

Hướng dẫn cấu hình dịch vụ Auditd và đẩy logs về SIEM-Qradar Tháng 9/2021



Hà Nội, Tháng 09 - 2021

Mục lục

1. GIỚI THIỆU VỀ DỊCH VỤ AUDITD TRÊN LINUX.....	1
1.1. TỔNG QUAN VỀ DỊCH VỤ AUDITD.....	1
1.2. CÁC TÍNH NĂNG CHÍNH	2
1.3. ĐÁNH GIÁ ƯU VÀ NHƯỢC ĐIỂM	5
1.4. CÀI ĐẶT	6
2. CÀI ĐẶT VÀ CẤU HÌNH DỊCH VỤ AUDITD	7
2.1. CÁC TẬP CẤU HÌNH DỊCH VỤ	7
2.2. CÁC TIỆN ÍCH BỔ TRỢ	11
2.3. XÂY DỰNG RULE GIÁM SÁT	15
2.3.1. <i>Giám sát tệp tin, thư mục</i>	15
2.3.2. <i>Giám sát system_call</i>	21
2.3.3. <i>Giám sát các lệnh thực thi của người dùng</i>	23
2.3.4. <i>Giám sát các kết nối mạng</i>	24
2.4. TRÍCH XUẤT KẾT QUẢ GIÁM SÁT	25
2.4.1. <i>Tìm kiếm với ausearch</i>	25
2.4.2. <i>Sinh báo cáo với aureport</i>	26
3. CẤU HÌNH SINH LOGS VÀ THU THẬP VỀ QRADAR.....	29
3.1. CẤU HÌNH SINH LOGS TRÊN MÁY CHỦ LINUX	29
3.1.1. <i>Cấu hình dịch vụ auditd</i>	29
3.1.2. <i>Cấu hình dịch vụ rsyslog</i>	34
3.1.3. <i>Cấu hình dịch vụ logrotate</i>	40
3.2. CẤU HÌNH NHẬN LOGS AUDITD TRÊN QRADAR	42
4. HƯỚNG DẪN TROUBLESHOOT	46
4.1. CẤU HÌNH DỊCH VỤ AUDITD.....	46
4.2. CẤU HÌNH DỊCH VỤ RSYSLOG	49
4.3. CẤU HÌNH LOG SOURCE	53
5. XÂY DỰNG SCRIPT TỰ ĐỘNG CẤU HÌNH CHO C06.....	55
6. TÀI LIỆU THAM KHẢO.....	57

1. Giới thiệu về dịch vụ auditd trên Linux

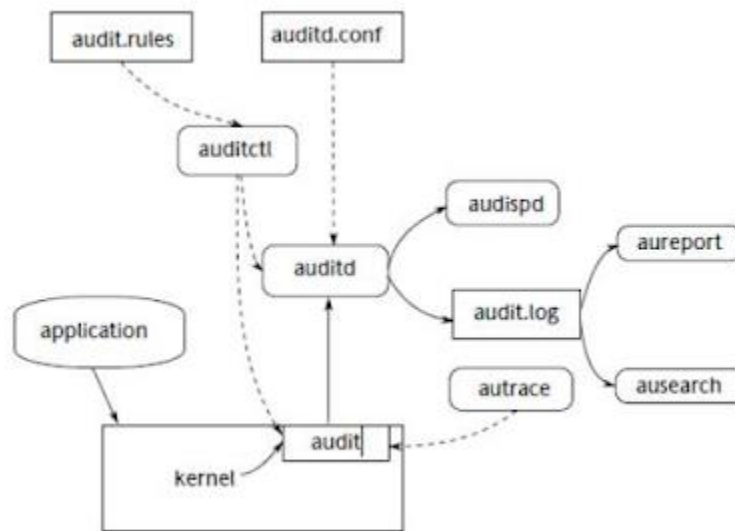
Hệ thống Audit trên Linux (Linux Audit System) cung cấp cách thức cho phép thu thập và theo dõi các thông tin liên quan đến an toàn của hệ thống. Dựa trên các quy tắc / luật (rule) đã cấu hình trước, Audit sẽ ghi lại thông tin về các sự kiện (event) đang xảy ra trên hệ thống thông qua các bản ghi (record) trong các tệp nhật ký (log). Những thông tin này sẽ cực kỳ hữu ích để xác định người đã vi phạm các chính sách bảo mật (security policy) của tổ chức và các hành vi mà hắn đã thực hiện.

Chú ý rằng các hệ thống Audit không cung cấp các tùy chọn để đảm bảo an toàn cho hệ thống, thay vào đó, nó được sử dụng để phát hiện các hành vi vi phạm chính sách bảo mật đang được áp dụng trên hệ thống. Những vi phạm này có thể được ngăn chặn bằng cách kết hợp với một số cơ chế bảo mật như SELinux.

1.1. Tổng quan về dịch vụ Auditd

Về cơ bản, hệ thống Audit trên Linux gồm 2 thành phần chính:

- Thành phần **User-Space Applications** gồm dịch vụ auditd và các tiện ích, công cụ hỗ trợ khác
- Thành phần **Kernel-Side** dùng để xử lý các lời gọi hệ thống (system call) nhận được từ User-Space Applications và chuyển chúng qua một trong các bộ lọc sau: *user, task, exit hoặc exclude*



Trong hệ thống **Audit** của Linux, thành phần quan trọng nhất là dịch vụ **auditd** (audit daemon), nó cho phép thu thập thông tin về các sự kiện đang xảy ra trên hệ thống dựa trên các luật đã cấu hình từ trước, và ghi lại kết quả dưới dạng các bản ghi trong tệp **audit.log** (đường dẫn mặc định là `/var/log/audit/audit.log`). Ngoài ra, còn có một số tiện ích, dịch vụ khác như:

- Dịch vụ **audispd** hoạt động như một chương trình điều phối, cho phép tương tác với **auditd** và gửi các sự kiện đến các chương trình khác để phân tích theo thời gian thực (real-time).
- Tiện ích **auditctl** cho phép tương tác với một số thành phần trong Audit Kernel để quản lý các luật, thiết lập một số cài đặt và tham số trong quá trình sinh logs.
- Một số tiện ích khác sẽ nhận đầu vào là nội dung của tệp audit logs và cho đầu ra theo yêu cầu của người dùng. Ví dụ, tiện ích **aureport** sẽ cho phép sinh báo cáo dựa trên tất cả các bản ghi trong tệp audit logs.

1.2. Các tính năng chính

Dịch vụ **auditd** cho phép ghi lại nhật ký hoạt động của toàn bộ người dùng, của các dịch vụ đã được cài đặt trên máy chủ Linux dưới dạng logs.

Người dùng cần được cấp quyền truy cập để có thể đọc thông tin trong các tệp logs này.

Khi phát hiện những hành vi bất thường trên hệ thống (chẳng hạn như hệ thống đã bị xâm phạm), người quản trị có thể kiểm tra logs được ghi bởi dịch vụ `auditd` để tìm kiếm thông tin, phục vụ cho việc điều tra và xử lý sự cố trên máy chủ. Ngoài ra, thông qua logs, người quản trị cũng sẽ nắm được toàn bộ hành vi của người dùng cũng như cách thức hoạt động của các dịch vụ, từ đó có thể tìm kiếm các mối đe dọa (threat) còn tồn tại trên hệ thống. Đây là cơ sở quan trọng để xây dựng các phương án gia cố (hardening) hệ thống, đảm bảo an toàn cho hệ thống máy chủ cung cấp dịch vụ trước các cuộc tấn công ngày càng tinh vi và phức tạp của kẻ xấu.

Người dùng được cấp quyền truy cập có thể sử dụng **`ausearch`** và **`aureport`** để trích xuất thông tin từ các bản ghi trong logs được ghi bởi dịch vụ `auditd`. Các luật cấu hình để sinh logs nằm trong tệp **`/etc/audit/audit.rules`** sẽ được **`auditctl`** đọc mỗi khi dịch vụ audit được khởi động. Ta có thể sử dụng **`auditctl`** để sửa các luật này. Toàn bộ cấu hình của dịch vụ audit sẽ được lưu tại đường dẫn **`/etc/audit/auditd.conf`**. Một số thông tin có thể được ghi lại trong logs của dịch vụ audit gồm:

- Thời gian xảy ra, phân loại và kết quả của mỗi sự kiện
- Liên kết mỗi sự kiện với thông tin người dùng đã kích hoạt nó
- Các thay đổi với tệp cấu hình dịch vụ audit và thông tin về truy cập tệp audit logs
- Thông tin liên quan đến các cơ chế xác thực, ví dụ như SSH, Kerberos, LDAP, ...
- Các thay đổi với các tệp tin quan trọng, tệp tin nhạy cảm như tệp mật khẩu **`/etc/passwd`**, ...
- Các thông tin kết nối mạng đến và đi trên hệ thống máy chủ, ...

Một số kịch bản (usecase) có thể được cấu hình giám sát và sinh logs bởi hệ thống Audit trên các máy chủ Linux:

+) **Theo dõi truy cập tệp tin:** Dịch vụ audit cho phép theo dõi các hành vi truy cập (access), thay đổi (modify), thực thi (execute) một tệp tin hoặc

thư mục; cũng như giám sát việc thay đổi thuộc tính (attribute) của tệp tin. Điều này rất có ích trong việc phát hiện truy cập các tệp quan trọng, các tệp nhạy cảm như tệp mật khẩu, tệp cấu hình dịch vụ SSH, ...

+) **Giám sát các lời gọi hệ thống (System Call):** Dịch vụ audit cho phép cấu hình để sinh logs mỗi khi một lời gọi hệ thống được sử dụng. Ví dụ, giám sát thay đổi về cấu hình thời gian của hệ thống bằng cách theo dõi một số lời gọi hệ thống như `settimeofday`, `clock_adjtime`, cũng như một số lời gọi hệ thống liên quan khác.

+) **Ghi lại các lệnh (command) đã được thực thi bởi người dùng:** Dịch vụ audit cho phép cấu hình theo dõi một tệp đã được thực thi hay chưa, do vậy ta có thể xây dựng các luật cho phép ghi lại việc thực thi của một lệnh cụ thể. Ví dụ, viết một luật định nghĩa cho mọi tệp thực thi trong thư mục `/bin`. Do vậy, khi người dùng thực thi chúng sẽ ghi lại logs trong tệp `audit.log`

+) **Ghi lại các đường dẫn hệ thống (system pathname) được thực thi:** Dịch vụ audit cho phép ghi lại đường dẫn của tệp được thực thi, ngay cả khi nó không được định nghĩa trong tệp luật.

+) **Ghi lại các sự kiện bảo mật:** Mô-đun xác thực `pam_faillock` cho phép ghi lại số lần đăng nhập không thành công và thông tin về tài khoản cố gắng thực hiện đăng nhập.

+) **Tìm kiếm các sự kiện:** Sử dụng tiện ích `ausearch` để lọc các sự kiện được ghi trong logs theo một số điều kiện nhất định.

+) **Sinh báo cáo tổng hợp:** Sử dụng tiện ích `aureport` để sinh báo cáo kết quả, ví dụ như kết quả danh sách các sự kiện được ghi lại hàng ngày, ... Điều này giúp người quản trị dễ dàng phân tích và điều tra thêm về các hành vi đáng ngờ.

+) **Giám sát các truy cập mạng:** Một số tiện ích như `iptables` và `ebtables` có thể được cấu hình để kích hoạt một số điều kiện trong dịch vụ audit, ví dụ như cho phép người quản trị giám sát việc truy cập mạng trên máy chủ.

Chú ý: Cấu hình các luật trong dịch vụ audit để sinh logs có thể ảnh hưởng tới hiệu năng (performance) của hệ thống máy chủ Linux.

1.3. Đánh giá ưu và nhược điểm

Dựa trên một số tính năng kể trên của dịch vụ auditd, có thể đánh giá một số ưu và nhược điểm của dịch vụ này như sau:

Ưu điểm	Nhược điểm
<ul style="list-style-type: none">➤ Là dịch vụ độc lập, không cần cài đặt thêm bất kỳ chương trình / tiến trình nào bên ngoài hệ thống➤ Cho phép giám sát, ghi logs các hoạt động của mọi người dùng, mọi dịch vụ đã cài đặt trên hệ thống, phục vụ tốt cho việc giám sát, điều tra và xử lý sự cố➤ Hỗ trợ phát hiện và phân tích mối đe dọa tiềm ẩn trên hệ thống➤ Có thể hoạt động như một hệ thống phát hiện xâm nhập IDS và có thể tích hợp với các hệ thống IDS khác	<ul style="list-style-type: none">➤ Khi khởi động lại máy chủ, toàn bộ các rules đã cấu hình bằng câu lệnh auditctl sẽ bị xóa và phải cấu hình lại từ đầu➤ Không giám sát được toàn bộ logs network mà chỉ giám sát được logs liên quan đến socket, đến các kết nối mạng trên hệ thống

Để khắc phục tình trạng mất các rules đã cấu hình sau khi hệ thống khởi động lại, ta có thể thực hiện 2 cách sau:

Cách 1: Thực hiện hai lệnh sau, sau khi đã thêm các rules vào tệp cấu hình:

```
$ echo "-D" > /etc/audit/rules.d/new.rules
$ auditctl -l >> /etc/audit/rules.d/new.rules
```

Cách 2: Trong thư mục **rules.d**, tạo một tệp **/etc/audit/rules.d/audit.rules** và một tệp bản sao (backup) của nó. Tuy nhiên, khi cần thêm các rules mới thì phải thêm trực tiếp vào tệp **audit.rules** mà không sử dụng được lệnh **auditctl**.

1.4. Cài đặt

Về cơ bản, cách cài đặt dịch vụ **auditd** là tương tự nhau trên các bản phân phối Linux và chúng thường được cài đặt mặc định trên một số hệ điều hành như **CentOS6, CentOS7, Red Hat Enterprise 7, Red Hat Enterprise 8, ...** Trong tài liệu này sẽ hướng dẫn cách cài đặt dịch vụ **auditd** trên hệ điều hành Ubuntu sử dụng nhánh **apt-get** để quản lý các gói cài đặt và hệ điều hành CentOS, Red Hat Enterprise sử dụng nhánh **yum** để quản lý các gói cài đặt. Để cài đặt dịch vụ **auditd** và các công cụ hỗ trợ, thực hiện lệnh sau:

```
# Trên Ubuntu
$ sudo apt-get install auditd audispd-plugins

# Trên CentOS/RHEL
$ sudo yum install audit audit-libs
```

Một số lệnh cơ bản khác để vận hành dịch vụ:

```
# Khởi động / dừng / khởi động lại dịch vụ
$ sudo service auditd start
$ sudo service auditd stop
$ sudo service auditd restart

# Kiểm tra trạng thái của dịch vụ
$ service auditd status

# Chỉ khởi động lại dịch vụ auditd nếu nó đang hoạt động
$ service auditd condrestart

# Reload lại cấu hình dịch vụ auditd từ tệp /etc/audit/auditd.conf
$ service auditd reload

# Rotate tệp logs trong thư mục /var/log/audit
$ service auditd rotate
```

Tham khảo một số lệnh liên quan đến dịch vụ **auditd**:

- Liên kết: [https://linuxhint.com/auditd_linux_tutorial/]


```
Installed Packages
audit.x86_64
audit-libs.x86_64
```

2. Cài đặt và cấu hình dịch vụ auditd

2.1. Các tệp cấu hình dịch vụ

❖ Tệp cấu hình auditd.conf

Tệp **auditd.conf** là tệp cấu hình chính của dịch vụ **audit** trên các máy chủ linux. Mặc định, tệp này nằm ở đường dẫn **/etc/audit/auditd.conf**. Để sửa tệp cấu hình này, sử dụng tiện ích **auditctl** hoặc sửa trực tiếp thông qua các trình sửa văn bản (editor) như **nano**, **vim**, **gedit**, ... Ví dụ, chạy lệnh: **\$ sudo nano /etc/audit/auditd.conf**

Ví dụ, cấu hình một tệp **auditd.conf** có thể như hình minh họa bên dưới. Các tham số có thể thay đổi để phù hợp với cấu hình thực tế của hệ thống.

```

GNU nano 2.3.1                                File: /etc/audit/auditd.conf
# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = HOSTNAME
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0

```

Trong tệp cấu hình, các dòng trống, hoặc các dòng bắt đầu bởi ký tự **#** sẽ bị bỏ qua. Để đáp ứng một số chính sách an toàn thông tin (security policies) trên máy chủ, cần chú ý một số tham số sau trong tệp cấu hình.

Tham số	Ý nghĩa
log_file	Đường dẫn thư mục lưu trữ logs của dịch vụ audit. Theo mặc định, thường nằm trong thư mục /var/log/audit/
max_log_file	Kích thước tối đa của một tệp logs được lưu trữ. Ví dụ, max_log_file = 8 thì tệp logs sẽ có kích thước tối đa là 8 MB
max_log_file_action	Hành động sẽ được thực hiện khi tệp logs đạt kích thước tối hạn max_log_file (đã thiết lập ở trên). Ví dụ chọn keep_logs để ngăn tệp audit.logs bị ghi đè, chọn ROTATE để ghi

	backup tệp logs hiện tại và tạo tệp mới để tiếp tục ghi logs
space_left	Chỉ định dung lượng trống (free space) còn lại trên ổ cứng để kích hoạt hành động được thiết lập trong space_left_action . Giá trị này cần thiết lập phù hợp để người quản trị có thời gian kiểm tra và thực hiện giải phóng dung lượng ổ cứng. Nó phụ thuộc vào tốc độ sinh tệp audit.logs
space_left_action	Nên thiết lập thành email , hoặc exec để cung cấp cách thức thông báo phù hợp
admin_space_left	Chỉ định dung lượng còn lại tối thiểu trên ổ cứng để kích hoạt hành động được thiết lập trong admin_space_left_action . Giá trị này cần được thiết lập để đủ không gian ghi lại nhật ký các hành động do người quản trị thực hiện
admin_space_left_action	Nên thiết lập thành single để đưa hệ thống về chế độ một người dùng (single-user) và cho phép người quản trị giải phóng dung lượng ổ đĩa
disk_full_action	Chỉ định hành động được kích hoạt khi không còn dung lượng trống trên phân vùng chứa audit logs, nên thiết lập thành half hoặc single . Điều này đảm bảo rằng hệ thống đang tắt, hoặc đang hoạt động ở chế độ một người dùng khi dịch vụ audit không còn khả năng ghi thêm logs
disk_error_action	Chỉ định hành động được kích hoạt trong trường hợp phát sinh lỗi trên phân vùng chứa các tệp audit logs. Nên đặt hành syslog , single hoặc half phụ thuộc vào chính sách bảo mật cục bộ của tổ chức liên quan đến việc xử lý các lỗi phần cứng
flush	Nên đặt thành incremental_async . Nó hoạt động kết hợp với tham số freq để xác định số lượng bản ghi có thể được gửi đến đĩa trước khi buộc phải đồng bộ với ổ cứng. Tham số freq thường được đặt thành 100. Chúng đảm bảo dữ liệu về các sự kiện audit sẽ được đồng

	bộ với tệp audit logs trên ổ đĩa, trong khi vẫn giữ hiệu suất tốt cho toàn bộ hoạt động
log_format	Cho biết cách thức thông tin được lưu trữ trên ổ đĩa. Có 2 tùy chọn là raw và enriched . Nếu chọn raw , các bản ghi sẽ được lưu ở định dạng giống như kết quả nhận được từ kernel. Nếu chọn ENRICHED sẽ cho phép chuyển đổi tất cả thông tin về uid , gid , syscall , architecture và địa chỉ socket trước khi ghi sự kiện vào tệp logs. Điều này sẽ giúp dễ dàng nắm thông tin trong các sự kiện khi logs được đẩy về hệ thống khác. Chú ý tùy chọn NOLOG hiện không được sử dụng nữa

Sau khi thay đổi cấu hình, cần khởi động lại dịch vụ **auditd** để áp dụng cấu hình mới. Chạy lệnh **\$ sudo service auditd restart**

Tham khảo: <https://man7.org/linux/man-pages/man5/auditd.conf.5.html>

❖ Tệp cấu hình **audit.rules**

Tệp **audit.rules** là tệp cấu hình các luật của dịch vụ **auditd** trên máy chủ Linux. Mặc định, tệp này nằm ở đường dẫn **/etc/audit/audit.rules**. Để thay đổi cấu hình các luật trong tệp, sử dụng tiện ích **auditctl** hoặc sử dụng các trình sửa văn bản như **nano**, **vim**, **gedit**, ...

Các luật (rule) của dịch vụ **auditd** sẽ được duyệt từ trên xuống dưới, theo thứ tự được lưu trong tệp **audit.rules**. Do vậy, khi xây dựng rules cần chú ý thứ tự của chúng, tránh để xảy ra trùng lặp.

❖ Tệp logs **audit.log**

Tệp **audit.log** là tệp ghi lại hoạt động của các dịch vụ, của người dùng trên hệ thống, được ghi bởi dịch vụ **auditd**. Mặc định, tệp này nằm ở đường dẫn **/var/log/audit/audit.log**.

Chú ý: Nếu dịch vụ **auditd** không hoạt động trên máy chủ bởi bất kỳ lý do gì, thông báo kiểm tra lại dịch vụ sẽ được gửi tới dịch vụ **rsyslog**.

2.2. Các tiện ích hỗ trợ

Bên dưới sẽ liệt kê một số công cụ, tiện ích hỗ trợ người quản trị trong việc quản lý và trích xuất thông tin từ hệ thống audit trên linux.

❖ Tiện ích **auditctl**

Tiện ích **auditctl** cho phép thiết lập cấu hình các luật giám sát của dịch vụ audit. Cú pháp sử dụng **auditctl** như sau:

```
$ auditctl [options]
```

Trong đó, giá trị options thường gồm các tham số sau:

Tham số	Ý nghĩa
-w	Đường dẫn của tệp tin, thư mục cần giám sát
-k	Dùng các từ khóa (keyword) để tạo các bộ lọc cho cấu hình rule
-p	Thiết lập các quyền theo chuẩn UNIX
-S	Thiết lập để dùng ghi nhật ký cho một cấu hình
-a	Lưu tất cả kết quả cho đầu vào được chỉ định của tùy chọn này

Ví dụ, để cấu hình theo dõi thay đổi của tệp **/etc/shadow**, sử dụng từ khóa **shadow_file** và quyền là **rwxa**, thực hiện lệnh:

```
$ auditctl -w /etc/shadow -k shadow_file -p rwx
```

Tham khảo liên kết: https://www.tutorialspoint.com/unix_commands/auditctl.htm

❖ Tiện ích **aureport**

Tiện ích **aureport** cho phép sinh báo cáo (report) từ các bản ghi trong logs của dịch vụ audit. Theo mặc định, tất cả các tệp **audit.log** trong thư mục **/var/log/audit** sẽ được truy vấn để sinh báo cáo. Nó cũng hỗ trợ xử lý đầu vào là các tệp raw logs được nhận thông qua đầu vào tiêu chuẩn (stdin). Khi đó, sử dụng lệnh **\$ aureport -if file_name**

```
$ aureport [options]
```

Trong đó, giá trị options thường gồm các tham số sau:

Tham số	Ý nghĩa
-k	Tạo report dựa trên các khóa đã được chỉ định trong cấu hình audit.rules
-i	Hiển thị thông tin dạng bản rõ, thay cho dạng số như là id. Ví dụ, hiển thị tên người dùng, thay vì giá trị user_id của người đó
-au	Tạo report về hành vi xác thực của tất cả người dùng
-l	Tạo report hiển thị thông tin đăng nhập của người dùng

Ví dụ, để hiển thị thông tin tất cả các lệnh đã được thực thi trên hệ thống, sử dụng lệnh:

```
[root@oracle7 ~]$ sudo aureport -x
```

Executable Report

=====

date time exe term host auid event

=====

```
1. 09/16/2021 17:38:08 /usr/bin/python2.7 (none) ? -1 211032
2. 09/16/2021 17:38:08 /usr/bin/rpm (none) ? -1 211033
3. 09/16/2021 17:38:08 /usr/bin/rpm (none) 8.8.8.8 -1 211034
4. 09/16/2021 17:38:08 /usr/bin/python2.7 (none) ? -1 211035
5. 09/16/2021 17:38:08 /usr/bin/rpm (none) ? -1 211036
6. 09/16/2021 17:38:08 /usr/bin/rpm (none) 8.8.8.8 -1 211037
7. 09/16/2021 17:38:08 /usr/bin/python2.7 (none) ? -1 211038
8. 09/16/2021 17:38:08 /usr/bin/rpm (none) ? -1 211039
9. 09/16/2021 17:38:08 /usr/bin/rpm (none) 8.8.8.8 -1 211040
10. 09/16/2021 17:38:10 /usr/sbin/rsyslogd (none) ? -1 211041
```

Để thống kê số lần các lệnh được thực thi, sử dụng lệnh sau:

```
[root@oracle7 ~]$ sudo aureport -x --summary
```

Executable Summary Report

=====

total file

=====

```
17228 /usr/bin/rpm
8614 /usr/bin/python2.7
2716 /usr/sbin/rsyslogd
187 /usr/sbin/sshd
```

```
79 /usr/sbin/aureport
70 /usr/bin/bash
```

Trong đó, cột đầu tiên hiển thị số lần và cột thứ hai hiển thị đường dẫn của lệnh được thực thi. Chú ý là chỉ những lệnh liên quan đến các dịch vụ bảo mật trên hệ thống mới được ghi lại.

Tham khảo liên kết:
https://www.tutorialspoint.com/unix_commands/aureport.htm

❖ Tiện ích **ausearch**

Tiện ích **ausearch** cho phép tìm kiếm thông tin các sự kiện (events) từ các bản ghi (record) trong audit logs. Mặc định, **ausearch** sẽ thực hiện truy vấn các bản ghi trong tệp **audit.log** tại đường dẫn **/var/log/audit/audit.log**. Tương tự như **aureport**, thì **ausearch** cũng cho phép tìm kiếm thông tin từ dữ liệu dạng thô (raw logs) nhận được từ đầu vào tiêu chuẩn (stdin). Khi đó, sử dụng lệnh **aureport -if file_name**

Một số cú pháp khi sử dụng **ausearch** là:

```
$ ausearch [options]
```

Trong đó, giá trị options thường gồm các tham số sau:

Tham số	Ý nghĩa
-p	Truy vấn dựa trên giá trị process id. Ví dụ \$ ausearch -p 6171
-m	Tìm kiếm các chuỗi ký tự trong tệp logs. Ví dụ \$ ausearch -m USER_LOGIN
-sv	Tìm kiếm các sự kiện có giá trị success value. Có 2 giá trị là yes và no
-ua	Tìm kiếm theo bộ lọc là tên người dùng. Ví dụ \$ ausearch -ua root
-t	Tìm kiếm theo bộ lọc là mốc thời gian. Ví dụ \$ ausearch -ts yesterday

Ví dụ để tìm kiếm người dùng đã đăng nhập hệ thống ngày hôm nay, thực hiện lệnh:

```
$ sudo ausearch -m LOGIN --start today -i
----
```

```
node=oracle7 type=LOGIN msg=audit(09/16/2021 19:01:02.016:231887) :
pid=13131 uid=root subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-
aid=unset auid=root tty=(none) old-ses=4294967295 ses=145 res=yes
```

Tham khảo liên kết:
https://www.tutorialspoint.com/unix_commands/ausearch.htm

❖ Tiện ích **audspd**

Tiện ích **audspd** hoạt động như một daemon cho phép ghép nối các sự kiện với nhau.

❖ Tiện ích **autrace**

Tiện ích **autrace** cho phép kiểm tra thông tin liên quan đến một tiến trình (process) cụ thể. Ví dụ, lệnh sau kiểm tra thông tin liên quan đến tiến trình **/bin/date**

```
$ sudo autrace /bin/date
```

Ví dụ lệnh sau cho phép kiểm tra các sự kiện có **Process ID** là **15563** từ nhật ký audit logs, trích xuất kết quả dưới dạng dữ liệu thô (raw) và chuyển nó tới **aureport** để sinh kết quả dưới dạng báo cáo.

```
$ sudo ausearch -p 15563 --raw | aureport -f -i
```

File Report

```
=====
```

```
# date time file syscall success exe auid event
```

```
=====
```

1. 09/16/2021 19:32:30 /var/log/ open yes /usr/sbin/sshd root 239915
2. 09/16/2021 19:32:30 /bin/bash execve yes /usr/bin/bash root 239920
3. 09/16/2021 19:32:30 /etc/profile open yes /usr/bin/bash root 239921
4. 09/16/2021 19:32:30 /etc/profile.d/ openat yes /usr/bin/bash root 239924
5. 09/16/2021 19:32:30 /etc/profile.d/256term.sh open yes /usr/bin/bash root 239925
6. 09/16/2021 19:32:30 /etc/profile.d/colorgrep.sh open yes /usr/bin/bash root 239926
7. 09/16/2021 19:32:30 /etc/profile.d/colorls.sh open yes /usr/bin/bash root 239929
8. 09/16/2021 19:32:30 /etc/profile.d/lang.sh open yes /usr/bin/bash root 239934

Để giám sát tính toàn vẹn và giám sát truy cập của một số tệp tin, thư mục trên Linux, sử dụng lệnh sau:

```
$ auditctl -w <đường dẫn> -p war -k <key>

# Ví dụ
$ auditctl -w /etc/passwd -p rwx -k watch_passwd
```

Trong đó, chuỗi giá trị **rwx** tương ứng với việc giám sát các quyền **r** (read) để đọc, quyền **w** (write) để ghi, quyền **x** (execution) để thực thi và quyền **a** (attribute) để thay đổi thuộc tính của tệp tin, thư mục.

Sử dụng lệnh **\$ sudo cat /etc/passwd** để đọc thông tin mật khẩu người dùng. Kết quả tệp **audit.log** sẽ ghi một số bản ghi sau:

```
type=SYSCALL      msg=audit(1618817627.976:220): arch=c000003e
syscall=257 success=yes exit=3 a0=ffffff9c a1=7fff37b5283c a2=0 a3=0
items=1 ppid=2160 pid=2323 auid=1000 uid=0 gid=0 euid=0 suid=0
fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="cat"
exe="/usr/bin/cat" subj=unconfined key="watch_passwd"

type=CWD msg=audit(1618817627.976:220): cwd="/home/a"

type=PATH          msg=audit(1618817627.976:220): item=0
name="/etc/passwd" inode=264036 dev=08:05 mode=0100644 ouid=0
ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0
cap_fver=0 cap_frootid=0
```

Tham khảo một số key/value cần chú ý (được in đậm) tại liên kết:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-understanding_audit_log_files

Kết quả sẽ bao gồm 3 bản ghi, có cùng mốc thời gian (timestamp) và số seri. Các bản ghi bắt đầu bằng từ khóa **type=** và mỗi bản ghi sẽ gồm một cặp **name=value** (tên=giá trị), được phân tách bằng một dấu cách (space) hoặc một dấu phẩy. Một số trường thông tin trong bản ghi có ý nghĩa sau:

Thuộc tính	Ý nghĩa
Bản ghi type=SYSCALL	

type	Cho biết loại bản ghi. Ví dụ giá trị là SYSCALL cho biết bản ghi này được ghi lại khi có một lời gọi hệ thống tới kernel.
msg	Ví dụ msg=audit(1618817627.976:220) Trường msg gồm 2 giá trị theo cấu trúc audit(time_stamp:ID) . Trong đó timestamp là mốc thời gian và ID là một giá trị duy nhất, định danh cho bản ghi. Nhiều bản ghi có thể cùng timestamp và ID nếu được tạo từ cùng một sự kiện. Mốc thời gian sử dụng định dạng thời gian UNIX (giây), tính từ 00:00:00 UTC vào ngày 1/1/1970. Các cặp giá trị name=value trong sự kiện sẽ được cung cấp bởi kernel hoặc user-space-applications
arch	Ví dụ arch= c000003e Cho biết thông tin về kiến trúc CPU của hệ thống. Giá trị c000003e được viết dưới dạng hexa. Khi tìm kiếm các bản ghi với ausearch , sử dụng tham số -i hoặc --interpret để tự động chuyển đổi các giá trị hexa thành ký tự. Ví dụ c000003e nghĩa là x86_64
syscall	Ví dụ syscall=257 Ghi lại kiểu của lời gọi hệ thống được gửi tới kernel. Giá trị này được quy định trong tệp /usr/include/asm/unistd_64.h. Ví dụ, giá trị 257 ứng với lời gọi hệ thống openat . Sử dụng \$ausyscall --dump để hiển thị danh sách tất cả các lời gọi hệ thống cùng với giá trị số định danh của chúng.
success	Ví dụ success=yes Ghi lại kết quả thực hiện lời gọi hệ thống là thành công (yes), thất bại (no)
exit	Ví dụ exit=3 Cho biết mã giá trị được trả về (exit code) của lời gọi hệ thống. Giá trị này sẽ khác nhau đối với các lời gọi hệ thống khác nhau.
a0, a1, a2, a3	Ví dụ a0=ffffff9c a1=7fff37b5283c a2=0 a3=0 Các trường từ a0 đến a3 ghi lại 4 tham số đầu tiên của các lời gọi hệ thống dưới dạng mã hexa. Chúng sẽ phụ thuộc vào lời gọi hệ thống thực tế được sử dụng.
items	Ví dụ items=1 Chứa số lượng bản ghi bổ trợ PATH theo sau bản ghi SYSCALL
ppid	Ví dụ ppid=2160

	Ghi lại process id của tiến trình cha (PPID – Parent Process ID). Trong trường hợp này 2160 là PPID của tiến trình cha, ví dụ như bash
pid	Ví dụ pid=2323 Ghi lại process id của tiến trình hiện tại (PID – Process ID). Trong trường hợp này, 2323 là PID của tiến trình cat
auid	Ví dụ auid=1000 Ghi lại id của người dùng đã đăng nhập (loginuid). Nó được gán cho người dùng khi đăng nhập và được kế thừa bởi mọi tiến trình, ngay cả khi định danh của người dùng thay đổi. Ví dụ, chuyển tài khoản được sử dụng bằng lệnh su - alex .
uid	Ví dụ uid=0 Ghi lại User ID của người dùng thực thi lệnh. Để chuyển từ giá trị uid dạng số, sang tên người dùng tương ứng, sử dụng lệnh \$ ausearch -i --uid UID
gid	Ví dụ gid=0 Ghi lại Group ID của người dùng
euid	Ví dụ euid=0 Ghi lại User ID thực sự (effective) của người dùng
suid	Ví dụ suid=0 Ghi lại User ID đã được gán cho người dùng
fuid	Ví dụ fuid=0 Ghi lại File System User ID của người dùng
egid	Ví dụ egid=0 Ghi lại Group ID thực sự (effective) của người dùng
sgid	Ví dụ sgid=0 Ghi lại Group ID được thiết lập cho người dùng
fsgid	Ví dụ fsgid=0 Ghi lại File System Group ID của người dùng
tty	Ví dụ tty=pts1 Ghi lại terminal được sử dụng để thực thi
ses	Ví dụ ses=3 Ghi lại Session ID của phiên sử dụng để thực thi
comm	Ví dụ comm="cat" Ghi lại tên của lệnh đã được sử dụng. Ví dụ như lệnh cat
exe	Ví dụ exe="/usr/bin/cat" Cho biết đường dẫn của tệp thực thi được sử dụng
subj	Ví dụ subj=unconfined Ghi lại ngữ cảnh SELinux và gán nhãn cho tiến trình tại thời điểm nó thực thi

key	Ví dụ key="watch_passwd" Xâu ký tự được gán cho rules đã sinh ra sự kiện
Bản ghi type=CWD	
type	Ví dụ type=CWD Cho biết loại bản ghi. Ví dụ giá trị là CWD cho biết thông tin về thư mục được sử dụng để gọi lời gọi hệ thống (SYSCALL) đã xác định ở bản ghi trước đó.
msg	Ví dụ msg=audit(1618817627.976:220)
cwd	Ví dụ cwd="/home/a" Cho biết đường dẫn của thư mục thực hiện lời gọi hệ thống
Bản ghi type=PATH	
type	Ví dụ type=PATH Cho biết loại bản ghi. Ví dụ giá trị là PATH cho biết các đường dẫn (path) đã được truyền tới lời gọi hệ thống dưới dạng tham số.
msg	Ví dụ msg=audit(1618817627.976:220)
item	Ví dụ item=0 Cho biết item nào trong tổng số các item đã được tham chiếu ở bản ghi SYSCALL. Giá trị này dựa trên số 0; số 0 có nghĩa là nó là item đầu tiên.
name	Ví dụ name="/etc/passwd" Cho biết đường dẫn của tệp hoặc thư mục đã được truyền cho lời gọi hệ thống dưới dạng đối số. Ví dụ trường hợp này là /etc/passwd
inode	Ví dụ inode=264036 Cho biết giá trị inode (inode number) được gán cho tệp tin hoặc thư mục trong bản ghi. Để xem giá trị inode gán cho một tệp tin, sử dụng lệnh \$ ls -li file_name Để xem tệp tin đã được gán cho inode, dùng lệnh \$ find / -inum i_value -print
dev	Ví dụ dev=08:05 Cho biết ID chính và ID phụ của thiết bị (device) chứa tệp tin hoặc thư mục được ghi trong sự kiện. Trong trường hợp này, giá trị đại diện cho thiết bị là /dev/8/5
mode	Ví dụ mode=0100644 Ghi lại quyền được gán cho tệp tin hoặc thư mục, được mã hóa dưới dạng số bát phân theo chuẩn UNIX. Ví dụ 0100644 có nghĩa là -rw-r--r--
oid	Ví dụ oid=0

	Ghi lại User ID của người dùng là chủ sở hữu (owner) của đối tượng
ogid	Ví dụ ogid=0 Ghi lại Group ID của người dùng là chủ sở hữu của đối tượng
rdev	Ví dụ rdev=00:00 Chứa mã định danh của thiết bị cho các tệp đặc biệt. Trong trường hợp này, nó không được sử dụng vì đây là tệp thông thường
obj	Ví dụ obj=system_u:object_r:passwd_file_t:s0 Ghi lại ngữ cảnh SELinux mà tệp hoặc thư mục trong bản ghi được gán nhãn tại thời điểm nó thực thi
nametype	Ví dụ nametype=NORMAL Ghi lại mục đích hoạt động của mỗi bản ghi PATH trong ngữ cảnh của một lời gọi hệ thống SYSCALL tổng hợp
cap_fp	Ví dụ cap_fp=0 Ghi lại dữ liệu liên quan đến việc thiết lập khả năng được phép (permit) dựa trên hệ thống tệp của các đối tượng là tệp tin hoặc thư mục
cap_fi	Ví dụ cap_fi=0 Ghi lại dữ liệu liên quan đến việc thiết lập khả năng kế thừa (inherited) dựa trên hệ thống tệp của các đối tượng là tệp tin hoặc thư mục
cap_fe	Ví dụ cap_fe=0 Ghi lại khả năng thiết lập bit hiệu quả (effective bit) dựa trên hệ thống tệp của các đối tượng là tệp tin hoặc thư mục
cap_fver	Ví dụ cap_fver=0 Ghi lại khả năng phiên bản dựa trên hệ thống tệp của đối tượng là tệp tin hoặc thư mục
Bản ghi type=PROCTITLE	
type	Ví dụ type=PROCTITLE Cho biết loại bản ghi. Ví dụ, giá trị là PROCTITLE cho biết đầy đủ lệnh đã kích hoạt một lời gọi hệ thống tới kernel.
proctitle	Ví dụ proctitle=636174002F6574632F7373682F737368645F636F6E666967 Ghi lại thông tin đầy đủ lệnh đã được sử dụng. Giá trị này được mã hóa bằng mã hexa. Sử dụng ausearch với tùy chọn -i hoặc --interpret để tự động chuyển các giá trị này sang giá trị bản rõ có thể đọc được. Ví dụ, giá trị

	636174002F6574632F7373682F737368645F636F6E666967 ứng với lệnh cat /etc/ssh/sshd_config
--	---

2.3.2. Giám sát system_call

Để giám sát một số lời gọi hệ thống (system call), sử dụng lệnh sau:

\$ auditctl -a <action>,<filter> -S <Syscall Name or number> -F field=value -k key_name
--

Trong đó, các giá trị sẽ có ý nghĩa sau:

Tham số	Ý nghĩa
action	Giá trị always/never Chọn một trong 2 giá trị là always (luôn ghi log) và never (không ghi log)
filter	Giá trị task/entry/exit/user/exclude Chỉ định các bộ lọc ở kernel khi một syscall được gọi
-S	Giá trị Syscall Name/Syscall ID Chỉ định giá trị lời gọi hệ thống cần giám sát (theo tên, hoặc theo ID). Tham khảo các giá trị này trong tệp /usr/include/asm/unistd_64.h Có thể nhóm nhiều syscall vào trong cùng một rules, sau tham số -S
-F	Giá trị field=value Thêm các bộ lọc bổ sung cho rules như dựa trên kiến trúc, Group ID, Process ID,
key_name	Chuỗi ký tự định danh cho rules sinh ra logs

Trong kernel của linux có 4 bộ lọc (filter) có thể được sử dụng trong rules. Chi tiết như trong bảng mô tả bên dưới:

Bộ lọc	Ý nghĩa
task	Thêm một rule cho mỗi task list. Nó sẽ chỉ được sử dụng khi task được gọi bởi một parent task khác. Ví dụ như kiểm tra các lời gọi hệ thống fork hoặc clone
exit	Thêm một rule khi có một task kết thúc. Ví dụ theo dõi tất cả các lời gọi hệ thống khi nó kết thúc
user	Thêm một rule khi có một task được tạo bởi người dùng. Nó cho phép lọc (loại bỏ) một số sự kiện bắt nguồn từ không gian người dùng. Theo mặc định, mọi sự kiện bắt nguồn từ không gian người dùng đều được phép. Nên nếu có một số sự kiện

	ta không muốn xem thì có thể thiết lập bộ lọc này để loại bỏ nó. Chú ý các trường uid, auid, gid và pid
exclude	Thêm một rule vào danh sách bộ lọc (thường là danh sách trắng). Nó cho phép loại bỏ một số sự kiện nhất định không được sinh ra.

Thông tin chi tiết, tham khảo tại:

- Liên kết: https://linuxhint.com/list_of_linux_syscalls/
- Liên kết: <https://man7.org/linux/man-pages/man7/audit.rules.7.html>

Ví dụ, để sinh logs mỗi khi một chương trình gọi các lời gọi hệ thống **adjtimex** hoặc **settimeofday**, trên các kiến trúc 64 bit, sử dụng lệnh sau:

```
$ auditctl -a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time_change
```

Ví dụ, để sinh logs mỗi khi một tệp tin bị xóa, hoặc bị đổi tên bởi người dùng có User ID lớn hơn hoặc bằng 1000, sử dụng lệnh bên dưới. Chú ý, tùy chọn **-F auid!=4294967295** sử dụng để loại bỏ những người dùng chưa có Login UID (chưa đăng nhập)

```
$ auditctl -a always,exit -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
```

Ngoài ra, cũng có thể giám sát hệ thống tệp bằng cách sử dụng các rule giám sát lời gọi hệ thống. Ví dụ, lệnh sau tương đương với rules **-w /etc/shadow -p wa** để giám sát tệp /etc/shadow

```
$ auditctl -a always,exit -F path=/etc/shadow -F perm=wa
```

Một số rule khác có thể sử dụng

```
# Giám sát lời gọi hệ thống mkdir để tạo thư mục
$ auditctl -a always,entry -S mkdir

# Giám sát lời gọi hệ thống open để mở một tệp tin nhưng không thành công
$ auditctl -a always,exit -S open -F success!=0
```



```
# Giám sát lời gọi hệ thống thực thi một chương trình execve, trên kiến trúc 32 bit, từ tài khoản root (uid = 0)
$ auditctl -a always,exit -F arch=b32 -S execve -F uid=0

# Giám sát lời gọi hệ thống thực thi một chương trình execve, trên kiến trúc 64 bit, từ tài khoản root (uid = 0)
$ auditctl -a always,exit -F arch=b64 -S execve -F uid=0
```

Ví dụ, khi thực hiện dừng một tiến trình nào đó với lệnh kill, ta sẽ được logs như sau:

```
$ sudo kill 1968

type=SYSCALL      msg=audit(1279134100.434:193):      arch=c000003e
syscall=62 success=yes exit=0 a0=7b0 a1=f a2=0 a3=0 items=0 ppid=1602
pid=1605 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
sgid=0 fsgid=0 tty=pts4 ses=4294967295 comm="bash" exe="/bin/bash"
key="teste_kill"

type=OBJ_PID      msg=audit(1279134100.434:193):      opid=1968  oauid=-1
oid=0 oses=-1 obj=<NULL> ocomm="sleep"
```

2.3.3. Giám sát các lệnh thực thi của người dùng

Để giám sát các lệnh được thực thi bởi người dùng, sử dụng các lệnh sau:

```
$ auditctl -a always,exit -S execve -F arch=b64 -F uid={uid_nguoi_dung}
$ auditctl -a always,exit -S execve -F arch=b32 -F uid={uid_nguoi_dung}
```

Trong đó, giá trị UID của người dùng trên hệ thống Linux được quy định như sau:

Giá trị uid	Ý nghĩa
0	Tài khoản root
1-99	Tài khoản hệ thống như daemon, mail, ...
100-999	Tài khoản hoặc nhóm có quyền quản trị và hệ thống như systemd-network, syslog,...
1000+	Tài khoản người dùng
65534	Tài khoản 'nobody'

Để xem thông tin về UID, GID được gán cho mỗi người dùng, xem trong các tệp sau:

```
$ cat /etc/passwd  
$ cat /etc/group
```

Ví dụ, khi xem danh sách các tệp tin, thư mục có trong thư mục **/etc** với lệnh **ls**, ta được logs như sau:

```
$ sudo ls /etc  
  
type=SYSCALL msg=audit(1618820463.416:4812): arch=c000003e  
syscall=59 success=yes exit=0 a0=55ef3e9f4778 a1=55ef3e9fcbc8  
a2=55ef3e9fd0 a3=0 items=2 ppid=4762 pid=4763 auid=1000 uid=0  
gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=3  
comm="ls" exe="/usr/bin/ls" subj=unconfined key="execv"  
  
type=EXECVE msg=audit(1618820463.416:4812): argc=2 a0="ls" a1="/etc"  
  
type=CWD msg=audit(1618820463.416:4812): cwd="/home/a"  
  
type=PATH msg=audit(1618820463.416:4812): item=0 name="/usr/bin/ls"  
inode=787126 dev=08:05 uid=1000 tai
```

Ngoài việc giám sát các hành vi của người dùng, ta cũng có thể giám sát việc thực thi của một tệp nào đó với cú pháp sau:

```
$ auditctl -a action,filter [-F arch=cpu -S system_call] -F  
exe=path_executable_file -k key_name
```

- Trong đó, các tham số khác tương tự như đã mô tả ở trên. Sử dụng bộ lọc **exe=path_executable_file** để trở đến đường dẫn tệp tin cần giám sát thực thi

Ví dụ, giám sát việc thực thi chương trình **/bin/ld** trên các hệ điều hành 64 bit, sử dụng lệnh sau:

```
$ auditctl -a always,exit -S execve -F exe=/bin/ld -F arch=b64 -k  
execution_bin_id
```

2.3.4. Giám sát các kết nối mạng

Để giám sát các kết nối mạng, các socket đã được thiết lập trên hệ thống linux, sử dụng luật sau:

```
$ auditctl -a always,exit -F arch=b64 -S socket -F success=1
```

```
$ auditctl -a always,exit -F arch=b32 -S socket -F success=1
```

Ví dụ, khi sử dụng lệnh curl để truy vấn đến google.com, ta được logs sau:

```
$ curl google.com
$ sudo ausearch -sc connect

type=SYSCALL msg=audit(1521667806.157:217090): arch=c000003e
syscall=59 success=yes exit=0 a0=fb6c0 a1=fb760 a2=fb55c0
a3=7ffe4ead6520 items=2 ppid=2000 pid=42971 auid=890466808 uid=0
gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=26
comm="curl" exe="/usr/bin/curl"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=(null)

type=EXECVE msg=audit(1521667806.157:217090): argc=2 a0="curl"
a1="google.com"

type=CWD msg=audit(1521667806.157:217090): cwd="/etc/audit/rules.d"

type=PATH msg=audit(1521667806.157:217090): item=0 name="/bin/curl"
inode=306502 dev=fd:01 mode=0100755 ouid=0 ogid=0 rdev=00:00
obj=unconfined_u:object_r:bin_t:s0 objtype=NORMAL

type=PATH msg=audit(1521667806.157:217090): item=1 name="/lib64/ld-
linux-x86-64.so.2" inode=8485228 dev=fd:01 mode=0100755 ouid=0
ogid=0 rdev=00:00 obj=unconfined_u:object_r:ld_so_t:s0
objtype=NORMAL
```

2.4. Trích xuất kết quả giám sát

2.4.1. Tìm kiếm với ausearch

Tiện ích **ausearch** cho phép tìm kiếm các sự kiện trong tệp audit logs. Theo mặc định, nó sẽ tìm kiếm trong tệp **/var/log/audit/audit.log**. Ngoài ra, nó cũng hỗ trợ tìm kiếm trên các tệp logs khác, sử dụng tùy chọn **\$ ausearch -if file_name**

Ví dụ, để tìm kiếm các hành vi cố gắng đăng nhập thất bại trên máy chủ, sử dụng lệnh:

```
$ sudo ausearch -i --message USER_LOGIN --success no
```

```
----  
node=oracle7      type=USER_LOGIN      msg=audit(09/17/2021  
14:14:15.074:2177) : pid=8645 uid=root auid=unset ses=unset  
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct=root  
exe=/usr/sbin/sshd hostname=? addr=172.16.11.11 terminal=ssh res=failed'
```

Ví dụ, để tìm kiếm tất cả thay đổi về tài khoản, nhóm, và vai trò, sử dụng lệnh:

```
$ ausearch -m ADD_USER -m DEL_USER -m ADD_GROUP -m  
USER_CHAUTHOK -m DEL_GROUP -m CHGRP_ID -m ROLE_ASSIGN -  
m ROLE_REMOVE -i
```

Ví dụ, để tìm kiếm tất cả các hành động được thực hiện bởi một người dùng nhất định, sử dụng Login ID của người dùng đó (auid) trong câu lệnh sau:

```
$ ausearch -ua 1000 -i
```

Ví dụ, để tìm kiếm tất cả các lỗi gọi hệ thống không thành công trong thời gian từ hôm qua đến hôm nay, sử dụng lệnh sau:

```
$ ausearch --start yesterday --end now -m SYSCALL -sv no -i  
----  
node=oracle7 type=PROCTITLE msg=audit(09/17/2021 14:20:30.605:2339)  
: proctitle=/usr/sbin/rsyslogd -n  
node=oracle7 type=SYSCALL msg=audit(09/17/2021 14:20:30.605:2339) :  
arch=x86_64 syscall=stat success=no exit=EACCES(Permission denied)  
a0=0x7f51bbb94520 a1=0x7f51bbb94650 a2=0x7f51bbb94650 a3=0x0  
items=0 ppid=1 pid=1209 auid=unset uid=root gid=root euid=root  
suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none)  
ses=unset comm=in:imfile exe=/usr/sbin/rsyslogd  
subj=system_u:system_r:syslogd_t:s0 key=(null)  
node=oracle7 type=AVC msg=audit(09/17/2021 14:20:30.605:2339) : avc:  
denied { getattr } for pid=1209 comm=in:imfile path=/var/log/audit  
dev="dm-0" ino=269406873 scontext=system_u:system_r:syslogd_t:s0  
tcontext=system_u:object_r:auditd_log_t:s0 tclass=dir permissive=0
```

Chi tiết về các tham số được sử dụng với ausearch, tham khảo tại đây.

- Liên kết: <https://man7.org/linux/man-pages/man8/ausearch.8.html>

2.4.2. Sinh báo cáo với aureport

Tiện ích **aureport** cho phép sinh báo cáo thống kê từ các bản ghi trong audit logs. Mặc định, nó sẽ truy vấn các bản ghi trong tất cả tệp **audit.log** trong thư mục **/var/log/audit** để sinh báo cáo. Ngoài ra, nó cũng hỗ trợ sinh báo cáo từ các tệp logs khác, sử dụng tùy chọn **\$ aureport -if file_name**

Ví dụ, để sinh báo cáo tất cả các sự kiện đã được ghi trong 3 ngày gần nhất, không bao gồm ngày hiện tại, sử dụng lệnh:

```
$ sudo aureport --start 09/14/2021 00:00:00 --end 09/17/2021 00:00:00
```

Summary Report

=====

Range of time in logs: 09/17/2021 00:00:03.824 - 09/16/2021 23:59:58.818

Selected time for report: 09/14/2021 00:00:00 - 09/17/2021 00:00:00

Number of changes in configuration: 4

Number of changes to accounts, groups, or roles: 0

Number of logins: 4

Number of failed logins: 0

Number of authentications: 8

Number of failed authentications: 0

Number of users: 2

Number of terminals: 13

Number of host names: 6

Number of executables: 21

Number of commands: 25

Number of files: 36

Number of AVC's: 5204

Number of MAC events: 4

Number of failed syscalls: 7391

Number of anomaly events: 0

Number of responses to anomaly events: 0

Number of crypto events: 76

Number of integrity events: 0

Number of virt events: 0

Number of keys: 9

Number of process IDs: 2294

Number of events: 12405

Ví dụ, để xem thông tin tất cả các tệp đã được thực thi, sử dụng lệnh

```
$ sudo aureport -x
```

Executable Report

```
=====
# date time exe term host auid event
=====
1. 09/16/2021 19:57:42 /usr/bin/rpm (none) ? -1 246634
2. 09/16/2021 19:57:42 /usr/bin/rpm (none) 8.8.8.8 -1 246635
3. 09/16/2021 19:57:42 /usr/bin/python2.7 (none) ? -1 246636
4. 09/16/2021 19:57:42 /usr/bin/rpm (none) ? -1 246637
5. 09/16/2021 19:57:42 /usr/bin/rpm (none) 8.8.8.8 -1 246638
```

Ví dụ, để thống kê số lượng được thực thi của mỗi tệp, sử dụng lệnh sau:

```
$ sudo aureport -x --summary
```

Executable Summary Report

```
=====
total file
=====
26162 /usr/sbin/rsyslogd
4608 /usr/bin/rpm
2187 /usr/bin/python2.7
390 /usr/sbin/sshd
117 /usr/sbin/crond
95 /usr/lib/systemd/systemd
92 /usr/bin/sudo
```

Ví dụ, để thống kê số lần đăng nhập thất bại của tất cả người dùng, sử dụng lệnh

```
$ sudo aureport -u --failed --summary -i
```

Failed User Summary Report

```
=====
total auid
=====
28419 unset
1 root
```

Ví dụ, để thống kê số lần đăng nhập thất bại của người dùng hệ thống (system user), sử dụng lệnh:

```
$ sudo aureport --login --summary -i
```

```
Login Summary Report
```

```
=====
```

```
total auid
```

```
=====
```

```
14 root
```

```
1 (unknown)
```

Ngoài ra, **aureport** cũng hỗ trợ xử lý đầu vào nhận được từ **ausearch**. Ví dụ, sinh báo cáo từ câu truy vấn tìm kiếm tất cả sự kiện truy cập tệp tin của người dùng có User ID là 1000

```
$ ausearch --start today --loginuid 1000 --raw | aureport -f --summary
```

Một số lệnh phổ biến sử dụng để thống kê logs liên quan đến hành vi đăng nhập, đăng xuất trên hệ thống Linux

```
# Thống kê các cảnh báo đăng nhập thành công
```

```
$ aureport -au -i --success
```

```
# Thống kê các cảnh báo đăng nhập thất bại
```

```
$ aureport -au -i --failed
```

```
# Thống kê các tài khoản người dùng đã thực hiện đăng nhập, đăng xuất thành công
```

```
$ aureport -l --success --summary -i
```

3. Cấu hình sinh logs và thu thập về Qradar

Phần này sẽ hướng dẫn cấu hình rules cho dịch vụ auditd để sinh logs, và cấu hình đẩy audit logs về hệ thống SIEM-Qradar.

3.1. Cấu hình sinh logs trên máy chủ linux

3.1.1. Cấu hình dịch vụ auditd

Bước 1: Kiểm tra thông tin hostname và phiên bản của hệ điều hành linux đang sử dụng với lệnh sau:

```
$ hostnamectl
```

Kết quả như hình minh họa bên dưới cho thấy máy chủ chạy hệ điều hành **RHEL 7.8**, tên máy chủ là **oracle7** và sử dụng kiến trúc x86_x64. Việc

xác định đúng phiên bản của hệ điều hành cho phép sử dụng các tiện ích phù hợp để quản lý và cài đặt các gói phần mềm.

rpm (RPM Package Manager) là một tiện ích được cài đặt sẵn trên các hệ điều hành **CentOS7**, **CentOS6** và **RHEL 7.x/8.x**. Nó cho phép cài đặt và quản lý các gói phần mềm trên hệ thống máy chủ trong trường hợp không có kết nối Internet.

dpkg là một tiện ích được cài đặt sẵn trên các hệ điều hành **Ubuntu 18.04** và **Ubuntu 16.04**, cho phép cài đặt và quản lý các gói phần mềm trên hệ thống máy chủ trong trường hợp không có kết nối Internet.

Chi tiết về cách sử dụng 2 tiện ích trên, tham khảo các liên kết sau:

- Về rpm, liên kết: <https://man7.org/linux/man-pages/man8/rpm.8.html>
- Về dpkg, liên kết: <https://man7.org/linux/man-pages/man1/dpkg.1.html>

```
[root@oracle7 ~]# hostnamectl
  Static hostname: oracle7
        Icon name: computer-vm
        Chassis: vm
        Machine ID: 4f8d414661ba412e83cea1ce876991aa
        Boot ID: 9f934ad081ce4cb8ada73c73ff47a565
  Virtualization: vmware
  Operating System: Oracle Linux Server 7.8
        CPE OS Name: cpe:/o:oracle:linux:7:8:server
        Kernel: Linux 4.14.35-1902.300.11.el7uek.x86_64
  Architecture: x86_64
[root@oracle7 ~]#
```

Bước 2: Cài đặt và kiểm tra dịch vụ **auditd**

Theo mặc định, trên một số hệ điều hành từ **CentOS6** trở lên và **RHEL 7.x** trở lên đã được cài đặt sẵn dịch vụ **auditd**. Tuy nhiên, trên một số hệ điều hành như **Ubuntu 18.04**, **Ubuntu 16.04** chưa được cài đặt sẵn gói dịch vụ này. Do vậy, sử dụng các lệnh sau để cài đặt và kiểm tra thông tin dịch vụ **auditd** đã được cài đặt trên máy chủ.

```
# Trên Ubuntu 18.04, Ubuntu 16.04 có kết nối Internet
$ sudo apt-get install auditd audispd-plugins
```



```
# Trên Ubuntu 18.04 không có kết nối Internet
$ dpkg --version
$ sudo dpkg -i libaudit1_2.8.2-1ubuntu1_amd64.deb
$ sudo dpkg -i libauparse0_2.8.2-1ubuntu1_amd64.deb
$ sudo dpkg -i auditd_2.8.2-1ubuntu1_amd64.deb

# Trên Ubuntu 16.04 không có kết nối Internet
$ sudo dpkg -i libaudit-common_2.8.2-1ubuntu1_all.deb
$ sudo dpkg -i libaudit1_2.8.2-1ubuntu1_amd64.deb
$ sudo dpkg -i libauparse0_2.8.2-1ubuntu1_amd64.deb
$ sudo dpkg -i auditd_2.8.2-1ubuntu1_amd64.deb

# Trên CentOS/RHEL có kết nối Internet
$ sudo yum install audit audit-libs

# Trên CentOS/RHEL không có kết nối Internet
$ rpm --version
$ sudo rpm -ivh audit-2.8.5-4.el7.x86_64.rpm
$ sudo rpm -ivh audit-libs-2.8.5-4.el7.x86_64.rpm
```

Kiểm tra phiên bản **auditd** đã được cài đặt trên máy chủ CentOS/RHEL

```
$ sudo rpm -qa | grep audit

audit-2.8.5-4.el7.x86_64
audit-libs-2.8.5-4.el7.x86_64
```

Kiểm tra trạng thái của dịch vụ **auditd**

```
$ sudo systemctl status auditd
```

Kết quả trả về như bên dưới cho thấy dịch vụ **auditd** đang chạy và không phát sinh lỗi

```
[root@oracle7 ~]# systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-09-17 19:37:50 +07; 41min ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 715 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Process: 710 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
  Main PID: 711 (auditd)
    CGroup: /system.slice/auditd.service
            └─711 /sbin/auditd

Sep 17 19:37:50 oracle7 augenrules[715]: lost 0
Sep 17 19:37:50 oracle7 augenrules[715]: backlog 1
Sep 17 19:37:50 oracle7 augenrules[715]: enabled 1
Sep 17 19:37:50 oracle7 augenrules[715]: failure 1
Sep 17 19:37:50 oracle7 augenrules[715]: pid 711
Sep 17 19:37:50 oracle7 augenrules[715]: rate_limit 0
Sep 17 19:37:50 oracle7 augenrules[715]: backlog_limit 8192
Sep 17 19:37:50 oracle7 augenrules[715]: lost 0
Sep 17 19:37:50 oracle7 augenrules[715]: backlog 1
Sep 17 19:37:50 oracle7 systemd[1]: Started Security Auditing Service.
[root@oracle7 ~]#
```

Nếu dịch vụ **auditd** đang bị vô hiệu hóa, thực hiện khởi động dịch vụ và kiểm tra trạng thái của dịch vụ.

```
$ sudo systemctl start auditd
$ sudo systemctl status auditd
```

Bước 3: Cấu hình rules sinh logs cho dịch vụ audit

Các rules của dịch vụ **auditd** được quản lý trong tệp **audit.rules** nằm tại đường dẫn **/etc/audit/audit.rules**. Nó được sinh từ tệp **/etc/audit/rules.d/audit.rules**.

+) Trước khi thay đổi, thực hiện sao lưu (backup) cấu hình hiện có của dịch vụ **auditd**. Sau đó, sao chép tệp cấu hình rules đã được GTSC-A05 xây dựng sẵn vào thư mục trên.

```
$ sudo cp /etc/audit/rules.d/audit.rules /etc/audit/rules.d/audit.rules.bak
$ sudo cp conf/audit.rules /etc/audit/rules.d/audit.rules
```

+) Nạp lại các rule mới vào kernel của hệ điều hành

```
$ sudo augenrules --load
```

Kết quả trả về như hình bên dưới

```
[root@oracle7 rules.d]# sudo augenrules --load
No rules
enabled 1
failure 1
pid 711
rate_limit 0
backlog_limit 8192
lost 0
backlog 1
enabled 1
failure 1
pid 711
rate_limit 0
backlog_limit 8192
lost 0
backlog 1
[root@oracle7 rules.d]#
```

+) Sửa tệp `/etc/audit/auditd.conf` để thay đổi định dạng logs (`log_format`) từ **RAW** sang **ENRICHED** bằng cách sửa trực tiếp trên giao diện bằng editor, hoặc sử dụng câu lệnh

```
Đổi từ log_format = RAW sang log_format = ENRICHED
$ sudo sed -i 's/log_format \= RAW/log_format \= ENRICHED/'
/etc/audit/auditd.conf
```

+) Khởi động dịch vụ `auditd` và kiểm tra trạng thái của dịch vụ

```
$ sudo service auditd restart
$ sudo systemctl enable auditd
$ sudo systemctl status auditd
```

Kết quả như hình bên dưới, cho thấy dịch vụ `auditd` đang hoạt động tốt. Nếu phát sinh lỗi (error), tham khảo phần troubleshoot để debug và gỡ lỗi.

```
[root@oracle7 ~]# service auditd restart
Stopping logging: [ OK ]
Redirecting start to /bin/systemctl start auditd.service
[root@oracle7 ~]# systemctl enable auditd
[root@oracle7 ~]# systemctl status auditd
• auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-09-18 00:18:32 +07; 16s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Main PID: 11105 (auditd)
   CGroup: /system.slice/auditd.service
           └─11105 /sbin/auditd

Sep 18 00:18:32 oracle7 augenrules[11109]: lost 0
Sep 18 00:18:32 oracle7 augenrules[11109]: backlog 1
Sep 18 00:18:32 oracle7 augenrules[11109]: enabled 1
Sep 18 00:18:32 oracle7 augenrules[11109]: failure 1
Sep 18 00:18:32 oracle7 augenrules[11109]: pid 11105
Sep 18 00:18:32 oracle7 augenrules[11109]: rate_limit 0
Sep 18 00:18:32 oracle7 augenrules[11109]: backlog_limit 8192
Sep 18 00:18:32 oracle7 augenrules[11109]: lost 0
Sep 18 00:18:32 oracle7 augenrules[11109]: backlog 1
Sep 18 00:18:32 oracle7 systemd[1]: Started Security Auditing Service.
[root@oracle7 ~]#
```

Khi chọn định dạng logs là **ENRICHED** thay cho **RAW** trong tệp cấu hình **auditd.conf**, ta sẽ thu được logs đã chuyển từ dạng số sang dạng đối tượng tương ứng như sau:

```
type=SYSCALL msg=audit(1631896186.861:323): arch=c000003e syscall=2
success=yes exit=3 a0=7ffc90e5e6f7 a1=0 a2=1fffffffff0000
a3=7ffc90e5dc60 items=1 ppid=10435 pid=10870 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=6
comm="cat" exe="/usr/bin/cat"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="TT1087_Account_Discovery"

type=SYSCALL msg=audit(1631899310.780:413): arch=c000003e
syscall=2 success=yes exit=3 a0=7ffffcb75704 a1=0 a2=1fffffffff0000
a3=7ffffcb73160 items=1 ppid=10435 pid=11155 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=6
comm="cat" exe="/usr/bin/cat"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="TT1087_Account_Discovery" ARCH=x86_64 SYSCALL=open
AUID="root" UID="root" GID="root" EUID="root" SUID="root"
FSUID="root" EGID="root" SGID="root" FSGID="root"
```

3.1.2. Cấu hình dịch vụ rsyslog

Để đẩy toàn bộ logs thu được bởi dịch vụ **auditd** về hệ thống SIEM-Qradar, sử dụng dịch vụ **rsyslog**. Theo mặc định, dịch vụ này đã được cài đặt trên các bản phân phối linux, cụ thể là Ubuntu 16.04 trở lên, CentOS6 trở lên, RHEL 7.x/8.x.

Bước 1: Kiểm tra cấu hình dịch vụ **rsyslog**

Để kiểm tra phiên bản dịch vụ **rsyslog** đã được cài đặt và trạng thái của dịch vụ, trên hệ điều hành CentOS/RHEL, sử dụng lệnh:

```
$ sudo rpm -qa | grep rsyslog
$ sudo systemctl status rsyslog
```

Kết quả như hình minh họa bên dưới, cho thấy dịch vụ **rsyslog** đang chạy bình thường.

```
[root@oracle7 audit]# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-09-17 19:38:15 +07; 4h 52min ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
   Main PID: 1100 (rsyslogd)
    CGroup: /system.slice/rsyslog.service
            └─1100 /usr/sbin/rsyslogd -n

Sep 17 19:38:00 oracle7 systemd[1]: Starting System Logging Service...
Sep 17 19:38:15 oracle7 rsyslogd[1100]: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="1100" x-info="http://w..."] start
Sep 17 19:38:15 oracle7 systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@oracle7 audit]#
```

Bước 2: Cấu hình **rsyslog** đẩy logs trên máy chủ về Qradar

Để cấu hình đẩy logs trên máy chủ linux về hệ thống SIEM-Qradar, cần bổ sung địa chỉ IP và cổng của Qradar Log Collector vào tệp cấu hình **/etc/rsyslog.conf**. Theo mặc định, thường sử dụng cổng **514/UDP**. Trước khi thực hiện thay đổi tệp **/etc/rsyslog.conf**, cần thực hiện sao chép cấu hình hiện tại của dịch vụ.

```
$ sudo cp /etc/rsyslog.conf /etc/rsyslog.conf.bak
```

Sử dụng một trong các trình editor như nano, ... để sửa tệp cấu hình **rsyslog.conf**. Đảm bảo dòng cấu hình sau tồn tại và không ở trạng thái bị comment (#) trong tệp cấu hình.

```
$IncludeConfig /etc/rsyslog.d/*.conf
```

Thêm địa chỉ IP của Qradar dùng để thu thập logs vào cuối tệp cấu hình **rsyslog.conf** và lưu lại.

```
.* @x.x.x.x:514
```

Khi đó, logs trên máy chủ linux sẽ được gửi tới Qradar Log Collector tại địa chỉ x.x.x.x (thay đổi thông số cho phù hợp với hệ thống Qradar của C06) thông qua cổng 514/UDP. Nếu sử dụng *.* @@IP_LogCollector:514 thì log sẽ được đẩy về thông qua cổng 514/TCP.

Bước 3: Cấu hình rsyslog đẩy logs dịch vụ audit

Để cấu hình đẩy logs của dịch vụ auditd về hệ thống SIEM-Qradar, cần thực hiện sao chép tệp **rsyslog_auditd.conf** đã được GTSC-A05 xây dựng vào thư mục **/etc/rsyslog.d/**. Trước khi thực hiện, cần tạo bản sao cho tệp cấu hình **rsyslog_auditd.conf** nếu nó đã tồn tại trong thư mục. Thực hiện các lệnh sau:

```
$ sudo cp /etc/rsyslog.d/rsyslog_auditd.conf /etc/rsyslog.d/rsyslog_auditd.conf.bak
$ sudo cp conf/rsyslog_auditd.conf /etc/rsyslog.d/
```

Khởi động lại dịch vụ **rsyslog** và kiểm tra trạng thái của dịch vụ

```
$ sudo systemctl restart rsyslog
$ sudo systemctl status rsyslog
```

Kết quả, nhận được thông báo lỗi mô-đun imfile của dịch vụ rsyslog khi đọc tệp **audit.log** trong thư mục **/var/log/audit/audit.log**. Gõ lệnh **\$ sudo systemctl status rsyslog -l** để xem chi tiết về lỗi.

```
[root@oracle7 ~]# sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-09-18 00:53:40 +07; 21s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
  Main PID: 11285 (rsyslogd)
    CGroup: /system.slice/rsyslog.service
            └─11285 /usr/sbin/rsyslogd -n

Sep 18 00:53:25 oracle7 systemd[1]: Stopped System Logging Service.
Sep 18 00:53:25 oracle7 systemd[1]: Starting System Logging Service...
Sep 18 00:53:40 oracle7 rsyslogd[11285]: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="11285" x-info="http://..."] start
Sep 18 00:53:40 oracle7 rsyslogd[11285]: imfile: on startup file '/var/log/audit/audit.log' does not exist but is configured...52.el7]
Sep 18 00:53:40 oracle7 systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
```

Kết quả, nhận được thông báo lỗi như sau;

```
Sep 18 00:53:40 oracle7 rsyslogd[11285]: imfile: on startup file
'/var/log/audit/audit.log' does not exist but is configured in static file
monitor - this may indicate a misconfiguration. If the file appears at a
```

```
later time, it will automatically be processed. Reason: Permission denied
[v8.24.0-52.el7]
```

Kiểm tra logs trong `/var/log/audit/audit.log`, ta thấy sự kiện sau đã được ghi lại

```
type=AVC msg=audit(1631936911.402:1355): avc: denied { search } for
pid=1094 comm="in:imfile" name="audit" dev="dm-0" ino=34340936
scontext=system_u:system_r:syslogd_t:s0
tcontext=system_u:object_r:auditd_log_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1631936916.409:1356): avc: denied { getattr } for
pid=1094 comm="in:imfile" path="/var/log/audit" dev="dm-0"
ino=34340936 scontext=system_u:system_r:syslogd_t:s0
tcontext=system_u:object_r:auditd_log_t:s0 tclass=dir permissive=0
```

Lỗi này do tính năng **SELinux** trên một số hệ điều hành đã được kích hoạt để ngăn hành vi đọc các tệp logs ngoài phạm vi (scope) được cấp cho dịch vụ. Để sửa lỗi này, thực hiện các bước sau:

+) Kiểm tra trạng thái của dịch vụ **SELinux**

```
$ getenforce
```

Kết quả trả về một trong 3 trạng thái sau:

- **Enforcing**: SELinux đang hoạt động và chặn các hành động không phù hợp với chính sách đã thiết lập
- **Permissive**: SELinux vẫn hoạt động nhưng không chặn các hành động vi phạm chính sách đã thiết lập, mà chỉ ghi lại logs cho biết hành vi đó đã được thực hiện
- **Disable**: SELinux đã bị vô hiệu hóa

+) Kiểm tra một số cấu hình hiện tại của dịch vụ SELinux

```
$ sudo sestatus
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
```

```
Policy deny_unknown status: allowed
Max kernel policy version: 31
```

+) Bổ sung SELinux Policy cho phép rsyslog đọc logs của dịch vụ auditd

```
# Cài đặt thêm một số mô-đun cho phép cấu hình SELinux Policy
$ sudo yum install checkpolicy policycoreutils-python -y

# Nếu máy chủ không có Internet, sử dụng rpm để cài đặt
$ sudo rpm -ivh setup/checkpolicy-2.5-8.el7.x86_64.rpm
$ sudo rpm -ivh setup/policycoreutils-python-2.5-34.el7.x86_64.rpm

# Cấu hình SELinux policy
$ sudo checkmodule -M -m -o setup/rsyslog.mod setup/rsyslog.te
$ sudo semodule_package -o setup/rsyslog.pp -m setup/rsyslog.mod
$ sudo semodule -i setup/rsyslog.pp
$ sudo semodule -d rsyslog
$ sudo semodule -e rsyslog
```

+) Khởi động lại dịch vụ rsyslog và kiểm tra trạng thái của các dịch vụ

```
$ sudo sestatus
$ sudo systemctl restart rsyslog
$ sudo systemctl status rsyslog
```

Tham khảo cấu hình SELinux tại liên kết:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/writing-a-custom-selinux-policy_using-selinux

Kết quả ta thấy dịch vụ rsyslog đã

```
[root@oracle7 auditd_config]# setools-console
-bash: setools-console: command not found
[root@oracle7 auditd_config]# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-09-18 14:58:45 +07; 18min ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
   Main PID: 1979 (rsyslogd)
    CGroup: /system.slice/rsyslog.service
            └─1979 /usr/sbin/rsyslogd -n

Sep 18 14:58:30 oracle7 systemd[1]: Stopped System Logging Service.
Sep 18 14:58:30 oracle7 systemd[1]: Starting System Logging Service...
Sep 18 14:58:45 oracle7 rsyslogd[1979]: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="1979" x-inf... start
Sep 18 14:58:45 oracle7 systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@oracle7 auditd_config]#
```


Chú ý: Trong trường hợp đã cấu hình đẩy logs theo hướng dẫn và vẫn thấy báo lỗi ở dịch vụ rsyslog không đọc được logs auditd, cần kiểm tra lại cấu hình trong tệp **rsyslog.conf** và comment lại một số dòng cấu hình sau. Sau đó, thực hiện restart lại dịch vụ rsyslog bằng tài khoản có quyền root và kiểm tra lại.

```
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
#$PrivDropToUser syslog
$PrivDropToGroup syslog
```

Bước 4: Kiểm tra kết nối của dịch vụ **rsyslog**. Chạy lệnh sau:

```
$ sudo ss -tulnp | grep "rsyslog"
```

```
udp      UNCONN      0      0      *:53700      *.*
users:(("rsyslogd",pid=1979,fd=10))
```

Kết quả trả về như vậy cho biết dịch vụ rsyslog đang dùng kết nối UDP để đẩy logs từ máy chủ Linux về hệ thống SIEM-Qradar.

Chú ý 1: Trên một số máy chủ như **CentOS, RHEL**, nếu chạy dịch vụ **SELinux** thì có thể cần chạy một số lệnh sau để cho phép lưu lượng của dịch vụ **rsyslog** được gửi đi qua network socket trên máy chủ.

```
$ sudo semanage -a -t syslogd_port_t -p udp 514
$ sudo semanage -a -t syslogd_port_t -p tcp 514
```

Trong một số trường hợp, nếu dịch vụ tường lửa trên máy chủ (firewalld, ufw, ...) được bật, cần mở cổng **514** để cho phép thiết lập các kết nối UDP/TCP để đẩy logs tới Log Collector của SIEM-Qradar.

```
Ubuntu:
$ sudo ufw allow 514/udp
$ sudo ufw allow 514/tcp
$ sudo ufw reload
```

CentOS:

```
$ sudo firewall-cmd --permanent --add-port=514/udp  
$ sudo firewall-cmd --permanent --add-port=514/tcp  
$ sudo firewall-cmd --reload
```

Tham khảo hướng dẫn cấu hình SELinux mở cổng kết nối tại liên kết: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s1-configuring_rsyslog_on_a_logging_server

3.1.3. Cấu hình dịch vụ logrotate

Sau khi đã cấu hình đầy thành công logs của dịch vụ auditd về hệ thống SIEM-Qradar, cần thiết lập cấu hình **logrotate** để đảm bảo logs sinh ra không làm đầy ổ cứng, ảnh hưởng tới hiệu năng của toàn bộ máy chủ.

+) Kiểm tra dịch vụ **logrotate** đã được cài đặt trên máy chủ bằng lệnh sau:

```
$ logrotate --version  
  
logrotate 3.8.6
```

Mặc định, logrotate đã được cài đặt sẵn trên các hệ điều hành Ubuntu, CentOS/RHEL, nên nếu máy chủ chưa cài đặt dịch vụ **logrotate**, có thể cài đặt theo các lệnh bên dưới.

```
Ubuntu:  
$ sudo apt-get install logrotate  
  
CentOS/RHEL:  
$ sudo yum install logrotate
```

Sau khi cài đặt thành công, một tệp cấu hình sẽ được tạo trong thư mục **/etc** để kiểm soát các hành vi của tiện ích này khi chạy. Đồng thời, một **cron job** chạy hằng ngày được tạo ra để chạy tiện ích này.

+) Kiểm tra dịch vụ logrotate

```
$ sudo ls /etc/cron.daily/  
logrotate man-db.cron
```

Cấu hình tệp **/etc/logrotate.conf** để thiết lập chính sách rotate cho logs. Đảm bảo tệp cấu hình bao gồm những dòng sau:

```
include /etc/logrotate.d
```

Kết quả sẽ hiển thị như hình minh họa

```
[root@oracle7 ~]# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.
```

Chú ý: Trước khi thay đổi tệp cấu hình `/etc/logrotate.conf`, cần tạo bản sao cho cấu hình hiện tại của dịch vụ **logrotate**.

```
$ sudo cp /etc/logrotate.conf /etc/logrotate.conf.bak
```

Để cấu hình rotate logs cho dịch vụ **auditd**, cần tạo sao chép tệp **logrotate_auditd** đã được GTSC-A05 xây dựng vào thư mục `/etc/logrotate.d`. Trước khi thực hiện, cần tạo bản sao cho các tệp cấu hình hiện tại (nếu có).

```
$ sudo cp /etc/logrotate.d/logrotate_auditd
/etc/logrotate.d/logrotate_auditd.bak
$ sudo cp conf/logrotate_auditd /etc/logrotate.d/logrotate_auditd
```

Logrotate sử dụng **crontab** để lập lịch chạy, do vậy sau khi thêm mới tệp cấu hình, không cần reload lại dịch vụ. Khi crontab thực thi, logrotate sẽ tự động sử dụng các tệp cấu hình mới. Để kiểm tra cấu hình, sử dụng lệnh sau:

```
$ sudo logrotate /etc/logrotate.d/logrotate_auditd
```

Chi tiết file cấu hình **logrotate_auditd**

```
/var/log/audit/*.log {  
    weekly  
    rotate 4  
    size 30M  
    compress  
    missingok  
}
```

Trong tệp cấu hình logrotate, có một số tham số sau:

- **/var/log/audit/*.log**: Các tệp log nằm trong thư mục cần rotate
- **weekly**: Các job được chạy hằng tuần
- **size 30M**: Thực hiện rotate khi các tệp tin có kích thước lớn hơn 30Mb
- **compress**: Thực hiện nén tệp rotate, mặc định sẽ sử dụng **gzip**
- **missingok**: Bỏ qua trong trường hợp tệp log không tồn tại

Chú ý: Người quản trị có thể tùy chỉnh các thông số trong tệp cấu hình logrotate của osquery, tùy thuộc vào hệ thống thực tế đang giám sát. Ví dụ, như tăng / giảm ngưỡng dung lượng tối đa của tệp logs, tăng / giảm số tệp tin sẽ được rotate.

Chi tiết tham khảo liên kết: <https://linux.die.net/man/8/logrotate>

3.2. Cấu hình nhận logs auditd trên Qradar

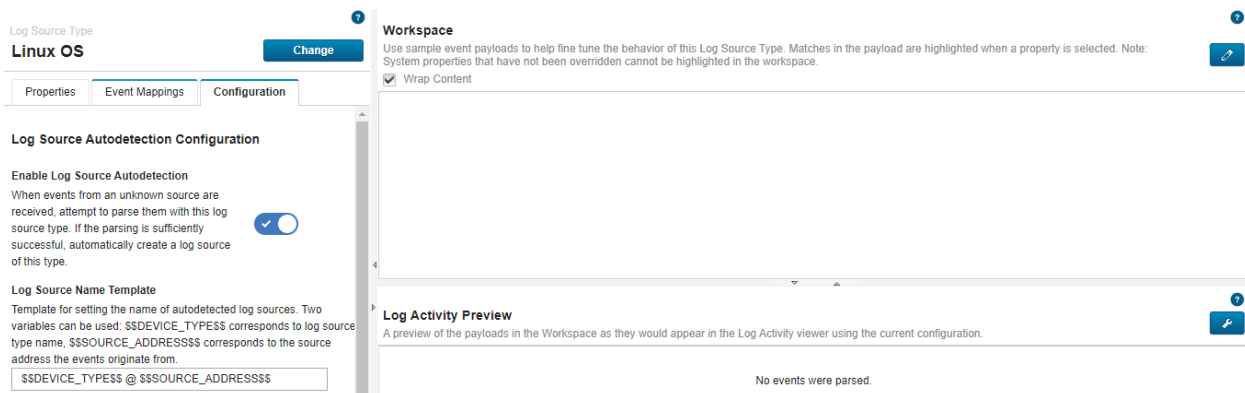
Trên Qradar, hay các SIEM khác nói chung mặc định đều hỗ trợ giao thức **Syslog**, cho phép lắng nghe trên cổng 514/UDP và 514/TCP. Ngoài ra, có thể sử dụng giao thức **TLS Syslog** lắng nghe trên cổng 6514/TCP để thiết lập các kết nối gửi và nhận logs an toàn. Trên Qradar, ta sẽ sử dụng Log Source Type là **Linux OS** và giao thức **Syslog** để nhận và quản lý logs từ các máy chủ Linux đẩy về.

❖ Cấu hình tự động tạo Log Source cho các máy chủ Linux

Bước 1: Trên giao diện quản trị Qradar, truy cập **Admin > Data Sources > Events > DSM Editor** để vào giao diện cấu hình Log Source

Bước 2: Chọn Log Source Type là **Linux OS** để quản lý logs cho các máy chủ Linux

Bước 3: Trong phần **Configuration**, chọn **Enable Log Source Automation** để tự động tạo Log Source mỗi khi nhận logs thông qua giao thức Syslog.



Chọn **Save** để lưu lại và chọn **Close** để thoát.

+) Kết quả, Qradar sẽ tự động tạo Log Source mới cho các máy chủ Linux khi nhận được logs thông qua giao thức Syslog.

Theo mặc định, nếu máy chủ linux đang đẩy logs theo Log Source Type là Linux OS thì nó sẽ tiếp tục đẩy audit logs vào log source đó.

❖ Cấu hình tạo Log Source thủ công trên Qradar

Trong một vài trường hợp, có thể do Qradar không được cấu hình chế độ tự động tạo Log Source, hoặc do có vấn đề nào đó phát sinh trong khi vận hành, ta cần phải tạo Log Source thủ công để nhận và quản lý log của máy chủ linux. Khi đó, ta thực hiện các bước sau:

Bước 1: Trên giao diện quản trị Qradar, truy cập **Admin > Apps > Qradar Log Source Management** để vào giao diện quản lý Log Source. Chọn **New Log Source** để tạo mới một Log Source cho máy chủ Linux.

Bước 2: Trong phần Log Source Type, chọn Linux OS

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Select a Log Source type

linu

Linux DHCP Server

Linux OS

Linux iptables Firewall

Bước 3: Trong phần Protocol, chọn Syslog

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Select a protocol type

Look up Protocol Type

Forwarded

Syslog

Bước 4: Cấu hình thông số cho Log Source. Chi tiết ý nghĩa của chúng được mô tả trong bảng bên dưới

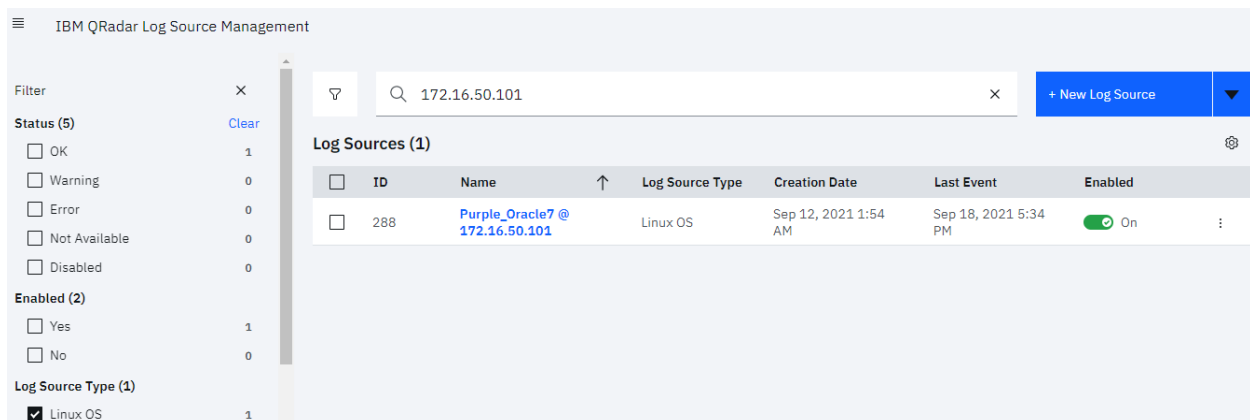
Thông số	Ý nghĩa
Name	Ví dụ Oracle 7 @ 172.16.50.101 Định danh cho Log Source. Thường đặt theo tên Hostname @ IP
Description	Mô tả tóm tắt ý nghĩa của log source
Enabled	Tích chọn để kích hoạt log source cho phép nhận logs
Groups	Chọn nhóm quản lý Log Source
Extension	Chọn Log Source Extensions nếu có để cho phép xử lý các sự kiện, trong trường hợp cấu hình parser bị lỗi
Language	Ví dụ: English Chọn ngôn ngữ sử dụng trong các sự kiện thu được của log source
Target Event Collector	Ví dụ: eventcollector0::localhost Chọn Log Collector cho phép nhận logs
Credibility	Ví dụ: 5 Chọn độ tin cậy cho Log Source

Coalescing Events	Bỏ chọn Cho phép gộp nhiều sự kiện vào và chỉ lấy một vài sự kiện để giảm EPS và giảm lượng logs cần lưu trữ. Tuy nhiên, điều này có thể gây mất logs
Store Event Payloads	Tích chọn Cho phép lưu lại các sự kiện để có thể search trên Qradar
Log Source Identifier	Ví dụ: oracle7 Giá trị dùng để Qradar định danh và phân loại logs vào các log source tương ứng. Thường sử dụng IP, hoặc hostname. Trong trường hợp này, để nhận logs của dịch vụ audit, cần sử dụng hostname của máy chủ linux
Incoming Payload Encoding	Ví dụ: UTF-8 Chuẩn mã hóa hỗ trợ cho payload

Sau đó, chọn **Finish** để kết thúc quá trình cấu hình.

Bước 5: Truy cập giao diện quản trị của Qradar, chọn **Admin > Deploy Changes** để áp dụng cấu hình mới. Chờ một vài phút để quá trình thiết lập cấu hình mới hoàn tất.

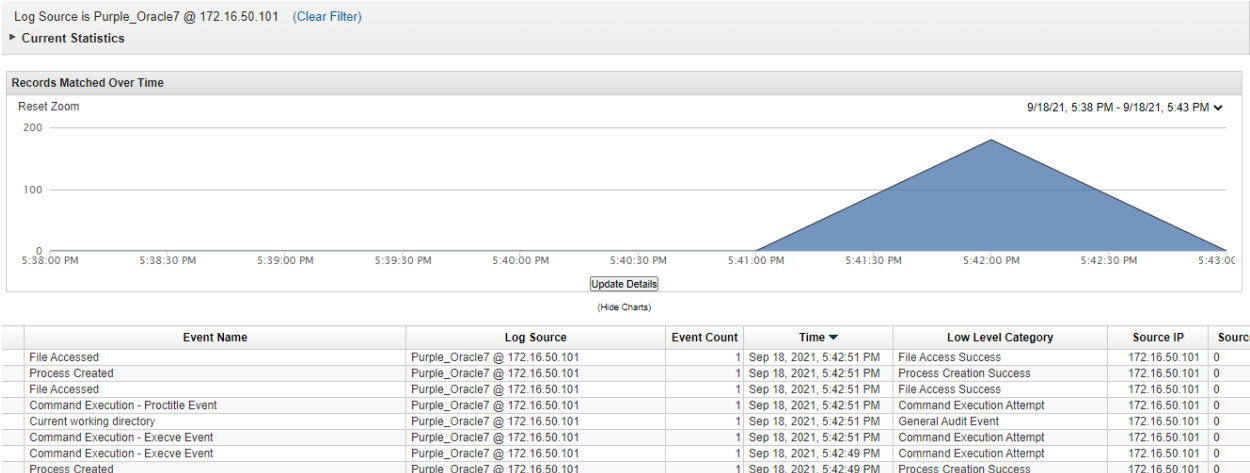
Trên Log Source Management, kết quả hiển thị như hình bên dưới cho thấy Log Source đã nhận được logs đầy về từ máy chủ Linux.



The screenshot shows the IBM QRadar Log Source Management interface. On the left, there are filters for Status (5) and Log Source Type (1). The main area displays a table of Log Sources (1) with the following details:

ID	Name	Log Source Type	Creation Date	Last Event	Enabled
288	Purple_Oracle7 @ 172.16.50.101	Linux OS	Sep 12, 2021 1:54 AM	Sep 18, 2021 5:34 PM	On

Kiểm tra chi tiết log source, ta thấy như hình minh họa bên dưới cho thấy log của dịch vụ auditd đã được đẩy về Qradar.



Kích vào xem một sự kiện, ta sẽ được kết quả như bên dưới. Trong đó, log của dịch vụ auditd sẽ được gắn thêm thẻ (tag) là audit_log vào phần Header, trước nó là thẻ oracle7 là hostname của máy chủ linux.

Source and Destination Information			
Source IP	172.16.50.101	Destination IP	172.16.50.101
Source Asset Name	172.16.50.101	Destination Asset Name	172.16.50.101
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information	
utf hex base64	
<input checked="" type="checkbox"/> Wrap Text	
<pre>182>Sep 18 17:41:09 oracle7 audit_log node=oracle7 type=PATH msg=audit(1631961669.852:5276): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=268436354 dev=fc:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:ld_so_t:s0 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0000000000000000 OUID="root" OGID="root"</pre>	

4. Hướng dẫn Troubleshoot

4.1. Cấu hình dịch vụ auditd

Các tệp cấu hình **auditd.conf** cho dịch vụ auditd có thể khác nhau, tùy thuộc vào bản phân phối linux sử dụng. Mặc định, nó nằm tại đường dẫn **/etc/audit/auditd.conf**

Trong tệp cấu hình, các dòng trống, hoặc các dòng bắt đầu bởi ký tự **#** sẽ bị bỏ qua. Để đáp ứng một số chính sách an toàn thông tin trên máy chủ, có thể xem xét thay đổi một số tham số sau:

Tham số	Ý nghĩa
log_file	Đường dẫn thư mục lưu trữ logs của dịch vụ audit. Theo mặc định, thường nằm trong thư mục /var/log/audit/
max_log_file	Kích thước tối đa của một tệp logs được lưu trữ. Ví dụ, max_log_file = 8 thì tệp logs sẽ có kích thước tối đa là 8 MB
max_log_file_action	Hành động sẽ được thực hiện khi tệp logs đạt kích thước tối hạn max_log_file (đã thiết lập ở trên). Ví dụ chọn keep_logs để ngăn tệp audit.logs bị ghi đè, chọn ROTATE để ghi backup tệp logs hiện tại và tạo tệp mới để tiếp tục ghi logs
space_left	Chỉ định dung lượng trống (free space) còn lại trên ổ cứng để kích hoạt hành động được thiết lập trong space_left_action . Giá trị này cần thiết lập phù hợp để người quản trị có thời gian kiểm tra và thực hiện giải phóng dung lượng ổ cứng. Nó phụ thuộc vào tốc độ sinh tệp audit.logs
space_left_action	Nên thiết lập thành email , hoặc exec để cung cấp cách thức thông báo phù hợp
admin_space_left	Chỉ định dung lượng còn lại tối thiểu trên ổ cứng để kích hoạt hành động được thiết lập trong admin_space_left_action . Giá trị này cần được thiết lập để đủ không gian ghi lại nhật ký các hành động do người quản trị thực hiện
admin_space_left_action	Nên thiết lập thành single để đưa hệ thống về chế độ một người dùng (single-user) và cho phép người quản trị giải phóng dung lượng ổ đĩa
disk_full_action	Chỉ định hành động được kích hoạt khi không còn dung lượng trống trên phân vùng chứa audit logs, nên thiết lập thành half hoặc single . Điều này đảm bảo rằng hệ thống đang tắt, hoặc đang hoạt động ở chế độ một người dùng khi dịch vụ audit không còn khả năng ghi thêm logs

disk_error_action	Chỉ định hành động được kích hoạt trong trường hợp phát sinh lỗi trên phân vùng chứa các tệp audit logs. Nên đặt hành syslog , single hoặc half phụ thuộc vào chính sách bảo mật cục bộ của tổ chức liên quan đến việc xử lý các lỗi phần cứng
flush	Nên đặt thành incremental_async . Nó hoạt động kết hợp với tham số freq để xác định số lượng bản ghi có thể được gửi đến đĩa trước khi buộc phải đồng bộ với ổ cứng. Tham số freq thường được đặt thành 100. Chúng đảm bảo dữ liệu về các sự kiện audit sẽ được đồng bộ với tệp audit logs trên ổ đĩa, trong khi vẫn giữ hiệu suất tốt cho toàn bộ hoạt động
log_format	Cho biết cách thức thông tin được lưu trữ trên ổ đĩa. Có 2 tùy chọn là raw và enriched . Nếu chọn raw , các bản ghi sẽ được lưu ở định dạng giống như kết quả nhận được từ kernel. Nếu chọn ENRICHED sẽ cho phép chuyển đổi tất cả thông tin về uid , gid , syscall , architecture và địa chỉ socket trước khi ghi sự kiện vào tệp logs. Điều này sẽ giúp dễ dàng nắm thông tin trong các sự kiện khi logs được đẩy về hệ thống khác. Chú ý tùy chọn NOLOG hiện không được sử dụng nữa
q_depth	Có trên bản Auditd 3.0/RHEL 8.x Độ lớn hàng đợi nội bộ (internal queue) của audit event dispatcher. Hàng đợi kích thước lớn cho phép xử lý nhiều sự kiện tốt hơn, nhưng có thể giữ các sự kiện không được xử lý khi daemon kết thúc. Nếu hệ thống thông báo bị mất các sự kiện (event), cần tăng giá trị này lên. Mặc định giá trị này là 1200

Sau khi thay đổi cấu hình, cần khởi động lại dịch vụ **auditd** để áp dụng cấu hình mới. Chạy lệnh **\$ sudo service auditd restart**

Tham khảo: <https://man7.org/linux/man-pages/man5/auditd.conf.5.html>

4.2. Cấu hình dịch vụ rsyslog

❖ Lỗi dịch vụ **rsyslog** không đọc được tệp audit log

+) kiểm tra trạng thái của dịch vụ **rsyslog** và nhận thông báo lỗi như sau:

```
$ sudo systemctl status rsyslog
```

Kết quả, nhận được thông báo lỗi mô-đun imfile của dịch vụ rsyslog khi đọc tệp **audit.log** trong thư mục **/var/log/audit/audit.log**. Gõ lệnh **\$ sudo systemctl status rsyslog -l** để xem chi tiết về lỗi.

```
[root@oracle7 ~]# sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-09-18 00:53:40 +07; 21s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
   Main PID: 11285 (rsyslogd)
    CGroup: /system.slice/rsyslog.service
            └─11285 /usr/sbin/rsyslogd -n

Sep 18 00:53:25 oracle7 systemd[1]: Stopped System Logging Service.
Sep 18 00:53:25 oracle7 systemd[1]: Starting System Logging Service...
Sep 18 00:53:40 oracle7 rsyslogd[11285]: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="11285" x-info="http://..."] start
Sep 18 00:53:40 oracle7 rsyslogd[11285]: imfile: on startup file '/var/log/audit/audit.log' does not exist but is configured...52.el7]
Sep 18 00:53:40 oracle7 systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
```

Kết quả, nhận được thông báo lỗi như sau;

```
Sep 18 00:53:40 oracle7 rsyslogd[11285]: imfile: on startup file
'/var/log/audit/audit.log' does not exist but is configured in static file
monitor - this may indicate a misconfiguration. If the file appears at a
later time, it will automatically be processed. Reason: Permission denied
[v8.24.0-52.el7]
```

Kiểm tra logs trong **/var/log/audit/audit.log**, ta thấy sự kiện sau đã được ghi lại

```
type=AVC msg=audit(1631936911.402:1355): avc: denied { search } for
pid=1094 comm="in:imfile" name="audit" dev="dm-0" ino=34340936
scontext=system_u:system_r:syslogd_t:s0
tcontext=system_u:object_r:auditd_log_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1631936916.409:1356): avc: denied { getattr } for
pid=1094 comm="in:imfile" path="/var/log/audit" dev="dm-0"
ino=34340936
scontext=system_u:system_r:syslogd_t:s0
tcontext=system_u:object_r:auditd_log_t:s0 tclass=dir permissive=0
```

Lỗi này do tính năng **SELinux** trên một số hệ điều hành đã được kích hoạt để ngăn hành vi đọc các tệp logs ngoài phạm vi (scope) được cấp cho dịch vụ. Để sửa lỗi này, thực hiện các bước sau:

+) Kiểm tra trạng thái của dịch vụ SELinux

```
$ getenforce
```

Kết quả trả về một trong 3 trạng thái sau:

- **Enforcing**: SELinux đang hoạt động và chặn các hành động không phù hợp với chính sách đã thiết lập
- **Permissive**: SELinux vẫn hoạt động nhưng không chặn các hành động vi phạm chính sách đã thiết lập, mà chỉ ghi lại logs cho biết hành vi đó đã được thực hiện
- **Disable**: SELinux đã bị vô hiệu hóa

+) Kiểm tra một số cấu hình hiện tại của dịch vụ SELinux

```
$ sudo sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Max kernel policy version:    31
```

+) Bổ sung cấu hình SELinux Policy cho phép rsyslog đọc logs của dịch vụ auditd. Tập cấu hình **rsyslog.te** đã được GTSC-A05 xây dựng đặt trong thư mục conf.

```
# Cài đặt thêm một số mô-đun cho phép cấu hình SELinux Policy
$ sudo yum install checkpolicy policycoreutils-python -y

# Nếu máy chủ không có Internet, sử dụng rpm để cài đặt
$ sudo rpm -ivh setup/checkpolicy-2.5-8.el7.x86_64.rpm
$ sudo rpm -ivh setup/policycoreutils-python-2.5-34.el7.x86_64.rpm

# Cấu hình SELinux policy
$ sudo checkmodule -M -m -o setup/rsyslog.mod setup/rsyslog.te
$ sudo semodule_package -o setup/rsyslog.pp -m setup/rsyslog.mod
$ sudo semodule -i setup/rsyslog.pp
```

```
$ sudo semodule -d rsyslog
$ sudo semodule -e rsyslog
```

+) Khởi động lại dịch vụ rsyslog và kiểm tra trạng thái của các dịch vụ

```
$ sudo systemctl restart rsyslog
$ sudo systemctl status rsyslog
```

Tham khảo cấu hình SELinux tại liên kết:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/writing-a-custom-selinux-policy_using-selinux

Kết quả ta thấy dịch vụ rsyslog đã

```
[root@oracle7 auditd_config]# setools-console
-bash: setools-console: command not found
[root@oracle7 auditd_config]# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-09-18 14:58:45 +07; 18min ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
   Main PID: 1979 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─1979 /usr/sbin/rsyslogd -n

Sep 18 14:58:30 oracle7 systemd[1]: Stopped System Logging Service.
Sep 18 14:58:30 oracle7 systemd[1]: Starting System Logging Service...
Sep 18 14:58:45 oracle7 rsyslogd[1979]: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="1979" x-inf... start
Sep 18 14:58:45 oracle7 systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@oracle7 auditd_config]#
```

❖ Lỗi dịch vụ **rsyslog** không tạo được kết nối TCP trên cổng 514 đẩy logs về Qradar

Thêm dòng ***.* @IP_Qradar_Log_Collector:514** vào tệp **/etc/rsyslog.conf** để cấu hình dịch vụ rsyslog đẩy logs thông qua cổng 514/TCP. Tuy nhiên, không thấy có kết nối được khởi tạo.

```
$ ss -tunlp | grep rsyslog
```

Kiểm tra dịch vụ SELinux đang được chạy không ? Trên một số máy chủ như **CentOS, RHEL** dịch vụ này mặc định đã được kích hoạt để phát hiện và ngăn chặn các hành vi có thể làm mất an toàn thông tin cho máy chủ.

```
$ sudo sestatus
```

SELinux status: enabled

```
SELinuxfs mount:      /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name:    targeted
Current mode:          enforcing
Mode from config file: enforcing
Policy MLS status:     enabled
Policy deny_unknown status: allowed
Max kernel policy version: 31
```

Kết quả trên cho thấy dịch vụ SELinux đang được kích hoạt. Tiếp tục kiểm tra các cổng kết nối đang được mở cho dịch vụ rsyslog

```
$ sudo semanage port -l | grep 514
cluster_port_t      tcp    5149, 40040, 50006-50008
cluster_port_t      udp    5149, 50006-50008
rsh_port_t          tcp    514
syslog_tls_port_t   tcp    6514, 10514
syslog_tls_port_t   udp    6514, 10514
syslogd_port_t      tcp    601, 20514
syslogd_port_t      udp    514, 601, 20514
virt_port_t         tcp    16509, 16514
virt_port_t         udp    16509, 16514
```

Kết quả trên cho thấy máy chủ đã mở cổng kết nối 514/TCP. Do vậy, chỉ cần kiểm tra lại trên hệ thống Qradar đã nhận được logs từ địa chỉ IP của máy chủ là được. Nếu cổng 514/TCP và 514/UDP chưa được mở, chạy một số lệnh sau:

```
$ sudo semanage port -a -t syslogd_port_t -p udp 514
$ sudo semanage port -a -t syslogd_port_t -p tcp 514
```

Trong một số trường hợp, nếu dịch vụ tường lửa trên máy chủ (firewalld, ufw, ...) được bật, cần mở cổng **514** để cho phép thiết lập các kết nối **UDP/TCP** để đẩy logs tới Log Collector của SIEM-Qradar.

```
Ubuntu:
$ sudo ufw allow 514/udp
$ sudo ufw allow 514/tcp
$ sudo ufw reload

CentOS:
$ sudo firewall-cmd --permanent --add-port=514/udp
```

```
$ sudo firewall-cmd --permanent --add-port=514/tcp
$ sudo firewall-cmd --reload
```

Tham khảo cấu hình SELinux mở cổng kết nối tại liên kết: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s1-configuring_rsyslog_on_a_logging_server

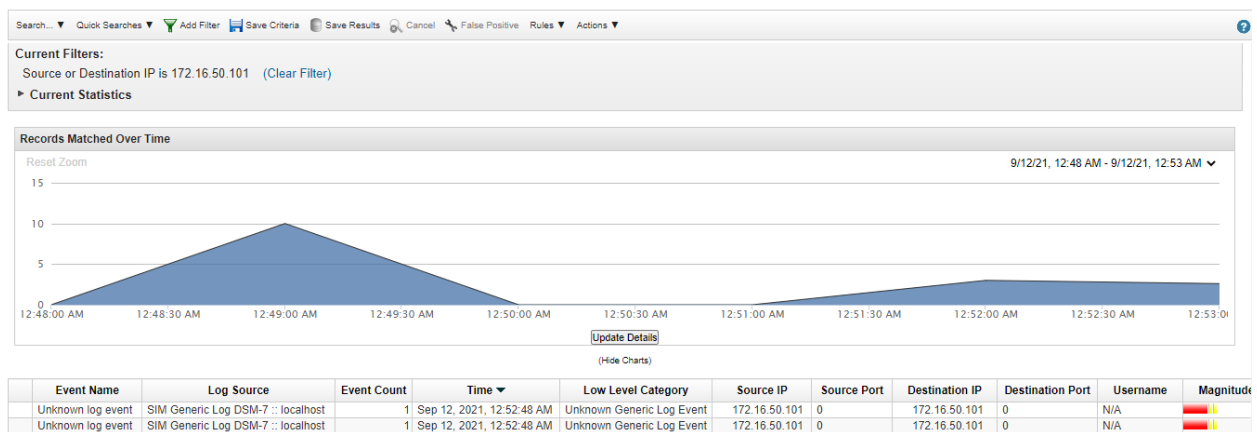
4.3. Cấu hình Log Source

Sau khi cấu hình dịch vụ rsyslog trên máy chủ linux để đẩy audit logs về Qradar, nếu trên Qradar đã nhận log source, tuy nhiên không xem được audit logs, thì ta cần kiểm tra lại như sau:

Bước 1: Trên giao diện Qradar, chọn **Log Activity** để truy cập tính năng Search các sự kiện

Chọn **Add Filter**, chọn Parameter là **Source or Destination IP**, chọn Operator là **Equals** và nhập Value là 172.16.50.101 (địa chỉ IP đang kiểm tra đẩy logs).

Kết quả trả về các sự kiện có Event Name là **Unknown log event**, thuộc Log Source là **SIM Generic Log DSM-7::localhost**, cho thấy logs đã đẩy về Qradar, nhưng không được xử lý bởi Log Source.



Bước 2: Cấu hình Log Source

Trên giao diện Qradar, truy cập **Admin > Apps > Log Source Management**, chọn Log Source tương ứng và chọn **Edit**. Nhập lại giá trị Log Source Identifier là **hostname** của máy chủ linux. Chọn **Save** để lưu lại.

5. Xây dựng script tự động cấu hình cho C06

Theo khảo sát ban đầu, hiện nay phía C06 đang sử dụng chủ yếu là các máy chủ Oracle Linux, chạy hệ điều hành RHEL 7.8 và RHEL 8.3. Trên các bản phân phối này mặc định đã được cài đặt và kích hoạt một số dịch vụ sau:

- Dịch vụ auditd. Trên máy chủ RHEL 7.8 sử dụng auditd-2.8 và trên máy chủ RHEL 8.3 sử dụng auditd-3.0
- Dịch vụ rsyslog để cấu hình đẩy logs
- Dịch vụ logrotate để cấu hình rotate audit logs tránh đầy ổ cứng
- Kích hoạt SELinux để chặn các hành vi vi phạm chính sách đã được thiết lập

Do vậy, phía GTSC-A05 sẽ xây dựng script cho phép tự động cấu hình dịch vụ auditd và cấu hình đẩy logs trên máy chủ linux về Qradar thông qua dịch vụ rsyslog. Trong script sẽ thực hiện thay đổi thiết lập một số cấu hình, mà không cài đặt thêm bất kỳ dịch vụ nào khác, tránh ảnh hưởng đến các máy chủ đang cung cấp dịch vụ.

Về nội dung, phía GTSC-A05 sẽ cung cấp một số tệp cấu hình, tệp thực thi sau;

- Tệp **audit.rules**: Chứa các rules đã được xây dựng sẵn, cho phép sinh đủ logs phục vụ quá trình giám sát an toàn thông tin trên máy chủ linux
- Tệp **rsyslog_auditd.conf**: Chứa cấu hình dịch vụ rsyslog cho phép đẩy audit logs về hệ thống SIEM-Qradar. Mặc định sử dụng giao thức UDP, trên cổng 514
- Tệp **logrotate_auditd**: Chứa cấu hình dịch vụ logrotate cho phép rotate lại audit logs định kỳ (một tuần) để tránh làm đầy bộ nhớ
- Tệp **rsyslog.te**: Chứa cấu hình SELinux cho phép dịch vụ rsyslog đọc audit logs
- Tệp **dashboard_linux_auditd.sh** cho phép tự động cấu hình các dịch vụ để đẩy audit log về hệ thống SIEM-Qradar.

Ngoài ra, phía GTSC-A05 còn cung cấp thêm 2 tệp **checkpolicy-2.5-8.el7.x86_64.rpm** và **policycoreutils-python-2.5-34.el7.x86_64.rpm** sử dụng để cấu hình SELinux trong trường hợp máy chủ chưa được cài đặt các tiện ích này. Các tệp này đều được tải trên kho lưu trữ linux tại địa chỉ sau: <https://centos.pkgs.org/>. Để thực hiện cấu hình, người quản trị thực hiện các thao tác sau:

Bước 1: Cấp quyền thực thi cho script cài đặt

```
$ cd linux_auditd  
$ sudo chmod +x *.sh
```

Bước 2: Chuyển Windows-style line endings sang Unix-style

```
$ sudo sed -i 's/\r$//' *.sh
```

Bước 3: Chạy script cấu hình

```
$ sudo ./dashboard_linux_auditd.sh
```

Nếu có bất kỳ lỗi phát sinh, tham khảo hướng dẫn Trouble Shoot trong tài liệu này

6. Tài liệu tham khảo

- [1] Liên kết: <https://techglimpse.com/how-to-use-auditing-system-in-linux-configure-audit-logs-and-generate-reports/>
- [2] Liên kết: https://linuxhint.com/auditd_linux_tutorial/
- [3] Liên kết: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/writing-a-custom-selinux-policy_using-selinux
- [4] Liên kết: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s1-configuring_rsyslog_on_a_logging_server