

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



**MÔN HỌC: PHÂN TÍCH MÃ ĐỘC**

**BÁO CÁO THỰC HÀNH BÀI 2**

**Giảng viên:** PGS.TS. Đỗ Xuân Chợt

**Sinh viên:** Hoàng Trung Kiên – B20DCAT098

Hà Nội – 5/2023

## Mục lục

1. Tìm hiểu về Nhật ký (Log) Unix trên CentOS. ....	3
a, Mục đích.....	3
b, Lý thuyết.....	3
2. Thực hành.....	4
<b>Nhiệm vụ 1:</b> Khám phá.....	4
<b>Nhiệm vụ 2:</b> Cấu hình lại rsyslog cho MARK .....	7
<b>Nhiệm vụ 3:</b> Cấu hình lại và Kiểm tra rsyslog. ....	9
Nhiệm vụ 4: Ghi log tập trung. ....	13
<b>Nhiệm vụ 5:</b> Các câu hỏi khác.....	18
3. Checkwork .....	21

## 1. Tìm hiểu về Nhật ký (Log) Unix trên CentOS.

### a, Mục đích.

Mục tiêu của bài tập này là để cung cấp cho sinh viên một trải nghiệm thực tế với cấu hình và kiểm thử syslog.

### b, Lý thuyết.

Trên CentOS, các nhật ký (log) hệ thống được quản lý bởi dịch vụ rsyslog. Các nhật ký này cung cấp thông tin về hoạt động của hệ thống, lỗi, cảnh báo và sự kiện quan trọng khác. Dưới đây là một số chi tiết về các nhật ký quan trọng trên CentOS:

-/var/log/messages:

- + Đây là nhật ký chung của hệ thống, ghi lại thông tin về các hoạt động hệ thống, cảnh báo và thông điệp quan trọng khác.

- + Bạn có thể tìm thấy thông tin về các dịch vụ, ứng dụng và kernel trong nhật ký này.

- + Các thông điệp cảnh báo (warning), lỗi (error), thông tin (info) và debug được ghi lại ở đây.

- + Nhật ký này cung cấp thông tin quan trọng để xem và phân tích khi có vấn đề xảy ra trên hệ thống.

- /var/log/secure:

- + Nhật ký này ghi lại các sự kiện liên quan đến bảo mật và đăng nhập.

- + Bạn có thể tìm thấy thông tin về đăng nhập thành công và thất bại, thay đổi mật khẩu, các hoạt động quản lý hệ thống trong nhật ký này.

- + Đây là một nhật ký quan trọng để kiểm tra và giám sát các hoạt động đăng nhập và bảo mật trên hệ thống.

- /var/log/boot.log:

- + Nhật ký này chứa thông tin về quá trình khởi động hệ thống.

- + Ghi lại các thông báo và lỗi liên quan đến quá trình khởi động.

- + Bạn có thể sử dụng nhật ký này để xem thông tin về quá trình khởi động hệ thống và tìm hiểu về các vấn đề liên quan đến khởi động.

- /var/log/dmesg:

- + Đây là nhật ký kernel, ghi lại các sự kiện quan trọng của kernel.

- + Bạn có thể tìm thấy thông tin về việc phát hiện phần cứng, lỗi và cảnh báo trong nhật ký này.

- + Nhật ký này cung cấp thông tin quan trọng về hoạt động của kernel và phần cứng.

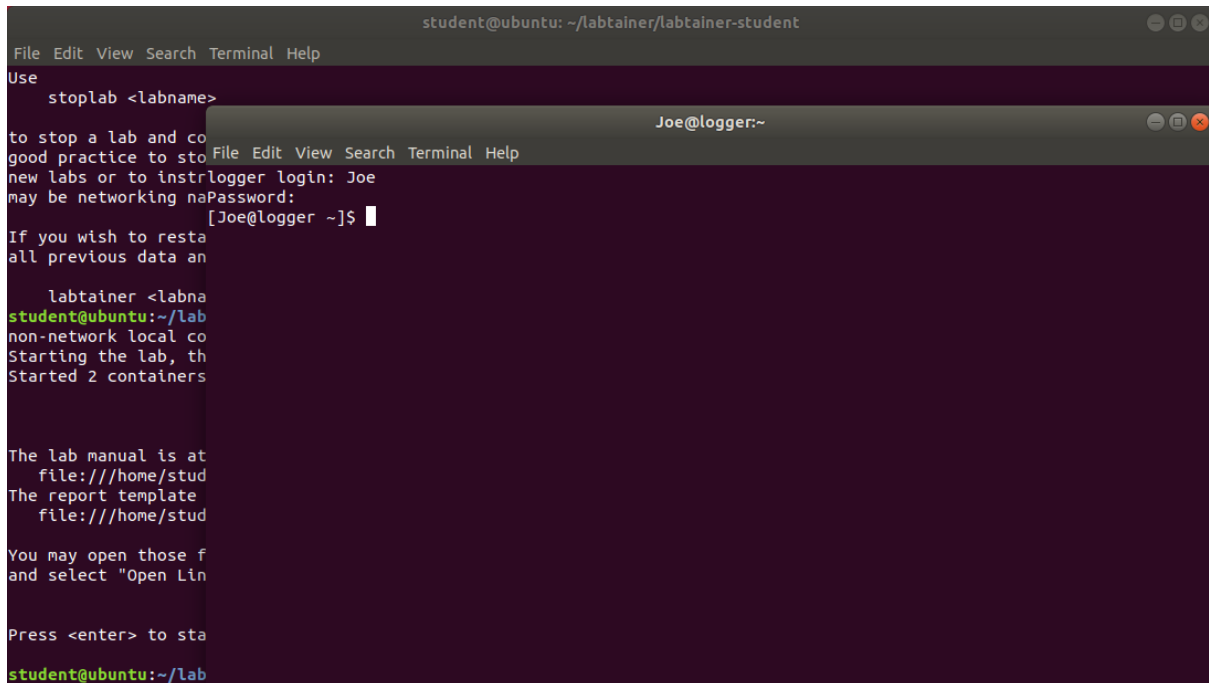
- Các nhật ký khác cũng tồn tại trên CentOS, bao gồm /var/log/httpd (nhật ký Apache), /var/log/mysql (nhật ký MySQL), /var/log/maillog (nhật ký mail), và nhiều loại nhật ký khác liên quan đến các dịch vụ cụ thể trên hệ thống CentOS.

## 2. Thực hành.

Khởi động lab: labtainer centos-log2

### Nhiệm vụ 1: Khám phá

Đăng nhập vào CentOS với tên người dùng Joe và mật khẩu "password4joe".



```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
Use
  stoplab <labname>
to stop a lab and co
good practice to sto
new labs or to instr
may be networking na
[Joe@logger ~]$
If you wish to resta
all previous data an
  labtainer <labna
student@ubuntu:~/lab
non-network local co
Starting the lab, th
Started 2 containers
The lab manual is at
file:///home/stud
The report template
file:///home/stud
You may open those f
and select "Open Lin
Press <enter> to sta
student@ubuntu:~/lab
```

- Trong terminal, nhập lệnh `sudo su` nhưng nhập sai mật khẩu cho người dùng root.
- Nhập lại lệnh `sudo su`, nhưng lần này nhập đúng mật khẩu cho root. Nếu làm đúng, dấu nhắc sẽ kết thúc bằng ký tự `#`.
- Khám phá thư mục log:
  - + Thay đổi thư mục làm việc hiện tại thành `/var/log`.
  - + Liệt kê nội dung của `/var/log`.

```
root@logger:/var/log
File Edit View Search Terminal Help
logger login: Joe
Password:
[Joe@logger ~]$ su
Password:
su: Authentication failure
[Joe@logger ~]$ sudo su
[root@logger Joe]# su
[root@logger Joe]# cd /var/log
[root@logger log]# ls
anaconda  grubby_prune_debug  maillog  rhsm  spooler  wtmp
btmp      lastlog              messages  secure  tallylog  yum.log
[root@logger log]#
```

```
[root@logger log]# ls -l /var/log/messages
-rw----- 1 root root 321768 Sep 27 07:42 /var/log/messages
[root@logger log]#
```

- ở vị trí đầu tiên chỉ ra rằng đây là một tệp tin thông thường, không phải một thư mục. rw- cho phép chủ sở hữu (root) có quyền đọc (r) và ghi (w) vào tệp tin, nhưng không có quyền thực thi (-). ----- cho thấy rằng không có nhóm hoặc người dùng khác có quyền truy cập vào tệp tin. Các dấu gạch ngang (-) cho mỗi cấp quyền chỉ ra rằng quyền truy cập đó không được cấp cho nhóm hoặc người dùng khác.

```
[root@logger log]# ls -l /var/log/secure
-rw----- 1 root root 9018 Sep 27 07:42 /var/log/secure
[root@logger log]#
```

Sep 26 14:05:44 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ;  
COMMAND=/home/Joe/.local/bin/Student.py Joe centos-log2.logger.student False  
Sep 27 07:51:22 logger su: pam\_unix(su:auth): authentication failure; logname=Joe  
uid=1000 euid=0 tty=pts/2 ruser=Joe rhost= user=root

- Mật khẩu sai:

+ Các bản ghi liên quan đến đăng nhập được lưu trong tệp văn bản có tên là secure. Các bản ghi mới nhất được ghi vào cuối tệp.

+ Mở tệp và tìm kiếm trạng thái failed khi cố gắng đăng nhập bằng tên người dùng Joe (không phải sự thất bại khi 'su' thành root).

-Sử dụng su:

+ Với tệp nhật ký secure vẫn mở, tìm mục ở cuối tệp liên quan đến hành động su thành root trước đó. Xem thông tin được lưu trữ về sử dụng su.

```
logger login: Joe
Password:
[Joe@logger ~]$ su
Password:
su: Authentication failure
[Joe@logger ~]$ sudo su
[root@logger Joe]# cd /var/log
[root@logger log]# ls
anaconda  grubby_prune_debug  maillog  rhsm  spooler  wtmp
btmptmp  lastlog  messages  secure  tallylog  yum.log
[root@logger log]# ls -l messages
ls: cannot access messages: No such file or directory
[root@logger log]# ls -l /var/log/messages
ls: cannot access /var/log/messages: No such file or directory
[root@logger log]# ls -l /var/log/messages
-rw-r----- 1 root root 322222 Sep 27 07:52 /var/log/messages
[root@logger log]# ls -l /var/log/secure
-rw-r----- 1 root root 9444 Sep 27 07:51 /var/log/secure
[root@logger log]# tail -n 20 /var/log/secure
Sep 26 14:01:32 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/rmdir /tmp/.mylockdir
Sep 26 14:05:43 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/cp --parents /root/.bash_history /home/Joe/.local/result
Sep 26 14:05:43 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+r -R /home/Joe/.local/result
Sep 26 14:05:43 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/cp --parents /var/log/messages /home/Joe/.local/result
Sep 26 14:05:43 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+r -R /home/Joe/.local/result
Sep 26 14:05:44 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/cp --parents /var/log/mydebug /home/Joe/.local/result
Sep 26 14:05:44 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+r -R /home/Joe/.local/result
Sep 26 14:05:44 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/Student.py Joe centos-log2.logger.student False
Sep 26 14:05:44 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/rmdir /tmp/.mylockdir
Sep 27 07:38:57 logger sshd[42]: Server listening on 0.0.0.0 port 22.
Sep 27 07:38:57 logger sshd[42]: Server listening on :: port 22.
Sep 27 07:39:49 logger login[94]: pam_unix(login:session): session opened for user Joe by (uid=0)
Sep 27 07:41:38 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=root
Sep 27 07:42:32 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/su
Sep 27 07:42:32 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Sep 27 07:42:37 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Sep 27 07:51:13 logger login[455]: pam_unix(login:session): session opened for user Joe by (uid=0)
Sep 27 07:51:22 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/2 ruser=Joe rhost= user=root
Sep 27 07:51:29 logger sudo: Joe : TTY=pts/2 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/su
Sep 27 07:51:29 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
[root@logger log]# ^C
[root@logger log]#
```

Tệp wtmp:

- Một trong số các tệp nhị phân trong thư mục nhật ký là tệp wtmp phổ biến, yêu cầu sử dụng các công cụ khác để trích xuất thông tin từ nó, chẳng hạn như lệnh last.

- Mở trang hỗ trợ “man” cho lệnh last bằng cách thực hiện các bước sau:

man last

- Đọc phần DESCRIPTION để tìm hiểu chức năng của lệnh.

- Điều hướng đến phần OPTIONS.

```
[root@logger log]# ls
anaconda  grubby_prune_debug  maillog  rhsm  spooler  wtmp
btmptmp  lastlog  messages  secure  tallylog  yum.log
[root@logger log]# ls -l /var/log/wtmp
-rw-rw-r-- 1 root utmp 1536 Sep 26 12:55 /var/log/wtmp
[root@logger log]#
```

**-t** YYYYMMDDHHMMSS

Display the state of logins as of the specified time. This is useful, e.g., to determine easily who was logged in at a particular time -- specify that time with -t and look for "still logged in".

#### SYNOPSIS

```
last [-R] [-num] [ -n num ] [-adFlowx] [ -f file ] [ -t YYYYMMDDHHMMSS ] [name...]
[ tty... ]
lastb [-R] [-num] [ -n num ] [ -f file ] [-adFlowx] [name...] [ tty... ]
```

```
[root@logger log]# last -t 20230927145930 wtmp
```

```
wtmp begins Tue Sep 26 12:55:06 2023
```

```
[root@logger log]#
```

Lựa chọn "-t" trong lệnh "last" được sử dụng để chỉ định thời gian kết thúc khi tìm kiếm lịch sử đăng nhập. Nó cho phép bạn xác định thời gian cuối cùng mà bạn muốn tìm kiếm các lần đăng nhập trước đó.

Cú pháp sử dụng lựa chọn "-t" là: last -t YYYYMMDDHHMMSS

Trong đó:

- "YYYY" là năm.
- "MM" là tháng.
- "DD" là ngày.
- "HH" là giờ.
- "MM" là phút.
- "SS" là giây.

Khi bạn sử dụng lựa chọn "-t", lệnh "last" sẽ chỉ hiển thị các lần đăng nhập trước thời điểm được chỉ định. Nó sẽ loại bỏ tất cả các lần đăng nhập sau thời gian đó khỏi kết quả tìm kiếm.

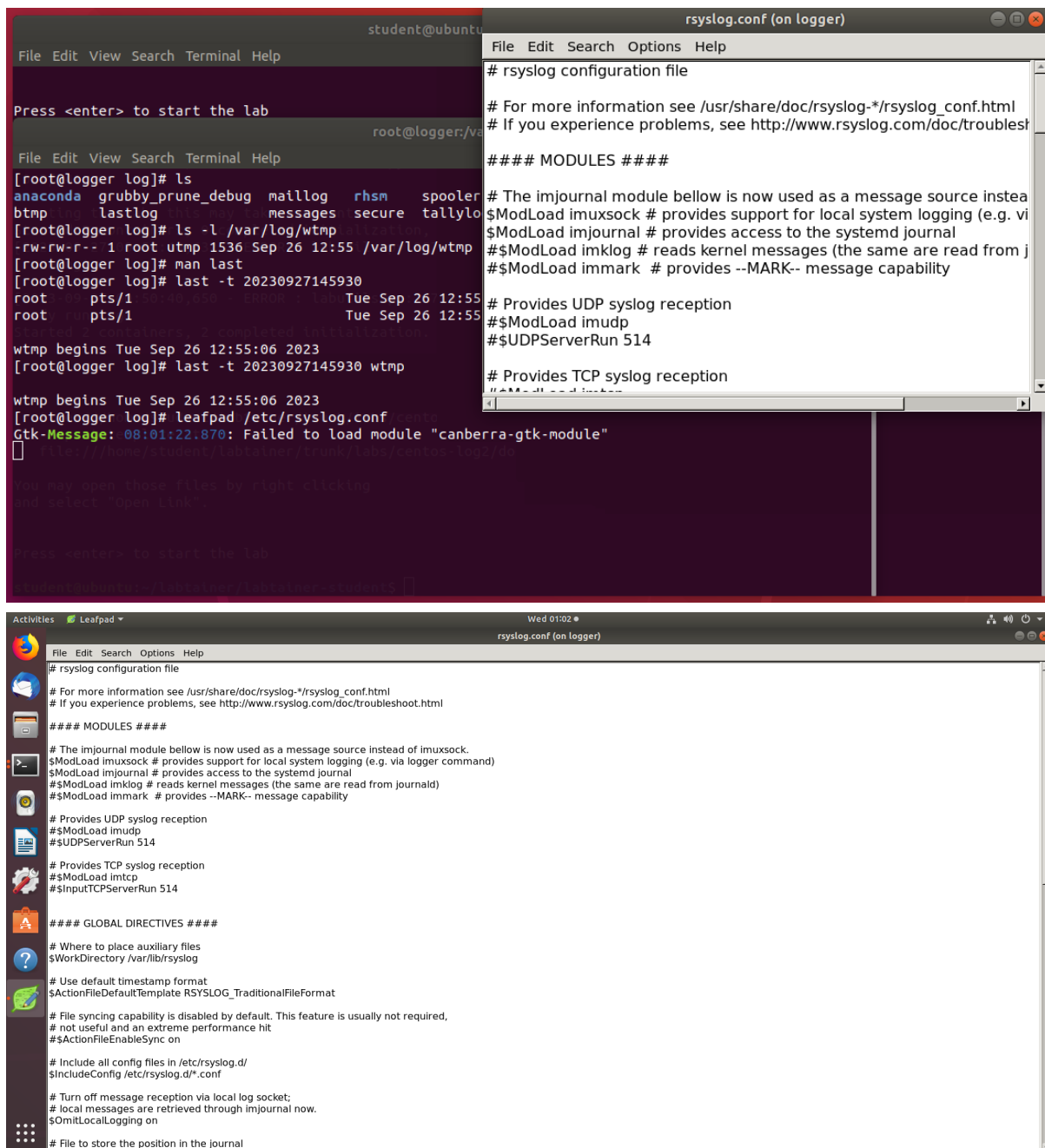
Ví dụ, nếu bạn muốn xem các lần đăng nhập trước ngày 1 tháng 10 năm 2023, bạn có thể sử dụng lệnh sau: last -t 20231001000000

Lựa chọn "-t" rất hữu ích khi bạn chỉ quan tâm đến các lần đăng nhập trước một thời điểm cụ thể và muốn loại bỏ các lần đăng nhập sau thời điểm đó khỏi kết quả tìm kiếm.

**Nhiệm vụ 2:** Cấu hình lại rsyslog cho MARK

- Mở tệp cấu hình rsyslog:

Trong khi vẫn chạy với đặc quyền root trong terminal, khởi chạy một trình soạn thảo từ dòng lệnh (như leafpad) để mở tệp /etc/rsyslog.conf



- Bật tính năng Mark:

Mặc định, việc chèn thời gian vào một tần suất đã chỉ định được vô hiệu hóa.

+ Trong phần "#### MODULES ####", tìm dòng có **\$ModLoad immark**, và xóa '#' để kích hoạt tính năng này.

+ Thiết lập tần suất của timestamps với việc thêm dòng tiếp theo dòng bên trên vừa mới thêm vào:

**\$MarkMessagePeriod 60**

"60" là số giây giữa các timestamps (giá trị mặc định thường là 20 phút)

+ Lưu thay đổi và thoát khỏi trình soạn thảo.



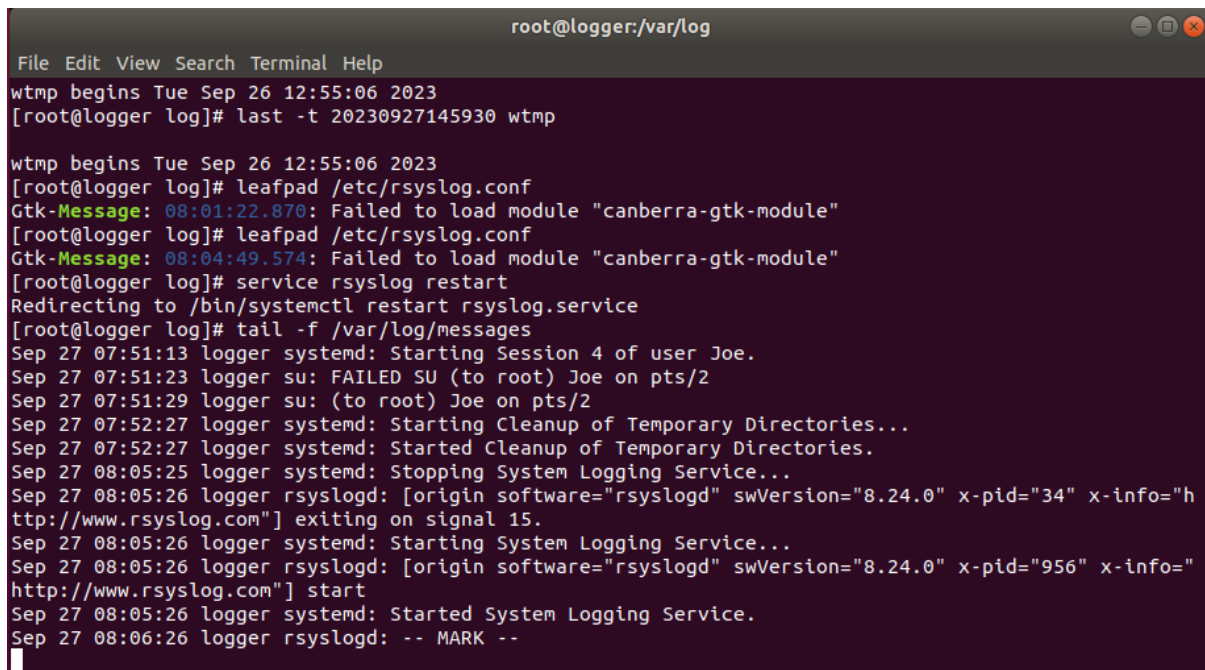
```
# The imjournal module below is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
$ModLoad immark # provides --MARK-- message capability
$MarkMessagePeriod 60
```

Khởi động lại tiến trình rsyslog.

Khởi động lại tiến trình rsyslog sẽ khiến nó khởi tạo lại và đọc lại tệp cấu hình (đồng nghĩa với việc thay đổi được áp dụng). Thực hiện các bước sau để khởi động lại:

service rsyslog restart

Tiếp tục chờ đợi cho đến khi thấy một bản ghi MARK xuất hiện trong nhật ký. Sau khi sinh viên đã thấy nó (hoặc sau hơn một phút), nhấn Ctrl-C để thoát khỏi tail.



```
root@logger:/var/log
File Edit View Search Terminal Help
wtmp begins Tue Sep 26 12:55:06 2023
[root@logger log]# last -t 20230927145930 wtmp

wtmp begins Tue Sep 26 12:55:06 2023
[root@logger log]# leafpad /etc/rsyslog.conf
Gtk-Message: 08:01:22.870: Failed to load module "canberra-gtk-module"
[root@logger log]# leafpad /etc/rsyslog.conf
Gtk-Message: 08:04:49.574: Failed to load module "canberra-gtk-module"
[root@logger log]# service rsyslog restart
Redirecting to /bin/systemctl restart rsyslog.service
[root@logger log]# tail -f /var/log/messages
Sep 27 07:51:13 logger systemd: Starting Session 4 of user Joe.
Sep 27 07:51:23 logger su: FAILED SU (to root) Joe on pts/2
Sep 27 07:51:29 logger su: (to root) Joe on pts/2
Sep 27 07:52:27 logger systemd: Starting Cleanup of Temporary Directories...
Sep 27 07:52:27 logger systemd: Started Cleanup of Temporary Directories.
Sep 27 08:05:25 logger systemd: Stopping System Logging Service...
Sep 27 08:05:26 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="34" x-info="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 08:05:26 logger systemd: Starting System Logging Service...
Sep 27 08:05:26 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="956" x-info="http://www.rsyslog.com"] start
Sep 27 08:05:26 logger systemd: Started System Logging Service.
Sep 27 08:06:26 logger rsyslogd: -- MARK --
```

**Nhiệm vụ 3:** Cấu hình lại và Kiểm tra rsyslog.

Đọc phần DESCRIPTION trong trang man của tiện ích logger:

man logger

```
root@logger:/var/log
File Edit View Search Terminal Help
NAME
    logger - a shell command interface to the syslog(3) system log module

SYNOPSIS
    logger [options] [message]

DESCRIPTION
    logger makes entries in the system log. It provides a shell command interface to the syslog(3) system log module.

OPTIONS
    -n, --server server
        Write to the specified remote syslog server instead of to the builtin syslog routines. Unless --udp or --tcp is specified the logger will first try to use UDP, but if it fails a TCP connection is attempted.

    -d, --udp
        Use datagram (UDP) only. By default the connection is tried to syslog port defined in /etc/services, which is often 514.

    -T, --tcp
        Use stream (TCP) only. By default the connection is tried to syslog-conn port defined in /etc/services, which is often 601.

Manual page logger(1) line 5/129 22% (press h for help or q to quit)
```

Tạo một mục trong /var/log/messages với mức ưu tiên "info" bằng cách thực hiện các bước sau:

`logger -p info "Hello World"`

```
root@logger:/var/log
File Edit View Search Terminal Help
logger login: Joe
Password:
[Joe@logger ~]$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-u user]
           [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-u user] file
...
[Joe@logger ~]$ su
Password:
su: Authentication failure
[Joe@logger ~]$ sudo su
[root@logger Joe]# cd /var/log
[root@logger log]# logger -p info "Hello World"
[root@logger log]#
```

Mở lại tệp cấu hình rsyslog tại /etc/rsyslog.conf và cuộn xuống phần “##### RULES #####”.

```

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
:msg, !contains, "apparmor"
*.info;mail.none;authpriv.none;cron.none    /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                /var/log/secure

# Log all the mail messages in one place.
mail.*                                    -/var/log/maillog

# Log cron stuff
cron.*                                    /var/log/cron

# Everybody gets emergency messages
*.emerg                                    :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                            /var/log/spooler

# Save boot messages also to boot.log
local7.*                                    /var/log/boot.log

```

Sử dụng grep (hoặc chọn công cụ khác) để xác minh rằng mục nhật ký đã được lưu trong tệp mà sinh viên nghĩ rằng nó sẽ được lưu

```

[root@logger log]# grep "Hello World" /var/log/messages
Sep 27 08:08:01 logger Joe: Hello World
Sep 27 08:22:31 logger Joe: Hello World
[root@logger log]#

```

. Mở lại tệp cấu hình syslog và cuộn xuống phần RULES.

Thêm một quy tắc syslog mới để đưa tất cả các thông báo với mức ưu tiên "debug" vào một tệp có tên là /var/log/mydebug. Tệp này chỉ nên chứa các thông báo debug.

```
rsyslog.conf (on logger)
File Edit Search Options Help

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* -/var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log

*.debug /var/log/mydebug

# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
```

sử dụng logger, hãy sử dụng nó để kiểm tra quy tắc mà sinh viên đã thêm vào rsyslog.conf

```
[root@logger log]# systemctl restart rsyslog
[root@logger log]# logger -p debug "B20DCAT098"
[root@logger log]# cat /var/log/mydebug
Sep 27 08:29:12 logger systemd: Stopping System Logging Service...
Sep 27 08:29:12 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1106" x-info="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 08:29:12 logger systemd: Starting System Logging Service...
Sep 27 08:29:12 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1651" x-info="http://www.rsyslog.com"] start
Sep 27 08:29:12 logger systemd: Started System Logging Service.
Sep 27 08:29:52 logger Joe: B20DCAT098
[root@logger log]#
```

Thực hiện các bước sau để hiển thị quyền liên quan đến lệnh logger:

ll/bin/logger

Không nên cho phép người dùng thông thường thực thi lệnh logger. Thay đổi quyền sao cho chỉ người dùng root và nhóm root mới có thể thực thi nó.

```
[root@logger log]# ll /bin/logger
-rwxr-xr-x 1 root root 29224 Dec  1 2017 /bin/logger
[root@logger log]# sudo chmod 750 /bin/logger
[root@logger log]# ll /bin/logger
-rwxr-x--- 1 root root 29224 Dec  1 2017 /bin/logger
[root@logger log]#
```

#### Nhiệm vụ 4: Ghi log tập trung.

1. Mở lại tệp cấu hình /etc/rsyslog.conf trên máy tính ghi log.
2. Tìm các mục sau trong tệp cấu hình và bỏ chú thích chúng (xóa dấu "#") để cho phép chấp nhận thông báo syslog trên cổng 514 qua TCP hoặc UDP:

```
*rsyslog.conf (on logger)
File Edit Search Options Help
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
$ModLoad immark # provides --MARK-- message capability
$MarkMessagePeriod 60

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on
```

#### 3. Khởi động lại rsyslog

systemctl restart rsyslog

```
[root@logger log]# systemctl restart rsyslog
[root@logger log]#
```

#### 4. Trên terminal chính của hệ thống lab

sử dụng lệnh: moreterm.py centos-log2 workstation

```
student@ubuntu:~/labtainer/labtainer-student$ moreterm.py centos-log2 workstation
student@ubuntu:~/labtainer/labtainer-student$
```

```
root@logger:/var/log
Sep 27 08:08:01 logger Joe: Hello World
Sep 27 08:22:31 logger Joe: Hello World
[root@logger log]# leafpad /etc/rsyslog.conf
Gtk+Message: WARNING: Glib::ModuleNotFoundError: Failed to load module "canberra-gtk-module"
[root@logger log]# systemctl restart rsyslog
[root@logger log]# logger -p debug "B20DCAT098"
[root@logger log]# cat /var/log/syslog
Sep 27 08:29:12 logger systemd: Stopping System Logging Service...
Sep 27 08:29:12 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1106" x-info="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 08:29:12 logger systemd: Starting System Logging Service...
Sep 27 08:29:12 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1651" x-info="http://www.rsyslog.com"] starting...
student@ubuntu:~/labtainer/labtainer-student

File Edit View Search Terminal Help
checkwork: command not found
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/centos-log2
Labname centos-log2

Student | logger_count | last_count | service_count | debug_log | exact_debug |
=====|=====|=====|=====|=====|=====|
B20DCAT098 | 4 | 14 | 2 | | |

What is automatically assessed for this lab:
log_mark: Altered rsyslog.conf, resulting in mark written to system log
logger_count, last_count, service_count: Counts of quantity of commands issued.
debug_log: Altered rsyslog.conf, resulting in debug messages going to a custom log file (though it may not be limited to debug messages)
exact_debug: Altered rsyslog.conf, resulting in only debug messages going to a custom log file
student@ubuntu:~/labtainer/labtainer-student$ moretern.py centos-log2 workstation
student@ubuntu:~/labtainer/labtainer-student$
```

5. Một terminal ảo mới được mở và kết nối với máy tính trạm. Máy tính này chia sẻ mạng với máy tính ghi log của sinh viên. Sử dụng "ifconfig" trên mỗi máy tính để xem địa chỉ IP của mỗi máy tính.

```
root@logger:/var/log
[root@logger log]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.25.0.2 netmask 255.255.255.0 broadcast 172.25.0.255
    ether 02:42:ac:19:00:02 txqueuelen 0 (Ethernet)
    RX packets 73 bytes 8734 (8.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@logger log]#

student@ubuntu:~/labtainer/labtainer-student$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.25.0.3 netmask 255.255.255.0 broadcast 172.25.0.255
    ether 02:42:ac:19:00:03 txqueuelen 0 (Ethernet)
    RX packets 79 bytes 9322 (9.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[Joe@workstation ~]$
```

6. Trên máy tính ghi log, sử dụng "tail" để xem các nhật ký: tail -f /var/log/\*





```
root@logger:/var/log
File Edit View Search Terminal Help
Sep 27 08:41:47 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0"
fo="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 08:41:47 workstation systemd: Starting System Logging Service...
Sep 27 08:41:47 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0"
nfo="http://www.rsyslog.com"] start
Sep 27 08:41:47 workstation systemd: Started System Logging Service.

==> /var/log/messages <==
Sep 27 08:42:16 workstation logger: Hello PTIT

==> /var/log/mydebug <==
Sep 27 08:42:16 workstation logger: Hello PTIT

==> /var/log/messages <==
Sep 27 08:42:19 logger rsyslogd: -- MARK --

==> /var/log/mydebug <==
Sep 27 08:42:19 logger rsyslogd: -- MARK --

==> /var/log/messages <==
Sep 27 08:42:34 workstation logger: Hello KienAT098

==> /var/log/mydebug <==
Sep 27 08:42:34 workstation logger: Hello KienAT098

What is automatically assessed for this lab:
log_mark: Altered rsyslog.conf, resulting in mark written to system log
logger_count, last_count, service_count: Counts of quantity of commands issued.
debug_log: altered rsyslog.conf, resulting in debug messages going to
a custom log file (though it may not be limited to debug messages)
exact_debug: Altered rsyslog.conf, resulting in only debug messages going to
a custom log file
student@ubuntu:~/labtainer/labtainer-student$ moreterm.py centos-log2 workstation
student@ubuntu:~/labtainer/labtainer-student$
```

```
root@workstation:/home/Joe
File Edit View Search Terminal Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.25.0.3 netmask 255.255.255.0 broadcast 172.25.0.255
ether 02:42:ac:19:00:03 txqueuelen 0 (Ethernet)
RX packets 79 bytes 9322 (9.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[Joe@workstation ~]$ sudo su
[root@workstation Joe]# leafpad /etc/rsyslog.conf
Gtk-Message: 08:39:30.990: Failed to load module "canberra-gtk-module"
^C
[root@workstation Joe]# systemctl restart rsyslog
[root@workstation Joe]# logger -p info "Hello PTIT"
[root@workstation Joe]# logger -p info "Hello KienAT098"
[root@workstation Joe]#
```

10. Thử nghiệm với các sự kiện liên quan đến bảo mật khác nhau như giảm đặc quyền và nâng cao đặc quyền trên máy tính trạm và thực hiện các lệnh logger từ máy tính trạm.

```
rsyslog.conf (on workstation)
File Edit Search Options Help

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
:msg, !contains, "apparmor"
*.info;mail.none;authpriv.none;cron.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* -/var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log

if $syslogseverity-text == 'debug' then /var/log/mydebug

#### begin forwarding rule ####
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
```

```
root@workstation:/home/Joe
File Edit View Search Terminal Help
[root@workstation Joe]# leafpad /etc/rsyslog.conf
Gtk-Message: 08:58:50.288: Failed to load module "canberra-gtk-module"
[root@workstation Joe]# systemctl restart rsyslog
[root@workstation Joe]# tail -f /var/log/messages
Sep 27 08:55:23 workstation logger: Hello KienAT098
Sep 27 08:55:27 workstation logger: Hello PTIT
Sep 27 08:57:55 workstation logger: Hello PTIT
Sep 27 08:57:59 workstation logger: Hello KienAT098
Sep 27 08:58:39 workstation logger: Hello KienAT098
Sep 27 09:01:14 workstation systemd: Stopping System Logging Service...
Sep 27 09:01:14 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="341" x-info="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 09:01:14 workstation systemd: Starting System Logging Service...
Sep 27 09:01:14 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="718" x-info="http://www.rsyslog.com"] start
Sep 27 09:01:14 workstation systemd: Started System Logging Service.
^C
[root@workstation Joe]# systemctl restart rsyslog
[root@workstation Joe]# logger -p debug "Hello KienAT098"
[root@workstation Joe]# cat /var/log/mydebug
Sep 27 09:02:57 workstation logger: Hello KienAT098
[root@workstation Joe]# leafpad /etc/rsyslog.conf
Gtk-Message: 09:04:05.782: Failed to load module "canberra-gtk-module"
^C
```



```
root@workstation:/home/Joe
File Edit View Search Terminal Help
root@workstation Joe]# logger -p info "Hello KienAT098"
root@workstation Joe]# logger -p info "Hello KienAT098"
root@workstation Joe]# leafpad /etc/rsyslog.conf
k-Message: 08:58:56.288: Failed to load module "canberra-gtk-module"
root@workstation Joe]# systemctl restart rsyslog
root@workstation Joe]# tail -f /var/log/messages
27 08:55:23 workstation logger: Hello KienAT098
27 08:55:27 workstation logger: Hello PTIT
27 08:57:55 workstation logger: Hello PTIT
27 08:57:59 workstation logger: Hello KienAT098
27 08:58:39 workstation logger: Hello KienAT098
27 09:01:14 workstation systemd: Stopping System Logging Service...
27 09:01:14 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.2
" x-pid="341" x-info="http://www.rsyslog.com"] exiting on signal 15.
27 09:01:14 workstation systemd: Starting System Logging Service...
27 09:01:14 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.2
" x-pid="718" x-info="http://www.rsyslog.com"] start
27 09:01:14 workstation systemd: Started System Logging Service.

root@workstation Joe]# systemctl restart rsyslog
root@workstation Joe]# logger -p debug "Hello KienAT098"
root@workstation Joe]# cat /var/log/mydebug
27 09:02:57 workstation logger: Hello KienAT098
root@workstation Joe]#
```

```
root@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# tail -f /var/log/messages
Sep 27 09:03:41 logger rsyslogd: -- MARK --
Sep 27 09:04:41 logger rsyslogd: -- MARK --
Sep 27 09:05:12 workstation logger: Hello KienAT098
Sep 27 09:05:41 logger rsyslogd: -- MARK --
Sep 27 09:05:54 workstation logger: Hello KienAT098
Sep 27 09:06:35 logger systemd: Stopping System Logging Service...
Sep 27 09:06:35 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="2069" x-info=
"http://www.rsyslog.com"] exiting on signal 15.
Sep 27 09:06:35 logger systemd: Starting System Logging Service...
Sep 27 09:06:35 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="2250" x-info=
"http://www.rsyslog.com"] start
Sep 27 09:06:35 logger systemd: Started System Logging Service.
Sep 27 09:07:35 logger rsyslogd: -- MARK --
^C
[root@logger log]# logger -p debug "Hello KienAT098"
[root@logger log]# cat /var/log/mydebug
Sep 27 08:29:12 logger systemd: Stopping System Logging Service...
Sep 27 08:29:12 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1106" x-info=
"http://www.rsyslog.com"] exiting on signal 15.
Sep 27 08:29:12 logger systemd: Starting System Logging Service...
Sep 27 08:29:12 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1651" x-info=
"http://www.rsyslog.com"] start
Sep 27 08:29:12 logger systemd: Started System Logging Service.
Sep 27 08:29:52 logger Joe: B20DCAT098
```

```
root@logger:/var/log
File Edit View Search Terminal Help
nfo="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 09:01:14 workstation systemd: Starting System Logging Service...
Sep 27 09:01:14 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="718" x-i
nfo="http://www.rsyslog.com"] start
Sep 27 09:01:14 workstation systemd: Started System Logging Service.
Sep 27 09:01:41 logger rsyslogd: -- MARK --
Sep 27 09:02:36 workstation systemd: Stopping System Logging Service...
Sep 27 09:02:36 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="718" x-i
nfo="http://www.rsyslog.com"] exiting on signal 15.
Sep 27 09:02:36 workstation systemd: Starting System Logging Service...
Sep 27 09:02:36 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="766" x-i
nfo="http://www.rsyslog.com"] start
Sep 27 09:02:36 workstation systemd: Started System Logging Service.
Sep 27 09:02:41 logger rsyslogd: -- MARK --
Sep 27 09:02:57 workstation logger: Hello KienAT098
Sep 27 09:03:41 logger rsyslogd: -- MARK --
Sep 27 09:04:41 logger rsyslogd: -- MARK --
Sep 27 09:05:00 workstation logger: Hello KienAT098
Sep 27 09:05:12 workstation logger: Hello KienAT098
Sep 27 09:05:41 logger rsyslogd: -- MARK --
Sep 27 09:05:54 workstation logger: Hello KienAT098
Sep 27 09:07:02 logger Joe: Hello KienAT098
Sep 27 09:07:18 workstation logger: Hello KienAT098
Sep 27 09:08:29 logger Joe: Hello KienAT098
[root@logger log]#
```

### Nhiệm vụ 5: Các câu hỏi khác.

1. Đối với tệp log `"/var/log/messages"` trên CentOS, quyền được cấp cho người dùng thông thường (non-root users) phụ thuộc vào cấu hình thư mục `/var/log` và quyền truy cập được gán cho tệp tin đó.

Mặc định trên CentOS, tệp log `"/var/log/messages"` có quyền truy cập như sau:

Quyền đọc (read) được cấp cho tất cả người dùng trên hệ thống.

Quyền ghi (write) và thay đổi (modify) chỉ được cấp cho người dùng root hoặc các người dùng thuộc nhóm root.

2. Trong tệp log `"/var/log/secure"` trên CentOS, từ ngữ "Failed" (thất bại) thường được sử dụng để chỉ một nỗ lực đăng nhập không thành công. Khi một người dùng cố gắng đăng nhập vào hệ thống và không thành công, một thông báo được ghi lại trong tệp log `"/var/log/secure"` với một dòng chứa từ "Failed" để chỉ ra rằng nỗ lực đăng nhập đã không thành công.

3. Trong hệ thống rsyslog, MARK là một thông báo đặc biệt được ghi vào nhật ký (log) để đánh dấu thời điểm hiện tại. Điều này có thể hữu ích trong một số tình huống thực tế, ví dụ:

Giám sát hoạt động hệ thống: Khi cấu hình rsyslog để ghi lại MARK vào nhật ký, bạn có thể sử dụng nó để theo dõi hoạt động tồn tại của hệ thống. Khi MARK được ghi vào nhật ký, nó cho biết rằng hệ thống vẫn hoạt động bình thường, và bạn có thể sử dụng thông tin này để kiểm tra sự ổn định và khả dụng của hệ thống.

Đồng bộ hóa các nhật ký: Trong một môi trường phân tán với nhiều hệ thống và các bản ghi nhật ký được ghi lại trên các máy chủ khác nhau, việc sử dụng MARK có thể giúp đồng bộ hóa các bản ghi nhật ký. Bằng cách đồng bộ hóa các MARK trên các hệ thống, bạn có thể xác định thời điểm chính xác mà các sự kiện nhật ký được ghi lại, đồng bộ hóa việc phân tích và theo dõi các hoạt động hệ thống.

4. Trong tệp log `"/var/log/secure"` trên CentOS, từ ngữ `"su"` được sử dụng để tăng đặc quyền (switch user) và trở thành người dùng khác có quyền hạn cao hơn.

5. Tùy chọn `-t` của lệnh `"last"` được sử dụng để chỉ định một thời gian cụ thể để lấy thông tin về các phiên đăng nhập trước đó. Chức năng của tùy chọn `-t` là giới hạn kết quả trả về từ lệnh `"last"` dựa trên thời gian.

6. Trong tệp cấu hình syslog, để phù hợp với bản ghi được gửi bằng lệnh logger với facility là `"user"` và priority là `"info"`, bạn có thể sử dụng quy tắc sau: `user.info`

`/var/log/user.log`

Trong quy tắc trên:

`"user.info"` là sự kết hợp giữa facility `"user"` và priority `"info"`.

`"/var/log/user.log"` là đường dẫn đến tệp log mà bạn muốn ghi lại bản ghi.

Quy tắc trên có nghĩa là tất cả các bản ghi với facility là `"user"` và priority là `"info"` sẽ được ghi lại vào tệp log `"/var/log/user.log"`.

7. Để đưa các thông báo gỡ lỗi vào tệp log `"/var/log/mydebug"`, có thể thêm quy tắc sau vào tệp cấu hình syslog: `*.debug /var/log/mydebug`

Trong quy tắc trên:

`"*.debug"` chỉ định rằng tất cả các facility và priority được đánh dấu là `"debug"` sẽ được ghi lại.

`"/var/log/mydebug"` là đường dẫn đến tệp log mà sinh viên muốn ghi lại các thông báo gỡ lỗi.

8. Sử dụng logger, hãy sử dụng nó để kiểm tra quy tắc đã thêm vào `rsyslog.conf`

9. Thực hiện các bước sau để hiển thị quyền liên quan đến lệnh logger:

`ll/bin/logger`

10. Trong tệp cấu hình `rsyslog.conf`, nếu rsyslog nhận được một bản ghi từ kernel với mức ưu tiên là `"emerg"` (emergency), nó sẽ thực hiện hành động được chỉ định trong quy tắc có mức ưu tiên cao nhất tương ứng với facility `"kernel"`.

Quy tắc với mức ưu tiên cao nhất cho facility `"kernel"` thường được định nghĩa bởi dòng sau trong tệp cấu hình `rsyslog.conf`: `kern.* /var/log/kern.log`

Trong đó:

`"kern.*"` chỉ định rằng tất cả các mức ưu tiên từ facility `"kernel"` sẽ được ghi lại.

`"/var/log/kern.log"` là đường dẫn đến tệp log mà bản ghi từ kernel sẽ được ghi vào.

Vì "emerg" là mức ưu tiên cao nhất, nếu một bản ghi từ kernel có mức ưu tiên là "emerg" được nhận, nó sẽ được ghi vào `/var/log/kern.log` theo quy tắc trên. Điều này cho phép ghi lại các bản ghi khẩn cấp từ kernel vào tệp log "kern.log" để theo dõi và xử lý các tình huống khẩn cấp.

11. Để xác định hành động cụ thể mà rsyslog sẽ thực hiện nếu nhận được một bản ghi từ facility "mail" với mức ưu tiên "notice" trong tệp cấu hình rsyslog.conf.

Trong tệp cấu hình rsyslog.conf, quy tắc cho facility "mail" và mức ưu tiên "notice" được định nghĩa bằng cú pháp sau: `mail.notice /var/log/mail.log`

Trong đó:

- "mail.notice" chỉ định rằng chỉ các bản ghi với mức ưu tiên "notice" từ facility "mail" sẽ được xử lý.

- `/var/log/mail.log` là đường dẫn đến tệp log mà các bản ghi từ facility "mail" và mức ưu tiên "notice" sẽ được ghi vào.

Vì trong trường hợp này, mức ưu tiên là "notice", nếu rsyslog nhận được một bản ghi từ facility "mail" với mức ưu tiên "notice", nó sẽ ghi bản ghi đó vào tệp log `/var/log/mail.log` theo quy tắc trên.

Do đó, hành động mà rsyslog sẽ thực hiện là ghi lại bản ghi từ facility "mail" với mức ưu tiên "notice" vào tệp log `/var/log/mail.log`. Điều này cho phép theo dõi và xử lý các thông báo quan trọng từ hệ thống mail.

12. Để xác định hành động mà rsyslog sẽ thực hiện nếu nhận được một bản ghi từ facility "local6" với mức ưu tiên "err" trong tệp cấu hình rsyslog.conf, chúng ta cần kiểm tra quy tắc tương ứng với facility và mức ưu tiên này.

Quy tắc cho facility "local6" và mức ưu tiên "err" trong tệp cấu hình rsyslog.conf có thể được định nghĩa dưới dạng: `local6.err /var/log/local6.log`

Trong đó:

- "local6.err" chỉ định rằng chỉ các bản ghi với mức ưu tiên "err" từ facility "local6" sẽ được xử lý.

- `/var/log/local6.log` là đường dẫn đến tệp log mà các bản ghi từ facility "local6" và mức ưu tiên "err" sẽ được ghi vào.

Vì mức ưu tiên là "err", nếu rsyslog nhận được một bản ghi từ facility "local6" với mức ưu tiên "err", nó sẽ ghi bản ghi đó vào tệp log `/var/log/local6.log` theo quy tắc trên.

Do đó, hành động mà rsyslog sẽ thực hiện là ghi lại bản ghi từ facility "local6" với mức ưu tiên "err" vào tệp log `/var/log/local6.log`. Điều này cho phép theo dõi và xử lý các thông báo lỗi quan trọng từ facility "local6".

13. Thực hiện việc đọc và phân tích tệp cấu hình rsyslog.conf để tìm hiểu cách các quy tắc hoạt động và hành động mà rsyslog thực hiện cho các bản ghi từ các facility và mức ưu tiên khác nhau.

14. Từ bài thực hành này, học được:

- +Hiểu về cấu trúc và cú pháp của tệp cấu hình rsyslog.conf.
- +Cách định nghĩa quy tắc hoạt động dựa trên facility và mức ưu tiên của bản ghi.
- +Cách xác định hành động mà rsyslog thực hiện cho từng quy tắc.
- +Cách định vị và ghi log các sự kiện quan trọng từ các facility khác nhau.

15. Để cải thiện bài thực hành này, có thể thực hiện các bước sau:

+Cung cấp ví dụ cụ thể hơn về tệp cấu hình rsyslog.conf để sinh viên có thể thực hiện các thử nghiệm và khám phá nhiều hơn. Ví dụ, có thể tạo các quy tắc cho các facility khác nhau và các mức ưu tiên khác nhau để xem rsyslog thực hiện hành động như thế nào.

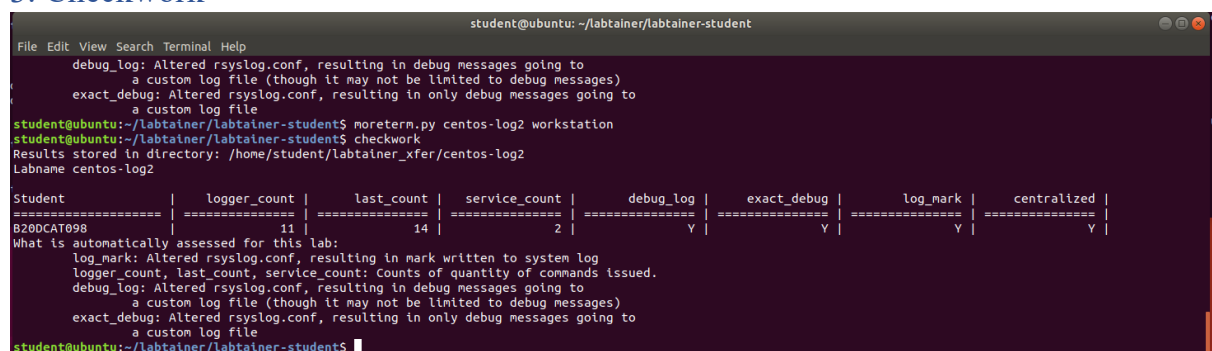
+ Cung cấp các bài tập thực hành bổ sung để sinh viên áp dụng kiến thức đã học vào các tình huống thực tế khác nhau. Ví dụ, yêu cầu sinh viên cấu hình rsyslog để ghi log từ các ứng dụng cụ thể hoặc ghi log vào các đích kèm tệp log khác nhau.

+ Cung cấp giải thích chi tiết về các tùy chọn và tham số trong tệp cấu hình rsyslog.conf để sinh viên có thể tùy chỉnh và điều chỉnh cấu hình theo nhu cầu của họ.

+ Đảm bảo rằng các mục tiêu học tập và kết quả mong đợi của bài thực hành được rõ ràng và có thể đạt được. Điều này giúp sinh viên hiểu rõ hơn về mục tiêu của bài thực hành và đánh giá kỹ năng và kiến thức của mình.

+ Cung cấp tài liệu tham khảo bổ sung hoặc tài liệu hướng dẫn để sinh viên có thể tiếp tục nghiên cứu và khám phá thêm về rsyslog và cách quản lý log hệ thống.

### 3. Checkwork



```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
debug_log: Altered rsyslog.conf, resulting in debug messages going to
a custom log file (though it may not be limited to debug messages)
exact_debug: Altered rsyslog.conf, resulting in only debug messages going to
a custom log file
student@ubuntu:~/labtainer/labtainer-student$ moreterm.py centos-log2 workstation
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/centos-log2
Labname centos-log2

Student | logger_count | last_count | service_count | debug_log | exact_debug | log_mark | centralized |
=====|=====|=====|=====|=====|=====|=====|=====|
820DCAT098 | 11 | 14 | 2 | Y | Y | Y | Y |
What is automatically assessed for this lab:
log mark: Altered rsyslog.conf, resulting in mark written to system log
logger_count, last_count, service_count: Counts of quantity of commands issued.
debug_log: Altered rsyslog.conf, resulting in debug messages going to
a custom log file (though it may not be limited to debug messages)
exact_debug: Altered rsyslog.conf, resulting in only debug messages going to
a custom log file
student@ubuntu:~/labtainer/labtainer-student$
```