Công ty An ninh mạng Viettel

Báo cáo về Logging

Sinh viên: Nguyễn Đan Trường

*MỤC LỤC*

[Chương 1. Syslog, Rsyslog 3](#_Toc153550929)

[Chương 2. Logrotate 10](#_Toc153550930)

[Chương 3. Systemd journal: Journalctl 14](#_Toc153550931)

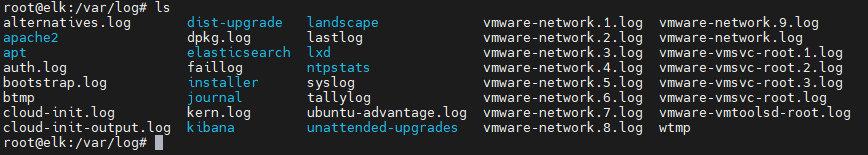
# Syslog, Rsyslog

Syslog là một giao thức client/server là giao thức dùng để chuyển log và thông điệp đến máy nhận log. Máy nhận log thường được gọi là syslogd, syslog daemon hoặc syslog server. Syslog có thể gửi qua UDP hoặc TCP. Các dữ liệu được gửi dạng cleartext. Syslog dùng port 514.

Ứng dụng của log:

* Phân tích nguyên nhân gốc rễ của một vấn đề
* Giúp cho việc khắc phục sự cố nhanh hơn khi hệ thống gặp vấn đề
* Giúp cho việc phát hiện, dự đoán một vấn đề có thể xảy ra đối với hệ thống…

Theo mặc định các bản tin log của hệ thống được syslog lưu vào trong thư mục /var/log và đươc lưu riêng rẽ đối với từng tác vụ trong hệ thống:

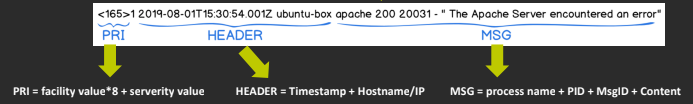


**Chi tiết file cấu hình của syslog**

File cấu hình của Syslog

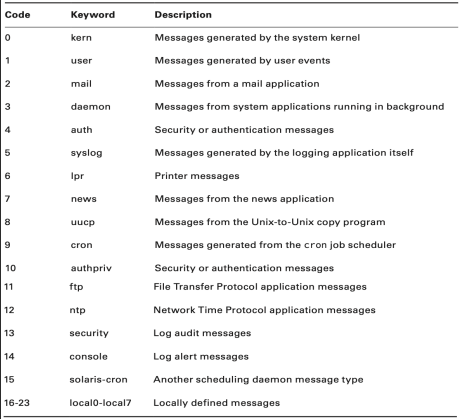
* Trong CentOS, file cấu hình là /etc/rsyslog.conf, file này chứa các rule về log
* Trong Ubuntu file cấu /etc/rsyslog.d/\*.

**Cấu trúc một bản ghi log**

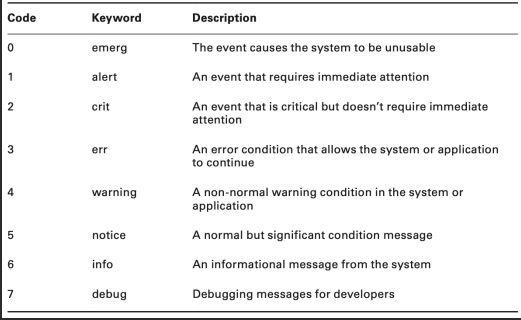
****

* **PRI = facility \* 8 + serverity**
* **Timestamp**: thời điểm khi log message được tạo.
* **Hostname**: là tên của máy chủ gửi log hoặc IP
* **MSG = process\_name + PID + MsgID+ Content**

**Facility**: chỉ nguồn gốc của log được sinh ra



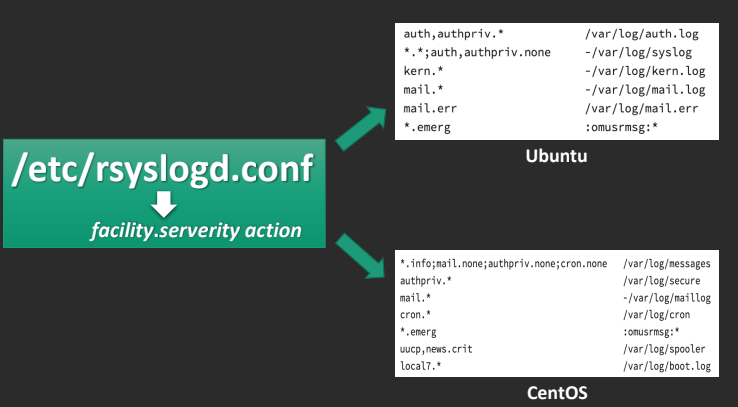
**Serverity**: chỉ mức độ quan trọng của log



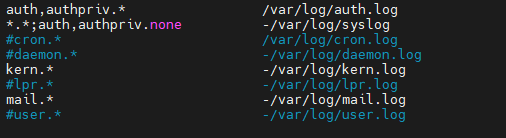
**Rsyslog**

Rsyslog là một phiên bản mở rộng và cải tiến của syslog, tập trung vào tốc độ ghi log so với syslog

**Rsyslog configuration**

****

Cú pháp cấu hình của rsyslog là: ***facility.serverity action***



VD:

\*.\* - /var/log/syslog : bất kể log từ nguồn nào và tất cả các mức serverity thì đều được ghi vào gile /var/log/syslog

\*.\*;auth,authpriv.none -/var/log/syslog: tất cả các loại sự kiện nhưng trừ log từ 2 nguồn “auth” và “authpriv” sẽ không được ghi vào tệp /var/log/syslog

Dấu `;` được sử dụng để phân tách giữa các quy tắc

Lưu ý: đối với các dòng lệnh như sau:

*mail.info /var/log/mail*

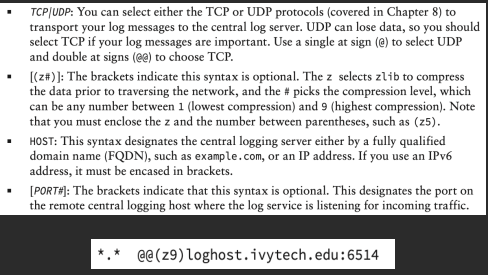
Khi đó bản tin log mail sẽ được ghi lại ở mức cảnh báo từ info trở lên, cụ thể là notice,warm, … Nếu bạn chỉ muốn nó log lại ở mức info thì phải sử dụng cấu hình sau:

*mail.=info /var/log/mail*

Tương tự nếu không muốn lưu mức info thì có thể dùng lệnh: *mail.!info*

**Rsyslog send logs to syslog server**

****

****

Rsyslog cũng hỗ trợ việc gửi log tới một server log tập trung. Các thức khai báo để gửi log như sau:

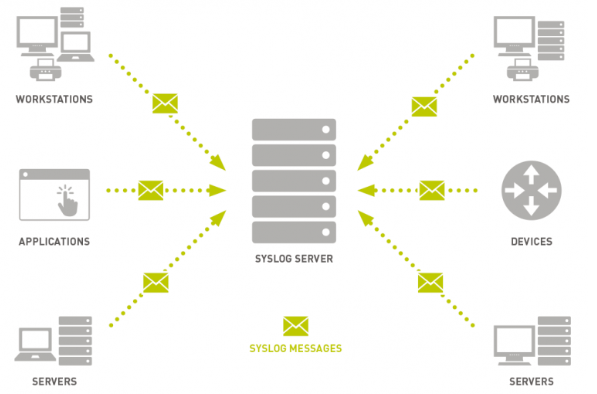
Facility.serverrity TCP|UDP[(z#)]HOST:[PORT#]

Việc cấu hình trên client còn phải dựa trên cấu hình đầu syslog server khai báo giao thức nào, lắng nghe trên port nào…

Tại tầng transport: Rsyslog hỗ trợ cả TCP và UDP

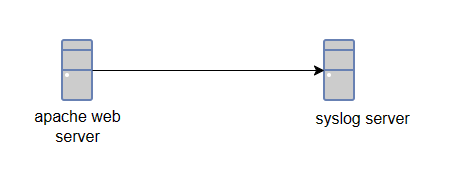
Z#: là phần optional, nếu khai báo thì log sẽ được nén trước khỉ gửi đi trên đường truyền. Mức độ nén được thể hiện từ 1 – 9

**Mô hình log tập trung**

****

Mô hình syslog tập trung là kiến trúc trong đó tất cả các logs từ nhiều nguồn khác nhau được chuyển đến một máy chủ để lưu trữ và quản lý.

**Cấu hình**

****

Lúc này máy Ubuntu chạy dịch vụ http và là máy client gửi log về syslog server

Bước 1: Chỉnh sửa file cấu hình /etc/rsyslog.conf của syslog server để nhận các bản tin log client gửi về:



Bỏ command 2 dòng này để máy chủ log mở port 514 UDP nhận log

Nếu bạn muốn trên máy chủ log tạo thành các thư mục riêng log đối với từng máy Client thì thêm dòng sau vào file cấu hình:



%HOSTNAME%  = %FROMHOST-IP%: có thể thay đổi là IP của client

Tiếp theo chuyển quyền sở hữu tệp tin /var/log cho syslog để có thể tạo file/thư mục:

*chown syslog.syslog /var/log*

Bước 2: Cấu hình trên client để đẩy log lên server





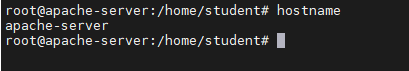
Bước 3: Thêm dòng sau đầu vào file cấu hình apache trong máy client: /etc/apache2/apache2.conf

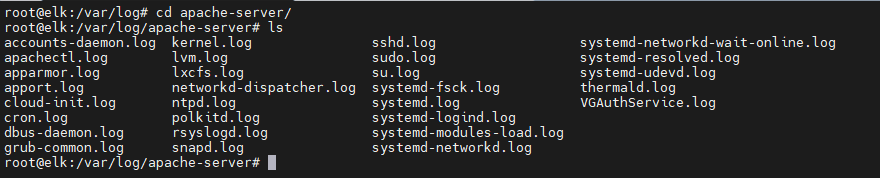


Thêm dòng sau vào file /etc/apache2/sites-enabled/000-default.conf



Dòng lệnh trên có ý nghĩa chuyển tất cả các Log của phần CustomLog vào đầu vào lệnh logger và lệnh logger cho ra đầu ra của log với nguồn là httpacces và với selector là local1.info

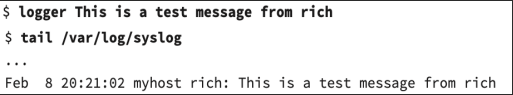


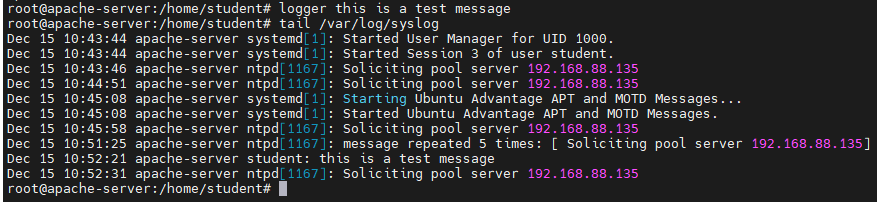


Ta thấy được trên server đã tạo ra một thư mục riêng cho client để lưu log.

**Testing using logger**

*logger [-isd] [-f file] [-p priority] [-t tag] [-u socket] [message]*

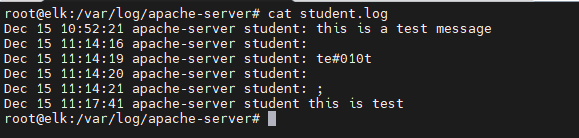
**

**

Logger là coogn cụ để ghi thông báo ào hệ thống log. Một số cách sử dụng logger:

* Ghi thông báo đơn giản: *logger "This is a simple log message."*
* Ghi thông báo với mức độ: *logger -p user.info "This is a test."*
* Ghi thông báo và đăt tên nguồn: *logger -t myscript "This is a test."*





# Logrotate

Phần lớn các distro sẽ cài đặt một cấu hình syslog mặc định bao gồm logging to messages và các log file khác trogn /var/log/. Để ngăn những file này ngày càng trở nên cồng kềnh và khó kiểm soát, một hệ thống quay vòng log (a log file rotation scheme) nên được cài đặt.

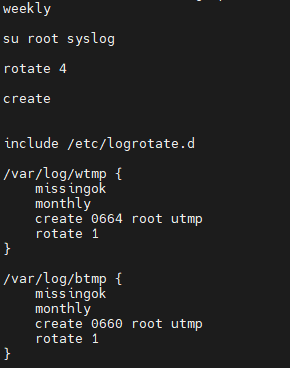
Tiện ích thi hành rotation là logrotate. Lệnh này được cấu hình sử dụng ch một hoặc nhiều file – được xác định bới các tham số đi cùng.

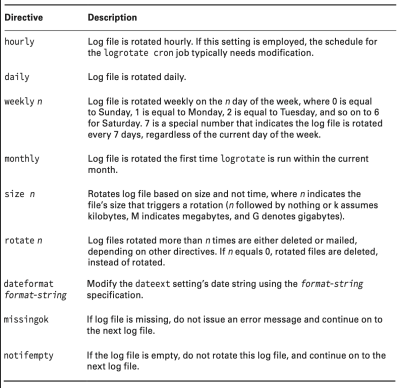
Logrotate sẽ được chạy hằng ngày:

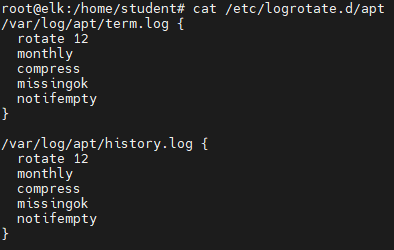


**Logrotate Configuration**

* /etc/logrotate.conf: đây là file cấu hình mặc định của logrotate. Ngoài ra nó còn include các file .conf trong thư mục /etc/logrotate.d/





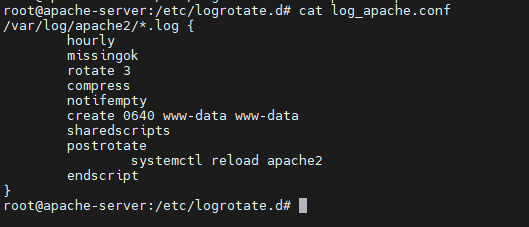


Ý nghĩa cấu hình:

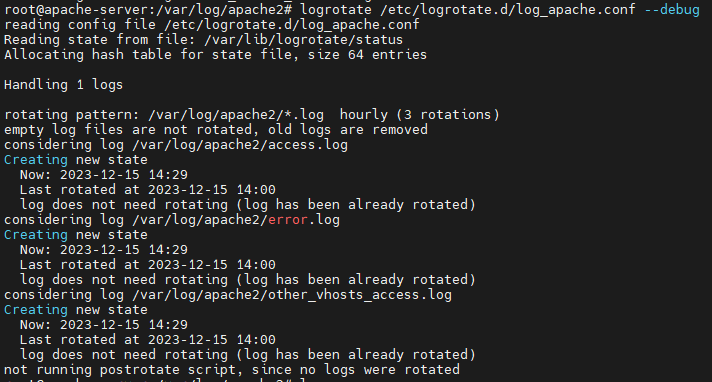
* Rotate 12: giữ lại 12 bản ghi log
* Monthly: thực hiện rotate log định kỳ hàng tháng
* Compress: nén các tập tin được rotate. Mặc định các tệp được nén dưới định dạng .gz. Có thể thay đổi định dạng nén bằng công cụ compresscmd
* Missingok: Nếu log file bị missing, vẫn tiếp tục thực hiện các file tiếp theo mà không cần thông báo lỗi
* Notifyempty: không rotate những file rỗng

**Example Config**

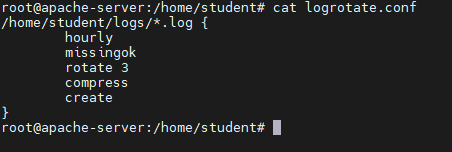
Bước 1: tạo 1 file config trong thư mục /etc/logrotate.d/:

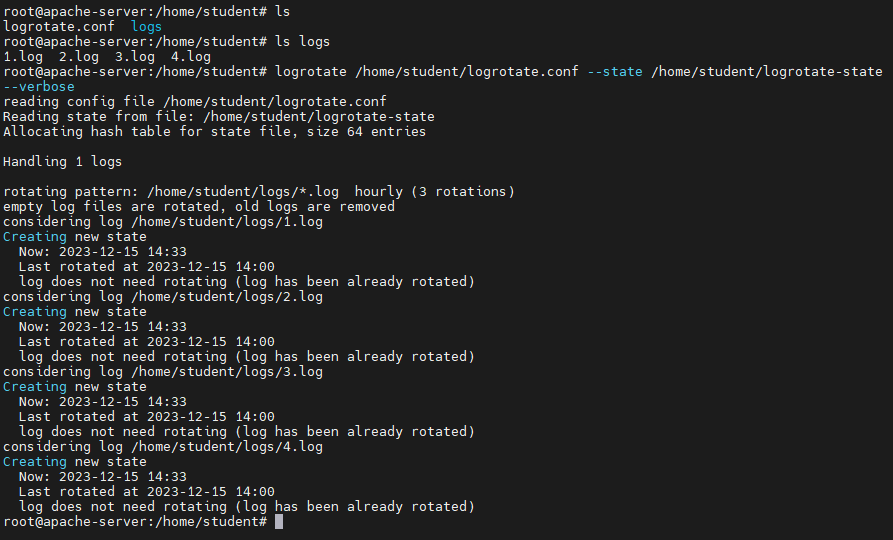


Thực hiện test bằng lệnh sau:



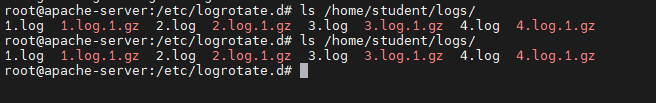
Test thử với thư mục /home/student/logs/





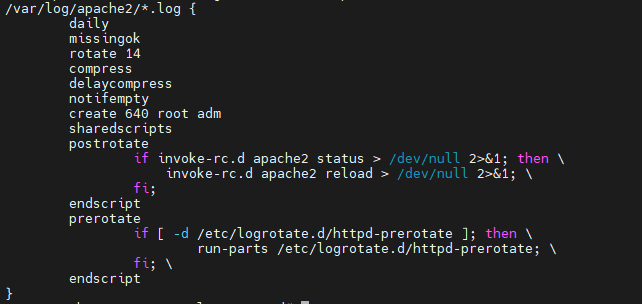
Đặt logrotate vào crontab:





Trong cấu hình logrotate, thường đi kèm với portrotate là vì. Postrotate được sử dụng để thực hiện các công việc sau khi quá trình rotate hoàn thành ví dụ như:

* Khởi động lại dịch vụ (reload): Điều này giúp áp dụng các thay đổi câu shinhf mới mà không cần phải khởi động lại toàn bộ dịch vụ. Trong trường hợp Apache, sử dụng reload thay vì restart giúp tránh gián đoạn kết nối đang tồn tại.
* Thông báo hoạc gửi cảnh báo: Có thể sử dụng postrotate để gửi thông báo hoặc cảnh báo đến hệ thống giám sát hoặc hệ thống quản trị log.
* Sao lưu log: Trong một số trường hợp, postrotate có thể được sử dụng để sao lưu các bản ghi cũ.

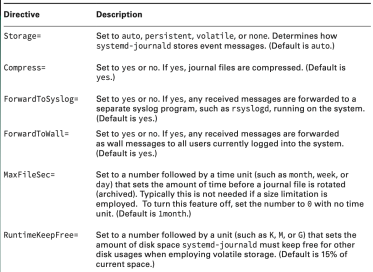


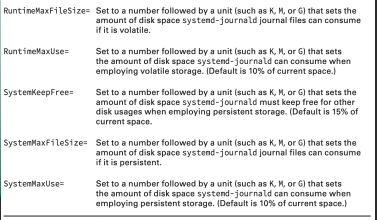
* create 640 root adm: Tạo mới tệp log với quyền 640 và thuộc tính chủ sở hữu là root:adm nếu tệp log không tồn tại.
* sharedscripts: Chia sẻ các script giữa các tệp log, chỉ thực hiện một lần sau khi quay vòng tất cả các tệp log.

# Systemd journal: Journalctl

Systemd-journald là một trình ghi log dựa trên nhật ký nhị phân (binary logging) được tích hợp sẵn trong systemd.

File cấu của journald được lưu trữ trong file: /etc/systemd/journald



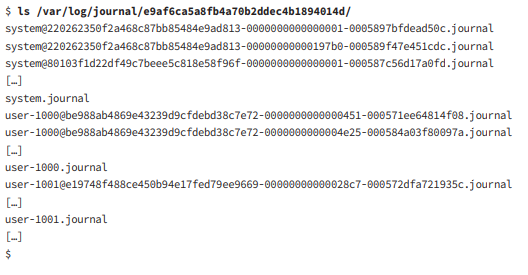


Cấu hình cách thức lưu trữ (Storage):

* Auto: kiểm tra tồn tại /var/log/journal => ghi log vào file nằm trong thư mục đó. Nếu không tồn tại thì sẽ ghi log vào thư mục /run/log/journal – file này sẽ mất khi reboot hệ thống
* Persistent: Log ghi vào file nằm trên đĩa cứng, đảm bảo việc khi khởi động lại thì log vẫn còn. (/var/log/journal)
* Volatile: ghi log vào thư mục /run/log/journal – mang tính tạm thời nếu không cần lưu trữ log file
* None: không ghi lại log vào đâu

Cấu hình được chia làm 2 loại chính là

* Runtime: đi kèm với cấu hình Storage = Volatile
* System: đi kèm với cấu hình Storage = Persistent



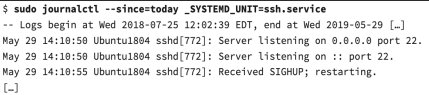
Quy tắc đặt tên log file:

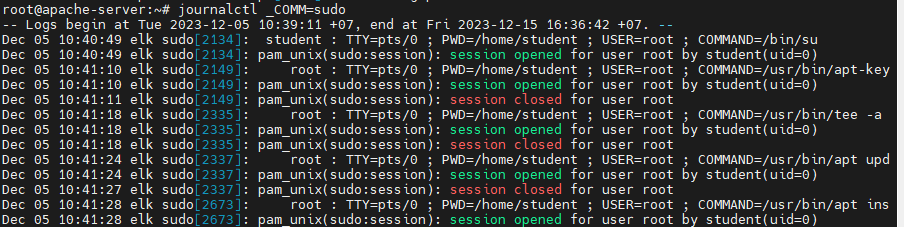
* User-UID.journal, và khi rotate log thì định dạng sẽ được thêm vào đăng sau một chuỗi ký tự để phân biệt.
* System.journal – [system@\_\_\_.journal](mailto:system@___.journal)

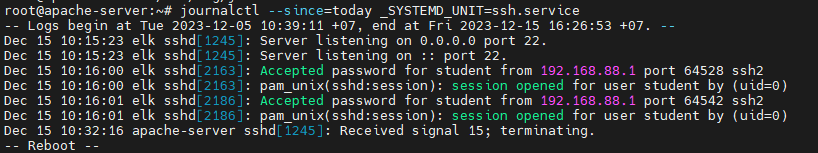
Khi trích xuất thông tin log thì hệ thóng sẽ dọc các file không rotate. Vì các file này đều được lưu trữ dưới dạng binary nên cần dùng công cụ journalctl để đọc và tương tác với file.

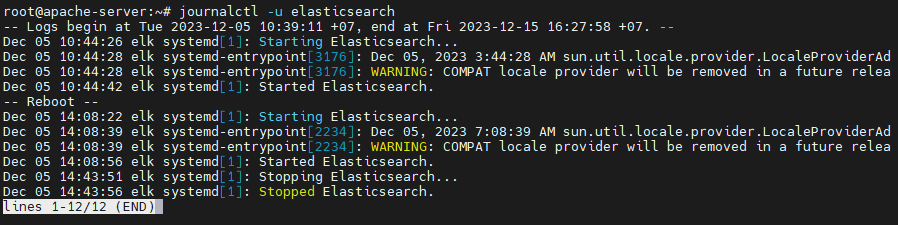
*journalctl [OPTIONS...] [MATCHES...]*

|  |  |
| --- | --- |
|  |  |

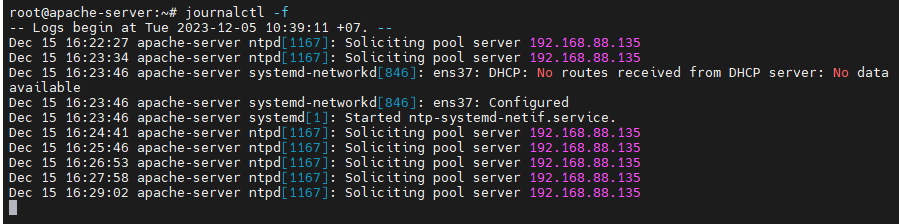




****

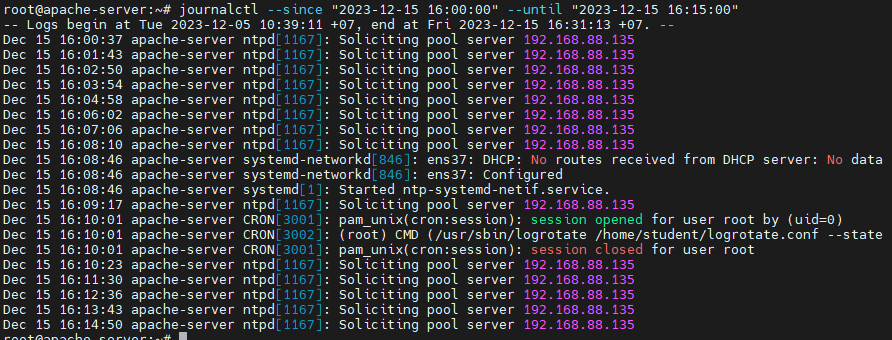
****

Hiển thị log theo thời gian thực



Hiển thị log theo một khoảng thời gian:

*journalctl --since "2023-12-15 16:00:00" --until "2023-12-15 16:15:00"*



**Systemd-journald and syslog working together**

Trong thực tế sẽ sử dụng kết hợp cả 2 vì systemd có có chế lưu log tối ưu hơn nhưng chưa có cơ chế đẩy log theo mô hình syslog server. Vì vậy cả 2 giải pháp lưu trữ này thường được kết hợp với nhau.

Có 2 phương án để kết hợp 2 giải pháp này:

* PA1: Cấu hình rsyslog là client của journald – rsyslog sẽ có cơ chế đọc dữ liệu từ journald.
* PA2: cấu hình journald forward các dữ liệu ra dạng text file và rsyslog có thể đọc hiểu được.

