8

User Administration

CERTIFICATION OBJECTIVES

Fundamental to the tasks associated with Linux administration is the management of users and groups. In this chapter, you'll examine different ways to manage the variety of users and groups available to Linux. Important skills in this area range from the simple login to user account management, group membership, group collaboration, and network authentication. The configuration of administrative privileges for Linux users can help the master administrator distribute responsibilities to others.

You'll see how to manage these tasks from the command line, with the help of the files of the shadow password suite. You'll also use tools like the User Manager and the Authentication Configuration tool to set up some of these tasks. As you should expect, Red Hat GUI tools can't do it all, which emphasizes the importance of understanding user management from the command line.

INSIDE THE EXAM

This chapter addresses several RHCSA objectives. Briefly explained, these objectives include the following:

■ Log in and switch users in multi-user runlevels

Briefly, that means you need to know how to log in with regular accounts when RHEL 6 is running in standard runlevels 3 and 5. To switch users, you need to know how to log out and log back in with a second account. Simple enough.

■ Create, delete, and modify local user accounts

■ Change and adjust password aging for local user accounts

■ Create, delete, and modify local groups , adjust group memberships

You could use commands like **useradd**, **usermod**, **groupadd**, **groupmod**, and **chage**, as well as the User Manager to accomplish these tasks. While this chapter explains how you can use both types of tools, there is no guarantee that the User Manager will be available during an exam.

■ Create and configure set-gid directories for collaboration

When the RHCT exam was active, the related objective was to "Configure filesystem permissions for collaboration." In other words, the objective is now more specific— you're told how to set one or more directories for collaboration between a group of users.

■ Configure a system to use an existing LDAP directory service for user and group information

In other words, you need to know how to take advantage of a Lightweight Directory Access Protocol (LDAP) server with changes to appropriate configuration files.

User Account Management

You need to know how to create and configure users. This means knowing how to configure and modify accounts, work with passwords, and organize users in groups. You also need to know how to configure the environment associated with each user account: in configuration files and in user settings.

If you've installed RHEL 6 via Kickstart or in text mode, or somehow otherwise avoided the First Boot process described in Chapter 1, the default Red Hat installation includes just a single login account: root. While no other accounts are required, it's important to set up some regular user accounts. Even if you're going to be the only user on the system, it's a good idea to create at least one nonadministrative account for day-to-day work. Then you can use the root account only when it's necessary to administer the system. Accounts can be added to Red Hat Enterprise Linux systems using various utilities, including direct editing of password configuration files (the manual method), the **useradd** command (the command line method), and the User Manager utility (the graphical method).

Different Kinds of Users

There are three basic types of Linux user accounts: administrative (root), regular, and service. The administrative root account is automatically created when Linux is installed, and it has administrative privileges for all services on a Linux system. A cracker who has a chance to take control of this account can take full control of that system.

For the times when you do log in as an administrator, RHEL builds in safeguards for root users. Log in as the root user, and then run the **alias** command. You'll see entries such as the following:

```
alias rm='rm -i'
```

Due to this particular alias, when the root user runs the **rm** command, the shell actually executes the **rm -i** command, which prompts for confirmation before the **rm** command deletes a file. Unfortunately, a command such as **rm -rf** *directoryname* supersedes this safety setting.

on the
jo b

As suggested by the technical editor, some administrators set a different alias for the rm command: alias rm='mv -t ~/.Trash'. *Files in that directory are like a standard trashbin; some administrators may set up a cron job, such as those described in Chapter 9, to delete files from that directory on a periodic basis. A trash directory is already available in the GNOME desktop, in each user's .local/share/Trash/files/ subdirectory.*

Regular users have the necessary privileges to perform standard tasks on a Linux computer. They can access programs such as word processors, databases, and web browsers. They can store files in their own home directories. Since regular users do not normally have administrative privileges, they cannot accidentally delete critical operating system configuration files. You can assign a regular account to most users, safe in the knowledge that they can't disrupt a system with the privileges they have on that account.

Services such as Apache, Squid, mail, games, and printing have their own individual service accounts. These accounts exist to allow each of these services to interact with Linux systems. Normally, you won't need to change any service account, but if you see that someone has logged in through one of these accounts, be wary. Someone may have broken into your system.

on the
jo b

One resource for checking whether your system has been cracked is the Distributed Intrusion Detection System at www.dshield.org. Check your public IP address against its database. If your system has been cracked, it's likely that someone is using it to attack other systems. While there are "false positives," IP addresses that have been cracked are logged in the www.dshield.org database.

on the
jo b

To review recent logins, run the utmpdump /var/log/wtmp | less *command. If the login is from a remote location, it will be associated with a specific IP address outside your network.*

The Shadow Password Suite

When Unix was first developed back in the 1960s and 1970s, security was not such a serious concern. Everything required for user and group management was contained in the /etc/passwd and /etc/group files. As suggested by the name, passwords were originally in the /etc/passwd file. The problem is that file is "world-readable." Anyone with a copy of that file, before the shadow password suite, would have a copy of the

password for every user. Even passwords that are encrypted in that file can eventually be decrypted. That is the motivation behind the development of the shadow password suite, where more sensitive information was moved to other files, readable only by the root administrative user.

The four files of the shadow password suite are /etc/passwd, /etc/group, /etc/shadow, and /etc/gshadow. Defaults in these files are driven by the /etc/login.defs file.

The /etc/passwd File

The /etc/passwd file contains basic information about every user. Open that file in a text editor. Browse around a bit. Atop the file is basic information for the root administrative user. Other users in this file may relate to services such as mail, ftp, and sshd. They may be specific users designed for logins.

There are seven columns of information in the /etc/passwd file, delineated by colons. Each column in /etc/passwd includes specific information described in Table 8-1.

TABLE 8-1 The Anatomy of /etc/passwd

Field	Example	Purpose
Username	mj	The user logs in with this name. Usernames can include hyphens (-) or underscores (_). However, they should not start with a number or include uppercase letters.
Password	x	The password. You should see either an *x*, an asterisk (*), or a seemingly random group of letters and numbers. An *x* points to /etc/shadow for the actual password. An asterisk means the account is disabled. A random group of letters and numbers represents the encrypted password.
User ID	500	The unique numeric user ID (UID) for that user. By default, Red Hat starts user IDs at 500.
Group ID	500	The numeric group ID (GID) associated with that user. By default, RHEL creates a new group for every new user, and the number matches the UID. Some other Linux and Unix systems assign all users to the default Users group (GID=100).
User info	Michael Jang	You can enter any information of your choice in this field. Standard options include the user's full name, telephone number, e-mail address, or physical location. You can leave this blank.
Home Directory	/home/mj	By default, RHEL places new home directories in /home/*username*.
Login Shell	/bin/bash	By default, RHEL assigns users to the bash shell. You can change this to any legal shell that you have installed.

The RHEL 6 version of /etc/passwd includes more secure features for user accounts when compared to some other Linux distributions. The only accounts with a real login shell are user accounts. If a cracker somehow breaks into a service account such as mail or nobody, with the false /sbin/nologin shell, that user doesn't automatically get access to the command line.

The /etc/group File

Every Linux user is assigned to a group. By default in RHEL 6, every user gets his own private group. The user is the only member of that group, as defined in the /etc/group configuration file. Open that file in a text editor. Browse around a bit. The first line in this file specifies information for the root administrative user's group. Some service users include other users as members of that group. For example, user qemu is a member of the kvm group, which gives services associated with the QEMU emulator privileges with the Kernel-based Virtual Machine (KVM).

There are four columns of information in the /etc/group file, delineated by colons. Each column in /etc/group specifies information described in Table 8-2.

The /etc/shadow File

The /etc/shadow file is a supplement to /etc/passwd. While it contains eight columns of information, the first column contains the same list of usernames as documented in /etc/passwd. As long as there's an *x* in the second column of each /etc/passwd entry, Linux knows to look at /etc/shadow for more information. Open that file in a text editor. Browse around a bit. You'll see the same pattern of information, starting with information for the root administrative user.

As shown in Table 8-3, while it includes the encrypted password in the second column, the remaining information relates to the way passwords are managed. In fact, the first two characters of the second column are based on the encryption hash for the password. If you see a $1, the password is hashed to the Message Digest 5 (MD5) algorithm, the standard through RHEL 5. If you see a $6, the password is protected with the 512-bit Secure Hash Algorithm (SHA-512), the standard for RHEL 6.

The /etc/gshadow File

The /etc/gshadow file is the group configuration file in the shadow password suite. It includes the administrator for the group. If desired, you can even configure a hashed password for that group administrator. Table 8-4 describes the columns in /etc/gshadow, from left to right.

TABLE 8-2	Field	Example	Purpose
The Anatomy of /etc/group	Groupname	mj	Each user gets his own group, with the same name as his username. You can also create unique group names.
	Password	x	The password. You should see either an *x* or a seemingly random group of letters and numbers. An *x* points to /etc/gshadow for the actual password. A random group of letters and numbers represents the encrypted password.
	Group ID	500	The numeric group ID (GID) associated with that user. By default, RHEL creates a new group for every new user. If you want to create a special group such as managers, you should assign a GID number outside the standard range; otherwise, Red Hat GIDs and UIDs would probably get out of sequence.
	Group members	mj,vp	Lists the usernames that are members of the group. If it's blank, and there is a username that is identical to the group name, that user is the only member of that group.

TABLE 8-3	Column	Field	Description
The Anatomy of /etc/shadow	1	Username	Username
	2	Password	Encrypted password; requires an *x* in the second column of /etc/passwd
	3	Password history	Date of the last password change, in number of days after January 1, 1970
	4	mindays	Minimum number of days that a user must keep a password
	5	maxdays	Maximum number of days after which a password must be changed
	6	warndays	Number of days before password expiration when a warning is given
	7	inactive	Number of days after password expiration when an account is made inactive
	8	disabled	Number of days after password expiration when an account is disabled

TABLE 8-4			
	Field	**Example**	**Purpose**
The Anatomy of /etc/gshadow	Groupname	mj	Each user gets his own group, with the same name as his username. Specific users may be assigned as administrators for unique groups.
	Password	!	Most groups have a *!*, which indicates no password; some groups may have a hashed password similar to that shown in the /etc/shadow file.
	Group ID	500	The numeric group ID (GID) associated with that user. By default, RHEL creates a new group for every new user. If you want to create a special group such as managers, you should assign a GID number outside the standard range; otherwise, Red Hat GIDs and UIDs would probably get out of sequence.
	Group members	mj,vp	A comma-delineated list of usernames that are members of the group. If it's blank, and there is a username that is identical to the group name, that user is the only member of that group.

The /etc/login.defs File

The /etc/login.defs file provides the baseline for a number of parameters in the shadow password suite. This section provides a brief analysis of each active directive in the default version of this file. As you'll see, the directives go somewhat beyond authentication. The first directive specifies the directory with locally delivered e-mail, listed by username:

```
MAIL_DIR /var/spool/mail
```

The next four directives relate to default password aging information. The directives are explained in the file comment, and in Table 8-5.

TABLE 8-5		
	Directive	**Purpose**
/etc/login.defs Password Aging Directives	PASS_MAX_DAYS	After this number of days, the password must be changed.
	PASS_MIN_DAYS	Passwords must be kept for at least this number of days.
	PASS_MIN_LEN	A warning is given when a user tries to use a password shorter than this length.
	PASS_WARN_AGE	Users are warned this number of days before PASS_MAX_DAYS.

As suggested earlier, User ID (UID) and Group ID (GID) numbers for regular users and groups start at 500. Since Linux supports UID and GID numbers above 4 billion (actually, up to 2^{32}), the maximum UID and GID numbers of 60000 as defined in the /etc/login.defs file may seem strange. However, it leaves higher numbers available for other authentication databases, such as those associated with LDAP and Microsoft Windows (via Samba). As suggested by the directives, **UID_MIN** specifies the minimum UID, **UID_MAX** specifies the maximum UID, and so on:

```
UID_MIN   500
UID_MAX   60000
GID_MIN   500
GID_MAX   60000
```

Normally, when the **useradd** command is run to create a new user, it automatically creates home directories as well, which is confirmed by the following directive:

```
CREATE_HOME yes
```

As described later in this chapter, other files drive a value of umask. But if those other files did not exist, this directive would govern the default umask for regular users:

```
UMASK     077
```

The following directive is critical in the implementation of the User Private Group scheme, where new users are also made members of their own private group, normally with the same UID and GID numbers. It means when new users are created (or deleted), the associated group is also added (or deleted):

```
USERGROUPS_ENAB yes
```

Finally, the following directive determines the algorithm used to encrypt passwords, normally SHA 512 for RHEL 6:

```
ENCRYPT_METHOD SHA512
```

Different encryption methods may be set up with the Authentication Configuration tool described later in this chapter.

Command Line Tools

There are two basic ways to add users through the command line interface. You can add users directly by editing the /etc/passwd file in a text editor such as vi. To this end, the **vipw** and **vigr** were described in Chapter 3. Alternatively, you can use text commands customized for the purpose.

Adding Users Directly

Open the /etc/passwd file in the text editor of your choice. As described in Chapter 3, you can do so with the **vipw** command. However, if you add users by directly editing the files of the shadow password suite, you'll have to do two more things:

- Add a user home directory. For example, for user donna, you'd have to add the /home/donna home directory, making sure that user donna and group donna both have ownership of that directory.
- Populate the user home directory. The default option is to copy the files from the /etc/skel directory, discussed later in this chapter. You'd also have to make sure that user donna and group donna have ownership of those files copied to the /home/donna directory.

Add Users to a Group Directly

Every Linux user is normally assigned to a group, at least his own private group. As implied in Chapter 3, the GID number listed in the /etc/group file has to match that shown for that user in the /etc/passwd file. The user is the only member of that group.

Of course, users can be members of other groups as well. For example, if to create a group named project, you could add the entries to the /etc/group and /etc/gshadow files. One way to do so in a text editor is with the **vigr** command. For example, the following entry might be appropriate for a group named project:

```
project:x:60001:
```

The number 60001 is used, as that is beyond the limit of the **GID_MAX** directive from the /etc/login.defs file described earlier. But that's just arbitrary. There's no prohibition against a lower number, as long as it is above 500 and does not interfere with existing GIDs. However, it is convenient when the UID and GID numbers of regular users match. In fact, it's important, as you'll see in the discussion of the /etc/bashrc file later in this chapter.

Of course, for a group to be useful, you'd have to add users already configured in the /etc/passwd file at the end of the line. The following example assumes these users already exist.

```
project:x:60001:michael,elizabeth,stephanie,tim
```

You'd also have to add this group to the /etc/gshadow file. You could do so directly with the **vigr -s** command. Alternatively, to set up a group administrator with a password, you could run the **gpasswd** command. For example, the **gpasswd project** command would set up a password for administering the group, associated with the **newgrp** and **sg** commands described later in this chapter. It would automatically add the encrypted password with the given group name to the /etc/gshadow file.

Add Users at the Command Line

Alternatively, you can automate this process with the **useradd** command. The **useradd pm** command would add user pm to the /etc/passwd file. In addition, the **useradd** command creates the /home/pm home directory; adds the standard files from the /etc/skel directory; and assigns the default shell, /bin/bash. But **useradd** is versatile. It includes a number of command options shown in Table 8-6.

TABLE 8-6	Option	Purpose
useradd Command Options	-u *UID*	Overrides the default assigned *UID*. By default, in RHEL this starts at 500 and can continue sequentially the maximum number of users supported by kernel 2.6, which is 2^{32}, something over four billion users.
	-g *GID*	Overrides the default assigned *GID*. By default, RHEL uses the same *GID* and *UID* numbers to each user. If you assign a *GID*, it must be either 100 (users) or already otherwise exist.
	-c *info*	Enters the comment of your choice about the user, such as her name.
	-d *dir*	Overrides the default home directory for the user, /home/*username*.
	-e *YYYY-MM-DD*	Sets an expiration date for the user account.
	-f *num*	Specifies a number of days after password expiration when the account is disabled.
	-G *group1,group2*	Makes the user a member of *group1* and *group2*, based on their current names as defined in the /etc/group file. A space between *group1* and *group2* would lead to an error.
	-s *shell*	Overrides the default shell for the user, /bin/bash.

Assign a Password

Once a new user is created, you can use the **passwd** *username* command to assign a password to that user. For example, the **passwd pm** command prompts you to assign a new password to user pm. RHEL is configured to discourage passwords that are based on dictionary words, shorter than five characters, too simple, based on palindromes, and other, similar criteria for security reasons. Nevertheless, such passwords are legal, and such a password is accepted by the **passwd** command when entered a second time.

Add or Delete a Group at the Command Line

When it's appropriate to add a special group to the shadow password suite, you may want to use the **groupadd** command. Generally, you'll want to use it with the **-g** switch. For example, the following command would set up a special project group with a GID of 60001:

```
# groupadd -g 60001 project
```

If you don't use the **-g** switch, the **groupadd** command takes the next available GID number. For example, if two regular users are configured on a system, they each have UID and GID numbers of 500 and 501, respectively. If you've run the **groupadd project** command without specifying a GID number, the project group is assigned a GID of 502. The next regular user that's created would get a UID of 502 and a GID of 503, which could lead to confusion.

Fortunately, the command to delete a group is simpler. If the project group has completed its work, you can delete that group from the shadow password suite database with the following command:
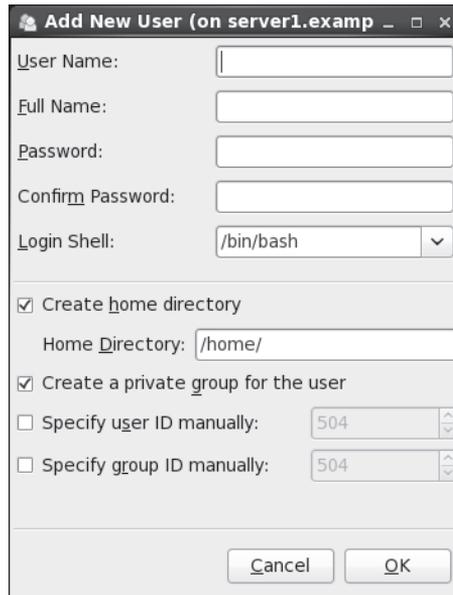
```
# groupdel project
```

EXERCISE 8-1

Add a User with the Red Hat User Manager

If the GUI is available, one alternative to user management commands such as **useradd** and **usermod** is the Red Hat User Manager. If possible, try to open it remotely over an **ssh -X** connection described in Chapter 2. For example, if you've configured the server1.example.com system as described in earlier chapters, connect to that system from a remote GUI with the **ssh -X root@192.168.122.50** command. Once logged in, enter the **system-config-users** command.

1. In the Red Hat User Manager, click the Add User button, or choose File | Add User. This will open the Create New User window, as shown here:

2. Complete the form. All entries are required, except Full Name. The entries are fairly self-explanatory (see the earlier discussions of each field). The password should be at least six characters and should ideally contain a mix of upper- and lowercase letters, numbers, and punctuation to keep it more secure from the standard password-cracking programs.

3. Enter the identical password in the Confirm Password field.

4. Note the number associated with the Specify User ID Manually and Specify Group ID Manually options; those are the UID and GID numbers that will be assigned to the new user. Click OK when you are done.

5. Repeat the process as desired for any additional new users that may be required. Make sure to create at least one new user prior to running Exercise 8-2.

EXERCISE 8-2

Real and Fake Shells

Do not run this exercise unless a regular user has already been created on the local system. Otherwise, an error might require a cold restart of the system. If desired, run Exercise 8-1 first, as that allows you to create a new regular user on the target system.

1. Open the /etc/passwd file. Find a current regular user, with a UID of 500 or above.

2. Identify the default shell. It's specified in the last column, normally /bin/bash for regular users.

3. Change the default shell to /sbin/nologin, and save the changes to the /etc/passwd file.

4. Open a different console. Press the CTRL-ALT-F2 keys to open a different console. (If you're already in the second virtual console, substitute F3, F4, F5, or F6 for F2. If you're in a KVM-based VM in the GUI, you can move to the second virtual console by clicking Send Key | CTRL-ALT-F2.)

5. Try logging in as the modified user. What happens?

6. Return to the original console. If it's the GUI, it should be accessible with either the ALT-F1 or ALT-F7 key combinations. If that is not possible (such as when the GUI is not installed), you should still be able to log in as the root administrative user.

7. Reopen the /etc/passwd file. Restore the /bin/bash shell to the target regular user.

Delete a User

The removal of a user account is a straightforward process. The easiest way to delete a user account is with the **userdel** command. By default, this command does not delete that user's home directory, so administrators can transfer files from that user perhaps to an employee who has taken over the tasks of the deleted user. Alternatively, the **userdel -r *username*** command deletes that user's home directory along with all of the files stored in that home directory.

This is a lot faster than the GUI method, for which you start the X Window System, open the Red Hat User Manager, select the user, and then click Delete. While it's probably easier for a less experienced user to remember the GUI method, text commands are faster.

Modify an Account

As a Linux administrator, you may want to add some limitations to user accounts. The easiest way to illustrate some of the changes is with the User Manager tool. Start the User Manager, select a currently configured user, and then click Properties to open the User Properties dialog box.

Click the Account Info tab for the account expiration information shown in Figure 8-1. As shown in the figure, you can limit the life of an account so that it expires on a specific date, or you can disable an account by locking it.

Click the Password Info tab. As shown in Figure 8-2, you can set several characteristics related to an individual user's password. Even when good passwords are set, frequent password changes can help provide additional security. The categories shown in the figure are self-explanatory; a *0* in any of these text boxes means that the limit does not apply.

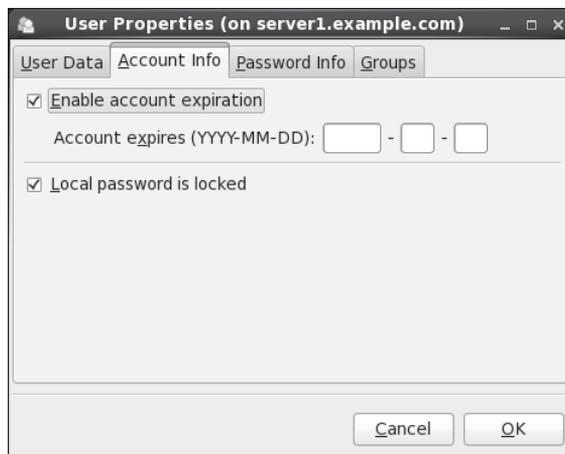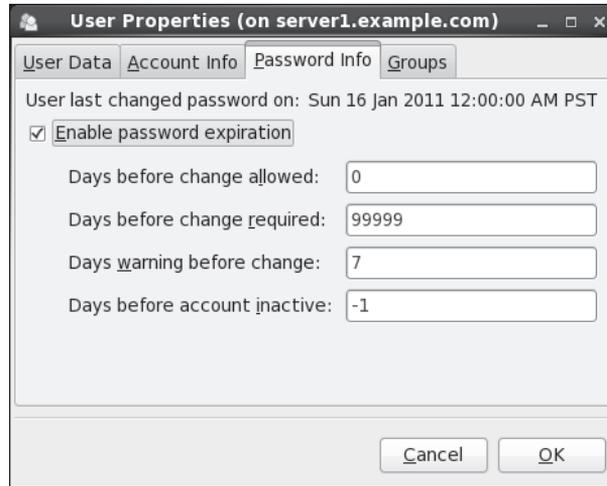**FIGURE 8-1**

Manage user account life.

Click the Groups tab. Users can belong to more than one group in Linux. Under the Groups properties tab shown in Figure 8-3, you can assign the target user to other groups. For example, to collect the files supporting the managers into one directory, you can assign appropriate users to the group named managers. Alternatively, you can then assign members of that project team to the project group through the Groups tab.

More User and Group Management Commands

While the Red Hat User Manager GUI utility is convenient, it's often faster to perform the associated administrative functions at the command line interface. I've described some of these commands such as **useradd**, **userdel**, **groupadd**, and **groupdel**. Three other key user administration commands are **usermod**, **groupmod**, and **chage**.

usermod

The **usermod** command modifies various settings in /etc/passwd. In addition, it also allows you to set an expiration date for an account or an additional group. For example, the following command sets the account associated with user test1 to expire on June 8, 2011:

```
# usermod -e 2011-06-08 test1
```

FIGURE 8-3

Assign a group.

The following command makes user test1 a member of the special group:

```
# usermod -G special test1
```

The **usermod** command is closely related to the **useradd** command; in fact, the **usermod** command can use all of the **useradd** command switches listed in Table 8-6. The **usermod** command includes several additional switches listed in Table 8-7.

groupmod

The **groupmod** command is relatively simple. It has two practical uses. The following command changes the GID number of the group named project, in this case, to 60002:

```
# groupmod -g 60002 project
```

TABLE 8-7

usermod
Command
Options

Option	Purpose
-aG *group1*	Appends to existing group memberships; multiple groups may be specified, split with a comma, with no spaces.
-l *newlogin*	Changes the username to *newlogin*, without changing the home directory.
-L	Locks a user's password.
-U	Unlocks a user's password.

In contrast, the following command changes the name of the group named project to secret:

```
# groupmod secret project
```

chage

The **chage** command is primarily used to manage aging information for a password, as stored in the /etc/shadow file. While some of the parameters can also be set with the **useradd** and **usermod** commands, most of the switches are different, as described in Table 8-8.

TABLE 8-8	Option	Purpose
chage Command Options	-d YYYY-MM-DD	Sets the last change date for a password; output shown in /etc/shadow as the number of days after January 1, 1970.
	-E YYYY-MM-DD	Assigns the expiration date for an account; output shown in /etc/shadow as the number of days after January 1, 1970.
	-I *num*	Locks an account *num* days after a password has expired; can be set to -1 to make the account permanent.
	-l	Lists all aging information.
	-m *num*	Sets a minimum number of days that a user must keep a password.
	-M *num*	Sets a maximum number of days that a user is allowed to keep a password; can be set to -1 to remove that limit.
	-W *num*	Specifies the number of days before a password must be changed; a user is warned at that time.

CERTIFICATION OBJECTIVE 8.02

Administrative Control

As the root administrative user is all-powerful, it's important for administrators to execute most actions as the regular user. Limits on regular users can help protect Linux systems from accidents. Regular users who have the root administrative password can temporarily take root privileges with the **su** command. The **su** command can do more with other accounts. In contrast, the **sg** command is associated with privileges on special groups.

While the **su** command is adequate for small networks, no administrator should work alone. With the help of the **sudo** command configured in the /etc/sudoers file, it's possible to set up dedicated administrators with partial or complete root administrative privileges.

The Ability to Log In as root

It's possible to keep users from logging in directly as the root administrative user. Local access is regulated in the /etc/securetty file. By default, it contains access directives for 12 virtual consoles. While only six virtual consoles are enabled in the /etc/init/start-ttys.conf file discussed in Chapter 5, it is possible to configure 12 (based on the number of function keys on a keyboard).

The virtual consoles listed in /etc/securetty determine the consoles where the root administrative user is allowed to log in. If the directives in this file were commented out, administrators would not be able to log in directly to the root account. They'd have to log in to a regular account and use either the **su** or **sudo** command for administration.

While it's still possible to log in remotely as the root administrative user with the **ssh** command, that ability can also be regulated. The configuration of the SSH server in this manner is an RHCE skill described in Chapter 12.

EXERCISE 8-3

Limit root Logins

In this exercise, you'll examine the effect of eliminating the consoles in the /etc/securetty file. But first, you'll confirm that the root administrative user can log

in to the standard consoles on virtual terminals 1 through 6. This exercise assumes that a regular account is available on the local system.

1. Move to the second virtual console. Press CTRL-ALT-F2; alternatively, in a KVM VM, click Send Key | CTRL-ALT-F2. At the *login:* prompt that appears, log in as the root user.

2. Repeat the process with the first, third, fourth, fifth, and sixth virtual consoles. Unless /etc/securetty has already been changed, you should be able to log in as the root user in all of these consoles.

3. Back up the current /etc/securetty file.

4. Open the /etc/securetty file in a text editor. Comment out all of the directives. Save the file.

5. Log out of the console. Try logging back in as the root administrative user. What happens? Repeat the process in other virtual consoles. What happens?

6. Log in to a console as a regular user. Does it work? Run the **su -** command to assume root privileges. Restore the original /etc/securetty file.

7. If a regular user account doesn't exist on the system, you'll have to reboot the system in single-user mode, as discussed in Chapter 5. You'll then be able to restore the /etc/securetty file from the prompt that appears.

The Ability to Log In

Beyond the /etc/securetty file is /etc/security/access.conf, which regulates access by all users. While the default version of this file is completely commented out, the comments provide useful examples. The first example would disallow (with the -) access to the first virtual console (tty1) to ALL users but root:

```
-:ALL EXCEPT root:tty1
```

Jump ahead in the file. The following line is a slightly more complex example that would disallow access to all users, except users who are members of the wheel group, along with the shutdown and sync users, on the LOCAL system.

```
-:ALL EXCEPT (wheel) shutdown sync:LOCAL
```

Scroll down further in the file. The following lines allow (with the +) the root user to access the system from three specific remote IP addresses, along with the localhost address:

```
+ : root : 192.168.200.1 192.168.200.4 192.168.200.9
+ : root : 127.0.0.1
```

If you're protecting a system from outside networks, this type of limitation on direct root administrative access makes sense. As long as the **su** or **sudo** command allows, users who log in remotely as regular users can still elevate their privileges accordingly.

Be aware, the directives in this file are considered in order. So if directives that allow access (with the +) come first, then the following directive denies access to all other users from all other local or remote systems:

```
- : ALL : ALL
```

The Proper Use of the su Command

In some cases, such as Red Hat exams, it's appropriate to log in as the root administrative user. But in practice, it's best to log in as a regular user. As a regular user, you can temporarily log in with root administrative privileges with the **su** command. Normally, that command prompts for the password of the root administrative user. After you've completed administrative tasks, it's best to log out of the root administrative account; the **exit** command would return to the regular account of that user.

The **su -** command is slightly different, as it accesses the full privileges of the root administrative account. If the password is accepted, it navigates to the root user's home directory, /root.

If you have the password of a second user, you can use the **su -** *username* command to log in directly to that account. For example, if I wanted to log in to user dickens' account, I'd run the **su - dickens** command. When I enter her password successfully, the command takes me to the /home/dickens directory.

Finally, the **su -c** command can be used to assume administrative privileges for one command. For example, the following command can be used to modify the first virtual drive on a system (assuming the root administrative password is successfully entered in response to the prompt:

```
$ su -c '/sbin/fdisk /dev/vda'
```

Limit Access to su

As discussed earlier, the ability to log in directly as the root administrative user can be regulated. Further limitations on administrative access are possible. For example, you can limit the users who are allowed to run the **su** command. This requires two basic steps.

First, you'll need to list the users who should have access to the **su** command. Make them a part of the wheel group. By default, this line in /etc/group looks like:

```
wheel:x:10:root
```

You can add selected users to the end of this line directly, with the **usermod -G wheel** *username* command, or with the User Manager.

Second, this requires a change to the configuration of Pluggable Authentication Modules (PAM). While PAM, as described in Chapter 10, is an RHCE objective, there's a commented directive available in the /etc/pam.d/su file ready for this purpose.

```
# auth    required pam_wheel.so use_uid
```

If this line is activated, only users who are members of the wheel group are allowed to use the **su** command.

The Proper Use of the sg Command

With the **sg** command, you can execute another command with the rights associated with a special group. This assumes you've set up a group password for the project group with the **gpasswd project** command. Then the **sg project -c** command allows you access to files and directories owned by the group named project. For example, if the /home/secret directory is owned by the project group, and you know the password set with the **gpasswd** command, the following command copies the important.doc file to the noted directory:

```
$ sg project -c 'cp important.doc /home/project'
```

Custom Administrators with the sudo Command

Alternatively, you can limit access to the **sudo** command. Regular users who are authorized in /etc/sudoers can access administrative commands with their own password. You don't need to give out the administrative password to everyone who thinks they know as much as a Red Hat certified professional.

To access /etc/sudoers in the vi editor, run the **visudo** command. The following directive is active by default, which allows the root user full access to administrative commands:

```
root      ALL=(ALL) ALL
```

Other users can be given administrative access. For example, if you want to allow user boris full administrative access, add the following directive to /etc/sudoers:

```
boris     ALL=(ALL) ALL
```

In this case, all boris needs to do to run an administrative command is to preface it with the **sudo** command. For example, if boris runs the following command, he's prompted for his own regular user password before the noted service is started.

```
$ sudo service vsftpd start
Password:
```

Alternatively, you can allow special users administrative access without a password. As suggested by the comments, the following directive in /etc/sudoers would allow all users who are members of the wheel group to run administrative commands without a password:

```
%wheel    ALL=(ALL)  NOPASSWD: ALL
```

But you don't have to allow full administrative access. For example, if you want to allow users who are members of the %users group to shut down the local system, activate the following directive:

```
%users  localhost=/sbin/shutdown -h now
```

In many Linux configuration files, the % sign in front of a directive specifies a group. Even though the users group has a GID of 100, it's acceptable to make regular users members of that group. For example, another directive shown in comments specifies a group of commands that can be run by users who are members of the %sys group:

```
%sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES,
LOCATE, DRIVERS
```

Each of the directives can be associated with a set of commands. For example, users in the sys group, who are allowed to run NETWORKING directives, can run the commands associated with the following directive:

```
Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient,
/usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig,
/sbin/mii-tool
```

In a similar fashion, you could set up a netadmin group of users who are allowed to run these commands with the following directive:

```
%netadmin ALL = NETWORKING
```

This assumes that groups such as netadmin exist in the /etc/group and /etc/gshadow files.

Other Administrative Users

Various services may be configured with their own groups of administrative users. For example, examine the following directive from the /etc/cups/cupsd.conf file:

```
SystemGroup sys root
```

Members of groups listed with the **SystemGroup** get administrative privileges on the RHEL 6 print server.

on the job

CUPS is no longer an acronym, to avoid concerns with the word "UNIX" as a trademark. CUPS is still the name of the default Linux print server.

CERTIFICATION OBJECTIVE 8.03

User and Shell Configuration

Each user on any Red Hat Enterprise Linux system has an *environment* when logged on to the system. The environment defines directories where Linux looks for programs to run, the look of the login prompt, the terminal type, and more. This section explains how you can configure the default environment for local users. All system-wide shell configuration files are kept in the /etc directory. These files are bashrc, profile, and the scripts in the /etc/profile.d directory. These files and scripts are supplemented by hidden files in each user's home directory, as just described. Let's take a look at these files.

Home Directories and /etc/skel

When a new user is created, with standard commands such as **useradd** or utilities such as the User Manager, a default set of configuration files is copied to the user's home directory from the /etc/skel directory.

Home Directory

The home directory is where a user starts when logging in to a RHEL system. The home directory for most users is /home/*username*, where *username* is the user's login name. Every user should normally have write permission in his own home directory, so each user is free to read and write his own files.

/etc/skel

The /etc/skel directory contains default environment files for new accounts. The **useradd** command and the Red Hat User Manager copies these files to the home directory for new users. The contents of /etc/skel may vary. While the standard files in this directory are hidden, administrators are free to add more files for new users. Standard files from one copy of /etc/skel are described in Table 8-9.

	File	Purpose
TABLE 8-9	.bashrc	This basic bash configuration file may include a reference to the general /etc/bashrc configuration file. Can include commands to run when the bash shell is started. One example is an alias such as **rm='rm -i'**.
Standard files in the /etc/skel Directory	.bash_logout	This file is executed when you exit a bash shell and can include commands appropriate for this purpose, such as commands for clearing a screen.
	.bash_profile	Configures the bash startup environment. Appropriate place to add environment variables or modify the directories in your user account PATH.
	.gnome2/	Includes settings for the GNOME Desktop Environment.
	.kde/	Specifies settings for the K Desktop Environment. Not added to /etc/skel and not copied to user home directories if KDE is not installed.
	.mozilla/	Includes options associated with the Firefox web browser, developed by the Mozilla project.

If you've installed more than a standard set of software packages on RHEL, additional configuration files and subdirectories may appear in the /etc/skel directory. For example, the installation of certain packages may include configuration files associated with emacs and the z shell (zsh) in this directory.

As the system administrator, you can edit these files or place custom files in /etc/skel. When new users are created, these files are propagated to the new users' home directories.

/etc/bashrc

The /etc/bashrc file is used for aliases and functions on a system-wide basis. Open this file in the text editor of your choice. Read each line in this file. Even if you don't understand the programming commands, you can see that this file sets the following bash shell parameters for each user. For example:

- It assigns a value of **umask**, which creates the default permissions for newly created files. It supports one set of permissions for root and system users (with user IDs below 200), and another for regular users. (Officially, RHEL reserves all user IDs above 500 for regular users; however, that is not reflected in /etc/bashrc.)

- It assigns and defines a prompt, which is what you see just before the cursor at the command prompt.

- It includes settings from *.sh files in the /etc/profile.d/ directory.

The settings here are supplemented by the .bashrc file in each user's home directory. The settings are supplemented by the .bash_profile and .bash_logout files in each user's home directory.

/etc/profile and /etc/profile.d

The /etc/profile file is used for system-wide environments and startup files.

The first part of the file sets the PATH for searching for commands. Additional directories are added to the PATH with the **pathmunge** command. (Unless you use the Korn shell, ignore the **ksh workaround** stanza.) Then it exports the **PATH**,

USER, **LOGNAME**, **MAIL**, **HOSTNAME**, **HISTSIZE**, and **HISTCONTROL**
variables and finally runs the scripts in the /etc/profile.d directory. You can check the
current value of any of these variables with the **echo $*variable*** command.

/etc/profile.d

The /etc/profile.d directory is designed to contain scripts to be executed by the
/etc/profile file. The following is a partial listing of the files; those with .sh extensions
apply to the default bash shell:

```
colorls.csh   gnome-ssh-askpass.csh   udisks-bash-completion.sh
colorls.sh    gnome-ssh-askpass.sh    vim.csh
cvs.csh       lang.csh                vim.sh
cvs.sh        lang.sh                 which2.csh
glib2.csh     less.csh                which2.sh
glib2.sh      less.sh
```

In most cases, there are two versions of a script, customized for different shell
environments. Look at the files in the /etc/profile script directory. You can see
that any script in this directory that ends with an .sh is included as part of the
configuration with /etc/profile. Scripts with other extensions, such as .csh, relate
to a different command shell.

EXERCISE 8-4

Another Way to Secure a System

One more way to help secure a system is to change the default permissions for new
files and directories. In this exercise, you'll reconfigure a system to remove access
permissions for default files from other users or groups.

1. Back up the current version of the /etc/bashrc file.
2. Open the /etc/bashrc file in a text editor. Two lines in the file set the **umask**.
   One of the two lines is selected, depending on the **if** statement above them.
   See if you can determine which value of **umask** is assigned to an average
   (nonroot) user.
3. The **if** statement tests to see whether the user ID (**UID**) and group ID (**GID**)
   are the same, and that the **UID** is greater than 199. (On RHEL, you can—
   but don't have to—change this to 499.)

In other words, the **umask** value of 002 is given to users with UIDs of 200 and above. A umask value of 022 is given to users with UID of 199 and below.

4. Change the first **umask** statement to exclude all permissions for groups and others. In other words, replace the **umask** of 002 with a **umask** of 077.

5. Save and exit the file.

6. Log in as a regular nonprivileged user. Use the **touch** command to make a new empty file. Use **ls -l** to verify the permissions on that file.

7. Log in as root. Again, use the **touch** command to make a new empty file and use **ls -l** to verify the permissions on that new file.

You have just changed the default umask for all regular users. While this is an excellent option for security, it would affect the steps used in other chapters. Therefore, one final step is important:

8. Restore the original version of /etc/bashrc from the backup created in Step 1.

Shell Configuration Files in User Home Directories

As described earlier, each user gets a copy of all files from the /etc/skel directory. Most of them are hidden, revealed only with commands like **ls -a**. As users start working with their accounts, more configuration files may be added to their home directories. Some users may work primarily with the default bash shell, while others include additional configuration in configuration files related to their GUI desktop environments such as GNOME.

The default Linux shell is bash, and until recently, it was specifically included as the only shell described in associated Red Hat exam objectives. While bash is no longer specifically included in the objectives, it is the default for RHEL 6.

Login, Logout, and User Switching

While this may seem like a "no-brainer" topic for Linux users with even a couple of days of experience, one of the RHCSA topics is to "Log in and switch users in multi-user runlevels." It includes concepts from different chapters. As discussed in Chapter 5, the multi-user runlevels are 2, 3, 4, and 5. Command-line logins are available at all of these runlevels. For the first RHEL 6 release, command-line logins appear as follows:

```
Red Hat Enterprise Linux Server release 6.0 (Santiago)
Kernel 2.6.32-71.el6.x86_64 on an x86_64

server1 login:
```

The hostname, as well as the versions of RHEL 6 and the kernel, will vary. But that's irrelevant to actual logins; all you need to do is type in a username, press ENTER, and type in a password when prompted.

Logouts from the command line are even simpler; the **exit**, **logout**, and CTRL-D commands all perform logouts from the command line. Of course, once you've logged out from a system, the login prompt just shown will appear.

As discussed earlier in this chapter, there's a different way to switch user accounts. For example, to switch from the current account to user donna's account, run the following command:

```
$ su - donna
```

The same **exit**, **logout**, and CTRL-D commands can be used to exit from user donna's account.

Of course, users can log in to and log out of the GUI. While the steps vary a bit by desktop environment, they are as simple as the steps required to log in to and log out of any other operating system.

CERTIFICATION OBJECTIVE 8.04

Users and Network Authentication

By default, access to a Linux computer requires a valid username and password. One problem with a large network of Linux systems is that without some central database, each user would require an account on every Linux computer.

Several services are available that can be used as a central authentication database. One now-obsolete option for the Red Hat exams is the Network Information Service (NIS). In contrast, the Lightweight Directory Access Protocol (LDAP) is specifically listed in the RHCSA objectives. Other services are available, namely Samba, which can be configured to support access by Linux systems and users to networks governed by a Microsoft database. In any of these cases, one database of passwords and usernames exists for a network.

<table>
<tr><td>e x a m
ⓦ a t c h</td></tr>
</table>

In the RHCSA objectives, the only network client authentication requirement is to be able to connect a client to a LDAP server. You're not required to actually create an LDAP server. In addition, NIS is no longer part of the objectives.

The focus of this section is LDAP as a client. You'll configure an RHEL 6 system as an LDAP client, set up authentication in the name service switch file, and repeat the process with Red Hat network authentication tools. First, I'll show you how you can configure LDAP clients using the command line interface and then use the Red Hat Authentication Configuration tool to repeat the process. So you'll know two methods for configuring LDAP clients.

In contrast to NIS, LDAP services can be configured on a variety of platforms. Of course, LDAP servers can be configured on RHEL 6, but they are not part of the current RHCSA or RHCE exam objectives. LDAP authentication databases can even be configured on Microsoft-based Active Directory (AD) services.

on the
Job

LDAP directory services and authentication is one focus of Red Hat's RH423 course. While Red Hat allows students with "equivalent experience" to take RH423, the RHCE is an acceptable prerequisite. So you're not expected to know LDAP servers for the RHCSA exam. If you want to set up a simplified LDAP server, explore the FreeIPA (Identity, Policy, and Audit) project at www.freeipa.org.

LDAP Client Configuration

To configure a RHEL computer as an LDAP client, you'll need the openldap-clients, openldap, and nss-pam-ldapd RPM packages. The openldap-clients and nss-pam-ldapd RPMs are both optional parts of the Directory Client package group. The openldap package, as a mandatory part of the Server package group, should be installed by default on the RHEL 6 systems for this book.

To configure an LDAP client, you'll need to configure various LDAP configuration files, namely /etc/pam_ldap.conf and /etc/openldap/ldap.conf. While the files can get quite complex, you don't have to reconfigure a lot just to set up an LDAP client.

/etc/pam_ldap.conf

The default version of the /etc/pam_ldap.conf file includes a number of different commands and comments. Standard changes required to set up a basic LDAP client are based on several directives shown in Table 8-10. Encryption-related directives in this file may be associated with both the Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS). If TLS is shown, the SSL directives work with them.

TABLE 8-10	Directive	Description
Client Configuration Parameters in /etc/pam_ldap .conf	host 127.0.0.1	Specifies the IP address for the LDAP server. This command assumes the LDAP server is on the local computer. Should be changed to the actual IP address of the LDAP server.
	base dc=example,dc=com	Sets the default **base** distinguished name, in this case, example.com. Should be changed to the domain of the network that is being served.
	ssl start_tls	Required if TLS support is used to encrypt passwords that are sent to the LDAP server.
	pam_password	Supports encryption schemes for passwords; options include **crypt**, **nds** (Novell Directory Services), and **ad** (Active Directory).
	nss_init, groups_ignoreusers root, ldap	Assumes no supplemental groups in the LDAP directory server.

As suggested by the name of the file, the pam_ldap.conf file applies Pluggable Authentication Modules to LDAP authentication. It is almost identical to the /etc/ldap.conf file from RHEL 5; the differences do not affect the successful configuration of an LDAP client.

Related directives are included at the end of the file; they may include the following. First, the Uniform Resource Identifier, as specified by the **uri**, should redirect the client to the actual IP address of the LDAP server.

```
uri ldap://127.0.0.1/
```

If secure communication is used, you may change **ldap** to **ldaps**; if you're also configuring the LDAP server, that corresponds to TCP/IP ports 389 and 636, respectively. An LDAP server won't work if a firewall blocks these ports. Of course, if secure communication is being used to LDAP, you'd want to change this to **ssl yes**:

```
ssl no
```

Of course, to enable secure connections, LDAP needs access to appropriate certificates. While TLS is the successor to SSL, it's commonly used in concert with SSL directives. The following directive specifies the directory with those certificates:

```
tls_cacertdir /etc/openldap/cacerts
```

While OpenLDAP does support the SHA512 passwords now included by default in the shadow password suite, the default is based on MD5 hashes.

```
pam_password md5
```

If you prefer the SHA512 hash, replace that directive with:

```
pam_password exop
```

/etc/openldap/ldap.conf

You'll need to specify the **URI**, **BASE**, and **TLS_CACERTDIR** variables in this file, just as was done in the /etc/pam_ldap.conf configuration file. Given the parameters in the preceding section, you may even see a fourth directive in that file:

```
URI ldap://127.0.0.1
HOST tester1.example.com
BASE dc=example,dc=com
TLS_CACERTDIR /etc/openldap/cacerts
```

If the LDAP server is not on the local system, and the network domain is not example.com, substitute accordingly. Individual users can supersede this file in a hidden .ldaprc file in their home directories.

The Name Service Switch File

The Name Service Switch file, /etc/nsswitch.conf, governs how a computer searches for key files such as password databases. It can be configured to look through LDAP and other server databases. For example, when an LDAP client looks for a computer hostname, it might start with the following entry from /etc/nsswitch.conf:

```
hosts: files ldap dns
```

This line tells your computer to search through name databases in the following order:

1. Start with the database of hostnames and IP addresses in /etc/hosts.
2. Search for the hostname in a map file based on LDAP.
3. If none of these databases includes the desired hostname, refer to the DNS server.

You can configure the /etc/nsswitch.conf configuration file to look at an LDAP server for the desired databases. For example, to set up a centralized username and

password database for your network, you'll need to configure at least the following commands in /etc/nsswitch.conf:

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

Other authentication databases can be configured; NIS is associated with the **nis** directive; Microsoft authentication before LDAP-based AD services is associated with **winbind**.

Red Hat Network Authentication Tools

If you're not familiar with LDAP, it may be simpler to configure a system with the Red Hat Authentication Configuration tool. In RHEL 6, you can start it in the GUI with the **system-config-authentication** command or in the console with the **authconfig-tui** command. This opens an Authentication Configuration tool; the GUI version is shown in Figure 8-4.

The Authentication Configuration tool has changed. By default, it's set to look at only the local authentication database. But if you click the drop-down text box, it presents three other options. LDAP is all that matters under the current

FIGURE 8-4

Authentication
Configuration
Options
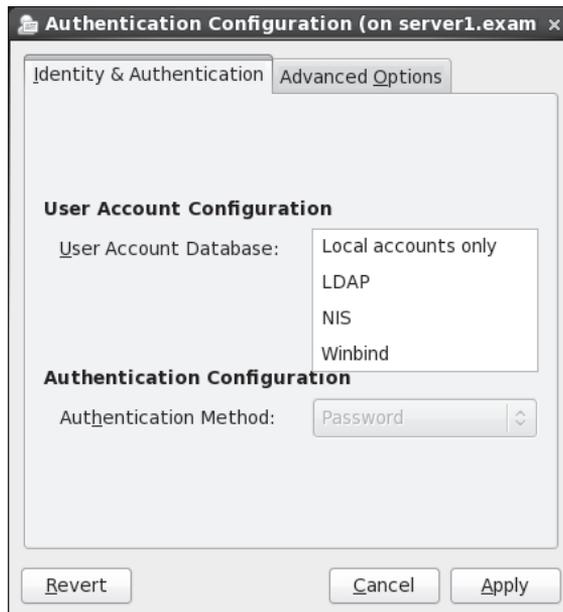
RHCSA objectives. When selected, the window changes, as shown in Figure 8-5. It defaults to the Kerberos Password Authentication Method, associated with client authentication under that system discussed in Chapter 11.

So if you see Kerberos in the window, click the associated text box, and select LDAP Password. The window changes again and provides the following warning:

```
You must provide ldaps:// server address or use TLS for LDAP authentication.
```

To eliminate that warning, select the Use TLS To Encrypt Connections option. If successful, what you see should resemble Figure 8-6.

This section assumes you're using LDAP as the User Account Database. The Authentication Configuration tool requires you to select the Use TLS To Encrypt Connections option. Those options won't be changed.

FIGURE 8-5

LDAP
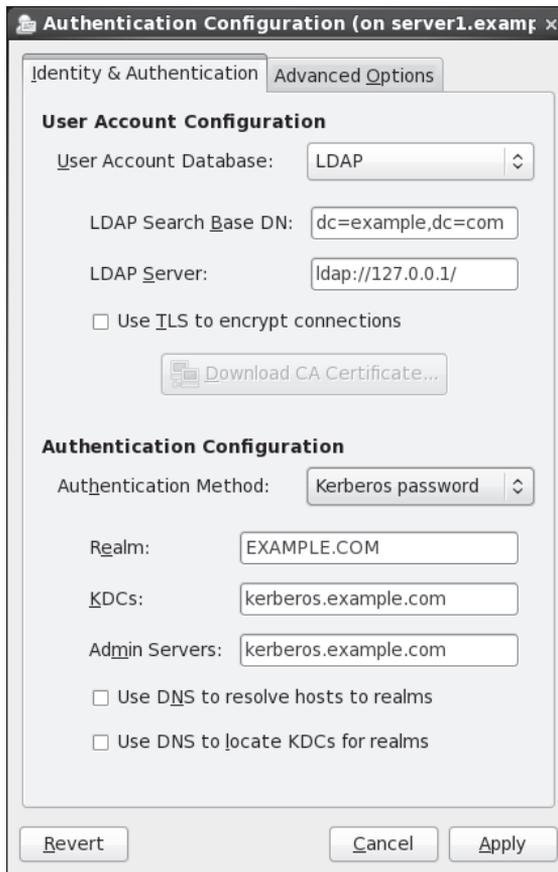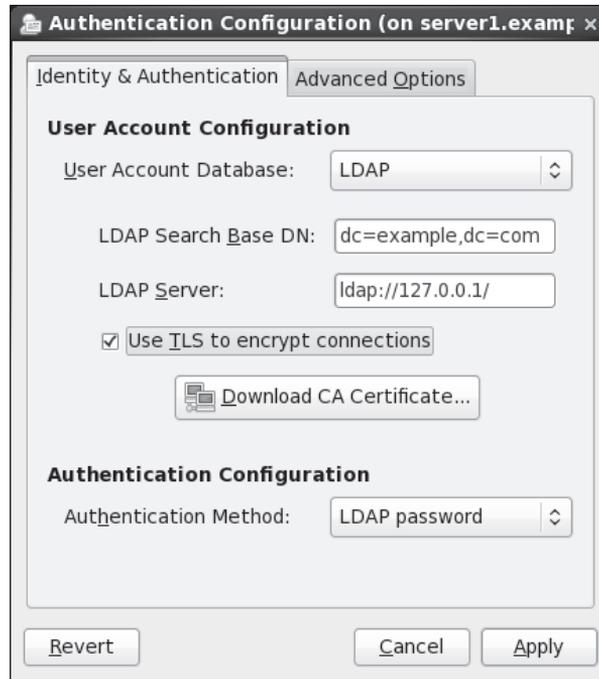Authentication
Configuration
Options

LDAP
Authentication
Configuration
Options

The remaining options may vary:

1. The LDAP Search Base DN text box includes the domain name for the LDAP server. For example, if the local system domain is my-domain.com, the text box should contain the following:

   `dc=my-domain,dc=com`

2. The LDAP server text box should include the URI of that server. If it's the local computer, you can use the 127.0.0.1 IP address. But that's unlikely, especially on an exam.

3. If LDAP is associated with a Certificate Authority (CA) certificate, click Download CA Certificate. It opens a window that allows you to specify the URL with the CA Certificate with the .pem extension.

Now select the other tab, Advanced Options. The options are shown in Figure 8-7. It's just for reference, and not related to the configuration of an LDAP client.

Advanced
Authentication
Options
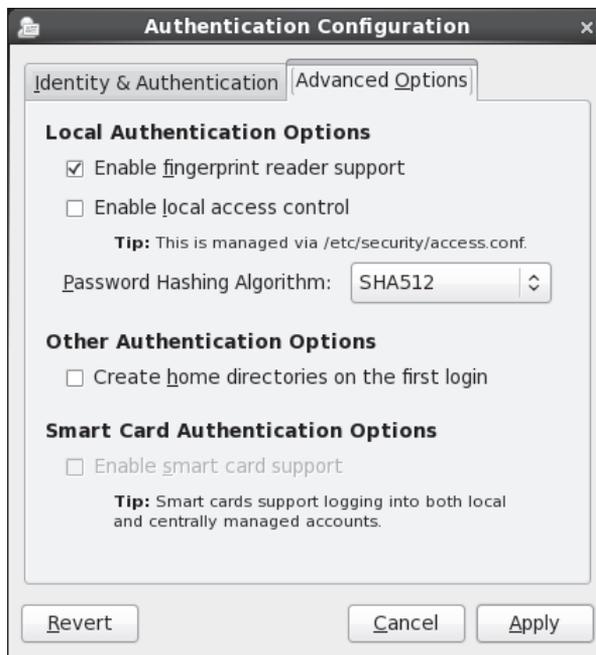
Once you've made desired changes, click OK; it may take a few seconds for the Authentication Configuration tool to write the changes to the noted configuration files.

CERTIFICATION OBJECTIVE 8.05

Special Groups

In the past, Linux groups of regular users allowed its members to share files. Red Hat has helped change this with the way it assigns unique UID and GID numbers to each user. When regular users are all made members of the same group, that also means everyone in that group has access to the home directories of all other group members. And that's often not desirable. Users may not want to share the files in their home directories with others.

On the other hand, RHEL gives each user a unique user ID and group ID in /etc/passwd. This is known as the *user private group* scheme. Users get exclusive access to their own groups and don't have to worry about other users reading the files in their home directories.

Standard and Red Hat Groups

In RHEL, each user gets her own special private group by default. As noted earlier, UIDs and GIDs normally start at 500, are assigned matching numbers, and proceed in ascending order. In addition, you can set up special groups of dedicated users, ideally with higher GIDs. For example, an administrator might configure accgrp for the accounting department, perhaps with a GID of 70000.

Shared Directories

Most people work in groups. They may want to share files. There may be good reasons for people in those groups to keep their information hidden from others. To support such groups, you can set up a shared directory, with access limited to the members of that group.

Assume you want to set up a shared directory, /home/accshared, for a group of accountants. To that end, you can set up a shared directory with the following basic steps:

1. Create the shared directory:

   ```
   # mkdir /home/accshared
   ```

2. Create a group for the accountants. Call it accgrp. Give it a group ID that doesn't interfere with existing group or user IDs. One way to do this is to add a line such as the following to the /etc/group file, or with the User Manager. Substitute desired usernames.

   ```
   accgrp:x:70000:robertc,alanm,victorb,roberta,alano,charliew
   ```

3. Set up appropriate ownership for the new shared directory. The following commands prevent any specific user from taking control of the directory and assign group ownership to accgrp:

   ```
   # chown nobody.accgrp /home/accshared
   # chmod 2770 /home/accshared
   ```

Any user who is a member of the accgrp group can now create files in and copy files to the /home/accshared directory. Any files generated within or copied to that directory will be owned by the accgrp group.

This is made possible by the 2770 permissions that assigned to the /home/accshared directory. Break that down into its component parts. The first digit (2) is the *set group ID bit,* also known as the *SGID bit.* When a SGID bit is set on a directory, any files created in that directory automatically have their group ownership set to be the same as the group owner of the directory. In addition, group ownership of files copied from other directories is reassigned, in this case, to the group named accgrp. There is a second way to set the SGID bit for the /home/accshared directory:

```
chmod g+s /home/accshared
```

The remaining digits are basic knowledge for any experienced Linux or Unix user. The **770** sets read, write, and execute permissions for the user and group that own the directory. Other users get no permissions to that directory. But since the user owner of the directory is the nonprivileged user named nobody, the group owner of the directory is most important. In this case, members of the accgrp group have read, write, and execute permissions to files created in this directory.

EXERCISE 8-5

Control Group Ownership with the SGID Bit

In this exercise, you will create new files in a directory designed to be shared by a group of users. You'll also see the difference in what happens before and after the SGID bit is set.

1. Add users called test1, test2, and test3. Specify passwords when prompted. Check the /etc/passwd and /etc/group files to verify that each user's private group was created:

```
# useradd test1; passwd test1
# useradd test2; passwd test2
# useradd test3; passwd test3
```

2. Edit the /etc/group file and add a group called tg1. Make the test1 and test2 accounts members of this group. You could add the following line to /etc/group directly or use the Red Hat User Manager:

```
tg1:x:99999:test1,test2
```

Before you proceed, make sure the group ID assigned to group tg1 (in this case, 99999) is not already in use. Make sure to add the following line to /etc/shadow. A group password is not required:

```
tg1:!::
```

3. Create a directory intended for use by the tg1 group:

```
# mkdir  /home/testshared
```

4. Change the user and group ownership of the shared directory:

```
# chown  nobody.tg1  /home/testshared
```

5. Log in as user test1. Make sure the login navigates to the /home/test1 direc-tory. Run the **umask** command to confirm that files created from this account will have appropriate permissions. (The output of the **umask** command for regular users such as test1 should be 0002.) If there's a problem with the home directory or the **umask** output, you may have made an error earlier in this chapter with user settings. If so, repeat Steps 1–5 on a different VM.

6. Run the **cd /home/testshared** command. Now try to create a file with the following commands. What happens?

```
$ date  >>test.txt
$ touch abcd
```

7. Now as the root user, set group write permissions on the testshared directory.

```
# chmod 770 /home/testshared
```

8. Log in again as user test1, navigate back to the /home/testshared directory, and then try to create a file in the new directory. So far, so good.

```
$ cd /home/testshared
$ date  >> test.txt
$ ls -l test.txt
```

9. Remove all permissions for other users on new files in the /home/testshared directory:

```
# chmod o-rwx /home/testshared/*
```

10. Now with the following command, check the ownership on the new file. Do you think other users in the tg1 group can access this file? If in doubt, log in as user test2 and see for yourself.

    ```
    $ ls -l
    ```

11. From the root account, set the SGID bit on the directory:

    ```
    # chmod g+s  /home/testshared
    ```

    (Yes, if you are efficiency-minded, you may know that the **chmod 2770 /home/testshared** command combines the effect of this and the previous **chmod** commands.)

12. Switch back to the test1 account, navigate back to the /home/testshared directory, and create another file. Remove permissions for other users on the newly created file. Check the ownership on the newly created file. Do you think that user test2 can now access this file? (To see for yourself, try it from the test2 account.)

    ```
    $ date >> testb.txt
    $ chmod o-rwx /home/testshared/testb.txt
    $ ls  -l
    ```

13. Now log in as the test2 account. Go into the /home/testshared directory. Try accessing the testb.txt file. Create a different file, and use **ls -l** to check permissions and ownership again. (To see that it worked, try accessing this file from the test1 account.)

14. Switch to the test3 account and check whether that user can or cannot create files in this directory, and whether that user can or cannot view the files in this directory.

CERTIFICATION SUMMARY

You can manage users and groups with the files of the shadow password suite. These files can be modified directly, with the help of commands such as **useradd** and **groupadd**, or the User Manager tool. The way users are configured is based on the /etc/login.defs file. Any variables or system-wide functions you may need to run can be kept in the /etc/bashrc or /etc/profile script. They can be modified by files in user home directories.

There are several ways to limit the use of administrative privileges. The ability to log in can be regulated in files such as /etc/securetty and /etc/security/access. conf. Access to the **su** command can be limited with the help of PAM. Partial and complete administrative privileges can be configured for the **sudo** command in the /etc/sudoers file.

You can use centralized network account management with the LDAP service. RHEL 6 systems can be configured as an LDAP client with the help of the /etc/pam_ldap.conf and /etc/openldap/ldap.conf files.

By default, Red Hat Enterprise Linux assigns unique user and group ID numbers to each new user. This is known as the user private group scheme. This scheme supports the configuration of special groups for a specific set of users. The users in the group can be configured with read and write privileges in a dedicated directory, courtesy of the SGID bit.

✓ TWO-MINUTE DRILL

Here are some of the key points from the certification objectives in Chapter 8.

User Account Management

- ❑ After installation, a system may have only a single login account: root. For everyday operation, it's best to create one or more regular accounts.
- ❑ The shadow password suite is configured in the /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow files.
- ❑ Administrators can add user and group accounts by directly editing the files of the shadow password suite, or with commands like **useradd** and **groupadd**. The way accounts are added are defined by the /etc/login.defs file.
- ❑ Accounts can be added with the Red Hat User Manager tool. You can also use this tool or related commands such as **chage** and **usermod** to modify other account parameters.

Administrative Control

- ❑ Logins as the root user can be regulated by the /etc/securetty file.
- ❑ Logins in general can be regulated by the /etc/security/access.conf file.
- ❑ Access to the **su** command can be regulated through the /etc/pam.d/su file.
- ❑ Custom administrative privileges can be configured in the /etc/sudoers file.

User and Shell Configuration

- ❑ The home directory for new login accounts is populated from the /etc/skel directory.
- ❑ Each user has an environment when logged on to the system, based on /etc/profile, and if the shell is bash, /etc/bashrc.
- ❑ All users have hidden shell configuration files in their home directories.

Users and Network Authentication

❑ LDAP allows you to configure one centrally managed username and password database with other Linux and Unix systems on a LAN.

❑ LDAP clients are configured in /etc/pam_ldap.conf and /etc/openldap/ldap.conf.

❑ Changes are required to /etc/nsswitch.conf to make a system look for a remote authentication database such as LDAP.

❑ Red Hat includes GUI and console tools that can help configure a system as an LDAP client.

Special Groups

❑ Red Hat's user private group scheme configures users with their own unique user and group ID numbers.

❑ With appropriate SGID permissions, you can configure a shared directory for a specific group of users.

❑ Setting the SGID bit is easy; use **chown** to set nobody as the user owner and the name of the group as the group owner. Then run the **chmod 2770** command on the shared directory.

SELF TEST

The following questions will help measure your understanding of the material presented in this chapter. As no multiple choice questions appear on the Red Hat exams, no multiple choice questions appear in this book. These questions exclusively test your understanding of the chapter. It is okay if you have another way of performing a task. Getting results, not memorizing trivia, is what counts on the Red Hat exams. There may be more than one answer to many of these questions.

User Account Management

1. What's the standard minimum user ID number for regular users on Red Hat distributions?

   _____

2. What command at a GUI-based text console starts the Red Hat User Manager?

   _____

Administrative Control

3. What file regulates the local consoles where the root user can log in?

   _____

4. What file supports the configuration of custom administrators?

   _____

5. When a regular user uses the **sudo** command to run an administrative command, what password is required?

   _____

User and Shell Configuration

6. If you want to add files to every new user account, what directory should you use?

   _____

7. The system-wide configuration file associated with the bash shell is

   _____

Users and Network Authentication

8. If the LDAP domain is example.org, what is the LDAP Search Base DN?

dc=_____

dc=_____

9. What's the full path to the file that refers to an LDAP database for authentication?

_____

Special Groups

10. What command would set the SGID bit on the /home/developer directory?

_____

11. What command would set up ownership of the developer group on the /home/developer directory?

_____

12. What command would add user alpha to the developer group? This question assumes the alpha user and the developer group already exists and alpha belongs to no group other than his own.

_____

LAB QUESTIONS

Red Hat presents its exams electronically. For that reason, the labs in this chapter are available from the CD that accompanies the book, in the Chapter8/ subdirectory. They're available in .doc, .html, and .txt formats, to reflect standard options associated with electronic delivery on a live RHEL 6 system. In case you haven't yet set up RHEL 6 on a system, refer to the first lab of Chapter 2 for installation instructions. The answers for each lab follows the Self Test answers for the fill-in-the-blank questions.

SELF TEST ANSWERS

User Account Management

1. The minimum user ID number for regular users on Red Hat distributions is 500.

2. The command in a GUI-based text console that starts the Red Hat User Manager is **system-config-users**.

Administrative Control

3. The file that regulates the local consoles where the root user can log in is /etc/securetty.

4. The file that supports the configuration of custom administrators is /etc/sudoers.

5. When a regular user uses the **sudo** command to run an administrative command, the regular password of that user is required.

User and Shell Configuration

6. To automatically add files to every new user account, you should use the /etc/skel directory.

7. The system-wide configuration file associated with the bash shell is /etc/bashrc.

Users and Network Authentication

8. If the LDAP domain is example.org, the LDAP Search Base DN is dc=example,dc=org.

9. The full path to the file that points to an LDAP database for authentication is /etc/nsswitch.conf.

Special Groups

10. The command that would set the SGID bit on the /home/developer directory is **chmod g+s /home/developer**. Numeric options such as **chmod 2770 /home/developer** are not correct, as they go beyond just setting the SGID bit.

11. The command would set up ownership of the developer group on the /home/developer directory is **chgrp developer /home/developer**.

12. The command that adds user alpha to the developer group is **usermod -G developer alpha**.

LAB ANSWERS

Lab 1

While there are a number of methods available to create new users and groups, they should all come to the same result.

1. The output to the **ls -l /home** command should include the following output, substituting today's date:

```
drwx------.  4 newguy   newguy   4096 Jan 19 12:13 newguy
drwx------.  4 intern   intern   4096 Jan 19 12:13 intern
```

2. Run the **ls -la /etc/skel** command. The output should include a number of hidden files, owned by the user root and the group root.

3. Run the **ls -la /home/newguy** and **ls -la /home/intern** commands. The output should include the same hidden files as in /etc/skel, but owned by the users associated with each home directory.

4. The end of the /etc/passwd and /etc/shadow file should include entries for both users. If you've set up a password for these users, it should be in encrypted format in the second column of /etc/shadow.

5. The following entry should exist somewhere in the middle of the /etc/group file. It is acceptable if other users are included at the end of the line.

```
users:x:100:newguy
```

6. The following line should be near to or at the end of the /etc/group file; the order of the users in the fourth column does not matter.

```
peons:x:123456:newguy,intern
```

Lab 2

The simplest way to limit root logins to the sixth virtual console is in the /etc/securetty file. The only active directives in that file should be:

```
vc/6
tty6
```

Of course, there are other ways to do just about anything in Linux. To try it out, press CTRL-ALT-F1 and try logging in as the root user. Press CTRL-ALT-F2, and repeat the process through virtual terminal 6.

Lab 3

Use the answers to the first part of Lab 1 as guidance to verify the ownership and permissions set /home/senioradm directory, along with the files therein. With respect to **sudo** privileges, you should see the following line in the /etc/sudoers file:

```
senioradm     ALL=(ALL)        ALL
```

To test the result, log in as the senioradm user, and run an administrative command, prefaced by a sudo. For example, try the following command:

```
# sudo system-config-firewall
```

Unless you've run the **sudo** command in the last few minutes, this action will prompt for a password. Enter the password created for user senioradm. It should open the Firewall Configuration tool.

Lab 4

Use the answers to Lab 1 as guidance to verify the ownership and permissions of the /home/junioradm directory, along with the files therein. With respect to **sudo** privileges, you should see the following line in the /etc/sudoers file:

```
junioradm     ALL=/sbin/fdisk
```

Next, try running the **fdisk** command such as:

```
$ sudo /sbin/fdisk -l
```

You'll be prompted for a password. Enter the password created for user junioradm. Unless the passwords are identical, the root password would not work. If successful, you should see a list of partitions for connected drives in the output.

Lab 5

Use the answers to Lab 1 as guidance to verify the ownership and permissions on /home/infouser directory, along with the files therein. If successful, that directory will include an info-*/ subdirectory. In addition, the /etc/skel directory should also include an info-*/ subdirectory. That subdirectory should have the same files as those shown in the /usr/share/doc/info-* directory. Of course, that works only if you copy the contents of the info-*/ subdirectory from the /usr/share/info directory to /etc/skel.

Lab 6

This is a straightforward process, using the following basic steps:

1. Create accounts for mike, rick, terri, and maryam if required. You can use the **useradd** command, edit the /etc/passwd file directly, or work through the User Manager.

2. Set up a group for these users. Configure a group ID outside the range of regular users in /etc/group with a line such as:

   ```
   galley:x:88888:mike,rick,terri,maryam
   ```

3. Create the /home/galley directory. Give it proper ownership and permissions with the following commands:

   ```
   # mkdir /home/galley
   # chown nobody.galley
   # chmod 2770 /home/galley
   ```