**Server AdministrationCompetencies ICTNWK504 and ICTNWK505**

**Lab 6 Error and event logging in Linux and Samba server**

**Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student ID\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

When you have finished this exercise, save the file with your name and student id at the beginning of the file name.

Eg John Smith \_ 12345\_ filename

Get this work checked before submission.

Create 3 users , *tjones, rhadlee* and *phung* and set passwords for them.

Start up a Linux virtual machine and windows XP machine set on NAT. Check connectivity between them.

**Part A ( 2 marks)**

**Exercise 1**

Login as root

1. a)Read the man pages for *syslog.conf* andexamine the entries in */etc/syslog.conf.* In later versions, the file is */etc/rsyslog.conf*

List the log files mentioned in this file.

 b) Take a screen shot of the entries in the file.

1. a) Where are the mail messages logged for all levels? \_\_\_\_\_\_\_\_\_\_\_

b) Where are all levels of the facility cron logged?\_\_\_\_\_\_\_\_\_\_\_\_\_

c) What information is sent to /var/log/messages ( hint : read the comments in /etc/syslog.conf)

d) How do you enable logging of all kernel messages to /dev/console?

( hint :there is now a # in front of the command. After making the changes, you have to send a hangup signal to syslogd)

1. Where is the information about the creation of users logged?

Produce a screen shot to justify your answer.

1. If you have login failure, where are they recorded?
2. Login as *tjones* with a wrong password.

Show a screen shot of the entry in the correct log file.

1. Type

dmesg

What does this output show

#nano /var/log/dmesg

Does this show the same entry as the output of the command?\_\_\_\_\_\_\_

1. Examine some of the log files and monitor the activities

/var/log/cron

/var/log/messages

 /var/log/maillog

 /var/log/boot.log

 /var/log/secure

What do you find in these files?

1. Go the GUI which represents the system logs. Go to System – administration – system logs. If you are using later versions of Centos, you may have to install this using the command

# yum install gnome-system-log

1. Get a screen shot of */var/log/secure*

 Have your work checked 1

**Exercise 2**

1. Log in as root in a graphical desktop such as KDE or GNOME
2. Start three terminals and have all three appear on the same screen. When you start the terminals resize their windows so that they are wide but short (about 2 inches high on the screen). Position the windows so that they are on top of each other.
3. In the first window, type **less /etc/syslog.conf** and press enter. The contents of the *syslog.conf* file should now be displayed. You can use the up and down arrow keys to see the entire file.
4. Select the second window. Type **tail –f /var/log/messages** and press **Enter**

 What do you find on the screen?

What does the option –f denote?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Select the third window. Type

# logger –p daemon.info This is a test of daemon.info

This tells the logger program to generate a logging message of daemon facility and info priority.

 What appears on the second window?

1. Press **Up Arrow** key in the third window. *Bash* shell recall the previous line. Press Enter.

Does anything appear on the second window?

----------------------------------------------------------------------------------

1. In the third window, type

# logger –p daemon.warning This is a test of daemon.warning

and press enter.

This timer causes lines appears on the second window. The second new lines contains the text of the most recent log message

**#** logger –p mail.info This is a test of mail.info

 Nothing appears in the second window. This is because this message was for the facility *mail.* . Select the first window and check where the mail messages are sent.

1. Select the second window and press Ctrl+C to get back to the shell prompt. Type

# tail –f /var/log/maillog and press Enter.

What is the last line?

Take a screen shot

1. Make sure that syslogd is started. Check this by the command

ps aux | grep syslogd

( rsyslogd in later versions)

If it is not listed, start the daemon by typing syslogd

Make *syslog* to do some additional logging. Have it send any log messages to priority **err or greater** to a file called *important.*

Create a file ***important*** under ***/var/log*** using touch command

Check whether the file is created

**# ls –l /var/log/im\***

1. Use the vi editor to add a new line to *syslog.conf* file

\*.err /var/log/important

1. Type

# killall –HUP syslogd

to tell the syslog daemon, its configuration file has changed.

1. Select the second window. Press **Ctrl+C** to return to the shell prompt. Type

# tail -f /var/log/important

Nothing appears since the file is empty.

1. Select the third window . Type

#logger –p mail.err This is a test of mail.err

 A message should appear on the second window

 Take a screen shot

1. Type

# logger –p mail.warning This is a test of mail.warning

Nothing appears on the second window since the priority of *warning* is lower than *error.*

What level of messages will be logged to the */var/log/important* file ?

1. Type on third window

# logger –p mail.alert this is a test of mail.alert

Does any message appear on the second window?

( yes/No)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Type

**#** logger –p mail.emerg This is a test of mail.emerg

Does the message appear on all windows? \_\_\_\_\_\_\_\_\_

Why? Justify your answer with relation to the entry in in /etc/syslog.conf \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Have your work checked 2

**Exercise 3**

**Review questions**

1. You want to monitor the messages log file and have any additional messages written to the log file also displayed on your screen. Which command does this?

 a) **head /var/log/messages**

* 1. **head –f /var/log/messages**
	2. **tail /var/log/messages**
	3. **tail –f /var/log/messages**
1. Which command sends a message of mail facility and info priority ?
2. **log mail, info this is a test**
3. **log –p mail info This is a test**
4. **logger –p mail.info This is a test**
5. **logger –w mail:info This is a test**
6. If you make a change to */etc/syslog.conf* you must inform the syslog daemon of the change by sending it a SIGUP signal . True or False? \_\_\_\_\_\_\_\_\_\_\_
7. Which of the following is the highest priority?
8. crit
9. alert
10. debug
11. warning

5. Which statement, placed in the *syslog.conf* file, sends all messages of **crit** priority and higher to the terminal screens of everyone logged in ?

 a) **mail.crit /var/log/everyone**

 **b) crit.\* \***

 **c) \*.crit | /var/log**

 **d) \*.crit \***

Have your work checked

 **3**

**Part B ( 2 marks)**

**Exercise 1**

You will be completing this exercise with a virtual machine. You will be using a windows XP machine and a Centos Linux virtual image.

Set the mode to NAT for both widows Xp and Linux image so that they have addresses in the same subnet.

1. At the Linux computer:

Open a terminal window

Type the command ifconfig and press Enter

Write the IP address for etho0 with subnet mask

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Start a windows computer and login to windows. Check the IP address of the windows computer

3. Check whether both the ip addresses are in the same subnet.

4. Check the connectivity between the windows client and the Linux machine.

5. Resolve any connectivity issues before proceeding

Hints: Check that both computers are on the same network address.

You will probably need turnoff the firewall on Windows.

1. Turn off the firewall on the Linux

Check the firewall on the Linux machine

iptables –L

Turn off the firewall

iptables –F

Check whether it has been turned off.

1. Download samba program to your linux server

# yum install samba

1. You have to set up the *smb.conf* file. First keep a backup of the original file

cd /etc/samba

cp smb.conf smb.conf.backup

vi smb.conf

1. Enter a simple config in this file. You may remove the existing configuration or put a comment (#) or ( ;) against the existing commands.

[global]
workgroup = wrkgrp
netbios name = smbserver
security = SHARE
load printers = No
default service = global
path = /home
available = No
encrypt passwords = yes
[share]
writeable = yes
admin users = smbuser
path = /home/share
force user = root
valid users = smbuser
public = yes
available = yes

save the file

Test this script using the command testparm

# testparm smb.conf

Are there any errors ?

1. What are the available options for security?

What do they indicate?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the username and the path in the share mode?

1. You need to create a Linux and samba user with the same username.

Add a linux user and set a password

**useradd smbuser**

**passwd smbuser**

For the same user set up a samba password.

**smbpasswd –a smbuser** ( set the password as smbuser)

set the same password for both accounts

1. Start the samba again to read the changes to the file

**service smb restart**

1. Check whether you have a directory *share* under */home*. If not create a directory under **/**home and give permissions 0777. Create a few files under */home/share.*

*#* cd /home/share

# touch file1 file2 file3

1. On the windows machine, set up a drive letter so that we can easily access these files.

Start – run – cmd < enter >

At the prompt type

# net use z: [\\ip\_of\_your\_samba\_server\share](file:///%5C%5Cip_of_your_samba_server%5Cshare) smbuser /user:smbuser

(eg:

if the ip address of your linux machine is 192.168.154.130

the command will be

net use z: [\\192.168.154.130\share](file:///%5C%5C192.168.154.130%5Cshare) smbuser /user:smbuser

The format of this command is

Net user drive name: [*\\ip*](file:///%5C%5Cip) *address of the server*\*share directory\_name* *smb\_password* /user:*smb user name* )

You assign a drive z: for access to the samba from the windows computer

You should get an output

 **Command completed successfully**

Show a screen shot

1. If there is an error denying access to the Linux samba server

Type the command on the Linux machine prompt

# setsebool –P samba\_enable\_home\_dirs=1

 What does the setsebool command do?

1. Click on **my computer** on windows xp machine. You will be able to see a new share drive z.
2. Show a screen shot of the drive
3. Show a screen shot of the files on the drive when you click on the link.
4. Restore the original config

cd /etc/samba

cp smb.conf.backup smb.conf

1. Study the command net use and write down the options

Explain the command you have used to assign a drive for access

 Get your work checked 1

**Review questions**

1. Which of these commands adds the username *smbuser1* to local *smbpasswd* file and sets a password in the Samba system for the user?
2. passwd smbuser1
3. smbpasswd smbuser1
4. smbpasswd –a smbuser1
5. smb passwd smbuser1
6. Match the following set of items
7. nmbd
8. smbd
9. winbindd

Name server message daemon

Daemon that handles communication with domain controllers

 Server message daemon

1. The contents of the *smb.conf* file can be validated using \_\_\_\_\_\_ command
2. net use
3. smb use
4. testparm
5. smbclient
6. Which of these statements is true?
7. Samba is an Open Source program running on a Linux server and it is designed to replace Microsoft file shares
8. Samba is an Microsoft program running on a Windows server and it is designed to replace Linux file shares
9. Samba is an Open Source program running on a Windows machine and it is designed to access Linux files
10. Samba is an Microsoft program running on a Linux server and it is designed to access Microsoft files.

 Get your work checked 2

**Marking Guide**

**Part A**

**Marks – 2**

2- Excellent all questions correctly answered, all screen shots given

1.5 – Good work. Some questions not answered and some screen shots missing. 75% of work done correctly

1 - Satisfactory –some of the questions answered correctly, some screen shots missing. Half the questions not answered. 50% of the questions and screen shots ok

1. Not submitted. Very poor work .

**Part B**

**Marks – 2**

**2 –** All screen shots given correctly . All questions answered

1 – Screenshot given ,but questions not answered fully

0 – screen shot not given