paravirtualization in this sense.

KVM does support *paravirtualized drivers*. Paravirtualized drivers are special device drivers that can "cheat" by talking directly to the hypervisor. This removes the need for the guest to use a less efficient interface to the hypervisor that acts like some existing hardware device, like a disk controller or network card. These *virtio* paravirtualized drivers are faster than using normal drivers for the virtual hardware presented by KVM to the guest. Likewise, the operating system kernel does not need to be modified in order to take advantage of paravirtualized devices, you only need new drivers to be written which supports them.



References

Virtualization Support in Red Hat Enterprise Linux
http://www.redhat.com/rhel/server/virtualization_support.html

Virtualization Limits in Red Hat Enterprise Linux
http://www.redhat.com/rhel/virtualization/compare/

Red Hat Enterprise Linux Virtualization
- Part I: Requirements and Limitations

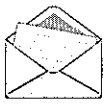
Virtual Guest Installation

When installing a virtual machine, there are several elements that must be chosen before proceeding with the rest of the installation via **Anaconda**.

Virtual Machine Specifications

1. A domain name must be specified
2. Specify the installation media for the first and second stages of **Anaconda**
3. Specify virtual hardware elements:
   - Number and type of CPU
   - Size of RAM
   - Virtual disk device (file or volume)
   - Network connection and MAC address

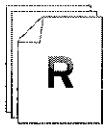
Virtual machines can be installed, managed, and accessed with **`virt-manager`**, a graphical tool. The instructor will demonstrate how to use **`virt-manager`** in class before you use it in the next practice exercise.



Note

Para-virtualized hard disks (that use the virtio drivers) appear to guests as **`/dev/vd*`** instead of **`/dev/sd*`**.

Use this space for notes



References

Red Hat Enterprise Linux Virtualization
- Chapter 6: Virtualized guest installation overview

Red Hat Enterprise Linux Virtualization
- Chapter 7: Installing Red Hat Enterprise Linux 6 as a virtualized guest

`virt-manager`(1) man page

Practice Performance Checklist

Virtual Guest Installation

In this lab you will install a new virtual machine with Red Hat Enterprise Linux using **virt-manager** and the graphical installer. Once you have successfully completed the lab you will need to remove both the virtual machine and its logical volume to reclaim system resources needed for other labs.

Perform the following steps on desktopX:

- ☐ Gracefully shutdown your serverX virtual machine (**vserver**) to reclaim system CPU and RAM resources.
- ☐ Create a logical volume 10 GB in size from the **vol0** volume group and name it **guest**.
- ☐ Create a Red Hat Enterprise Linux 6 virtual machine with the following characteristics:
  - Name = guest
  - Install media = network install from http://instructor.example.com/pub/rhel6/dvd
  - Memory (RAM) = 768 MB
  - CPUs = 1
  - Storage device = the logical volume created in the previous step
- ☐ When the installation begins, choose your keyboard and language. Build your guest system according to the following specifications:
  - When asked about the Virtio Block Device, choose **Re-initialize all**.
  - Choose the appropriate time zone
  - Assign **redhat** as the root password
  - Choose the Desktop software set
  - Use the defaults for everything else

- H/W Assistant virtualization require
- KVM allows both win, linux installed on VM with special kernel
- simple design

Configuring Guests to Start at Boot Time

Practice Group Exercise

Search & Learn: Virtual Machine Automatic Boot

What steps must you take to configure a virtual guest to automatically start at boot time?

1. Launch Virtual Machine Manager.
2. Double-click on the guest virtual machine profile.
3.
4.
5. Check or uncheck the **Start virtual machine on host boot up** check box and click **Apply**.
6. Add the following to the **`/etc/sysconfig/libvirt-guests`** file:

   ```
   ON_BOOT=ignore
   ```

Practice Performance Checklist

Configuring Virtual Machines at Boot-time

- ☐ Configure the **serverX** (vserver) virtual machine to not start at boot time.
- ☐ Configure the **guest** virtual machine to start at boot time.
- ☐ Reboot the physical machine (desktopX).
- ☐ Confirm the **guest** virtual machine started automatically.
- ☐ Configure the **guest** virtual machine to not start at boot time.
- ☐ Reboot the physical machine (desktopX).
- ☐ Confirm the virtual machine did not start automatically.
- ☐ IMPORTANT: After you successfully complete the lab, delete the **guest** virtual machine and the logical volume it uses for storage. Those resources will need to be available for the criterion test.

Test

Criterion Test

Case Study

Virtual Workstation for William Wonderboy

William Wonderboy just joined the company as a software developer. He needs a machine of his own to write code and do testing without disturbing the work of others. You have been assigned the task of building a virtual machine for him to use.

Create a virtual machine named **wonderboy** with an LVM storage device named **/dev/vol0/wonderboy**. Use the installation media found at the following URI:

- http://instructor.example.com/pub/rhel6/dvd

Mr. Wonderboy's virtual machine must have 768 MB RAM and 10 GB of disk storage.

Use a static IP address of 192.168.0.200+X/24, with a gateway and DNS server of 192.168.0.254. Set the hostname to **hostX.example.com**.

Choose an appropriate time zone. Use **redhat** as the root password.

The virtual disk should be partitioned as follows (you will have to re-initialize the disk):

- 250 MB for **/boot**
- 1 GB of swap space
- 6 GB for /
- The rest of the space allocated to **/home**

Choose the **Software Development Workstation** software set.

Once the installation is complete, configure NTP to connect to instructor.example.com

Configure this machine to start automatically when the physical host reboots.

How would you address the case study described above? Take notes on your process in the space below and then implement it.

Personal Notes

Unit Summary

Introduction to KVM Virtualization

In this section you learned how to:

- Describe the basic function, components, and benefits of KVM virtualization

Virtual Guest Installation

In this section you learned how to:

- Install a virtual guest according to specification

Configuring Guests to Start at Boot Time

In this section you learned how to:

- Configure the guest to start when the virtualization host boots

UNIT TWENTY

CONTROL THE BOOT PROCESS

Introduction

Topics covered in this unit:

- Boot an alternate kernel
- Boot into a specific runlevel
- Overcome bootloader misconfigurations
- /boot/grub/grub.conf
- Kernel boot parameters
- /etc/inittab

Booting an Alternate Kernel

The heart of the Linux operating system is the *kernel*, which acts as the interface between user code and system hardware. From time to time, a newer version of the kernel for Red Hat Enterprise Linux is released, which may enable new features or fix software bugs.

In order to use a new kernel, the system must be rebooted. Normally, the newest version of the kernel installed on the system is used. However, Red Hat Enterprise Linux allows multiple kernel versions to be installed at the same time. This allows you to test a kernel update, and if there is a critical regression or other problem with the update, you can easily fall back to a kernel that is known to work for your system.

In this section, we will look at how to manually select what kernel to boot when the system is started. Later, we will look at how you can make this selection permanent.

Write a definition for each of these key terms:

1. bootloader

2. GRUB

You can use the bootloader to:

- Boot into an older kernel if a new kernel is incompatible with your hardware due to a regression
- Boot into single user mode when doing system maintenance or to get control of a machine with an unknown **root** password

Procedure To Boot an Alternate Kernel

1. Interrupt the GRUB countdown: **Esc** key
2. Use arrow keys to select alternate kernels
3. Hit **Enter** when the kernel you want to boot is highlighted

Comparison

GRUB is similar in function to **NTLDR** in older versions of Microsoft Windows, or to **winload.exe** and the **Windows Boot Manager** in Windows 7 and Windows Server 2008.

Likewise, the Red Hat Enterprise Linux kernel is a versioned executable file installed on the system as **/boot/vmlinuz-*** which is loaded and run by GRUB. This executable is similar in function to the Windows **ntkrpamp.exe** (or **ntoskrnl.exe**) file.

References

Red Hat Enterprise Linux Installation Guide

- Appendix E: The GRUB Boot Loader

Practice Performance Checklist

Booting an Alternate Kernel

Perform all of the following steps on serverX.

- ☐ Configure **yum** to point to the **Errata** repository on the **instructor** machine with the following command:

```
[root@serverX ~]# wget http://instructor/pub/gls/errata.repo -O /etc/yum.repos.d/
errata.repo
```

- ☐ Install the **kernel** update that is available. This will take over 3 minutes to install.

- ☐ Boot into the new kernel.

- ☐ Reboot and choose the old kernel.

Booting into a Different Runlevel

Runlevel Definitions

1. Write a definition for this key term:

   runlevel

2. In Red Hat Enterprise Linux, what are each of these runlevels typically used for?

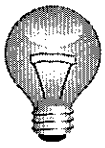
   runlevel 5 - Graphical desktop

   runlevel 3 - _____

   runlevel 1 - _____

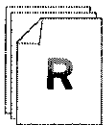
Changing Runlevels

- Execute **`init`** ***`rlnum`*** at the shell prompt, where *`rlnum`* is the runlevel number. This will change the runlevel immediately.
- Pass the runlevel number as an argument to the kernel via GRUB at boot time. This will override the default runlevel.



Important

Note that while runlevels are numbered, only *one* runlevel is entered at boot time. (In other words, if the system is booting to runlevel 5, it *does not* pass through runlevels 1 through 4 first!) A runlevel specifies a particular state the system and its services should be in once it has been completely entered.



References

Red Hat Enterprise Linux Installation Guide

- Technical Appendix E.8: Changing Runlevels at Boot Time

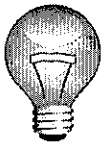
Practice Performance Checklist

Changing the root Password

This timed drill is designed to give you practice changing the root password on a system with an unknown root password.

Perform all of the following steps on serverX.

- ☐ Begin by running the **lab-setup-bootbreak-4** script. This will change the root password to something unknown and mark the current time.
- ☐ Get into the system and reset the root password to **redhat**.



Important

At the release of Red Hat Enterprise Linux 6, there was an SELinux bug which blocked the **passwd** command from working in single-user mode. This is fixed by a bug fix update (see http://rhn.redhat.com/errata/RHBA-2010-0845.html).

If you have the original *selinux-policy* package installed, you must run the **setenforce 0** command in runlevel 1 before the **passwd** command for it to work. After changing the password you should run **setenforce 1** again to put SELinux back in enforcing mode.

- ☐ Once you have reset the password, change the system into runlevel 5 and run the **lab-grade-bootbreak-4** script.
- ☐ View the feedback from the script to ensure you completed the task correctly. The grading script will display a time, write it down.
- ☐ Repeat the process again at least five times.
- ☐ Circle your best time.

Resolve GRUB Issues

The GRand Unified Bootloader (GRUB) provides the bridge in the boot process between the hardware and the Linux kernel. When the system boots, the BIOS starts and normally loads GRUB in stages from the hard drive; from the first 446 bytes of the disk, then from the space between the first sector and the start of the first partition, then from files in **/boot**. GRUB then reads its configuration file, **/boot/grub/grub.conf**, which controls what operating systems and kernels are available to boot.

Comparison

The **/boot/grub/grub.conf** file is similar in purpose to the **boot.ini** file in versions of Microsoft Windows that use the NTLDR boot loader.

The GRUB Boot Screen

When GRUB starts up, a graphical splash screen can be accessed by pressing **Return**, **Space** or any other key. This screen has a list of menu entries, normally bootable images. You can select between the different images with the up and down arrow keys, and press **Return** to select a particular entry for booting. If you want to pass arguments to boot images through menu editing mode or access the GRUB command line, and a GRUB password is set, you will need to type **p** followed by your GRUB password.

Each menu entry which boots Red Hat Enterprise Linux typically has three GRUB directives:

- **root**, which indicates the location of the file system containing **/boot**
- **kernel**, which indicates the location of the kernel to boot relative to **root** and any command-line options or arguments to pass to the kernel
- **initrd**, which indicates the location of the "initial RAM disk" that is loaded early in the boot process by the kernel which contains critical device drivers needed at boot time

Temporary GRUB Correction

1. Interrupt the GRUB countdown: **Esc** key
2. Use **e** to edit current configuration
3. Select lines to correct with arrow keys
4. Type **e** again to edit the current line

Important

Typing **Esc** at this point takes you back to the menu, throwing your changes away.

5. Type **b** to boot with the current changes

References

Red Hat Enterprise Linux Installation Guide

- Technical Appendix E.5: GRUB Interfaces

Practice Performance Checklist

Getting Past a GRUB Misconfiguration

Perform all of the following steps on serverX.

- ☐ Run the **`lab-setup-bootbreak-5`** script to introduce an issue with the boot process.
- ☐ Fix the issue so the system can boot and you can log in.

Making Persistent GRUB Changes

The second stage of GRUB uses **/boot/grub/grub.conf** which has a format of global options followed by boot stanzas. Here is a sample **grub.conf** file:

```
[root@demo ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/vgsrv-root
#          initrd /initrd-[generic-]version.img
#boot=/dev/vda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux (2.6.32-71.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-71.el6.x86_64 ro root=/dev/mapper/vgsrv-root
 rd_LVM_LV=vgsrv/root rd_LVM_LV=vgsrv/swap rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=en_US.UTF-8
 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=pc KEYTABLE=us crashkernel=auto rhgb quiet
        initrd /initramfs-2.6.32-71.el6.x86_64.img
```

- Comment lines begin with a # character
- **default=*number*** - *number* is the default boot stanza (starting from 0)
- **timeout=*number*** - specifies how long the countdown occurs
- **hiddenmenu** - hides the menu display until a key is struck
- **rhgb quiet** - consider removing these kernel arguments to view more diagnostic information during boot

References

Red Hat Enterprise Linux Installation Guide
- Technical Appendix E.7: GRUB Menu Configuration File

Red Hat Enterprise Linux Deployment Guide
- Section 23.6: Verifying the Boot Loader

info grub

Practice Performance Checklist

Making Persistent GRUB Changes

Perform all of the following steps on serverX.

- ☐ Reboot and confirm the issue from the previous problem is not persistently fixed. You will need to apply the fix as before to boot the system.
- ☐ Edit the configuration file to fix the issue permanently.
- ☐ Revert to the older kernel. Ensure that when you reboot, the older kernel is the default kernel.

Passing Kernel Arguments

Search & Learn: Kernel Arguments

1. Install the **kernel-doc** package.
2. Reference the material in **kernel-parameters.txt** found in the **/usr/share/doc/kernel-doc*/Documentation/** directory.
3. Each team must research and summarize the following kernel parameters:

   Team 1:

   - **console**

   Team 2:

   - **enforcing**
   - **selinux**

   Team 3:

   - **init**

   Team 4:

   - **root**
   - **ro**
   - **rw**

References

Kernel documentation: "Kernel Parameters"
/usr/share/doc/kernel-doc-*/Documenation/kernel-parameters.txt

bootparams(7) man page

Practice Performance Checklist

Passing Kernel Arguments

Earlier we had to turn off SELinux enforcing mode to change the **root** password in runlevel 1. There is a kernel parameter that allows us to do that without using commands from the shell. Perform the following steps on serverX.

- ☐ Before you reboot your serverX machine, check its default SELinux status by executing the **getenforce** command. Confirm the system normally boots into Enforcing mode.
- ☐ Reboot your serverX machine and pass **enforcing=0** to the kernel when the system boots.
- ☐ Once serverX finishes booting, check its SELinux status. Confirm the system booted into Permissive mode.

Changing the Default Runlevel

The runlevel determines which services are started automatically on your Linux system. Most Linux desktop systems are set to boot to runlevel 5 (multi-user, networking, graphical interface). Many server systems boot to runlevel 3 (multi-user, networking, no graphical login), where the system comes up to a text-based interface.

The command **who -r** will return the runlevel the system is currently using, as will the right-hand number in the output of **runlevel**.

The default runlevel is read from the **/etc/inittab** file. For example, the line below would cause the system to boot to runlevel 5 by default.

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

Note

In Red Hat Enterprise Linux 6, the new **Upstart** boot system is configured to read the default runlevel from **/etc/inittab** for backward compatibility purposes. None of the other services formerly controlled from that file, including login prompts, can be set up in that file in RHEL 6. Those settings are kept in **/etc/init/** directory instead. For more information see the **init**(8) and **init**(5) man pages.

References

Red Hat Enterprise Linux Installation Guide

- Technical Appendix E.8: Changing Runlevels at Boot Time

Comments in **/etc/inittab**

Practice Performance Checklist

Changing the Default Runlevel

You are configuring a new system that you will be accessing remotely. The system is currently booting into runlevel 5 by default, but this machine will be housed in a data center where you will only log into it remotely. Perform the following steps on serverX.

- ☐ Change serverX to boot to runlevel 3 by default.
- ☐ Reboot serverX.
- ☐ You have successfully completed this lab if serverX boots into textual mode without human interaction.

Test

Criterion Test

Exercise

Bad Brian Blowup Recovery

Before you begin...

Run **`lab-setup-bootbreak`** on desktopX to reset serverX back to its original state.

Carefully perform the following steps. Ask your instructor if you have problems or questions.

Brian was a summer intern who acted as a system administrator for one of your critical servers, serverX. Your company's strained relationship with him finally blew up and resulted in his immediate firing. Sadly, when Bad Brian went out the door he took the root password for serverX with him.

You have been assigned the responsibility of getting control of serverX back:

1. Run the **`lab-setup-bootbreak-6`** script on serverX to prepare it for this lab exercise. This will assign your system with an unknown root password and reboot the system.
2. Set the root password to **`redhat`**.
3. Install the kernel update, but configure the system so the old kernel will continue to be used by default.
4. Pass the **`selinux=1`** argument to the kernel at boot time.
5. Set runlevel 3 as the default.
6. Once your system is booted, run the **`lab-grade-bootbreak-6`** script on serverX to determine how well you did.

Personal Notes

Unit Summary

Booting an Alternate Kernel

In this section you learned how to:

- Use the GRUB menu to select a different kernel to boot from

Booting into a Different Runlevel

In this section you learned how to:

- Use GRUB to boot the system into a specific runlevel

Resolve GRUB Issues

In this section you learned how to:

- Use GRUB to correct a broken GRUB configuration so the system will boot

Making Persistent GRUB Changes

In this section you learned how to:

- Persistently correct a GRUB misconfiguration
- Configure the system to boot from a different default kernel

Passing Kernel Arguments

In this section you learned how to:

- Pass additional kernel parameters to the booting kernel using GRUB

Changing the Default Runlevel

In this section you learned how to:

- Configure the system to boot into a specific runlevel

UNIT TWENTY ONE

DEPLOY FILE SHARING SERVICES

Introduction

Topics covered in this unit:

- FTP server deployment
- FTP server configuration
- Web server deployment
- Web server configuration

Deploy an FTP Server

FTP, the File Transfer Protocol, is one of the oldest network protocols still in common use on the Internet. It provides a simple way for systems to transfer files to and from a remote server over the network.

The name of the FTP server package in Red Hat Enterprise Linux 6 is **vsftpd**, which stands for Very Secure File Transfer Protocol Daemon. The service name is also called **vsftpd**.

The default configuration file supports **anonymous** download-only access to a **chroot**ed tree located at **/var/ftp/**. This means that a remote FTP client can connect to the server as user *anonymous* or *ftp* with no password, and download files from the **/var/ftp** directory on the FTP server which are readable by its local **ftp** user. It also permits users on the system to connect with their password, download any files on the system they can read, and upload files to any location on the system they can write. If you plan to use the FTP server for this purpose, the default configuration settings are reasonable and do not need to be changed.

Use this space for notes

Package - of FTP
vsftpd

Four Steps for Deploying a Network Service

Enter the appropriate menu selection for each step:

1. Install: _____
2. Start: _____
3. Enable: _____
4. Test: Use an FTP client such as **Firefox** or **Nautilus** to see if the service is working (can you download a file from the server?)

References

Red Hat Enterprise Linux Deployment Guide

- Chapter 7: Controlling Access to Services

Practice Performance Checklist

Deploy an FTP server

Perform the following steps on serverX unless directed otherwise.

Deploy an FTP server. Verify it is working and enabled.

- ☐ Install the **`vsftpd`** package.
- ☐ Start the **`vsftpd`** service.
- ☐ Enable the **`vsftpd`** service.
- ☐ Publish a copy of **`/etc/hosts`** to the anonymous FTP document root.
- ☐ Test the FTP server on desktopX with an ftp client (**Nautilus**) to connect to the server ftp://serverX.example.com. Download the **`hosts`** file to student's home directory.

Note

Although you could use **Firefox** to test your FTP server, use **Nautilus** instead because it can be used to test FTP authentication.

FTP Server Configuration

Another common FTP server configuration is an anonymous-only FTP server that only allows the anonymous client to download files, and disables all local users and uploads. In order to configure this, some changes will need to be made to the **vsftpd** configuration.

An FTP deployment best practice is to turn off local user access. When users authenticate to transfer files to/from a system with FTP, their account names and passwords are vulnerable to an eavesdropping attacker. (If secure file transfer is needed by users, the **rsync** command over SSH, or the SFTP service provided by **sshd** are better choices.) Anonymous FTP by its nature is public, and files provided through anonymous FTP are assumed to be public and not sensitive.

The **vsftpd** configuration file is found in **/etc/vsftpd/vsftpd.conf** and the document root is found in **/var/ftp/**. When you make changes to the FTP server, do not forget to restart the service.

Make sure you understand the following options:

- **anonymous_enable=YES**: enables the anonymous FTP user
- **local_enable=NO**: disables all non-anonymous local user accounts
- **write_enable=NO**: disables any user from uploading files to the FTP server

Use this space for notes

References

vsftpd.conf(5) man page

Practice Performance Checklist

Restrict FTP Access

Perform the following steps on serverX unless directed otherwise.

Because FTP is an insecure protocol, it is a security risk to allow normal users to connect and authenticate. Configure your FTP server to permit anonymous connections only.

- ☐ Use an ftp client to connect to **`serverX.example.com`** and authenticate as **`student`** to confirm it allows non-anonymous users.
- ☐ Which file is the main vsftpd configuration file?
- ☐ Which configuration file directive controls non-anonymous access to the system?
- ☐ Configure vsftpd to deny access by local, non-anonymous users.
- ☐ Retest your server and confirm student no longer has authenticated access to your FTP server.

Deploy a Web Server

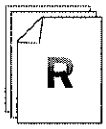
As we have seen, there is a pattern to deploying a network service: Install, Start, Enable and Test.

In this section, the class will work in small groups to walk through the deployment of an Apache web server in its default configuration. You will set it up to serve out a web page with a link to your FTP server's **/var/ftp/pub** directory.

The Apache web server package is named **httpd**, which is also the name of the service once installed. The **httpd** configuration file is found in **/etc/httpd/conf/httpd.conf** and the document root which contains HTML pages it serves is **/var/www/html/** by default. If you make changes to the web server's configuration file, do not forget to restart the **httpd** service.

The walk through exercise begins on the next page.

Use this space for notes



References

Red Hat Enterprise Linux Deployment Guide

- Chapter 11: The Apache HTTP Server

Apache HTTP Server Version 2.2 Documentation ***(if httpd-manual is installed)***
http://localhost/manual/

Apache HTTP Server Version 2.2 Documentation
http://httpd.apache.org/docs/2.2/

Practice Performance Checklist

Deploy a Web Server

Perform the following steps on serverX unless directed otherwise.

The instructor will split up the class into groups. Once you are in your group, do the following:

Given that the name of the web server package is **`httpd`**, deploy a web server on serverX. It should provide HTTP file services. It should be active when your server is rebooted.

- ☐ Install the **`httpd`** package.
- ☐ Start the **`httpd`** service.
- ☐ Enable the **`httpd`** service.
- ☐ Create a symbolic link in your web server document root to the **/pub** directory in your FTP server and call it **pub**. ln -s /var/ftp/pub/ pub
- ☐ Create an **`index.html`** file in the document root of your web server with the following contents:

```
<h1>Classroom Web Services</h1>
<p>
<a href="pub">Click here</a> to view public files.
</p>
```

- ☐ Reboot and verify this content is available through your web browser before you notify the public to ensure your customers can access it as well. restart service httpd
- ☐ Test the web server using the **Firefox** browser.

Test

Criterion Test

Performance Checklist

Deploy File Sharing Services

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise.

Nickel and Copper Cutlery want to publish an on-line catalog to their customers. Deploy FTP and HTTP services on serverX and confirm they are working and enabled at boot.

Perform the following steps on serverX unless directed otherwise.

- ☐ Create a file called **`index.html`** with exactly two lines that contain the following content:

```
NICKEL AND COPPER CUTLERY
On-line catalog coming soon!
```

- ☐ Configure serverX to provide both FTP and web services. Disable non-anonymous FTP access.
- ☐ Configure your serverX machine to serve identical file content to both anonymous FTP and HTTP users. The following URLs should both display the file you created above:
  - ftp://serverX/pub/index.html
  - http://serverX/index.html
- ☐ Reboot your serverX machine. Use a web browser to confirm your services are functioning correctly.

Personal Notes

Unit Summary

Deploy an FTP Server

In this section you learned how to:

- Install and activate an FTP server

FTP Server Configuration

In this section you learned how to:

- Configure the FTP server to only provide anonymous download service

Deploy a Web Server

In this section you learned how to:

- Install and activate an HTTP server
- Publish custom content using HTTP

UNIT TWENTY TWO

SECURE NETWORK SERVICES

Introduction

Topics covered in this unit:

- Firewall activation
- Opening firewall ports
- SELinux concepts
- SELinux modes
- SELinux management tool
- Displaying SELinux attributes

Activate and Deactivate Firewall Protection

Firewalls

Computer security is often compared to an "onion" model, where there are many independent layers of security policy. In Linux, the *firewall* is a layer of protection implemented by the kernel which sits between network applications and the network. The firewall provides administrators a single point of control to allow or deny access to network applications.

The firewall can easily be managed using the **System** → **Administration** → **Firewall** application (**`system-config-firewall`**). This utility, which has been significantly enhanced since Red Hat Enterprise Linux 5, enables fairly in-depth configuration of the firewall.

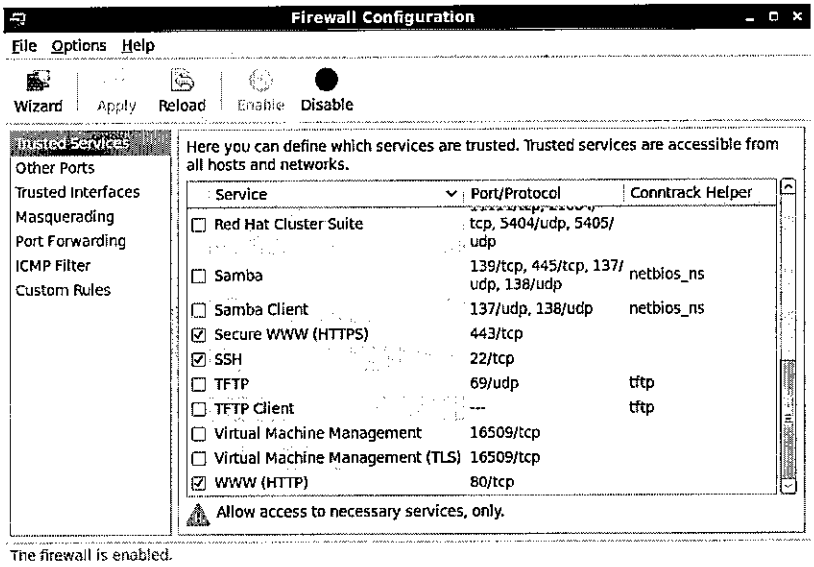


Figure 22.1. The Firewall Adminstration Tool

The firewall is normally enabled by default after manual installation. There are two sets of default settings, **Server** and **Desktop**. Both settings allow all outbound traffic generated by the system to pass, but only allow the following inbound IPv4 and IPv6 traffic to be received by the system:

- Traffic originating from the host to itself (from the **`lo`** interface)
- ICMP traffic (**`ping`** requests, **`Destination Unreachable`** messages, and so on)
- Traffic that is part of a network communication started by the local host (for example, incoming responses to NTP queries made by the host with the firewall, responses from web sites to a local **Firefox** program, and so on
- Requests for **SSH** sessions (traffic to port 22/TCP)

The **Desktop** configuration also allows

- Printing as a **CUPS Client** (traffic to port 631/UDP)
- Acting as an **SMB Client** (traffic to ports 137/UDP and 138/UDP)

- **mDNS** service for Zeroconf discovery (traffic to port 5353/UDP)
- **IPSec** (traffic to port 500/UDP and using the AH and ESP protocols)

You can revert to the default settings by selecting **Server** or **Desktop** from **Options** → **Load Default Configuration** and clicking on **Apply**.

While more complicated configurations are possible, the firewall can be enabled or disabled, and access to selected applications can be allowed or denied, from the default **Trusted Services** panel.

Important

Advanced Students: In Red Hat Enterprise Linux 6, the **Firewall Configuration** tool sets identical rules for both IPv4 and IPv6 network traffic, using **`iptables`**(8) and **`ip6tables`**(8). If you are using these command line tools to adjust your firewall settings, make sure that you do not forget about updating your **`ip6tables`** rules.

References

Red Hat Enterprise Linux Security Guide
- Section 2.5.2: Basic Firewall Configuration

Note

Looking Ahead: The command line tools for working with the firewall mentioned above, such as **`iptables`**(8), and advanced firewall configurations, are discussed in more depth in *Red Hat System Administration III*. If you are already familiar with the command line syntax used by **`iptables`**, note that you can add **Custom Rules** in that syntax in the **Firewall Configuration** utility. Additional firewall documentation is also available at the *Netfilter/iptables Home Page*, **`http://www.netfilter.org/`**.

Practice Performance Checklist

Enable and Disable the Firewall

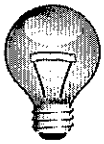
Perform the following steps on serverX unless directed otherwise.

- ☐ Activate the firewall with the default ports enabled.
- ☐ Deactivate the firewall.

Modify the Firewall to Allow Access to Trusted Services

In this section, the instructor will lead the class in an activity to explore how to modify firewall settings. You will be divided into small groups, and each group will determine and record the steps needed to modify the firewall to allow incoming access for a specified service. One student will work through the steps, while the others will observe and take notes. You may use your workbook and other resources to assist you.

At the end of this section, everyone will work through a similar procedure in the practice checklist to help you reinforce what you have learned about how to do this.



Important

Be careful if you are making changes to firewall settings on a remote system. In particular, be sure not to block the network traffic you are using to communicate with the remote system.

Use this space for notes

References

Red Hat Enterprise Linux Security Guide

- Section 2.5.2: Basic Firewall Configuration

Practice Performance Checklist

Allow HTTP and FTP through the Firewall

Perform the following steps on serverX unless directed otherwise.

- ☐ Enable the firewall
- ☐ Deploy an FTP server on serverX
- ☐ Deploy an HTTP server
- ☐ Allow the FTP, HTTP, and SSH services through the firewall

Basic SELinux Security Concepts

كل حاجة معنوية إن ما هو مسموح

SELinux, or *Security-Enhanced Linux*, is an additional mechanism which protects the security of your system.

In a way, it can be thought of as a parallel permissions system to the standard permissions system. In the regular permissions model, processes run as users, and the files and other resources on the system are labeled with permissions that control which users have what access to which files.

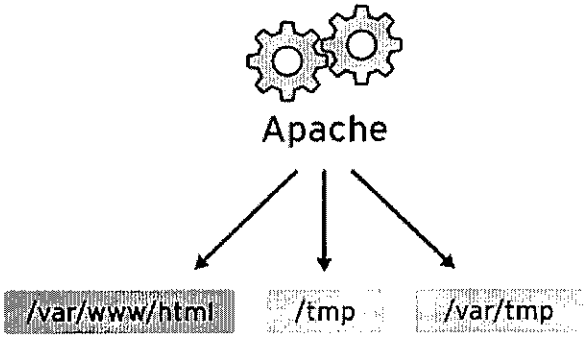
SELinux adds a parallel set of permissions, in which each process runs with an *SELinux security context*, and files and other resources on the system are also labeled with a security context. The difference from normal permissions is that a configurable *SELinux policy* controls which process contexts can access which file contexts. Red Hat provides a default policy which most people use.

Another difference with SELinux, is that to have access to a file, you have to have both regular access and SELinux access. So, even if your process is running as the superuser, **root**, it may be denied access to a file or resource based on the SELinux security context of the process and of the file or resource!

This allows us to limit the scope of security compromises on the system, even to the root account, by ensuring that processes are *confined* by the SELinux policy and their security context into only being able to do things that they should be normally authorized to do.

Use this space for notes

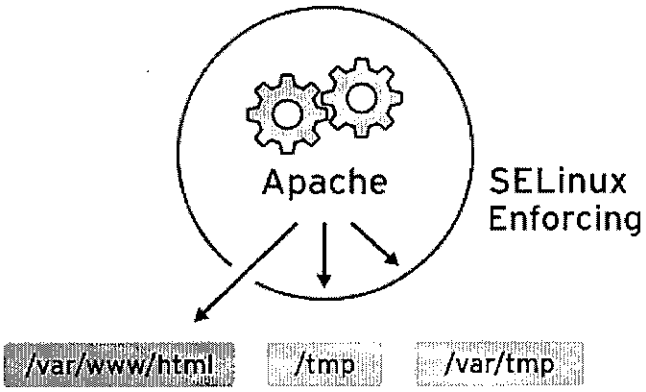
Here is an example of a normal system that does not have SELinux turned on, which is running the **Apache HTTPD** web server:



The web server is available to remote access over the Internet. That means that malicious people can try to break into the system through a security bug in the web server. If they succeed, they will have control of a process running as user **apache** and group **apache**. Anything readable by

that user can now be accessed by the attacker; anything writable by that user can be written by that attacker. This includes files and directories that the web server normally has no business working with. A further local-only security bug in one of those may enable the attacker to gain superuser access.

So, how can SELinux change this?

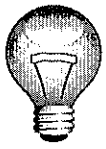


This is the same system, with SELinux turned on. By default, the SELinux policy denies all access, unless rules are included in the policy which permit certain process contexts to access certain file and resource contexts. (The reference policy provided by Red Hat has a carefully tuned set of rules for production systems provided for you.)

The web server's **`httpd`** processes are labeled with the SELinux context **`system_u:system_r:httpd_t`**. The important part of the context is the third colon-separated field, the *SELinux type*: **`httpd_t`**.

The files and resources on the system are also labeled with SELinux contexts, and again the important part is the SELinux type. For example, files in **`/var/www/html`** have the type **`httpd_sys_content_t`**. Files in **`/tmp`** and **`/var/tmp`** normally have the type **`tmp_t`**.

The SELinux policy has a rule that allows processes running as **`httpd_t`** to access files labeled as **`httpd_sys_content_t`**. There is no rule allowing those processes to access files labeled **`tmp_t`**, so those accesses will be denied, *even if regular file permissions indicate that they should be allowed.*



Important

In order for a process to access a file, it must be permitted *both* by regular permissions and by the SELinux types and policy. If *either* regular permissions or SELinux block access, access is denied.

Note that this is true even if you are logged in as root! Even though root is always allowed access under regular permissions, the process may be running as a context which is blocked by SELinux.

One of the goals of SELinux is to protect the user data from system services that have been compromised. This extends even to the root account.

SELinux has a special type, **unconfined_t**, that ignores all SELinux restrictions. When you log in to **root** on the system, you are normally running as **unconfined_t**, allowing you to ignore all normal permissions (since you are **root**) and all SELinux restrictions (since you are **unconfined_t**). The **id** command will show you your shell's current context. When you run programs, the program may start in a more restricted context instead of **unconfined_t**, based on the type with which the program's executable file has been labeled.

Use this space for notes

References

Red Hat Enterprise Linux Security-Enhanced Linux

- Chapter 2: Introduction

Practice Quiz

Basic SELinux Concepts

1. To which of the following does SELinux apply security context (check all that apply)?

   (select one or more of the following...)
   - a. Ports
   - b. Processes
   - c. Files
   - d. Directories
   - e. Remote file systems

2. SELinux can be used to:

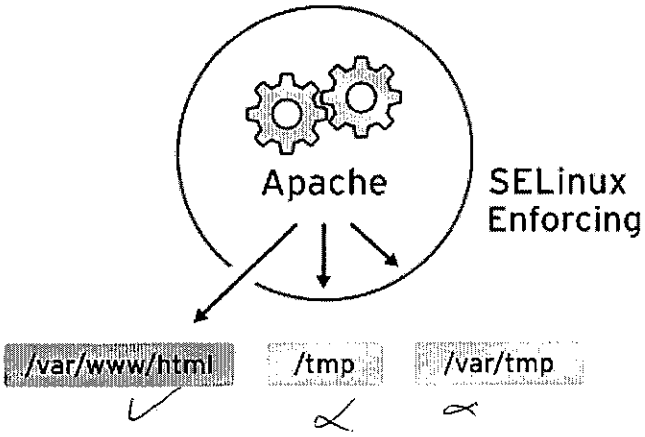
   (select one or more of the following...)
   - a. Protect a service from running on other ports.
   - b. Protect user data from applications like the web server
   - c. Block remote systems from accessing local ports → fw
   - d. Keep the system updated → RHN
   - e. Access a web server → webserver

3. Which of the following are standard SELinux context types?

   (select one or more of the following...)
   - a. selinux_type
   - b. object_r
   - c. httpd_sys_content_t
   - d. tmp_t
   - e. user_u

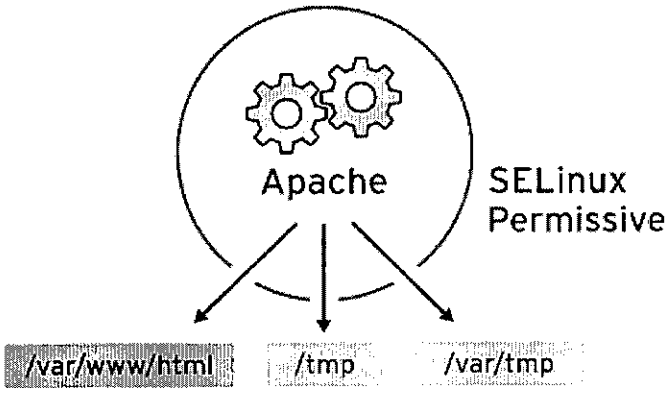
SELinux Modes

For troubleshooting purposes, we can temporarily disable SELinux protection, by changing the *SELinux mode*.



In *enforcing* mode, SELinux actively denies access to the web server attempting to read files with `tmp_t` type context. In enforcing mode, SELinux both logs violations and enforces rules.

Use this space for notes

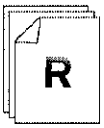


Permissive mode is often used to troubleshoot issues. In permissive mode, SELinux allows all interactions, even if there is no explicit rule, and it logs all of the denied interactions. This mode

can be used to determine if you are having an SELinux issue. No reboot is required to go from enforcing to permissive or back again.

Use this space for notes

A third mode, *disabled*, completely disables SELinux. You must reboot to disable SELinux entirely, or to get from disabled mode to enforcing mode or permissive mode.



References

Red Hat Enterprise Linux Security-Enhanced Linux

- Section 5.5: SELinux Modes

Practice Quiz

SELinux Modes

1. SELinux _____ permissive _____ mode allows logging, but not protection.

2. SELinux _____ enforcing _____ mode protects the system.

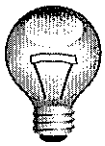
3. Which of the following are valid SELinux modes?

   (select one or more of the following...)

   ✓ a. enforcing
   b. testing
   ✓ c. permissive
   ✓ d. disabled
   e. logging

Use the SELinux Management Tool to Change SELinux Modes

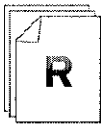
Manage the SELinux mode with the **System** → **Administration** → **SELinux Management** utility. The **System Default Enforcing Mode** sets the default applied at boot time. **Current Enforcing Mode** changes Enforcing/Permissive mode immediately. There is no need to apply changes; all changes occur immediately.



Important

Do NOT double click, be patient!

Use this space for notes



References

Red Hat Enterprise Linux Security-Enhanced Linux

- Section 5.5: SELinux Modes

Practice Performance Checklist

Changing Enforcing and Permissive Modes

Perform the following steps on serverX unless directed otherwise.

- ☐ Set the SELinux mode to permissive.
- ☐ Set the SELinux mode to enforcing.

Display the SELinux Contexts of Processes and Files

SELinux types on files and directories can be viewed or changed from **Nautilus**:

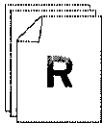
1. Right-click on a file or directory
2. Choose **Properties**
3. Choose the **Permissions** tab
4. View/set the context in the **SELinux Context** box

Use this space for notes

SELinux type contexts for processes can be viewed from **System Monitor**:

1. Open the utility by selecting **Applications** → **System Tools** → **System Monitor**
2. Go to **Edit** → **Preferences**
3. In the **Processes** tab, under **Information Fields**, select the **Security Context** checkbox and **Close** the preferences window
4. Back in the main window's **Processes** tab, note that you can now see the SELinux contexts of processes

Use this space for notes



References

Red Hat Enterprise Linux Security-Enhanced Linux

- Chapter 3: SELinux Contexts

Practice Quiz

SELinux Type Contexts on Files and Processes

Deploy a web server.

For each of the following, find the SELinux type context.

1. /var/www/html/ has
   _____ type
2. /tmp/ has _____ type
3. /etc/hosts has _____ type.
4. The **`httpd`** process has
   _____ type.
5. /etc/httpd/conf/httpd.conf has
   _____ type.
6. /home/student has _____ type.
7. The **sshd** process has
   _____ type.

Test

Criterion Test

Performance Checklist

Secure Web Services

Before you begin...

Execute **`lab-setup-secure-web`** as **`root`** on desktopX to prepare serverX for the criterion test.

Perform the following steps on serverX unless directed otherwise.

- ☐ Deploy a web server on serverX.
- ☐ Install the **`mod_ssl`** package.
- ☐ Restart the web service.
- ☐ Enable the firewall and allow the HTTP and HTTPS ports.
- ☐ Create **`/tmp/d.html`** and *move* it to the web server document root.
- ☐ Try to display *http://serverX/d.html* - it should fail.
- ☐ Change the context on **`d.html`** to **`httpd_sys_content_t`**.
- ☐ Run the **`lab-grade-secure-web`** grading script to confirm you did the exercise correctly.

Personal Notes

Unit Summary

Activate and Deactivate Firewall Protection

In this section you learned how to:

- Activate and deactivate the system firewall using GUI tools

Modify the Firewall to Allow Access to Trusted Services

In this section you learned how to:

- Use a GUI tool to modify the firewall rules to allow or deny access to specific predefined services

Basic SELinux Security Concepts

In this section you learned how to:

- Identify basic SELinux security concepts such as context, user/role/type, and policy

SELinux Modes

In this section you learned how to:

- Describe the functional differences between SELinux enforcing and permissive modes when SELinux security is enabled

Use the SELinux Management Tool to Change SELinux Modes

In this section you learned how to:

- Use GUI tools to activate and deactivate SELinux on their system

Display the SELinux Contexts of Processes and Files

In this section you learned how to:

- Display the SELinux context of running processes
- Display the SELinux context of files

UNIT TWENTY THREE

COMPREHENSIVE REVIEW

Do You Still Have Questions?

This unit is the final, comprehensive review for this course. Hopefully it will give you an opportunity to see see how much you have learned and to solidify the content that was learned.

Before you get broken up into teams and are assigned various tasks to complete, spend a few minutes asking questions about any of the topics introduced in this course that you feel uncomfortable with.

Practice Resequencing Exercise

Deploying Secure Network Services

Below are the steps you will take to deploy network services. Assume you will deploy VNC, FTP, and HTTP services in that order. Mark the order the steps should be taken:

__ Deploy a web server.

__ Connect to a remote serverZ for all tasks. The **`student`** password is **`student`**; the **`root`** password is **`redhat`**.

__ Restore the SELinux context for the files in the HTTP server document root and the FTP server document root.

__ Deploy a VNC server for the **`student`** user on display 2. Use a password of **`redhat`**.

__ Verify that you can view the files in the HTTP server document root and the FTP server document root.

__ Move the **`/tmp/ftp2.txt`** file to the FTP server document root.

__ Create the **`/tmp/http1.html`** and **`/tmp/http2.html`** files.

__ Deploy an FTP server.

__ serverZ = server__.example.com

__ Create the **`/tmp/ftp1.txt`** and **`/tmp/ftp2.txt`** files.

__ Enable the firewall and allow access to the HTTP, FTP, SSH and VNC (port 5902) services.

__ Move the **`/tmp/http1.html`** file to the HTTP server document root.

Personal Notes

Appendix A. Solutions

Get Started with the GNOME Graphical Desktop

Practice Performance Checklist

Using the GNOME Desktop

Do each of the following tasks on your desktop machine. Mark each task as you complete it.

- ☐ Log in as **visitor** with the original password of **password**.

  At the GNOME login screen click on the **visitor** user account then provide **password** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Change the **visitor** password from **password** to **55TurnK3y**.

  Select the **System** → **Preferences** → **About Me** menu item. A window will appear displaying information about the **visitor** user.

  Click the **Change Password...** button. Type **password** in the dialog box that appears then click **OK**. Another dialog box will appear asking for the new password. Type **55TurnK3y** then click **OK**. Repeat to confirm the new password and click **Close** once the information is updated.

  Click **Close** again to close the About Me information window.

- ☐ Log out.

  Select the **System** → **Log Out visitor...** menu item then click the **Log Out** button in the confirmation window that appears.

- ☐ Log back in as **visitor** with the new password of **55TurnK3y**.

  At the GNOME login screen click on the **visitor** user account then provide **55TurnK3y** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Lock the screen.

  Select the **System** → **Lock Screen** menu item.

- ☐ Unlock the screen.

  Move the mouse to have the password dialog box appear. Provide **55TurnK3y** as the password then click the **Unlock** button. The GNOME desktop should reappear.

- ☐ Without logging out, switch to the user **student** with a password of **student**.

  Left-click on the **visitor** user name displayed in the upper-right corner of the screen then select the **Switch User** menu item. When the GNOME login screen appears, click on the **student** user account then provide **student** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Log out from the **student** account. Provide visitor's password when the screensaver appears to get back to the GNOME desktop.

  Select the **System** → **Log Out student...** menu item then click the **Log Out** button in the confirmation window that appears.

  Provide **55TurnK3y** as the password then click the **Unlock** button. The GNOME desktop should reappear.

- ☐ Shut down your machine.

  Select the **System** → **Shut Down...** menu item. Click the **Shut Down** button in the confirmation screen that appears.

- ☐ Power on your machine to be ready for future lab work.

Note

If your hardware is configured to PXE boot by default, a boot menu may appear when you power on your workstation. Select the fourth boot option, **Boot from local drive**, in this situation.

Press the power button for the specific hardware used in your classroom.

Practice Performance Checklist

Using gedit

- ☐ Log into your desktop machine as **student**.

  At the GNOME login screen click on the **student** user account then provide **student** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Launch the **gedit** text editor.

  Select **Applications** → **Accessories** → **gedit Text Editor** to open **gedit**.

- ☐ Open the **gedit-fix-practice.txt** file in the **student** folder and follow the directions contained therein.

  - Click the **Open** button and the contents of the **student** will appear. Left-click the **gedit-fix-practice.txt** file to select the file. Click the **Open** button to begin editing.
  - As you edit the file, you will use the following features:
    - Search and Replace: Select the **Search for and replace text** button.
    - Insert text: Click where you want to add text and begin typing.

- Copy/paste text: Highlight text with your mouse, right-click and select **copy**, move cursor to where you want the text, right-click and select **paste**.
- Delete selected text: Highlight text you want to delete and press **`Delete`**.
- Delete a paragraph: Highlight several lines and select **`Delete`**.
- Save changes to original file: Select the **Save** button.
- Save changes to a new file: Select **File** → **Save As** and choose a new file name.

Within gedit, there are many other features you can explore on your own. Select **Tools** → **Check Spelling** to open an interactive spell checker. If you make a mistake, select **Edit** → **Undo** (or press **`Ctrl+z`**) to undo the change. If you are working on files with a particular document or code format, select **View** → **Highlight Mode** to highlight text in an appropriate way.

Test

Criterion Test

Performance Checklist

GNOME Skills

Before you begin...

Close **`gedit`** and logout **`student`** from the previous exercise.

Select the **System** → **Log Out student...** menu item then click the **Log Out** button in the confirmation window that appears.

- ☐ Successfully log in as **`visitor`** with the password of **`55TurnK3y`**.

  At the GNOME login screen click on the **`visitor`** user account then provide **`55TurnK3y`** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Change **`visitor`** password from **`55TurnK3y`** to **`Test123Time`**.

  Select the **System** → **Preferences** → **About Me** menu item. A window will appear displaying information about the **`visitor`** user.

  Click the **Change Password...** button. Type **`55TurnK3y`** in the dialog box that appears then click **OK**. Another dialog box will appear asking for the new password. Type **`Test123Time`** then click **OK**. Repeat to confirm the new password and click **Close** once the information is updated.

  Click **Close** again to close the About Me information window.

- ☐ Without logging out, switch to the user **`student`** with a password of **`student`**.

Left-click on the **visitor** user name displayed in the upper-right corner of the screen then select the **Switch User** menu item. When the GNOME login screen appears, click on the **student** user account then provide **student** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Lock the screen.

  Select the **System** → **Lock Screen** menu item.

- ☐ Unlock the screen.

  Move the mouse to have the password dialog box appear. Provide **student** as the password then click the **Unlock** button. The GNOME desktop should reappear.

- ☐ Log out from the **student** account. You will probably have to provide the **visitor** password to continue.

  Select the **System** → **Log Out student...** menu item then click the **Log Out** button in the confirmation window that appears.

  Provide **Test123Time** as the password then click the **Unlock** button. The GNOME desktop should reappear.

- ☐ Reboot your machine.

  Select the **System** → **Shut Down...** menu item. Click the **Restart** button in the confirmation screen that appears.

Exercise

Editing Files with gedit

1. Log into your desktop machine as **student**.

   At the GNOME login screen click on the **student** user account then provide **student** when prompted for the password. Click **Log In** once the password has been typed in.

2. Launch the **gedit** text editor.

   Select **Applications** → **Accessories** → **gedit Text Editor** to open **gedit**.

3. Open the **gedit-fix-test.txt** file in the **student** folder.

   - Click the **Open** button and the contents of the **student** will appear. Left-click the **gedit-fix-test.txt** file to select the file. Click the **Open** button to begin editing.

4. Save a copy of that file to **gedit-fix-test-solution.txt** in the **student** folder.

   Select **File** → **Save As...** then type **gedit-fix-test-solution.txt** in the **Name** field in the dialog box.

5. Edit **gedit-fix-test-solution.txt** as described in that file. The resulting file should appear similar to the following:

```
This is the document that needs to be fixed for the GNOME Desktop/
gedit test.

Insert your name at the end of this line: John Doe
This paragraph needs to be copied later in the document.

Delete the extra word that does not belong in this sentence.

Copy the paragraph above below this paragraph. Make sure there is a
 blank line between the two paragraphs.

This paragraph needs to be copied later in the document.

This should be the last paragraph of the document. Save your corrected
 version of this document under its original name.
```

6. Save your changes to the document.

   Click the **Save** button.

7. Create a new text file in the **student** folder called **gedit-new-test.txt** with the following single line of content:

```
I can create new text files with gedit.
```

   Select **File** → **New** to create a new window for editing. Type the text above into the editor window. Click the **Save** button. When the dialog box appears, type **gedit-new-test.txt** in the **Name** field in the dialog box. Click the **Save** button in the dialog box to confirm.

Manage Files Graphically with Nautilus

Practice Performance Checklist

Managing Local Files with Nautilus

In this lab you will use the Nautilus file manager to manipulate sample files as **student**.

- ☐ Log into the GNOME desktop as the user **student**.

  At the GNOME login screen click on the **student** user account then provide **student** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Once the GNOME desktop appears, open the folder called **Labs**. Double-click the **Nautilus Lab Setup** launcher. It will ask for confirmation then create several files you will manipulate in this practice exercise.

  Double click the **Labs** icon on the GNOME desktop then double click the **Nautilus Lab Setup** icon in the window that appears.

- ☐ Open **student**'s home folder.

  Double click the **student's Home** icon on the GNOME desktop.

- ☐ Create a folder called **targetdir** under student's home folder.

  Right-click the background inside the student home folder window, select **Create Folder**, and type **targetdir** as the folder name.

- ☐ Copy the file **original1.txt** from student's home folder into **targetdir** without changing the name of the file.

  Click and hold left mouse button on **original1.txt**, press and hold the **Alt** key, drag-and-drop the file on the **targetdir** folder. Select **Copy Here** when prompted.

- ☐ Create a link from **original2.txt** in student's home folder into **targetdir** with the same name.

  Left-click and hold the mouse button on **original2.txt**, press and hold the **Alt** key, drag-and-drop the file on the **targetdir** folder. Select **Link Here** when prompted.

- ☐ Move the file **original3.txt** from student's home folder into **targetdir**.

  Drag-and-drop the **original3.txt** file on the **targetdir** folder.

- ☐ Change the name of **original9.txt** to **original4.txt**. It should remain in student's home folder.

  Right-click the **original9.txt** file, select **Rename**, and type **original4.txt** as the new file name.

- ☐ Delete the file called **original5.txt** from student's home folder.

  Right-click the **original5.txt** file and select **Move to Trash**.

- ☐ Delete the folder called **originaldir** from student's home folder.

  Right-click the **originaldir** folder and select **Move to Trash**.

- ☐ Reclaim the disk space used by the file and folder you just deleted in the previous two steps.

  Right-click the trash can in the lower-right corner and select **Empty Trash**. Click the **Empty Trash** button in the confirmation dialog box that appears.

Practice Performance Checklist

Managing Remote Files with Nautilus

Start the **Connect to Server** window to select a remote server. Using the Nautilus window that appears, you can access remote files and copy files to and from the server.

- ☐ Log into the GNOME desktop as the user **student**.

  At the GNOME login screen click on the **student** user account then provide **student** when prompted for the password. Click **Log In** once the password has been typed in.

- ☐ Select **Places** → **Connect to Server...** from the top panel.

- ☐ From the **Connect to Server** window, choose the following:
  - **Server type** - Choose **SSH**
  - **Server** - Enter serverX where *X* is replaced by your desktop number (for example, server12 if your desktop were desktop12)
  - **Folder** - Enter **/home/student**
  - **User Name** - Enter **student**

- ☐ Select **Connect**. If this is the first time this user has connected, you will be prompted to accept the SSH key. Click the **Log In Anyway** button to continue.

- ☐ Enter **student** as the password and check the **Forget password immediately** button. A Nautilus window opens, displaying the contents of the selected remote folder (it may be empty).

- ☐ Disconnect the folder from the remote system, serverX.

  Right-click on the **sftp for student on serverX** icon on the GNOME desktop and select **Unmount**. The icon and any open windows associated with it should disappear once the remote folder has been disconnected.

Test

Criterion Test

Performance Checklist

Copy, Move, and Remove Remote Files

Once you have opened a connection to a remote folder, use your mouse and keyboard to work with the files and folders available from the remote server.

- ☐ From your desktopX machine, open **student**'s home folder on serverX using SSH. The password for **student** is **student**.

  1. Click **Places** → **Connect to Server** and fill in the following values:

     - **Service Type:** SSH
     - **Server:** serverX
     - **Folder:** /home/student
     - **User Name:** student

     Then click **OK**.

  2. If this is the first time you are connecting to your server, you will be presented with a dialog box asking to confirm the server's host key. In this case, click **Log in Anyway**.

  3. Enter **password** when prompted for the password.

- ☐ Open the desktopX **student**'s home folder.

  Double click the **student's Home** icon on the GNOME desktop.

- ☐ Create a folder called **nautilus-test** in the serverX student's home folder.

  Right-click in the window that was created in the first step, select **Create Folder**, and enter **nautilus-test** for the name.

- ☐ Copy the file **original1.txt** from student's desktopX home folder into the serverX **nautilus-test** folder without changing the name of the file.

  Use your mouse to drag-and-drop **original1.txt** from student's home folder (on desktopX) onto the **nautilus-test** folder in student's home folder (on serverX).

- ☐ From **student**'s desktopX home folder, open the **targetdir** folder and move the file **original3.txt** to the serverX **student**'s home folder.

  Click and hold on **original3.txt**, press and hold the **Alt** key, and drag-and-drop the file on the new folder. When prompted, select **Move Here**.

- ☐ Change the name of **original3.txt** to **original9test.txt**. It should remain in **student**'s home folder on serverX.

Right-click the **original3.txt** file and select **Rename**. Change the highlighted folder name to **original9test.txt**. It should remain in student's home folder on serverX.

☐ Delete the file called **original8.txt** from the serverX **student**'s home folder.

Right-click the file called **original8.txt** in the student's home folder (serverX) and select **Move to Trash**. View the warning and choose either Delete or skip deleting the file. If you delete it, no copy of the deleted file is kept in the local Trash.

☐ Close both windows when you are done.

Warning

If you are using the Red Hat Virtual Training environment, be careful not to use the **Ctrl+q** hotkey to close Nautilus windows. While convenient, it may also close your client application.

Notice that an icon representing the connection to the remote folder stays on the desktop (named **sftp for student on serverX**). Double-click that icon if you want to open the remote folder again. Right-click and select **Unmount** if you want to remove the icon from your desktop.

☐ Connect to the **ftp** windows share on **instructor.example.com** as **guest20XX** where *XX* is your desktop number. The password is **password**.

1. Click **Places** → **Connect to Server** and fill in the following values:
   - **Service Type:** Windows share
   - **Server:** instructor
   - **Share:** ftp
   - **User Name:** guest20XX

   Then click **Connect**.
2. In the resulting dialog box, enter **password** for the password, leave all other fields unchanged, and click **Connect**.

☐ Copy the file **example-ca.crt** from the share to the desktop on your local machine.

This is the default behavior when you drag-and-drop a file from a remote folder.

- ☐ Right-click the **ftp on instructor** folder on your desktop and select **Unmount** to disconnect from the share.

Get Help in a Graphical Environment

Practice Quiz

Researching Local Documentation

1. Which document, with section reference, describes in detail what panel applets are in the GNOME desktop?

   GNOME Desktop User Guide, Section 4.4: Applets

2. Which document, with section reference, describes how to copy and paste in the graphical text editor?

   Gedit Manual, Section 4.1: Editing Text

3. Which document, with section reference, describes the various ways to add a launcher to a GNOME panel.

   GNOME Desktop User Guide, Section 4.5.1: Adding a Launcher to a Panel

4. Which document, with section reference, describes the shortcut keys for the Gedit text editor?

   Gedit Manual, Section 8: Shortcut Keys

5. Which document, with section reference, describes what each mouse buttons does when using GNOME?

   GNOME Desktop User Guide, Section 1.1.1: Mouse Button Conventions

6. Which document, with section reference, describes how to get started writing notes using the panel applet?

   Gnote Manual, Section 2: Getting Started

Practice Resequencing Exercise

Working with Red Hat Global Support Services

Below are the steps taken when interacting with Red Hat Global Support Services. Mark the order the steps should be taken:

4 Gather relevant diagnostic info (log information, core dumps, etc.)
1 Define the problem
6 Contact Red Hat via phone or web
5 Determine the severity level
3 Gather background information
2 Search documentation and kbase articles

Test

Criterion Test

Consult local documentation (not the Internet) to answer the following questions.

Quiz

Get Help in a Graphical Environment

1. What is "browser mode" in the graphical file manager (Nautilus)? Browser mode is similar to Windows Explorer. The current window changes when going into a subdirectory rather than having a new window opened.

   How do you start "browser mode"? Right click on a folder and select Browse Folder.

   Where did you find the answer? Desktop User Guide, section 6.3 - Browser Mode.

2. How can Nautilus be configured to always open folders in browser mode? Open Nautilus. Select **Edit** → **Preferences** then click the Behavior tab. Check box by Always open in browser windows.

   Where did you find the answer? Desktop User Guide, section 6.12.2 - Behavior Preferences

3. Which document provides more information on how to use the **`gedit`** text editor? Use the search function to answer this question. Gedit Manual Search for **`gedit`** and the manual is the first choice presented.

4. What are the two default key shortcuts for taking screen shots? Print Screen (captures whole display) and Alt-Print Screen (captures current window only).

   Where did you find the answer? Desktop User Guide, section 7.2 - Taking screenshots or section 1.2.1 - Global shortcut keys

5. What are workspaces? Workspaces are virtual screens with the same desktop panels and functionality, but they allow different windows and applications to be active in them.

   What are the keyboard shortcuts used to switch between workspaces? Shortcut keys, Ctrl-Alt-Left Arrow and Ctrl-Alt-Right Arrow switch workspaces.

   Where did you find the answers? Desktop User Guide, section 2.4 - Workspaces and section 2.4.1 - Switching between workspaces

Configure Local Services

Practice Quiz

The Role of the root User

Complete the chart below with the similarities and differences between the Linux **root** user and the Windows Administrator user.

Linux **root** user	Windows **Administrator** user
Used for administration tasks	Used for administration tasks
Does not log in directly	Usually log in directly
Does not always display a dialog requesting elevated privileges (e.g., command-line access)	Displays a dialog when elevated privileges are needed
Privilege not given to other accounts	Privilege often given to other accounts

Table A.1. T-chart

Practice Performance Checklist

Manage the System Clock

Perform the following steps on serverX unless directed otherwise.

- ☐ Configure serverX to synchronize with instructor.example.com using NTP.
  1. Launch the Date & Time management tool.
  2. Click the Date and Time tab.
  3. Enable NTP, point to **instructor.example.com**.
  4. Synchronize clock immediately.
- ☐ Set the timezone to the appropriate setting for your locale.
  1. Click the Time Zone tab.
  2. Set the timezone for your locale.
- ☐ Make the hardware clock store UTC time.
  1. On the Time Zone tab, select UTC.

Practice Group Exercise

Manage Print Queues

Perform the following steps on serverX unless directed otherwise.

1. Create a local print queue and share it with other systems. Name the print queue **`local`** and make it a PostScript printer that points to either the serial or parallel port on your system.

   Run the print utility: **System** → **Administration** → **Printing**

   Click on the New button. If you have a serial port, highlight **Serial Port #1**, otherwise, highlight **Parallel Port #1**. Click the Forward button.

   Generic should be highlighted, so click the Forward button. Change the model to **PostScript Printer** and click the Forward button.

   Change the **Printer name** to **`local`**. Click the Apply button. Click No when asked to print a test page.

   To share the printer, go to **Server** → **Settings**. Check the **Publish shared printers connected to this system** checkbox. Click OK and click OK again when reminded about the firewall.

   Verify that the **`local`** printer is shared. Right-click on the **`local`** printer and choose **Properties**. Highlight **Policies** in the left pane and ensure the **Shared** checkbox is checked.

2. After your partner has configured his or her printer, create a second print queue on your system that points to your partner's **`local`** print queue. Name the print queue **`remote`** and make it a raw print queue that forwards jobs to your partner's **`local`** print queue.

   This would be simple if the name of the queue were not **`remote`** because the printer should already show up as **`local@192.168.0.Y+100`**. To give the remote printer a new name, you must go through the steps of creating a new printer. Click on the New button. Click on the **Network Printer** drop-down menu in the left pane. Choose **Find Network Printer**. In the **Host:** box, enter the name of your partner's system: **`serverY.example.com`** and click Find. It should populate the **Queue:** with **`/printers/local`**. Click Forward. Change the **Printer Name** to **`remote`** and click Apply.

3. When you finish, print some text files to **`local`** and **`remote`** to verify.

Note

If you are using a serial port, the print jobs are sent to it almost immediately and cleared, so it may be difficult to verify that your print queues are working properly. If this is the case, use the "count" files (e.g., **`c00001`**, **`c00002`**, etc.) in **`/var/spool/cups/`** to verify. There will be a new count file created every time a print job goes through the queue.

Open **Firefox** or **Gedit** and print something (**`Ctrl`**+**`p`**). Send at least one job to the **`local`** printer and one job to the **`remote`** printer.

Practice Performance Checklist

Print Job Management

Perform the following steps on desktopX unless directed otherwise.

- ☐ Disable the default print queue on your system.

  Run the print utility: **System** → **Administration** → **Printing**

  Locate the default print queue (it should have a checkmark in a green circle). Right-click on the default printer and choose **Properties**. Highlight **Policies** in the left pane and uncheck **Enabled** under **State** in the right pane. Click OK.

- ☐ Submit a print job to the print queue.

  Open **Firefox** or **Gedit** and print something (**`Ctrl`**+**`p`**). Send the job to the **`local`** printer.

- ☐ List the jobs in the default print queue.

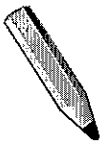
  Right-click on the default printer in the printer utility and choose **View Print Queue**.

- ☐ Cancel the print job you just submitted.

  Right-click on the pending job and choose **Cancel**. Click Yes to confirm you want to cancel the job. Close the print status application.

- ☐ Enable the default print queue

  In the printer utility, right-click on the default printer and choose **Properties**. Highlight **Policies** in the left pane and check **Enabled** under **State** in the right pane. Click OK.



Test

Criterion Test

Exercise

Configure and Manage a Printer

Perform the following steps on desktopX unless directed otherwise.

1. Configure a network printer to send print jobs to an IPP print queue on instructor.example.com called /printers/printer*X* where *X* is your desktop number.

   Open the printer utility (**System** → **Administration** → **Printing**).

Click **New**. Expand **Network Printer** in the left pane. Select **Internet Printing Protocol (ipp)** and enter **`instructor.example.com`** as the **Host** and **`/printers/printerX`** as the **Queue**. Alternately, you could select **Find Network Printer** and enter **`instructor.example.com`** as the hostname, then click **Find**. Make sure **`/printers/printerX`** is in the **queue**, then click **Verify**.

Note

You must enter a fully-qualified domain name when searching for a network printer, or CUPS may not find it.

Once you have entered and verified the printer, click **Forward**.

2. Your print queue should be called **`remote-testX`** (where *X* is your station number) and should be the default print queue. Use **`PostScript Printer`** as the model.

   Choose **`Generic`** as the printer and click **Forward**. Choose **`PostScript Printer`** as the model and click **Forward**. Enter **`remote-testX`** as the **Printer Name** and click **Forward**.

   If **`remote-printer`** is not the default, right-click on **`remote-testX`** and choose **Set As Default**.

3. Once you have completed your work, open the **Labs** folder on your GNOME desktop and double click the **Printer Management Grading** icon.

Get Started with Bash

Practice Quiz

Bash Syntax

1. Options modify how a command will work and begin with - or --.
2. Optional, additional parameters are called arguments and are enclosed by [ ] in Linux documentation.
3. The following usage notation,

   `--create|--list|--extract`

   indicates what about the options?

   Exactly one of the three options given may be used.

Useful Bash Features

What are two useful shell features demonstrated by your instructor?

1. Tab completion - allows you to complete commands once you have typed enough to make it unique.
2. Shell history - allows you to view commands previously run and edit or execute them.

Practice Performance Checklist

Using Bash

- ☐ Log in graphically to your serverX host as **student**.
- ☐ Open a terminal window.

  To open a Terminal window, select **Applications** → **System Tools** → **Terminal**.

  ```
  [student@serverX ~]$
  ```

- ☐ Switch your shell prompt to run as the **root** user.

  ```
  [student@serverX ~]$ su -
  Password: redhat
  [root@serverX ~]#
  ```

- ☐ Change the password of the **visitor** account to **visitor**.

  ```
  [root@serverX ~]# passwd visitor
  ```

```
Changing password for user visitor.
New password: visitor
BAD PASSWORD: it is based on a dictionary word
BAD PASSWORD: is too simple
Retype new password: visitor
passwd: all authentication tokens updated successfully.
```

- Exit the **root** shell.

```
[root@serverX ~]# exit
[student@serverX ~]$
```

Practice Performance Checklist

Launching Graphical Tools from Bash

- Log in to your serverX host graphically as **student**.

- Open a terminal window.

  To open a Terminal window, select **Applications** → **System Tools** → **Terminal**.

- Within the window switch to a **root** shell.

```
[student@serverX ~]$ su -
Password: redhat
[root@serverX ~]#
```

- Launch **nautilus** in the foreground from the command line.

```
[root@serverX ~]# nautilus
```

- Use the keyboard shortcut to get your shell prompt back without terminating the process.

```
[root@serverX ~]# nautilus
 Ctrl+z
[1]+  Stopped                 nautilus
```

- Put **nautilus** in the background.

```
[root@serverX ~]# bg
[1]+ nautilus &
```

- List your current shell jobs.

```
[root@serverX ~]# jobs
[1]+  Running                 nautilus &
```

- ☐ Exit the root shell.

```
[root@serverX ~]# Ctrl+d
[student@serverX ~]$
```

Test

Criterion Test

Performance Checklist

Get Started with Bash

From a Terminal window, use the bash shell to launch a Nautilus file manager as root user. Copy a file and create a folder in Nautilus.

- ☐ Log in to your serverX host as **student**.

- ☐ Open a Terminal window and become **root**.

  To open a Terminal window, select **Applications** → **System Tools** → **Terminal**.

```
[student@serverX ~]$ su -
Password: redhat
[root@serverX ~]#
```

- ☐ Launch **nautilus** from the command line.

```
[root@serverX ~]# nautilus &
```

- ☐ Navigate to the **/etc** folder and copy **issue** to **issue.backup**.

  From the Nautilus window, select **File** → **Open Location**.

  Type **/etc** into the Location field and click Open.

  Right-click on the **issue** file and select **Copy**.

  Right-click in the **/etc** folder and select **Paste**.

  Right-click the copied **issue** file, select **Rename**, type **issue.backup** and press **Enter**.

- ☐ Create a new folder called **/usr/local/music**.

  From the **Nautilus** window, select **File** → **Open Location**.

  Type **/usr/local** and select Open. A **Nautilus** window opens to the **/usr/local** folder.

  Right-click in the **Nautilus** window that is open to the **/usr/local** directory and select **Create Folder**.

Type **music** as the name of the folder and press **Enter**.

Manage Physical Storage I

Practice Quiz

Physical Storage Concepts

1. The IBM PC disk architecture supports how many primary partitions maximum?

   (select one of the following...)
   a. 2
   b. 4
   c. 15
   d. 32

2. Which of the following ***cannot*** be formatted and used as a file system?

   (select one of the following...)
   a. Primary partition
   b. Extended partition

      Primary and logical partitions can be formatted with file systems, so answers a, c, and d are incorrect. Extended partitions cannot be formatted with file systems because they are partitions which contain other partitions, so b is the correct answer.
   c. Logical partition
   d. All of the above
   e. None of the above

Practice Quiz

List Available Disk Devices

Use **Disk Utility** on your desktopX workstation to answer the following questions:

1. /dev/sda is the Linux device name for the first hard drive on your desktopX.example.com machine.

2. Is there free space available on that device? If so, how much? There should be free space available on the device. The amount of free space will vary based on the size of the disk.

Practice Quiz

List Available Disk Devices (Redux)

Before you begin, reset the serverX virtual machine. Log into your desktopX workstation as **student** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reset your virtual server's storage and boot it after a fresh installation.

Use **Disk Utility** on your serverX virtual server to answer the following questions:

1. /dev/vda is the Linux device name for the first hard drive on your serverX.example.com machine.

2. Is there free space available on that device? If so, how much? Yes - approximately 1.4 GB

Test

Criterion Test

Case Study

Configure Partitions and File Systems Persistently

Before you begin...

Login as **student** on desktopX. When the GNOME desktop appears, open the folder called **Labs**. Double-click on the **Physical Storage Lab Setup** launcher. A window will appear confirming you want to reset your virtual machine. Type **y**.

Double click the **Labs** icon on the GNOME desktop then double click the **Physical Storage Lab Setup** icon in the window that appears.

When a colleague built your server - serverX, they didn't use all of the available disk space to permit future growth. A persistent area for storage needs to be created separate from your existing Linux file system hierarchy.

Create a new partition on your hard disk that is 1 GB in size and leave at least a small amount of disk space unused. It should *not* be encrypted and it should contain an ext4 file system that mounts under the **/extras** mount point persistently when the system boots.

Once you have completed your work, reboot serverX. Log into it as **student**, open the **Labs** folder and double click the **Physical Storage Grading** icon to confirm that you have completed the lab correctly.

1. Login as **student** on your desktopX workstation. Use the Virtual Machine Manager to login as **root** on your serverX virtual machine to perform system administration functions.

Important

Although this solution has you log in as root in order to complete the exercise, a better solution would be similar to the one for the assessment where you logged in as student and used **su** to run selected shell commands as root. The only disadvantage of that approach is that it requires some knowledge of the shell to execute.

- Select **Applications** → **System Tools** → **Virtual Machine Manager** from the GNOME menus in desktopX. Open the console to the vserver virtual machine. Double-click the **vserver** icon.

- Login as **root** on serverX. At the serverX.example.com graphical login screen, click **Other...**. In the **Username** field, type **root** then click the **Log In** button. Provide **redhat** in the **Password** field, then click the **Log In** button again.
- A warning dialog box will appear. Logging in graphically as **root** should generally be avoided. For now, click the **Close** button to get **root** access.

2. Run the Disk Utility.

   On serverX select **Applications** → **System Tools** → **Disk Utility** from the GNOME desktop menu.

3. Create a new partition that is 1 GB. Use an ext4 file system and leave the **Encrypted** box unchecked. Create an extended and logical partition if necessary.

   - In the **Disk Utility** window, select the storage device representing your hard disk. On serverX, the device is represented by **/dev/vda** and should appear as a **6.4 GB Hard Disk** in the **Storage Devices** frame.
   - Click in the **Free** area under the **Volumes** bar.
   - Click **Create Partition**.
   - On the **Create partition on** window, use the **Size** slider or box to select the size (1 GB), select the **Type** (Ext4), the **Name** (extras), and ensure that **Take Ownership** is checked and **Encrypt Underlying Device** is unchecked. Then select **Create**.
   - The new partition and device should appear in the **Volumes** bar. Note the device name (probably **/dev/vda3**).
   - Close the Disk Utility window.

4. Use Nautilus to create the **/extras** mount point.

   Double-click the **Computer** icon on the GNOME desktop then open the **Filesystem** folder. Right-click, then select **Create Folder** and type **extras** for the new folder name.

5. Put an entry in **/etc/fstab** (being careful not to change any other entries):

   ```
   /dev/vda3   /extras   ext4   defaults   1 2
   ```

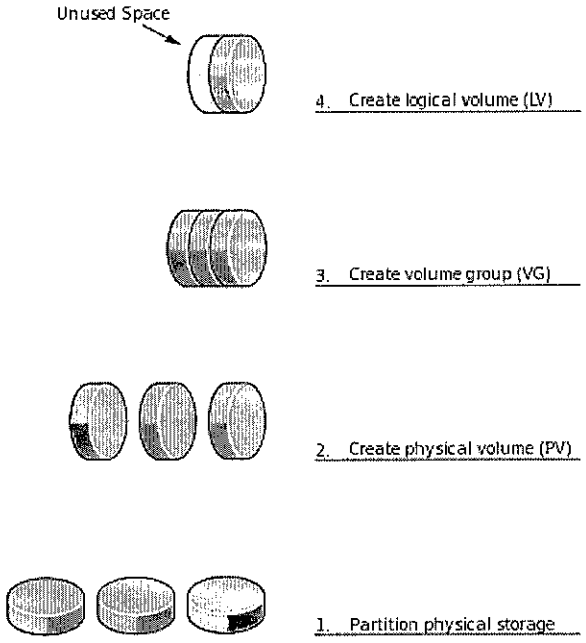
   - Launch gedit by selecting **Applications** → **Accessories** → **gedit Text Editor** from the GNOME desktop menu. Click the **Open** button, navigate to the **/etc** folder, select the **fstab** file, then click the **Open** button.
   - Add the text above to the bottom of the file. Double check your typing to make sure it is correct.
   - Click the **Save** button to commit your changes. Close the gedit window since you are finished editing text files.

6. Mount the new file system and confirm it mounted properly.

Launch the Disk Utility application. Select the **6.4 GB Hard Disk** in the **Storage Devices** frame. Select **extras** in the **Volumes** bar then click the **Mount Volume** button. "Mounted at /extras" should appear beside the **Mount point** field.

7. Once you have completed your work, reboot serverX. Log into it as **student**, open the **Labs** folder and double click the **Physical Storage Grading** icon to confirm that you have completed the lab correctly.

Manage Logical Volumes



Practice Resequencing Exercise

General LVM Concepts and Terms

2 Create physical volume(s)
1 Create physical partition(s)
4 Create logical volume(s)
3 Create volume group

Search & Learn: LVM

In this section, we will have a short activity that will give you a chance to explore the graphical **Logical Volume Management** utility, **`system-config-lvm`**. You will have about five minutes to explore the utility before working on the quiz on the next page.

Note

Do not make any changes to your configuration at this point.

The following steps are to be performed on your serverX machine.

1. Open the Logical Volume Management tool: **System** → **Administration** → **Logical Volume Management.**
2. Examine the physical volumes and how they are used.
3. Examine the volume group that is defined and its logical volumes.

Practice Quiz

Displaying Current LVM Usage

Perform the following steps on serverX unless directed otherwise.

1. What is the name of your volume group? vgsrv
2. What is the total size of the volume group? 4.47 GB
3. How much, if any, unused space is in the volume group? 384 MB
4. How many total and free physical extents does the volume group have? 143 total and 12 free physical extents
5. How big is each physical extent in the volume group? 32 MB

Steps to Deploy Logical Volumes

Work as a class to complete the following list of steps required to create logical volume storage. Some of the steps have been provided, but you will need to write in the missing steps. The completed list of steps is available in the Solutions appendix of this student guide.

1. Create a New Partition (Review)

a. Use Disk Utility to create a new empty partition (without a file system).

b. Edit the new partition and change its type to Linux LVM (0x8e)

c. Optionally reboot to incorporate partition changes.

2. Initialize the New Partition As an LVM Physical Volume

a. Select **System** → **Administration** → **Logical Volume Management** from the GNOME desktop menus.

b. Expand the **Uninitialized Entities** in the left pane.

c. Expand the disk with the new partition.

d. Select the new partition (make sure the partition type is 0x8e in the right pane).

e.

Click the **Initialize Entity** button.

f. Confirm by clicking **Yes**.

3. Create a Volume Group Using the New Physical Volume

a. Click the **Create new Volume Group** button.

b. Specify the **Volume Group Name**.

c. Click **OK**.

4. Create a Logical Volume within the New Volume Group

a. Expand the new volume group.

b. Select **Logical View**.

c. Click the **Create New Logical Volume** button.

d. Specify the logical volume name.

e. Specify the logical volume size or click the **Use remaining** button.

f. Specify file system properties such as file system type, mount point, etc.

g. Click **OK**.

h. Confirm to create the mount point when necessary.

Practice Performance Checklist

Initial LVM Deployment

Before you begin...

Reset the serverX virtual machine. Log into your desktopX workstation as **student** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reset your virtual server's storage and boot it after a fresh installation.

Perform the following steps on serverX unless directed otherwise. Perform all physical partitioning so additional partitions can be created if needed.

☐ Create a new partition of type Linux LVM (0x8e) that is approximately 400 MB in size.

1. Launch the Disk Utility application by selecting **Applications** → **System Tools** → **Disk Utility** from the GNOME desktop menus.

2. Select the **6.4 GB Hard Disk** entry in the left pane. It represents the entire hard drive for the virtual machine (**/dev/vda**).

3. Select **Free** in the **Volumes** bar. Click the **Create Partition** button. Select **406 MB** for the **Size**. Select **Empty** for **Type**. Click the **Create** button. If a dialog box appears and asks for authentication, provide the root password (**redhat**).

4. Select the new **Unknown partition** in the **Volumes** bar then click the **Edit Partition** button. Select **Linux LVM (0x8e)** from the **Type** menu then click the **Apply** button. Close the **Disk Utility** window.

- ☐ Initialize the new partition as a physical volume.

  1. Select **System** → **Administration** → **Logical Volume Management** from the GNOME desktop menus. If an authentication window appears, provide **redhat** in the **Password** field then click the **OK** button.

  2. Expand the **Uninitialized Entities** entry in the left pane, then expand the **/dev/vda** disk device. Select **Partition 3** and confirm the **Partition Type** is **Linux LVM (0x8e)**.

  3. Click the **Initialize Entity** button, then confirm that you want to format that device. **Partition 3** should appear in the **Unallocated Volumes** list in the left pane if everything was done correctly.

- ☐ Use the physical volume to create a new volume group called **vg.learn**.

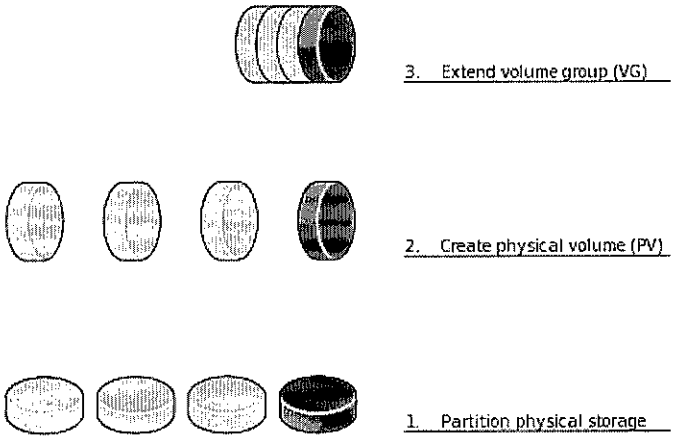
  Click the **Create new Volume Group** button at the bottom of the center pane. Type **vg.learn** in the **Volume Group Name** field then click **OK**. **vg.learn** should appear in the list of **Volume Groups** in the left pane.

- ☐ Create a logical volume called **data** within **vg.learn** that consumes all physical extents. It should contain an ext4 file system that mounts as **/data** persistently.

  Select **Logical View** under **vg.learn** in the left pane.

  Click the **Create New Logical Volume** button at the bottom of the center pane. Type **data** in the **LV name** field. Click the **Use Remaining** button to determine the **LV size**. For the **Filesystem** select ext4, check both the **Mount** and **Mount when rebooted** checkboxes, and specify **/data** in the **Mount point** field. Click **OK**. If a dialog window appears asking to create the mount point, confirm it is **OK** to create the mountpoint if necessary.

- ☐ Use Nautilus to browse to **/data** and confirm it exists with a **lost+found** folder as its only contents.



Steps to Extend a Volume Group

1. Click the **Add to existing Volume Group** button.
2. Select the desired volume group in the dialog box.
3. Click the **Add** button.

Practice Performance Checklist

Extending a Volume Group

Perform the following steps on serverX unless directed otherwise.

- ☐ Create a new partition of type Linux LVM (0x8e) that consumes all remaining disk space.
  1. Launch the Disk Utility application by selecting **Applications** → **System Tools** → **Disk Utility** from the GNOME desktop menus.
  2. Select the **6.4 GB Hard Disk** entry in the left pane. It represents the entire hard drive for the virtual machine (**/dev/vda**).
  3. Select **Free** in the **Volumes** bar. Click the **Create Partition** button. By default the **Size** field specifies all available space on the disk. Select **Empty** for **Type**. Click the **Create** button. If a dialog box appears and asks for authentication, provide the root password (**redhat**).
  4. Select the new **Unknown partition** in the **Volumes** bar then click the **Edit Partition** button. Select **Linux LVM (0x8e)** from the **Type** menu then click the **Apply** button. Close the **Disk Utility** window.
- ☐ Initialize the new partition as a physical volume.

1. Select **System** → **Administration** → **Logical Volume Management** from the GNOME desktop menus. If an authentication window appears, provide **redhat** in the **Password** field then click the **OK** button.
2. Expand the **Uninitialized Entities** entry in the left pane, then expand the **/dev/vda** disk device. Select **Partition 4** and confirm the **Partition Type** is **Linux LVM (0x8e)**.
3. Click the **Initialize Entity** button, then confirm that you want to format that device. **Partition 4** should appear in the **Unallocated Volumes** list in the left pane if everything was done correctly.

☐ Add the physical volume to the **vg.learn** volume group.

Click the **Add to existing Volume Group** button at the bottom of the middle pane. Select the **vg.learn** volume group then click **Add**.

Steps to Extend a Logical Volume and Its File System

1. Open the Logical Volume Management tool: **System** → **Administration** → **Logical Volume Management**.
2. Browse the logical devices in the left pane and select the logical volume you want to extend.
3. Click the **Edit Properties** button.
4. Specify the logical volume size or click the **Use remaining** button.
5. Click **OK**.

Practice Performance Checklist

Extending a Logical Volume

Perform the following steps on serverX unless directed otherwise.

☐ Open a Nautilus browser window, and navigate to the **/data** directory. Note the "available space" in the lower lefthand corner.

☐ Grow the data logical volume and its file system (**/data**) by 200 MB so it is a total size of about 600 MB.

1. Select **System** → **Administration** → **Logical Volume Management** from the GNOME desktop menus. If an authentication window appears, provide **redhat** in the **Password** field then click the **OK** button.
2. Expand the entry for **vg.learn** and expand its **Logical View** in the left pane.
3. Select the **data** entry below the **Logical View**. Click the **Edit Properties** button.

4. Adjust the slider bar under **Size** so the logical volume size is approximately 0.6 GB. Click the **OK** button.

☐ Re-examine the "available space" in the Nautilus browser window for the **/data** directory. Confirm that more space is now available.

Steps to Remove a Physical Volume

1. Open the Logical Volume Management tool: **System** → **Administration** → **Logical Volume Management**.
2. Browse the logical devices in the **left** pane and select the logical volume you want to remove.
3. Select all groups of logical volume extents on the device.
4. Click the **Migrate Selected Extent(s) From Volume** button.
5. Click the **Remove Volume from Volume Group** button.

Practice Performance Checklist

Removing a Physical Volume

Perform the following steps on serverX unless directed otherwise.

☐ Migrate all physical extents from the original partition that was used to create the **vg.learn** volume group.

1. Launch **System** → **Administration** → **Logical Volume Management** if it isn't already running.
2. Expand the entry for **vg.learn**, expand its **Physical View**, then expand the **/dev/vda** entry in the left pane.
3. Select the **Partition 3** entry below **/dev/vda** then highlight the **data Linear Mapping** in the center pane by clicking on it.
4. Click the **Migrate Selected Extent(s) From Volume** button. Click the **OK** button.

☐ Remove the original partition from the **vg.learn** volume group.

With the **/dev/vda3** physical volume still selected, click the **Remove Volume from Volume Group** button. Click **Yes** when the confirmation dialog box appears.

☐ Remove the physical volume from LVM.

1. Expand the entry for **Unallocated Volumes** then expand the **/dev/vda** entry in the left pane. Select the **Partition 3** entry below **/dev/vda**.

2. Click the **Remove volume from LVM** button. Click **Yes** when the confirmation dialog box appears.

Test

Criterion Test

Case Study

Manage Logical Volumes

Before you begin...

Login as **student** on desktopX. When the GNOME desktop appears, open the folder called **Labs**. Double-click on the **Logical Volume Lab Setup** launcher. A window will appear confirming you want to reset your virtual machine. Type **y**.

Double click the **Labs** icon on the GNOME desktop then double click the **Logical Volume Lab Setup** icon in the window that appears.

You have just been assigned to administer a freshly installed server - serverX. Management would like some adjustments made to the disk allocation according to the following specifications:

- The **/home** file system is too small and should be expanded to take 500 MB total space.
- Use the remaining disk space to create a volume group called **extra** with a logical volume called **iso** that contains an ext4 file system that will be mounted as **/iso**. Allocate the file system so it can be migrated to a larger device and grown without down time.

When you have completed the tasks, reboot serverX and run the **Logical Volume Grading** grading script.

1. To resize the **/home** file system, start by opening the Logical Volume Management window.

   On serverX, select: **System** → **Administration** → **Logical Volume Management**. Type the root password, when prompted.

2. Select the home logical volume.

   Select the down arrows next to the **Volume Group** (vgsrv), **Logical View**, and logical volume (**home**).

3. Begin editing the logical volume.

   With your **home** logical volume highlighted, select **Edit Properties**. The **Edit Logical Volume** window appears.

4. Change the size of the home logical volume to 500MB.

   Change the **LV Size** field to 0.5 Gigabytes. (Or, you may change Gigabytes to Megabytes and make the **LV Size** about 500.) Then select **OK** and close the **Logical Volume Management** window.

5. To create a new Volume Group (iso) and Logical Volume (extra) you must start by creating a new physical partition. Open the Disk Utility window on serverX, select **Applications** → **System Tools** → **Disk Utility**. Then create an LVM physical partition that consumes the all the free space.
   - In the **Disk Utility** window, select the storage device representing your hard disk. (On serverX, the device is represented by **/dev/vda** and should appear as a **Hard Disk** under **Peripheral Devices**.)
   - Click in the **Free** area under the **Volumes** bar.
   - Click **Create Partition**.
   - In the **Create Partition On** window, use the **Size** slider or box to select all remaining space and select the **Type (Empty)**. Then select **Create**. (Type the root password if prompted.)
   - Close the **Disk Utility** window.
6. Open the Logical Volume Management window.

   On serverX, select: **System** → **Administration** → **Logical Volume Management**. Type the root password, when prompted.
7. From the **Logical Volume Management** window make the new physical partition into an LVM physical volume.

   Select down arrows next to **Uninitialized Entities**, **/dev/vda** and the new partition (probably **Partition 3**). Then select **Initialize Entity**. Select **Yes** when prompted. **Partition 3** should appear highlighted under the **Unallocated Volumes** heading.
8. Using the new LVM physical partition, create a volume group called **extra**.

   With the new partition highlighted under the **Unallocated Volumes** heading, select **Create new Volume Group**. Type **extra** as the volume name and select **OK**.
9. Using the new **extra** volume group, create a logical volume called **iso**. Do not use all the available space. Set up the logical volume to mount automatically at boot time under **/iso**.
   - Select the down arrows next to **Volume Groups** and **extra**, then select **Logical View**.
   - Select **Create New Logical Volume**.
   - In the **Create New Logical Volume** window, set the following values:
     - LV Name: **iso**
     - LV size: **1GB** (be sure to leave at least a little free space)
     - Filesystem: **Ext4**
     - Check **Mount** and **Mount when rebooted**.
     - Mount point: **/iso**

- Click **OK** and select **Yes** to verify, when prompted.

10. Once you have completed your work, reboot serverX. Log into it as **student**, open the **Labs** folder and double click the **Logical Volume Grading** icon to confirm that you have completed the lab correctly.

Monitor System Resources

Practice Quiz

Monitor Running Processes

Before you begin, login to serverX as student, open the **Labs** folder and double-click the **Process Management Setup** launcher. It will create processes that you will examine and manipulate throughout this unit.

Perform the following steps on serverX unless directed otherwise.

1. Which process running on your serverX machine is currently consuming the most CPU?
   hippo
2. Which process on your serverX machine is currently consuming the most memory?
   elephant

Search & Learn: process101

In this section, we will divide up into small groups and have a short classroom activity to familiarize you with **System Monitor**. There is a process running on your system with the name **`process101`**. You will first adjust its nice value, then terminate the process, using **System Monitor**. Complete solutions are available in the appendix.

1. Change the **`nice`** value of **`process101`** to **`7`**. Write down the steps you took to make that happen:
   a. Launch System Monitor by selecting **Applications** → **System Tools** → **System Monitor**.
   b. Highlight the process in question.
   c. Select **Edit** → **Change Priority...**.
   d. Adjust the slider to the desired priority.
   e. Click the **Change Priority** button.
   f. Verify the priority in the **Nice** column.
2. Terminate the **`process101`** process. Write down the steps you took to terminate the process:
   a. Launch System Monitor by selecting **Applications** → **System Tools** → **System Monitor**.
   b. Highlight the process in question.

c. Click the **End Process** button in the bottom-right corner.

d. Click the **End Process** button in the confirmation dialog box.

e. If the process does not terminate:

   a. Highlight the process.

   b. Select **Edit** → **Kill Process**.

   c. Click on the **Kill Process** button in the dialog box to confirm

Practice Performance Checklist

Terminate and Change Process Priority

Change the priority of a CPU hog and terminate a memory hog on serverX.

Perform the following steps on serverX unless directed otherwise.

☐ Change the priority of the process called **hippo** that is using a lot of CPU resources to 5.

1. Launch System Monitor by selecting **Applications** → **System Tools** → **System Monitor**.
2. Identify the CPU intensive process by displaying all processes and sorting them by the **CPU%** field. You should see that the process called **hippo** is consuming the most CPU resources.
3. Use the mouse to select and highlight the **hippo** process.
4. Select the **Edit** → **Change Priority...** menu choice to adjust the process priority.
5. Slide the **Nice value** slider bar to the right unit 5 is selected.
6. Click the **Change Priority** button. Provide the **root** password to obtain privileges needed to terminate the process.
7. Click the **End Process** button in the confirmation window. Provide the **root** password to obtain privileges needed to terminate the process.

☐ Terminate the process called **elephant** that is using a lot of memory resources.

1. Launch System Monitor by selecting **Applications** → **System Tools** → **System Monitor**.
2. Identify the memory intensive process by displaying all processes and sorting them by the **Memory** field. You should see that the process called **elephant** is consuming the most memory resources.

3. Use the mouse to select and highlight the **elephant** process.
4. Click the **End Process** button in the lower-right corner of the monitoring tool.
5. Click the **End Process** button in the confirmation window. Provide the **root** password to obtain privileges needed to terminate the process.

☐ When you have completed the tasks, double-click the **Process Management Grading** launcher icon in the **Labs** folder on student's GNOME desktop. This will confirm if you identified and managed the correct processes.

Practice Exercise

Monitor Disk Usage

Perform the following steps on serverX unless directed otherwise.

1. Which file system has the most free disk space on serverX?

   The / file system has the most disk space.

2. Which top level directory in / uses the most space on serverX?

   The **/usr** directory is using the most space.

3. Which top level directory in **/home** uses the least space on serverX?

   /home/visitor uses the least space.

   Note: You must be root to find this information.

Test

Criterion Test

Exercise

Monitoring Processes and Filesystems

Before you begin...

Login as **student** on desktopX. When the GNOME desktop appears, open the folder called **Labs**. Double-click the **Process Management Test Setup** launcher. A window will appear confirming you want to reset your virtual machine. Type **y**. Be patient and wait a couple minutes for serverX to be prepared for this lab.

Perform the following steps on serverX unless directed otherwise.

1. Identify the process that consumes the most memory on serverX and terminate it.

   - On serverX, start the System Monitor. Select **Applications** → **System Tools** → **System Monitor**.

- Select the Processes tab, click on any Process Name shown in the left column, select View, and select All Processes.
- Click the Memory column until the processes with the highest memory usage appear at the top.
- Right-click the process name with the highest memory usage (look for a process called bloatware) and select End Process. Enter the root password if prompted.
- The process should be terminated and removed from the list of processes.

2. Identify the process that consumes the most CPU on serverX and change the priority to 10.
   - From System Monitor, select the Processes tab.
   - Click the %CPU column until the processes with the highest amount of CPU usage appears at the top (look for running-circles).
   - Right-click the name of the process with the highest CPU and select Change Priority.
   - From the Change Priority window, move the slider bar to 10 and select Change Priority. Enter the root password, if prompted.
   - If the selection worked, the nice value for the process should appear as 10.
3. Determine which file system has the least amount of available free space.
   - Select the File Systems tab.
   - Select the Free heading.
   - You should see that the **/boot** file system has the least amount of free space.
   - Close the System Monitor window.
4. Open the **/home/student/Desktop/least-free-space-filesystem.txt** file on serverX, then edit it so that only the directory that matches what you found in the previous step appears in the file.

   Run **gedit /home/student/Desktop/least-free-space-filesystem.txt** and edit the file so that only **/boot** appears in that file.
5. Determine which top level directory in **/usr** consumes the most disk space?
   - Select **Applications** → **System Tools** → **Disk Usage Analyzer**.
   - Click the Select Folder button, browse to the /usr folder, and select the Size column until the highest disk usage folders appear at the top.
   - You should see that the **/usr/share** directory consumes the most space.
6. Open the **/home/student/Desktop/usr-directory.txt** file on serverX, then edit it so that only the directory that matches what you found in the previous step appears in the file?

Run **`gedit /home/student/Desktop/usr-directory.txt`** and edit the file so that only **`/usr`** appears in that file.

7. When you finish, double-click the **Process Management Test Grading** icon in the **Labs** folder on the GNOME desktop to confirm that you have completed the lab correctly.

Manage System Software

Practice Quiz

Red Hat Network Registration

1. The graphical tool that begins the registration with the Red Hat Network is **`rhn_register`**.
2. The first registration choice determines whether a system registers with Hosted RHN or RHN Satellite.
3. Optionally additional web proxy server and authentication information may need to be be provided.
4. An RHN user name or RHN account and its matching password must be provided for successful Red Hat Network registration.
5. The last questions to be answered during the registration process are system name and whether to upload hardware and software or package profile information.

Practice Case Study

Software Management

Before you begin...

Reset the serverX virtual machine. Log into your desktopX workstation as **`student`** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reboot your virtual server and reset its storage back to the original state when it was first installed.

Perform the following steps on serverX unless directed otherwise.

You have a new server to administrate that has very specific software requirements. It must have the latest version of the following packages installed (including any dependencies):

xsane (new package)

gimp (new package)

yum (updated package)

samba-client (updated package)

For security reasons it should not have the **`vsftpd`** package installed.

Do not install all updates. Only install updates for the packages listed above if they are available.

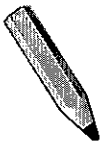
When you are ready to check your work, run the **`Software Management Grading`** script in the **Labs** folder on serverX.

1. On serverX, run the **Add/Remove Software** application (**System** → **Administration** → **Add/Remove Software**). Search for the *xsane* package and check the checkbox when you find it. Search for the *gimp* package and check the checkbox when you find it. Click the Apply button to apply your changes.

2. Search for the *vsftpd* package and uncheck the checkbox when you find it. Click the Apply button to apply your changes. Click on the Remove button when asked to confirm. Close the **Add/Remove Software** application.

3. Run the **Software Update** application (**System** → **Administration** → **Software Update**). Verify that *yum* is selected and click the Install Update button.

   Run the **Software Update** application again. *Deselect* every package *except samba-client*. Click on the Install Update button.



Test

Criterion Test

Case Study

Update and Install Software

Before you begin...

Reset the serverX virtual machine. Log into your desktopX workstation as **`student`** then double-click the **Reset Virtual Server** launcher on your GNOME desktop. This will reboot your virtual server and reset its storage back to the original state when it was first installed.

Perform the following steps on serverX unless directed otherwise.

You have a new server, serverX, to administrate that has very specific software requirements. It must have the latest version of the following packages installed (including any dependencies):

kernel (existing package with an update)

xsane-gimp (new package)

yum (updated package)

bzip2 (updated package)

For security reasons it should not have the **`festival`** package installed.

Do not install all updates. Only install updates for the packages listed above if they are available.

When you are ready to check your work, run the **`Software Management Test Grading`** script in the **`Labs`** folder on serverX.

1. On serverX, run the **Add/Remove Software** application (**System** → **Administration** → **Add/Remove Software**). Search for the *xsane-gimp* package and check the checkbox when you find it. Click the Apply button to apply your changes.

2. Search for the *festival* package and uncheck the checkbox when you find it. Click the Apply button to apply your changes. Click on the Remove button when asked to confirm the package and its dependencies. Close the **Add/Remove Software** application.

3. Run the **Software Update** application (**System** → **Administration** → **Software Update**). Verify that *yum* is selected and click the Install Update button.

Run the **Software Update** application again. *Deselect* every package *except kernel* and *bzip2*. Click on the Install Updates button.

Get Help in a Textual Environment

Practice Performance Checklist

Using man

- ☐ Consult the **man** page for **gedit**(1).
- ☐ Identify how to edit a specific file using **gedit** from the command line.

  gedit ***filename***
- ☐ Determine the option you specify to cause **gedit** to begin the editing session with the cursor at the end of the file.

  gedit + ***filename***
- ☐ Consult the **man** page for **su**(1).
- ☐ Determine what **su** does when the username argument is omitted.

  su assumes the username of *root*.
- ☐ Identify how **su** behaves when a dash option by itself is specified.

  su starts a *login shell*, as opposed to a *non-login shell*.
- ☐ Consult the **man** page for **passwd**(1). Determine the options that will lock and unlock a user account when this command is used by **root**.

  passwd -l ***username***

  passwd -u ***username***
- ☐ Locate the two principles to remember according to the **passwd man** page authors. Search for the word **principle**.
- ☐ Consult the man-page documenting the syntax of the **/etc/passwd** file. What is stored in the third field of each line?

  The UID (numeric user ID) for the relevant account.

Practice Quiz

1. Which command will list detailed information about a zip archive? **zipinfo**(1) found with **man -k zip**
2. Which man page contains a list of parameters that can be passed to the kernel at boot time? **bootparam**(7) found with **man -k boot**

3. Which command is used to tune ext4 file system parameters? **tune2fs**(8) found with **man -k ext4**

Man Page vs. Info Page Navigation

Fill in the table below as your instructor presents this material. (Also see the Info nodes for **info** for review.)

Key Binding	**man** Navigation	**pinfo** Navigation
PgDn / PgUp	Read the next/previous page	Read the next/previous page
/	Search for a pattern	Search for a pattern
q	Quit reading the documentation	Quit reading the documentation
DownArrow / UpArrow	Scroll one line at a time	Move between topics for section
n	Find the next occurrence of an earlier search	Display next topic
p	N/A	Display previous topic
u	N/A	Up a level to overview

Table A.2. **man**/**pinfo** Comparison

Practice Performance Checklist

Read Documentation Using pinfo

- ☐ Invoke **pinfo** without any arguments.
- ☐ Navigate to the topic **Common options** and go to that **info** page.
- ☐ Skim through this **info** page and find out if long options can be abbreviated.
- ☐ Determine what **--** by itself means as an argument to a command.

  The expression -- is used to signify an end to command line switches and the start of "normal" arguments in cases where the distinction might not be clear.
- ☐ Without exiting **pinfo**, go up a level to the **GNU Coreutils** page.

- ☐ Go up another level to the top level page.
- ☐ Search for the pattern **nano** and enter that topic.
- ☐ Locate the topic in the **`Introduction`** entitled **`Command line options`** and skim it very quickly.
- ☐ Go up to the **`Introduction`** level then skip to the next topic.
- ☐ Exit **`pinfo`**.
- ☐ Invoke **`pinfo`** and specify **nano** as your topic/command of interest on the command line.
- ☐ Select the **`Editor Basics`** topic.
- ☐ Read the **`Entering Text`** and **`Special Functions`** subtopics.

Practice Quiz

1. Where can you find the latest news about the vim package? http://www.vim.org/

   Which file contained this information? /usr/share/doc/vim-common-version/README.txt

2. What is the URI for the wiki for the yum package? http://yum.baseurl.org/wiki

   Which file contained this information? **`/usr/share/doc/yum-`*`version`*`/`README**

3. What are the commands or utilities provided by the diffutils package? **`diff`**, **`diff3`**, **`sdiff`** and **`cmp`** according to **`/usr/share/doc/diffutils-`*`version`*`/`README**

Establish Network Connectivity

Practice Group Exercise

Essential Network Concepts

Are the following network configurations feasible? If not, what is wrong with them?

1. Scenario 1

```
IP address: 192.168.7.351
Netmask: 255.255.255.0
Gateway: 192.168.7.1
```

   Invalid IPv4 address (351) and missing DNS information

2. Scenario 2

```
IP address: 10.1.2.3
Netmask: 255.255.255.0
Gateway: 10.1.2.1
DNS server: 172.17.4.53
```

   This configuration is feasible

3. Scenario 3

```
IP address: 192.168.7.0
Netmask: 255.255.255.0
Gateway: 192.168.7.1
DNS server: 192.168.0.254
```

   IP address is invalid (a broadcast address)

4. Scenario 4

```
IP address: 10.4.5.6
Netmask: 255.255.255.0
Gateway: 10.4.6.1
DNS server: 192.168.0.254
```

   Gateway is not on the same subnet.

5. Scenario 5

```
IP address: 172.17.23.5
Netmask: 255.255.0.0
Gateway: 172.17.0.1
DNS server: 192.168.0.254
```

   This configuration is feasible.

6. Scenario 6

```
IP address: 2001:db8::219:a0ff:fe26:a221
Prefix: /64
Gateway: 2001:db8::fe
DNS server: 2001:db8:0:1::1
```

This configuration is feasible, for IPv6.

Note that the IP address is on the 2001:db8::/64 (**`2001:0db8:0000:0000::`**) network, while the DNS server is on the 2001:db8:0:1::/64 (**`2001:0db8:0000:0001::`**) network.

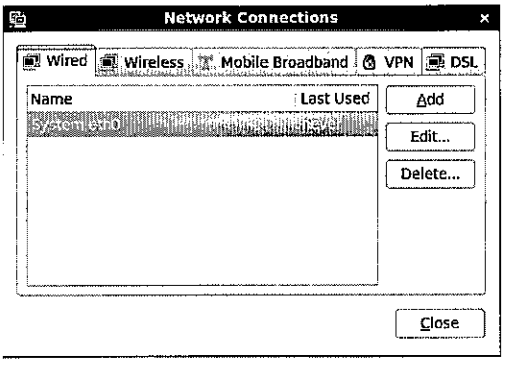
Practice Performance Checklist

Linux Network Configuration

Use **`NetworkManager`** to create a static network configuration profile for your serverX machine:

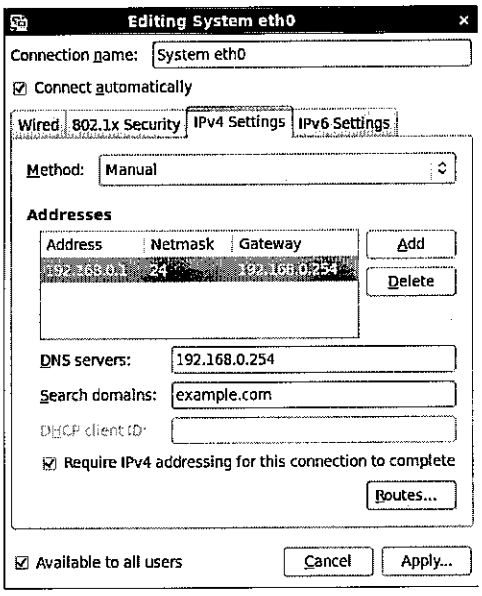
- ☐ Create a network connection called **`Wired static`**.
- ☐ Ensure that the connection will start automatically at boot.
- ☐ Define static IPv4 settings with an IP address of 192.168.0.X+100.
- ☐ Defined the netmask as 255.255.255.0.
- ☐ Set the default gateway to 192.168.0.254.
- ☐ Define the DNS server as 192.168.0.254.

1. *Right*-click on the *NetworkManager* applet icon, and choose **Edit Connections....**



2. Select **eth0** and **Edit**.
3. Navigate to the **IPv4 Setings** panel.

4. Choose a configuraiton **Method** of **Manual**.
5. **Add** a new address line.
6. Fill in the following paramaters.
   a. **Address:** 192.168.0.100+X
   b. **Netmask:** 24 (or 255.255.255.0)
   c. **Gateway:** 192.168.0.254
   d. **DNS Servers:** 192.168.0.254
   e. **Search domains:** example.com



7. **Apply** the configuration and close.

Test
Criterion Test

Case Study
Weekend Network Adjustment

Before you begin...

Although most of the work is done on your serverX machine, execute the **`lab-setup-netconfig`** script on desktopX before beginning the criterion test.

The network administrator spent last weekend making changes to the office network. Somehow the memorandum notifying the network users of the changes didn't get published before the changes were made.

Configure your Linux server to communicate with the new network configuration.

First, lets see if the problem can be fixed by re-starting the network interface. Click on the **Network Manager** icon in the upper right, and then click on "System eth0". This will attempt to re-connect to the network using your current settings. Confirm that even with the restarted interface, you still have difficulty accessing the instructor machine. Some useful commands might include **ping** and **host**

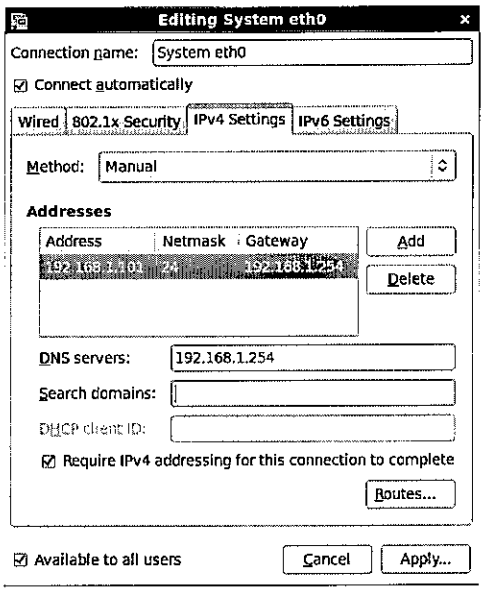
```
[student@serverX ~]$ host instructor
[student@serverX ~]$ host instructor.example.com
[student@serverX ~]$ ping 192.168.0.254
```

Since the changes don't seem to be something we can fix by renewing our lease, we will need to contact the network administrator for correct settings. In this case, your network administrator is the instructor. You will need to know:

- **IP address:** 192.168.1.X+100
- **Netmask:** 24
- **Gateway:** 192.168.1.254
- **DNS Server:** 192.168.1.254
- **DNS domain:** example.com

Once you have this information, you will want to enter it into **NetworkManager** to configure your connection. Right-click on the network icon in the upper right of your desktop, and choose the **Edit Connections** option. On the **Wired** tab of the **Network Connections** window, select **System eth0** and then click the button labeled **Edit**.

In the new window, choose the **IPv4 Settings** tab. Select **Manual** from the **Method** drop-down menu. Click on the **Add** button to add an IP address, and enter the IP, netmask, and gateway information as given by your instructor. Enter your DNS server and Search domain information in the corresponding test boxes. Click **Apply** and supply the root password when prompted. Test connectivity as before.



When you have fulfilled the requirements, run **`lab-grade-netconfig`** on serverX to check your work.

•

Administer Users and Groups

Practice Performance Checklist

User and Group Administration

Perform the following steps on serverX unless directed otherwise.

- ☐ Create a user account with the following attributes:

  User name = **`practice`**

  Full name = **`Joe Practice`**

  Password = **`practice`**

  - On serverX, start the User Manager: **System** → **Administration** → **Users and Groups**.
  - Select **Add User**. The Add New User window appears.
  - Fill in the **User name** (practice), **Full Name** (Practice User), and **Password** (practice), then click OK. Use the password anyway, if prompted that it is not a strong password.

- ☐ Create a user account with the following attributes:

  User name = **`baduser`**

  Full name = **`Bad User`**

  Password = **`baduser`**

  - Select **Add User**. The Add New User window appears.
  - Fill in the **User Name** (baduser), **Full Name** (Bad User), and **Password** (baduser), then click OK. Use the password anyway, if prompted that it is not a strong password.

- ☐ Create a supplementary group called **`pgroup`** with a group ID of **`30000`**.

  - Select **Add Group**. The Add New Group window appears.
  - Fill in the **Group Name** (pgroup), select **Specify Group ID Manually** (30000), then click OK.

- ☐ Create a supplementary group called **`badgroup`**.

  - Select **Add Group**. The Add New Group window appears.
  - Fill in the **Group Name** (badgroup), then click OK.

- ☐ Add the **`practice`** user to the **`pgroup`** group as a supplementary group.

  - Select the **Groups** tab, double-click on the *pgroup* Group name, click the **Group Users** tab, and select check boxes next to practice. Then click OK.

- ☐ Modify the password for student to **password**.
  - In the User Manager window, double-click the **User Name** (student).
  - Update the **Password** and **Confirm Password** fields to *password*, and confirm.
- ☐ Modify student's account so the password expires after 30 days.
  - In the User Manager window, double-click the **User Name** (student) and select the **Account Info** tab.
  - Select the **Enable Account Expiration** check box and type in the **Account Expires** date which is 30 days in the future.
- ☐ Lock the **practice** user account so they cannot log in.
  - In the User Manager window, double-click the **User Name** (practice) and select the **Account Info** tab.
  - Select the **Local Password is Locked** check box.
- ☐ Delete the user called **baduser**.
  - In the User Manager window, select the **User Name** (baduser).
  - Chose the **Delete** action, and confirm.
- ☐ Delete the supplementary group called **badgroup**.
  - In the User Manager window, navigate to the **Group** panel, and select the Group Name (badgroup).
  - Chose the **Delete** action, and confirm.

Test

Criterion Test

Case Study

Administer Users and Groups

Before you begin...

Run **lab-setup-server** on desktopX to prepare serverX for the exercise.

```
[root@desktopX ~]# lab-setup-server
```

Perform the following steps on serverX unless directed otherwise.

A team of consultants have been hired to work on a project. Create user accounts for each consultant and add them to a group called **consultants** as a supplementary group with a group ID of **40000**.

Their accounts should expire when their contract ends in 90 days and their passwords should have to be changed every month.

The following is the list of consultants with their user names (and they should all have an initial password of **`default`**):

- Sam Spade = sspade
- Betty Boop = bboop
- Dick Tracy = dtracy

When you finish, run the **`lab-grade-newusers`** evaluation script to confirm you have done everything correctly.

1. Open the User Manager window to begin adding user accounts.

   On serverX, start the User Manager: **System → Administration → Users and Groups.**

2. Select Add User and add the user information to create the accounts listed previously.
   - Select Add User. The Add New User window appears.
   - Fill in the user name (sspade) Full Name (Sam Spade), and Password (default), then click OK. Use the password anyway, if prompted that it is not a strong password.
   - Repeat the previous two steps for bboop (Betty Boop) and dtracy (Dick Tracy).
   - Set aside the User Manager window for the moment.

3. Create a new group named consultants (GID 40000) and add the three new users as members of that group.
   - Select Add Group. The Add New Group window appears.
   - Fill in the Group Name (consultants), select Specify Group ID Manually (40000), then click OK.
   - Select the Groups tab, double-click on the consultants Group name, click the Group Users tab, and select check boxes next to bboop, dtracy, and sspade. Then click OK.
   - Set aside the User Manager window for the moment.

4. Determine the date 90 days in the future and set each of the three new user accounts to expire on that date.
   - Open a shell as any user and type the following to determine the date 90 days from today)

     ```
     [student@serverX ~]$ date -d "+90 days"
     ```

   - Back in the User Manager window, double-click the User Name (sspade) and select the Account Info tab.

- Select the Enable Account Expiration check box and type in the Account Expires date. For example, if the account were to expire on January 19, 2012, you would type in 2012 01 19 as the date.
- Repeat these steps for the users bboop and dtracy.

5. Set each of the new user accounts to have their passwords expire in 30 days.
   - Select the Users tab, then double-click on sspade. The User Properties window appears.
   - Select the Password Info tab, select Enable Password Expiration, set the Days Before Change Required to 30, then click OK.
   - Repeat the previous two steps for bboop (Betty Boop) and dtracy (Dick Tracy).
6. Open a Terminal window on serverX as root and run the **`lab-grade-newusers`** evaluation script to confirm you have done everything correctly.

Manage Files from the Command Line

Practice Quiz

Linux File System Hierarchy

1. /etc contains most of the system configuration files.
2. / is the root directory.
3. User home directories are found below /home but root's home directory is /root.
4. The /var directory contains variable data like web sites and FTP sites.
5. Temporary files are stored in /tmp and /var/tmp.
6. Removable devices are normally mounted on /media.
7. Device files are kept in /dev.
8. Files used during the boot process are stored in /boot.

Practice Quiz

Navigating with Absolute Path Names

Use the **nautilus** screenshot from this section to answer the following questions.

1. What command would make Brad's home directory your current directory? cd /home/brad OR cd ~brad
2. What command would change your current directory back to your (student's) home directory? cd /home/student OR cd ~student OR cd ~ OR cd
3. How would you display the list of files in the current directory? ls
4. What command would you use to list the pictures in Mark's **pics** folder? ls /home/mark/pics OR ls ~mark/pics
5. You are in Brad's home directory. How would you list the files in your own home directory with the fewest keystrokes? ls ~
6. You are not sure where your current directory is. What command would display your current location? pwd
7. What single command would you use to list the files in both the **abba** and **blondie** directories? ls /home/mark/mp3/abba /home/mark/mp3/blondie
8. What is the absolute path name to the **playlist.txt** file? /home/mark/mp3/playlist.txt OR ~mark/mp3/playlist.txt
9. There is a file called **requiem.mp3** inside the **mozart** folder. What is that file's absolute path name? /home/mark/mp3/mozart/requiem.mp3

10. BONUS: There is a directory called **Desktop** inside student's home directory. What is the absolute path name to **Desktop**? /home/student/Desktop OR ~student/Desktop

Command Reading Exercise

1. Team 1:
   - **cp**

     Copy files: **cp** ***source target***

   - **ln -s**

     Create a symbolic link (shortcut): **ln -s** ***source target***

   - **mv**

     Move files: **mv** ***source target***

2. Team 2:
   - **rm [-rf]**

     Remove files: **rm [-rf]** ***file***

     -r: recursively; **-f**: force

   - **touch**

     Create new emtpy file: **touch** ***file***

     Will update last modified timestamp of existing file.

3. Team 3:
   - **mkdir**

     Create new directory: **mkdir** ***target***

   - **rmdir**

     Remove empty directory: **rmdir** ***target***

Practice Performance Checklist

Manage Files with Absolute Path Names

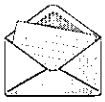
Before you begin...

These tasks require some existing files.

Log in as **root** on serverX and run **lab-setup-filemgmt**.

```
[root@serverX ~]# lab-setup-filemgmt
```

Do all of your work from the command line, do not use Nautilus to manage your files.



Note

Use absolute path names for every filename argument when performing the following tasks.

Perform the following steps on serverX unless directed otherwise.

- ☐ Log in as **student** on serverX.

- ☐ Create a folder called **bowe-labs** in your home directory.

```
[student@serverX ~]$ mkdir /home/student/bowe-labs
```

- ☐ Copy all of the files from the chemistry folder in Bowe's home directory to your **bowe-labs** directory.

```
[student@serverX ~]$ cp /home/bowe/chemistry/* /home/student/bowe-labs
```

- ☐ Log in as **mark** on serverX (password is **password**).

- ☐ Sort some of his music collection. Move the **call-me.mp3** and the **roxanne.mp3** files from the **mozart** folder into the **blondie** and the **the-police** folders respectively.

```
[mark@serverX ~]$ mv /home/mark/mp3/mozart/call-me.mp3 /home/mark/mp3/blondie
[mark@serverX ~]$ mv /home/mark/mp3/mozart/roxanne.mp3 /home/mark/mp3/the-police
```

- ☐ Remove his **playlist.txt** file from the **mp3** folder.

```
[mark@serverX ~]$ rm /home/mark/mp3/playlist.txt
```

- ☐ When you have completed all of the tasks, login as **root** on serverX and run the **lab-grade-filemgmt-1** script.

```
[root@serverX ~]# lab-grade-filemgmt-1
```

Absolute vs. Relative Path Names

Fill in the below table as discussed with your instructor:

Absolute Path Names	Relative Path Names
Path name begins with a slash (/).	Path name does not begin with a slash (/).

Absolute Path Names	Relative Path Names
Uses slashes to separate directories in the path name.	Same as absolute path name.
Linux begins searching at the root (/) directory for the file.	Linux begins searching at the shell's current working directory.
Does not change unless the file is moved.	Changes when the current working directory is changed with **cd**.
Special absolute path names: • ~ = your home directory • ***~user*** = *user*'s home directory	Special relative path names: • **.** = your current working directory • **..** = the parent of your current working directory (**../..** is two levels left, or up)

Table A.3. Absolute Versus Relative Path Name Comparison

Example Path Names

1. How would you move the **call-me.mp3** file from the **mozart** folder to the **blondie** folder using absolute path names?

```
mv /home/mark/mp3/mozart/call-me.mp3 /home/mark/mp3/blondie

mv ~mark/mp3/mozart/call-me.mp3 ~mark/mp3/blondie
```

2. How would this command look if Mark used relative path names if he was in his home directory?

```
mv mp3/mozart/call-me.mp3 mp3/blondie
```

3. If Mark was going to do a lot of organizing, it might be easier to move to where the files are before moving them. What commands would Mark use in this case?

```
cd mp3

mv mozart/call-me.mp3 blondie
```

Practice Performance Checklist

Save Typing with Relative Path Names

Before you begin...

Run **lab-setup-server** on desktopX to prepare serverX for the exercise. Subsequently, run **lab-setup-filemgmt** on serverX to create user accounts and files needed for the lab.

```
[root@desktopX ~]# lab-setup-server

[root@serverX ~]# lab-setup-filemgmt
```

- ☐ Log in as **student** on serverX.

- ☐ Create a folder called **bowe-labs** in your home directory.

```
[student@serverX ~]$ mkdir bowe-labs
```

- ☐ Copy all of the files from the chemistry folder in Bowe's home directory to your **bowe-labs** directory.

```
[student@serverX ~]$ cp ~bowe/chemistry/* bowe-labs
```

- ☐ Log in as **mark** on serverX (password is **password**).

- ☐ Sort some of his music collection. Move the **call-me.mp3** and the **roxanne.mp3** files from the **mozart** folder into the **blondie** and the **the-police** folders respectively.

```
[mark@serverX ~]$ cd mp3
[mark@serverX mp3]$ mv mozart/call-me.mp3 blondie
[mark@serverX mp3]$ mv mozart/roxanne.mp3 the-police
```

- ☐ Change into Mark's home directory.

```
[mark@serverX mp3]$ cd
```

- ☐ Use a relative path name to remove his **playlist.txt** file from the **mp3** folder.

```
[mark@serverX ~]$ rm mp3/playlist.txt
```

- ☐ When you have completed all of the tasks, login as **root** on serverX and run the **lab-grade-filemgmt-2** script.

```
[root@serverX ~]# lab-grade-filemgmt-2
```

- ☐ Bonus:

  Log in as **student** on serverX and create a directory called **marks-music**.

```
[student@serverX ~]$ mkdir marks-music
```

- ☐ With a single command, copy all of Mark's individual mp3 files into the **marks-music** folder.

  Hint: Shell wildcards can help you accomplish this task.

```
[student@serverX ~]$ cp ~mark/mp3/*/*.mp3 marks-music
```

Test

Criterion Test

Case Study

Organizing Brad's Photo Collection

Before you begin...

If you have not previously done so, run **lab-setup-filemgmt** on serverX to create user accounts and files needed for the criterion test.

Brad has been busy taking digital pictures. He works at Red Hat and has pictures from work He has pictures of his wife Jenny. He also has pictures of some famous cities he has visited.

He downloaded all of his pictures into a folder called **camera** below his home directory, but he needs your help sorting through them and organizing them into the appropriate folders below the **photos** directory below his home directory.

Login as **brad** on serverX (password is **password**) and organize his photos into the following subdirectories below **photos**:

- **family** - this folder is reserved for pictures of Jenny
- **places** - Brad's tourist photos belong here
- **work** - his Red Hat photos should go here

Some of the photos Brad took have **bad** in their name. Delete these pictures from the collection.

Finally, create a symbolic link to the **family** folder called **jenny**. This link should exist in Brad's **photos** folder.

When you finish, login as **root** on serverX and run the **lab-grade-filemgmt-3** script.

1. If not run earlier,

```
[root@serverX ~]# lab-setup-filemgmt
```

2. Open a Terminal window and login as brad on serverX.

```
[student@serverX ~]$ su - brad
Password: password
[brad@serverX ~]$
```

3. Delete all image files with the word **bad** in them from the **camera** directory.

```
[brad@serverX ~]$ rm camera/*bad*
```

4. Move all image files beginning with **jenny** from the **camera** directory to the **photos/family** directory under brad's home directory.

```
[brad@serverX ~]$ mv camera/jenny_* photos/family/
```

5. Move all image files beginning with **new_york** and **tokyo** from the **camera** directory to the **photos/places** directory under brad's home directory.

```
[brad@serverX ~]$ mv camera/new_york* photos/places
[brad@serverX ~]$ mv camera/tokyo* photos/places
```

6. Move all image file beginning with **redhat** and from the **camera** directory to the **photos/work** directory under brad's home directory.

```
[brad@serverX ~]$ mv camera/redhat* photos/work
```

7. Create a symbolic link from the **family** directory to the name **jenny** in the **camera** directory.

```
[brad@serverX ~]$ cd photos
[brad@serverX ~]$ ln -s family jenny
```

8. Open a Terminal window on serverX as root and run the **lab-grade-filemgmt-3** evaluation script to confirm you have done everything correctly.

Secure Linux File Access

Practice Quiz

Linux User, Group, Other Concepts

Answer the True/False questions based on the following user and file configurations.

```
Users and their groups:

    lucy     lucy,ricardo
    ricky    ricky,ricardo
    ethel    ethel,mertz
    fred     fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **lfile1** file.

1. **lucy** can change the contents of **lfile1**.

   (select one of the following...)
   a. True
   b. False

2. **fred** can change the contents of **lfile1**.

   (select one of the following...)
   a. True
   b. False

3. **fred** can delete **lfile1**.

   (select one of the following...)
   a. True
   b. False

4. **ricky** can change the contents of **lfile1**.

   (select one of the following...)
   a. True
   b. False

5. **ricky** can delete **lfile1**.

   (select one of the following...)

a. True
b. False

```
Users and their groups:

    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **`lfile2`** file.

1. **`ricky`** can view the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

2. **`ricky`** can change the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

3. **`ricky`** can delete **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

4. **`ethel`** can view the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

5. **`ethel`** can change the contents of **`lfile2`**.

   (select one of the following...)
   a. True
   b. False

```
Users and their groups:

    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **rfile1** file.

1. **lucy** can view the contents of **rfile1**.

   (select one of the following...)
   a. True
   b. False

2. **lucy** can change the contents of **rfile1**.

   (select one of the following...)
   a. True
   b. False

3. **fred** can view the contents of **rfile1**.

   (select one of the following...)
   a. True
   b. False

4. **fred** can change the contents of **rfile1**.

   (select one of the following...)
   a. True
   b. False

```
Users and their groups:

    lucy      lucy,ricardo
    ricky     ricky,ricardo
    ethel     ethel,mertz
    fred      fred,mertz

File attributes (permissions, user & group ownership, name):

    drwxrwxr-x   ricky   ricardo   dir (which contains the following files)
      -rw-rw-r--   lucy    lucy      lfile1
      -rw-r--rw-   lucy    ricardo   lfile2
      -rw-rw-r--   ricky   ricardo   rfile1
      -rw-r-----   ricky   ricardo   rfile2
```

Questions regarding the **rfile2** file.

1. **lucy** can view the contents of **rfile2**.

   (select one of the following...)
   a. True
   b. False

2. **lucy** can change the contents of **rfile2**.

   (select one of the following...)
   a. True
   b. False

3. **fred** can view the contents of **rfile2**.

   (select one of the following...)
   a. True
   b. False

4. **fred** can change the contents of **rfile2**.

   (select one of the following...)
   a. True
   b. False

Practice Performance Checklist

Manage File Security Using GUI Tools

Before you begin...

Run **lab-setup-users-2** on serverX to prepare for the exercise by creating the needed users and groups.

Perform the following steps on serverX unless directed otherwise.

- ☐ Log out of the GNOME desktop on serverX

- ☐ Log into the GNOME desktop on serverX as **alice** with a password of **password**.

- ☐ Open a window with a Bash prompt.

  Select **Applications** → **System Tools** → **Terminal**.

- ☐ Become the **root** user at the shell prompt.

```
[alice@serverX ~]$ su -
Password: redhat
```

- ☐ Launch **nautilus** from the root shell.

```
[root@serverX ~]# nautilus
```

- ☐ Create a folder in **/home** called **ateam**.

  Double click the **/home** directory.

  Right-click the background inside the **/home** folder window, select **Create Folder**, and type **ateam** as the folder name.

- ☐ Change the group ownership of the **ateam** folder to **ateam**.

  Right-click the folder **ateam** and select **Properties**, then change to the **Permissions** tab.

  In the Permissions tab, select the pull-down for **Group** and choose **ateam** from the list.

- ☐ Ensure the folder access of **ateam** allows group members to create and delete files.

  In the Permissions tab, select the pull-down for **Folder Access** under **Group** and choose **Create and delete files** from the list.

- ☐ Ensure the folder access of ateam forbids others from accessing its files.

  In the Permissions tab, select the pull-down for **Folder Access** under **Others** and choose **None** from the list.

- ☐ Create a folder in **/home** called **bteam**.

  Right-click the background inside the **/home** folder window, select **Create Folder**, and type **bteam** as the folder name.

- ☐ Change the group ownership of the **bteam** folder to **bteam**.

  Right-click the folder **bteam** and select **Properties**, then change to the **Permissions** tab.

  In the Permissions tab, select the pull-down for **Group** and choose **bteam** from the list.

- ☐ Ensure the folder access of **bteam** allows group members to create and delete files.

  In the Permissions tab, select the pull-down for **Folder Access** under **Group** and choose **Create and delete files** from the list.

- ☐ Ensure the folder access of bteam allows others to access its files.

  In the Permissions tab, select the pull-down for **Folder Access** under **Others** and choose **Access files** from the list.

- ☐ Log out from the GNOME desktop as **alice**.

  Select **System** → **Log Out alice...**.

- ☐ Log into the GNOME desktop as **andy** with a password of **password**.

- ☐ Navigate to the **/home/ateam** folder.

  Double click **andy's Home** icon on the GNOME desktop.

  Click the **Open the parent folder** icon, then double click the **ateam** folder.

- ☐ Create an empty file called **andyfile1**.

  Right-click the background inside the **/home/ateam** folder window, select **Create Document** → **Empty File**, and type **andyfile1** as the file name.

- ☐ Record the default user and group ownership of the new file and its permissions.

  Right-click the file **andyfile1** and select **Properties**, then change to the **Permissions** tab.

  In the Permissions tab, note the user and group ownership are both set to **andy** with the owner and group permissions set to **Read and Write** while all others are set to **Read-only**.

- ☐ Create an empty file called **andyfile2**.

  Right-click the background inside the **/home/ateam** folder window, select **Create Document** → **Empty File**, and type **andyfile2** as the file name.

- ☐ Change the group ownership of **andyfile2** to **ateam**.

  Right-click the file **andyfile2** and select **Properties**, then change to the **Permissions** tab.

  In the Permissions tab, select the pull-down for **Group** and choose **ateam** from the list.

- ☐ Switch GNOME users to **alice**.

  Select **System** → **Log Out andy...** and choose **Switch User**.

- ☐ Navigate to the **/home/ateam** folder.

  Double click **alice's Home** icon on the GNOME desktop.

  Click the **Open the parent folder** icon, then double click the **ateam** folder.

- ☐ Note the difference in appearance between **andyfile1** and **andyfile2**.

- ☐ Switch GNOME users to **betty** with a password of **password**.

  Select **System** → **Log Out alice...** and choose **Switch User**.

- ☐ Navigate to the **/home** folder.

  Double click **betty's Home** icon on the GNOME desktop.

  Click the **Open the parent folder** icon.

- ☐ Note the difference in appearance between the **ateam** and **bteam** folders.

Practice Performance Checklist

Manage File Security from the Command Line

Perform the following steps on serverX unless directed otherwise.

- ☐ Log into the GNOME desktop on serverX as **alice** with a password of **password**.

- ☐ Open a window with a Bash prompt.

  Select **Applications** → **System Tools** → **Terminal**.

- ☐ Become the **root** user at the shell prompt.

```
[alice@serverX ~]$ su -
Password: redhat
```

- ☐ Create a directory in **/home** called **ateam-text**.

```
[root@serverX ~]# mkdir /home/ateam-text
```

- ☐ Change the group ownership of the **ateam-text** directory to **ateam**.

```
[root@serverX ~]# chgrp ateam /home/ateam-text
```

- ☐ Ensure the permissions of **ateam-text** allows group members to create and delete files.

```
[root@serverX ~]# chmod g+w /home/ateam-text
```

- ☐ Ensure the permissions of **ateam-text** forbids others from accessing its files.

```
[root@serverX ~]# chmod 770 /home/ateam-text
```

- ☐ Ensure the permissions of **ateam-text** causes files created in that directory to inherit the group ownership of **ateam**.

```
[root@serverX ~]# chmod 2770 /home/ateam-text
```

- ☐ Log out from the GNOME desktop as **alice**.

- ☐ Log into the GNOME desktop as **andy** with a password of **password**.

- ☐ Navigate to the **/home/ateam-text** folder (remember to open a terminal window first).

```
[andy@serverX ~]$ cd /home/ateam-text
```

- ☐ Create an empty file called **andyfile3**.

```
[andy@serverX ateam-text]$ touch andyfile3
```

- ☐ Record the default user and group ownership of the new file and its permissions.

```
[andy@serverX ateam-text]$ ls -l andyfile3
-rw-rw-r--.  1 andy ateam 0 Feb  8 22:24 andyfile3
```

- ☐ Switch GNOME users to **alice**.

- ☐ Navigate to the **/home/ateam-text** folder.

```
[alice@serverX ~]$ cd /home/ateam-text
```

- ☐ Determine **alice**'s privileges to access and/or modify **andyfile3**.

```
[alice@serverX ateam-text]$ echo "text" >> andyfile3
[alice@serverX ateam-text]$ cat andyfile3
test
```

Test

Criterion Test

Case Study

Securing the Stooges

Before you begin...

Run **lab-setup-stooges** as root from desktopX to reset your virtual server, serverX, and have the necessary users and groups created for you.

```
[root@desktopX ~]# lab-setup-stooges
```

Your serverX machine has three accounts, **curly**, **larry**, and **moe**, who are members of a group called **stooges**.

Create a directory called **/home/stooges** where these three users can work collaboratively on files. Modify the permissions on this directory so only the user and group access, create, and delete files in that directory. Files created in this directory should automatically be assigned a group ownership of **stooges**.

When you finish, run the evaluation script **lab-grade-stooges** from serverX to make sure that you have done everything correctly.

1. Open a Terminal window and become root on serverX.

   ```
   [student@serverX ~]$ su -
   Password: redhat
   [root@serverX ~]#
   ```

2. Create the **/home/stooges** directory.

   ```
   [root@serverX ~]# mkdir /home/stooges
   ```

3. Change group permissions on the /home/stooges directory so it belongs to the stooges group.

   ```
   [root@serverX ~]# chgrp stooges /home/stooges
   ```

4. Set permissions on the **/home/stooges** directory so it is a set GID bit directory (2), the owner (7) and group (7) have full read/write/execute permissions, and other users have no permission (0) to the directory.

   ```
   [root@serverX ~]# chmod 2770 /home/stooges
   ```

5. Check that the permissions were set properly.

   ```
   [root@serverX ~]# ls -ld /home/stooges
   drwxrws---. 2 root stooges 1024 Dec 9 1:38 /home/stooges
   ```

6. Open a Terminal window on serverX as root and run the **`lab-grade-stooges`** evaluation script to confirm you have done everything correctly.

Administer Remote Systems

SSH Basics

Fill in the blanks as your instructor demonstrates the use of **ssh** and covers these key points.

1. SSH is more secure than telnet because all communication between hosts is encrypted.
2. **ssh -X user@host.fqdn** initiates a remote connection to host.fqdn as **user** .
3. The first time an SSH connection is made to a system, the public key of the remote system is stored locally so its identity can be verified each time a future connection is started.
4. The exit command is used to finish an SSH session and return to the local shell.

Practice Quiz

Remote Shell Access

Connect to serverX from desktopX using a remote shell. Answer the following questions running commands from that remote shell:

1. The Disk Utility command is **palimpsest**. /dev/vda is the name of the hard drive on serverX.
2. Red Hat Enterprise Linux 6 (Santiago) is the name of the OS release according to **/etc/redhat-release**.
3. Run **nautilus** or use the command-line in the remote shell on serverX to perform the following:
   - Create a file named **a1.txt** in **/root**
   - Create a directory named **b2** in **/home/student** which is owned by the **student** user and the **student** group.

Compare and Contrast: Local vs. Remote File Copy

Fill in the open fields.

	Local File Copy	Remote File Copy
Command	**cp**	**rsync**
Syntax	**cp *original-file new-file***	**rsync *original-file new-file***
Arguments	Can use pathnames for arguments	In addition to pathnames, the files can have the following syntax: **target:pathname**, where **target** = **[user@]host.fqdn**. Specify **user@** when the remote username

	Local File Copy	Remote File Copy
		is different than the current username.
Scope of operation	Only works with local files	Works with local files ***and*** remote files
How handle directories?	**-r** or **-a** command line switch.	**-r** or **-a** command line switch.

Table A.4. Local vs. Remote File Copy Comparison

Practice Performance Checklist

Remote File Transfers

Perform the following steps on desktopX unless directed otherwise.

- ☐ Use **rsync** to backup **student**'s home directory on desktopX to the **/tmp** directory on serverX.

```
[student@desktopX ~]$ rsync -a /home/student serverX:/tmp
```

- ☐ Create a new file named **z.txt** in **student**'s home directory.

```
[student@desktopX ~]$ echo test > ~/z.txt
```

- ☐ Use the same **rsync** command to backup **student**'s home directory on desktopX to the **/tmp** directory on serverX.

```
[student@desktopX ~]$ rsync -av /home/student serverX:/tmp
```

- ☐ Remove the **Desktop** directory from the backup on serverX. Run the same **rsync** command.

```
[student@desktopX ~]$ ssh serverX 'rm -rf /tmp/student/Desktop'
...
[student@desktopX ~]$ rsync -av /home/student serverX:/tmp
...
```

Create an Archive

1. Launch Archive Manager: **Applications** → **Accessories** → **Archive Manager**
2. Click Create a new archive button
3. Choose name and type of archive then click Create

4. Use the Add files to the archive or the Add a folder to the archive buttons to add content to the archive

5. File → Close when finished

Browse and Extract from an Archive

1. In Nautilus, right click on the icon for the archive and select Open with Archive Mounter

2. An icon will appear on the desktop, navigate it with Nautilus like a standard directory

3. Use Nautilus copy commands (drag and drop) to copy files and/or folders from the archive

Compress/Decompress a File

1. Right-click on the file in Nautilus

2. Select Compress

3. Choose file extension to determine the type of compression

4. Click Create

   Perform same steps as above, except select Extract Here to decompress a single compressed file

   For an archive, open the archive in Archive Manager, then select File → Save As and choose a different extension. For example change from `.tar.gz` to `.tar`.

Practice Performance Checklist

File Roller Archive

- ☐ Archive **student**'s home directory on desktopX into **/tmp/student.tar.gz**.

  Launch the Archive Manager (Applications → Accessories → Archive Manager) on desktopX. Click on the New button. Enter **student** in the Name field. Expand the Browse for other folders list. In the left pane, click on File System. In the right pane, double-click on tmp. Change the Archive type field to Tar compressed with gzip (.tar.gz). Click the Create button.

Click the Add Folder button. Click **student** in the left pane and click Add. Once it has finished, close the **Archive Manager**.

- ☐ Send **/tmp/student.tar.gz** to **/tmp** on serverX.

```
[student@desktopX ~]$ rsync /tmp/student.tar.gz serverX:/tmp/
```

- ☐ Extract the **Desktop** folder from the archive to **/home/student** on serverX.

Launch the **Archive Manager** (**Applications** → **Accessories** → **Archive Manager**) on serverX. Click on the Open button. In the left pane, click on **File System**. In the right pane, double-click on **tmp**. Double-click on **student.tar.gz**. In the window that opens, double-click on **student**. Browse to the **Desktop** folder and highlight it. Click on the Extract button. Click **student** in the left pane and click Extract. When it has completed, click on the Close button. Close the **Archive Manager**.

Practice Performance Checklist

Securely Transferring Backups

- ☐ Create an SSH key-pair as **student** on desktopX using no passphrase.

```
[student@desktopX ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):  Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase):   Enter
Enter same passphrase again:  Enter
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
...
```

- ☐ Send the SSH public key to the **student** account on serverX.

```
[student@desktopX ~]$ ssh-copy-id serverX
The authenticity of host 'serverX (192.168.0.101)' can't be established.
RSA key fingerprint is 33:fa:a1:3c:98:30:ff:f6:d4:99:00:4e:7f:84:3e:c3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'serverX,192.168.0.101' (RSA) to the list of known
 hosts.
student@serverX's password: student
Now try logging into the machine, with "ssh 'serverX'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

- ☐ Run the **rsync** command used before to backup **student**'s home directory on desktopX to the **/tmp** directory on serverX.

```
[student@desktopX ~]$ rsync -r /home/student serverX:/tmp
```

Test

Criterion Test

Exercise

SSH Keys and File Archives

Before you begin...

Run **lab-setup-server** on desktopX to prepare serverX for the exercise.

In the instructions that follow, pay particular attention to the contexts of the two different hosts.

```
[root@desktopX ~]# lab-setup-server
```

1. Install the SSH public key generated previously on desktopX to the **student** account on serverX.

   ```
   [student@desktopX ~]$ ssh-copy-id serverX
   student@serverX's password: student
   Now try logging into the machine, with "ssh 'serverX'", and check in:

     .ssh/authorized_keys

   to make sure we haven't added extra keys that you weren't expecting.
   ```

2. Archive **student**'s home directory on desktopX into **/tmp/student.tar.bz2**.

   Launch the **Archive Manager** (**Applications** → **Accessories** → **Archive Manager**) on desktopX. Click on the **New** button. Enter **student** in the **Name** field. Expand the **Browse for other folders** list. In the left pane, click on **File System**. In the right pane, double-click on **tmp**. Change the **Archive type** field to **Tar compressed with bzip2 (.tar.bz2)**. Click the **Create** button.

   Click the **Add Folder** button. Click **student** in the left pane and click **Add**. Once it has finished, close the **Archive Manager**.

3. Copy the **/tmp/student.tar.bz2** file on desktopX to **/tmp** on serverX.

   ```
   [student@desktopX ~]$ rsync /tmp/student.tar.bz2 serverX:/tmp/
   ```

4. Remove **student**'s home directory on serverX.

   ```
   [student@desktopX ~]$ ssh -X root@serverX
   root@serverX's password: redhat
   [root@serverX ~]# rm -fr /home/student/
   [root@serverX ~]# exit
   ```

```
[student@desktopX ~]$
```

5. Login to serverX as root using a secure connection from desktopX. Restore **student**'s home directory from the **/tmp/student.tar.bz2** archive. Hint: the command to launch the Archive Manager is **file-roller**.

   Login to serverX as root using a secure connection from desktopX and run the Archive Manager:

```
[student@desktopX ~]$ ssh -X root@serverX
root@serverX's password: redhat
[root@serverX ~]# file-roller &
```

   Click on the Open button. In the left pane, click on **File System**. In the right pane, double-click on **tmp**. Double-click on **student.tar.bz2**. In the window that opens, highlight **student**. Click on the Extract button. Click **File System** in the left pane and double-click on **home** in the right pane. Click Extract. When it has completed, click on the Close button. Close the **Archive Manager**.

6. As student, install the SSH public key from the backup you just restored on serverX to desktopX. Verify you can use the SSH keys to get from serverX to desktopX without typing a password.

```
[root@serverX ~]# su - student
[student@serverX ~]$ ssh-copy-id desktopX
The authenticity of host 'desktopX (192.168.0.X)' can't be established.
RSA key fingerprint is 3b:2d:7a:6f:f6:1f:26:37:e9:86:a4:aa:51:4a:9d:0d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'desktopX,192.168.0.1' (RSA) to the list of known
 hosts.student@desktopX's password: student
Now try logging into the machine, with "ssh 'desktopX'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

[student@serverX ~]$ ssh desktopX hostname
desktopX.example.com
```

7. When you are ready to check your work, run **lab-grade-remote** on serverX.

```
[root@serverX ~]# lab-grade-remote
```

Configure General Services

Four Steps to Deploy a Service

1. Install
2. Start
3. Enable
4. Test

Securing SSH Search & Learn

1. Use the **Add/Remove Software** application to determine which package provides the SSH service (search for **ssh server**).

   Open the software manager (**System** → **Administration** → **Add/Remove Software**). Search for **ssh server**. *openssh-server* is the package that provides the SSH service.

2. Use the file listing of the package discovered in the previous question to determine the primary configuration file for the service.

   Highlight the *openssh-server* package and go to **Selection** → **Get file list**. **/etc/ssh/sshd_config** is the primary configuration file.

3. Reviewing the man page for the configuration file, which directive disables root login?

   ```
   [root@serverX ~]# man sshd_config
   /root login
   ```

   Answer: **PermitRootLogin**

4. Which directive in that configuration file disables password login?

   ```
   [root@serverX ~]# man sshd_config
   /password
   ```

   Answer: **PasswordAuthentication**

Practice Performance Checklist

Securing SSH

Before you begin...

Run **lab-setup-server** on desktopX to prepare serverX for the exercise.

- ☐ If not done earlier, generate SSH keys on desktopX.

  Copy the public key to the **student** account on serverX and verify that the keys are working.

```
[student@desktopX ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):  Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase):   Enter
Enter same passphrase again:  Enter
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
...
[student@desktopX ~]$ ssh-copy-id serverX
The authenticity of host 'serverX (192.168.0.X+100)' can't be established.
RSA key fingerprint is 33:fa:a1:3c:98:30:ff:f6:d4:99:00:4e:7f:84:3e:c3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'serverX,192.168.0.X+100' (RSA) to the list of known
 hosts.
student@serverX's password: student
Now try logging into the machine, with "ssh 'serverX'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

- ☐ Configure SSH on serverX to prevent root logins.

  Modify the **/etc/ssh/sshd_config** file so that the line looks as follows (be sure to remove the comment):

  ```
  PermitRootLogin no
  ```

- ☐ Restart the SSH service.

  Launch the **Services** application: **System** → **Administration** → **Services**. Highlight the **sshd** service in the left pane and click the Restart button.

- ☐ Confirm that **root** cannot log in with SSH, but **student** is permitted to log in.

  ```
  [student@desktopX ~]$ ssh root@serverX
  Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
  [student@desktopX ~]$ ssh student@serverX
  [student@serverX ~]$
  ```

- ☐ Configure SSH on serverX to prevent password authentication.

  Modify the **/etc/ssh/sshd_config** file so that the line looks as follows:

  ```
  PasswordAuthentication no
  ```

- ☐ Restart the SSH service.

  Launch the **Services** application: **System** → **Administration** → **Services**. Highlight the **sshd** service in the left pane and click the Restart button.

- Confirm that **visitor** cannot log in using a password, but **student** is permitted to log in using the SSH keys created earlier.

```
[student@desktopX ~]$ ssh visitor@serverX
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[student@desktopX ~]$ ssh student@serverX
[student@serverX ~]$
```

Practice Exercise

Deploy a VNC Server

Perform the following steps on serverX unless directed otherwise.

1. Install the *tigervnc-server* package on serverX.

   Launch the software manager: **System** → **Administration** → **Add/Remove Software**. Search for **vnc** and ensure the *tigervnc-server* package is installed.

2. Configure VNC display 1 for student and display 2 for visitor.

   Add the following to **/etc/sysconfig/vncservers**:

```
VNCSERVERS="1:student 2:visitor"
```

3. Set **redhat** as the VNC password for both student and visitor.

```
[student@serverX ~] vncpasswd
Password: redhat
Verify: redhat[student@serverX ~] su - visitor
Password: password
[visitor@serverX ~] vncpasswd
Password: redhat
Verify: redhat
```

4. Start and enable the **vncserver** service.

Note

When starting the **vncserver** service, the status may not get updated. If this happens, close down the **Services** application and restart it to check the status.

   Launch the **Services** application: **System** → **Administration** → **Services**. Select the **vncserver** service and click the Start button. Then click the Enable button.

5. You will test the connection in the next section.

Practice Exercise

Connect to VNC Securely

1. Configure the VNC server on serverX to allow local connections only (unless you already did this in the previous exercise).

   Edit **/etc/sysconfig/vncservers** and add, if needed, the following:

   ```
   VNCSERVERARGS[1]="-localhost"
   VNCSERVERARGS[2]="-localhost"
   ```

   Restart the **vncserver** service. Launch the **Services** application: **System** → **Administration** → **Services**. Select the **vncserver** service and click the Restart button.

2. Connect to the VNC server on serverX securely from desktopX using an SSH tunnel.

   ```
   [student@desktopX ~] vncviewer -via serverX localhost:1
   ```

Test

Criterion Test

Exercise

Secure Remote Administration

Before you begin...

Run **lab-setup-server** on desktopX to prepare serverX for the exercise.

```
[root@desktopX ~]# lab-setup-server
```

1. Create SSH keys for **student** on desktopX (if necessary).

   ```
   [student@desktopX ~]$ ssh-keygen
   ```

2. Copy **student**'s public key to the **student** account on serverX.

   ```
   [student@desktopX ~]$ ssh-copy-id serverX
   ```

3. Configure SSH on serverX to prevent root logins and password authentication.

   As root, add the following line to **/etc/ssh/sshd_config**:

   ```
   PermitRootLogin no
   PasswordAuthentication no
   ```

   Restart the **sshd** service.

Launch the **Services** application: **System** → **Administration** → **Services**. Highlight the **sshd** service in the left pane and click the Restart button.

4. Configure VNC for **student** using a password of **redhat** on display 1.

   If necessary, install the **tigervnc-server** package.

   As root, add the following line to **/etc/sysconfig/vncservers**:

   ```
   VNCSERVERS="1:student"
   ```

   As student, set a VNC password:

   ```
   [student@serverX ~] vncpasswd
   Password: redhat
   Verify: redhat
   ```

5. Allow connections to VNC only from localhost.

   As root, add the following line to **/etc/sysconfig/vncservers**:

   ```
   VNCSERVERARGS[1]="-localhost"
   ```

   Start and enable the **vncserver** service.

   Launch the **Services** application: **System** → **Administration** → **Services**. Select the **vncserver** service and click the Start button. Then click the Enable button.

6. When you are ready to check your work, run **lab-grade-securevnc** on desktopX.

   ```
   [root@desktopX ~] lab-grade-securevnc
   ```

Manage Physical Storage II

Practice Quiz

File System Parameters

1. **/boot** has a journal

   (select one of the following...)
   a. True
   b. False

2. **/boot** does not have any default mount options

   (select one of the following...)
   a. True
   b. False

3. A newly formatted ext4 file system includes **acl** as a default mount option.

   (select one of the following...)
   a. True
   b. False

4. / includes **user_xattr** as a default mount option.

   (select one of the following...)
   a. True
   b. False

5. A file system created by **Disk Utility** has a file system label.

   (select one of the following...)
   a. True
   b. False

Practice Performance Checklist

Modifying File System Parameters

Perform the following steps on serverX unless directed otherwise directed.

- ☐ Create a new 256 MB partition on serverX and use ext4 as the file system type.

  Select **Applications** → **System Tools** → **Disk Utility** to open **Disk Utility**. Highlight your hard drive in the left panel and click on the free space in the diagram of your disk under **Volumes**. Set the **Size** to 256 MB and the **Type** to ext4. Do not create the file system yet!

- ☐ Add a label of **/test** to the file system.

  Set the **Name** of the file system to **/test** in the **Disk Utility** window you were working with in the last step. Click **Create.** Authenticate as root if necessary.

- ☐ Add **user_xattr** and **acl** as default mount options.

  Use **Disk Utility** to determine the device name of your new partition, **/dev/*your-device***. Then open a shell prompt and use **su** to become root. Run the following command:

```
[root@serverX ~]# tune2fs -o user_xattr,acl /dev/your-device
```

- ☐ Mount the file system on **/test**

  You will need to make sure the **/test** directory exists as well. As root, run the commands

```
[root@serverX ~]# mkdir /test
[root@serverX ~]# mount /dev/your-device /test
```

Practice Performance Checklist

Delete a File System

Perform the following steps on serverX unless directed otherwise.

- ☐ Delete the 256 MB partition you just created in the last lab.

  Open a shell as root with **su**. Make sure that no programs have their current working directory in **/test** or its subdirectories (if any), and that no programs have files open in **/test**. Unmount the file system with **umount /test**.

  In **Disk Utility**, highlight the partition in the diagram under **Volumes** and click **Delete Partition.** Confirm that you want to delete the partition, and enter the root password if necessary.

Filesystems vs. Swap Partitions

Fill in the below table with comparable swap area information.

Standard File System	Swap Area
Purpose: Store various files and directories	Purpose: Extend system virtual memory
Stored on physical disk (Partition ID **0x83**)	Stored on physical disk (Partition ID: **0x82**)
Can reside in an LVM logical volume	Can reside in an LVM logical volume

Standard File System	Swap Area
Activated by **mount** and deactivated by **umount**	Activated by **swapon** and deactivated by **swapoff**
Persist a system crash	Contents are lost when a system crashes (similar to RAM)

Table A.5. Standard File System/Swap Area Comparison

Practice Quiz

Swap Space Concepts

1. swap space is used when the system begins to run out of RAM.
2. The swapon command is used to activate a swap space.
3. The swapoff command is used to deactivate a swap space.
4. The physical ID for a swap partition is **0x82**.

Creating Filesystems vs. Creating Swap Partitions

Compare and contrast creating a swap space with creating a regular file system.

File System Creation	Swap Space Creation
Launch **Disk Utility** and create a new partition formatted with a file system	Launch Disk Utility and create a new partition formatted as swap space.
Create a mount point	Add a **/etc/fstab** entry, specifying ***swap*** as both the mount point and file system (2nd and 3rd columns).
Edit **/etc/fstab** to create a persistent entry	Activate the swap area: **swapon -a**
Remount the file system to confirm it mounts properly	Confirm it is active: **swapon -s**

File System Creation	Swap Space Creation

Table A.6. Compare file system/swap space creation

Practice Performance Checklist

Manage Swap Space

You added some additional RAM to serverX and you want to ensure you have enough swap space to support it. You need to create a new swap partition of 1 GB in size.

- ☐ Use all available physical extents in **vgsrv** up to 1 GB to create a new logical volume called **swap2**.
- ☐ In the **Disk Utility**, make this logical volume swap space.
- ☐ Make an entry in **/etc/fstab** for the swap device.

  Add the following to **/etc/fstab**:

  ```
  /dev/vgsrv/swap2   swap swap defaults   0 0
  ```

- ☐ Enable the swap space.

  ```
  [root@serverX ~] swapon -a
  ```

Test

Criterion Test

Performance Checklist

Physical Storage II

- ☐ Run **lab-setup-storage-2** on desktopX to prepare serverX for this exercise.
- ☐ Create two new physical partitions 512 MB in size each.
- ☐ With the first partition, create swap space and make it persistent.
  - ☐ Run **Applications** → **System Tools** → **System Monitor** and note the amount of swap space displayed.

- ☐ Run **Applications** → **System Tools** → **Disk Utility**
- ☐ Select your system's main hard disk in the sidebar on the left. You will you know you have the right one when **`Device: /dev/vda`** is listed in the drive details.
- ☐ Select the free space on your disk, click **Create Partition**, and fill in the following:
  - **Size: `512MB`**
  - Type: **`Swap Space`**
  - Name: **`swap2`**

  Click **Create** when finished.
- ☐ Add the following to **`/etc/fstab`**:

```
LABEL=swap2   swap swap defaults   0 0
```

- ☐ Enable the swap space.

```
[root@serverX ~] swapon -a
```

- ☐ Return to the **System Monitor** tool and note the swap space again. It should have increased.

☐ With the second partition, create an ext4 file system persistently mounted on **`/opt`** with **`acl`** as a default mount option.

- ☐ If necessary, run **Applications** → **System Tools** → **Disk Utility** and select your hard disk as before.
- ☐ Select the free space on your disk, click **Create Partition**, and fill in the following:
  - **Size: `512MB`**
  - Type: **`Ext4`**
  - Name: **`/opt`**

  Click **Create** when finished.
- ☐ As root, open **`/etc/fstab`** in a text editor, and add a line like the following:

```
LABEL=/opt /opt ext4 acl  1 2
```

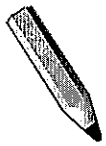
- ☐ Mount the new file system.

```
[root@serverX ~] mount -a
```

- ☐ In **Disk Utility**, select your new partition and confirm that the **Mount Point** is listed as **`/opt`**

- ☐ Reboot then run the **`lab-grade-storage-2`** grading script on serverX.

Install Linux Graphically



Test

Criterion Test

Exercise

Install Linux Graphically

Before you begin...

This task completely reinstalls your desktopX.example.com system. All data on your system are destroyed, so be sure to copy off any data you want to keep before starting this task.

1. Reboot your desktop system, interrupting the boot process to boot off your network interface card.
   - From your desktopX workstation, select **System** → **Shutdown**. When prompted, select Restart.
   - When you see the computer's BIOS screen, quickly press the key that lets you select a boot device (possibly the F12 function key).
   - Choose to boot from the computer's network interface card. If there are multiple NICs, the one you want may be listed as the Onboard NIC.
2. Select **Install or upgrade an existing system** from the boot screen.

   If your NIC is able to PXE boot properly, you should see the Red Hat boot screen. Use the down arrow to highlight **Install or upgrade an existing system** and press **`Enter`**.
3. Choose your Language and Keyboard, when prompted.
4. Choose URL as the install type and select **`http://instructor/pub/rhel6/dvd`** as the installation source.

   When prompted, you will probably use the eth0 interface with IPV4 networking and DHCP to get address information.
5. Choose Basic Storage Devices, Fresh Installation, and set desktopX.example.com as the hostname. (Use the same desktop name the system had when you started the install.)
6. Choose your timezone and set the **`root`** password to **`redhat`**.
7. Configure the partitions as follows:
   - **`/boot`** 200 MB physical partition
   - **`/home`** 1024 MB physical partition, encrypted using a passphrase of **`password`**
   - 50 GB physical volume for use with a volume group
     - 20 GB logical volume for /

  - 2 GB logical volume for swap
- When presented with partitioning choices, select Create Custom Layout.
- When presented with partitioning choices, select Create Custom Layout.
- When presented with partitioning choices, select Create Custom Layout.
- Select and delete all existing partitions.
- Create the /boot partition: Select the Free space, then click the Create button. Select Standard Partition and select Create. Set the partition as /boot, ext4 file system type, 200MB, fixed size.
- Create the /home partition: Select the Free space. Select Standard Partition and select Create. Set the partition as /home, ext4, 1024MB, fixed size. Also select the Encrypt check box.
- Create an LVM physical volume: Select the Free space, then click the Create button. Select LVM Physical Volume and select Create. Set the size as 50000MB and click OK.
- Create a LVM volume group: Select Create. Select LVM Volume Group and click Create. Choose a volume group name (such as desktopXVG0).
- Create a / LVM logical volume: Click Add. Select / as the mount point, ext4 as the type, choose a logical volume name (such as desktopXVol00), set the size to 20000 MB, and select OK.
- Create a swap logical volume: Click Add. Select swap as the file system type and 2000 MB as the size, then click OK and OK again.
- Set encrypted password for volume: When prompted set password as the passphrase for the /home volume. Write the changes to disk when prompted.

8. No changes are required for the bootloader, so click Next.
9. Select **Desktop** to set the basic install type. Select the **`Customize now`** button, then click **`Next`**. Besides those packages already selected, select the **FTP server** package group. Click Next and the packages begin installing.
10. When installation is complete, press **`Enter`** to reboot as prompted.
11. During boot-up, enter the passphrase (password) to unlock the /home partition when prompted.
12. When you see the welcome screen (**`firstboot`**), answer the questions as appropriate. Do not register with RHN. When prompted, create a user account called student with the password student. You can turn off or disregard Kdump, when you get to it.
13. Once the installation and **`firstboot`** have completed, download and run the grading script. It can be found at the following URL: *http://instructor/pub/gls/ulbin/lab-grade-installation*
    - Login as student.

- Open a Terminal window.
- Become root user (su -).
- Get the lab-grade-installation script, make it executable, and run it to test that you completed the installation properly:

```
[root@desktopX ~]# wget http://instructor/pub/gls/ulbin/lab-grade-installation
[root@desktopX ~]# chmod a+x lab-grade-installation
[root@desktopX ~]# ./lab-grade-installation
```

14. After you have completed the criterion test, reinstall the standard classroom desktop system. To do this, reboot your desktop system, interrupting the boot process to boot off your network interface card. Select **Install GLS Workstation** from the GRUB menu that appears.

    - From your desktopX workstation, select **System** → **Shutdown**. When prompted, select Restart.
    - When you see the computer's BIOS screen, quickly press the key that lets you select a boot device (possibly F12 function key).
    - Choose to boot from the computer's network interface card. If there are multiple NICs, the one you want may be listed as the Onboard NIC.
    - If your NIC is able to PXE boot properly, you should see the Red Hat installation boot screen. Use the arrow keys to highlight **Install GLS workstation** and press **Enter**. A fresh install should start and run automatically (this will take several minutes to complete).

Manage Virtual Machines

Practice Performance Checklist

Virtual Guest Installation

In this lab you will install a new virtual machine with Red Hat Enterprise Linux using **`virt-manager`** and the graphical installer. Once you have successfully completed the lab you will need to remove both the virtual machine and its logical volume to reclaim system resources needed for other labs.

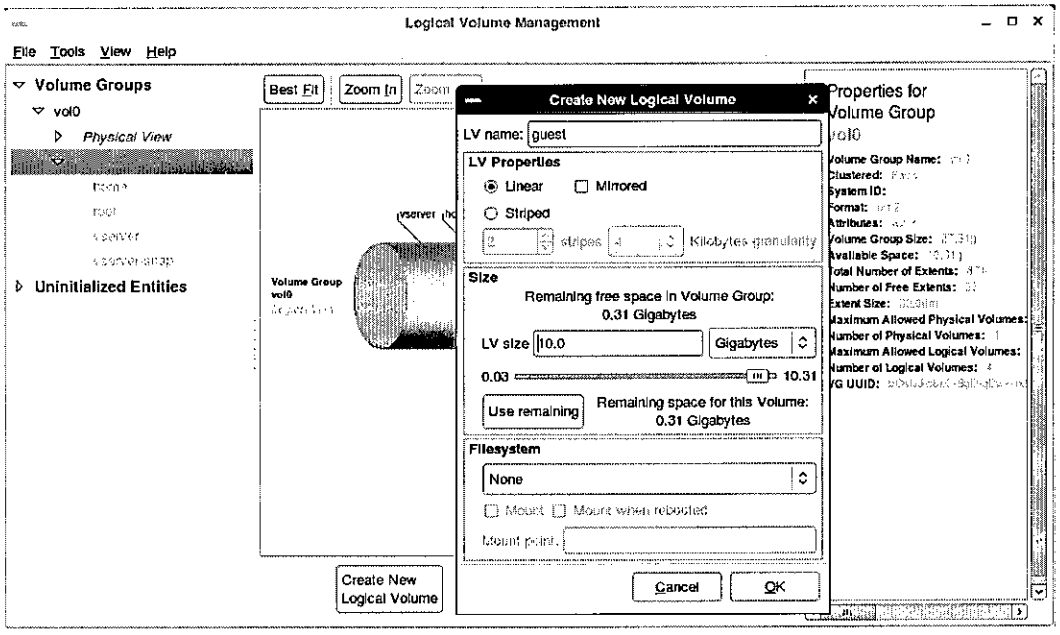
Perform the following steps on desktopX:

- ☐ Gracefully shutdown your serverX virtual machine (**`vserver`**) to reclaim system CPU and RAM resources.

  Launch **`virt-manager`** by selecting **Applications** → **System Tools** → **Virtual Machine Manager**. Right-click on the icon for the **vserver** virtual machine then select **Shut Down** → **Shut Down**.

- ☐ Create a logical volume 10 GB in size from the **`vol0`** volume group and name it **`guest`**.

  1. Open the **System+Adminstration** → **Logical Volume Management** application.
  2. In the lefthand navigation panel, select **vol0+Logical View** .
  3. Select the **Create New Logical Volume** from the lower panel.
  4. In the resulting dialog, specify a **LV name** of *guest*, and a **LV size** of *10 Gigabytes*. Leave the remaing **LV properties** and **Filesystem** at their default values of *Linear* and *None*.



5. Choose **OK** to confirm the change, and exit.

☐ Create a Red Hat Enterprise Linux 6 virtual machine with the following characteristics:
- Name = guest
- Install media = network install from http://instructor.example.com/pub/rhel6/dvd
- Memory (RAM) = 768 MB
- CPUs = 1
- Storage device = the logical volume created in the previous step

Within **`virt-manager`**, right-click on the **localhost (QEMU)** item and select **New**. When the "New VM" dialog box appears, type **`guest`** for the name and choose the **Network Install (HTTP, FTP, or NFS)** radio button for installation method. Click the **Forward** button when you are ready to proceed.

Type **`http://instructor.example.com/pub/rhel6/dvd`** in the **URL** field. Click the **Forward** button when you are ready to proceed. If a warning dialog box appears cautioning about the permissions of **`/home/student/.virtinst/boot`**, then click **Yes** and move on.

In the next dialog box, select **`768 MB`** for **Memory (RAM)** and leave the **CPUs** set to 1. Click the **Forward** button when you are ready to proceed.

For storage, select the **Select managed or other existing storage** radio button, then specify the **`/dev/vol0/guest`** pathname. Click the **Forward** button when you are ready to continue.

After reviewing the final dialog box, click **Finish** to complete the creation of the virtual machine and begin your interaction with the Red Hat installer, Anaconda.

When the text-based menus appear, select the appropriate language and keyboard choices for your locale. Each time choose **OK** to proceed to the next menu. Once the network settings have been specified, the graphical installer will appear. Select **View** → **Resize to VM** from the **`virt-manager`** menus.

☐ When the installation begins, choose your keyboard and language. Build your guest system according to the following specifications:
- When asked about the Virtio Block Device, choose **`Re-initialize all`**.
- Choose the appropriate time zone
- Assign **`redhat`** as the root password
- Choose the Desktop software set
- Use the defaults for everything else

Click the **Next** button to move beyond the introductory screen.

On the storage screen, make sure the **Basic Storage Devices** radio button is selected and click **Next**. If a **Warning** dialog box appears suggesting the storage needs to be reinitialized, click the **Re-initialize all** button to wipe the virtual machine's drive.

When the network configuration screen appears, leave the default hostname chosen. The network will be configured because a network installation is being performed. Click then **Next** button to continue.

Choose an appropriate timezone and make sure the **System clock uses UTC** checkbox is checked. Click **Next** to continue.

Specify the root password of **redhat** twice then click the **Next** button. When the **Weak Password** dialog box appears, ignore the warning and click the **Use Anyway** button to continue.

Since the problem exercise said to use the default partitioning scheme, click the **Next** button to advance past the disk partitioning screen. Click the **Write changes to disk** button when the warning dialog box appears. You will see the disk get partitioned and formatted at this point.

The software selection screen will appear next. Select the radio button for the **Desktop** software set instead of the default **Basic Server**. Click the **Next** button to continue. After the software dependency checks complete the installation will begin.

Practice Group Exercise

Search & Learn: Virtual Machine Automatic Boot

What steps must you take to configure a virtual guest to automatically start at boot time?

1. Launch Virtual Machine Manager.
2. Double-click on the guest virtual machine profile.
3. Choose **View** → **Details**
4. Select **Boot Options**
5. Check or uncheck the **Start virtual machine on host boot up** check box and click **Apply**.
6. Add the following to the **/etc/sysconfig/libvirt-guests** file:

```
ON_BOOT=ignore
```

Practice Performance Checklist

Configuring Virtual Machines at Boot-time

- ☐ Configure the **serverX** (vserver) virtual machine to not start at boot time.

- ☐ Configure the **guest** virtual machine to start at boot time.

  Launch the Virtual Machine Manager and double-click on the **guest** virtual machine. Choose **View** → **Details** and select **Boot Options**. Ensure the **Start virtual machine on host boot up** check box is checked and click **Apply** if necessary. Add **`ON_BOOT=ignore`** to **`/etc/sysconfig/libvirt-guests`**.

- ☐ Reboot the physical machine (desktopX).

  ```
  [root@desktopX ~]# reboot
  ```

- ☐ Confirm the **guest** virtual machine started automatically.

  Open the Virtual Machine Manager and verify that **guest** shows that it is running.

- ☐ Configure the **guest** virtual machine to not start at boot time.

  Uncheck the autostart check box following the steps above.

- ☐ Reboot the physical machine (desktopX).

  ```
  [root@desktopX ~]# reboot
  ```

- ☐ Confirm the virtual machine did not start automatically.

  Follow the steps above to ensure that the **guest** virtual machine is not started.

- ☐ IMPORTANT: After you successfully complete the lab, delete the **guest** virtual machine and the logical volume it uses for storage. Those resources will need to be available for the criterion test.

  Open the **Virtual Machine Manager**. If the **guest** virtual machine is running, right-click on the **guest** virtual machine and select **Shutdown** → **Force Off**. Right-click on the **guest** virtual machine and select **Delete**, then click **Delete**.

  1. Open the **System** → **Adminstration** → **Logical Volume Management** application.
  2. In the lefthand navigation panel, select **vol0** → **Logical View** → **guest** .
  3. Select the **Remove Logical Volume** from the lower panel.
  4. Confirm the change and and exit.

Test

Criterion Test

Case Study

Virtual Workstation for William Wonderboy

William Wonderboy just joined the company as a software developer. He needs a machine of his own to write code and do testing without disturbing the work of others. You have been assigned the task of building a virtual machine for him to use.

Create a virtual machine named **wonderboy** with an LVM storage device named **/dev/vol0/wonderboy**. Use the installation media found at the following URI:

- http://instructor.example.com/pub/rhel6/dvd

Mr. Wonderboy's virtual machine must have 768 MB RAM and 10 GB of disk storage.

Use a static IP address of 192.168.0.200+X/24, with a gateway and DNS server of 192.168.0.254. Set the hostname to **hostX.example.com**.

Choose an appropriate time zone. Use **redhat** as the root password.

The virtual disk should be partitioned as follows (you will have to re-initialize the disk):

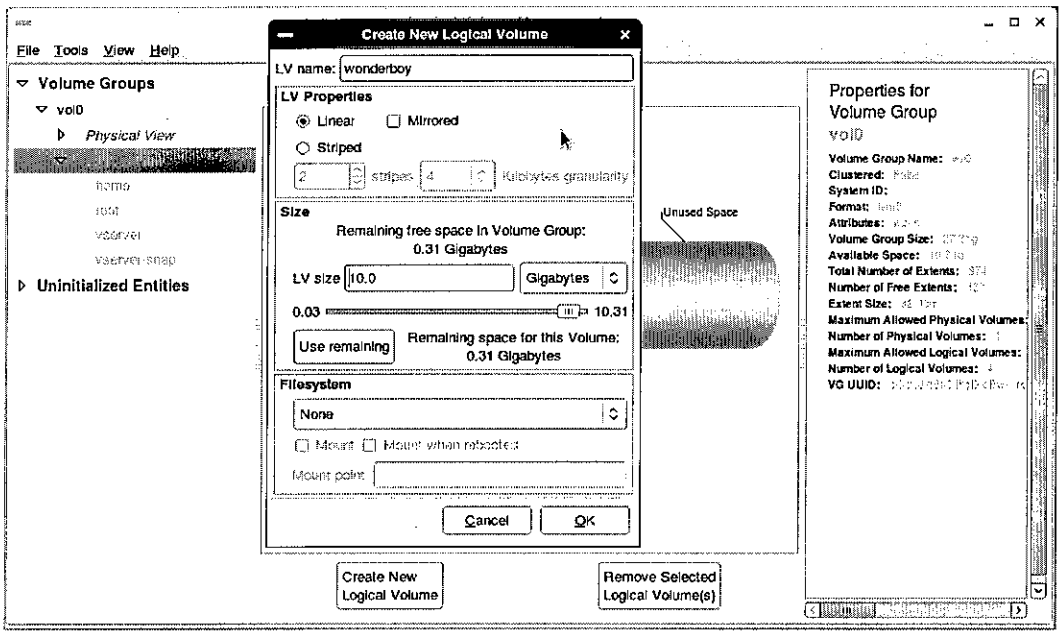
- 250 MB for **/boot**
- 1 GB of swap space
- 6 GB for **/**
- The rest of the space allocated to **/home**

Choose the **Software Development Workstation** software set.

Once the installation is complete, configure NTP to connect to instructor.example.com

Configure this machine to start automatically when the physical host reboots.

1. On desktopX, create a 10 GB logical volume named *wonderboy*.
    1. Open the **System** → **Adminstration** → **Logical Volume Management** application.
    2. In the lefthand navigation panel, select **vol0** → **Logical View** .
    3. Select the **Create New Logical Volume** from the lower panel.
    4. In the resulting dialog, specify a **LV name** of *wonderboy*, and a **LV size** of *10 Gigabytes*. Leave the remaing **LV properties** and **Filesystem** at their default values of *Linear* and *None*.



5. Choose **OK** to confirm the change, and exit.

2. On desktopX, open Virtual Machine Manger.

```
[root@desktopX ~]# virt-manager
```

3. Create a new virtual machine.

   a. Right-click on **localhost(QEMU)**, choose **New**.

   b. In the **Name** field type *wonderboy*.

      In **Choose how you would install the operating system**, select **Network Install (HTTP, FTP, or NFS)**.

   c. **Provide the operating system install URL**, use *http://instructor.example.com/pub/rhel6/dvd*.

      Hit the **Enter** key and notice that the values next to **OS type** and **Version** will auto-populate.

Note

If you receive a message about the search permissions choose **No** to move forward.

   d. Modify **Memory (RAM)** to read **768**. Leave the remaining values as defaults.

e. Choose **Select managed or other existing storage.** Browse to or type in **/dev/vol0/wonderboy**. Leave the remaining values as defaults.

f. Verify values and click **Finish.**

4. Use Anaconda to install the guest.

a. Select Language.

b. Select Keyboard Type.

c. De-select IPv6 support.

d. Select **Basic Storage Devices.**

e. Select **Re-initialize all** or, if this is an installation that is over a previous installation, you will be prompted for **Fresh** or **Upgrade Installation.** Choose **Fresh Installation** if that is the case.

f. Set **Hostname** to *hostX.example.com*

g. Choose **Configure Network.**

i. Click on **Wired** tab (if necessary).

ii. Highlight **System eth0** and click **Edit.**

iii. Click on **IPv4 Settings.**

iv. Change **Method** to **Manual.**

v. Add, IP address: 192.168.0.X+200.

NOTE: Netmask should automatically fill to **24.**

vi. Click the area under the **Gateway** column, then, add 192.168.0.254 for your gateway.

vii. Add, **DNS servers:** 192.168.0.254

viii. Click **Apply** then close Network Connections.

h. Choose appropriate Timezone and check UTC.

i. Enter *redhat* as root's password.

j. Choose **Create Custom Layout**, and create the following partitions.

i. Delete any existing partitions (if necessary).

ii. Create: **Standard partition**, mount point /boot, ext4, size 250MB.

iii. Create: **Standard partition**, File System Type: swap, size 1024MB.

iv. Create: **Standard partition**, mount point /, ext4, size 6144MB.

v. Create: **Standard partition**, mount point /home, ext4, select **Fill to maximum allowable size.**

Select **Next** to continue.

If prompted with **Format Warnings** choose **Format.**

Choose **Write changes to disk.**

k. For **Boot loader configuration**, use defaults.

l. For **Package Selection**, select the **Software Development Workstation** software set. Leave the remaining values as defaults.

m. Monitor the intallation.

n. When prompted, reboot the system.

5. Because we installed a graphical desktop we will see the first-boot **Welcome screen.**

a. Click **Forward** for **License information**, then, **Forward** again.

b. For **Set Up Software Updates**, select **No, I prefer to register at a later time.**

c. When prompted for connecting to Red Hat Network, click on **No thanks, I'll connect later.**

d. Create a User

i. **Username:** *wonderboy.*

ii. **Full Name:** *William Wonderboy.*

iii. **Password:** *redhat.*

iv. **Confirm password:** *redhat.*

e. Date and Time

i. Click **Synchronize date and time over network.**

ii. Remove all current entries by highlighting an entry then clicking delete.

iii. Click on **Add**, then enter instructor.example.com, hit **`Enter`**. Then, click **Forward.**

The system will locate NTP server (instructor.example.com) and continue.

f. You may see **Insufficient memory to configure kdump!** message click **OK.**

g. Click **Finish.**

6. Configure your machine to automatically start when the host machine reboots.

a. In the *virt-manager* window for your guest, choose the **View** → **Details** menu item.

b. Navigate to the *Boot Options* panel.

c. Select the **Start virtual machine on host boot up** check box and click **Apply**.

Control the Boot Process

Write a definition for each of these key terms:

1. bootloader
   a program that loads an operating system kernel into memory and executes it.

2. GRUB
   GRand Unified Bootloader, the bootloader used by Red Hat Enterprise Linux

Practice Performance Checklist

Booting an Alternate Kernel

Perform all of the following steps on serverX.

- ☐ Configure **yum** to point to the **Errata** repository on the **instructor** machine with the following command:

```
[root@serverX ~]# wget http://instructor/pub/gls/errata.repo -O /etc/yum.repos.d/
errata.repo
```

- ☐ Install the **kernel** update that is available. This will take over 3 minutes to install.

```
[root@serverX ~]# yum update -y kernel
```

- ☐ Boot into the new kernel.

  Gracefully reboot the system with the **reboot** command. GRUB will be configured to boot using the new kernel by default.

- ☐ Reboot and choose the old kernel.

  Again, reboot the system with the **reboot** command. When the GRUB countdown appears, hit the **Esc** key to display the GRUB menu. Use the arrow keys to select the lower-numbered kernel then hit **Enter** to begin the boot process.

Runlevel Definitions

1. Write a definition for this key term:

   runlevel
   The state of a system that defines which services are available.

2. In Red Hat Enterprise Linux, what are each of these runlevels typically used for?

   runlevel 5 - Graphical desktop

   runlevel 3 - Multi-user non-GUI

runlevel 1 - Single-user mode, no network (similar to "Safe Mode" in Windows)

Practice Performance Checklist

Changing the root Password

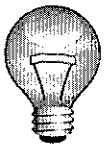
This timed drill is designed to give you practice changing the root password on a system with an unknown root password.

Perform all of the following steps on serverX.

- ☐ Begin by running the **lab-setup-bootbreak-4** script. This will change the root password to something unknown and mark the current time.

```
[root@serverX ~]# lab-setup-bootbreak-4
```

- ☐ Get into the system and reset the root password to **redhat**.



Important

At the release of Red Hat Enterprise Linux 6, there was an SELinux bug which blocked the **passwd** command from working in single-user mode. This is fixed by a bug fix update (see http://rhn.redhat.com/errata/RHBA-2010-0845.html).

If you have the original *selinux-policy* package installed, you must run the **setenforce 0** command in runlevel 1 before the **passwd** command for it to work. After changing the password you should run **setenforce 1** again to put SELinux back in enforcing mode.

Interrupt the GRUB countdown (**Esc** key). Use **e** to edit current configuration. Select **kernel** line to correct with arrow keys. Type **e** again to edit the current line, appending a **Space** and the argument "**single**". Type **b** to boot with the current changes.

```
# setenforce 0
# passwd
Changing password for user root.
New password: redhat
BAD PASSWORD: it is based on a dictionary word
BAD PASSWORD: is too simple
Retype new password: redhat
passwd: all authentication tokens updated successfully.
# setenforce 1
```

- ☐ Once you have reset the password, change the system into runlevel 5 and run the **lab-grade-bootbreak-4** script.

```
# init 5
...
[root@serverX ~]# lab-grade-bootbreak-4
```

- ☐ View the feedback from the script to ensure you completed the task correctly. The grading script will display a time, write it down.
- ☐ Repeat the process again at least five times.
- ☐ Circle your best time.

Practice Performance Checklist

Getting Past a GRUB Misconfiguration

Perform all of the following steps on serverX.

- ☐ Run the **lab-setup-bootbreak-5** script to introduce an issue with the boot process.
- ☐ Fix the issue so the system can boot and you can log in.

  The problem to be solved is a misspelled GRUB directive or file name. The boot process must be interrupted so hit the **Esc** when the GRUB countdown appears. Type the **e** command to display the GRUB configuration that is being used and identify the error. Use the editing commands displayed below the GRUB menu to correct the typographical error. Type the **b** command to accept the changes and begin the boot process.

Practice Performance Checklist

Making Persistent GRUB Changes

Perform all of the following steps on serverX.

- ☐ Reboot and confirm the issue from the previous problem is not persistently fixed. You will need to apply the fix as before to boot the system.

  Repeat the steps you performed in the previous problem to get the system booted enough to display a shell prompt.
- ☐ Edit the configuration file to fix the issue permanently.

  Edit the GRUB configuration file with your favorite text editor to correct the typographical error permanently:

  ```
  [root@serverX ~]# vim /boot/grub/grub.conf
  ```

- ☐ Revert to the older kernel. Ensure that when you reboot, the older kernel is the default kernel.

  Modify the GRUB configuration file so the **`default`** directive selects the older kernel. Remember that GRUB boot stanzas begin numbering from 0.

Search & Learn: Kernel Arguments

1. Install the **`kernel-doc`** package.
2. Reference the material in **`kernel-parameters.txt`** found in the **`/usr/share/doc/kernel-doc*/Documentation/`** directory.
3. Each team must research and summarize the following kernel parameters:

   Team 1:

   - **`console`**

     Console redirection: **`console=ttyS0`**

   Team 2:

   - **`enforcing`**

     SELinux control: **`enforcing=0|1`**

     `enforcing=1` sets Enforcing mode. **`enforcing=0`** sets Permissive mode.

   - **`selinux`**

     SELinux control:**`selinux=0|1`**

     `selinux=0` disables SELinux entirely. **`selinux=1`** enables SELinux.

   Team 3:

   - **`init`**

     Init process: **`init=/bin/bash`**

   Team 4:

   - **`root`**

     Mount root file system:

     `root=/path/to/root/volume`

   - **`ro`**

     `ro` - read-only root file system

   - **`rw`**

rw - read-write root file system

Practice Performance Checklist

Passing Kernel Arguments

Earlier we had to turn off SELinux enforcing mode to change the **root** password in runlevel 1. There is a kernel parameter that allows us to do that without using commands from the shell. Perform the following steps on serverX.

- ☐ Before you reboot your serverX machine, check its default SELinux status by executing the **getenforce** command. Confirm the system normally boots into Enforcing mode.

```
[root@serverX ~]# getenforce
Enforcing
```

- ☐ Reboot your serverX machine and pass **enforcing=0** to the kernel when the system boots.

  Stop the GRUB countdown with the **Esc** key then used the **a** command to add the extra **enforcing=0** argument to the kernel. Type **Enter** to accept the changes and begin the boot process.

- ☐ Once serverX finishes booting, check its SELinux status. Confirm the system booted into Permissive mode.

```
[root@serverX ~]# getenforce
Permissive
```

Practice Performance Checklist

Changing the Default Runlevel

You are configuring a new system that you will be accessing remotely. The system is currently booting into runlevel 5 by default, but this machine will be housed in a data center where you will only log into it remotely. Perform the following steps on serverX.

- ☐ Change serverX to boot to runlevel 3 by default.

  Change the line in **/etc/inittab** to the following:

```
id:3:initdefault:
```

- ☐ Reboot serverX.

```
[root@serverX ~]# reboot
```

- ☐ You have successfully completed this lab if serverX boots into textual mode without human interaction.

Test
Criterion Test

Exercise
Bad Brian Blowup Recovery

Before you begin...

Run **`lab-setup-bootbreak`** on desktopX to reset serverX back to its original state.

Brian was a summer intern who acted as a system administrator for one of your critical servers, serverX. Your company's strained relationship with him finally blew up and resulted in his immediate firing. Sadly, when Bad Brian went out the door he took the root password for serverX with him.

You have been assigned the responsibility of getting control of serverX back:

1. Run the **`lab-setup-bootbreak-6`** script on serverX to prepare it for this lab exercise. This will assign your system with an unknown root password and reboot the system.

2. Set the root password to **`redhat`**.

   Because the system won't initialize it will be necessary to boot into runlevel 1 and fix the misconfigured ram disk entry and root's password.

   1. Intercept grub during the initialization process by hitting any key when the grub menu displays.

   2. Highlight the title line of choice and hit **e** to edit.

   3. Highlight the ramdisk line and hit **e** to edit.

   4. Modify the ram disk line by removing *-BROKEN* from the entry, hit **<ENTER>**.

   5. Highlight the kernel line then hit **e** to edit.

   6. Add a space and the number one ("1") at the end of the kernel line, hit **<ENTER>**, then hit **b** to boot the system using your temporary modifications to grub.

   7. When the shell prompt displays run **passwd** and set root's password to *redhat*.

      (Due to a bug in early releases of Red Hat Enterprise Linux 6, the single user mode shell did not have the correct SELinux context to execute the **passwd** command. Although a fix was soon released, the solutions below temporarily suspend and restore SELinux as a reminder of this issue.)

```
Telling INIT to go to single user mode.
[root@localhost /]# setenforce 0
[root@localhost /]# passwd
```

```
Changing password for user root.
New password: redhat
BAD PASSWORD: it is based on a dictionary word
BAD PASSWORD: is too simple
Retype new password: redhat
passwd: all authentication tokens updated successfully.
[root@localhost /]# setenforce 1
```

8. Type **exit** to boot the system into multiuser mode, bringing up the network so additional fixes can be made.

3. Install the kernel update, but configure the system so the old kernel will continue to be used by default.

```
[root@server1 ~]# yum update kernel
...
Dependencies Resolved

================================================================================
 Package               Arch         Version                  Repository     Size
================================================================================
Installing:
 kernel                x86_64       2.6.32-71.7.1.el6        Updates        22 M
Updating for dependencies:
 kernel-firmware       noarch       2.6.32-71.7.1.el6        Updates       1.1 M

Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       1 Package(s)

Total download size: 23 M
Is this ok [y/N]: y
...
Complete!
```

Edit **/boot/grub/grub.conf** changing *default=0* to match the index of the old kernel stanza, such as *default=1*. (Recall that the first stanza is considered stanza *0*).

NOTE: You should also inspect the ram disk line to ensure that it is correct.

4. Pass the **selinux=1** argument to the kernel at boot time.

   Edit **/boot/grub/grub.conf**, adding *selinux=1* to the end of the kernel line past all other arguments.

5. Set runlevel 3 as the default.

   Edit **/etc/inittab**, changing *5* to *3* in the second field of the only active line.

6. Once your system is booted, run the **lab-grade-bootbreak-6** script on serverX to determine how well you did.

Deploy File Sharing Services

Four Steps for Deploying a Network Service

Enter the appropriate menu selection for each step:

1. Install: System → Administration → Add/Remove Software
2. Start: System → Administration → Services
3. Enable: System → Administration → Services
4. Test: Use an FTP client such as **Firefox** or **Nautilus** to see if the service is working (can you download a file from the server?)

Practice Performance Checklist

Deploy an FTP server

Perform the following steps on serverX unless directed otherwise.

Deploy an FTP server. Verify it is working and enabled.

- ☐ Install the **vsftpd** package.

  To install the FTP server, go to: **System** → **Administration** → **Add/Remove Software**. Type **vsftp** then the **Find** button.

  Ensure that **Very Secure Ftp Daemon** has a check mark, then click the **Apply** button.

- ☐ Start the **vsftpd** service.

  To start the **vsftpd** service, go to: **System** → **Administration** → **Services**. Find and highlight the **vsftpd** entry in the list on the left.

  Click on the **Start** button up above.

- ☐ Enable the **vsftpd** service.

  To enable the **vsftpd** service, go to: **System** → **Administration** → **Services**. Find and highlight the **vsftpd** entry in the list on the left.

  Click on the **Enable** button up above.

- ☐ Publish a copy of **/etc/hosts** to the anonymous FTP document root.

  Use **Nautilus** (as **root**) to copy **/etc/hosts** to the **/var/ftp/** directory.

- ☐ Test the FTP server on desktopX with an ftp client (**Nautilus**) to connect to the server ftp://serverX.example.com. Download the **hosts** file to student's home directory.

Note

Although you could use **Firefox** to test your FTP server, use **Nautilus** instead because it can be used to test FTP authentication.

To test the **vsftpd** service, go to: **Places** → **Connect to Server...**.

Leave as **Public FTP**. Enter **serverX.example.com** as **Server**, then click the **Connect** button.

Right click the **hosts** file and choose **Copy to** → **Home Folder**.

Practice Performance Checklist

Restrict FTP Access

Perform the following steps on serverX unless directed otherwise.

Because FTP is an insecure protocol, it is a security risk to allow normal users to connect and authenticate. Configure your FTP server to permit anonymous connections only.

- ☐ Use an ftp client to connect to **serverX.example.com** and authenticate as **student** to confirm it allows non-anonymous users.

  To test the **vsftpd** service, go to: **Places** → **Connect to Server...**.

  Change **Service type** to be **FTP (with login)**. Enter **serverX.example.com** as **Server**, **student** as **User Name**, then click the **Connect** button.

- ☐ Which file is the main vsftpd configuration file?

  /etc/vsftpd/vsftpd.conf

- ☐ Which configuration file directive controls non-anonymous access to the system?

  local_enable

- ☐ Configure vsftpd to deny access by local, non-anonymous users.

  Edit the **/etc/vsftpd/vsftpd.conf** configuration file and modify the following line as:

  ```
  local_enable=no
  ```

  To restart the **vsftpd** service, go to: **System** → **Administration** → **Services**. Find and highlight the **vsftpd** entry in the list on the left.

  Click on the **Restart** button up above.

- Retest your server and confirm student no longer has authenticated access to your FTP server.

  To test the **vsftpd** service, go to: **Places** → **Connect to Server...**.

  Change **Service type** to be **FTP (with login)**. Enter **serverX.example.com** as **Server**, **student** as **User Name**, then click the **Connect** button.

Practice Performance Checklist

Deploy a Web Server

Perform the following steps on serverX unless directed otherwise.

The instructor will split up the class into groups. Once you are in your group, do the following:

Given that the name of the web server package is **httpd**, deploy a web server on serverX. It should provide HTTP file services. It should be active when your server is rebooted.

- Install the **httpd** package.

  To install the Apache web server, go to: **System** → **Administration** → **Add/Remove Software**. Type **httpd** then the **Find** button.

  Ensure that **Apache HTTP Server** has a check mark (and optionally, **Documentation for the Apache HTTP server**), then click the **Apply** button.

- Start the **httpd** service.

  To start the **httpd** service, go to: **System** → **Administration** → **Services**. Find and highlight the **httpd** entry in the list on the left.

  Click on the **Start** button up above.

- Enable the **httpd** service.

  To enable the **httpd** service, go to: **System** → **Administration** → **Services**. Find and highlight the **httpd** entry in the list on the left.

  Click on the **Enable** button up above.

- Create a symbolic link in your web server document root to the **/pub** directory in your FTP server and call it **pub**.

```
[root@serverX ~]# cd /var/www/html
[root@serverX html]# ln -s ../../ftp/pub pub
```

- Create an **index.html** file in the document root of your web server with the following contents:

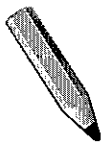
```
<h1>Classroom Web Services</h1>
```

```
<p>
<a href="pub">Click here</a> to view public files.
</p>
```

- ☐ Reboot and verify this content is available through your web browser before you notify the public to ensure your customers can access it as well.

- ☐ Test the web server using the **Firefox** browser.

  Pointing the **Firefox** browser to *http://serverX.example.com*



Test

Criterion Test

Performance Checklist

Deploy File Sharing Services

Before you begin...

Run **`lab-setup-server`** on desktopX to prepare serverX for the exercise.

Nickel and Copper Cutlery want to publish an on-line catalog to their customers. Deploy FTP and HTTP services on serverX and confirm they are working and enabled at boot.

Perform the following steps on serverX unless directed otherwise.

- ☐ Create a file called **`index.html`** with exactly two lines that contain the following content:

  ```
  NICKEL AND COPPER CUTLERY
  On-line catalog coming soon!
  ```

- ☐ Configure serverX to provide both FTP and web services. Disable non-anonymous FTP access.

  Install and enable the web service:

  To install the Apache web server, go to: **System** → **Administration** → **Add/Remove Software**. Type **`httpd`** then the **Find** button.

  Ensure that **Apache HTTP Server** has a check mark (and optionally, **Documentation for the Apache HTTP server**), then click the **Apply** button.

  To start and enable the **`httpd`** service, go to: **System** → **Administration** → **Services**. Find and highlight the **httpd** entry in the list on the left.

  Click on the **Start** button up above.

  Click on the **Enable** button up above.

  Install the ftp service:

To install the FTP server, go to: **System** → **Administration** → **Add/Remove Software**. Type **vsftp** then the **Find** button.

Ensure that **Very Secure Ftp Daemon** has a check mark, then click the **Apply** button.

Open **/etc/vsftpd/vsftpd.conf** in a text editor, find the **local_enable** setting, and set it to **NO**. Save the file when you have finished.

Enable the ftp service:

To start and enable the **vsftpd** service, go to: **System** → **Administration** → **Services**. Find and highlight the **vsftpd** entry in the list on the left.

Click on the **Start** button up above.

Click on the **Enable** button up above.

- ☐ Configure your serverX machine to serve identical file content to both anonymous FTP and HTTP users. The following URLs should both display the file you created above:

  - ftp://serverX/pub/index.html
  - http://serverX/index.html

  Because files outside of **/var/ftp** are not accessible to anonymous FTP users by default, you will need to create **index.html** in **/var/ftp/pub/**, then make a symbolic link to it from the web server's DocumentRoot, **/var/www/html/**

  First, create **/var/ftp/pub/index.html** with the content described above:

```
NICKEL AND COPPER CUTLERY
On-line catalog coming soon!
```

  Next, create the symbolic link:

```
[root@serverX ~]# ln -s /var/ftp/pub/index.html /var/www/html/
```

- ☐ Reboot your serverX machine. Use a web browser to confirm your services are functioning correctly.

Secure Network Services

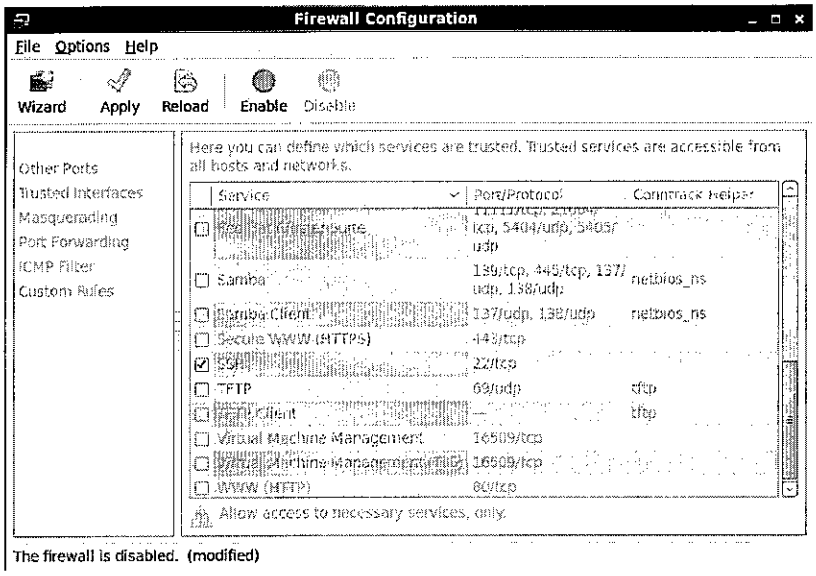
Practice Performance Checklist

Enable and Disable the Firewall

Perform the following steps on serverX unless directed otherwise.

☐ Activate the firewall with the default ports enabled.

- Open **System** → **Applications** → **Firewall**.
- Select **Enable**, and then **Apply**.



☐ Deactivate the firewall.

- Open **System** → **Applications** → **Firewall**.
- Select **Disable**, and then **Apply**.

Practice Performance Checklist

Allow HTTP and FTP through the Firewall

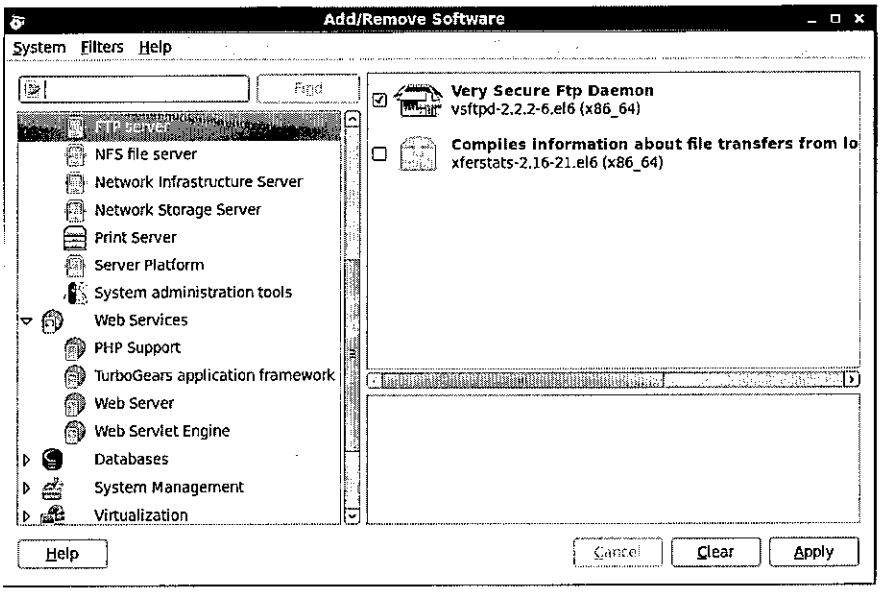
Perform the following steps on serverX unless directed otherwise.

☐ Enable the firewall

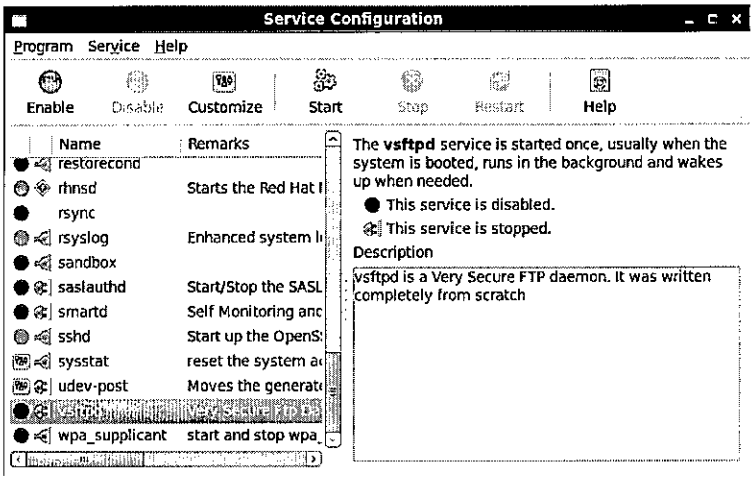
- Open **System** → **Applications** → **Firewall**.
- Select **Enable**, and then **Apply**.

☐ Deploy an FTP server on serverX

- Open **System** → **Applications** → **Add/Remove Software.**
- Navigate to **Servers** → **FTP Server.**
- Select the **Very Secure FTP Dasemon** (vsftpd).
- Select **Apply** to install the package.



- Open **System** → **Applications** → **Services.**
- In the lefthand panel, navigate to **vsftpd.**
- Select **Enable** and **Start** to start the FTP server.



- ☐ Deploy an HTTP server
  - Open **System** → **Applications** → **Add/Remove Software.**
    - Navigate to **Web Services** → **Web Server.**
    - Select the **Apache HTTP Server** (httpd).
    - **Apply** to install the package.
  - Open **System** → **Applications** → **Services.**
    - In the lefthand panel, navigate to **httpd.**
    - Select **Enable** and **Start** to start the HTTP server.
- ☐ Allow the FTP, HTTP, and SSH services through the firewall
  - Open **System** → **Applications** → **Firewall.**
  - In the default **Trusted Services** panel, enable **FTP**, **WWW (HTTP)**, and **SSH.**
  - Choose **Apply** to commint your change.

Practice Quiz

Basic SELinux Concepts

1. To which of the following does SELinux apply security context (check all that apply)?

   (select one or more of the following...)
   a. Ports
   b. Processes
   c. Files
   d. Directories
   e. Remote file systems

2. SELinux can be used to:

   (select one or more of the following...)
   a. Protect a service from running on other ports.
   b. Protect user data from applications like the web server
   c. Block remote systems from accessing local ports

      This describes a firewall.
   d. Keep the system updated

      This describes something like Red Hat Network.
   e. Access a web server

This describes a web browser like Firefox.

3. Which of the following are standard SELinux context types?

   (select one or more of the following...)
   a. selinux_type

      This is non-existent.
   b. object_r

      This is an SELinux role.
   c. httpd_sys_content_t
   d. tmp_t
   e. user_u

      This is an SELinux context user.

Practice Quiz

SELinux Modes

1. SELinux permissive mode allows logging, but not protection.

2. SELinux enforcing mode protects the system.

3. Which of the following are valid SELinux modes?

   (select one or more of the following...)
   a. enforcing
   b. testing
   c. permissive
   d. disabled
   e. logging

Practice Quiz

SELinux Type Contexts on Files and Processes

Deploy a web server.

For each of the following, find the SELinux type context.

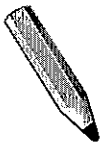
1. /var/www/html/ has httpd_sys_content_t type

2. /tmp/ has tmp_t type

3. /etc/hosts has etc_t type.

4. The **`httpd`** process has httpd_t type.

5. /etc/httpd/conf/httpd.conf has _httpd_config_t type.
6. /home/student has _user_home_dir_t type.
7. The **sshd** process has _sshd_t type.



Test

Criterion Test

Performance Checklist

Secure Web Services

Before you begin...

Execute **`lab-setup-secure-web`** as **`root`** on desktopX to prepare serverX for the criterion test.

Perform the following steps on serverX unless directed otherwise.

- ☐ Deploy a web server on serverX.
  - Open **System** → **Applications** → **Add/Remove Software**.
    - Navigate to **Web Services** → **Web Server**.
    - Select the **Apache HTTP Server** (httpd).
    - **Apply** to install the package.
  - Open **System** → **Applications** → **Services**.
    - In the lefthand panel, navigate to **httpd**.
    - Select **Enable** and **Start** to start the HTTP server.
- ☐ Install the **`mod_ssl`** package.
  - Open **System** → **Applications** → **Add/Remove Software**.
    - Navigate to **Web Services** → **Web Server**.
    - Select the **SSL/TLS module for the Apache HTTP Server** (mod_ssl).

      Caution! Do not select the similarly named *mod_nss* package.
    - **Apply** to install the package.
- ☐ Restart the web service.
  - Open **System** → **Applications** → **Services**.
    - In the lefthand panel, navigate to **httpd**.

- Select **Restart** to restart the HTTP server.

☐ Enable the firewall and allow the HTTP and HTTPS ports.

☐ Create **/tmp/d.html** and *move* it to the web server document root.

```
[student@serverX ~]$ touch /tmp/d.html
[student@serverX ~]$ su -
[root@serverX ~]# mv /tmp/d.html /var/www/html/
```

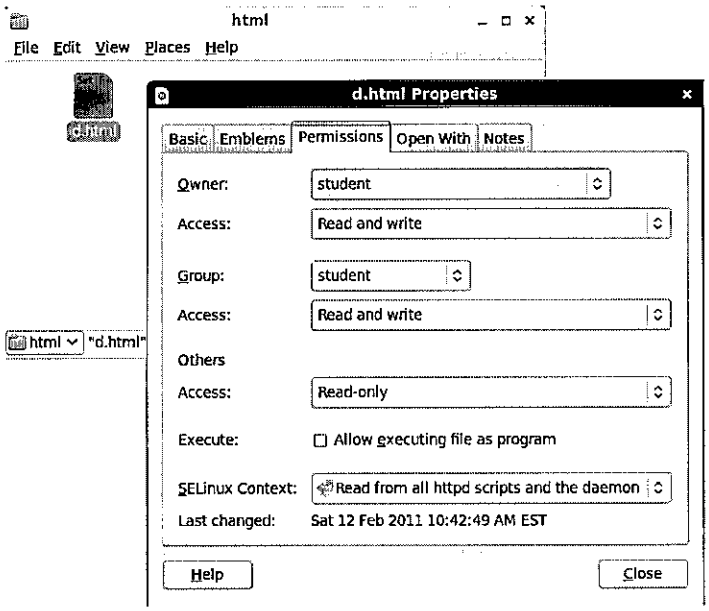
☐ Try to display *http://serverX/d.html* - it should fail.

☐ Change the context on **d.html** to **httpd_sys_content_t**.

- As root, launch a **Nautilus** browser and browse **/var/www/html**.

```
[student@serverX ~]$ su -
[root@serverX ~]# nautilus /var/www/html
```

- Right-click on the file **d.html**, choose **Properties**, and navigate to the **Permissions** panel.
- Adjust the SELinux context to **Read for all httpd scripts and the daemon** .



- ☐ Run the **`lab-grade-secure-web`** grading script to confirm you did the exercise correctly.

Comprehensive Review

Practice Resequencing Exercise

Deploying Secure Network Services

Below are the steps you will take to deploy network services. Assume you will deploy VNC, FTP, and HTTP services in that order. Mark the order the steps should be taken:

7 Deploy a web server.
2 Connect to a remote serverZ for all tasks. The **student** password is **student**; the **root** password is **redhat**.
10 Restore the SELinux context for the files in the HTTP server document root and the FTP server document root.
3 Deploy a VNC server for the **student** user on display 2. Use a password of **redhat**.
12 Verify that you can view the files in the HTTP server document root and the FTP server document root.
6 Move the **/tmp/ftp2.txt** file to the FTP server document root.
8 Create the **/tmp/http1.html** and **/tmp/http2.html** files.
4 Deploy an FTP server.
1 serverZ = server__.example.com
5 Create the **/tmp/ftp1.txt** and **/tmp/ftp2.txt** files.
11 Enable the firewall and allow access to the HTTP, FTP, SSH and VNC (port 5902) services.
9 Move the **/tmp/http1.html** file to the HTTP server document root.