

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484**

CA THỰC HÀNH: 02

NHÓM LỚP: INT1484-02

**TÊN BÀI: CENTOS-LOG2 – KHÁM PHÁ NHẬT KÝ (LOG) UNIX
TRÊN CENTOS**

Sinh viên thực hiện:

B22DCAT063 Lê Tiến Dương

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

| | |
|---|-----------|
| MỤC LỤC | 2 |
| DANH MỤC CÁC HÌNH VẼ..... | 3 |
| DANH MỤC CÁC TỪ VIẾT TẮT..... | 5 |
| CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH | 6 |
| 1.1 Mục đích..... | 6 |
| 1.2 Tìm hiểu lý thuyết | 6 |
| 1.2.1 CentOS | 6 |
| 1.2.2 Syslog | 6 |
| 1.2.3 Quy trình hoạt động của Syslog trên CentOS (với Rsyslog) | 7 |
| 1.2.4 Lợi ích của việc sử dụng Syslog trên CentOS..... | 8 |
| CHƯƠNG 2. NỘI DUNG THỰC HÀNH | 9 |
| 2.1 Chuẩn bị môi trường | 9 |
| 2.2 Các bước thực hiện..... | 9 |
| 2.2.1 Khởi động lab | 9 |
| 2.2.2 Các nhiệm vụ..... | 9 |
| 2.2.3 Kết thúc lab | 30 |
| CHƯƠNG 3. KẾT QUẢ THỰC HÀNH | 31 |
| TÀI LIỆU THAM KHẢO..... | 32 |

DANH MỤC CÁC HÌNH VẼ

| | |
|---|----|
| Hình 1 – Khởi động bài lab | 9 |
| Hình 2 – Đăng nhập người dùng Joe..... | 9 |
| Hình 3 – su với mật khẩu sai | 10 |
| Hình 4 – Nhập đúng mật khẩu root | 10 |
| Hình 5 – Xem thư mục /var/log..... | 10 |
| Hình 6 – Quyền của tệp messages..... | 11 |
| Hình 7 – Đăng nhập Joe thất bại | 11 |
| Hình 8 – Mở tệp secure và tìm kiếm trạng thái failed..... | 11 |
| Hình 9 – Nhập “password” làm tên người dùng | 12 |
| Hình 10 – Xem tệp nhật ký Secure | 12 |
| Hình 11 – Tìm các mục liên quan đến hành động root | 12 |
| Hình 12 – Đọc phần DESCRIPTION | 13 |
| Hình 13 – Đọc OPTIONS của lệnh last | 14 |
| Hình 14 – Mở tệp /etc/rsyslog.conf..... | 14 |
| Hình 15 – Thiết lập tần suất của timestamps | 15 |
| Hình 16 – Lưu thay đổi và khởi động lại rsyslog..... | 15 |
| Hình 17 – Xem thay đổi | 16 |
| Hình 18 – Đọc phần DESCRIPTION | 16 |
| Hình 19 – Tạo bản ghi “Hello World” với logger..... | 17 |
| Hình 20 – Mở lại tệp cấu hình rsyslog | 17 |
| Hình 21 – Xem quy tắc chỉ định nơi lưu bản ghi | 17 |
| Hình 22 – Xác minh bản ghi | 18 |
| Hình 23 – Mở lại tệp cấu hình rsyslog | 18 |
| Hình 24 – Thêm quy tắc cho rsyslog..... | 18 |
| Hình 25 – Khởi động lại rsyslog | 19 |
| Hình 26 – Tạo bản ghi debug | 19 |
| Hình 27 – Kiểm tra tệp /var/log/mydebug | 19 |
| Hình 28 – Sửa lại file rsyslog..... | 20 |
| Hình 29 – Khởi động lại rsyslog | 20 |
| Hình 30 – Thêm hai bản ghi debug và info..... | 20 |
| Hình 31 – Kiểm tra file /var/log/mydebug | 21 |
| Hình 32 – Kiểm tra và thay đổi quyền của logger | 21 |
| Hình 33 – Sửa tệp rsyslog | 22 |
| Hình 34 – Khởi động lại dịch vụ rsyslog | 22 |
| Hình 35 – Khởi động terminal cho máy trạm | 22 |
| Hình 36 – Kiểm tra IP máy ghi log | 23 |
| Hình 37 – Kiểm tra IP máy trạm | 23 |
| Hình 38 – Nâng quyền máy trạm | 24 |
| Hình 39 – Sửa lại file rsyslog..... | 24 |
| Hình 40 – Khởi động lại rsyslog | 24 |
| Hình 41 – Xem log | 25 |
| Hình 42 – Tạo bản ghi và thay đổi quyền | 25 |
| Hình 43 – Xem log | 26 |

| | |
|--|----|
| Hình 44 – Người dùng thông thường không có quyền..... | 26 |
| Hình 45 – Từ chỉ một nỗ lực không thành công | 26 |
| Hình 46 – Sinh viên tăng đặc quyền bằng su | 28 |
| Hình 47 – OPTIONS của lệnh last | 28 |
| Hình 48 – Xem quy tắc chỉ định nơi lưu bản ghi | 28 |
| Hình 49 – Thêm quy tắc để đưa ra các thông báo gỡ lỗi..... | 29 |
| Hình 50 – Kết quả checkwork..... | 31 |

DANH MỤC CÁC TỪ VIẾT TẮT

| Từ viết tắt | Thuật ngữ tiếng Anh/Giải thích | Thuật ngữ tiếng Việt/Giải thích |
|--------------------|---------------------------------------|---|
| RHEL | Red Hat Enterprise Linux | Bản phân phối Linux thương mại của Red Hat |
| EUID | Effective User ID | UID hiệu lực (thực thi) |
| TTY | Teletypewriter | Thiết bị dòng lệnh đầu cuối |
| PAM | Pluggable Authentication Modules | Mô-đun xác thực có thể cắm vào hệ thống Linux |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 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.

1.2 Tìm hiểu lý thuyết

1.2.1 CentOS

1.2.1.1 CentOS là gì?

CentOS (Community ENTerprise Operating System) là một bản phân phối Linux mã nguồn mở, miễn phí và được xây dựng dựa trên các gói nguồn của Red Hat Enterprise Linux (RHEL). RHEL, một bản phân phối Linux thương mại được đánh giá cao về tính ổn định và độ tin cậy, là nền tảng vững chắc cho CentOS. Mục tiêu chính của dự án CentOS là cung cấp một hệ điều hành cấp doanh nghiệp, tương thích nhị phân hoàn toàn với RHEL, nhưng loại bỏ các thành phần độc quyền liên quan đến thương hiệu và bản quyền.

1.2.1.2 Đặc điểm nổi bật của CentOS

- *Tính ổn định và độ tin cậy:* Kế thừa từ RHEL, CentOS nổi tiếng với sự ổn định vượt trội. Các bản cập nhật thường tập trung vào việc vá lỗi bảo mật và đảm bảo tính ổn định của hệ thống, hạn chế tối đa việc giới thiệu các tính năng mới có thể gây ra rủi ro trong môi trường sản xuất. Chu kỳ phát hành của CentOS cũng tương đối dài, mang lại sự nhất quán và dễ dàng quản lý cho các hệ thống triển khai lâu dài.
- *Miễn phí và mã nguồn mở:* Một trong những ưu điểm lớn nhất của CentOS là hoàn toàn miễn phí để sử dụng, phân phối và sửa đổi. Bản chất mã nguồn mở cho phép người dùng kiểm tra, tùy chỉnh và đóng góp vào sự phát triển của hệ điều hành. Điều này tạo ra một cộng đồng người dùng và nhà phát triển lớn mạnh, sẵn sàng hỗ trợ lẫn nhau.
- *Khả năng tương thích cao:* CentOS được thiết kế để tương thích nhị phân với RHEL. Điều này có nghĩa là các ứng dụng và phần mềm được phát triển cho RHEL thường có thể chạy tốt trên CentOS mà không cần sửa đổi. Đây là một lợi thế lớn cho các tổ chức muốn tận dụng sự ổn định của RHEL nhưng với chi phí thấp hơn.
- *Hệ thống quản lý gói mạnh mẽ (Yum/DNF):* CentOS sử dụng trình quản lý gói Yum (Yellowdog Updater, Modified) trong các phiên bản cũ hơn và DNF (Dandified Yum) trong các phiên bản gần đây. Các công cụ này cho phép người dùng dễ dàng cài đặt, cập nhật, gỡ bỏ và quản lý các gói phần mềm từ các kho lưu trữ (repositories) một cách nhất quán và tự động hóa các tác vụ quản lý phần mềm phức tạp.
- *Bảo mật được ưu tiên:* CentOS thường xuyên nhận được các bản cập nhật bảo mật từ Red Hat (sau một khoảng trễ nhất định). Điều này đảm bảo rằng hệ thống luôn được bảo vệ trước các lỗ hổng bảo mật mới nhất. Tính ổn định của hệ thống cũng góp phần vào việc duy trì một môi trường an toàn.
- *Lựa chọn hàng đầu cho máy chủ:* Với những ưu điểm về tính ổn định, bảo mật, khả năng quản lý và chi phí, CentOS đã trở thành một lựa chọn phổ biến cho việc triển khai các máy chủ trong nhiều lĩnh vực khác nhau, bao gồm máy chủ web, máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ ảo hóa và điện toán đám mây.

1.2.2 Syslog

1.2.2.1 Syslog là gì?

Syslog là một giao thức tiêu chuẩn được sử dụng rộng rãi trong các hệ thống giống Unix, bao gồm cả CentOS, để thu thập và quản lý các thông điệp nhật ký (log messages) từ nhiều nguồn khác nhau trên hệ thống và trong mạng. Mục đích chính của syslog là cung cấp một cơ chế tập trung để ghi lại các sự kiện quan trọng, giúp cho việc giám sát hệ thống, phân tích sự cố, kiểm tra bảo mật và tuân thủ các quy định trở nên dễ dàng và hiệu quả hơn.

1.2.2.2 Các thành phần cơ bản của hệ thống Syslog

- **Syslog Daemon:** Đây là tiến trình nền (daemon) chạy trên hệ thống, chịu trách nhiệm lắng nghe các thông điệp syslog đến từ các ứng dụng cục bộ và có thể từ các hệ thống từ xa qua mạng. Trên CentOS, các syslog daemon phổ biến bao gồm rsyslog (thường là daemon mặc định và được khuyến nghị sử dụng vì tính năng mạnh mẽ và linh hoạt) và syslog-ng (một lựa chọn thay thế với nhiều tính năng nâng cao).
- **Syslog Client:** Đây là các ứng dụng, tiện ích hệ thống, hoặc thậm chí các thiết bị mạng (như router, switch) tạo ra các thông điệp nhật ký khi có các sự kiện xảy ra. Các client này gửi các thông điệp nhật ký đến syslog daemon.
- **Syslog Message (Thông điệp nhật ký):** Mỗi thông điệp syslog chứa một số thông tin quan trọng, bao gồm:
 - **Facility (Cơ sở):** Xác định loại chương trình hoặc hệ thống con đã tạo ra thông điệp. Các facility phổ biến bao gồm kern (kernel - nhân hệ điều hành), user (ứng dụng người dùng), mail (hệ thống thư điện tử), daemon (các tiến trình nền), authpriv (các thông điệp liên quan đến ủy quyền và bảo mật), cron (các tác vụ theo lịch trình), và nhiều facility khác được định nghĩa.
 - **Severity Level (Mức độ nghiêm trọng):** Chỉ mức độ quan trọng hoặc khẩn cấp của sự kiện được ghi lại. Các mức độ nghiêm trọng được sắp xếp theo thứ tự giảm dần về mức độ nghiêm trọng. Ví dụ: emerg (khẩn cấp - hệ thống không sử dụng được), alert (cảnh báo - cần hành động ngay lập tức), crit (nghiêm trọng - lỗi nghiêm trọng), err (lỗi), warn (cảnh báo), notice (thông báo quan trọng), info (thông tin), debug (thông tin gỡ lỗi).
 - **Hostname:** Tên của máy chủ hoặc thiết bị đã gửi thông điệp nhật ký. Điều này đặc biệt hữu ích khi thu thập nhật ký từ nhiều hệ thống trên mạng.
 - **Timestamp:** Thời điểm sự kiện được ghi lại.
 - **Message:** Nội dung chi tiết mô tả sự kiện đã xảy ra.

1.2.3 Quy trình hoạt động của Syslog trên CentOS (với Rsyslog)

Tạo nhật ký: Các ứng dụng và tiến trình trên hệ thống CentOS tạo ra các thông điệp nhật ký khi có các sự kiện xảy ra. Các thông điệp này được định dạng theo tiêu chuẩn syslog, bao gồm facility và severity level.

Gửi đến Syslog Daemon: Các thông điệp nhật ký này được gửi đến syslog daemon (rsyslogd) thông qua một socket đặc biệt, thường là /dev/log (cho các ứng dụng cục bộ) hoặc qua giao thức UDP/TCP port 514 (cho các hệ thống từ xa).

Xử lý theo cấu hình: rsyslogd nhận các thông điệp này và xử lý chúng dựa trên các quy tắc được định nghĩa trong tệp cấu hình chính (/etc/rsyslog.conf) và các tệp cấu hình bổ sung trong thư mục /etc/rsyslog.d/. Các quy tắc này xác định cách các thông điệp nhật ký sẽ được xử lý dựa trên facility, severity level và nguồn gốc.

Lưu trữ và hành động: Dựa trên các quy tắc cấu hình, rsyslogd có thể thực hiện nhiều hành động khác nhau, bao gồm:

- Ghi các thông điệp vào các tệp nhật ký khác nhau trên hệ thống (ví dụ: /var/log/messages cho các thông điệp chung, /var/log/auth.log cho các thông điệp liên quan đến xác thực, /var/log/maillog cho các thông điệp của hệ thống thư điện tử).
- Chuyển tiếp các thông điệp nhật ký đến một máy chủ syslog từ xa để lưu trữ và phân tích tập trung.
- Gửi thông báo qua email hoặc tin nhắn SMS khi có các sự kiện quan trọng xảy ra.
- Ghi nhật ký vào cơ sở dữ liệu.
- Thực hiện các hành động tùy chỉnh thông qua các module mở rộng.

1.2.4 Lợi ích của việc sử dụng Syslog trên CentOS

- *Quản lý nhật ký tập trung:* Cho phép thu thập và quản lý nhật ký từ nhiều nguồn khác nhau (máy chủ, ứng dụng, thiết bị mạng) trên một hệ thống duy nhất, giúp đơn giản hóa việc theo dõi và phân tích.
- *Khả năng phân tích và khắc phục sự cố:* Nhật ký cung cấp thông tin chi tiết về các sự kiện xảy ra trên hệ thống, giúp quản trị viên dễ dàng xác định nguyên nhân của các vấn đề và thực hiện các biện pháp khắc phục.
- *Giám sát bảo mật:* Syslog có thể ghi lại các hoạt động liên quan đến bảo mật, như đăng nhập, đăng xuất, lỗi xác thực, giúp phát hiện các hoạt động đáng ngờ hoặc xâm nhập trái phép.
- *Tuân thủ quy định:* Nhiều tiêu chuẩn và quy định về bảo mật và quản lý hệ thống yêu cầu việc lưu trữ và quản lý nhật ký chi tiết. Syslog cung cấp một giải pháp tiêu chuẩn để đáp ứng các yêu cầu này.
- *Linh hoạt và tùy biến:* Với rsyslog và syslog-ng, người dùng có thể cấu hình một cách linh hoạt các quy tắc xử lý nhật ký, định nghĩa các đích lưu trữ khác nhau và thực hiện các hành động tùy chỉnh.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

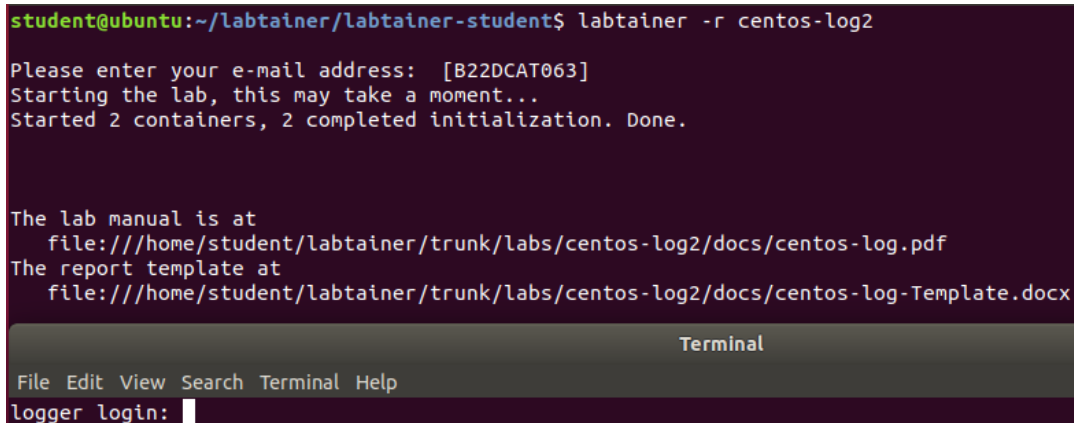
2.1 Chuẩn bị môi trường

- Phần mềm ảo hóa: VMWare Workstation.
- Máy trạm chạy hệ điều hành Linux cài đặt Labtainer.

2.2 Các bước thực hiện

2.2.1 Khởi động lab

labtainer centos-log2



```
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r centos-log2
Please enter your e-mail address: [B22DCAT063]
Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization. Done.

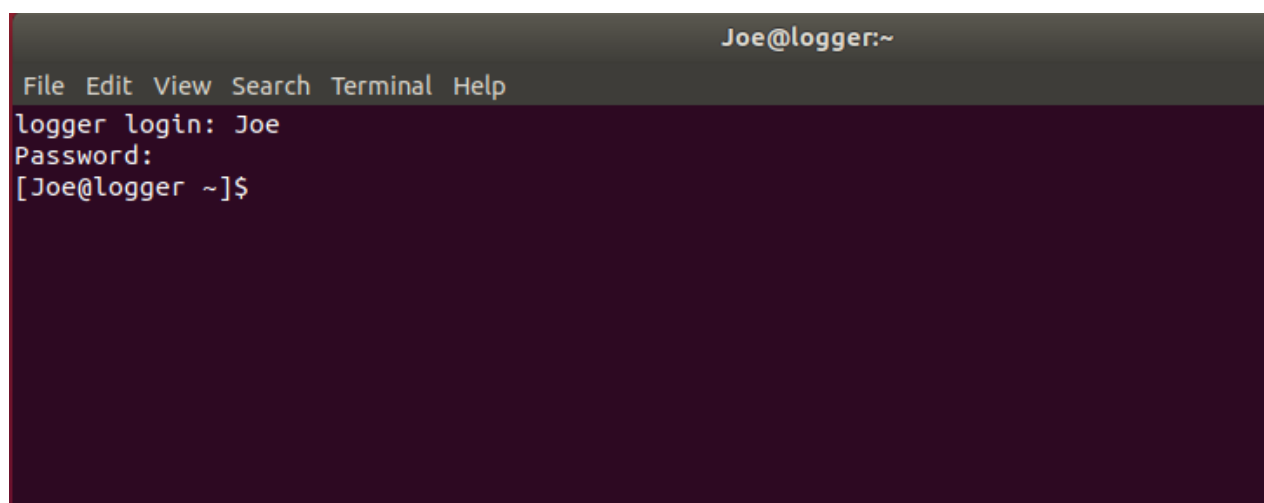
The lab manual is at
  file:///home/student/labtainer/trunk/labs/centos-log2/docs/centos-log.pdf
The report template at
  file:///home/student/labtainer/trunk/labs/centos-log2/docs/centos-log-Template.docx

Terminal
File Edit View Search Terminal Help
logger login: █
```

Hình 1 – Khởi động bài lab

2.2.2 Các nhiệm vụ

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



```
Joe@logger:~
File Edit View Search Terminal Help
logger login: Joe
Password:
[Joe@logger ~]$
```

Hình 2 – Đăng nhập người dùng Joe

2.2.2.1 Nhiệm vụ 1: Khám phá

- Thử lệnh `sudo su` với mật khẩu sai.

Trong terminal, gõ:

su

Khi được yêu cầu nhập mật khẩu root, hãy nhập sai.

Hệ thống sẽ báo lỗi vì mật khẩu sai.

```
Joe@logger:~  
File Edit View Search Terminal Help  
[Joe@logger ~]$ su  
Password:  
su: Authentication failure  
[Joe@logger ~]$
```

Hình 3 – su với mật khẩu sai

- Nhập lại lệnh *su*, nhưng lần này nhập đúng mật khẩu cho root. Nếu làm đúng, dấu nhắc sẽ kết thúc bằng ký tự '#'.

```
Joe@logger:/home/Joe  
File Edit View Search Terminal Help  
[Joe@logger ~]$ su  
Password:  
[root@logger Joe]#
```

Hình 4 – Nhập đúng mật khẩu root

- Khám phá thư mục log.

Chuyển đến thư mục */var/log* và liệt kê nội dung thư mục:

cd /var/log

ls

```
Joe@logger:/var/log  
File Edit View Search Terminal Help  
[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]#
```

Hình 5 – Xem thư mục /var/log

Các thư mục sẽ có màu xanh.

Chú ý các tệp có đuôi như .old (bản sao nhật ký cũ) hoặc -yyyymmdd (nhật ký được xoay vòng theo ngày).

Xem quyền truy cập của tệp messages:

`ls -l messages`

```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# ls -l messages
-rw----- 1 root root 177688 Apr 24 01:42 messages
[root@logger log]#
```

Hình 6 – Quyền của tệp messages

- 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. Thử đăng nhập Joe với mật khẩu sai.

```
Terminal
File Edit View Search Terminal Help
logger login: Joe
Password:

Login incorrect
logger login: █
```

Hình 7 – Đăng nhập Joe thất bại

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). (Dòng bôi trắng).

```
Joe@logger:~
File Edit View Search Terminal Help
Apr 24 01:40:17 logger sshd[68]: Server listening on 0.0.0.0 port 22.
Apr 24 01:40:17 logger sshd[68]: Server listening on :: port 22.
Apr 24 01:40:19 logger sudo: root : TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/tar -x --keep-directory-symlink -f /var/tmp/labsys.tar -C /
Apr 24 01:40:23 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown -R Joe:Joe /home/Joe/.local
Apr 24 01:40:23 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /
Apr 24 01:40:23 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /etc/
Apr 24 01:40:23 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /etc/securetty
Apr 24 01:40:24 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /etc/login.defs
Apr 24 01:40:24 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /sbin/
Apr 24 01:40:24 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /sbin/login
Apr 24 01:40:24 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /sbin/faux_init
Apr 24 01:40:24 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/rm -f /run/nologin
Apr 24 01:40:25 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/ParameterParser.py Joe 7448016a62f48da25b3408f8a9a16d6e centos-log2.logger.student /home/Joe/.local/config/parameter.config
Apr 24 01:40:25 logger su: pam_unix(su:session): session opened for user Joe by (uid=0)
Apr 24 01:40:25 logger sudo: Joe : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown syslog:adm /dev/xconsole
Apr 24 01:40:25 logger su: pam_unix(su:session): session closed for user Joe
Apr 24 01:40:25 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/sed -i /^\. Don't log private.*a :msg, !contains, "apparmor" /etc/rsyslog.conf
Apr 24 01:40:25 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/hookBash.sh /home/Joe
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/yum-source.sh
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/dbus-uuidgen
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/touch /sbin/consoletype
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+rw /sbin/consoletype
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/mkdir -p /var/labtainer/did_param
Apr 24 01:40:46 logger login[254]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 24 01:41:48 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=root
Apr 24 01:42:11 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)
Apr 24 01:43:15 logger su: pam_unix(su:session): session closed for user root
Apr 24 01:43:25 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=Joe
Apr 24 01:44:24 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/less /var/log/secure
Apr 24 01:45:13 logger login[254]: pam_unix(login:session): session closed for user Joe
Apr 24 01:45:20 logger login[733]: pam_unix(login:auth): check pass; user unknown
Apr 24 01:45:20 logger login[733]: pam_unix(login:auth): authentication failure; logname=Joe uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 24 01:45:22 logger login[733]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
```

Hình 8 – Mở tệp secure và tìm kiếm trạng thái failed

- Tìm lỗi nhập sai tên người dùng

Đăng nhập với tên người dùng là “password”.

```

Joe@logger:~
File Edit View Search Terminal Help
[Joe@logger ~]$ exit
logout
logger login: password
Password:

Login incorrect
logger login:

```

Hình 9 – Nhập “password” làm tên người dùng

Với tệp nhật ký secure vẫn mở, tìm dòng ghi chú cho biết sinh viên đã nhập "password" làm tên người dùng. (Dòng bôi trắng).

```

Apr 24 01:40:25 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/hookBash.sh /home/Joe
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/yum-source.sh
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/dbus-uuidgen
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/touch /sbin/consoletype
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+rw /sbin/consoletype
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/mkdir -p /var/labtainer/did_param
Apr 24 01:40:46 logger login[254]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 24 01:41:48 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=root
Apr 24 01:42:11 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)
Apr 24 01:43:15 logger su: pam_unix(su:session): session closed for user root
Apr 24 01:43:25 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=Joe
Apr 24 01:44:24 logger sudo: Joe: TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/less /var/log/secure
Apr 24 01:45:13 logger login[254]: pam_unix(login:session): session closed for user Joe
Apr 24 01:45:20 logger login[733]: pam_unix(login:auth): check pass; user unknown
Apr 24 01:45:20 logger login[733]: pam_unix(login:auth): authentication failure; logname=Joe uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 24 01:45:22 logger login[733]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure

```

Hình 10 – Xem tệp nhật ký Secure

- 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.

```

Joe@logger:~
File Edit View Search Terminal Help
Apr 24 01:40:17 logger sshd[68]: Server listening on 0.0.0.0 port 22.
Apr 24 01:40:17 logger sshd[68]: Server listening on :: port 22.
Apr 24 01:40:19 logger sudo: root: TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/tar -x --keep-directory-symlink -f /var/tmp/labsys.tar -C /
Apr 24 01:40:23 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown -R Joe:Joe /home/Joe/.local
Apr 24 01:40:23 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /
Apr 24 01:40:23 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /etc/
Apr 24 01:40:23 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /etc/securetty
Apr 24 01:40:24 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /etc/login.defs
Apr 24 01:40:24 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /sbin/
Apr 24 01:40:24 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /sbin/login
Apr 24 01:40:24 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown root:root /sbin/faux_init
Apr 24 01:40:24 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/rm -f /run/nologin
Apr 24 01:40:25 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/ParameterParser.py Joe 7448016a62f48da25b3408f8a9a16d6e cento
s-log2.logger.student /home/Joe/.local/config/parameter.config
Apr 24 01:40:25 logger su: pam_unix(su:session): session opened for user Joe by (uid=0)
Apr 24 01:40:25 logger sudo: Joe: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chown syslog:adm /dev/xconsole
Apr 24 01:40:25 logger su: pam_unix(su:session): session closed for user Joe
Apr 24 01:40:25 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/sed -i /a . Don't log private.* /a :msg, !contains, "apparmor" /etc/rsyslog
.conf
Apr 24 01:40:25 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/hookBash.sh /home/Joe
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/yum-source.sh
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/dbus-uuidgen
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/touch /sbin/consoletype
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+rw /sbin/consoletype
Apr 24 01:40:26 logger sudo: root: TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/mkdir -p /var/labtainer/did_param
Apr 24 01:40:46 logger login[254]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 24 01:41:48 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=root
Apr 24 01:42:11 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)
Apr 24 01:43:15 logger su: pam_unix(su:session): session closed for user root
Apr 24 01:43:25 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=Joe
Apr 24 01:44:24 logger sudo: Joe: TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/less /var/log/secure
Apr 24 01:45:13 logger login[254]: pam_unix(login:session): session closed for user Joe

```

Hình 11 – Tìm các mục liên quan đến hành động root


```
Joe@logger:/var/log
File Edit View Search Terminal Help
OPTIONS
-f file
    Tells last to use a specific file instead of /var/log/wtmp.

-num
    This is a count telling last how many lines to show.

-n num
    The same.

-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".

-f file
    Specifies a file to search other than /var/log/wtmp.

-R
    Suppresses the display of the hostname field.

-a
    Display the hostname in the last column. Useful in combination with the next flag.

-d
    For non-local logins, Linux stores not only the host name of the remote host but
    its IP number as well. This option translates the IP number back into a hostname.

-F
    Print full login and logout times and dates.

-i
    This option is like -d in that it displays the IP number of the remote host, but it
    displays the IP number in numbers-and-dots notation.

-o
    Read an old-type wtmp file (written by linux-libc5 applications).

-w
    Display full user and domain names in the output.

-x
    Display the system shutdown entries and run level changes.
```

Hình 13 – Đọc OPTIONS của lệnh last

2.2.2.2 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 nano) để mở tệp /etc/rsyslog.conf

```
Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf

# 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

# 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
```

Hình 14 – Mở tệp /etc/rsyslog.conf

- Bật tính năng MARK

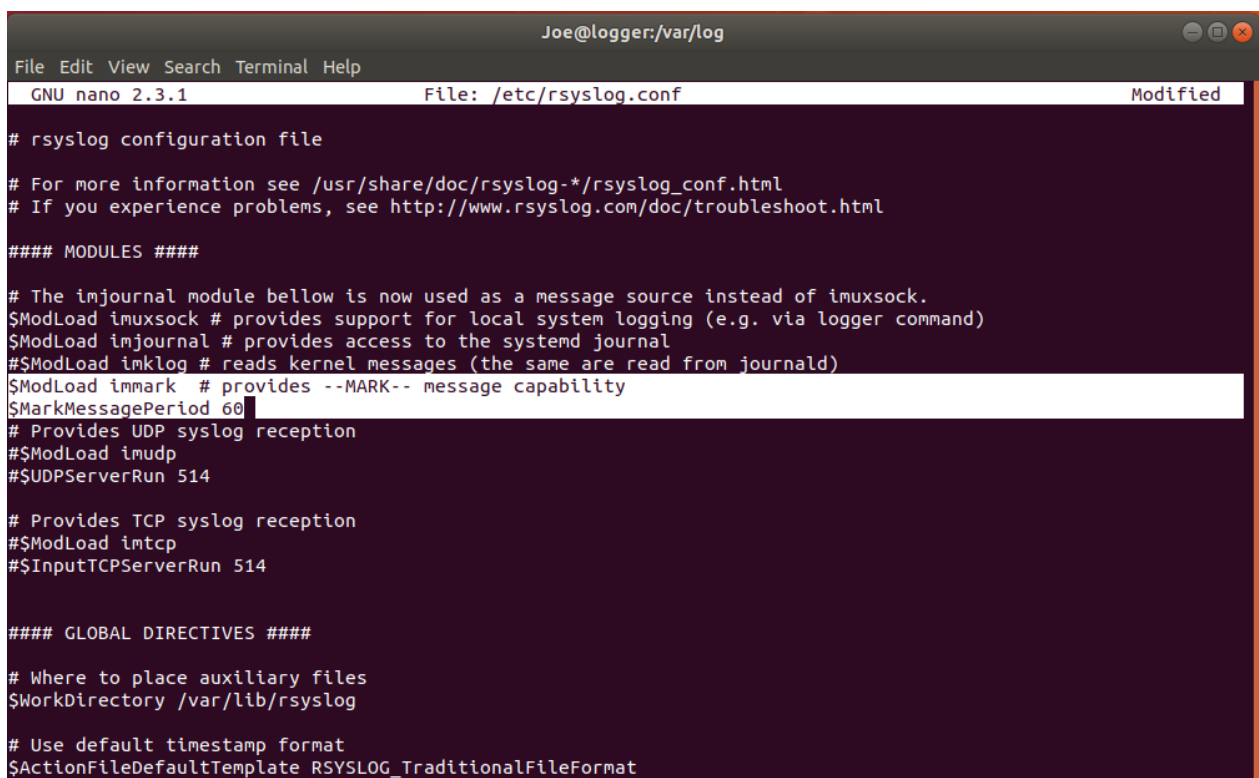
Mặc định, việc chèn thời gian vào một tần suất đã chỉ định được vô hiệu hóa.

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).



```

Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf Modified

# 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
  
```

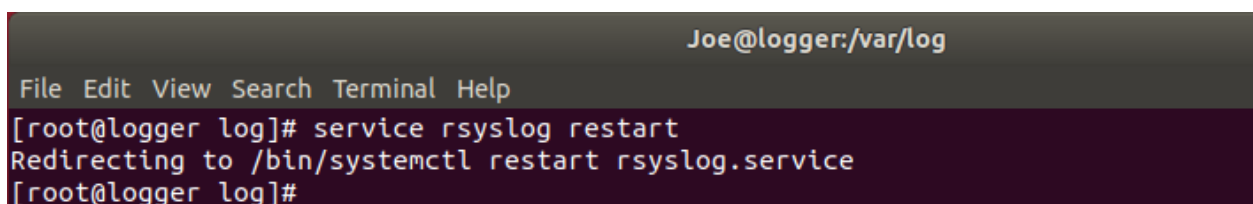
Hình 15 – Thiết lập tần suất của timestamps

Lưu thay đổi và thoát khỏi trình soạn thảo.

- 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



```

Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# service rsyslog restart
Redirecting to /bin/systemctl restart rsyslog.service
[root@logger log]#
  
```

Hình 16 – Lưu thay đổi và khởi động lại rsyslog

- Xem thay đổi này đã được thực hiện trong các nhật ký bằng cách sử dụng lệnh tail như sau.

tail -f /var/log/messages

Lệnh tail hiển thị một số dòng cuối cùng của tệp (khác với lệnh head, hiển thị một số dòng đầu tiên của tệp). Tùy chọn "-f" cho biết để chờ đợi "mãi mãi" và hiển thị thêm dòng khi chúng được thêm vào cuối tệp. Chờ 60 giây để thấy bản ghi MARK xuất hiện. Sau đó nhấn Ctrl-C để thoát khỏi tail.

```

Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# tail -f /var/log/messages
Apr 24 02:24:26 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="157" x-info="http://www.rsyslog.com"] exiting on signal 15.
Apr 24 02:24:26 logger systemd: Starting System Logging Service...
Apr 24 02:24:26 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1078" x-info="http://www.rsyslog.com"] start
Apr 24 02:24:26 logger systemd: Started System Logging Service.
Apr 24 02:25:26 logger rsyslogd: -- MARK --
Apr 24 02:25:27 logger systemd: Stopping System Logging Service...
Apr 24 02:25:27 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1078" x-info="http://www.rsyslog.com"] exiting on signal 15.
Apr 24 02:25:27 logger systemd: Starting System Logging Service...
Apr 24 02:25:27 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1137" x-info="http://www.rsyslog.com"] start
Apr 24 02:25:27 logger systemd: Started System Logging Service.
Apr 24 02:26:28 logger rsyslogd: -- MARK --

```

Hình 17 – Xem thay đổi

2.2.2.3 Nhiệm vụ 3: Cấu hình lại và kiểm tra rsyslog

Trong phần này, sinh viên sẽ làm quen với tiện ích logger để tạo thủ công các mục syslog. Một quản trị viên hệ thống có thể sử dụng lệnh này để ghi lại các thay đổi mà họ thực hiện trên hệ thống, và nó có thể được sử dụng để kiểm tra các thay đổi trong cấu hình syslog. Sinh viên sẽ thực hiện một số thay đổi trong các quy tắc syslog, sau đó sử dụng logger để kiểm tra các thay đổi đó.

- Đọc phần DESCRIPTION trong trang man của tiện ích logger:

man logger

```

Joe@logger:/var/log
File Edit View Search Terminal Help
DESCRIPTION
  logger makes entries in the system log. It provides a shell command interface to the sys-
  log(3) system log module.

```

Hình 18 – Đọc phần DESCRIPTION

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

logger -p info "Hello World"

Khi không chỉ định cơ sở dữ liệu, như trong trường hợp của lệnh trên, cơ sở dữ liệu "user" được sử dụng mặc định.

```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# logger -p info "Hello World"
[root@logger log]#
```

Hình 19 – Tạo bản ghi “Hello World” với logger

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

```
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf
# 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)
$ModLoad imjournal # provides access to the system journal
#$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
```

Hình 20 – Mở lại tệp cấu hình rsyslog

Xem quy tắc chỉ định nơi lưu bản ghi từ bước 2.

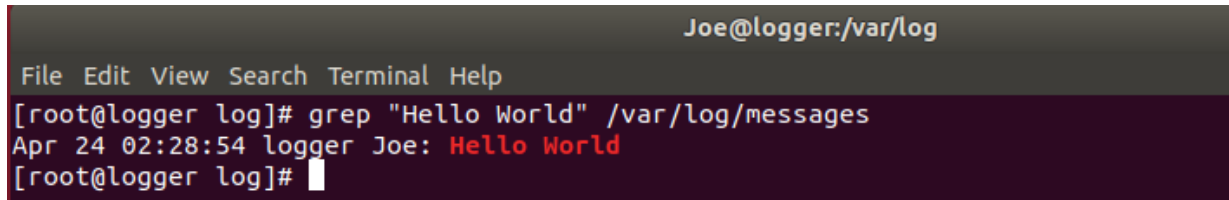
```
Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on
# File to store the position in the journal
$IMJournalStateFile imjournal.state
##### 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
```

Hình 21 – Xem quy tắc chỉ định nơi lưu bản ghi

- Thoát khỏi trình soạn thảo.
- 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.

Kiểm tra xem bản ghi "Hello World" có trong /var/log/messages không:

grep "Hello World" /var/log/messages



```

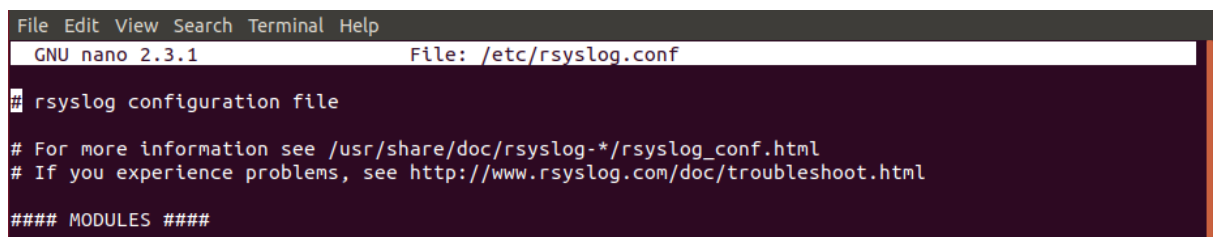
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# grep "Hello World" /var/log/messages
Apr 24 02:28:54 logger Joe: Hello World
[root@logger log]#

```

Hình 22 – Xác minh bản ghi

- 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.



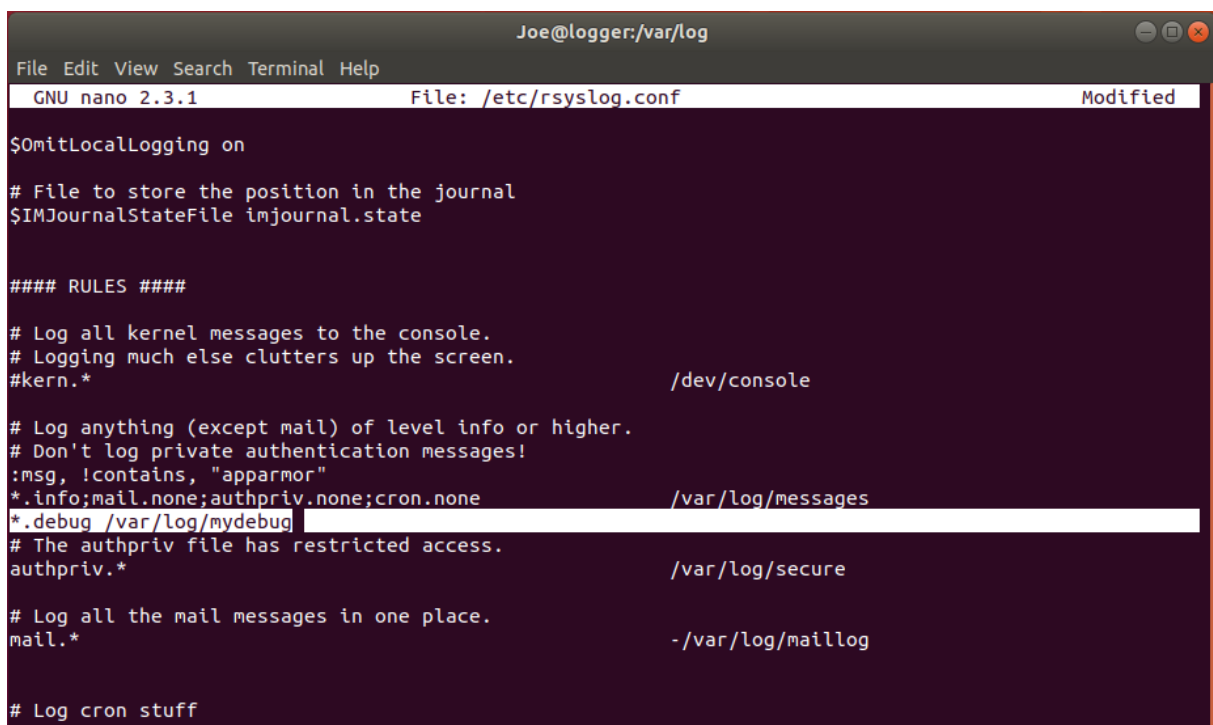
```

File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf
# 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 ####

```

Hình 23 – Mở lại tệp cấu hình rsyslog

Trong phần #### RULES ####, thêm dòng:



```

Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf Modified
$OmitLocalLogging on
# File to store the position in the journal
$IMJournalStateFile imjournal.state

#### 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
*.debug /var/log/mydebug
# 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

```

Hình 24 – Thêm quy tắc cho rsyslog

- Lưu các thay đổi của vào tệp cấu hình và sau đó thoát khỏi trình soạn thảo.
- Khởi động lại rsyslog (để quy tắc mới có hiệu lực):

systemctl restart rsyslog

```

Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# systemctl restart rsyslog
[root@logger log]#

```

Hình 25 – Khởi động lại rsyslog

Nếu thay đổi trong rsyslog.conf có lỗi cú pháp, nó sẽ được báo cáo ở cuối tệp /var/log/messages.

- Sử dụng logger để kiểm tra quy tắc mà sinh viên đã thêm vào rsyslog.conf ở bước #6 ở trên.

Thêm bản ghi:

logger -p debug "Test debug message"

```

Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# logger -p debug "Test debug message"
[root@logger log]#

```

Hình 26 – Tạo bản ghi debug

Kiểm tra tệp /var/log/mydebug:

cat /var/log/mydebug

```

Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# cat /var/log/mydebug
Apr 24 02:32:47 logger systemd: Stopping System Logging Service...
Apr 24 02:32:47 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1137" x-info="http://www.rsyslog.com"] exiting on signal 15.
Apr 24 02:32:47 logger systemd: Starting System Logging Service...
Apr 24 02:32:47 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1435" x-info="http://www.rsyslog.com"] start
Apr 24 02:32:47 logger systemd: Started System Logging Service.
Apr 24 02:33:04 logger Joe: "Test debug message"
[root@logger log]#

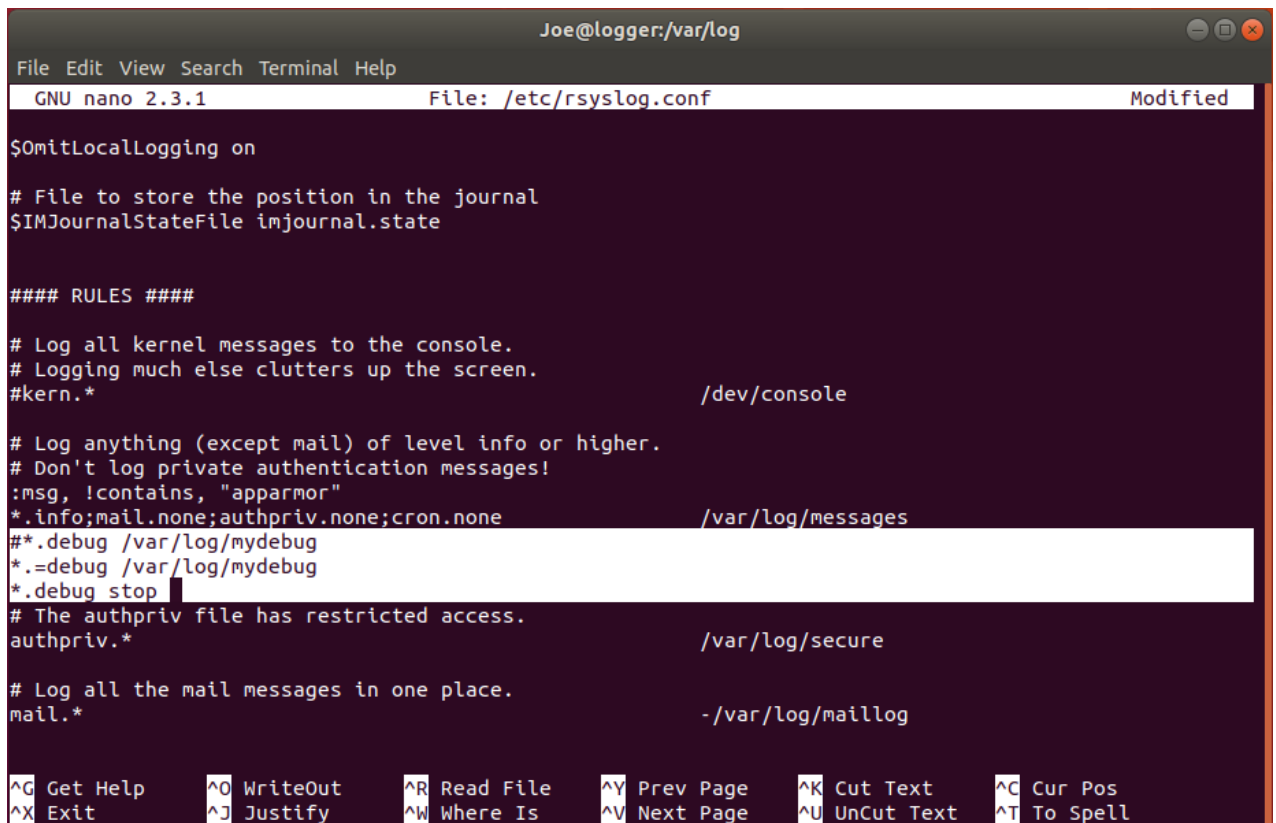
```

Hình 27 – Kiểm tra tệp /var/log/mydebug

Sau đó sửa lại và thêm quy tắc cho tệp rsyslog, thêm # ở đầu dòng *.debug /var/log/mydebug và thêm 2 dòng sau:

**.=debug /var/log/mydebug*

**.debug stop*



```
Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf Modified

$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

#### RULES ####

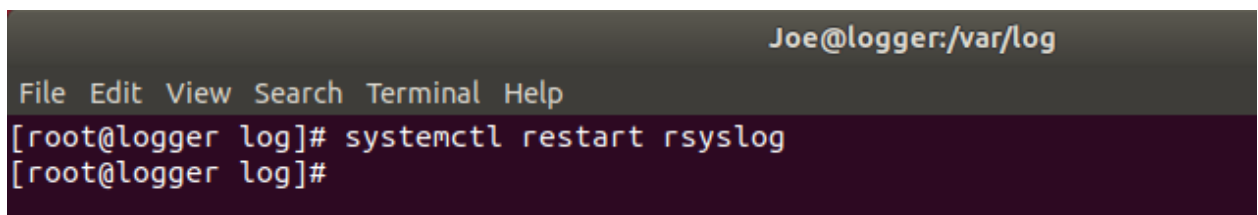
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# 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
#*.debug /var/log/mydebug
#*=debug /var/log/mydebug
*.debug stop
# The authpriv file has restricted access.
authpriv.* /var/log/secure

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

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Hình 28 – Sửa lại file rsyslog



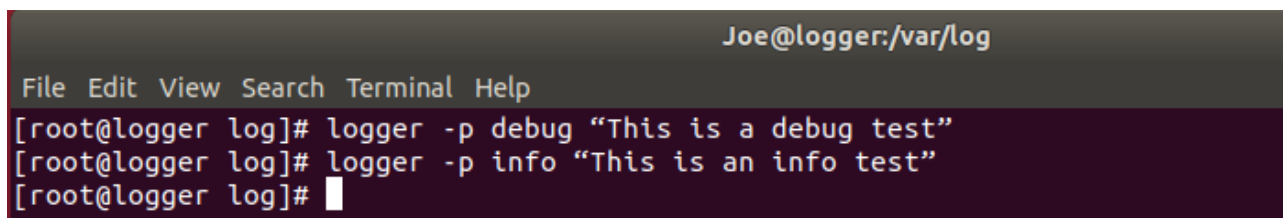
```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# systemctl restart rsyslog
[root@logger log]#
```

Hình 29 – Khởi động lại rsyslog

Thêm 2 bản ghi debug và info

logger -p debug "This is a debug test"

logger -p info "This is an info test"



```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# logger -p debug "This is a debug test"
[root@logger log]# logger -p info "This is an info test"
[root@logger log]#
```

Hình 30 – Thêm hai bản ghi debug và info

Kiểm tra file /var/log/mydebug: Ta chỉ thấy bản ghi của debug

```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# cat /var/log/mydebug
Apr 24 02:32:47 logger systemd: Stopping System Logging Service...
Apr 24 02:32:47 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1137" x-info="http://www.rsyslog.com"] exiting on signal 15.
Apr 24 02:32:47 logger systemd: Starting System Logging Service...
Apr 24 02:32:47 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1435" x-info="http://www.rsyslog.com"] start
Apr 24 02:32:47 logger systemd: Started System Logging Service.
Apr 24 02:33:04 logger Joe: "Test debug message"
Apr 24 02:33:47 logger rsyslogd: -- MARK --
Apr 24 02:34:47 logger rsyslogd: -- MARK --
Apr 24 02:35:09 logger Joe: "This is a debug test"
[root@logger log]#
```

Hình 31 – Kiểm tra file /var/log/mydebug

- 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.

```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# ll /bin/logger
-rwxr-xr-x 1 root root 29224 Dec 1 2017 /bin/logger
[root@logger log]# chmod 750 /bin/logger
[root@logger log]# ll /bin/logger
-rwxr-x-- 1 root root 29224 Dec 1 2017 /bin/logger
[root@logger log]#
```

Hình 32 – Kiểm tra và thay đổi quyền của logger

2.2.2.4 Nhiệm vụ 4: Ghi log tập trung

Giả sử sinh viên có một số hệ thống Linux cần quản lý. Thay vì cấu hình và xem xét việc ghi log trên từng hệ thống, sinh viên có thể xác định một hệ thống ghi log tập trung và sau đó chuyển tiếp các thông báo log từ mỗi hệ thống đến hệ thống ghi log tập trung đó. Ở phần này, sinh viên sẽ cấu hình hệ thống "logger" hiện có để chấp nhận các thông báo log từ các máy tính từ xa, và sinh viên sẽ cấu hình một máy tính trạm để chuyển tiếp các log của nó đến hệ thống ghi log.

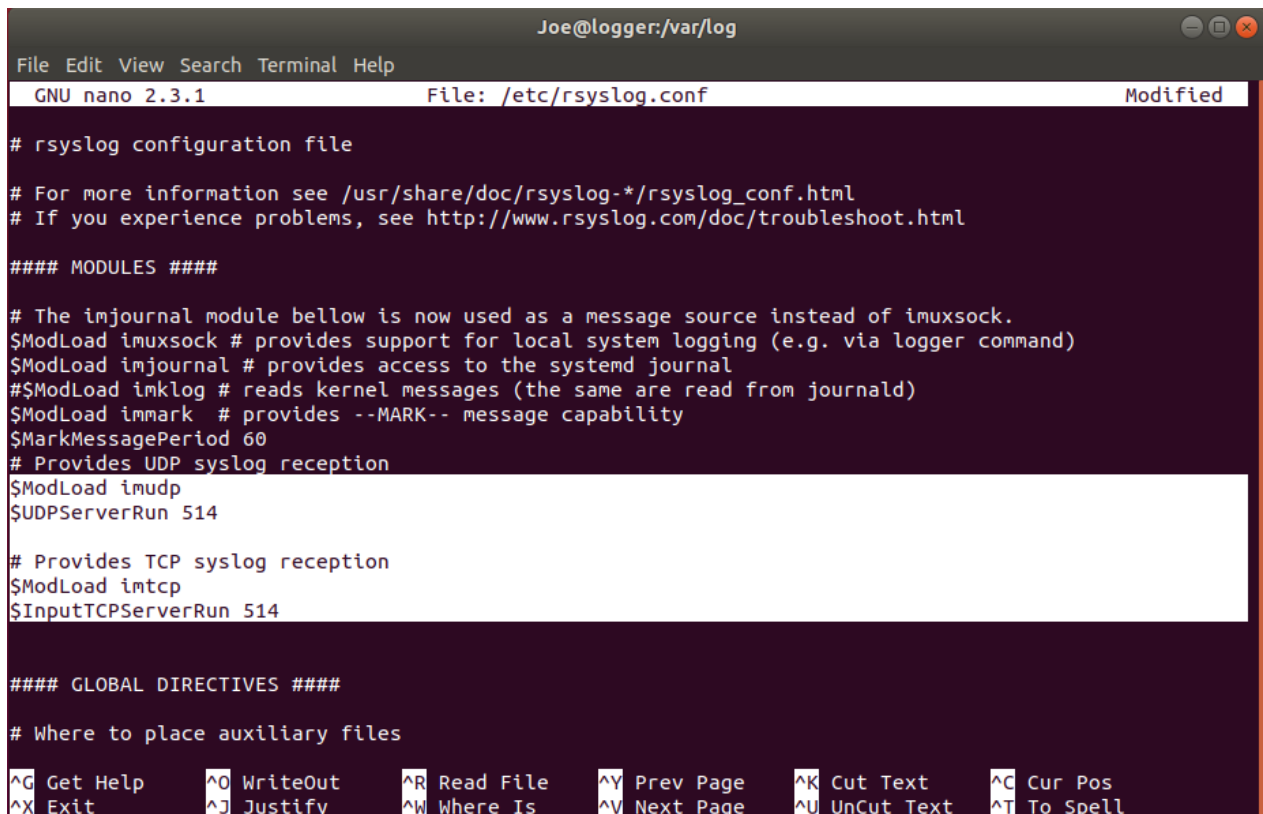
- Mở lại tệp cấu hình /etc/rsyslog.conf trên máy tính ghi log.
- Tìm các mục sau trong tệp cấu hình và bỏ chú thích chúng (xóa dấu "#") để cho phép chấp nhận thông báo syslog trên cổng 514 qua TCP hoặc UDP:

\$ModLoad imudp

\$UDPServerRun 514

\$ModLoad imtcp

\$InputTCPServerRun 514



```
Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf Modified

# 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

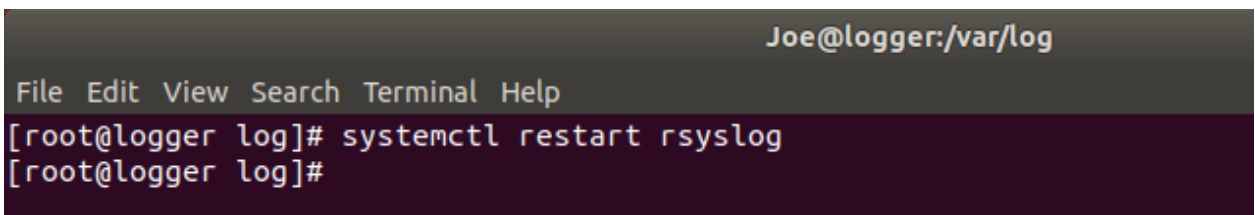
#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Hình 33 – Sửa tệp rsyslog

Lưu và khởi động lại dịch vụ rsyslog.



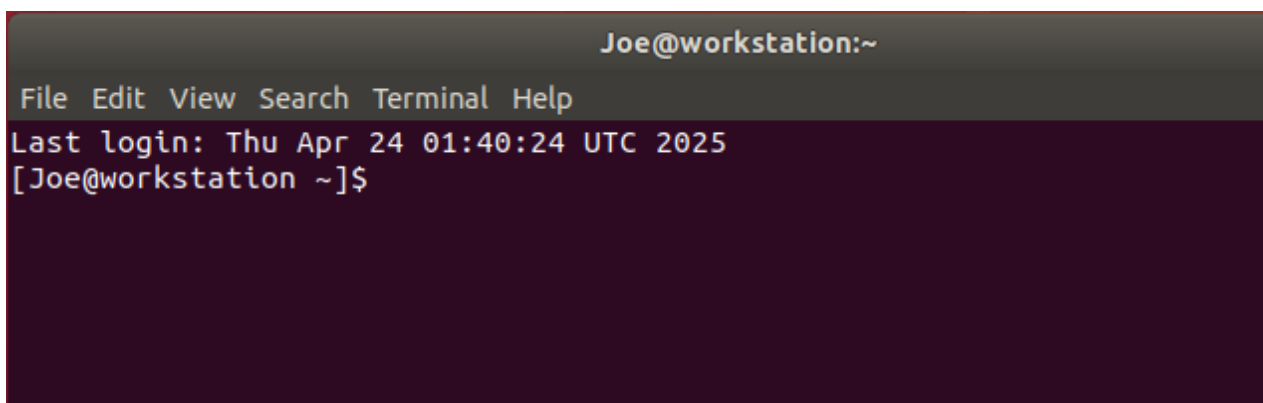
```
Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# systemctl restart rsyslog
[root@logger log]#
```

Hình 34 – Khởi động lại dịch vụ rsyslog

- Kết nối với máy trạm.

Trên terminal chính của hệ thống lab sử dụng lệnh:

moreterm.py centos-log2 workstation



```
Joe@workstation:~
File Edit View Search Terminal Help
Last login: Thu Apr 24 01:40:24 UTC 2025
[Joe@workstation ~]$
```

Hình 35 – Khởi động terminal cho máy trạm

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.

```
Joe@logger:~  
File Edit View Search Terminal Help  
[Joe@logger ~]$ 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 11814 (11.5 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  
  
[Joe@logger ~]$
```

Hình 36 – Kiểm tra IP máy ghi log

```
Joe@workstation:~  
File Edit View Search Terminal Help  
Last login: Thu Apr 24 01:40:24 UTC 2025  
[Joe@workstation ~]$ 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 76 bytes 12080 (11.7 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 ~]$
```

Hình 37 – Kiểm tra IP máy trạm

Ghi lại IP của máy ghi log (172.25.0.2).

- Sử dụng "sudo su" để nâng cao đặc quyền trên máy tính trạm.

sudo su

```
root@workstation:/home/Joe
File Edit View Search Terminal Help
[Joe@workstation ~]$ sudo su
[root@workstation Joe]#
```

Hình 38 – Nâng quyền máy trạm

- Mở tệp /etc/rsyslog.conf trên máy tính trạm và tìm phần "RULES". Ở cuối phần đó, thêm dòng sau để chuyển hướng tất cả các thông báo đến máy tính ghi log:

`*.* @172.25.0.2`

```
root@workstation:/home/Joe
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf Modified

# 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)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList # run asynchronously
#$ActionResumeRetryCount -1 # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*. * @@remote-host:514
# ### end of the forwarding rule ###
*. * @172.25.0.2
```

Hình 39 – Sửa lại file rsyslog

- Bây giờ hãy khởi động lại rsyslog trên máy tính trạm và quan sát các thông báo log trên máy tính ghi log.

```
root@workstation:/home/Joe
File Edit View Search Terminal Help
[root@workstation Joe]# systemctl restart rsyslog
[root@workstation Joe]#
```

Hình 40 – Khởi động lại rsyslog

Trên máy ghi log, xem log:

`tail -f /var/log/*`


```
Joe@logger:/home/Joe
File Edit View Search Terminal Help
id=0 tty=/dev/pts/1 ruser= rhost=
Apr 24 01:45:22 logger login[733]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
Apr 24 01:45:36 logger login[733]: pam_unix(login:session): session opened for user Joe by Joe(uid=0)
Apr 24 01:45:47 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/less /var/log/secure
Apr 24 01:47:26 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/less /var/log/secure
Apr 24 01:49:38 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)

==> /var/log/spooler <==

==> /var/log/tallylog <==

==> /var/log/wtmp <==
Gpts/1ts/1root♦♦ hW♦♦ Gpts/1ts/1root♦♦ h♦♦ Spts/1ts/1root♦♦ hSpts/1ts/1root♦♦ hv
==> /var/log/yum.log <==
Jan 24 18:43:26 Installed: cairo-1.15.12-4.el7.x86_64
Jan 24 18:43:26 Installed: libXft-2.3.2-2.el7.x86_64
Jan 24 18:43:26 Installed: pango-1.42.4-4.el7_7.x86_64
Jan 24 18:43:27 Installed: avahi-libs-0.6.31-19.el7.x86_64
Jan 24 18:43:27 Installed: 1:cups-libs-1.6.3-40.el7.x86_64
Jan 24 18:43:28 Installed: hicolor-icon-theme-0.12-7.el7.noarch
Jan 24 18:43:28 Installed: gtk2-2.24.31-1.el7.x86_64
Jan 24 18:43:28 Installed: 1:emacs-filesystem-24.3-22.el7.noarch
Jan 24 18:43:28 Installed: desktop-file-utils-0.23-2.el7.x86_64
Jan 24 18:43:29 Installed: leafpad-0.8.18.1-1.el6.x86_64
```

Hình 41 – Xem log

- 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.

Tạo bản ghi: *logger "Test from workstation"*

Thay đổi quyền: *su*

```
root@workstation:/home/Joe
File Edit View Search Terminal Help
[root@workstation Joe]# logger "Test from workstation"
[root@workstation Joe]# su
[root@workstation Joe]#
```

Hình 42 – Tạo bản ghi và thay đổi quyền

Quan sát log trên máy ghi log.

```

Joe@logger:/home/Joe
File Edit View Search Terminal Help
/var/log/secure
Apr 24 01:49:38 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)

==> /var/log/spooler <==

==> /var/log/tallylog <==

==> /var/log/wtmp <==
Gpts/1ts/1root♦♦          h♦♦          Spts/1ts/1root♦♦          hSpts/1ts/1root♦♦          hv

==> /var/log/yum.log <==
Jan 24 18:43:26 Installed: cairo-1.15.12-4.el7.x86_64
Jan 24 18:43:26 Installed: libXft-2.3.2-2.el7.x86_64
Jan 24 18:43:26 Installed: pango-1.42.4-4.el7_7.x86_64
Jan 24 18:43:27 Installed: avahi-libs-0.6.31-19.el7.x86_64
Jan 24 18:43:27 Installed: 1:cups-libs-1.6.3-40.el7.x86_64
Jan 24 18:43:28 Installed: hicolor-icon-theme-0.12-7.el7.noarch
Jan 24 18:43:28 Installed: gtk2-2.24.31-1.el7.x86_64
Jan 24 18:43:28 Installed: 1:emacs-filesystem-24.3-22.el7.noarch
Jan 24 18:43:28 Installed: desktop-file-utils-0.23-2.el7.x86_64
Jan 24 18:43:29 Installed: leafpad-0.8.18.1-1.el6.x86_64

==> /var/log/messages <==
Apr 24 02:45:02 logger rsyslogd: -- MARK --
Apr 24 02:46:02 logger rsyslogd: -- MARK --
Apr 24 02:46:52 workstation logger: Test from workstation
Apr 24 02:46:53 workstation su: (to root) root on pts/1
Apr 24 02:47:02 logger rsyslogd: -- MARK --

```

Hình 43 – Xem log

2.2.2.5 Nhiệm vụ 5: Các câu hỏi khác

1. Đối với tệp log có tên /var/log/messages, quyền nào được cấp cho người dùng thông thường?

Người dùng thông thường không có quyền gì với tệp /var/log/messages

```

Joe@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# ls -l messages
-rw----- 1 root root 177688 Apr 24 01:42 messages
[root@logger log]#

```

Hình 44 – Người dùng thông thường không có quyền

2. Trong /var/log/secure, từ ngữ nào được sử dụng để chỉ một nỗ lực đăng nhập không thành công?

```

Apr 24 01:40:25 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/home/Joe/.local/bin/hookBash.sh /home/Joe
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/yum-source.sh
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/dbus-uuidgen
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/touch /sbin/consoletype
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/chmod a+rw /sbin/consoletype
Apr 24 01:40:26 logger sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/mkdir -p /var/labtainer/did_param
Apr 24 01:40:46 logger login[254]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 24 01:41:48 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=root
Apr 24 01:42:11 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)
Apr 24 01:43:15 logger su: pam_unix(su:session): session closed for user root
Apr 24 01:43:25 logger su: pam_unix(su:auth): authentication failure; logname=Joe uid=1000 euid=0 tty=pts/1 ruser=Joe rhost= user=Joe
Apr 24 01:44:24 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/less /var/log/secure
Apr 24 01:45:13 logger login[254]: pam_unix(login:session): session closed for user Joe
Apr 24 01:45:20 logger login[733]: pam_unix(login:auth): check pass; user unknown
Apr 24 01:45:20 logger login[733]: pam_unix(login:auth): authentication failure; logname=Joe uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 24 01:45:22 logger login[733]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure

```

Hình 45 – Từ chỉ một nỗ lực không thành công

3. Liên quan đến Mục #2 ở trên, hãy mô tả một tình huống thực tế mà thông tin này có thể hữu ích.

- Mô tả: Bạn là quản trị viên hệ thống của một máy chủ CentOS dùng trong nội bộ công ty. Một ngày, bạn nhận được phản ánh rằng tài khoản "ketoan" không truy cập được hệ thống để nhập dữ liệu vào phần mềm kế toán.
- Bước kiểm tra:
 - Bạn kiểm tra log /var/log/secure với lệnh:

```
grep " authentication failure " /var/log/secure
```
 - Và thấy các dòng sau:

```
Apr 21 09:12:34 centos-server login: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=tty1 ruser= rhost= user=ketoan
```



```
Apr 21 09:12:37 centos-server login: FAILED LOGIN 1 FROM tty1 FOR 'ketoan', Authentication failure
```



```
Apr 21 09:12:39 centos-server login: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=tty1 ruser= rhost= user=ketoan
```
- Phân tích:
 - Người dùng "ketoan" đã nhập sai mật khẩu nhiều lần.
 - Lỗi do "authentication failure" chứ không phải hệ thống lỗi.
 - Có thể người dùng quên mật khẩu hoặc có người cố tình thử mật khẩu của người khác.
- Hành động khắc phục:
 - Xác nhận lại với người dùng "ketoan" xem có quên mật khẩu không.
 - Đặt lại mật khẩu mới nếu cần: `sudo passwd ketoan`
 - Gửi cảnh báo bảo mật nội bộ nếu nghi ngờ có ai đó đang cố đăng nhập trái phép bằng tài khoản người khác.
 - Nếu lặp lại nhiều lần, nên bật tính năng khóa tài khoản tạm thời sau nhiều lần sai bằng PAM hoặc Fail2Ban.

4. Trong /var/log/secure, từ ngữ nào được sử dụng để chỉ rằng sinh viên đã tăng đặc quyền bằng lệnh su?

- “session opened for user root by ” từ ngữ nào được sử dụng để chỉ rằng sinh viên đã tăng đặc quyền bằng lệnh su

```
Joe@logger:/home/Joe
File Edit View Search Terminal Help
[root@logger Joe]# grep "session opened for user root by" /var/log/secure
Apr 24 01:42:11 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)
Apr 24 01:49:38 logger su: pam_unix(su:session): session opened for user root by Joe(uid=1000)
[root@logger Joe]#
```

Hình 46 – Sinh viên tăng đặc quyền bằng su

5. Hãy mô tả chức năng được cung cấp bởi tùy chọn -t của lệnh last.

- Tùy chọn -t YYYYMMDDHHMMSS trong lệnh last được dùng để hiển thị trạng thái đăng nhập tại một thời điểm cụ thể.

```
Joe@logger:/var/log
File Edit View Search Terminal Help
OPTIONS
-f file      Tells last to use a specific file instead of /var/log/wtmp.
-num        This is a count telling last how many lines to show.
-n num      The same.
-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".
-f file      Specifies a file to search other than /var/log/wtmp.
-R          Suppresses the display of the hostname field.
-a          Display the hostname in the last column. Useful in combination with the next flag.
-d          For non-local logins, Linux stores not only the host name of the remote host but
            its IP number as well. This option translates the IP number back into a hostname.
-F          Print full login and logout times and dates.
-i          This option is like -d in that it displays the IP number of the remote host, but it
            displays the IP number in numbers-and-dots notation.
-o          Read an old-type wtmp file (written by linux-libc5 applications).
-w          Display full user and domain names in the output.
-x          Display the system shutdown entries and run level changes.
```

Hình 47 – OPTIONS của lệnh last

6. Quy tắc nào trong tệp cấu hình syslog sẽ phù hợp với bản ghi mà sinh viên đã gửi bằng lệnh logger (tức là một facility là "user" và một priority là "info")?

- Quy tắc chỉ định nơi lưu bản ghi

`*.info;mail.none;authpriv.none;cron.none` `/var/log/messages`

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

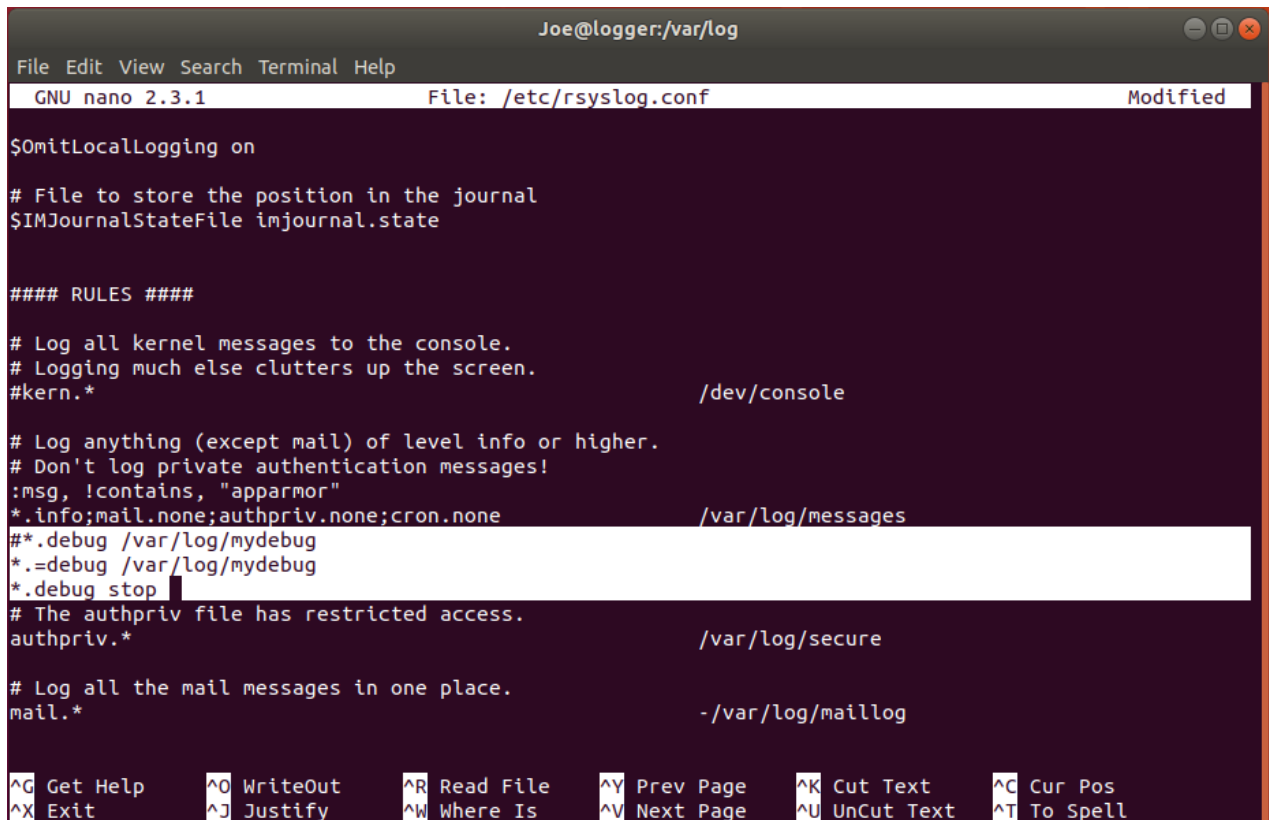
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
:msg, !contains, "apparmor"
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

Hình 48 – Xem quy tắc chỉ định nơi lưu bản ghi

7. Quy tắc nào sinh viên đã thêm để đưa các thông báo gỡ lỗi (và chỉ các thông báo gỡ lỗi) vào /var/log/mydebug?

**.=debug /var/log/mydebug*

**.debug stop*



```
Joe@logger:/var/log
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/rsyslog.conf Modified

$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

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

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

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Hình 49 – Thêm quy tắc để đưa ra các thông báo gỡ lỗi

8. Sinh viên đã kiểm tra quy tắc gỡ lỗi mới như thế nào?

- Thêm 2 bản ghi debug và info

logger -p debug "This is a debug test"

logger -p info "This is an info test"

- Kiểm tra file /var/log/mydebug: Ta chỉ thấy bản ghi của debug

9. Sinh viên đã sử dụng lệnh nào để thay đổi quyền trên logger để chỉ người dùng root và nhóm root mới có thể thực thi nó?

chmod 750 /bin/logger

10. Nhìn vào tất cả các quy tắc hoạt động trong rsyslog.conf, hành động nào sẽ rsyslog thực hiện nếu nhận được một bản ghi từ kernel với mức ưu tiên là emerg?

.emerg :omusrmsg:

11. Nhìn vào tất cả các quy tắc hoạt động trong rsyslog.conf, hành động nào sẽ rsyslog thực hiện nếu nhận được một bản ghi từ facility mail với mức ưu tiên là notice?

mail. -/var/log/maillog*

12. Nhìn vào tất cả các quy tắc hoạt động trong rsyslog.conf, hành động nào sẽ rsyslog thực hiện nếu nhận được một bản ghi từ facility local6 với mức ưu tiên là err?

uucp,news.crit /var/log/spooler

13. Mô tả bất kỳ thử nghiệm hoặc khám phá bổ sung nào sinh viên đã thực hiện.

- Kiểm tra việc sử dụng hệ thống journal với rsyslog:

\$ModLoad imjournal

- Sau đó, có thể đã kiểm tra các bản ghi hệ thống được ghi vào systemd journal và đảm bảo rằng rsyslog có thể truy cập và xử lý các bản ghi từ journal này.

14. Sinh viên đã học được điều gì từ bài thực hành này?

- Cấu hình và kiểm tra hệ thống ghi log trên CentOS, đặc biệt là với rsyslog.
- Hiểu rõ cách sử dụng và kiểm tra các tệp nhật ký hệ thống, bao gồm cả các lỗi đăng nhập và sử dụng su.
- Tạo và kiểm tra các mục syslog bằng tiện ích logger.
- Cấu hình rsyslog để xử lý các bản ghi từ các máy tính từ xa, giúp triển khai hệ thống ghi log tập trung.
- Cải thiện kiến thức về quản trị hệ thống và bảo mật qua các tệp log.

15. Cần làm gì để cải thiện bài thực hành này?

- *Hướng dẫn chi tiết hơn:* Cung cấp hướng dẫn rõ ràng hơn về cách sử dụng các công cụ như tail, grep, và logger để sinh viên dễ dàng hiểu cách kiểm tra và xác minh các thay đổi trong cấu hình syslog.
- *Thêm ví dụ thực tế:* Mô tả các tình huống thực tế trong việc ghi log và quản lý hệ thống, chẳng hạn như cách xử lý sự kiện bảo mật, hoặc các trường hợp nhật ký lỗi và các thông báo quan trọng.
- *Kiểm tra lỗi cú pháp:* Cung cấp một phần kiểm tra cú pháp rsyslog.conf trước khi khởi động lại dịch vụ, giúp sinh viên dễ dàng phát hiện lỗi trước khi áp dụng thay đổi.
- *Mở rộng về bảo mật log:* Cung cấp thêm kiến thức về bảo mật log, như cách hạn chế quyền truy cập vào các tệp log và bảo vệ thông tin nhạy cảm.
- *Kết hợp với tình huống thực tế:* Cung cấp các kịch bản thực tế về sự cố hệ thống và yêu cầu sinh viên sử dụng công cụ ghi log để phân tích và giải quyết vấn đề, giúp sinh viên có cái nhìn sâu sắc hơn về cách ứng dụng kiến thức này trong môi trường thực tế.

2.2.3 Kết thúc lab

stoplab centos-log2

CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork centos-log2
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 |
|------------|--------------|------------|---------------|-----------|-------------|----------|-------------|
| B22DCAT063 | 8 | 1 | 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

Hình 50 – Kết quả checkwork

TÀI LIỆU THAM KHẢO

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Trang chủ chính thức của CentOS Project: <https://www.centos.org/>
- [3] Tài liệu chính thức của Red Hat Enterprise Linux (RHEL):
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/
- [4] CentOS Wiki: <https://wiki.centos.org/>
- [5] Tài liệu về rsyslog: <https://www.rsyslog.com/doc/>