

SECTION 12 Manage Security

In this section of the workbook, you learn how to do the following:

- “Manage System Logging” on 12-1

Exercise 12-1 *Manage System Logging*

System logging is an essential part of system security.

The purpose of this exercise is to show you how you can create individual log files according to your needs. You will also understand how to modify what is logged in the default log files and how to influence the way log files are archived.

In this exercise, you do the following:

- [Part I: Modify the Syslog Configuration](#)
- [Part II: Configure logrotate](#)

Part I: Modify the Syslog Configuration

Do the following:

1. Make a backup copy of `/etc/syslog.conf` by entering
cp /etc/syslog.conf /etc/syslog.conf.original
2. Edit the file `/etc/syslog.conf`:
 - a. Open the file `/etc/syslog.conf` in an editor by pressing **Alt + F2** and entering
kdesu kate /etc/syslog.conf
Then enter a password of **novell** and select **OK**.

Because of the files modified or created during this exercise (and the importance of following steps precisely), there is a good possibility that you will have problems.

Make sure the `/etc/syslog.conf` file is edited correctly, that the contents of the `/etc/logrotate.d/local4` are accurate, and that the file is saved in the correct directory.

You need to perform the `logrotate` (Part II) from a terminal (instead of a terminal window) to avoid conflicts with existing system `logrotate` functionality.

SECTION 12 Manage Security

In this section of the workbook, you learn how to do the following:

- “Manage System Logging” on 12-1

Exercise 12-1 *Manage System Logging*

System logging is an essential part of system security.

The purpose of this exercise is to show you how you can create individual log files according to your needs. You will also understand how to modify what is logged in the default log files and how to influence the way log files are archived.

In this exercise, you do the following:

- [Part I: Modify the Syslog Configuration](#)
- [Part II: Configure logrotate](#)

Part I: Modify the Syslog Configuration

Do the following:

1. Make a backup copy of `/etc/syslog.conf` by entering
cp /etc/syslog.conf /etc/syslog.conf.original
2. Edit the file `/etc/syslog.conf`:
 - a. Open the file `/etc/syslog.conf` in an editor by pressing **Alt + F2** and entering
kdesu kate /etc/syslog.conf
Then enter a password of **novell** and select **OK**.

Because of the files modified or created during this exercise (and the importance of following steps precisely), there is a good possibility that you will have problems.

Make sure the `/etc/syslog.conf` file is edited correctly, that the contents of the `/etc/logrotate.d/local4` are accurate, and that the file is saved in the correct directory.

You need to perform the `logrotate` (Part II) from a terminal (instead of a terminal window) to avoid conflicts with existing system `logrotate` functionality.

- b. Add the following lines at the bottom of the file to allow for logging of the local4 facility on the levels of debug, notice, info, err, and alert:

```
local4.debug    /var/log/local4.debug
local4.notice   /var/log/local4.notice
local4.info     /var/log/local4.info
local4.err      /var/log/local4.err
local4.alert    /var/log/local4.alert
```
- c. Make sure there is an empty line at the end of the file by pressing **Enter**.
- d. Save the changes but keep the Kate window open by selecting **File > Close**; then select **Save**.
3. From a terminal window, su to root (**su -**) with a password of **novell**.
4. Restart the syslog daemon by entering **rcsyslog restart**.
5. Check the configuration by logging an entry to the info level in the local4 facility:
 - a. To monitor the activity of the log file, enter
tail -f /var/log/local4.info
 - b. Open another terminal window (su to **root**) and log an entry to the info level in the local4 facility by entering
logger -p local4.info "Info message 1"
 - c. Check the results in the second terminal window.
The message is logged in the file /var/log/local4.info.
The message should also be logged in the file /var/log/localmessages because of other entries in /etc/syslog.conf.
 - d. In the terminal window where the log activity is being monitored with tail -f, stop the monitoring by pressing **Ctrl + c**.

- b. Add the following lines at the bottom of the file to allow for logging of the local4 facility on the levels of debug, notice, info, err, and alert:

```
local4.debug    /var/log/local4.debug
local4.notice   /var/log/local4.notice
local4.info     /var/log/local4.info
local4.err      /var/log/local4.err
local4.alert    /var/log/local4.alert
```
- c. Make sure there is an empty line at the end of the file by pressing **Enter**.
- d. Save the changes but keep the Kate window open by selecting **File > Close**; then select **Save**.
3. From a terminal window, su to root (**su -**) with a password of **novell**.
4. Restart the syslog daemon by entering **rcsyslog restart**.
5. Check the configuration by logging an entry to the info level in the local4 facility:
 - a. To monitor the activity of the log file, enter
tail -f /var/log/local4.info
 - b. Open another terminal window (su to **root**) and log an entry to the info level in the local4 facility by entering
logger -p local4.info "Info message 1"
 - c. Check the results in the second terminal window.
The message is logged in the file /var/log/local4.info.
The message should also be logged in the file /var/log/localmessages because of other entries in /etc/syslog.conf.
 - d. In the terminal window where the log activity is being monitored with tail -f, stop the monitoring by pressing **Ctrl + c**.

6. Repeat step 4 to send a message at each of the log levels (such as **logger -p local4.debug "Info message 2"**) and monitor the messages with **tail -f** for the associated log file (such as **tail -f /var/log/local4.debug**).

Notice that at certain levels messages from other levels are also recorded.



Only those log level files with entries will be compressed in Part II of the exercise during log rotation.

Part II: Configure logrotate

Now that the local4 facility is being logged to separate files, you can use the program logrotate to manage the files for the system by creating a file `/etc/logrotate.d/local4` that does the following:

- Compresses the old logs in gzip format.
- Saves the old logs with a date extension.
- Limits the oldest log to one day.
- Limits the rotated logs saved to 5.
- Limits the maximum size of the file to 20 bytes.
- Proceeds without error if a log file is missing.
- Logs the date in the local4.info file each time a new log file is generated.

Do the following:

1. From the Kate window in a new document, enter

6. Repeat step 4 to send a message at each of the log levels (such as **logger -p local4.debug "Info message 2"**) and monitor the messages with **tail -f** for the associated log file (such as **tail -f /var/log/local4.debug**).

Notice that at certain levels messages from other levels are also recorded.



Only those log level files with entries will be compressed in Part II of the exercise during log rotation.

Part II: Configure logrotate

Now that the local4 facility is being logged to separate files, you can use the program logrotate to manage the files for the system by creating a file `/etc/logrotate.d/local4` that does the following:

- Compresses the old logs in gzip format.
- Saves the old logs with a date extension.
- Limits the oldest log to one day.
- Limits the rotated logs saved to 5.
- Limits the maximum size of the file to 20 bytes.
- Proceeds without error if a log file is missing.
- Logs the date in the local4.info file each time a new log file is generated.

Do the following:

1. From the Kate window in a new document, enter

```
/var/log/local4.err /var/log/local4.info  
/var/log/local4.alert /var/log/local4.debug  
/var/log/local4.notice  
{  
  compress  
  dateext  
  maxage 1  
  rotate 5  
  size=20  
  postrotate  
    date >> /var/log/local4.info  
  endscript  
}
```

Make sure the logfile names in the first line are separated with spaces.

2. Save the file by selecting **File > Save**; then enter **/etc/logrotate.d/local4** and select **Save**.
3. Close the Kate window by selecting **File > Quit**.
4. Switch to virtual terminal 1 by pressing **Ctrl + Alt + F1**.
5. Log in as **root** with a password of **novell**.
6. Rotate the logs manually by entering
logrotate /etc/logrotate.conf
7. Check the directory **/var/log** for the zipped local4 log files by entering

```
ls -l /var/log | less
```

You see files such as the following:

- **local4.info-current_date.gz**
- **local4.notice-current_date.gz**

For example, if the current date is July 15, 2006, then the zipped file for local4.info would be **local4.info-20060715**.

If your VMWare host is a Linux machine, press Ctrl + Alt and hold them. Then press Space, and then, while still holding Ctrl + Alt down, press F1. Otherwise your host will switch to console 1, not the guest.

```
/var/log/local4.err /var/log/local4.info  
/var/log/local4.alert /var/log/local4.debug  
/var/log/local4.notice  
{  
  compress  
  dateext  
  maxage 1  
  rotate 5  
  size=20  
  postrotate  
    date >> /var/log/local4.info  
  endscript  
}
```

Make sure the logfile names in the first line are separated with spaces.

2. Save the file by selecting **File > Save**; then enter **/etc/logrotate.d/local4** and select **Save**.
3. Close the Kate window by selecting **File > Quit**.
4. Switch to virtual terminal 1 by pressing **Ctrl + Alt + F1**.
5. Log in as **root** with a password of **novell**.
6. Rotate the logs manually by entering
logrotate /etc/logrotate.conf
7. Check the directory /var/log for the zipped local4 log files by entering

```
ls -l /var/log | less
```

You see files such as the following:

- **local4.info-current_date.gz**
- **local4.notice-current_date.gz**

For example, if the current date is July 15, 2006, then the zipped file for local4.info would be **local4.info-20060715**.

If your VMWare host is a Linux machine, press Ctrl + Alt and hold them. Then press Space, and then, while still holding Ctrl + Alt down, press F1. Otherwise your host will switch to console 1, not the guest.



Only those log files with entries are zipped.

8. Exit the list by typing **q**.
9. Check the contents of the local4.info zipped archive by entering
less /var/log/local4.info-current_date.gz
zcat /var/log/local4.info-current_date.gz
10. Log out as root by entering **exit**.
11. Return to the KDE desktop by pressing **Ctrl + Alt + F7**.
12. Close all open windows.

(End of Exercise)



Only those log files with entries are zipped.

8. Exit the list by typing **q**.
9. Check the contents of the local4.info zipped archive by entering
less /var/log/local4.info-current_date.gz
zcat /var/log/local4.info-current_date.gz
10. Log out as root by entering **exit**.
11. Return to the KDE desktop by pressing **Ctrl + Alt + F7**.
12. Close all open windows.

(End of Exercise)

