

BỘ THÔNG TIN VÀ TRUYỀN THÔNG  
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÁO CÁO THỰC TẬP  
TỐT NGHIỆP ĐẠI HỌC**

**Đề tài:**

**“TÌM HIỂU VÀ TRIỂN KHAI HỆ THỐNG  
QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ  
GRAYLOG”**

Người hướng dẫn : ThS. NGUYỄN HOÀNG THÀNH  
Sinh viên thực hiện : NGUYỄN TUẤN KIỆT  
Mã số sinh viên : N18DCAT035  
Lớp : D18CQAT01-N  
Khóa : 2018 – 2023  
Hệ : ĐẠI HỌC CHÍNH QUY

TP.HCM, tháng 08 năm 2022

## **LỜI CẢM ƠN**

Lời đầu tiên, em xin phép gửi lời tri ân sâu sắc đến các thầy cô trường Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP.HCM đã tận tình dẫn dắt và truyền đạt cho em rất nhiều kiến thức quý báu trong những năm học vừa qua.

Đặc biệt, em xin gửi lời cảm ơn chân thành nhất tới ThS.Nguyễn Hoàng Thành. Thầy đã truyền đạt kiến thức, hướng dẫn em nghiên cứu và thực hành trong suốt quá trình thực hiện đề tài. Em không chỉ tiếp thu thêm được nhiều kiến thức mới mà còn học được tinh thần và thái độ làm việc nghiêm túc từ thầy. Đó sẽ là những hành trang cần thiết cho quá trình làm việc trong tương lai.

Sau cùng, em xin chúc quý thầy cô khoa Công nghệ thông tin 2 và thầy Nguyễn Hoàng Thành thật dồi dào sức khỏe để tiếp tục truyền đạt kiến thức cho thế hệ mai sau.

TP Hồ Chí Minh, ngày tháng năm 2022

**SINH VIÊN THỰC HIỆN ĐỀ TÀI**

**Nguyễn Tuấn Kiệt**

# MỤC LỤC

LỜI CẢM ƠN.....	i
DANH MỤC CÁC KÍ HIỆU VIẾT TẮT .....	iv
DANH MỤC CÁC BẢNG, SƠ ĐỒ, HÌNH.....	v
LỜI MỞ ĐẦU .....	1
CHƯƠNG 1 : TỔNG QUAN HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ .....	2
1.1. NHẬT KÝ .....	2
1.2. QUẢN LÝ NHẬT KÝ .....	3
1.3. QUẢN LÝ NHẬT KÝ TẬP TRUNG .....	3
1.4. CÁC CÔNG CỤ QUẢN LÝ NHẬT KÝ ĐƯỢC SỬ DỤNG NHƯ THẾ NÀO? .....	4
1.4.1. LOG COLLECTION .....	4
1.4.2. TỔNG HỢP NHẬT KÝ .....	6
1.4.3. PHÂN TÍCH CÚ PHÁP NHẬT KÝ .....	6
1.4.4. CHUẨN HÓA NHẬT KÝ .....	7
1.4.5. MÓI TƯƠNG QUAN CỦA CÁC SỰ KIỆN .....	9
1.4.6. PHÂN TÍCH NHẬT KÝ .....	9
1.5. NHỮNG LỢI ÍCH CHÍNH CỦA VIỆC QUẢN LÝ VÀ GIÁM SÁT NHẬT KÝ .....	9
1.5.1. GIÁM SÁT HỆ THỐNG .....	10
1.5.2. CẢNH BÁO ĐỘ TRUNG THỰC CAO .....	10
1.5.3. BẢO MẬT NÂNG CAO .....	10
1.5.4. KHẮC PHỤC SỰ CỐ NHANH HƠN .....	11
1.5.5. SỬ DỤNG TÀI NGUYÊN ĐƯỢC TỐI ƯU HÓA.....	12
1.5.6. CẢI THIỆN TƯ THẾ TUÂN THỦ.....	12
1.6. CÁC CÔNG CỤ QUẢN LÝ NHẬT KÝ ĐƯỢC SỬ DỤNG .....	12
CHƯƠNG 2: NGHIÊN CỨU HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG.....	13
2.1. KIẾN TRÚC GRAYLOG.....	13
2.2. CÁC THÀNH PHẦN CỦA GRAYLOG.....	15
2.3. CÁC TÍNH NĂNG CỦA GRAYLOG.....	16
2.3.1 THU TẬP LOG.....	16

<b>2.3.2 XỬ LÝ.....</b>	<b>17</b>
<b>2.3.3 CHUYÊN TIẾP VÀ LUU TRỮ.....</b>	<b>18</b>
CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG.....	19
<b>3.1. MÔ HÌNH TRIỂN KHAI.....</b>	<b>19</b>
<b>3.2. CÀI ĐẶT GRAYLOG-SERVER TRÊN CENTOS 7 .....</b>	<b>20</b>
<b>3.3. CẤU HÌNH THU THẬP LOG CLIENT 1 CENTOS 7 THÔNG QUA GRAYLOG-SIDECAR.....</b>	<b>26</b>
<b>3.4. CẤU HÌNH THU THẬP LOG CLIENT 2 WINDOWS THÔNG QUA GRAYLOG-SIDECAR.....</b>	<b>36</b>
<b>3.5. CẤU HÌNH THU THẬP LOG CỦA CLIENT 1 CENTOS 7 THÔNG QUA SYSLOG.....</b>	<b>43</b>
<b>3.6. CẤU HÌNH GRAYLOG SERVER TÍCH HỢP CẢNH BÁO QUA EMAIL .....</b>	<b>46</b>
<b>3.7. CẤU HÌNH GRAYLOG SERVER TÍCH HỢP CẢNH BÁO QUA SLACK .....</b>	<b>54</b>
CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO .....	62
<b>4.1. CẢNH BÁO LOGIN SSH.....</b>	<b>62</b>
<b>4.2. CẢNH BÁO LOGIN RDP .....</b>	<b>65</b>
<b>4.3. CẢNH BÁO NMAP SCAN.....</b>	<b>70</b>
<b>4.4. CẢNH BÁO FLOOD ICMP.....</b>	<b>73</b>
CHƯƠNG 5: KẾT LUẬN.....	77
<b>5.1 KẾT QUẢ ĐẠT ĐƯỢC .....</b>	<b>77</b>
<b>5.2 HẠN CHẾ .....</b>	<b>77</b>
TÀI LIỆU THAM KHẢO .....	78

## **DANH MỤC CÁC KÍ HIỆU VIẾT TẮT**

EPS: Events Per Second	Sự kiện mỗi giây
IDS: Intrusion Detection Systems	Hệ thống phát hiện xâm nhập
IPS:Intrusion Prevention Systems	Hệ thống ngăn chặn xâm nhập
EDR: Endpoint Detection and Response solutions	Các giải pháp phát hiện và phản hồi điểm cuối
CNTT: Information Technology	Công nghệ thông tin
JSON: JavaScript Object Notation	Một kiểu dữ liệu mở trong JavaScrip
CEF:Common Event Format	Định dạng sự kiện chung
GELF: Graylog Extended Log Format	Định dạng nhật ký mở rộng Graylog
HTTP:Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
API: Application Programming Interface	Giao diện lập trình ứng dụng
REST: Representational State Transfer	Một đại diện cho sự chuyển đổi dữ liệu
VNC: Virtual Network Computing	Một loại phần mềm điều khiển từ xa giúp bạn có thể điều khiển một máy tính khác qua kết nối mạng
RDP: Remote Desktop Protocol	Một giao thức của Microsoft cung cấp cho người dùng giao diện đồ họa để kết nối với một máy tính khác qua kết nối mạng internet.

# DANH MỤC CÁC BẢNG, SƠ ĐỒ, HÌNH

Hình 1. 1 JSON .....	7
Hình 1. 2 Syslog .....	7
Hình 1. 3 Một ví dụ về log .....	11
Hình 2. 1 Kiến trúc tối giản Graylog .....	13
Hình 2. 2 Kiến trúc Multi-Node Graylog .....	14
Bảng 2. 3 Các thành phần của Graylog .....	15
Hình 2. 4 Ví dụ về vòng đời của log trong Graylog .....	17
Hình 3. 1 Mô hình triển khai .....	19
Hình 3. 2 Mở UltraVNC để kết nối đến Graylog server .....	19
Hình 3. 3 Nhập password để kết nối VNC .....	20
Hình 3. 4 Đã kết nối VNC thành công .....	20
Hình 3. 5 Cấu hình Selinux /etc/sysconfig/selinux graylogserver .....	21
Hình 3. 6 Cấu hình Selinux /selinux/config graylogserver .....	21
Hình 3. 7 Cấu hình Chrony graylogserver .....	22
Hình 3. 8 Check chronyc sources graylogserver .....	22
Hình 3. 9 Check timedatectl graylogserver .....	22
Hình 3. 10 Tạo file mongodb repo graylogserver .....	23
Hình 3. 11 Tạo file elasticsearch graylogserver .....	23
Hình 3. 12 Edit file elasticsearch.yml graylogserver .....	24
Hình 3. 13 Thêm password secret vào server.conf graylogserver .....	24
Hình 3. 14 Thêm password cho tài khoản đăng nhập vào server.conf graylogserver .....	25
Hình 3. 15 Đặt timezone trong server.conf graylogserver .....	25
Hình 3. 16 Đặt web interface cho nhiều card truy cập trong server.conf graylogserver .....	25
Hình 3. 17 Thêm http_enable_cors = true trong server.conf graylogserver .....	25
Hình 3. 18 Sử dụng root admin user trong server.conf graylogserver .....	25
Hình 3. 19 Test login vào web interface Graylog graylogserver .....	26
Hình 3. 20 Cấu hình Selinux /etc/sysconfig/selinux client1 .....	26
Hình 3. 21 Cấu hình Selinux /selinux/config client1 .....	27
Hình 3. 22 Cấu hình Chrony client1 .....	27
Hình 3. 23 Check chronyc sources client1 .....	27
Hình 3. 24 Check timedatectl client1 .....	27
Hình 3. 25 Tạo token sidecar graylogserver .....	28
Hình 3. 26 Nhập tên token graylogserver .....	29
Hình 3. 27 Tạo thành công token graylogserver .....	29
Hình 3. 28 Cấu hình sidecar client1 .....	30
Hình 3. 29 Tạo Input Beats graylogserver .....	30
Hình 3. 30 Edit thông tin Input Beats graylogserver .....	31
Hình 3. 31 Chọn Save để save Input graylogserver .....	32
Hình 3. 32 Input Beats đã tạo thành công graylogserver .....	32
Hình 3. 33 Truy cập Sidecar graylogserver .....	33
Hình 3. 34 Tạo configuration sidecar graylogserver .....	33
Hình 3. 35 Chính sửa các thông tin cần thiết sidecar client1 graylogserver .....	33
Hình 3. 36 Chọn Filebeat , chọn configuration vừa tạo graylogserver .....	34
Hình 3. 37 Khởi động trình thu thập log từ client1 graylogserver .....	34
Hình 3. 38 Đã hoàn thành trình thu thập log sidecar client1 graylogserver .....	34
Hình 3. 39 Show messages sidecar client1 graylogserver .....	35
Hình 3. 40 Mở Putty SSH client1 .....	35
Hình 3. 41 SSH thành công vào client1 .....	35
Hình 3. 42 Đã nhận được log trên graylogserver khi có máy SSH vào client1 .....	36
Hình 3. 43 Tải sidecar cho window .....	36
Hình 3. 44 Cài đặt sidecar window .....	37
Hình 3. 45 Chọn I agree .....	37

Hình 3. 46 Edit sidecar window .....	38
Hình 3. 47 Chọn Finish .....	39
Hình 3. 48 Truy cập Sidecar graylogserver.....	39
Hình 3. 49 Chọn Create Configuration .....	39
Hình 3. 50 Edit các thông tin trong sidecar client2 graylogserver .....	40
Hình 3. 51 Chọn Filebeat , chọn configuration vừa tạo .....	40
Hình 3. 52 Khởi động trình thu thập dữ liệu client2 graylogserver .....	41
Hình 3. 53 Đã tạo thành công sidecar client2.....	41
Hình 3. 54 Show messages sidecar client2.....	41
Hình 3. 55 SSH vào client2.....	41
Hình 3. 56 SSH thành công vào client2 .....	42
Hình 3. 57 ã nhận được log trên graylogserver khi có máy SSH vào client2 .....	42
Hình 3. 58 Câu hình file rsyslog .....	43
Hình 3. 59 Input Syslog UDP.....	43
Hình 3. 60 Câu hình Input Syslog UDP .....	44
Hình 3. 61 Chọn Save để hoàn thành input syslog.....	45
Hình 3. 62 Syslog đã hoàn thành.....	45
Hình 3. 63 Chọn Show received message tại syslog để xem log client1 bằng syslog .....	46
Hình 3. 64 Log được gửi bằng Syslog từ client1 đã được nhận thành công .....	46
Hình 3. 65 Câu hình postfix để gửi mail .....	47
Hình 3. 66 Thêm gmai sender cho postfix .....	47
Hình 3. 67 Cho phép truy cập ứng dụng trong mail .....	48
Hình 3. 68 Test gửi mail.....	48
Hình 3. 69 Gửi mail thành công .....	48
Hình 3. 70 Câu hình gửi mail trong server.conf .....	49
Hình 3. 71 Tạo notification gửi mail .....	49
Hình 3. 72 Điện thông tin cần thiết để tạo email notification 1 .....	49
Hình 3. 73 Điện thông tin cần thiết để tạo email notification 2 .....	50
Hình 3. 74 Test Notification.....	50
Hình 3. 75 Tạo thành công Notification qua gmail.....	50
Hình 3. 76 Gmail test đã gửi thành công.....	51
Hình 3. 77 Tạo Event để cảnh báo .....	51
Hình 3. 78 Nhập tên mô tả cần cảnh báo.....	51
Hình 3. 79 Chọn Filter & Aggregation .....	52
Hình 3. 80 Nhập các thông tin cần thiết để cảnh báo .....	52
Hình 3. 81 Event Fields.....	52
Hình 3. 82 Chọn Notification .....	53
Hình 3. 83 Chọn Email Notification .....	53
Hình 3. 84 Các Notification đã được chọn .....	53
Hình 3. 85 Chọn Done để hoàn thành Alert Event.....	53
Hình 3. 86 Các log về SSH .....	54
Hình 3. 87 Gmail đã nhận được cảnh báo về đăng nhập thành công SSH.....	54
Hình 3. 88 Chi tiết Gmail cảnh báo.....	54
Hình 3. 89 Tạo Channels graylog trong Slack .....	55
Hình 3. 90 Copy URL workspace Slack .....	55
Hình 3. 91 Add Incoming WebHooks.....	56
Hình 3. 92 Tạo Webhooks thành công cho channel graylog.....	56
Hình 3. 93 Tạo Notification Slack .....	57
Hình 3. 94 Test cảnh báo qua Slack và Save Notification .....	58
Hình 3. 95 Đã nhận được thông báo test trên Slack .....	59
Hình 3. 96 Notification Slack đã hoàn thành .....	59
Hình 3. 97 Câu hình Event qua Slack .....	59
Hình 3. 98 Chọn Add notification trong event SSH đã tạo lúc trước.....	60
Hình 3. 99 Chọn Slack Notification .....	60
Hình 3. 100 Chọn next để tiếp tục.....	60
Hình 3. 101 Chọn Done để hoàn thành event cảnh báo qua Slack.....	60
Hình 3. 102 Đã nhận được cảnh báo đăng nhập thành công ssh trên Slack.....	61

Hình 4. 1 Tạo event cảnh báo SSH .....	62
Hình 4. 2 Chọn Filter & Aggregation .....	62
Hình 4. 3 Điền các thông tin cần thiết của cảnh báo SSH .....	63
Hình 4. 4 Next để qua bước event fields .....	63
Hình 4. 5 Chọn Notifications qua Gmail và Slack .....	63
Hình 4. 6 Hoàn thành cảnh báo SSH qua Gmail và Slack .....	64
Hình 4. 7 SSH thành công vào client1 .....	64
Hình 4. 8 Slack đã cảnh báo SSH thành công trên client 1 .....	64
Hình 4. 9 Gmail đã cảnh báo SSH thành công trên client 1 .....	65
Hình 4. 10 Tạo event cảnh báo Login RDP .....	65
Hình 4. 11 Chọn Filter & Aggregation .....	65
Hình 4. 12 Điền thông tin cần thiết của cảnh báo Login RDP .....	66
Hình 4. 13 Event Fields .....	66
Hình 4. 14 Chọn Notification qua Gmail và Slack .....	66
Hình 4. 15 Hoàn thành event cảnh báo RDP .....	67
Hình 4. 16 RDP vào client2 .....	67
Hình 4. 17 Nhập mật khẩu RDP .....	67
Hình 4. 18 RDP thành công vào client2 .....	68
Hình 4. 19 Gmail đã nhận được cảnh báo RDP .....	68
Hình 4. 20 Slack đã nhận được cảnh báo RDP .....	69
Hình 4. 21 Tạo event cảnh báo Nmap Scan .....	70
Hình 4. 22 Chọn Filter & Aggregation .....	70
Hình 4. 23 Điền thông tin cần thiết của cảnh báo Nmap Scan .....	71
Hình 4. 24 Nếu phát hiện trên 50 lần mới gửi thông báo .....	71
Hình 4. 25 Event Fields .....	71
Hình 4. 26 Chọn Notification qua Gmail và Slack .....	72
Hình 4. 27 Hoàn thành event cảnh báo Nmap Scan .....	72
Hình 4. 28 Nmap vào Client1 .....	72
Hình 4. 29 Gmail đã nhận được cảnh báo Nmap Scan .....	73
Hình 4. 30 Slack đã nhận được cảnh báo Nmap Scan .....	73
Hình 4. 31 Tạo event cảnh báo Flood ICMP .....	73
Hình 4. 32 Chọn Filter & Aggregation .....	74
Hình 4. 33 Điền thông tin cần thiết của cảnh báo Flood ICMP .....	74
Hình 4. 34 Phát hiện trên 10 lần thì gửi cảnh báo .....	74
Hình 4. 35 Event Fields .....	74
Hình 4. 36 Chọn Notification qua Gmail và Slack .....	75
Hình 4. 37 Hoàn thành event cảnh báo RDP .....	75
Hình 4. 38 Flood icmp vào client1 .....	75
Hình 4. 39 Gmail đã nhận được cảnh báo Flood ICMP .....	76
Hình 4. 40 Slack đã nhận được cảnh báo Flood ICMP .....	76

## **LỜI MỞ ĐẦU**

Việc giám sát thu thập, xử lý và phân tích các nhật ký, hay vết truy cập (access log, từ đây gọi tắt là log) mang nói chung và các log truy cập các dịch vụ mạng nói riêng là nhiệm vụ không thể thiếu trong các hệ thống giám sát, phát hiện bất thường, phát hiện tấn công, xâm nhập hệ thống và mạng. Từ dữ liệu log thu thập được, qua quá trình xử lý, phân tích, chúng ta có thể trích xuất được các thông tin quan trọng về dấu hiệu, hoặc khả năng xuất hiện của các hành vi truy cập bất thường, các dạng mã độc và các dạng tấn công, xâm nhập. Kết quả phân tích, phát hiện dấu hiệu xuất hiện của các truy cập bất thường, mã độc, tấn công, xâm nhập là đầu vào quyết định việc đưa ra các cảnh báo nguy cơ mất an toàn thông tin đối với hệ thống. Đồng thời, kết quả phân tích, phát hiện cũng là một trong các căn cứ quan trọng hỗ trợ việc đánh giá, lựa chọn và triển khai các giải pháp đảm bảo an toàn phù hợp cho thông tin, hệ thống và các tài nguyên mạng. Vấn đề này càng quan trọng hơn trong bối cảnh an toàn thông tin ở Việt Nam đã và đang trở thành vấn đề nóng được các cơ quan, tổ chức chính phủ, các doanh nghiệp và cả xã hội quan tâm.

Thông qua đề tài “TÌM HIỂU VÀ TRIỀN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG” của bản thân. Em mong muốn góp một phần nhỏ vào việc nghiên cứu và tìm hiểu phân tích các phương thức đọc log cho việc học tập và nghiên cứu. Từ đó nâng cao trình độ cũng như kiến thức của bản thân.

Tuy nhiên, vì thời gian và kiến thức còn hạn chế nên trong quá trình làm đề tài em không thể tránh khỏi những thiếu sót, kính mong nhận được những thời nhận xét và góp ý của quý thầy cô.

## CHƯƠNG 1 : TỔNG QUAN HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ

### 1.1. NHẬT KÝ

Tệp nhật ký là dữ liệu được tạo tự động khi các sự kiện nhất định xảy ra trong hệ thống, mạng và ứng dụng. Họ tạo ra các hồ sơ ghi lại các hoạt động cho:

- Người dùng
- May chủ
- Mạng
- Các hệ điều hành
- Ứng dụng / phần mềm

Ví dụ: nhật ký sự kiện có thể theo dõi:

- Khi một máy tính đã được sao lưu
- Lỗi ngăn ứng dụng chạy
- Các tệp do người dùng yêu cầu từ một trang web

Các đội bảo mật và vận hành CNTT sử dụng chúng để điều tra và phản ứng với hoạt động bất thường của hệ thống.

Nhật ký có thể có hai định dạng khác nhau. Một số có thể được mở và đọc bởi con người. Các tài liệu khác được lưu giữ cho mục đích kiểm tra và chủ yếu chỉ có thể đọc được bằng máy.

Một số ví dụ về các loại nhật ký bao gồm:

- Nhật ký kiểm tra
- Nhật ký giao dịch
- Nhật ký sự kiện
- Nhật ký lỗi
- Nhật ký tin nhắn
- Nhật ký bảo mật

Cuối cùng, nhật ký có nhiều định dạng hoặc tiện ích mở rộng, như

- .log
- .txt
- JSON
- .csv
- .dat

Tùy thuộc vào phần mở rộng và khả năng đọc, chúng ta có thể mở các tệp nhật ký bằng:

- Trình soạn thảo văn bản tiêu chuẩn như Notepad
- Các ứng dụng xử lý văn bản như OpenOffice hoặc Microsoft Word
- Ứng dụng dòng lệnh như PowerShell
- Microsoft Excel
- OpenOffice Calc
- LibreOffice Calc

## **1.2. QUẢN LÝ NHẬT KÝ**

Quản lý nhật ký là quá trình quản lý nhật ký sự kiện, bao gồm các hoạt động sau đối với nhật ký:

- Generating
- Transmitting
- Lưu trữ
- Phân tích
- Disposing

Quản lý nhật ký là rất quan trọng để tuân thủ. Vì các bản ghi sự kiện chứa tất cả dữ liệu về hoạt động xảy ra trong môi trường, chúng đóng vai trò như tài liệu cho các cuộc đánh giá.

## **1.3. QUẢN LÝ NHẬT KÝ TẬP TRUNG**

Giải pháp quản lý nhật ký tập trung là một công nghệ cho phép các tổ chức quản lý tất cả các loại nhật ký khác nhau. Chúng bao gồm những thứ từ khắp các môi trường tại chỗ, đám mây và môi trường kết hợp của chúng bằng cách bật các tính năng sau:

- **Collection:** nhập nhật ký từ nhiều hệ thống, mạng, ứng dụng và thiết bị khác nhau
- **Aggregation:** kết hợp số lượng, khối lượng và nhiều nguồn nhật ký gia tăng vào một vị trí duy nhất
- **Parsing:** lấy ra thông tin quan trọng từ mỗi bản ghi sự kiện để có thể sử dụng
- **Normalization:** tạo định dạng chuẩn cho tất cả dữ liệu nhật ký sự kiện
- **Correlation:** kết hợp thông tin về các sự kiện trên tất cả các môi trường để có khả năng hiển thị tốt hơn vào hoạt động
- **Analysis:** tự động hóa các điểm dữ liệu tương quan để tạo cảnh báo có độ trung thực cao

Một công cụ ghi nhật ký tập trung cung cấp cho các hoạt động và cảnh báo bảo mật có độ trung thực cao để chúng có thể phát hiện, điều tra và phản hồi các vấn đề nhanh hơn.

Chúng ta có thể sử dụng các công cụ quản lý nhật ký như Graylog để nhập các ứng dụng hoặc nhật ký hệ thống khác nhau. Bằng cách này, chúng ta có thể xem và trích xuất dữ liệu có giá trị từ chúng.

## **1.4. CÁC CÔNG CỤ QUẢN LÝ NHẬT KÝ ĐƯỢC SỬ DỤNG NHƯ THẾ NÀO?**

Với giải pháp quản lý nhật ký tập trung, mọi người đều có thể nhìn thấy những gì đang xảy ra trên môi trường CNTT đa dạng. Quan trọng hơn, quản lý nhật ký tập trung giúp dễ dàng thực hiện hành động hơn đối với những việc nhu máy chủ ngừng hoạt động hoặc sự cố bảo mật. Tuy nhiên, điều quan trọng là phải hiểu cách thức hoạt động của các giải pháp quản lý nhật ký tập trung để hiểu rõ hơn giá trị của chúng.

### **1.4.1. LOG COLLECTION**

Bước đầu tiên trong quản lý nhật ký là xác định cách thu thập và lưu trữ dữ liệu nhật ký. Đây là giá trị cơ bản của giải pháp quản lý nhật ký tập trung.

Các phần khác nhau của môi trường CNTT tạo ra dữ liệu nhật ký bao gồm:

- Các hệ điều hành
- Firewalls
- Servers
- Switch
- Routers
- Workstations
- Applications
- Hệ thống phát hiện xâm nhập (IDS)
- Hệ thống ngăn chặn xâm nhập (IPS)
- Anti-virus solutions
- Các giải pháp phát hiện và phản hồi điểm cuối (EDR)

Mỗi hệ thống, phần mềm và thiết bị có thể tạo ra hàng chục EPS (sự kiện mỗi giây). Đây là lý do tại sao sử dụng công cụ thu thập nhật ký có thể xử lý số lượng nhật ký tương ứng.

Giải pháp quản lý nhật ký tập trung cho phép chúng ta định cấu hình và tùy chỉnh dữ liệu nhật ký mà chúng ta muốn.

## CHIẾN LUỢC THU THẬP NHẬT KÝ

Chúng ta muốn định cấu hình cài đặt thu thập dữ liệu nhật ký để loại bỏ dữ liệu thừa và đảm bảo rằng chúng ta thu thập tất cả thông tin có liên quan. Đây là cách tiếp cận tối giản để cải thiện hiệu suất và hiệu quả.

Một cách khác để tiếp cận việc thu thập nhật ký là đi theo chiến lược tối đa. Điều này có nghĩa là thu thập mọi thông tin có thể để công cụ quản lý nhật ký có thể sắp xếp và phân tích nó. Mặc dù cách tiếp cận này có nhiều nhược điểm, nhưng hai nhược điểm lớn nhất là:

- **Tăng chi phí:** Việc lưu trữ một lượng lớn dữ liệu rất tốn kém và cần thêm nhân viên để quản lý quy trình

- **Giảm hiệu quả:** Các tập dữ liệu cực lớn được lưu trữ trực tuyến sẽ làm giảm hiệu suất tổng thể.

## LUU TRỮ VÀ LUU GIỮ NHẬT KÝ DÀI HẠN

Bộ sưu tập cung cấp cho chúng ta khả năng lưu trữ và lưu giữ nhật ký lâu dài. Nhiều nhiệm vụ tuân thủ có các yêu cầu về lưu trữ và lưu giữ nhật ký, vì vậy chúng ta nên coi đây là một phần của bộ sưu tập nhật ký của mình. Nói chung, các phương pháp hay nhất để xuất lưu trữ dữ liệu nhật ký ít nhất một năm trong trường hợp cần điều tra.

Khi lưu trữ nhật ký, chúng ta có thể chọn sao lưu dữ liệu vào máy chủ tại chỗ hoặc trên đám mây. Quyết định này thường đi kèm với quyết định của một công ty trong việc trải qua quá trình chuyển đổi kỹ thuật số và di chuyển các nguồn lực của mình trực tuyến.

## LOG ROTATION

Log rotation tự động hóa quá trình đổi tên, thay đổi kích thước, di chuyển hoặc xóa các tệp nhật ký quá lớn hoặc quá cũ.

Chúng ta có thể chọn khoảng thời gian mà sau đó nhật ký sẽ là:

- Đã xóa,
- Được nén để tiết kiệm không gian
- Được gửi qua email đến một vị trí khác.

Bằng cách này, không gian lưu trữ mới sẽ mở ra cho các tệp nhật ký gần đây hơn.

Graylog hợp lý hóa việc lập chỉ mục và xoay vòng nhật ký để lưu trữ được tối ưu hóa .

### **1.4.2.TỔNG HỢP NHẬT KÝ**

Việc tổng hợp tất cả dữ liệu nhật ký ở một nơi có thể là một thách thức nếu không có giải pháp quản lý nhật ký tập trung. Một số thách thức bao gồm:

- Khối lượng lớn dữ liệu
- Ghi dữ liệu chính xác
- Định dạng đa dạng trên các hệ thống, mạng, ứng dụng và thiết bị

Ngay cả khi hệ thống quản lý nhật ký của chúng ta có thể xử lý khối lượng lớn dữ liệu, điều quan trọng là dữ liệu này được tạo ra nhanh như thế nào. Các công cụ quản lý nhật ký sẽ có thể theo kịp tốc độ này. Đây là lý do tại sao EPS của một công cụ là điều chúng ta nên cân nhắc khi chọn một công cụ.

### **1.4.3.PHÂN TÍCH CÚ PHÁP NHẬT KÝ**

Chúng ta muốn tập trung vào dữ liệu quan trọng nhất để đáp ứng nhu cầu của mình. Phân tích cú pháp nhật ký là quá trình lấy ra dữ liệu chúng ta cần nhất.

Mỗi mục nhập nhật ký sự kiện được phân loại theo loại. Thông thường, chúng ta sẽ có các loại nhật ký sự kiện sau:

- Thông tin: mô tả cơ bản về điều gì đó đang xảy ra được cho là sẽ xảy ra
- Cảnh báo: Thông báo về một sự kiện có thể không quan trọng bây giờ nhưng cho biết sự cố có thể xảy ra sau này
  - Lỗi: Đã xảy ra sự cố, dẫn đến sự cố nghiêm trọng
  - Kiểm tra thành công: Nhật ký bảo mật cho biết đã hoàn thành thành công sự kiện bảo mật đã được kiểm toán
  - Kiểm tra không thành công: Nhật ký bảo mật chỉ ra rằng sự kiện bảo mật được kiểm tra đã không hoàn tất thành công

Ngoài ra, mỗi nhật ký đánh giá có thể chứa các thông tin sau:

- Ngày
- Thời gian
- Người sử dụng
- Máy tính / Thiết bị
- ID sự kiện
- Nguồn
- Loại sự kiện
- Mô tả sự kiện

### 1.4.4. CHUẨN HÓA NHẬT KÝ

Phân tích cú pháp dữ liệu giúp chúng ta nhận được các phần dữ liệu chúng ta cần. Chuẩn hóa nhật ký giúp chúng ta tạo định dạng chuẩn trên tất cả các nhật ký sự kiện.

Ví dụ: sau đây là một số loại định dạng nhật ký khác nhau mà chúng ta có thể đang thu thập:

- **Syslog:** thông báo sự kiện từ các thiết bị mạng như bộ định tuyến và thiết bị chuyển mạch
- **JavaScript Object Notation (JSON):** **định dạng có thể được đọc bởi cả người và máy**
- **Nhật ký sự kiện windows:** bản ghi từ hệ điều hành và ứng dụng dựa trên Windows
- **Định dạng sự kiện chung (CEF):** định dạng dựa trên văn bản, có thể mở rộng dễ đọc

#### JSON

post code:	"90210"
country:	"United States"
country abbreviation:	"US"
<b>places:</b>	
▼ 0:	
place name:	"Beverly Hills"
longitude:	"-118.4065"
state:	"California"
state abbreviation:	"CA"
latitude:	"34.0901"

Hình 1. 1 JSON

{"mã bưu điện": "90210", "quốc gia": "Hoa Kỳ", "tên viết tắt của quốc gia": "Hoa Kỳ", "địa điểm": [{"place name": "Beverly Hills", "kinh độ": "-118.4065", "tiểu bang": "California", "viết tắt của tiểu bang": "CA", "vĩ độ": "34.0901"}]}

#### Syslog

```
Feb 1 16:55:26 graylog2 kernel: [1903717.646250] mce: CPU2: Core temperature above threshold, cpu clock throttled (total events = 322420)
Feb 1 16:55:26 graylog2 kernel: [1903717.646730] mce: CPU2: Core temperature/speed normal
Feb 1 16:59:22 graylog2 kernel: [1903953.096045] perf: interrupt took too long (18484 > 18461), lowering kernel.perf_event_max_sample_rate to 10750
Feb 2 06:15:04 graylog2 kernel: [1951694.270757] mce: CPU0: Core temperature above threshold, cpu clock throttled (total events = 432871)
Feb 2 06:15:04 graylog2 kernel: [1951694.271236] mce: CPU0: Core temperature/speed normal
Feb 2 08:15:03 graylog2 kernel: [1958893.556240] mce: CPU0: Core temperature above threshold, cpu clock throttled (total events = 432932)
Feb 2 08:15:03 graylog2 kernel: [1958893.556721] mce: CPU0: Core temperature/speed normal
```

Hình 1. 2 Syslog

Môi trường của chúng ta có thể đang thu thập nhật ký sự kiện sử dụng hai hoặc nhiều định dạng này, như Syslog và Windows Event Log . Tuy nhiên, vì các định dạng đặt tên cho các phần thông tin khác nhau, nên việc phân tích cú pháp chỉ trích xuất các phần đó. Chuẩn hóa chuẩn hóa cách dữ liệu được trình bày để chúng ta có được thông tin chi tiết có ý nghĩa.

Ví dụ: Định dạng nhật ký mở rộng Graylog (GELF) chuẩn hóa các bản ghi sự kiện phức tạp và đa dạng. Nó cho phép chúng ta thu thập các sự kiện có cấu trúc từ mọi nơi để có được thông tin chi tiết chúng ta cần.

```
'{"short_message": "metrics", "_cpu": "88", "_mem": "1024", "_disk": "90", "_guid": "b375dc4c-dd07-479b-9288-b152aa583318"}'
```

### **1.4.5. MỐI TƯỞNG QUAN CỦA CÁC SỰ KIỆN**

Trong một môi trường CNTT hiện đại, phức tạp, chúng ta có rất nhiều hệ thống, mạng và ứng dụng được kết nối với nhau. Chúng ta cần hiểu tất cả các yếu tố phụ thuộc và có thể theo dõi vấn đề để tìm ra nguyên nhân gốc rễ.

Các sự kiện tương quan là quá trình kết hợp nhiều sự kiện để xem các mối quan hệ tồn tại. Ví dụ: máy chủ ngừng hoạt động có thể ảnh hưởng đến hiệu suất của ứng dụng. Tuy nhiên, nhóm CNTT của chúng ta đã nhận được cuộc gọi từ bộ phận trợ giúp về việc ứng dụng chậm.

Bằng cách so sánh các sự kiện, chúng ta có thể thực hiện phân tích nguyên nhân gốc rễ nhanh hơn.

### **1.4.6. PHÂN TÍCH NHẬT KÝ**

Với phân tích nhật ký, chúng ta sử dụng dữ liệu mà chúng ta đang thu thập, phân tích cú pháp, chuẩn hóa và tương quan.

Các công cụ quản lý nhật ký tập trung tự động hóa và đơn giản hóa quá trình phân tích dữ liệu nhật ký. Hình ảnh hóa như biểu đồ và đồ thị nhấn mạnh mối tương quan và tương đồng giữa các sự kiện và dữ liệu. Bằng cách này, việc phát hiện các vấn đề và theo dõi nguyên nhân của chúng sẽ dễ dàng hơn.

Các trường hợp sử dụng hàng đầu để phân tích nhật ký bao gồm:

- Sự tuân thủ
- Bảo vệ
- Xử lý sự cố
- Cải thiện hiệu suất

## **1.5. NHỮNG LỢI ÍCH CHÍNH CỦA VIỆC QUẢN LÝ VÀ GIÁM SÁT NHẬT KÝ**

Quản lý nhật ký rất quan trọng vì nó cho phép chúng ta thực hiện một cách tiếp cận có hệ thống để hiểu rõ hơn trong thời gian thực về hoạt động và bảo mật.

Một số lợi ích của việc quản lý và giám sát nhật ký bao gồm:

- Giám sát Hệ Thống
- Cảnh báo có độ trung thực cao
- Bảo mật nâng cao
- Khắc phục sự cố nhanh hơn
- Sử dụng tài nguyên được tối ưu hóa

- Cải thiện tư thế tuân thủ

### **1.5.1. GIÁM SÁT HỆ THỐNG**

Một trong những lợi ích của quản lý nhật ký là cho phép chúng ta theo dõi mọi thứ xảy ra trên môi trường CNTT đa dạng của chúng ta. Ngoài ra, nhiều người có cùng tầm nhìn để giao tiếp tốt hơn như một phần của giám sát hệ thống. Ví dụ: giám sát hệ thống tập trung cho phép:

- Hoạt động CNTT
- DevOps
- Nhà phát triển
- Quản trị viên Hệ thống
- Hoạt động an ninh

Khả năng hiển thị này có thể cung cấp thông tin chi tiết về các vấn đề hiệu suất cho biết các vấn đề tiềm ẩn hoặc trong tương lai.

Với Graylog, chúng ta có thể chia sẻ thông tin bằng cách sử dụng email, công cụ cộng tác và hệ thống bán vé.

### **1.5.2. CẢNH BÁO ĐỘ TRUNG THỰC CAO**

Khả năng tương quan và phân tích dữ liệu nhật ký sự kiện của quản lý nhật ký tập trung cũng có nghĩa là chúng ta có thể tạo các cảnh báo có độ trung thực cao. Chúng ta có thể điều chỉnh cài đặt giám sát để theo dõi lựa chọn sự kiện tùy chỉnh với các cảnh báo thời gian thực có thể tùy chỉnh. Những cảnh báo này cho phép chúng ta phản ứng nhanh hơn và giảm thời gian chết.

### **1.5.3. BẢO MẬT NÂNG CAO**

Các cảnh báo có độ trung thực cao cũng cho phép tăng cường bảo mật. Chúng ta có thể có một nhóm bảo mật chuyên dụng hoặc những người trong nhóm CNTT quản lý các chức năng bảo mật. Trong cả hai trường hợp, tất cả mọi người đều bị choáng ngợp bởi số lượng lớn các cảnh báo, trong đó có nhiều cảnh báo là dương tính giả.

Chúng ta có thể giảm số lượng xác thực giả để ưu tiên các hoạt động phản hồi bảo mật bằng cách tương quan các sự kiện. Điều này cải thiện khả năng phát hiện, giảm thời gian phản hồi và giảm thiểu rủi ro. Các tác nhân đe dọa thời gian ở trong môi trường của chúng ta càng ít, chúng càng có thể gây ra ít thiệt hại hơn.

Ngoài ra, chúng ta có thể sử dụng quản lý nhật ký để biến SIEM của mình thành một công cụ bảo mật chủ động với khả năng săn tìm mối đe dọa.

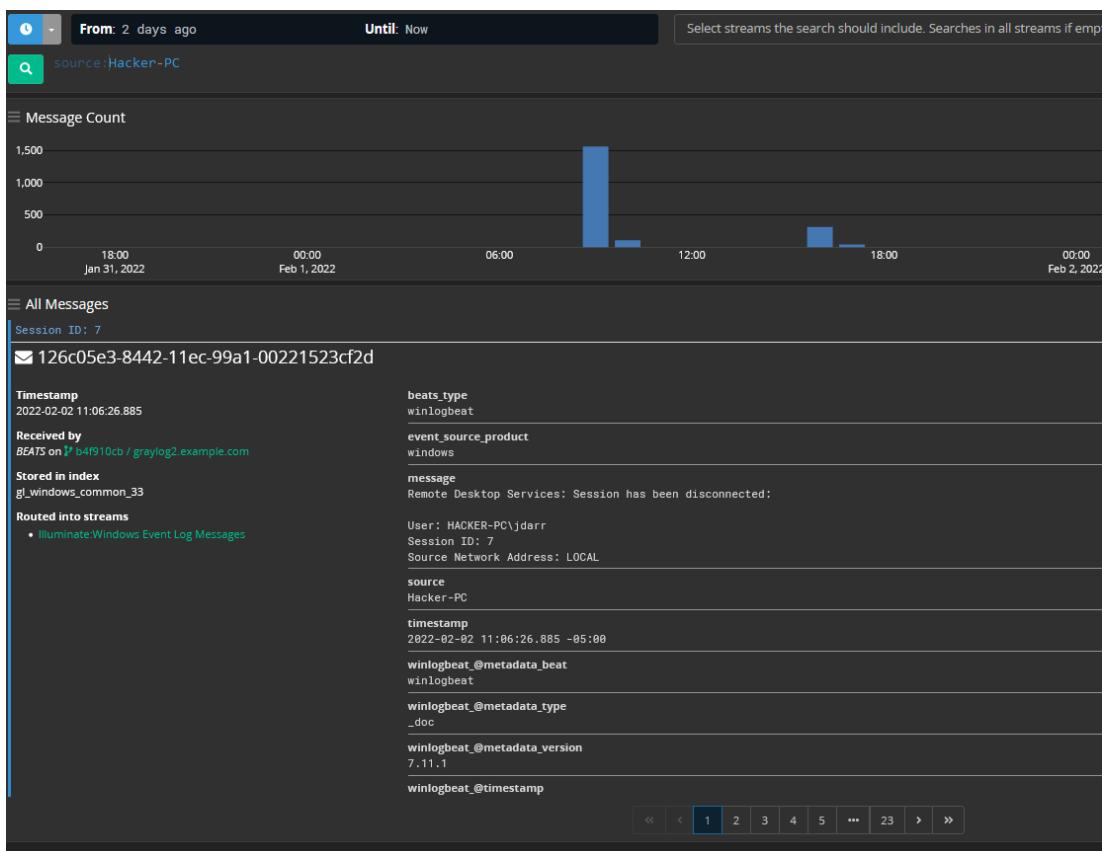
### 1.5.4. KHẮC PHỤC SỰ CỐ NHANH HƠN

Quản lý nhật ký cho phép chúng ta kiểm soát tốt hơn và hiểu rõ hơn về các quy trình trong môi trường của chúng ta. Các giải pháp quản lý nhật ký được trang bị các phương tiện để khai thác dữ liệu. Họ có thể đào qua khối lượng dữ liệu nhật ký để khám phá các mẫu mà nếu không sẽ bị ẩn.

Chúng ta có thể tùy chỉnh tìm kiếm và phân tích để hưởng lợi từ lượng lớn dữ liệu được lưu trữ trong nhật ký bằng phân tích nhật ký. Khả năng tìm kiếm nâng cao cho phép chúng ta sử dụng cả nhật ký có cấu trúc và không có cấu trúc. Bằng cách này, chúng ta có thể thu thập thông tin về các sự kiện cụ thể giúp xác định nguyên nhân gốc rễ.

Điều này giúp chúng ta dễ dàng hơn:

- Tạo lại dòng thời gian của các sự kiện có vấn đề
- Khám phá kết nối với các sự kiện khác
- Xác định nguồn gốc của vấn đề.



Hình 1.3 Một ví dụ về log

**1.5.5. SỬ DỤNG TÀI NGUYÊN ĐƯỢC TỐI ƯU HÓA**

Giám sát hiệu suất có thể giúp chúng ta theo dõi việc sử dụng tài nguyên. Thông thường, một người nào đó sẽ gửi một phiếu tới bộ phận trợ giúp nói rằng một ứng dụng không phản hồi. Tuy nhiên, đây có thể là kết quả của một máy chủ quá tải.

Quản lý nhật ký tập trung cung cấp cho chúng ta khả năng hiển thị các vấn đề về hiệu suất và tắc nghẽn. Bằng cách tối ưu hóa việc sử dụng tài nguyên, chúng ta giảm bớt gánh nặng cho nhóm CNTT của mình.

Đối với môi trường đám mây, quản lý nhật ký tập trung có thể cung cấp cho chúng ta khả năng hiển thị về việc sử dụng xung quanh:

- Khối lượng công việc
- Các ứng dụng
- Nhiều môi trường
- Tài sản bị lãng quên

Khả năng hiển thị của điều này có thể giúp chúng ta tối ưu hóa chi tiêu trên đám mây.

**1.5.6. CẢI THIỆN TƯ THẾ TUÂN THỦ**

Báo cáo nhật ký tóm tắt các hoạt động tìm kiếm và phân tích với các con số và thuộc tính trực quan.

Chúng ta có thể sử dụng báo cáo nhật ký để trình bày những phát hiện của mình cho những người không có kiến thức nền tảng về kỹ thuật. Thông tin này có thể được chia sẻ với lãnh đạo cấp cao hoặc Hội đồng quản trị. Bằng cách xem xét các báo cáo này, họ có dữ liệu để chứng minh khả năng quản trị đối với chương trình bảo mật, điều quan trọng là phải tuân thủ.

**1.6. CÁC CÔNG CỤ QUẢN LÝ NHẬT KÝ ĐƯỢC SỬ DỤNG**

Có thể thực hiện các bước quản lý nhật ký trong nhà. Tuy nhiên, đó là một quá trình tốn nhiều thời gian, đòi hỏi nhiều tùy chỉnh và lập kế hoạch. Xử lý quản lý nhật ký mà không có công cụ ghi nhật ký tương tự như lập trình từ đầu thay vì sử dụng các thư viện và tập lệnh hiện có - có thể làm được nhưng lãng phí về thời gian và tài nguyên.

Giải pháp quản lý nhật ký tập trung của Graylog được xây dựng có mục đích với các nhóm CNTT. Chúng tôi muốn họ tối ưu hóa giá trị của nhật ký của họ.

Graylog cung cấp các cảnh báo có độ trung thực cao và khả năng tìm kiếm nhanh như chớp. Những điều này làm giảm các chỉ số chính được sử dụng cho các hoạt động CNTT và báo cáo bảo mật. Bằng cách này, chúng ta có thể tập trung sự chú ý của mình vào các hoạt động quan trọng hàng ngày trong việc quản lý một môi trường CNTT phức tạp

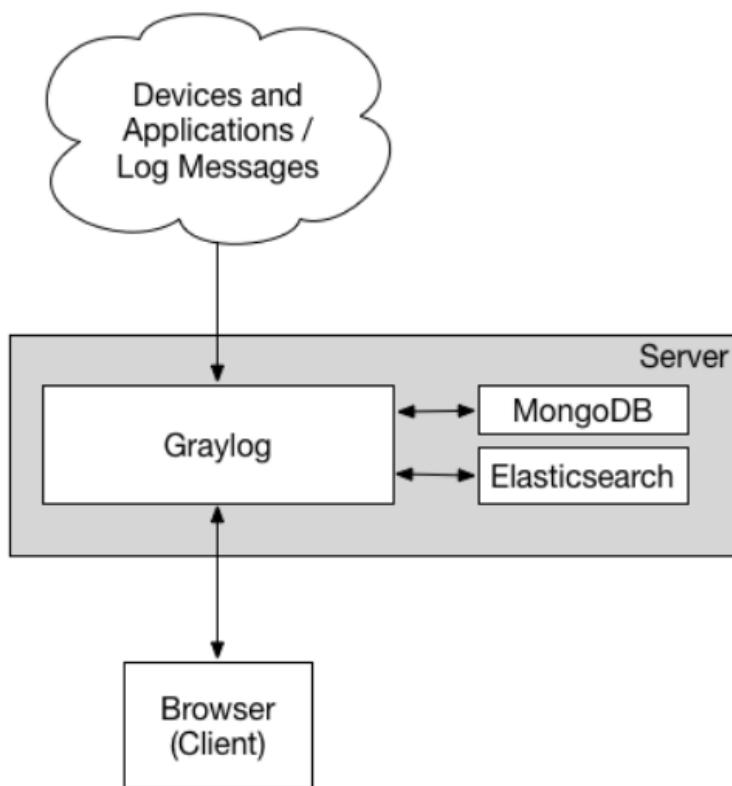
## CHƯƠNG 2: NGHIÊN CỨU HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

### 2.1. KIẾN TRÚC GRAYLOG

Graylog là một trong những công cụ quản lý log mã nguồn mở, phân tích các bản ghi đến, trích xuất dữ liệu quan trọng từ chúng, cung cấp tính năng tìm kiếm và trực quan hóa nhật ký trên giao diện web. Graylog được viết bằng Java và sử dụng một vài công cụ mã nguồn mở như Elasticsearch, MongoDB. Hai công cụ này kết hợp với Graylog và Graylog UI tạo thành một giải pháp quản lý log mạnh mẽ.

Mỗi hệ thống Graylog tối thiểu bao gồm Graylog Server, MongoDB và Elasticsearch. Mỗi thành phần này đều yêu cầu bắt buộc và không thể thay thế bằng bất kỳ công cụ nào khác.

Trong một mô hình triển khai Graylog tối giản, tất cả ba thành phần được cài đặt trên một máy chủ duy nhất. Một thiết lập Graylog tối giản có thể được sử dụng cho các hệ thống nhỏ, ít quan trọng hoặc để thử nghiệm. Hình 3.1 thể hiện kiến trúc Graylog tối giản [11], không có thành phần nào thừa và có thể thiết lập một cách dễ dàng, nhanh chóng.

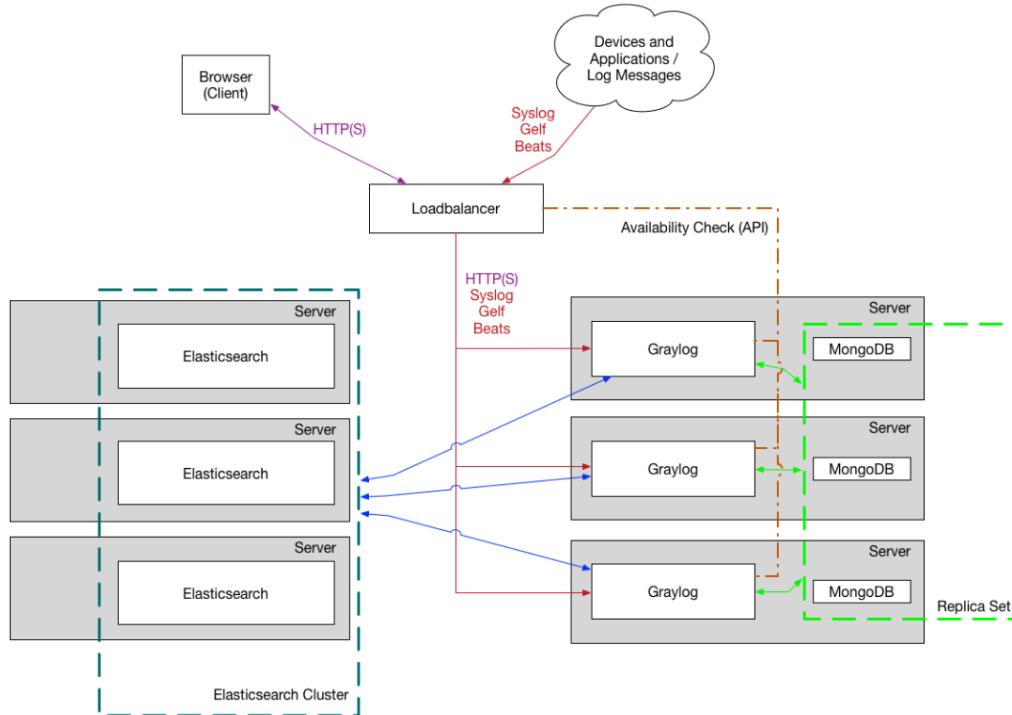


Hình 2. 1 Kiến trúc tối giản Graylog

Trong một hệ thống multi-node đơn giản, các thành phần Graylog và Elasticsearch đều nằm trên các máy chủ riêng của chúng. Hầu hết, MongoDB đều được cài đặt trên cùng một máy chủ với Graylog vì nó được sử dụng chủ yếu cho thông tin

cấu hình ứng dụng. Tải trên MongoDB thấp nên nó thường không cần đến máy chủ riêng.

Đối với môi trường lớn hơn, hoặc khi yêu cầu tính khả dụng cao, Graylog có thể được triển khai với cấu hình multi-node phức tạp. Cả Graylog và Elasticsearch đều có thể được nhóm lại để cung cấp khả năng phục hồi trong trường hợp lỗi nút. Hệ thống multi-node thường được triển khai để xử lý một khối lượng lớn các bản ghi log. Hình 2.2 thể hiện mô hình triển khai hệ thống multi-node của Graylog [11].



Hình 2.2 Kiến trúc Multi-Node Graylog

Thiết kế multi-node phức tạp sẽ được triển khai cho các môi trường hoạt động lớn hơn. Nó bao gồm hai hoặc nhiều nút Graylog phía sau bộ cân bằng tải có nhiệm vụ phân phối tải xử lý. Bộ cân bằng tải có thể ping các nút Graylog qua HTTP trên

Graylog REST API để kiểm tra xem chúng còn sống hay không và loại các nút chết ra khỏi cụm.

Có một vài quy tắc chung khi mở rộng tài nguyên cho Graylog như sau:

- Các nút Graylog nên tập trung vào CPU. Chúng cũng phục vụ giao diện web cho người dùng.
- Các nút Elasticsearch nên có càng nhiều RAM càng tốt và các ổ đĩa cứng nhanh nhất có thể. Tất cả mọi thứ phụ thuộc vào tốc độ I/O ở đây.
- MongoDB lưu trữ metadata và thông tin về cấu hình nên không cần nhiều tài nguyên.

Các bản tin được nhập vào chỉ được lưu trữ trong Elasticsearch. Nếu bị mất dữ liệu trong cụm Elasticsearch thì các bản tin sẽ bị mất, trừ khi đã tạo bản sao lưu trước đó.

## 2.2. CÁC THÀNH PHẦN CỦA GRAYLOG

Graylog bao gồm bốn thành phần chính, đó là Graylog UI, Graylog Server, MongoDB và ElasticSearch.

<b>GRAYLOG</b>	<b>GRAYLOG UI</b>	<ul style="list-style-type: none"> <li>- Cung cấp giao diện web cho người dùng</li> <li>- Cung cấp khả năng tìm kiếm và phân tích</li> <li>- Cung cấp giao diện cho môi trường cấu hình Graylog</li> </ul>
	<b>GRAYLOG SERVER</b>	<ul style="list-style-type: none"> <li>- Chứa công cụ xử lý log</li> <li>- Tích hợp tất cả các thành phần của Graylog</li> </ul>
	<b>MongoDB</b>	<ul style="list-style-type: none"> <li>- Được sử dụng để lưu trữ dữ liệu cấu hình</li> <li>- Chứa metadata, chẳng hạn như thông tin người dùng hoặc cấu hình luồng</li> </ul>
	<b>ElasticSearch</b>	<ul style="list-style-type: none"> <li>- Dùng để lưu trữ bản tin</li> <li>- Cung cấp công cụ tìm kiếm mạnh mẽ và nhanh chóng</li> </ul>

Bảng 2.3 Các thành phần của Graylog

Elasticsearch là một công cụ tìm kiếm mã nguồn mở rất mạnh và có khả năng mở rộng cao. Có thể tìm kiếm, phân tích và lưu trữ một lượng lớn dữ liệu và nó hoạt động như một công cụ phân tích gần như thời gian thực. Có nghĩa là có một độ trễ nhỏ giữa thời gian khi dữ liệu được lập chỉ mục và khi chúng có sẵn để tìm kiếm. Elasticsearch lưu trữ các chỉ mục theo định dạng tinh vi được tối ưu hóa cho tìm kiếm toàn văn bản. Chỉ mục là tập hợp dữ liệu, trong Elasticsearch được gọi là tài liệu, với các đặc điểm tương tự. Graylog sử dụng một cụm Elasticsearch chuyên dụng có thể bao gồm nhiều nút. Tất cả các nút Elasticsearch được định nghĩa trong file cấu hình chính của Graylog: /etc/graylog/server/server.conf. Graylog cũng hỗ trợ phát hiện nút tự động để có danh sách các nút Elasticsearch có sẵn. Cụm Elasticsearch được Graylog sử dụng có thể bao gồm nhiều nút trong đó một nút là một thẻ hiện của Elasticsearch. Một nút có thể lưu trữ dữ liệu hoặc bản sao dữ liệu. Mục đích của việc lưu trữ các bản sao dữ liệu trong chuyển đổi dự phòng là trong trường hợp nút chính bị hỏng, nút lưu trữ bản sao được đẩy lên vai trò của nút chính và không có dữ liệu nào bị mất. Các nút mới được thêm vào cụm Elasticsearch để tăng hiệu suất. Điều đó có nghĩa rằng hiệu suất của máy chủ

Graylog là được đánh giá cao bởi hiệu quả của cụm Elasticsearch.

MongoDB là một cơ sở dữ liệu NoSQL lưu trữ dữ liệu theo cấu trúc có định dạng JSON. Graylog sử dụng MongoDB để lưu trữ các thông tin cấu hình, metadata và web UI, chẳng hạn như người dùng, quyền, luồng, chỉ mục, thông tin cấu hình, v.v. MongoDB không lưu trữ dữ liệu log, cũng không phải chạy trên một máy chủ chuyên dụng bởi vậy nó không có tác động lớn đến máy chủ Graylog.

Graylog User Interface cho phép truy cập vào giao diện web trực quan, cung cấp khả năng tìm kiếm, phân tích và làm việc với dữ liệu tổng hợp. Graylog UI tìm nạp tất cả dữ liệu thông qua HTTP từ Graylog REST API. API được sử dụng làm kênh giao tiếp chính giữa máy chủ UI và máy chủ Graylog. Ưu điểm là với dữ liệu từ REST API, có thể xây dựng lối vào riêng theo nhu cầu.

Graylog Server là một thành phần chịu trách nhiệm nhận dữ liệu từ máy khách và mục đích chính của nó là tích hợp và giao tiếp với các thành phần khác

### **2.3.CÁC TÍNH NĂNG CỦA GRAYLOG**

Một nhật ký được nhận bởi máy chủ Graylog, sau đó được xử lý bởi Bộ lọc bản tin, là bộ xử lý bản tin chịu trách nhiệm phân tích cú pháp, thay đổi và thiết lập các trường tĩnh cho một nhật ký hợp lệ. Log được thay đổi theo các quy tắc được xác định trước và được định tuyến thành các danh mục được gọi là Luồng. Đối với các luồng khác nhau, chúng ta có thể xác định các quy tắc dựa trên các quy tắc cụ thể. Trên mỗi luồng, có một bộ chỉ mục khác được áp dụng. Bộ chỉ mục kiểm soát các bản tin được lưu trữ trong Elasticsearch như thế nào, ví dụ, số lượng các phân đoạn Elasticsearch hoặc các chính sách xoay vòng và lưu trữ. Từ luồng, nhật ký được chuyển tiếp đến một hệ thống khác hoặc lưu trữ cục bộ trên máy chủ Graylog

#### **2.3.1 THU THẬP LOG**

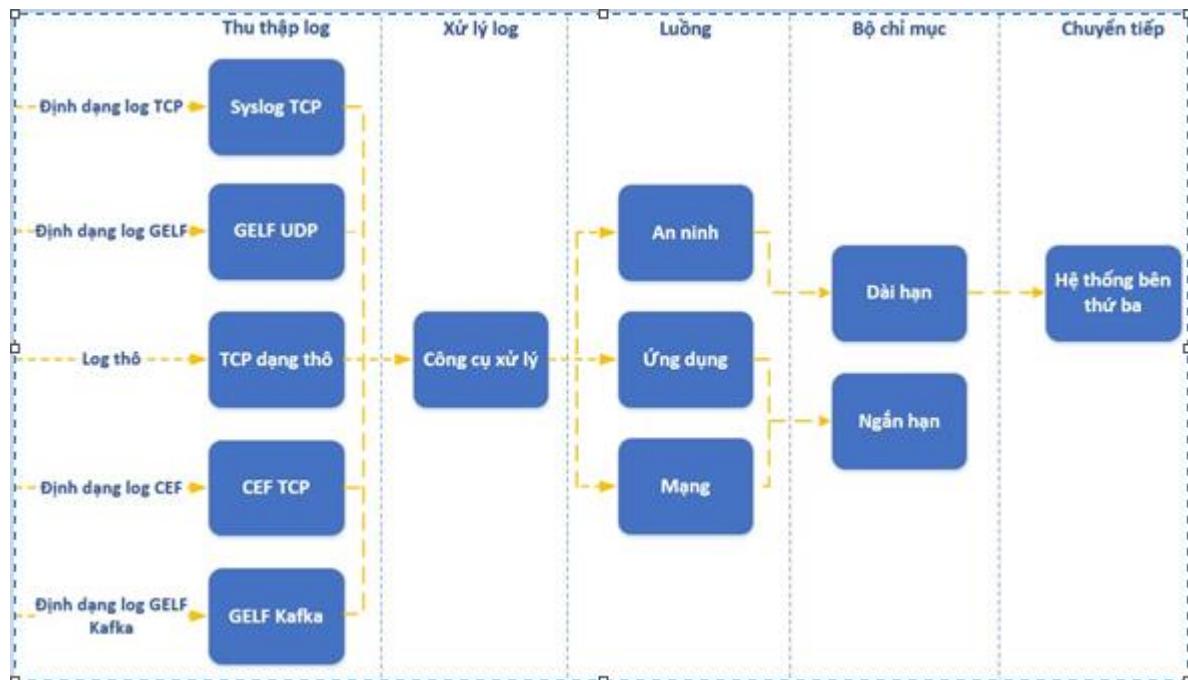
Graylog hỗ trợ ba loại nguồn dữ liệu đầu vào khác nhau:

- Các giao thức và định dạng chuẩn: Syslog là giao thức được sử dụng phổ biến nhất để gửi bản tin sự kiện. Giao thức Syslog có thể được sử dụng để ghi lại các loại sự kiện khác nhau và nó được hỗ trợ bởi một loạt các thiết bị. Bản tin sự kiện có thể được tạo bằng định dạng này bằng cách sử dụng rsyslog, đây là trình quản lý nhật ký mặc định trong các bản phân phối Linux phổ biến hoặc công cụ syslog-ng. Graylog cũng có thể nhận log thô, ở dạng thô hoặc ở định dạng JSON. Graylog có hỗ trợ sẵn cho các giao thức truyền tải TCP, UDP và hàng đợi vận chuyển Apache Kafka và RabbitMQ. Việc thu thập thông điệp nhật ký nội bộ của Graylog không được hỗ trợ theo mặc định nhưng có thể sử dụng plugin của bên thứ ba cho phép thu thập log nội bộ.

- Công cụ thu thập bên thứ ba: Graylog hỗ trợ một hệ thống gọi là Bộ thu thập Graylog, một dịch vụ cho các hệ thống Windows và Linux được sử dụng như một bộ thu thập log. Bộ thu thập log được cài đặt trên máy chủ chuyển tiếp các bản ghi nhật ký hoặc Eventlog tới máy chủ Graylog. Mỗi bộ thu thập chứa thông tin cấu hình như địa chỉ máy chủ Graylog, định dạng log cho phép. Bộ thu thập sử dụng NXLog, Filebeat hoặc Winlogbeat để thu thập nhật ký máy chủ. Bộ thu thập chuyển tiếp các bản tin đã

thu thập đến một địa chỉ IP và cổng máy chủ Graylog được cho phép, trên đó máy chủ Graylog đang hoạt động.

- GELF: Graylog có định dạng log riêng được gọi là Graylog Extended Log Format (GELF), là một chuỗi JSON nên được sử dụng đặc biệt để chuyển tiếp và xử lý các log ứng dụng. GELF hỗ trợ nhiều ngôn ngữ lập trình và có khả năng ghi lại mọi sự khác biệt được tạo ra bởi một ứng dụng cụ thể. GELF cung cấp cấu trúc nén và tối ưu hóa cho các mục đích của Graylog.



Hình 2. 4 Ví dụ về vòng đời của log trong Graylog

### 2.3.2 XỬ LÝ

Xử lý log đã nhận được thực hiện trong Luồng Graylog. Luồng là các nhóm ảo của log cho phép phân loại log theo các quy tắc được chỉ định. Nghĩa là có thể nhóm các bản ghi theo các trường khác nhau, chẳng hạn như mức độ nghiêm trọng của log hoặc địa chỉ IP nguồn. Các Luồng hỗ trợ hai loại quy tắc khác nhau. Đầu tiên là khi một bản tin phải khớp với tất cả các quy tắc được đưa ra (logic AND) hoặc khi một bản tin phải khớp với ít nhất một trong các quy tắc được đưa ra (logic OR). Log đến được xử lý một cách trực tiếp trong Bộ lọc bản tin. Bộ lọc bản tin là chuỗi chịu trách nhiệm phân tích log, thiết lập các trường tĩnh và gán log cho các luồng thích hợp. Hệ thống này phân tích các bản tin bởi một thành phần được gọi là Bộ trích xuất, trích xuất các trường tĩnh từ một bản tin log. Cấu trúc của mỗi định dạng log là khác nhau, đó là lý do tại sao các trình giải nén di động có thể được sử dụng cho các định dạng khác nhau. Bộ chỉ mục là một sự tổng hợp kiểm soát cách mà log được lưu trữ trên máy chủ Graylog. Nó định nghĩa các chính sách luân phiên, lưu trữ và cấu hình bộ nhớ Elasticsearch. Có thể thiết lập các chính sách luân chuyển khác nhau dựa trên kích thước luồng, thời gian hoặc số lượng bản tin và các chính sách lưu trữ được sử dụng để xóa log cũ nhằm ngăn không cho sử dụng quá nhiều dung lượng ổ đĩa. Mỗi luồng có một tập chỉ mục riêng của nó, tức là đối với các nhóm log khác nhau, có thể sử dụng các chính sách khác nhau.

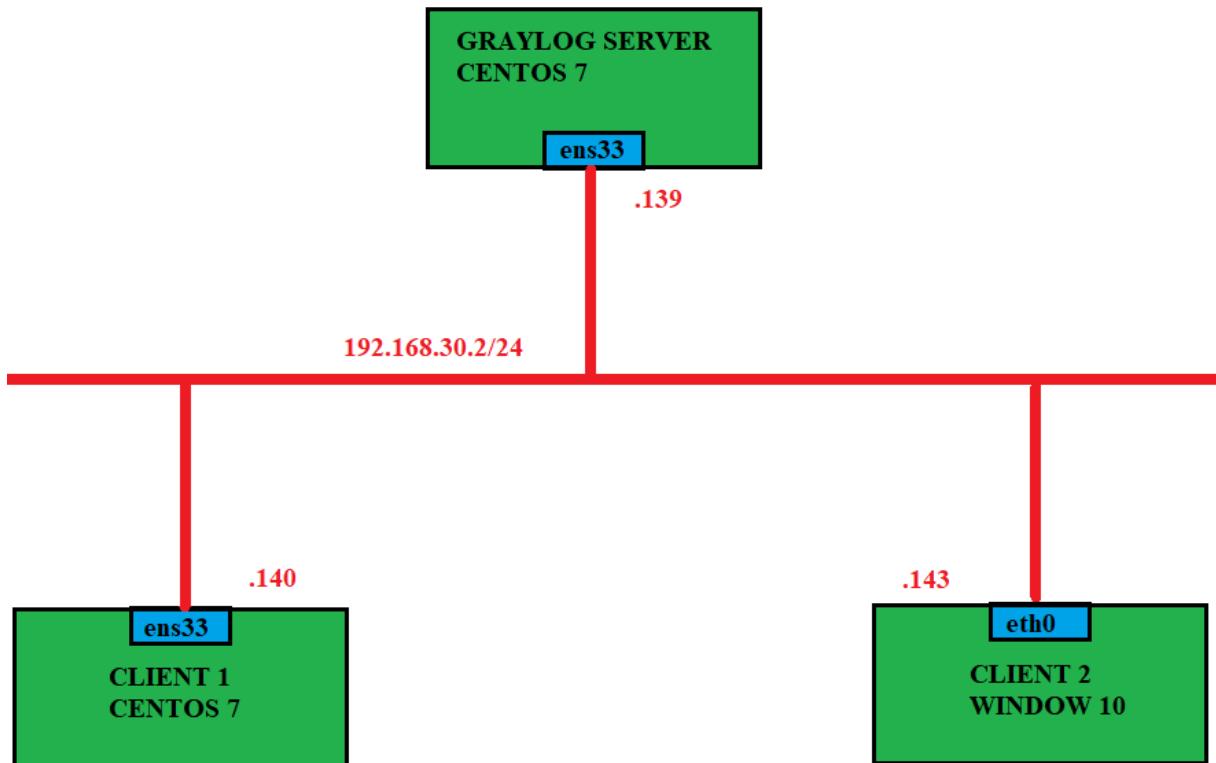
### 2.3.3 CHUYỂN TIẾP VÀ LUU TRỮ

Graylog có thể chuyển tiếp log tới các hệ thống khác hoặc lưu chúng cục bộ trên máy chủ. Graylog hỗ trợ chuyển tiếp log tới các hệ thống khác như SIEM hoặc một máy chủ Linux khác và định dạng được hỗ trợ duy nhất là GELF. Lưu trữ các bản tin là điều cần thiết cho các mục đích phân tích. Nó rất quan trọng nếu chúng ta muốn phân tích log trong các khoảng thời gian khác nhau và so sánh kết quả từ chúng. Hay nếu chúng ta muốn tìm kiếm, đồng thời hiển thị và theo dõi các thay đổi theo thời gian. Đôi với những trường hợp như vậy, log phải có sẵn. Log cũ hơn trong một thời gian nhất định không bắt buộc phải có sẵn ở bất cứ lúc nào nên được lưu trữ. Chính sách lưu trữ được hiểu cho mỗi bộ chỉ mục. Graylog chỉ có thể lưu trữ log cục bộ và không lưu trữ log trên các hệ thống bên ngoài khác như cơ sở dữ liệu hoặc NAS.

Hình 2.4 cho thấy các quá trình khác nhau, bao gồm thu thập và xử lý log, luồng, chỉ mục và chuyển tiếp mà hệ thống Graylog cung cấp. Trên hình, chúng ta có thể thấy 5 đầu vào log là Syslog TCP, GELF UDP, Log thô, CEF TCP, GELF Kafka được xác nhận để nhận log. Ta cũng thấy các ví dụ về 3 luồng là an ninh, ứng dụng, mạng và 2 bộ chỉ mục được dùng để ghi lại, lưu trữ log dài hạn và ngắn hạn. Ta thấy có thể chuyển tiếp log cho hệ thống của bên thứ ba. Đây là một ví dụ về cách hệ thống Graylog có thể được kết hợp.

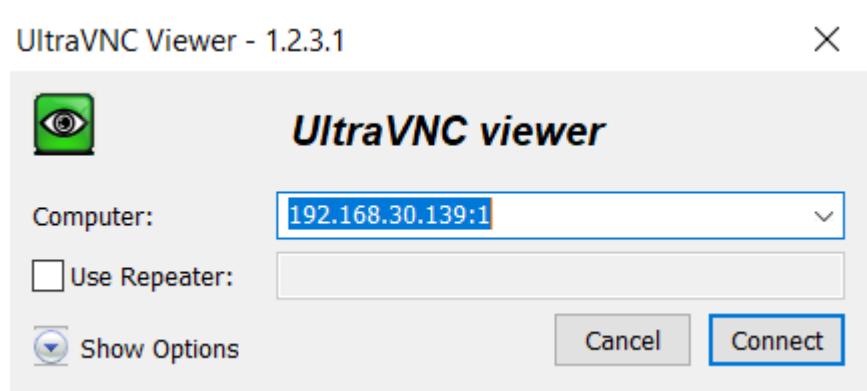
## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

### 3.1. MÔ HÌNH TRIỂN KHAI



Hình 3. 1 Mô hình triển khai

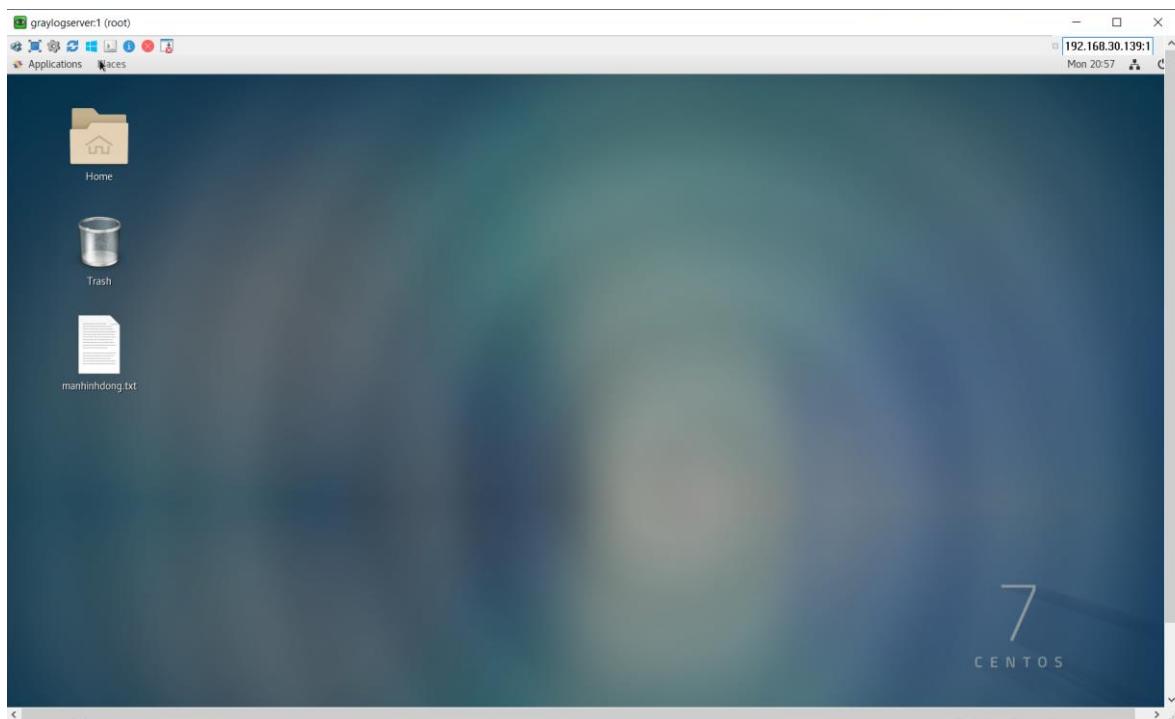
Connect VNC tới Graylog Server để cấu hình trên server:



Hình 3. 2 Mở UltraVNC để kết nối đến Graylog server



Hình 3. 3 Nhập password để kết nối VNC



Hình 3. 4 Đã kết nối VNC thành công

### 3.2. CÀI ĐẶT GRAYLOG-SERVER TRÊN CENTOS 7

#### • Thiết lập môi trường

Thực hiện update và cài đặt gói bổ trợ:

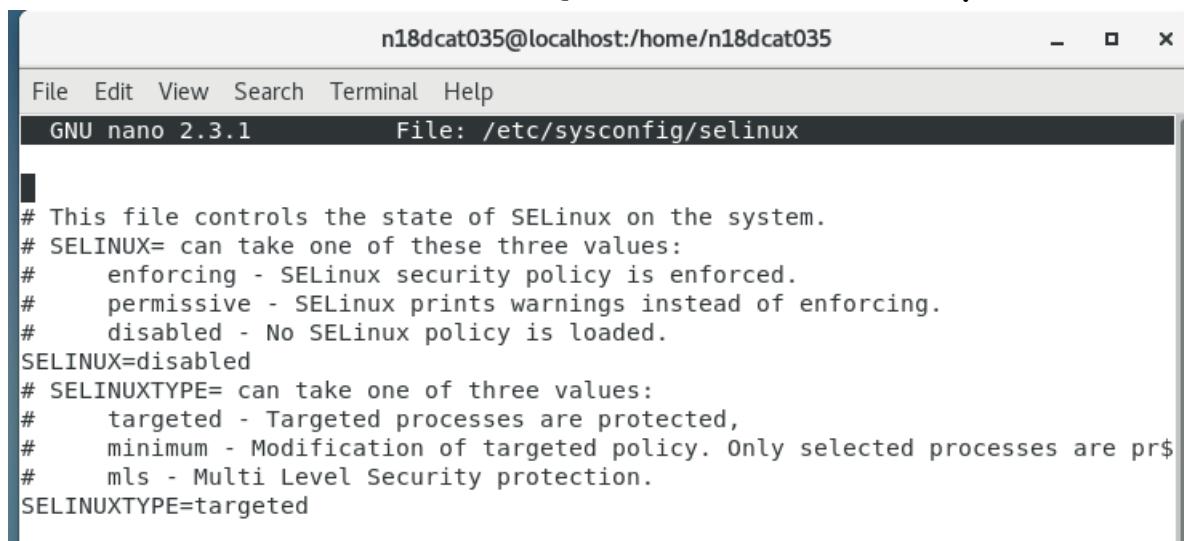
```
yum install -y epel-release
yum update -y
yum install -y git wget curl byobu
yum install -y pwgen
yum install -y httpd
```

Khởi động dịch vụ http:

```
systemctl start httpd
systemctl enable httpd
```

Tắt selinux:

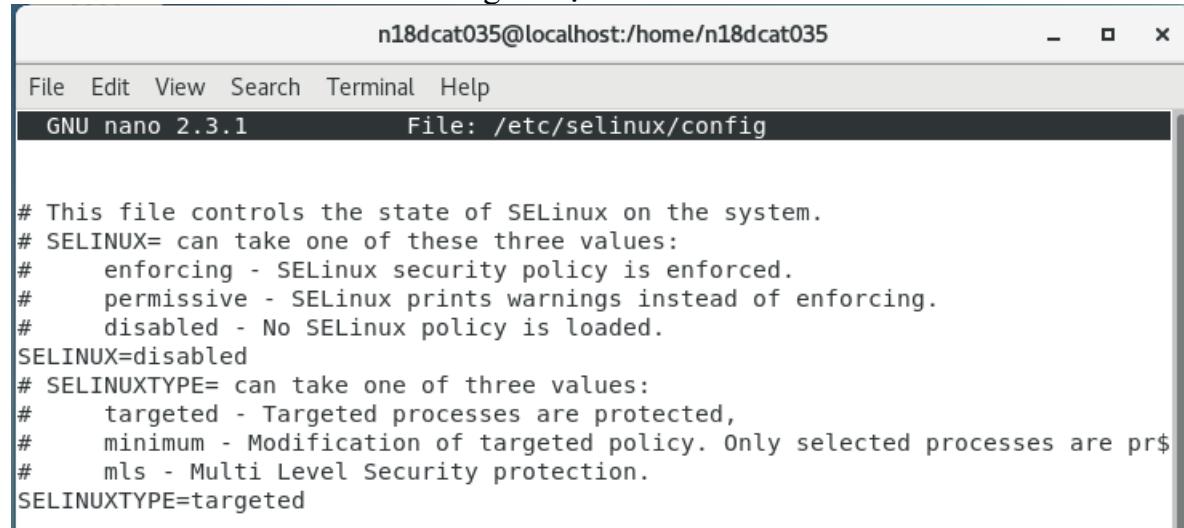
Chỉnh sửa /etc/sysconfig/selinux và đặt SELINUX thành disable



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are pr$ 
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Hình 3. 5 Cấu hình Selinux /etc/sysconfig/selinux graylogserver

## Chỉnh sửa /etc/selinux/config và đặt SELINUX thành disable



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are pr$ 
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Hình 3. 6 Cấu hình Selinux /selinux/config graylogserver

- Cài đặt NTP

Cấu hình thời gian là 1 bước rất quan trọng vì để nhận log 1 cách chính xác nhất thì thời gian cũng phải chính xác. Có 2 cách cài ntp là ta có thể cấu hình thủ công ntp server hoặc đồng bộ từ máy chủ ntp (trong hoặc ngoài mạng)

Trong trường hợp này mình sẽ đồng bộ thời gian từ máy chủ ntp bên trong mạng.

Cấu hình ntp trên cả máy Client và Server:

```
yum install -y chrony
```

Để thời gian được đồng bộ, sửa file cấu hình /etc/chrony.conf như sau:

```
[root@localhost n18dcat035]# cat /etc/chrony.conf | egrep -v '^$|^#'
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
allow 192.168.30.0/24
logdir /var/log/chrony
```

Hình 3. 7 Cấu hình Chrony graylogserver

Khởi động và kích hoạt chrony:

```
systemctl start chronyd
systemctl enable chronyd
```

Kiểm tra lại đồng bộ hóa thời gian:

```
chronyc sources
```

```
[root@localhost n18dcat035]# chronyc sources
210 Number of sources = 4
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
```

MS Name/IP address	Stratum	Poll	Reach	LastRx	Last sample
^+ time.cloudflare.com	3	6	377	9 +1337us [+1653us]	+/- 95ms
^+ time.cloudflare.com	3	6	377	10 +1620us [+1935us]	+/- 95ms
^* 203.113.174.44	3	6	377	9 -17us [+300us]	+/- 75ms
^+ unknown.tino.vn	2	6	377	9 -3750us [-3750us]	+/- 100ms

Hình 3. 8 Check chronyc sources graylogserver

Kiểm tra thời gian hệ thống:

```
timedatectl
```

```
[root@localhost n18dcat035]# timedatectl
    Local time: Fri 2022-09-02 15:26:13 +07
    Universal time: Fri 2022-09-02 08:26:13 UTC
        RTC time: Fri 2022-09-02 08:26:13
        Time zone: Asia/Ho_Chi_Minh (+07, +0700)
    NTP enabled: yes
    NTP synchronized: yes
      RTC in local TZ: no
        DST active: n/a
```

Hình 3. 9 Check timedatectl graylogserver

- Cài đặt Java

```
yum install -y java-1.8.0-openjdk-headless.x86_64
```

- Cài đặt MongoDB

Khai báo repo cho MongoDB:

Tạo file /etc/yum.repos.d/mongodb-org.repo và khai báo nội dung như sau:

```
[root@localhost yum.repos.d]# cat mongodb-org.repo
[mongodb-org-4.2]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/4.2/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-4.2.asc
```

Hình 3. 10 Tạo file mongodb repo graylogserver

Cài đặt MongoDB:

```
yum install -y mongodb-org
```

Khởi động MongoDB:

```
systemctl daemon-reload
systemctl enable mongod.service
systemctl start mongod.service
```

Kiểm tra trạng thái của MongoDB:

```
systemctl status mongod
```

- Cài đặt Elasticsearch

Khai báo repo cho Elasticsearch:

```
rpm --import http://packages.elastic.co/GPG-KEY-
elasticsearch
```

Chạy lệnh sau để tạo file /etc/yum.repos.d/elasticsearch.repo và khai báo nội dung cho repo:

```
[root@localhost yum.repos.d]# cat elasticsearch.repo
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/oss-7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Hình 3. 11 Tạo file elasticsearch graylogserver

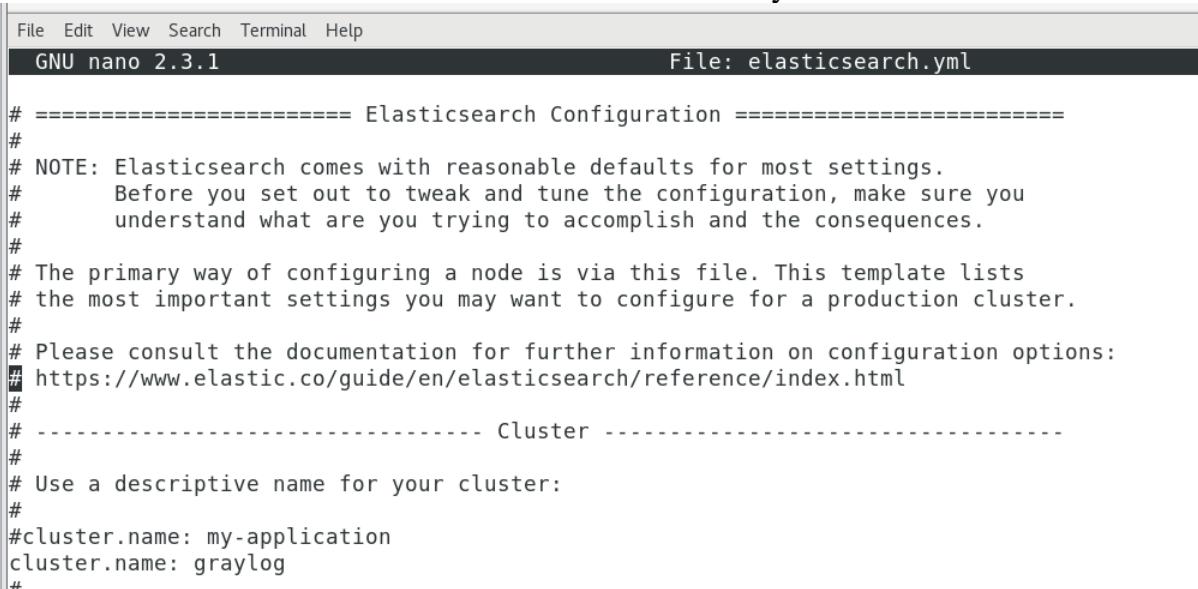
Cài đặt Elasticsearch

```
yum install -y elasticsearch
```

Backup file cấu hình elasticsearch:

```
cp /etc/elasticsearch/elasticsearch.yml
/etc/elasticsearch/elasticsearch.yml.bk
```

Sửa file cấu hình /etc/elasticsearch/elasticsearch.yml của elasticsearch như sau:



```

File Edit View Search Terminal Help
GNU nano 2.3.1                                         File: elasticsearch.yml

# ===== Elasticsearch Configuration =====
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
# Before you set out to tweak and tune the configuration, make sure you
# understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
#cluster.name: my-application
cluster.name: graylog
#

```

Hình 3. 12 Edit file elasticsearch.yml graylogserver

Khởi động lại elasticsearch

```

systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl restart elasticsearch.service

```

Kiểm tra trạng thái của elasticsearch

```
systemctl status elasticsearch.service
```

- Cài đặt graylog

Tải về repo của graylog:

```

sudo rpm -Uvh
https://packages.graylog2.org/repo/packages/graylog-4.2-
repository_latest.rpm

```

Cài đặt graylog 4:

```

yum update && sudo yum install -y graylog-server graylog-
enterprise-plugins graylog-integrations-plugins graylog-
enterprise-integrations-plugins

```

Thực hiện backup trước khi sửa file cấu hình phòng khi bị lỗi:

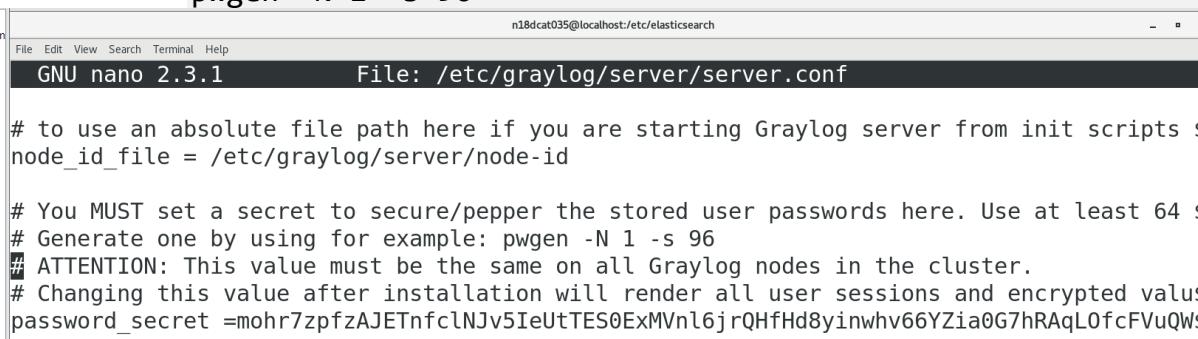
```

cp /etc/graylog/server/server.conf
/etc/graylog/server/server.conf.bk

```

Tạo chuỗi hash gồm 96 ký tự để khai báo cho password\_secret sau đó lưu vào file cấu hình /etc/graylog/server/server.conf:

```
pwgen -N 1 -s 96
```



```

n18dcat035@localhost:/etc/elasticsearch
File Edit View Search Terminal Help
GNU nano 2.3.1                                         File: /etc/graylog/server/server.conf

# to use an absolute file path here if you are starting Graylog server from init scripts $node_id_file = /etc/graylog/server/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 $
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted valus
password_secret =mohr7zpfzAJETnfclNJv5IeUtTES0ExMVnl6jrQHfHd8yinwhv66YZia0G7hRAqL0fcFVuQW$
```

Hình 3. 13 Thêm password secret vào server.conf graylogserver

Tạo mật khẩu đăng nhập cho tài khoản admin để đăng nhập graylog:

```
echo -n Aa123456@ | sha256sum
```

```
n18dc035@localhost:/etc/elasticsearch
```

```
File Edit View Search Terminal Help
GNU nano 2.3.1      File: /etc/graylog/server/server.conf
```

```
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you nee$
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 =e11298cd0fdcbfe59a4701dfd2494a2a3815706b8029ef65a672d1fc35480b3
```

Hình 3. 14 Thêm password cho tài khoản đăng nhập vào server.conf graylogserver

Trong đó: Aa123456@ là mật khẩu sử dụng để đăng nhập vào graylog bằng user admin

Đặt timezone cho graylog:

```
# The time zone setting of the root user
# Default is UTC
root_timezone = Asia/Ho_Chi_Minh
```

Hình 3. 15 Đặt timezone trong server.conf graylogserver

Đặt địa chỉ sử dụng để truy cập web interface bằng nhiều card mạng:

```
http_bind_address = 0.0.0.0:9000
```

Hình 3. 16 Đặt web interface cho nhiều card truy cập trong server.conf graylogserver

```
http_enable_cors = true
```

Hình 3. 17 Thêm http\_enable\_cors = true trong server.conf graylogserver

Bỏ comment để sử dụng user admin:

```
# The default root user is named 'admin'
root_username = admin
```

Hình 3. 18 Sử dụng root admin user trong server.conf graylogserver

Khởi động dịch vụ graylog-server:

```
systemctl daemon-reload
systemctl enable graylog-server.service
systemctl start graylog-server.service
```

Kiểm tra trạng thái của graylog-server:

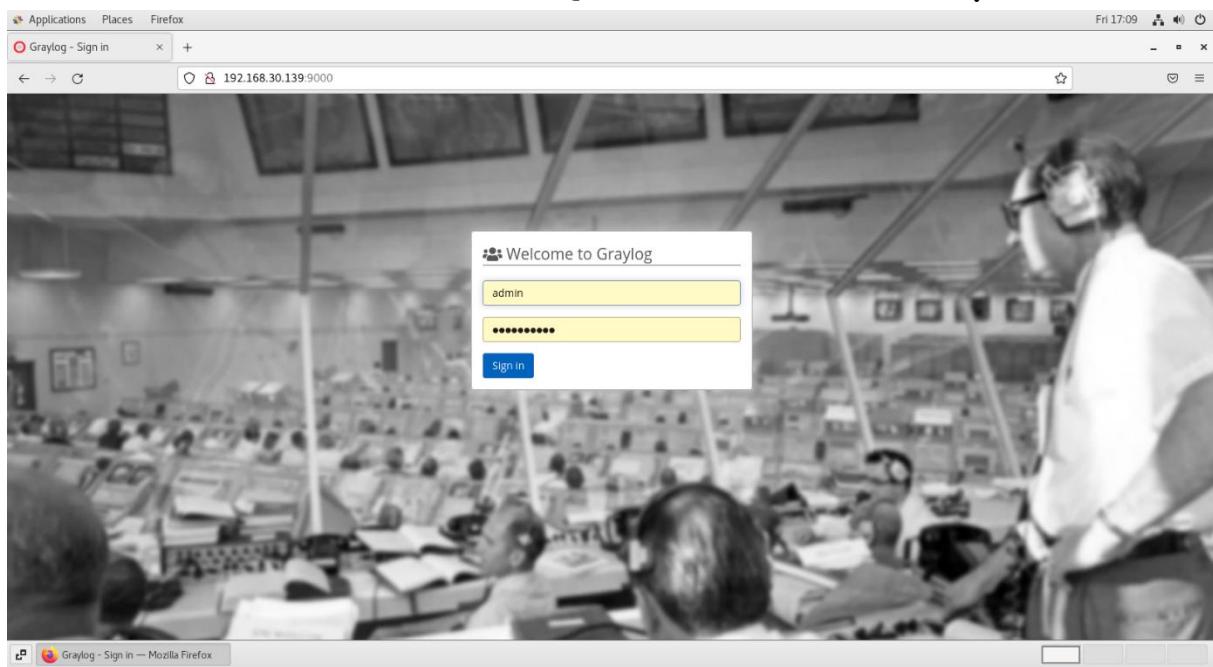
```
systemctl status graylog-server
```

Để truy cập graylog qua port 9000, ta cần tiến hành mở port trên firewall :

```
firewall-cmd --zone=public --add-port=9000/tcp --
permanent
firewall-cmd --reload
```

- Login

Login với địa chỉ 192.168.30.139:9000 bằng user: admin và password: Aa123456@@ để đăng nhập vào Web interface của dịch vụ graylog.



Hình 3. 19 Test login vào web interface Graylog graylogserver

### 3.3. CẤU HÌNH THU THẬP LOG CLIENT 1 CENTOS 7 THÔNG QUA GRAYLOG-SIDECAR

- Thiết lập môi trường

Thực hiện update và cài đặt gói bổ trợ:

```
yum install -y epel-release
yum update -y
yum install -y git wget curl byobu
yum install -y pwgen
```

Tắt selinux:

```
nano /etc/sysconfig/selinux
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# Commented out to enable SELinux by default
```

Hình 3. 20 Cấu hình Selinux /etc/sysconfig/selinux client1

```
nano /etc/selinux/config
```

```
client1@localhost:/home/client1
File Edit View Search Terminal Help
GNU nano 2.3.1          File: /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
```

*Hình 3. 21 Cấu hình Selinux /selinux/config client1*

- Cài đặt NTP

Cấu hình ntp trên cả máy Client và Server:

```
yum install -y chrony
```

Để thời gian được đồng bộ, sửa file cấu hình /etc/chrony.conf như sau:

```
[root@localhost client1]# cat /etc/chrony.conf | egrep -v '^$|^#'
server 192.168.30.139 iburst
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
logdir /var/log/chrony
```

*Hình 3. 22 Cấu hình Chrony client1*

Lưu ý: 192.168.30.139 là địa chỉ IP của ntp server trong mạng.

Khởi động và kích hoạt chrony:

```
systemctl start chronyd
systemctl enable chronyd
```

Kiểm tra lại đồng bộ hóa thời gian:

```
chronyc sources
```

```
[root@localhost client1]# chronyc sources
210 Number of sources = 1
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
* 192.168.30.139        3    6   377   39      +11us[ +17us] +/-   60ms
```

*Hình 3. 23 Check chronyc sources client1*

Kiểm tra thời gian hệ thống:

```
timedatectl
```

```
[root@localhost client1]# timedatectl
Local time: Fri 2022-09-02 17:38:14 +07
Universal time: Fri 2022-09-02 10:38:14 UTC
RTC time: Fri 2022-09-02 10:38:13
Time zone: Asia/Ho_Chi_Minh (+07, +0700)
NTP enabled: yes
NTP synchronized: yes
RTC in local TZ: no
DST active: n/a
```

*Hình 3. 24 Check timedatectl client1*

- Cài đặt Filebeat và Sidecar

Cài đặt file Beats

```
#curl -L -O https://artifacts.elastic.co/downloads/beats
/filebeat/filebeat-8.4.1-x86_64.rpm
#sudo rpm -vi filebeat-8.4.1-x86_64.rpm
```

- Cài đặt graylog-sidecar

Tải về kho lưu trữ và cài đặt graylog-sidecar:

```
#sudo rpm -Uvh
https://packages.graylog2.org/repo/packages/graylog-
sidecar-repository-1-2.noarch.rpm
#sudo yum install graylog-sidecar
```

Lưu ý: Để cấu hình sidecar, trước tiên ta cần đăng nhập vào Web Interface của graylog để tạo và lấy Token. Một mã token có thể dùng chung cho nhiều client cùng sử dụng sidecar.

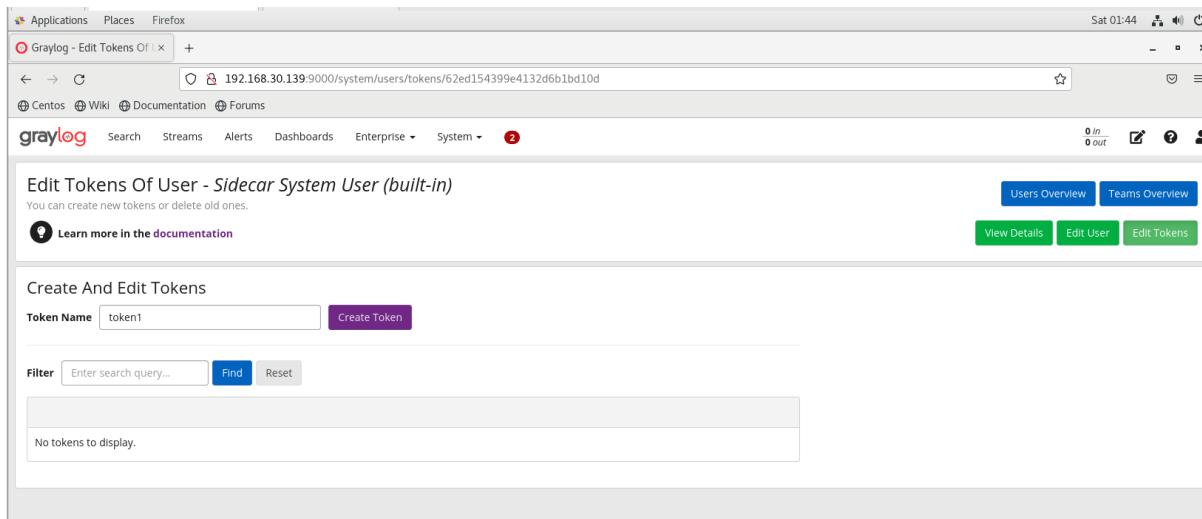
Sau đây là các bước để tạo và copy mã token:

Bước 1: Vào Web Interface của graylog, truy cập tab System/Sidecars , sau đó chọn Create or reuse a token for the graylog-sidecar user.

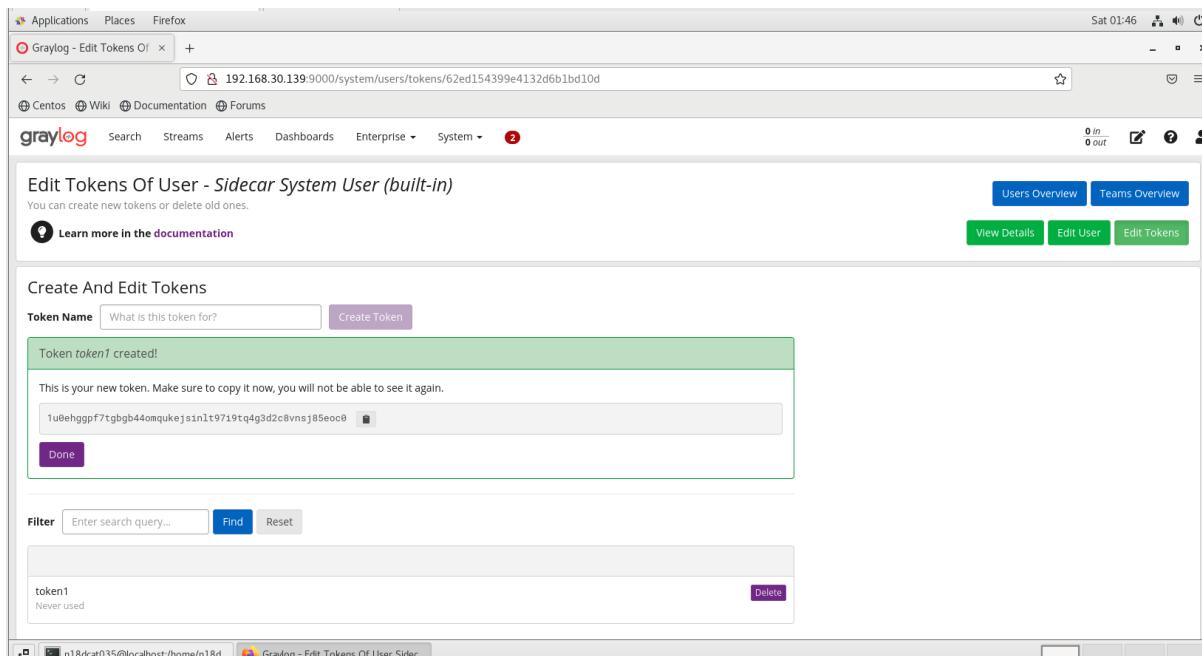
The screenshot shows a Firefox browser window with the URL [192.168.30.139:9000/system/users/tokens/62ed154399e4132d6b1bd10d](http://192.168.30.139:9000/system/users/tokens/62ed154399e4132d6b1bd10d). The page title is "Edit Tokens Of User - Sidecar System User (built-in)". It includes tabs for "Users Overview" and "Teams Overview". Below the tabs are buttons for "View Details", "Edit User", and "Edit Tokens". The main content area is titled "Create And Edit Tokens" and contains a "Token Name" input field with placeholder "What is this token for?", a "Create Token" button, and a "Filter" section with a search input and "Find" and "Reset" buttons. A message at the bottom states "No tokens to display." The status bar at the bottom of the browser window shows "Graylog 4.2.11+ec7c16b on localhost (Red Hat, Inc. 1.8.0\_342 on Linux 3.10.0-1160.71.1.el7.x86\_64)".

Hình 3. 25 Tạo token sidecar graylogserver

Bước 2: Nhập tên và chọn Create Token để tạo token, nên tạo tên token theo nhóm để gợi nhớ và sử dụng chung.



Hình 3. 26 Nhập tên token graylogserver



Hình 3. 27 Tạo thành công token graylogserver

Bước 3: Sau đó ta copy mã token để sử dụng cho việc cấu hình graylog-sidecar.

Mã token có dạng như sau:

**1u0ehggpf7tgbgb44omqukejsinlt97i9tq4g3d2c8vnsj85eoc0**

Lưu ý: Nếu muốn lấy mã token đã tạo trước đó, ta có thể thực hiện các bước như tạo token, sau đó tìm mã token sẵn có và copy.

Quay lại máy Graylog-sidecar (client 1) để chỉnh sửa file config, các thao tác sửa đổi được thực hiện ở file /etc/graylog/sidecar/sidecar.yml.

Thực hiện backup file phòng khi cấu hình bị lỗi:

```
#cp /etc/graylog/sidecar/sidecar.yml
/etc/graylog/sidecar/sidecar.yml.bk
```

Cấu hình tệp /etc/graylog/sidecar/sidecar/sidecar.yml

```
[root@localhost client1]# cat /etc/graylog/sidecar/sidecar.yml | egrep -v '^$|^#' 
server_url: "http://192.168.30.139:9000/api/" 
server_api_token: "l220nv5tk00c0psp9kep8vg4pd1qd14ma527tnv2obbvn0mbgn9" 
node_id: "file:/etc/graylog/sidecar/node-id" 
node_name: "client1" 
tls_skip_verify: true 
log_path: "/var/log/graylog-sidecar"
```

Hình 3. 28 Cấu hình sidecar client

Tiến hành khởi động dịch vụ graylog-sidecar:

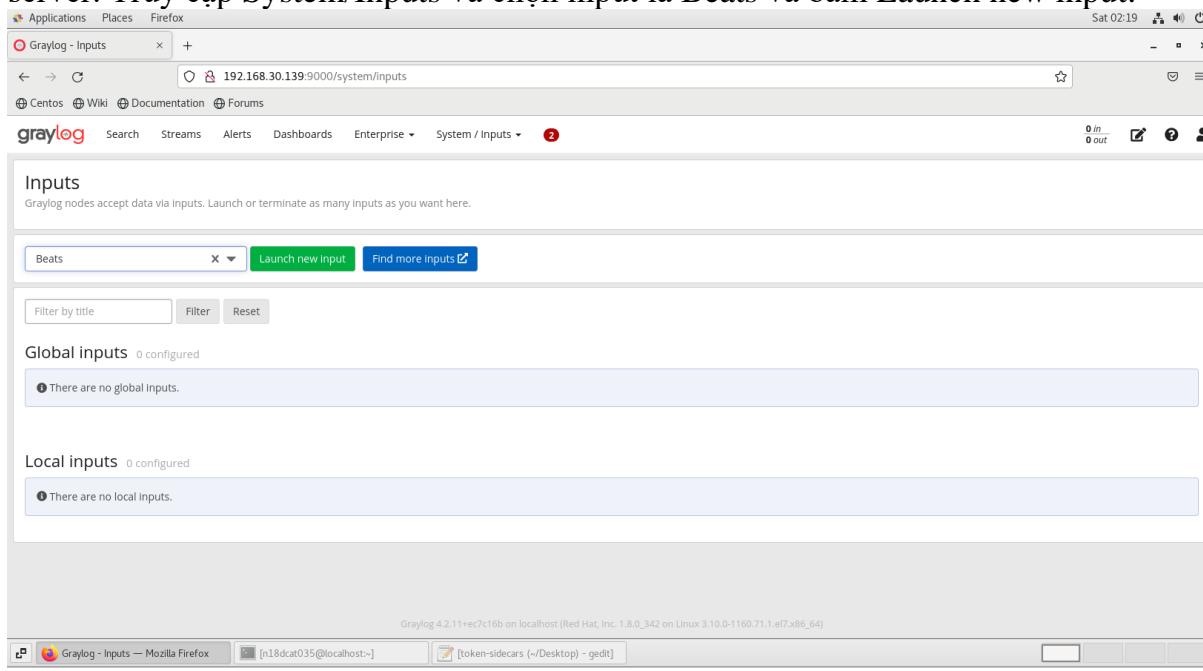
```
graylog-sidecar -service install
systemctl start graylog-sidecar
systemctl enable graylog-sidecar
```

Kiểm tra lại trạng thái graylog-sidecar:

```
systemctl status graylog-sidecar
```

- Cấu hình Sidecar trên Web Interface của graylog-server
  - Khai báo input cho Sidecar

Để graylog-server biết nơi cần nhận log, ta cần khai báo input cho graylog-server. Truy cập System/Inputs và chọn input là Beats và bấm Launch new input:



Hình 3. 29 Tạo Input Beats graylogserver

Tiếp đến ta edit input như sau:

Launch new Beats input

Global  
Should this input start on all nodes

**Node**  
32f5ed63 / localhost

On which node should this input start

**Title**  
beats

Select a name of your new input that describes it.

**Bind address**  
0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

**Port**  
5044

Port to listen on.

**Receive Buffer Size (optional)**  
1048576

The size in bytes of the recvBufferSize for network connections to this input.

**No. of worker threads (optional)**  
2

Number of worker threads processing network connections for this input.

**TLS cert file (optional)**

Path to the TLS certificate file

Hình 3. 30 Edit thông tin Input Beats graylogserver

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

Path to the TLS certificate file

**TLS private key file (optional)**

Path to the TLS private key file

**Enable TLS**

Accept TLS connections

**TLS key password (optional)**

The password for the encrypted key file.

**TLS client authentication (optional)**

Whether clients need to authenticate themselves in a TLS connection

**TLS Client Auth Trusted Certs (optional)**

TLS Client Auth Trusted Certs (File or Directory)

**TCP keepalive**

Enable TCP keepalive packets

**Override source (optional)**

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

**Do not add Beats type as prefix**

Do not prefix each field with the Beats type, e.g. "source" -> "filebeat\_source".

Hình 3.31 Chọn Save để save Input graylogserver

Sau khi tạo, ta có được input của file beats như sau:

The screenshot shows the Graylog web interface at the URL `192.168.30.139:9000/system/inputs`. The page displays the 'Global inputs' section, which is currently empty. Below it, the 'Local inputs' section shows one configured input named 'beats'. The 'beats' input details are as follows:

```
beats Beat: RUNNING  
On node ★ 32f5ed63 / localhost  
bind_address: 0.0.0.0  
no_beats_prefix: false  
number_worker_threads: 2  
override_source: <empty>  
port: 5044  
recv_buffer_size: 1048576  
tcp_keepalive: false  
tls.cert_file: <empty>  
tls.client_auth: disabled  
tls.client_auth_cert_file: <empty>  
tls.enable: false  
tls.key_file: <empty>  
tls.key_password:*****
```

Below the configuration, there are buttons for 'Show received messages', 'Manage extractors', 'Stop Input', and 'More actions'. On the right side of the page, there is a 'Throughput & Metrics' panel showing network statistics: 1 minute average rate: 0 msg/s, Network IO: ~0B ~0B (total ~0B ~0B), Active connections: 0 (0 total), and Empty messages discarded: 0.

Hình 3.32 Input Beats đã tạo thành công graylogserver

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

### o Cấu hình Sidecars

#### Truy cập vào System/Sidecar:

Hình 3. 33 Truy cập Sidecar graylogserver

Chọn Config sidecar để cấu hình cho đầu vào log. Sau đó chọn tab Configuration sau đó chọn Create Configuration:

Hình 3. 34 Tạo configuration sidecar graylogserver

Khai báo các thông số và sửa địa chỉ ip thành địa chỉ của graylog-server, sau đó bổ sung trường fields.source: \${sidecar.nodeName}

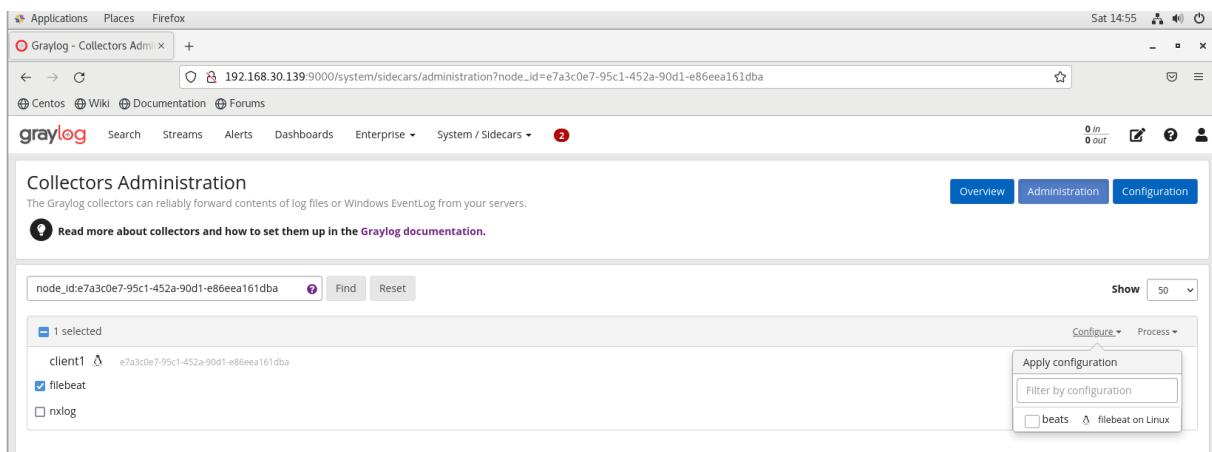
```
1 # Needed for Graylog
2 fields.under_host: true
3 fields.collector.node_id: ${sidecar.nodeName}
4 fields.giz_source_collector: ${sidecar.nodeName}
5 fields.giz_target_collector: ${sidecar.nodeName}
6 filebeat.inputs:
7   - input_type: log
8     path: "/var/log/*/*"
9     type: log
10    output.logstash:
11      hosts: ["192.168.30.139:5044"]
12      path: "/var/lib/graylog-log-sidecar/collectors/filebeat/data"
13      logs: "/var/lib/graylog-log-sidecar/collectors/filebeat/log"
```

Hình 3. 35 Chính sửa các thông tin cần thiết sidecar client1 graylogserver

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

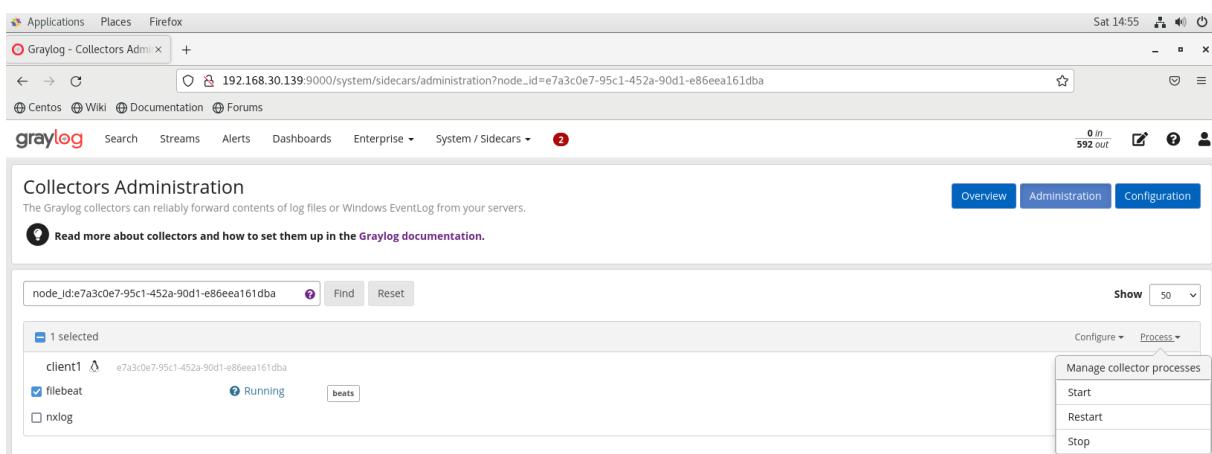
Tiếp theo, chọn tab Administration, tích chọn filebeat. Sau đó chọn configuration vừa tạo :



The screenshot shows the 'Collectors Administration' page of the Graylog web interface. The URL is 192.168.30.139:9000/system/sidecars/administration?node\_id=e7a3c0e7-95c1-452a-90d1-e86eea161dba. The 'Administration' tab is active. A search bar contains 'node\_id:e7a3c0e7-95c1-452a-90d1-e86eea161dba'. Below it, a list shows '1 selected': 'client1' (selected) and 'filebeat' (checked). On the right, there's a 'Configure' dropdown with 'Apply configuration' highlighted.

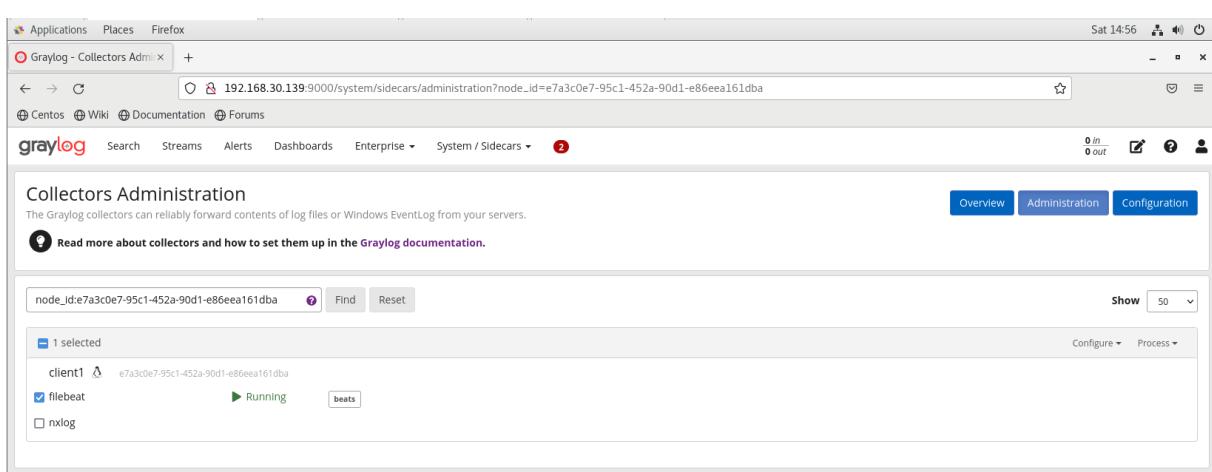
Hình 3. 36 Chọn Filebeat , chọn configuration vừa tạo graylogserver

Tiếp đến chọn Process -> Start để khởi động trình thu thập log từ client1, có một cửa sổ bật lên, chọn Confirm để tiếp tục:



The screenshot shows the 'Collectors Administration' page with the 'Process' tab active. The URL is 192.168.30.139:9000/system/sidecars/administration?node\_id=e7a3c0e7-95c1-452a-90d1-e86eea161dba. The 'filebeat' collector is listed as 'Running'. A dropdown menu next to 'Process' includes 'Start', 'Restart', and 'Stop' options.

Hình 3. 37 Khởi động trình thu thập log từ client1 graylogserver



The screenshot shows the 'Collectors Administration' page with the 'filebeat' collector now listed as 'Running'. The URL is 192.168.30.139:9000/system/sidecars/administration?node\_id=e7a3c0e7-95c1-452a-90d1-e86eea161dba.

Hình 3. 38 Đã hoàn thành trình thu thập log sidecar client1 graylogserver

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

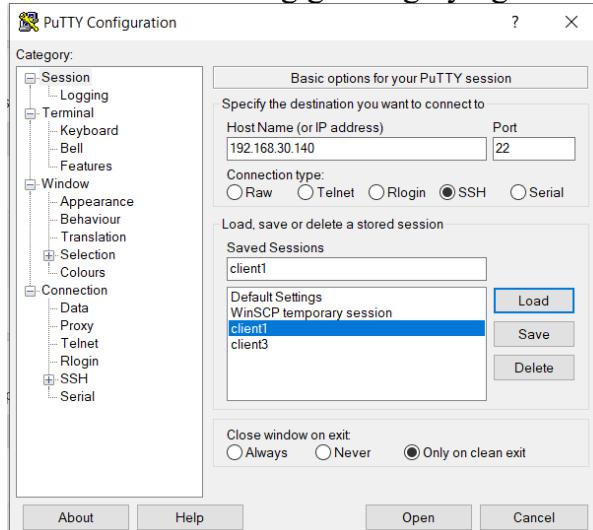
- Kiểm tra kết quả

Chuyển sang tab Overview và chọn Show messages:

The screenshot shows the 'Sidecars Overview' page in a Firefox browser. The URL is 192.168.30.139:9000/system/sidecars. The page lists two sidecars: 'client1' and 'client3'. Both are shown as 'Running' with 'Linux' operating systems. They were last seen 'a few seconds ago'. Their Node IDs are e7a3c0e7-95c1-452a-90d1-e86eea161dba and d9ee55af-52ed-4fe9-9c77-81187efebace respectively. Both are running version 1.2.0. There are 'Manage sidebar' and 'Show messages' buttons for each.

Hình 3. 39 Show messages sidecar client1 graylogserver

Sau đó ssh vào máy client1 và kiểm tra log gửi về graylog-server:

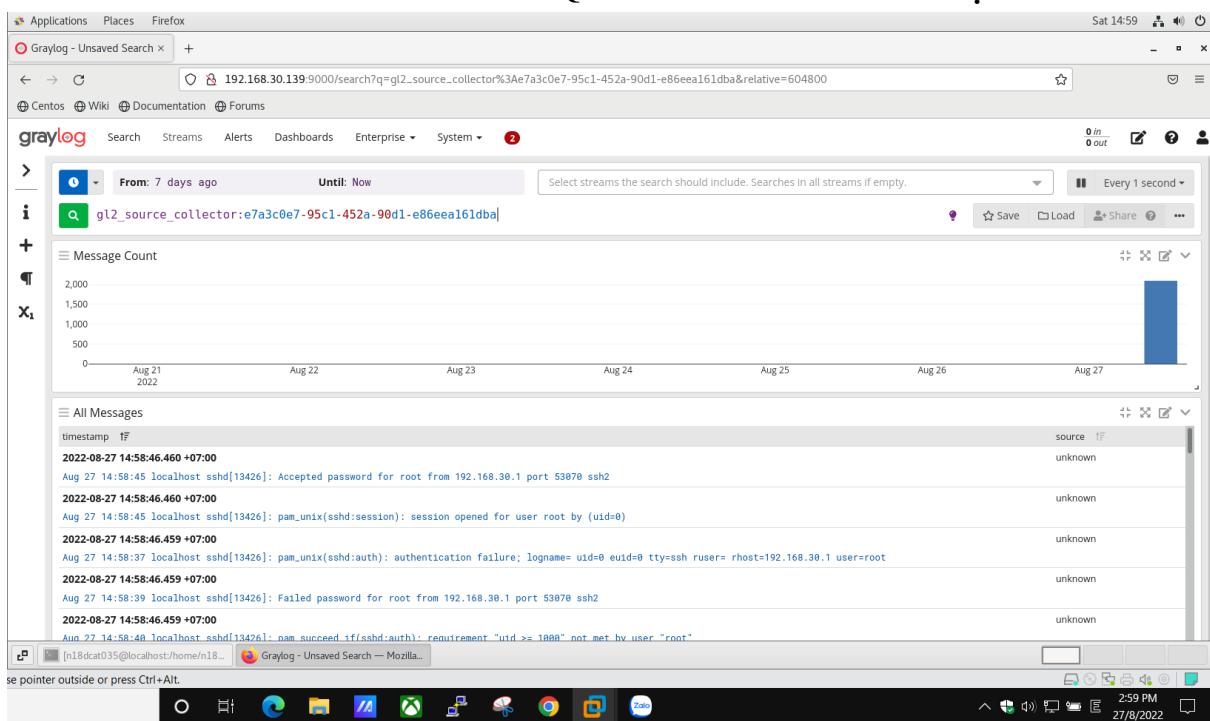


Hình 3. 40 Mở Putty SSH client1

The screenshot shows an SSH terminal window. The user is attempting to log in as 'root' from 'localhost' to '192.168.30.140'. The password is entered three times, but access is denied each time. The terminal also displays a message about failed logins and the last successful login.

```
root@localhost:~  
[root] login as: root  
[root] root@192.168.30.140's password:  
Access denied  
[root] root@192.168.30.140's password:  
Access denied  
[root] root@192.168.30.140's password:  
Last failed login: Sat Aug 27 15:02:40 +07 2022 from 192.168.30.1 on ssh:notty  
There were 2 failed login attempts since the last successful login.  
Last login: Sat Aug 27 14:58:45 2022 from 192.168.30.1  
[root@localhost ~]#
```

Hình 3. 41 SSH thành công vào client1



Có log đầy về như hình trên là đã cài thành công !!

### 3.4. CẤU HÌNH THU THẬP LOG CLIENT 2 WINDOWS THÔNG QUA GRAYLOG-SIDECAR

- Cài đặt và cấu hình
    - Cài đặt graylog sidecar trên windows 10
- Ở phần trước đã hướng dẫn tạo token trên graylog-server, bây giờ ta chỉ việc copy mã token đã tạo trước đó để phục vụ cho việc cấu hình hiện tại.

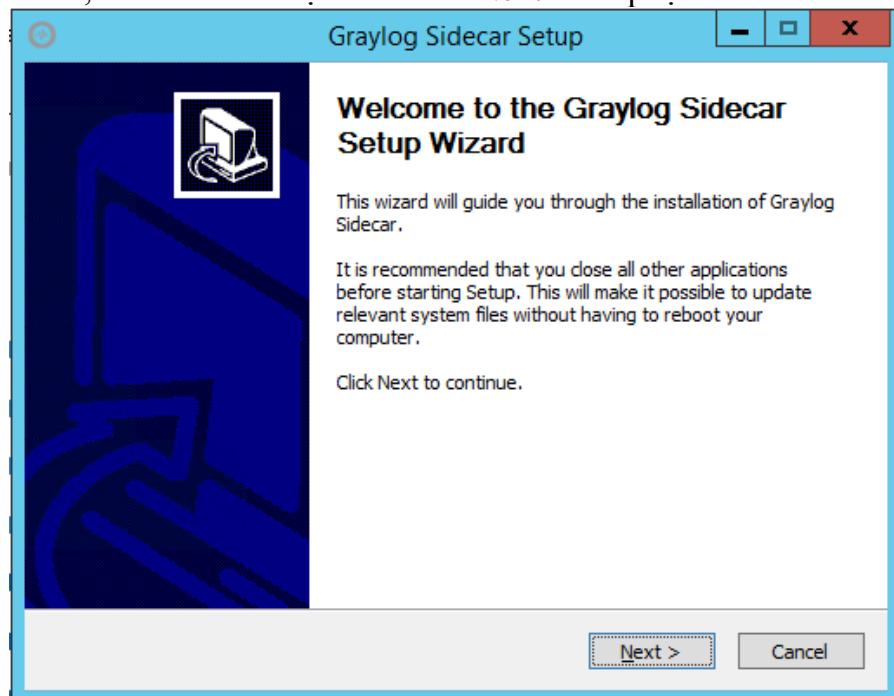
#### Tải graylog-sidecar

<a href="#">graylog-sidecar-1.2.0-1.armv7.rpm</a>	2.37 MB	02 Jun 2022
<a href="#">graylog-sidecar-1.2.0-1.i386.rpm</a>	2.41 MB	02 Jun 2022
<a href="#">graylog-sidecar-1.2.0-1.x86_64.rpm</a>	2.64 MB	02 Jun 2022
<a href="#">graylog-sidecar-1.2.0.0.tar.gz</a>	24.6 MB	02 Jun 2022
<a href="#">graylog-sidecar_1.2.0-1_amd64.deb</a>	2.66 MB	02 Jun 2022
<a href="#">graylog-sidecar_1.2.0-1_armv7.deb</a>	2.39 MB	02 Jun 2022
<a href="#">graylog-sidecar_1.2.0-1_i386.deb</a>	2.43 MB	02 Jun 2022
<a href="#">graylog_sidecar_installer_1.2.0-1.exe</a>	62.8 MB	02 Jun 2022
<a href="#">graylog_sidecar_installer_1.2.0-1.exe.sha256.txt</a>	65 Bytes	02 Jun 2022
<a href="#">Source code (zip)</a>		02 Jun 2022
<a href="#">Source code (tar.gz)</a>		02 Jun 2022

2 people reacted

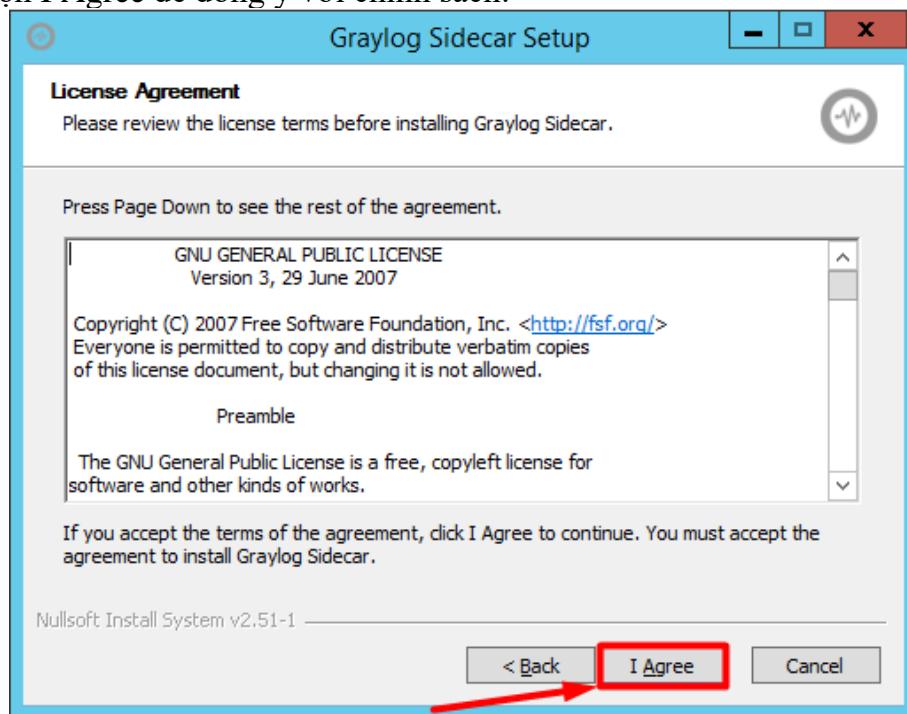
Hình 3. 43 Tải sidecar cho window

Khi tải về, tiến hành cài đặt file. Bấm Next để tiếp tục:



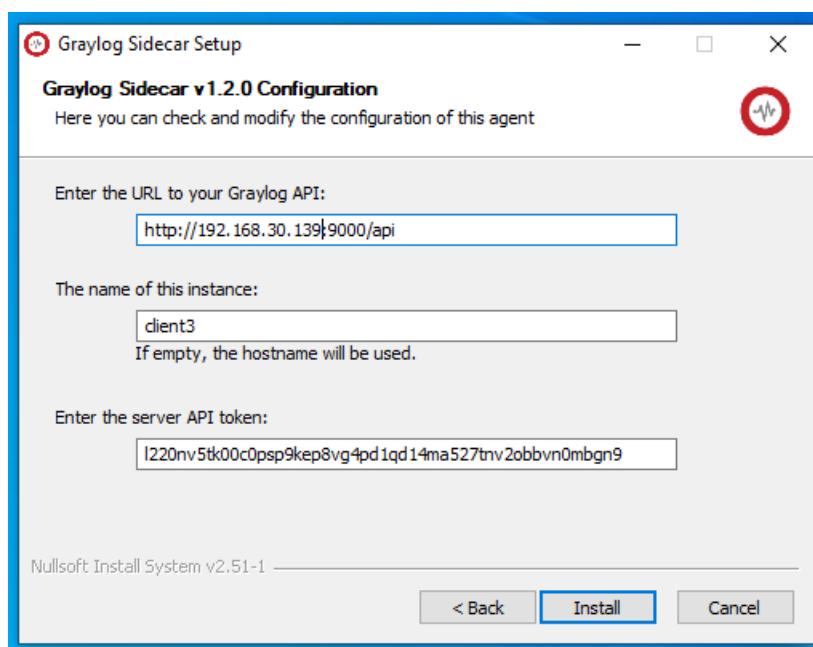
Hình 3. 44 Cài đặt sidebar window

Chọn I Agree để đồng ý với chính sách:



Hình 3. 45 Chọn I agree

Tiếp theo khai báo 1 số thông số cấu hình cho graylog-sidecar:



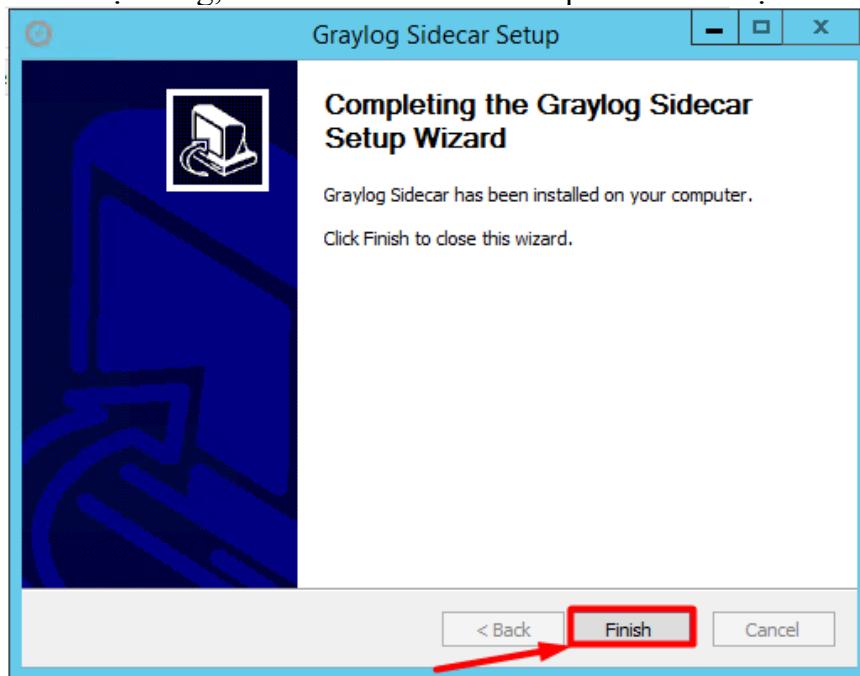
Hình 3. 46 Edit sidecar window

Ở ô đầu tiên ta khai báo địa chỉ api của graylog-server

Tiếp theo ta khai báo hostname cho graylog server

Ở tại ô cuối cùng, ta điền giá trị api token của graylog-server đã tạo trước đó

Sau khi cài đặt xong, bấm Finish để kết thúc quá trình cài đặt:



Hình 3. 47 Chọn Finish

Mở CMD và thực hiện các lệnh để khởi động graylog sidecar

```
"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -  
service install  
"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -  
service start
```

- Cấu hình trên graylog server để nhận log từ windows
  - Cấu hình sidecars

#### Truy cập vào System/Sidecar:

Name	Status	Operating System	Last Seen	Node Id	Sidecar Version		
client1	▶ Running	Linux	a few seconds ago	e7a3c0e7-95c1-452a-90d1-e86eea161dba	1.2.0	<a href="#">Manage sidecar</a>	<a href="#">Show messages</a>
client3	▶ Running	Windows	a few seconds ago	c713cd04-7845-4a10-9101-c62558fce335	1.2.0	<a href="#">Manage sidecar</a>	<a href="#">Show messages</a>

Hình 3. 48 Truy cập Sidecar graylogserver

Chọn Config sidecar để cấu hình cho đầu vào log. Sau đó chọn tab Configuration sau đó chọn Create Configuration:

Configuration	Color	Collector	Actions
beats	None	filebeat on Linux	<a href="#">Edit</a> <a href="#">More actions</a>

Hình 3. 49 Chọn Create Configuration

Khai báo các thông số và sửa địa chỉ ip thành địa chỉ của graylog-server, sau đó bổ sung trường fields.source: \${sidecar.nodeName}

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

The screenshot shows the Graylog configuration interface. A new configuration named 'windowbeat' is being created. The configuration color is set to blue. The collector is 'winlogbeat on Windows'. The configuration code is as follows:

```
1 # Needed for Graylog
2 fields_under_root: true
3 fields.collector node_id: ${sidecar.nodeName}
4 fields.g12_source_collector: ${sidecar.nodeId}
5
6 output.logstash:
7   hosts: ["192.168.30.139:5044"]
8 path:
9   data: C:\Program Files\Graylog\sidecar\cache\winlogbeat\data
10  logs: C:\Program Files\Graylog\sidecar\logs
11 tags:
12   - windows
13   winlogbeat:
14     event_logs:
15       - name: Application
16       - name: System
17       - name: Security
```

Required. Collector configuration, see quick reference for more information.

Migrate Preview

Create Cancel

Hình 3. 50 Edit các thông tin trong sidecar client2 graylogserver

Tiếp theo, chọn tab Administration, tích chọn filebeat. Sau đó chọn configuration vừa tạo :

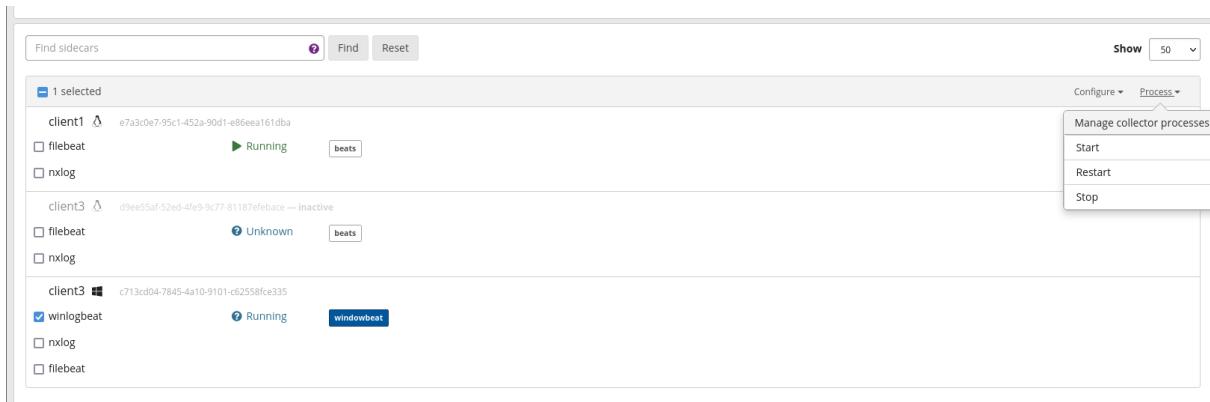
The screenshot shows the Graylog Collectors Administration interface. The 'winlogbeat' configuration is selected. The interface includes a search bar, a toolbar with 'Overview', 'Administration', and 'Configuration' buttons, and a sidebar with 'Configure' and 'Process' options.

Hình 3. 51 Chọn Filebeat , chọn configuration vừa tạo

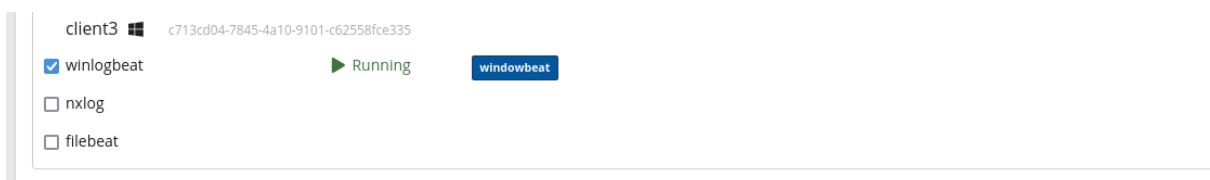
# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

Tiếp đến chọn Process -> Start để khởi động trình thu thập log từ client3, có một cửa sổ bật lên, chọn Confirm để tiếp tục:



Hình 3. 52 Khởi động trình thu thập dữ liệu client2 graylogserver



Hình 3. 53 Đã tạo thành công sidecar client2

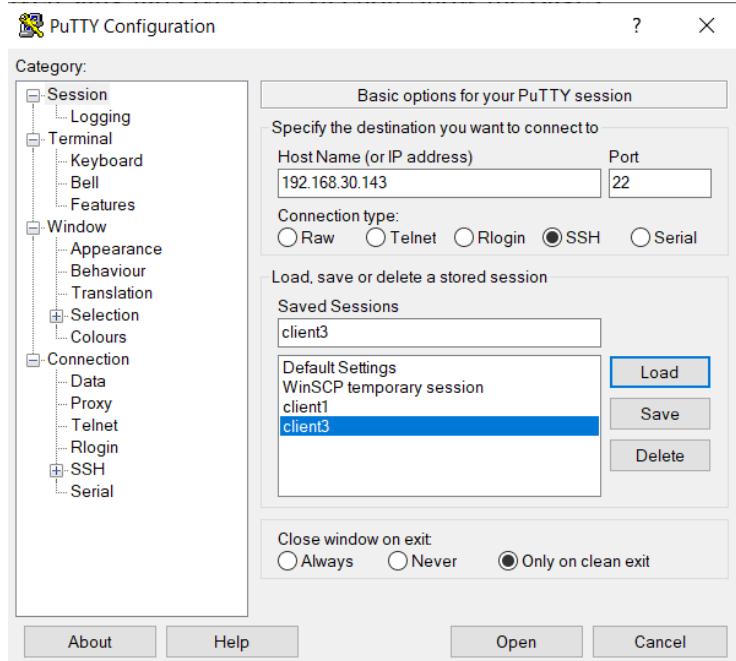
- Kiểm tra kết quả

Chuyển sang tab Overview và chọn Show messages:

Name	IP	Status	Operating System	Last Seen	Node Id	Sidebar Version	Manage sidebar	Show messages
client1		▶ Running	Linux	a few seconds ago	e7a3c0e7-95c1-452a-90d1-e86eea161dba	1.2.0	<a href="#">Manage sidebar</a>	<a href="#">Show messages</a>
client3		▶ Running	Windows	a few seconds ago	c713cd04-7845-4a10-9101-c62558fce335	1.2.0	<a href="#">Manage sidebar</a>	<a href="#">Show messages</a>

Hình 3. 54 Show messages sidecar client2

Sau đó SSH vào 1 tài khoản trên windows và kiểm tra log gửi về graylog-server:



Hình 3. 55 SSH vào client2

```

client3@client3: ~
login as: client3
client3@192.168.30.142's password:
Access denied
client3@192.168.30.142's password:
Access denied
client3@192.168.30.142's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-124-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 updates can be applied immediately.

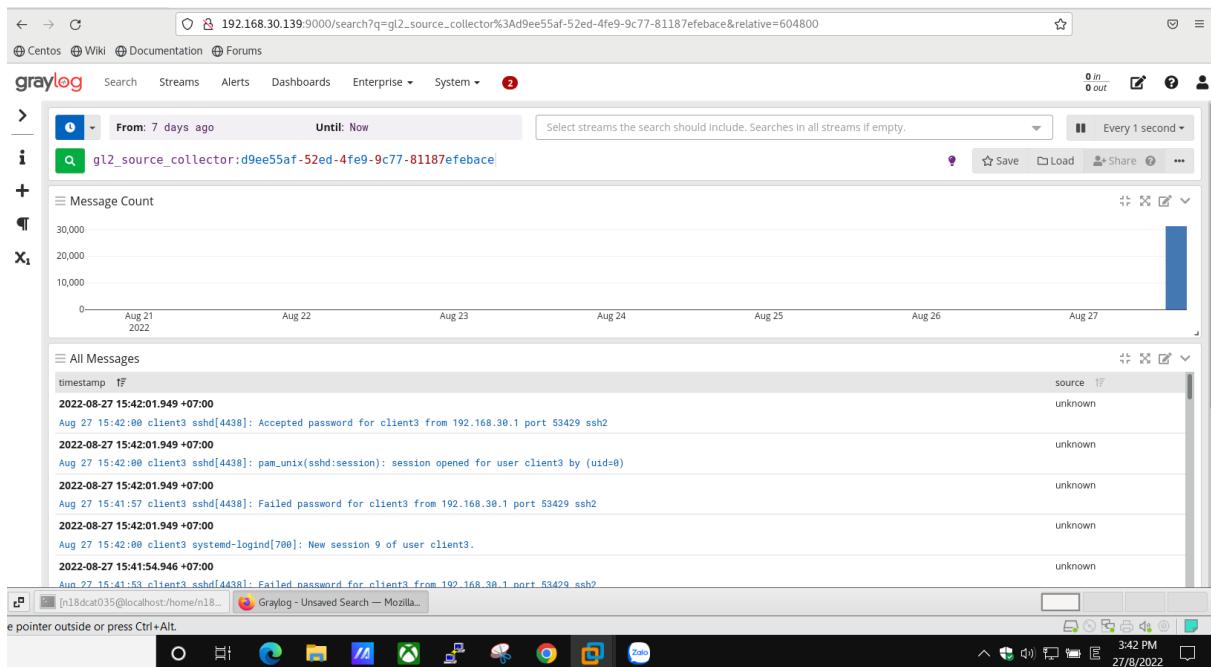
Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

client3@client3:~$
```

Hình 3. 56 SSH thành công vào client2



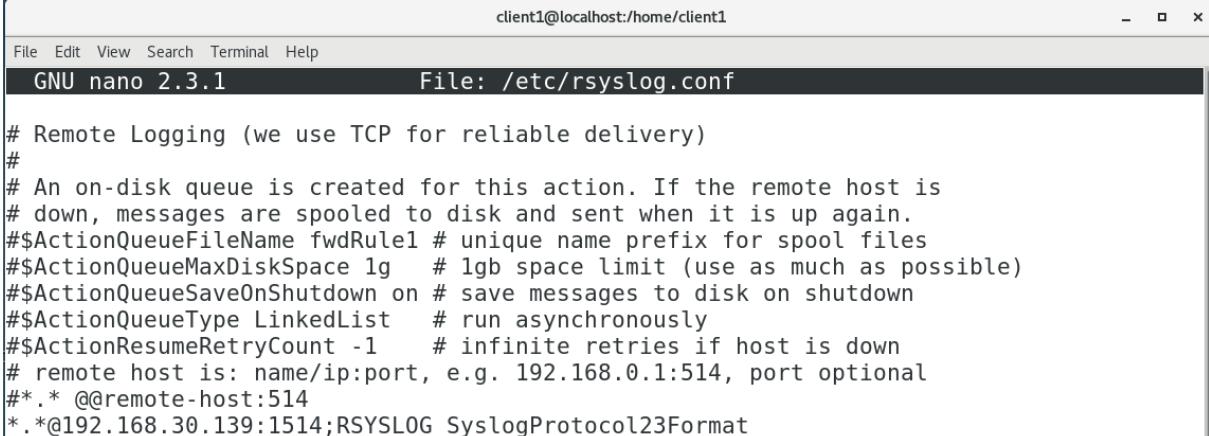
Hình 3. 57 ã nhận được log trên graylogserver khi có máy SSH vào client2

Có log đầy về như hình trên là đã cài thành công !!

### 3.5. CẤU HÌNH THU THẬP LOG CỦA CLIENT 1 CENTOS 7 THÔNG QUA SYSLOG

- Cấu hình rsyslog

Tiến hành cấu hình IP và port để gửi log về graylog server:



```
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList  # run asynchronously
#$ActionResumeRetryCount -1   # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.*/@remote-host:514
*.*/@192.168.30.139:1514;RSYSLOG_SyslogProtocol23Format
```

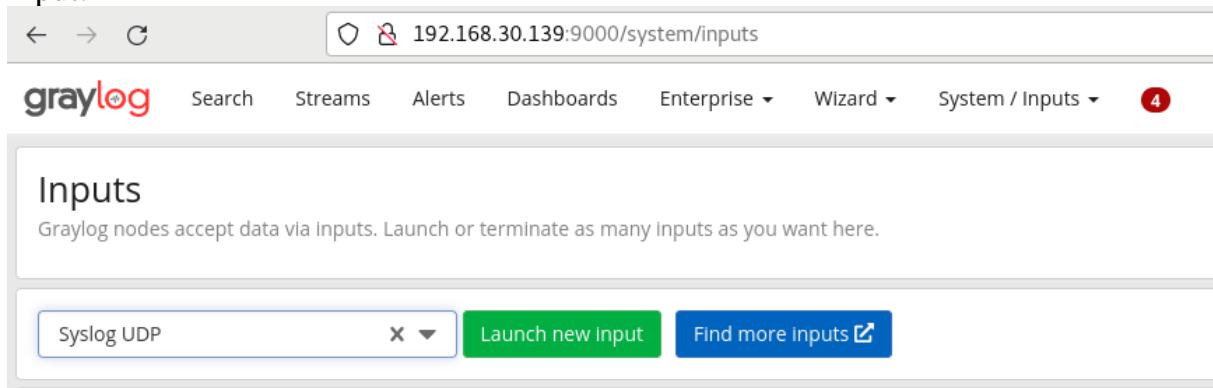
Hình 3. 58 Cấu hình file rsyslog

Khởi động lại dịch vụ rsyslog

`systemctl restart rsyslog`

- Cấu hình syslog trên Web Interface của graylog-server
  - Khai báo input cho syslog

Để graylog-server biết nơi cần nhận log, ta cần khai báo input cho graylog-server. Truy cập System/Inputs và chọn input là Syslog UDP và bấm Launch new input:



Hình 3. 59 Input Syslog UDP

Tiếp đến ta đặt tên cho input, cấu hình ip của interface nhận log và port. (port phải trùng với port khai báo ở client)

Editing Input aaaa X

Global  
Should this input start on all nodes

**Node**  
32f5ed63 / localhost ▼  
On which node should this input start

**Title**  
Syslog

**Bind address**  
0.0.0.0  
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

**Port**  
1514 ^ ▼  
Port to listen on.

**Receive Buffer Size (optional)**  
262144 ^ ▼  
The size in bytes of the recvBufferSize for network connections to this input.

**No. of worker threads (optional)**  
2 ^ ▼  
Number of worker threads processing network connections for this input.

Hình 3. 60 Cấu hình Input Syslog UDP

**Override source (optional)**

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

Force rDNS?

Force rDNS resolution of hostname? Use if hostname cannot be parsed. (Be careful if you are sending DNS logs into this input because it can cause a feedback loop.)

Allow overriding date?

Allow to override with current date if date could not be parsed?

Store full message?

Store the full original syslog message as full\_message?

Expand structured data?

Expand structured data elements by prefixing attributes with their SD-ID?

**Cancel**

**Save**

Hình 3. 61 Chọn Save để hoàn thành input syslog

Sau khi tạo, ta có được input của file syslog như sau:

Syslog Syslog UDP RUNNING  
On node ★ 32f5ed63 / localhost

```
allow_override_date: true
bind_address: 0.0.0.0
expand_structured_data: false
force_rdns: false
number_worker_threads: 2
override_source: <empty>
port: 1514
recv_buffer_size: 262144
store_full_message: true
```

Show received messages

Throughput  
1 minute ave  
Network IO:  
Empty messag

Hình 3. 62 Syslog đã hoàn thành

## BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

- Kiểm tra kết quả

Tại input của syslog, ta chọn Show received messages:

```
allow_override_date: true
bind_address: 0.0.0.0
expand_structured_data: false
force_rdns: false
number_worker_threads: 2
override_source: <empty>
port: 1514
recv_buffer_size: 262144
store_full_message: true
```

Throughput / Metrics  
1 minute average rate: 0 msg/s  
Network IO: ▾0B ▲0B (total ▾3.4KiB ▲0B)  
Empty messages discarded: 0

Hình 3. 63 Chọn Show received message tại syslog để xem log client1 bằng syslog

Sau đó ssh vào máy client1 và kiểm tra log gửi về graylog-server:

From: All Time Until: Now Select streams the search should include. Searches in all streams if empty.

gl2\_source\_input:630b8a7c9a5cf6d357702eb6

Message Count

All Messages

2022-09-02 18:30:57.364 +07:00 pam\_unix(sshd:session): session opened for user root by (uid=0)

2022-09-02 18:30:57.359 +07:00 New session 10 of user root.

2022-09-02 18:30:57.359 +07:00 Started Session 10 of user root.

2022-09-02 18:30:57.357 +07:00 Created slice User Slice of root.

2022-09-02 18:30:57.347 +07:00 Accepted password for root from 192.168.30.1 port 64290 ssh2

Hình 3. 64 Log được gửi bằng Syslog từ client1 đã được nhận thành công

Có log đầy đủ như hình trên là đã cài thành công !!

### 3.6. CẤU HÌNH GRAYLOG SERVER TÍCH HỢP CẢNH BÁO QUA EMAIL

- Remove Sendmail

Trước tiên cần kiểm tra xem sendmail đã được cài đặt chưa bằng câu lệnh  
rpm -qa | grep sendmail

Nếu có kết quả trả về chứng tỏ sendmail đã được cài đặt. Ta cần remove nó  
yum remove sendmail\*

- Install postfix

Cài đặt postfix và một số gói liên quan

```
yum -y install postfix cyrus-sasl-plain mailx
```

Đặt postfix như MTA mặc định của hệ thống

```
alternatives --set mta /usr/sbin/postfix
```

Nếu câu lệnh bị lỗi và trả về output /usr/sbin/postfix has not been configured as an alternative for mta thì thực hiện lệnh sau:

```
alternatives --set mta /usr/sbin/sendmail.postfix
```

Restart và enable postfix

```
systemctl restart postfix
systemctl enable postfix
```

Configure Postfix

Mở file main.cf để chỉnh sửa

```
nano /etc/postfix/main.cf
```

Thêm vào cuối file những dòng sau

```
myhostname = localhost.localdomain
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```

Hình 3. 65 Cấu hình postfix để gửi mail

Configure Postfix SASL Credentials

Tạo file /etc/postfix/sasl\_passwd và thêm vào dòng sau

[smtp.gmail.com]:587 username:password

```
[smtp.gmail.com]:587 n18dcat035@student.ptithcm.edu.vn:kietdeptrais01
```

Hình 3. 66 Thêm gmail sender cho postfix

Phân quyền cho file vừa tạo

```
postmap /etc/postfix/sasl_passwd
chown root:postfix /etc/postfix/sasl_passwd*
chmod 640 /etc/postfix/sasl_passwd*
systemctl reload postfix
```

- Cho phép ứng dụng truy cập gmail

Nếu bạn sử dụng gmail làm địa chỉ người gửi thì bạn phải cho phép ứng dụng truy cập gmail của bạn

Đăng nhập bằng gmail để thực hiện gửi mail đã khai báo bên trên trình duyệt và truy cập vào địa chỉ sau

<https://myaccount.google.com/lesssecureapps>

Bật chế độ cho phép ứng dụng truy cập

← Quyền truy cập của ứng dụng kém an toàn

Một số ứng dụng và thiết bị sử dụng công nghệ đăng nhập kém an toàn, khiến tài khoản của bạn dễ bị tấn công. Chúng tôi khuyên bạn tắt quyền truy cập của các ứng dụng đó. Bạn vẫn có thể cấp quyền truy cập để dùng các ứng dụng đó, nhưng rủi ro có thể xảy ra. Google sẽ tự động TẮT tùy chọn cài đặt này nếu bạn không sử dụng. [Tim hiểu thêm](#)

Cho phép ứng dụng kém an toàn: BẬT



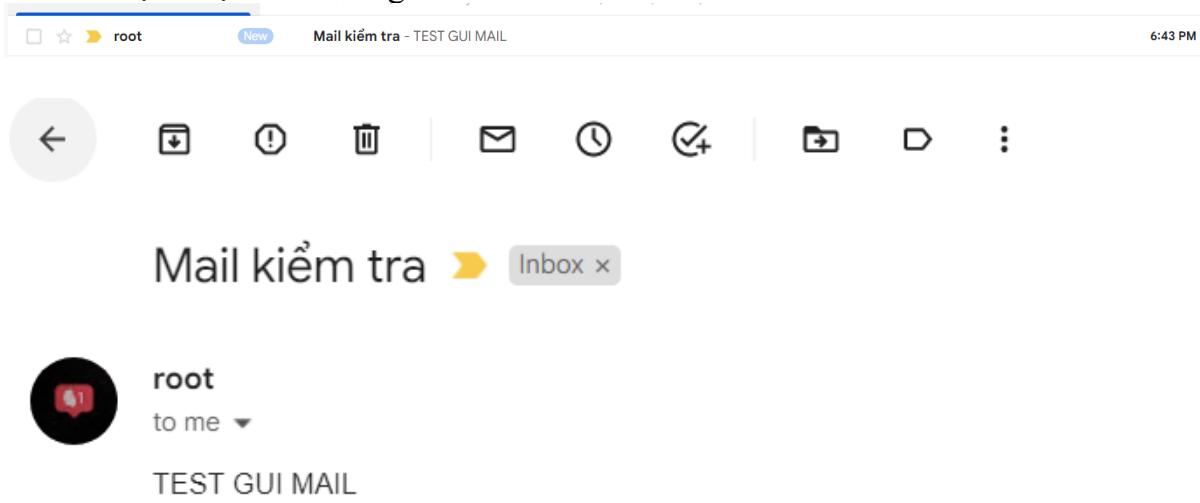
Hình 3. 67 Cho phép truy cập ứng dụng trong mail

Kiểm tra lại xem đã gửi mail thành công hay chưa

```
[root@localhost n18dcat035]# echo "TEST GUI MAIL" | mail -s "Mail kiểm tra" tuankiethkt020@gmail.com
```

Hình 3. 68 Test gửi mail

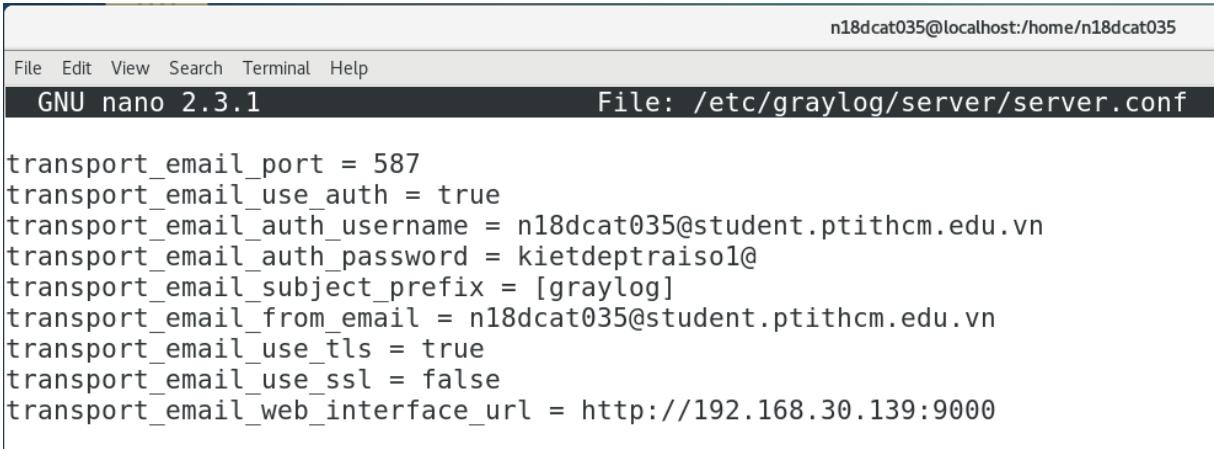
Tôi đã nhận được mail vừa gửi



Hình 3. 69 Gửi mail thành công

- Cấu hình cảnh báo Email

Sau khi cài đặt postfix thành công, thêm phần cấu hình sau vào cuối file /etc/graylog/server/server.conf:



```

transport_email_port = 587
transport_email_use_auth = true
transport_email_auth_username = n18dcat035@student.ptithcm.edu.vn
transport_email_auth_password = kietdeptrais01@
transport_email_subject_prefix = [graylog]
transport_email_from_email = n18dcat035@student.ptithcm.edu.vn
transport_email_use_tls = true
transport_email_use_ssl = false
transport_email_web_interface_url = http://192.168.30.139:9000

```

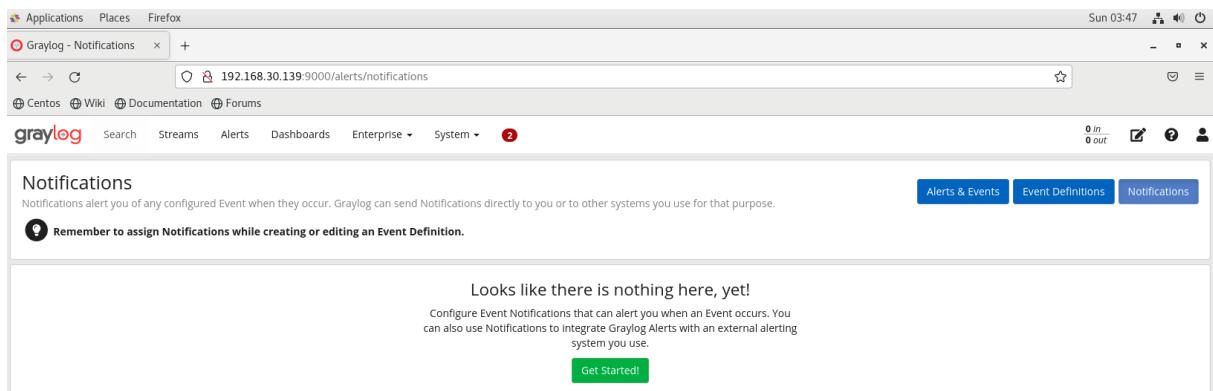
Hình 3. 70 Cấu hình gửi mail trong server.conf

Lưu lại thay đổi và khởi động lại dịch vụ graylog-server:

```
systemctl restart graylog-server
```

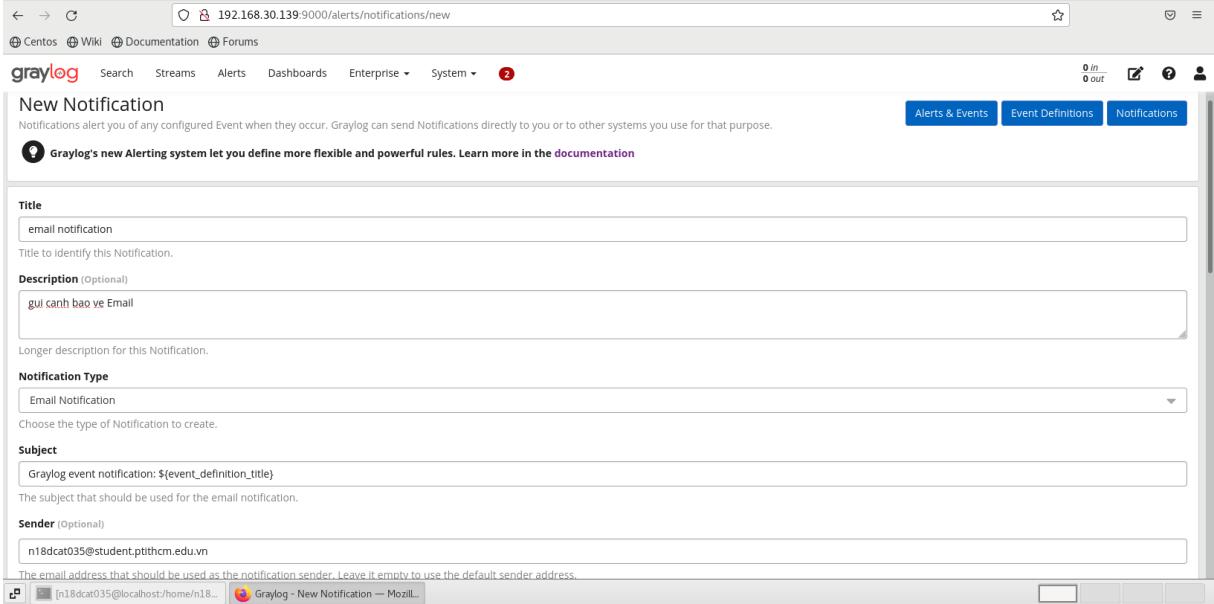
- Cấu hình Cảnh báo Email

Trên Web Interface của graylog-server vào Alerts -> Notification -> Get Started



Hình 3. 71 Tạo notification gửi mail

Điền thông tin vào các trường như bên dưới:



New Notification

Notifications alert you of any configured Event when they occur. Graylog can send Notifications directly to you or to other systems you use for that purpose.

**Title**  
email notification

**Description (Optional)**  
gui canh bao ve Email

**Notification Type**  
Email Notification

**Subject**  
Graylog event notification: \${event\_definition\_title}

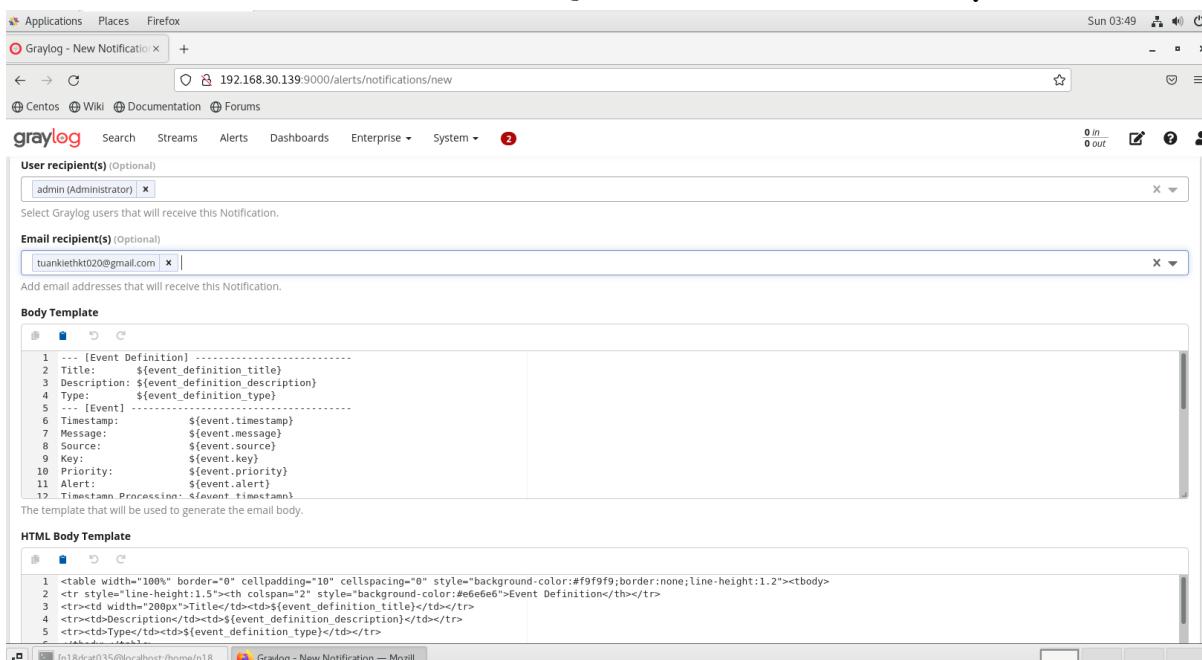
**Sender (Optional)**  
n18dcat035@student.ptithcm.edu.vn

The email address that should be used as the notification sender. Leave it empty to use the default sender address.

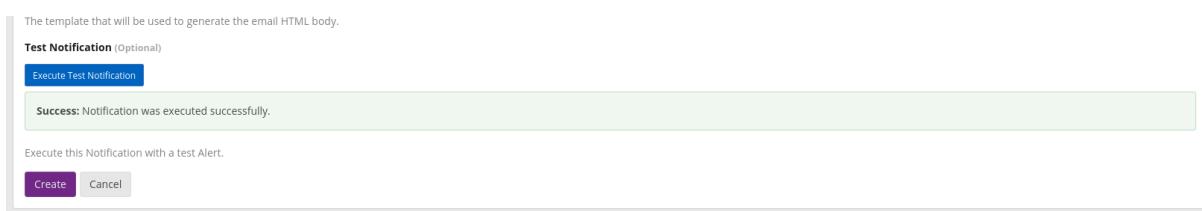
Hình 3. 72 Điền thông tin cần thiết để tạo email notification I

# BÁO CÁO TTTN ĐẠI HỌC

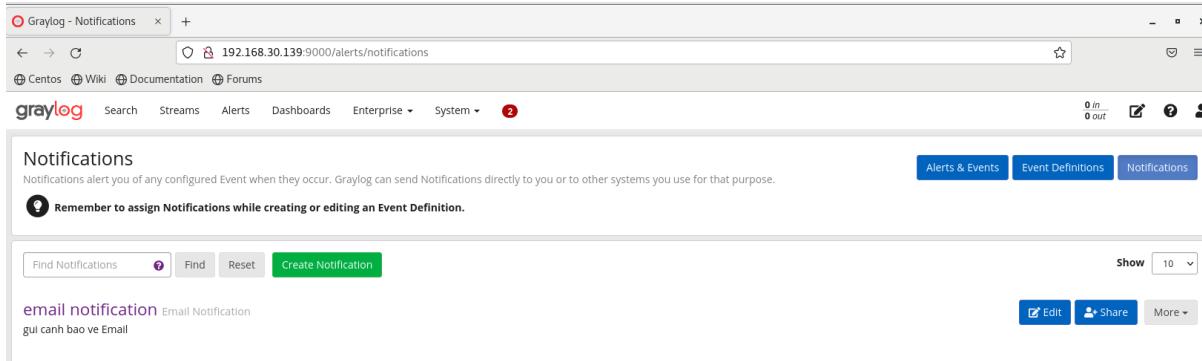
## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG



Hình 3. 73 Diễn thông tin cần thiết để tạo email notification 2



Hình 3. 74 Test Notification

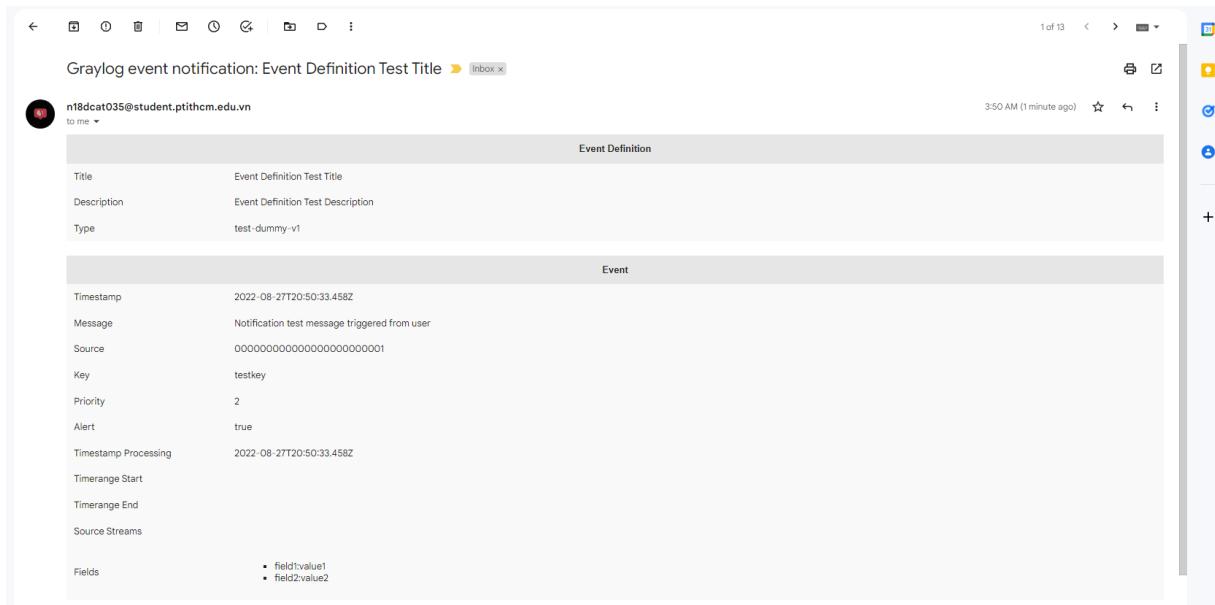


Hình 3. 75 Tạo thành công Notification qua gmail

Đặt tiêu đề cho cảnh báo  
Mô tả ngắn về cảnh báo này  
Chọn Notification Type là Email Notification  
Nhập vào email của người gửi, tức là email đã được định cấu hình trong file config của graylog-server  
Chọn user là admin  
Nhập vào email của người nhận, khi có đăng nhập thành công thì cảnh báo sẽ được gửi về email này.  
Kích vào Exxcute Test Notification để gửi thử 1 mail test, nếu trạng thái trả về Success tức là cấu hình đã thành công.  
Chọn Create để tạo cảnh báo email  
Truy cập email kiểm tra ta thấy có 1 email test được gửi đến:

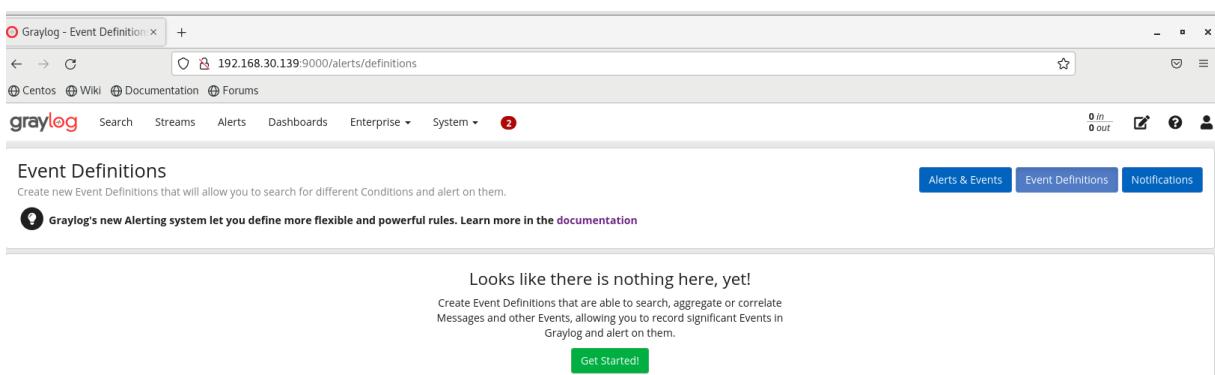
# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG



Hình 3. 76 Gmail test đã gửi thành công

- Cấu hình event cảnh báo  
Chuyển sang tab Event Definitions và chọn Get Started! để cấu hình event cảnh báo.



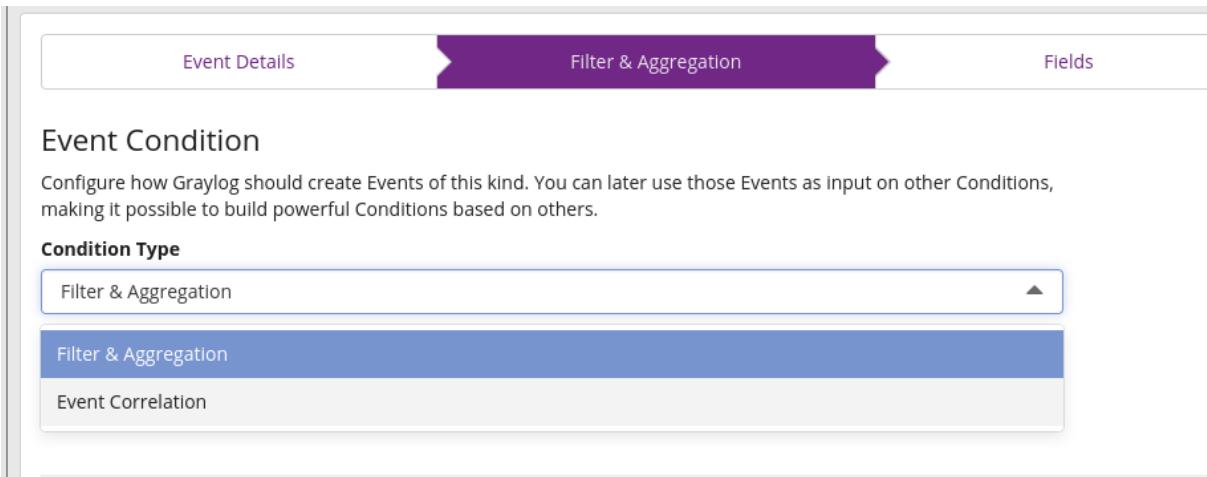
Hình 3. 77 Tạo Event để cảnh báo

Nhập vào tiêu đề và mô tả ngắn cho sự kiện:

The screenshot shows the 'New Event Definition' form. The title is 'SSH check'. The description is 'SSH check'. The priority is set to 'Normal'. At the bottom right, there are 'Previous' and 'Next' buttons.

Hình 3. 78 Nhập tên mô tả cần cảnh báo

Chọn Condition Type là Filter & Aggregation:



Hình 3. 79 Chọn Filter &amp; Aggregation

Tiếp theo nhập vào các thông tin như sau:

Hình 3. 80 Nhập các thông tin cần thiết để cảnh báo

Ở mục Search Query, vì mình muốn tạo cảnh báo khi có ssh thành công vào hệ thống nên ta nhập vào là ACTION: Accepted.

Tại Streams, ta chọn là All messages

Chọn Next để tiếp tục

Lưu ý: Search within the last và Execute search every là tìm trong vòng 1 phút cuối cùng và thời gian cách mỗi lần tìm kiếm là 1 phút.

Tiếp đến là Event Fields, là 1 trường bổ sung thông tin về cảnh báo và thêm ngữ cảnh khi cảnh báo nhưng là 1 trường không bắt buộc nên ta có thể bỏ qua:

Hình 3. 81 Event Fields

Mục tiếp theo là mục Notification , click chọn Add Notification và chọn cảnh báo về Email đã tạo trước đó:

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

Event Details      Filter & Aggregation      Fields      Notifications      Summary

Notifications (optional) [Manage Notifications](#)

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

This Event is not configured to trigger any Notifications yet.

Add Notification      Previous      Next

Hình 3. 82 Chọn Notification

Ta chọn notification là Email Alert:

Event Details      Filter & Aggregation      Fields      Notifications      Summary

Add Notification

Choose Notification

email notification

Select a Notification to use on Alerts of this kind or create a new Notification that you can later use in other Alerts.

Done      Cancel      Previous      Next

Hình 3. 83 Chọn Email Notification

Sau đó chọn next để xác nhận:

Event Details      Filter & Aggregation      Fields      Notifications      Summary

Notifications (optional) [Manage Notifications](#)

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

Notification	Type	Actions
email notification	Email Notification	<a href="#">Remove from Event</a>

Add Notification      Previous      Next

Notification Settings

Grace Period

Message Backlog

Number of messages to be included in Notifications.

Hình 3. 84 Các Notification đã được chọn

Tại bước này cung cấp 1 bản tóm tắt về định nghĩa cảnh báo vừa tạo.  
Chọn Done để hoàn tất cài đặt Alert:

graylog      Search      Streams      Alerts      Dashboards      Enterprise      System      2

Event Details      Filter & Aggregation      Fields      Notifications      Summary

Event Summary

Details

Title: SSH check  
Description: SSH check  
Priority: Normal

Filter & Aggregation

Type: Filter  
Search Query: ACTION: Accepted  
Streams: All messages  
Search within: 1 minutes  
Execute search every: 1 minutes  
Enable scheduling: no

Fields

No Fields configured for Events based on this Definition.

Notifications

Settings: Grace Period is disabled  
Notifications will include 50 messages

email notification  
Email Notification  
[More details](#)

Cancel      Done

Hình 3. 85 Chọn Done để hoàn thành Alert Event

- Kiểm tra cấu hình cảnh báo
- Tiến hành ssh vào các máy client để kiểm tra xem có cảnh báo gửi về hay không.
- Sau đó ta kiểm tra trên slack đã thấy có cảnh báo ssh alert gửi về từ các client:

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

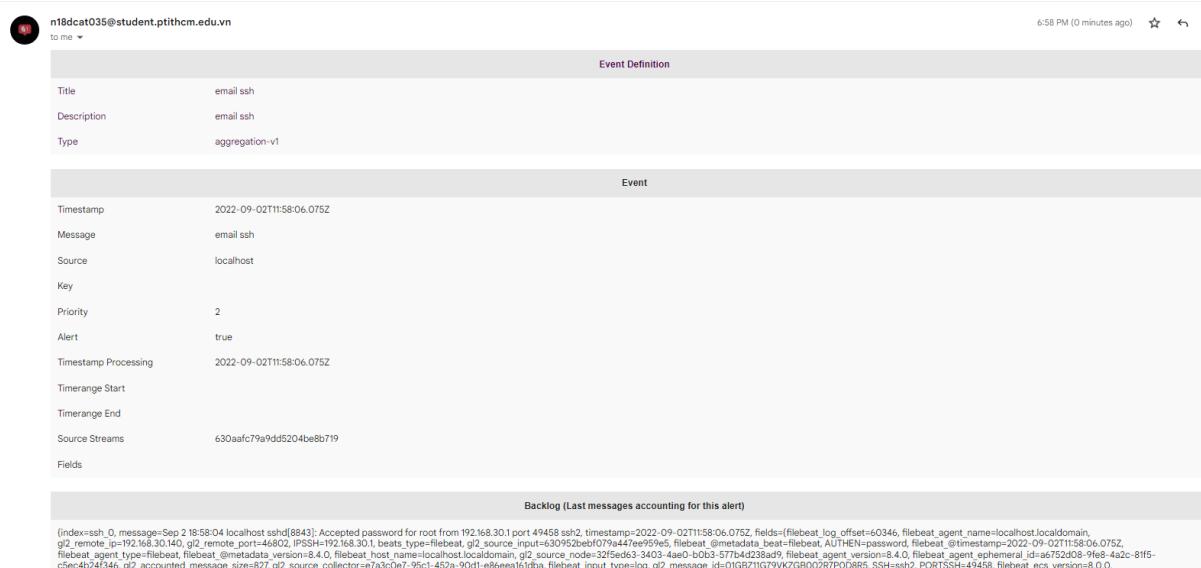
```
All Messages

2022-08-28 04:56:37.047 +07:00
Aug 28 04:56:38 localhost sshd[5273]: pam_unix(sshd:session): session closed for user root
2022-08-28 04:47:04.945 +07:00
Aug 28 04:47:04 localhost sshd[5273]: Accepted password for root from 192.168.30.1 port 55881 ssh2
2022-08-28 04:47:04.945 +07:00
Aug 28 04:47:04 localhost sshd[5273]: pam_unix(sshd:session): session opened for user root by (uid=0)
2022-08-28 04:47:01.943 +07:00
Aug 28 04:46:55 localhost sshd[5273]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.30.1 user=root
2022-08-28 04:47:01.943 +07:00
Aug 28 04:46:58 localhost sshd[5273]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
2022-08-28 04:47:01.943 +07:00
```

Hình 3. 86 Các log về SSH



Hình 3. 87 Gmail đã nhận được cảnh báo về đăng nhập thành công SSH



Hình 3. 88 Chi tiết Gmail cảnh báo

### 3.7. CẤU HÌNH GRAYLOG SERVER TÍCH HỢP CẢNH BÁO QUA SLACK

- Cấu hình cảnh báo Slack

Di chuyển đến thư mục plugin của Graylog-server:

```
cd /usr/share/graylog-server/plugin/
```

Tải về plugin của slack:

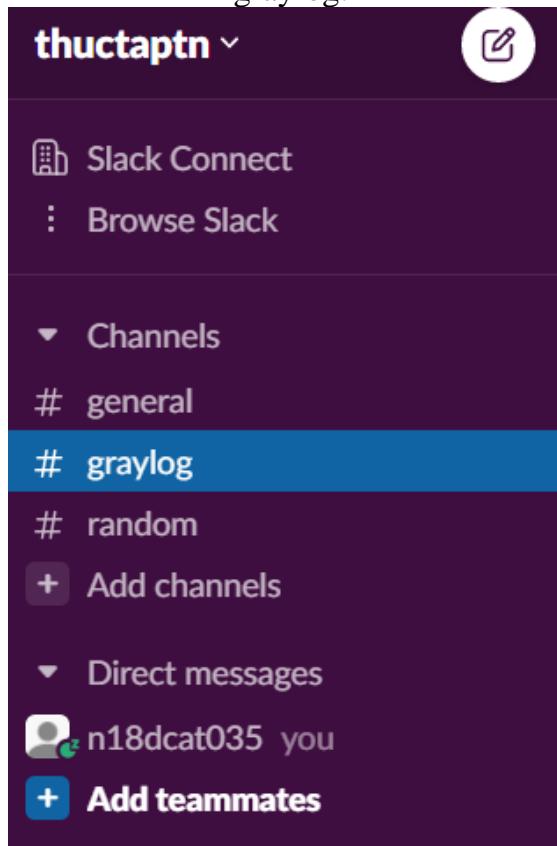
```
wget https://github.com/graylog-labs/graylog-plugin-slack/releases/download/3.1.0/graylog-plugin-slack-3.1.0.jar
```

Khởi động lại dịch vụ graylog-server :

```
systemctl restart graylog-server
```

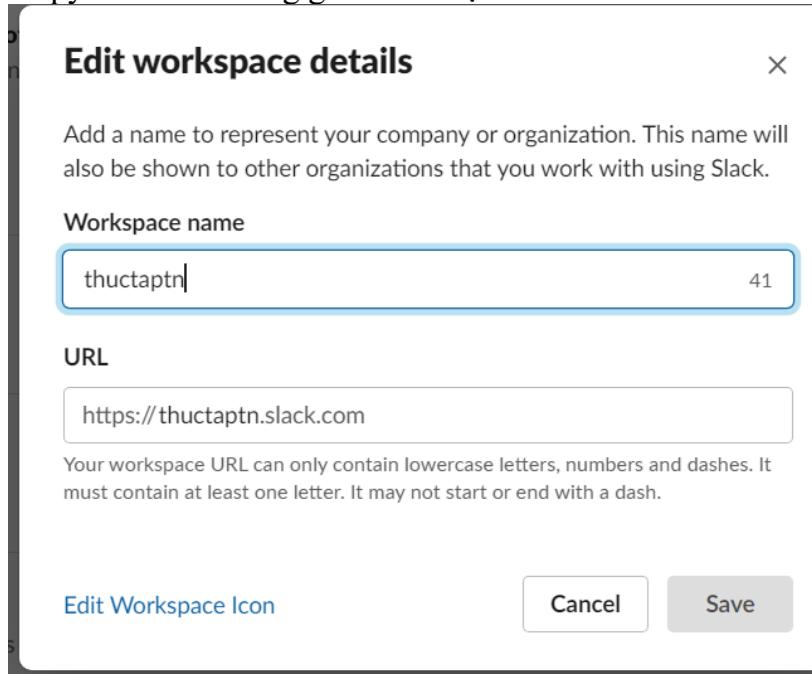
```
systemctl status graylog-server
```

Trên kênh slack tạo 1 channel có tên là graylog:



Hình 3. 89 Tạo Channels graylog trong Slack

Sau đó copy link của không gian làm việc:



Hình 3. 90 Copy URL workspace Slack

Truy cập địa chỉ sau với <organization> là link vừa copy:

```
https://<organization>/apps/new/A0F7XDUAZ-webhooks-  
entrants  
https://thuctaptn.slack.com/apps/new/A0F7XDUAZ-webhooks-  
entrants
```

Chọn channel là graylog vừa tạo và tích hợp thêm Webhooks đến:

The screenshot shows the Slack App Directory interface. At the top, there is a search bar labeled "Search App Directory" and a "Browse" button. Below the search bar, the breadcrumb navigation shows: "Browse apps > Custom Integrations > Incoming WebHooks > New configuration". The main content area is titled "Incoming WebHooks" with a sub-description "Send data into Slack in real-time." A note in a box states: "Please note, this is a legacy custom integration - an outdated way for teams to integrate with Slack. These integrations lack newer features and they will be deprecated and possibly removed in the future. We do not recommend their use. Instead, we suggest that you check out their replacement: Slack apps." Below this note, text explains that Incoming Webhooks are a simple way to post messages from external sources into Slack using normal HTTP requests with a JSON payload. It also mentions that Message Attachments can be used. A callout box with a warning icon advises users to check the "Getting Started" guide for common integration types and tips. The "Post to Channel" section allows selecting a channel, with "#graylog" selected. A large green button at the bottom right says "Add Incoming WebHooks integration".

Hình 3. 91 Add Incoming WebHooks

Sau đó ta sẽ có được URL Webhooks, copy và note lại để sau sử dụng cho việc gửi cảnh báo về channel:

The screenshot shows the "Setup Instructions" page for an Incoming Webhook. The title is "Setup Instructions" and it says: "We'll guide you through the steps necessary to configure an Incoming Webhook so you can start sending data to Slack." A "close" button is in the top right corner. Below this, a "Webhook URL" field contains the copied URL: <https://hooks.slack.com/services/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>.

Hình 3. 92 Tạo Webhooks thành công cho channel graylog

Tiếp đến, trên Web Interface của graylog-server vào Alerts -> Notification -> Create Notification

Sau đó điền các thông tin như sau:

New Notification

Notifications alert you of any configured Event when they occur. Graylog can send Notifications directly to you or to other systems

**Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation**

**Title**  
Slack Notifacation

Title to identify this Notification.

**Description (Optional)**  
THONG BAO QUA SLACK

Longer description for this Notification.

**Notification Type**  
Slack Notification

Choose the type of Notification to create.

**Configuration color**  
Change color

Choose a color to use for this configuration.

**Webhook URL**  
https://hooks.slack.com/services/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

Slack "Incoming Webhook" URL

**Channel**  
#graylog

Name of Slack #channel or @user for a direct message

Hình 3. 93 Tạo Notification Slack

The screenshot shows the Graylog web interface for creating a new Slack notification. The URL in the browser bar is 192.168.30.139:9000/alerts/notifications/new. The interface includes sections for:

- Custom Message (optional)**: Fields for Title and Type, with a note about appending custom messages below the alert title.
- Message Backlog Limit (optional)**: A field set to 0, with a note about limiting backlog messages.
- User Name (optional)**: Set to "Graylog".
- Icon URL (optional)**: An empty input field for the icon URL.
- Icon Emoji (optional)**: An empty input field for the icon emoji.
- Test Notification (Optional)**: A button to "Execute Test Notification" which results in a green success message: "Success: Notification was executed successfully."
- Action Buttons**: "Create" and "Cancel" buttons at the bottom.

Hình 3. 94 Test cảnh báo qua Slack và Save Notification

- Để dễ nhận biết, ta nhập vào tiêu đề cho cảnh báo.
- Mô tả ngắn cho cảnh báo này
- Chọn Notification Type là Slack Notification
- Nhập vào Webhook URL đã copy trước đó
- Nhập vào tên channel đã tạo để nhận cảnh báo trên slack trước đó.
- Tích chọn Link Names
- Kích vào Execute Test Notification để gửi thử 1 cảnh báo. Khi trạng thái trả về là Success tức là cấu hình đã đúng.
- Chọn Create để tạo cảnh báo về slack.

Truy cập vào channel graylog trên slack để kiểm tra message test:

The screenshot shows the Slack interface with the '#graylog' channel selected. The sidebar on the left shows the user 'thuctaptn' has selected the '#graylog' channel. The channel feed displays several messages from 'n18dcat035' and the Graylog app, indicating successful integration and alert triggers.

Hình 3. 95 Đã nhận được thông báo test trên Slack

Ta thấy đã có message!

The screenshot shows the Graylog UI under the 'Notifications' tab. It displays two notifications: 'CANH BAO ICMP FLOOD' (Email Notification) and 'Slack Notification' (Slack Notification). Both notifications have been completed, as indicated by the 'Edit', 'Share', and 'More' buttons.

Hình 3. 96 Notification Slack đã hoàn thành

- Cấu hình event cảnh báo
- Chọn Edit để chỉnh sửa Event:

The screenshot shows the Graylog UI under the 'Event Definitions' tab. It displays two event definitions: 'CANH BAP FLOOD ICMP' (Filter & Aggregation) and 'email ssh' (Filter & Aggregation). The 'CANH BAP FLOOD ICMP' event runs every 1 minute and triggers 1 notification.

Hình 3. 97 Cấu hình Event qua Slack

Chuyển tới tab Notifications để thêm cảnh báo cho Email và chọn Add Notification để thêm cấu hình cảnh báo:

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG QUẢN LÝ VÀ PHÂN TÍCH NHẬT KÝ GRAYLOG

**Hình 3. 98 Chọn Add notification trong event SSH đã tạo lúc trước**

Sau đó chọn Notification là Email Notification và chọn Done để add:

**Hình 3. 99 Chọn Slack Notification**

Chọn Next để tiếp tục:

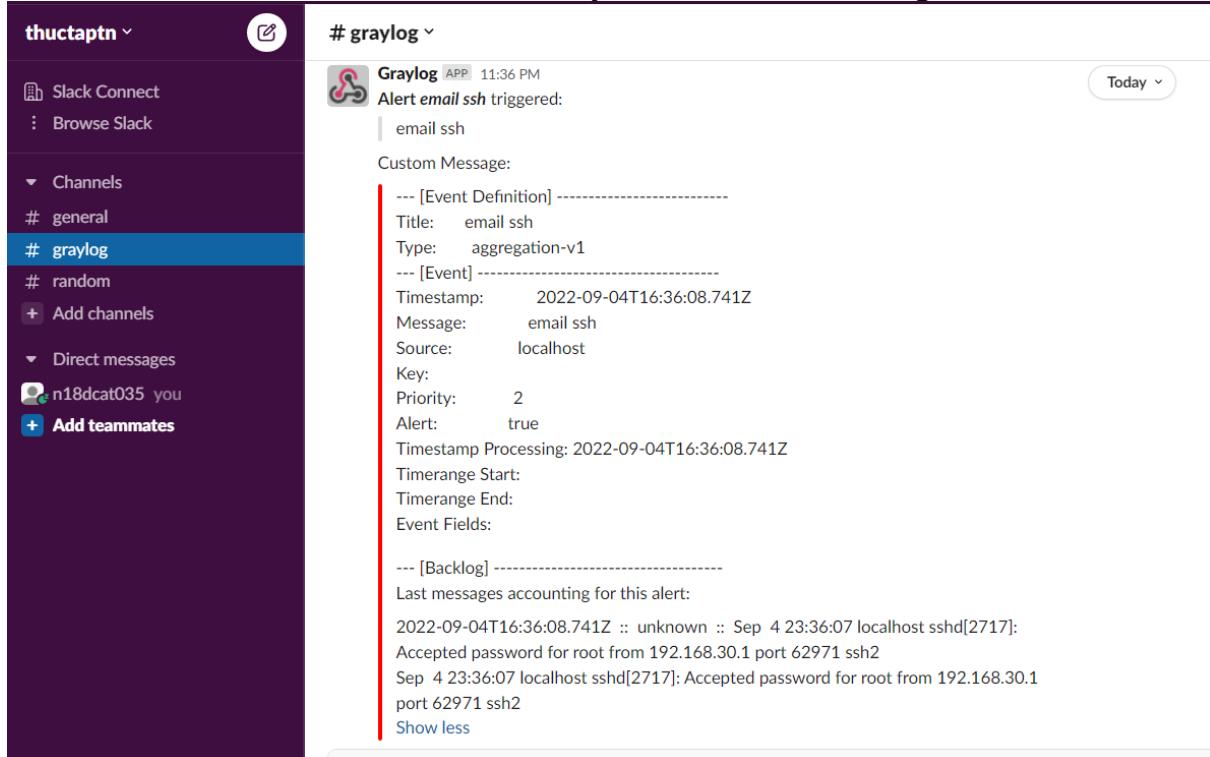
**Hình 3. 100 Chọn next để tiếp tục**

Chọn Done để hoàn tất cài đặt alert:

**Hình 3. 101 Chọn Done để hoàn thành event cảnh báo qua Slack**

- Kiểm tra cấu hình cảnh báo  
Tiến hành ssh vào các máy client để kiểm tra xem có cảnh báo gửi về hay không.

Sau đó ta kiểm tra trên slack đã thấy có cảnh báo ssh alert gửi về từ các client:

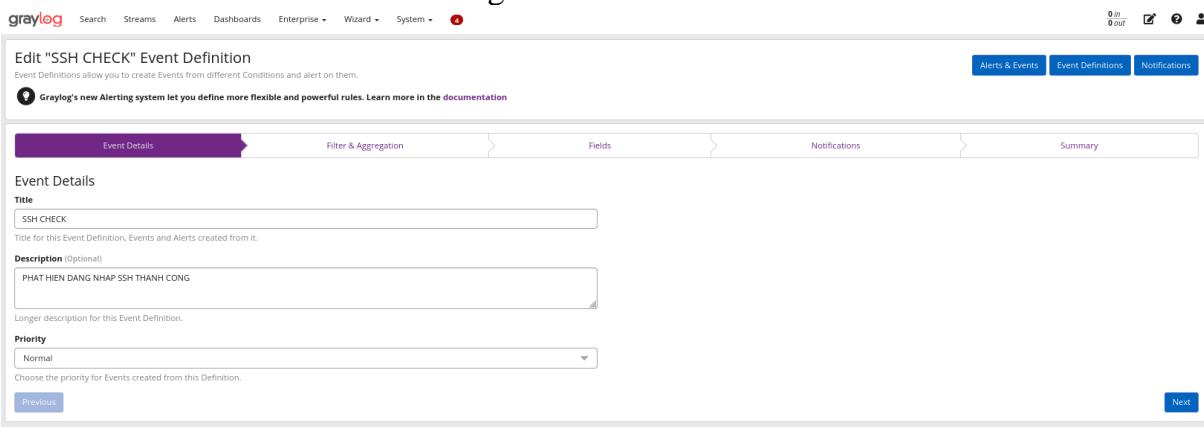


Hình 3. 102 Đã nhận được cảnh báo đăng nhập thành công ssh trên Slack

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO

### 4.1. CẢNH BÁO LOGIN SSH

Cấu hình event cảnh báo Login SSH như sau:

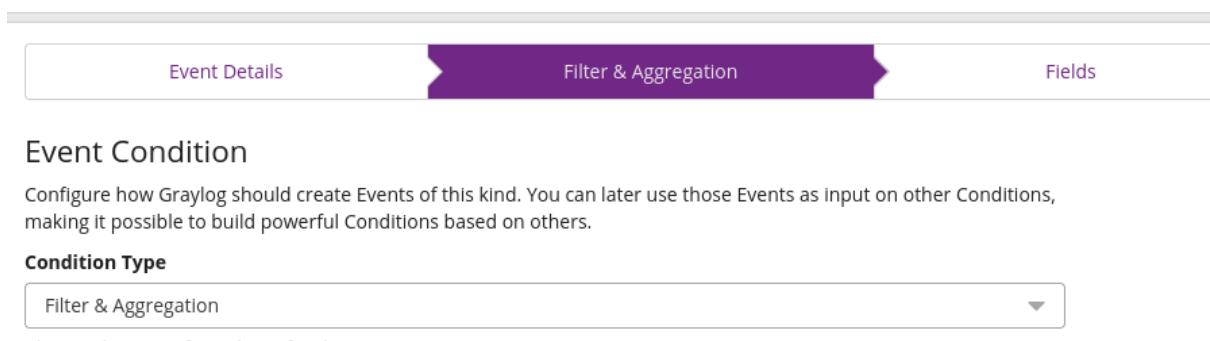


Hình 4. 1 Tạo event cảnh báo SSH

### Edit "SSH CHECK" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation



Hình 4. 2 Chọn Filter & Aggregation

## Filter

Add information to filter the log messages that are relevant for this Event Definition.

## Search Query

message:"Accepted"

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

## Streams (Optional)

sidecar X

Select streams the search should include. Searches in all streams if empty.

## Search within the last

1

minutes ▾

## Execute search every

1

minutes ▾

Enable

Should this event definition be executed automatically?

## Create Events for Definition if...

- Filter has results
- Aggregation of results reaches a threshold

Previous

Hình 4. 3 Diền các thông tin cần thiết của cảnh báo SSH

## Edit "SSH CHECK" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Alerts & Events Event Definitions Notifications

💡 Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Event Details Filter & Aggregation Fields Notifications Summary

## Event Fields (optional)

Include additional information in Events generated from this Event Definition by adding custom Fields. That can help you search Events or having more context when receiving Notifications.

This Event does not have any custom Fields yet.

Add Custom Field Previous

Next

Hình 4. 4 Next để qua bước event fields

## Edit "SSH CHECK" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Alerts & Events Event Definitions Notifications

💡 Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Event Details Filter & Aggregation Fields Notifications Summary

## Notifications (optional)

Manage Notifications

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

Notification	Type	Actions
email notification	Email Notification	<span style="border: 1px solid #ccc; padding: 2px;">Remove from Event</span>
Slack Notification	Slack Notification	<span style="border: 1px solid #ccc; padding: 2px;">Remove from Event</span>

Add Notification

## Notification Settings

## Grace Period

seconds ▾

Graylog sends Notifications for Alerts every time they occur. Set a Grace Period to control how long Graylog should wait before sending Notifications again. Note that Events with keys will have a Grace Period for each different key value.

## Message Backlog

Number of messages to be included in Notifications.

Previous

Next

Hình 4. 5 Chọn Notifications qua Gmail và Slack

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO

The screenshot shows the Graylog web interface with the following details:

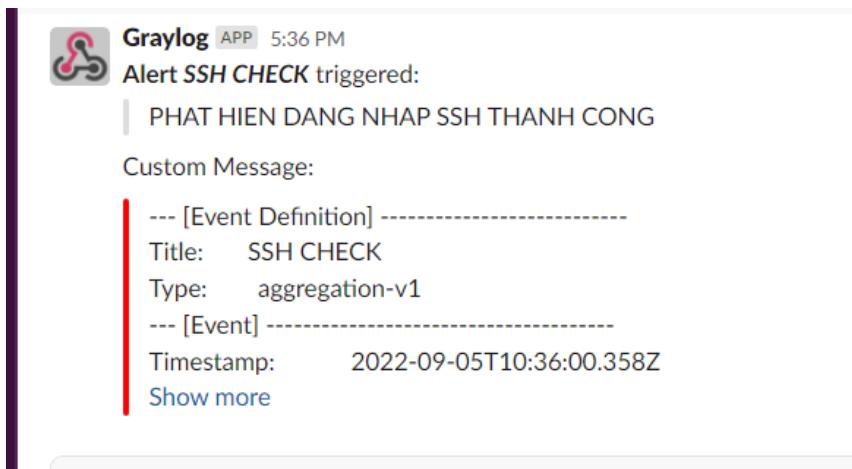
- Event Details:** Title: SSH CHECK, Description: PHAT HIEN DANG NHAP SSH THANH CONG, Priority: Normal.
- Filter & Aggregation:** Type: Filter, Search Query: message:"Accepted", Streams: sidecar, Search within: 1 minutes, Execute search every: 1 minutes, Enable scheduling: yes.
- Notifications:** Settings: Grace Period is disabled, Notifications will include 50 messages.
  - Slack Notification: Slack Notification, More details
  - Email notification: Email Notification, More details

Hình 4. 6 Hoàn thành cảnh báo SSH qua Gmail và Slack

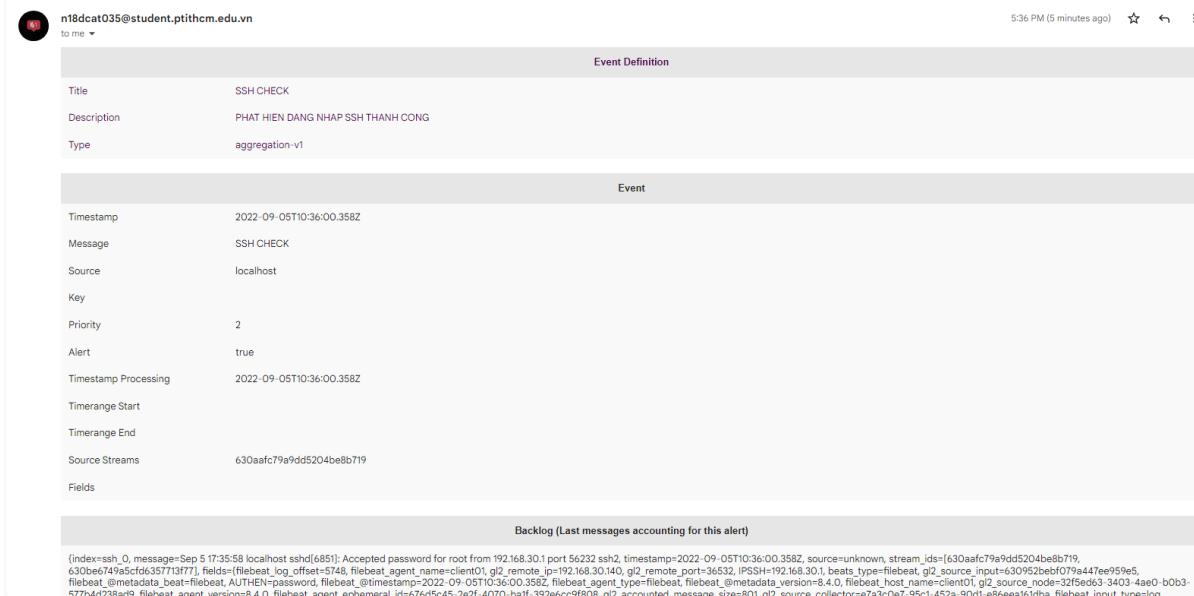
### SSH vào Client1

```
root@client01:~  
login as: root  
root@192.168.30.140's password:  
Last login: Mon Sep  5 16:21:28 2022 from 192.168.30.1  
[root@client01 ~]# whoami  
root  
[root@client01 ~]#
```

Hình 4. 7 SSH thành công vào client1



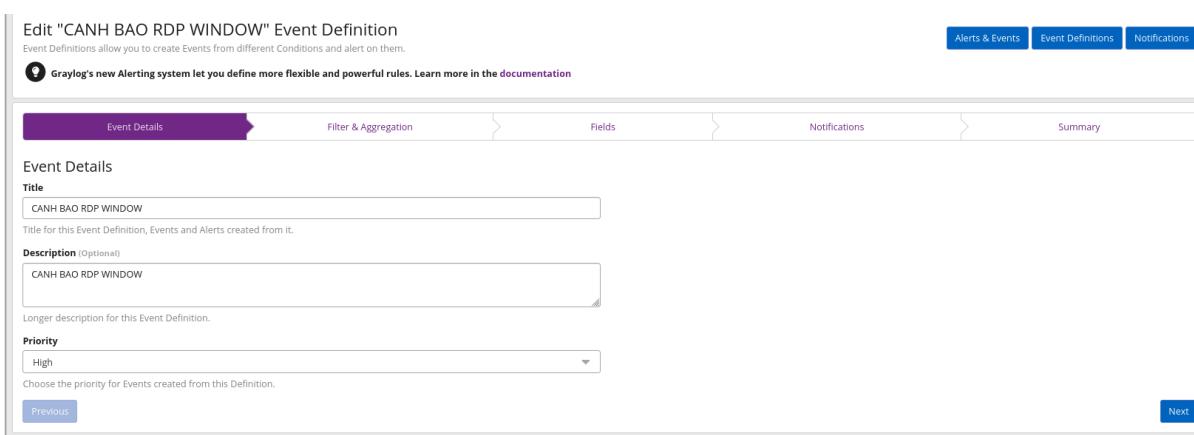
Hình 4. 8 Slack đã cảnh báo SSH thành công trên client 1



Hình 4. 9 Gmail đã cảnh báo SSH thành công trên client

## 4.2. CẢNH BÁO LOGIN RDP

Câu hình event cảnh báo Login RDP như sau:



Hình 4. 10 Tạo event cảnh báo Login RDP

### Event Condition

Configure how Graylog should create Events of this kind. You can later use those Events as input on other Conditions, making it possible to build powerful Conditions based on others.

#### Condition Type

Filter & Aggregation

Choose the type of Condition for this Event.

Hình 4. 11 Chọn Filter &amp; Aggregation

## Filter

Add information to filter the log messages that are relevant for this Event Definition.

## Search Query

```
winlogbeat_winlog_event_id:"4624" AND message:"An account was successfully logged on"
```

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

## Streams (Optional)

 X
X ▼

Select streams the search should include. Searches in all streams if empty.

## Search within the last

↑
minutes ▾

## Execute search every

↑
minutes ▾
 Enable

Should this event definition be executed automatically?

## Create Events for Definition if...

 Filter has results

 Aggregation of results reaches a threshold

Previous

Hình 4. 12 Điện thông tin cần thiết của cảnh báo Login RDP

Hình 4. 13 Event Fields

Hình 4. 14 Chọn Notification qua Gmail và Slack

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO

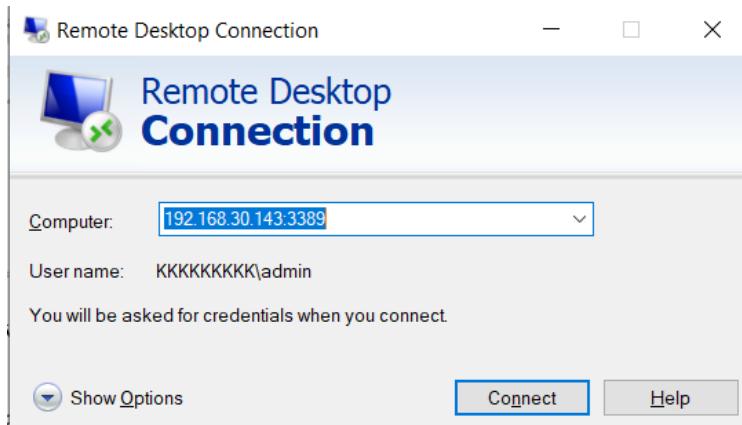
The screenshot shows the Logstash configuration interface with the following sections:

- Event Details:** Title: CANH BAO RDP WINDOW, Description: CANH BAO RDP WINDOW, Priority: High.
- Filter & Aggregation:** Type: Filter, Search Query: winlogbeat\_winlog\_event\_id:"4624" AND message:"An account was successfully logged on", Streams: EVENT\_RDP\_WINDOW, Search within: 1 minutes, Execute search every: 1 minutes, Enable scheduling: yes.
- Fields:** No Fields configured for Events based on this Definition.
- Notifications:** Settings: Grace Period is disabled, Notifications will include 50 messages.
  - Email notification: Email Notification, More details
  - Slack Notification: Slack Notification, More details

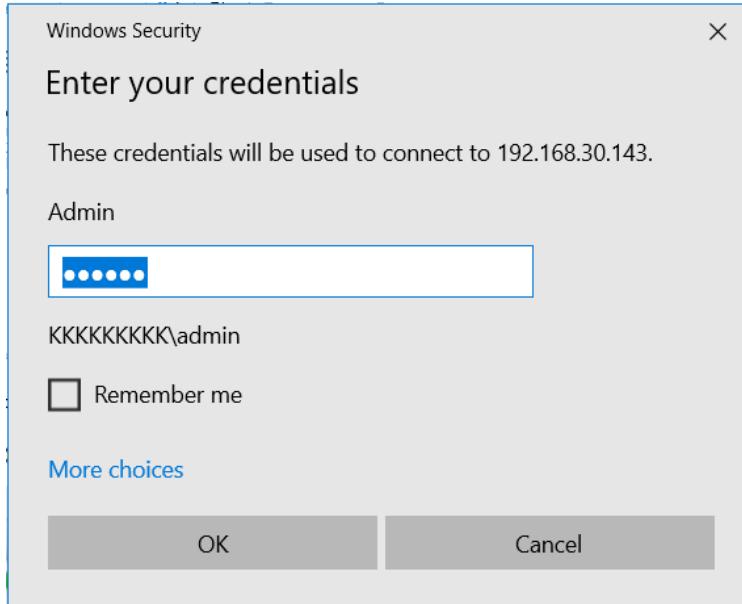
Buttons at the bottom right: Cancel, Done.

Hình 4. 15 Hoàn thành event cảnh báo RDP

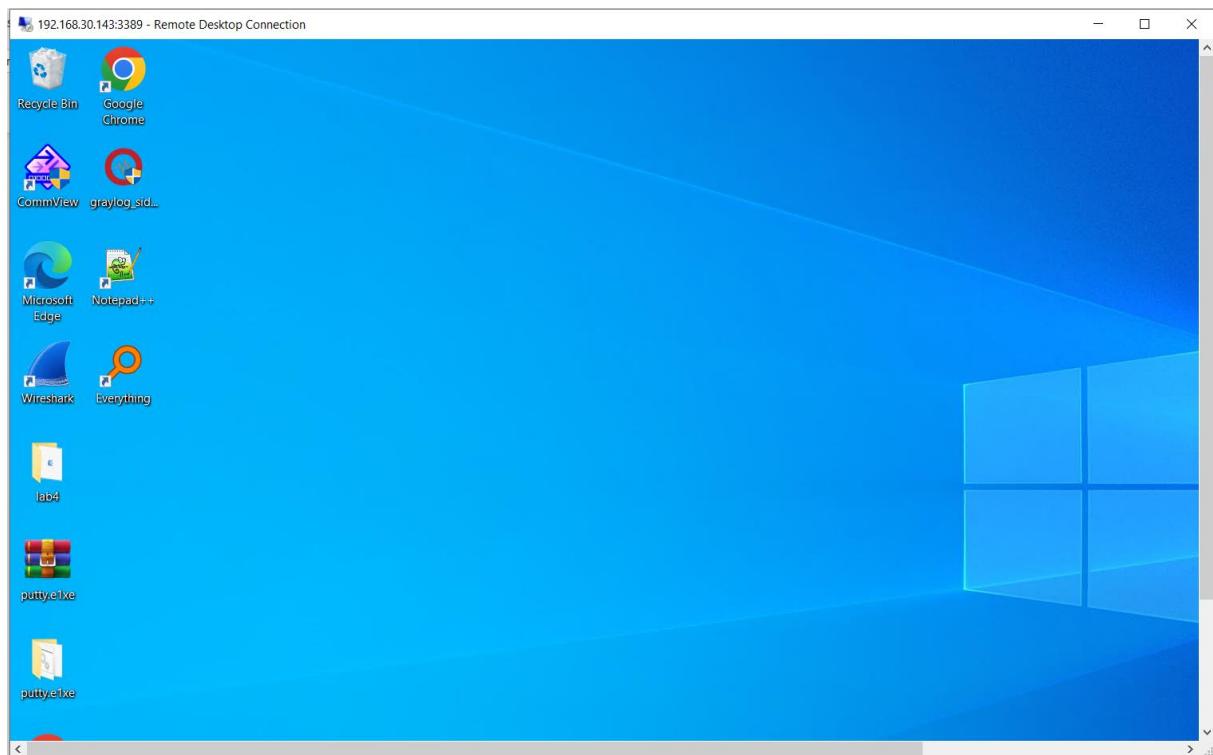
Kết nối RDP vào Client 2



Hình 4. 16 RDP vào client2



Hình 4. 17 Nhập mật khẩu RDP

*Hình 4. 18 RDP thành công vào client2*

Graylog event notification: CANH BAO RDP WINDOW ➤ [Inbox](#) ✎ ↵

n18dcat035@student.ptithcm.edu.vn to me 6:08 PM (1 minute ago) ☆ ↵

Event Definition	
Title	CANH BAO RDP WINDOW
Description	CANH BAO RDP WINDOW
Type	aggregation-v1

Event	
Timestamp	2022-09-05T11:06:58.850Z
Message	CANH BAO RDP WINDOW
Source	localhost
Key	
Priority	3
Alert	true
Timestamp Processing	2022-09-05T11:06:58.850Z
Timerange Start	

*Hình 4. 19 Gmail đã nhận được cảnh báo RDP*

Graylog APP 6:07 PM

Alert CANH BAO RDP WINDOW triggered:

CANH BAO RDP WINDOW

Custom Message:

--- [Event Definition] -----  
Title: CANH BAO RDP WINDOW  
Type: aggregation-v1

--- [Event] -----  
Timestamp: 2022-09-05T11:06:58.850Z  
[Show more](#)

Alert CANH BAO RDP WINDOW triggered:

CANH BAO RDP WINDOW

Custom Message:

--- [Event Definition] -----  
Title: CANH BAO RDP WINDOW  
Type: aggregation-v1

--- [Event] -----  
Timestamp: 2022-09-05T11:06:58.850Z  
[Show more](#)

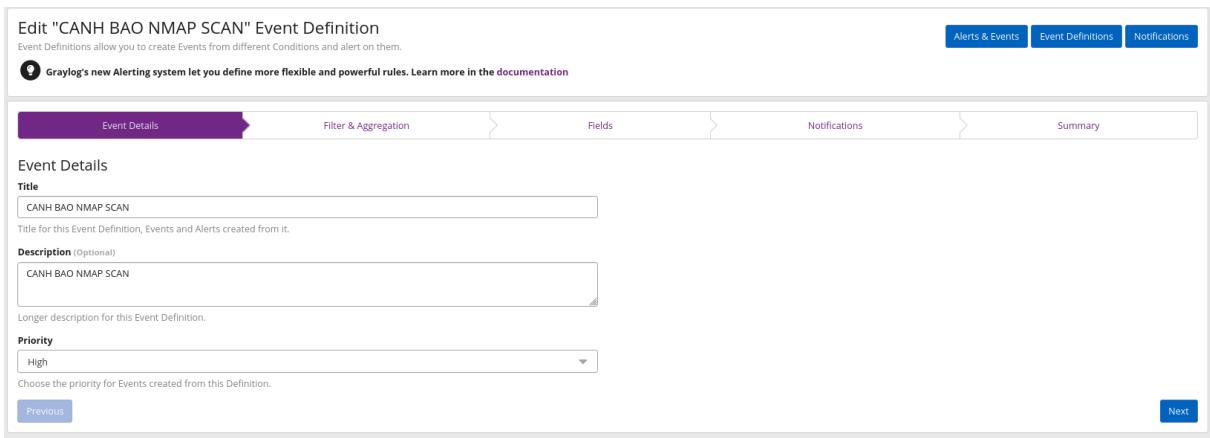
Hình 4. 20 Slack đã nhận được cảnh báo RDP

### 4.3. CẢNH BÁO NMAP SCAN

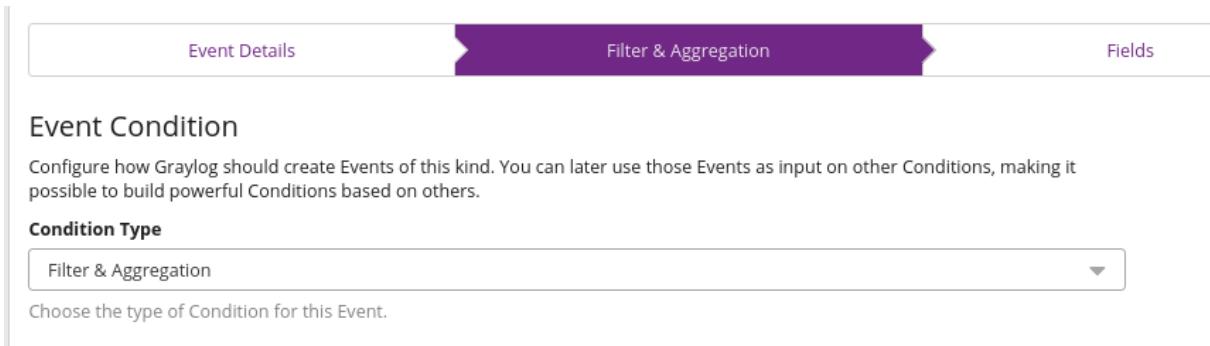
Rule Iptables để bắt Nmap Scan đưa vào log

```
-A INPUT -p tcp -m tcp --tcp-flags
FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -j LOG --log-prefix
"NMAP Xmas scan: " --log-level 7
```

Cấu hình event cảnh báo Nmap Scan như sau:



Hình 4. 21 Tạo event cảnh báo Nmap Scan



Hình 4. 22 Chọn Filter & Aggregation

## Filter

Add Information to filter the log messages that are relevant for this Event Definition.

### Search Query

message:"NMAP"

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

### Streams (Optional)

NMAP SCAN x



Select streams the search should include. Searches in all streams if empty.

### Search within the last

5



minutes ▼

### Execute search every

1



minutes ▼

#### Enable

Should this event definition be executed automatically?

### Create Events for Definition if...

Filter has results

Aggregation of results reaches a threshold

Hình 4. 23 Diều thông tin cần thiết của cảnh báo Nmap Scan

### Aggregation

Summarize log messages matching the Filter defined above by using a function. You can optionally group the Filter results by identical field values.

#### Group by Field(s) (Optional)

PING - string x



Select Fields that Graylog should use to group Filter results when they have identical values. Example:

Assuming you created a Filter with all failed log-in attempts in your network, Graylog could alert you when there are more than 5 failed log-in attempts overall. Now, add `username` as Group by Field and Graylog will alert you for each `username` with more than 5 failed log-in attempts.

### Create Events for Definition

Messages must meet all of the following rules:

If	Is	Threshold	
count()	>	50	<span style="border: 1px solid #ccc; padding: 0 2px;">-</span> <span style="border: 1px solid #ccc; padding: 0 2px;">+</span> Add Group
Condition summary			
<input checked="" type="checkbox"/> Condition is valid			
Preview: count() > 50			

Previous Next

Hình 4. 24 Nếu phát hiện trên 50 lần mới gửi thông báo

### Edit "CANH BAO NMAP SCAN" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

[Alerts & Events](#) [Event Definitions](#) [Notifications](#)

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Event Details	Filter & Aggregation	Fields	Notifications	Summary
Event Fields (optional) Include additional information in Events generated from this Event Definition by adding custom Fields. That can help you search Events or having more context when receiving Notifications. This Event does not have any custom Fields yet.				
<a href="#">Add Custom Field</a>	<a href="#">Previous</a>	<a href="#">Next</a>		

Hình 4. 25 Event Fields

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO

Edit "CANH BAO NMAP SCAN" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Notifications (optional)

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

Notification	Type	Actions
email notification	Email Notification	<a href="#">Remove from Event</a>
Slack Notification	Slack Notification	<a href="#">Remove from Event</a>

[Add Notification](#)

Manage Notifications [Edit](#)

Notification Settings

Grace Period

0 seconds

Graylog sends Notifications for Alerts every time they occur. Set a Grace Period to control how long Graylog should wait before sending Notifications again. Note that Events with keys will have a Grace Period for each different key value.

Message Backlog

50

Number of messages to be included in Notifications.

Previous Next

Hình 4. 26 Chọn Notification qua Gmail và Slack

graylog

Search Streams Alerts Dashboards Enterprise ▾ Wizard ▾ System ▾ 4

Event Summary

Details

Title: CANH BAO NMAP SCAN

Description: CANH BAO NMAP SCAN

Priority: High

Fields

No Fields configured for Events based on this Definition.

Filter & Aggregation

Type: Aggregation

Search Query: message:"NMAP"

Streams: NMAP SCAN

Search within: 5 minutes

Execute search every: 1 minutes

Enable scheduling: yes

Group by Field(s): PING

Create Events if: count() > 50

Notifications

Settings: Grace Period is disabled

Notifications will include 50 messages

email notification: Email Notification [More details](#)

Slack Notification: Slack Notification [More details](#)

Cancel Done

Hình 4. 27 Hoàn thành event cảnh báo Nmap Scan

### Tiến hành Nmap vào client

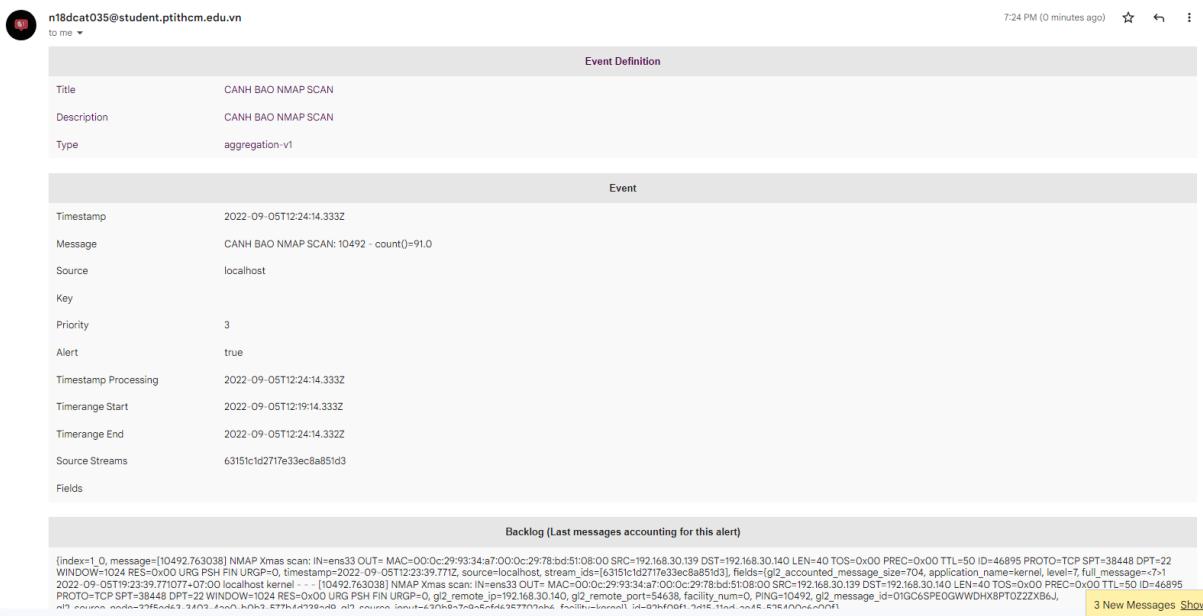
```
[root@graylogserver n18dcat035]# nmap -v -sX 192.168.30.140
Starting Nmap 6.40 ( http://nmap.org ) at 2022-09-05 19:23 +07
Initiating ARP Ping Scan at 19:23
Scanning 192.168.30.140 [1 port]
Completed ARP Ping Scan at 19:23, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:23
Completed Parallel DNS resolution of 1 host. at 19:23, 0.03s elapsed
Initiating XMAS Scan at 19:23
Scanning 192.168.30.140 [1000 ports]
Increasing send delay for 192.168.30.140 from 0 to 5 due to 409 out of 1363 dropped probes since last increase.
Increasing send delay for 192.168.30.140 from 5 to 10 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 192.168.30.140 from 10 to 20 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 192.168.30.140 from 20 to 40 due to 11 out of 24 dropped probes since last increase.
Completed XMAS Scan at 19:23, 21.75s elapsed (1000 total ports)
Nmap scan report for 192.168.30.140
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT      STATE          SERVICE
22/tcp    open|filtered  ssh
111/tcp   open|filtered  rpcbind
MAC Address: 00:0C:29:93:34:A7 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 22.05 seconds
          Raw packets sent: 1460 (58.388KB) | Rcvd: 4382 (765.798KB)
[root@graylogserver n18dcat035]#
```

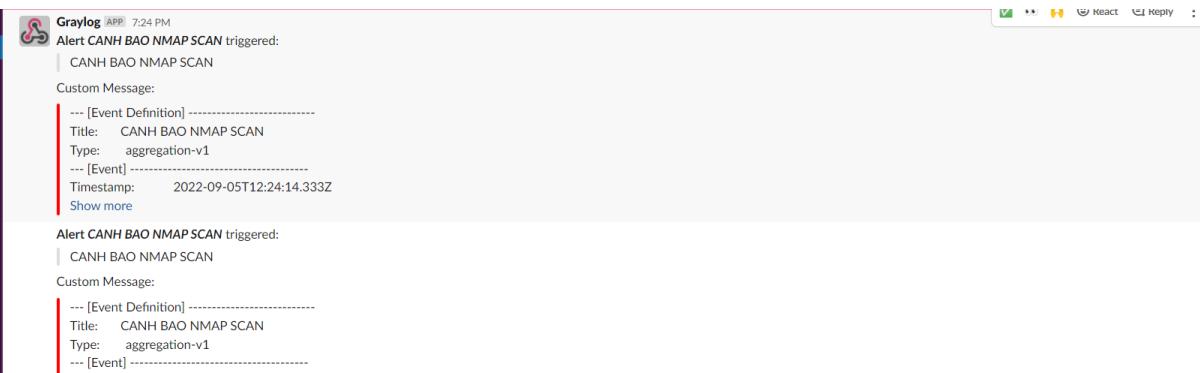
Hình 4. 28 Nmap vào Client

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO



Hình 4. 29 Gmail đã nhận được cảnh báo Nmap Scan



Hình 4. 30 Slack đã nhận được cảnh báo Nmap Scan

## 4.4. CẢNH BÁO FLOOD ICMP

Rule Iptables để bắt log ICMP

```
-A INPUT -p icmp --icmp-type 8 -m limit --limit 1/sec --limit-burst 10 -j LOG --log-prefix "PING "
```

Cấu hình event cảnh báo Flood ICMP như sau:

Edit "CANH BAP FLOOD ICMP" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Event Details

Title: CANH BAP FLOOD ICMP

Description (Optional): FLOOD ICMP

Priority: High

Choose the priority for Events created from this Definition.

Event Details Filter & Aggregation Fields Notifications Summary

Alerts & Events Event Definitions Notifications

Hình 4. 31 Tạo event cảnh báo Flood ICMP

The screenshot shows the Graylog interface with the 'Event Details' tab at the top. Below it, a purple bar contains the text 'Filter & Aggregation'. To the right of the bar are tabs for 'Fields' and 'Summary'. The main area is titled 'Event Condition' with the sub-instruction: 'Configure how Graylog should create Events of this kind. You can later use those Events as input on other Conditions, making it possible to build powerful Conditions based on others.' A dropdown menu labeled 'Condition Type' is open, showing 'Filter & Aggregation' as the selected option.

Hình 4. 32 Chọn Filter &amp; Aggregation

## Filter

Add information to filter the log messages that are relevant for this Event Definition.

### Search Query

ICMP

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

### Streams (Optional)

rsyslog X

X ▼

Select streams the search should include. Searches in all streams if empty.

### Search within the last

1

▼ minutes ▼

### Execute search every

1

▼ minutes ▼

Enable

Should this event definition be executed automatically?

### Create Events for Definition if...

Filter has results

Aggregation of results reaches a threshold

Hình 4. 33 Điện thoại tin cần thiết của cảnh báo ICMP

The screenshot shows the 'Create Events for Definition' section. It starts with an 'Aggregation' step, which is collapsed. Below it is a 'Group by Field(s) (Optional)' step where 'PING - string' is selected. This is followed by a note: 'Select Fields that Graylog should use to group Filter results when they have identical values. Example: Assuming you created a Filter with all failed log-in attempts in your network, Graylog could alert you when there are more than 5 failed log-in attempts overall. Now, add `username` as Group by Field and Graylog will alert you for each `username` with more than 5 failed log-in attempts.' The next step is 'Create Events for Definition', which includes a condition: 'If count() > 10' and a summary: 'Condition is valid'. At the bottom are 'Previous' and 'Next' buttons.

Hình 4. 34 Phát hiện trên 10 lần thì gửi cảnh báo

The screenshot shows the 'Edit "CANH BAP FLOOD ICMP" Event Definition' screen. It includes tabs for 'Alerts & Events', 'Event Definitions', and 'Notifications'. The main area has tabs for 'Event Details', 'Filter & Aggregation', 'Fields', 'Notifications', and 'Summary'. The 'Event Details' tab is active. Below it is a section for 'Event Fields (optional)' with a note: 'Include additional information in Events generated from this Event Definition by adding custom Fields. That can help you search Events or having more context when receiving Notifications.' A note also states: 'This Event does not have any custom Fields yet.' At the bottom are 'Add Custom Field', 'Previous', and 'Next' buttons.

Hình 4. 35 Event Fields

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO

Edit "CANH BAP FLOOD ICMP" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Notifications (optional)

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

Notification	Type	Actions
email notification	Email Notification	<a href="#">Remove from Event</a>
Slack Notification	Slack Notification	<a href="#">Remove from Event</a>

Add Notification

Manage Notifications

Notification Settings

Grace Period

Message Backlog

Number of messages to be included in Notifications.

Previous Next

Hình 4. 36 Chọn Notification qua Gmail và Slack

graylog

Search Streams Alerts Dashboards Enterprise Wizard System

Event Details Filter & Aggregation Fields Notifications Summary

Event Summary

Details

Title: CANH BAP FLOOD ICMP

Description: FLOOD ICMP

Priority: High

Fields

No Fields configured for Events based on this Definition.

Filter & Aggregation

Type: Aggregation Search Query ICMP Streams

Search within: 1 minutes Execute search every: 1 minutes Enable scheduling: yes Group by Field(s): PING Create Events if count() > 10

Notifications

Settings

Grace Period is disabled Notifications will include 50 messages

email notification Email Notification More details

Slack Notification Slack Notification More details

Cancel Done

Graylog 4.2.12+2e659fb on localhost (Red Hat, Inc. 1.8.0\_342 on Linux 3.10.0-1160.71.1.el7.x86\_64)

Hình 4. 37 Hoàn thành event cảnh báo RDP

Flood icmp bằng ping3 vào client1

```
[root@graylogserver n18dcat035]# hping3 192.168.30.140 --flood --icmp
HPING 192.168.30.140 (ens33 192.168.30.140): icmp mode set, 28 headers + 0 data bytes
hpPing in flood mode, no replies will be shown
^C
--- 192.168.30.140 hping statistic ---
1786239 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Hình 4. 38 Flood icmp vào client1

# BÁO CÁO TTTN ĐẠI HỌC

## CHƯƠNG 4: XÂY DỰNG CÁC KỊCH BẢN TÂN CÔNG VÀ CẢNH BÁO

Graylog event notification: CANH BAP FLOOD ICMP ➤ [Inbox](#)

n18dcat035@student.ptithcm.edu.vn to me

Event Definition

Title	CANH BAP FLOOD ICMP
Description	FLOOD ICMP
Type	aggregation-v1

Event

Timestamp	2022-09-05T12:41:29.532Z
Message	CANH BAP FLOOD ICMP: PING - count()=36.0
Source	localhost
Key	
Priority	3
Alert	true
Timestamp Processing	2022-09-05T12:41:29.532Z
Timerange Start	2022-09-05T12:40:29.532Z
Timerange End	2022-09-05T12:41:29.531Z
Source Streams	630bc5739a5cf6d35770d592
Fields	

Backlog (Last messages accounting for this alert)

```
(index=1,0, message=PING IN=ens3 OUT= MAC=00:0c:29:93:34:47:00:0c:29:78:bd:5108:00 SRC=192.168.30.139 DST=192.168.30.140 LEN=28 TOS=0x00 PREC=0x00 TTL=64 ID=62659 PROTO=ICMP TYPE=8 CODE=0 ID=54108 SEQ=1280, timestamp=2022-09-05T12:41:03.028Z, source=localhost, stream_id=630bc5739a5cf6d35770d592, fields=[{g2_accounted_message_size=>603, application_name=>kernel, level=>4, full_message=>4-1 2022-09-05T19:41:03.028730-07:00 localhost kernel --- PING IN=ens3 OUT= MAC=00:0c:29:93:34:47:00:0c:29:78:bd:5108:00 SRC=192.168.30.139 DST=192.168.30.140 LEN=28 TOS=0x00 PREC=0x00 TTL=64 ID=62659 PROTO=ICMP TYPE=8 CODE=0 ID=54108 SEQ=1280, g2_remote_ip=>192.168.30.140, g2_remote_port=>54638, facility_num=>0, PING=PING, g2_message_id=>01C67F955513UJ402560JWC1, g2_source_node=>32f5ed63-3403-4ae0-b063-377b4d9238ad9, g2_source_input=>630bc5739a5cf6d35770d592, facility=>kernel}, {id=00912290-2d18-1fed-ae45-925400c0ec00}],
```

Hình 4. 39 Gmail đã nhận được cảnh báo Flood ICMP

Graylog APP 7:41 PM

Alert CANH BAP FLOOD ICMP triggered:

FLOOD ICMP

Custom Message:

--- [Event Definition] -----  
Title: CANH BAP FLOOD ICMP  
Type: aggregation-v1  
--- [Event] -----  
Timestamp: 2022-09-05T12:41:29.532Z  
[Show more](#)

Alert CANH BAP FLOOD ICMP triggered:

FLOOD ICMP

Custom Message:

--- [Event Definition] -----  
Title: CANH BAP FLOOD ICMP  
Type: aggregation-v1  
--- [Event] -----  
Timestamp: 2022-09-05T12:42:29.532Z  
[Show more](#)

Hình 4. 40 Slack đã nhận được cảnh báo Flood ICMP

## CHƯƠNG 5: KẾT LUẬN

### 5.1 KẾT QUẢ ĐẠT ĐƯỢC

Đề tài “**Tìm hiểu và triển khai hệ thống quản lý và phân tích nhật ký Graylog**” có thể dùng như nguồn tài liệu cho mọi người trong quá trình mới bắt đầu thực hiện nghiên cứu Log management.

Trong quá trình thực hiện đề tài, em học được nhiều kĩ thuật mới trong quá trình ghi log từ client và đẩy log từ client để server

Đồng thời em cũng thấy được sự hạn chế của cơ chế đọc log và phân tích log  
Xét về tổng thể em cảm thấy hài lòng với đề tài.

### 5.2 HẠN CHẾ

Do hạn chế về thời gian nghiên cứu, cũng như kinh nghiệm nên em vẫn chưa hoàn thiện được đề tài như mong đợi. Các phần lý thuyết còn chưa rõ ràng, chưa đi sâu các cơ chế

## TÀI LIỆU THAM KHẢO

### Danh mục các Website tham khảo:

1. <https://www.graylog.org/post/what-is-log-management-a-complete-logging-guide>
2. Đặng Trần Lê Anh(2019), Nghiên cứu các kỹ thuật xử lý và phân tích log
3. <https://docs.graylog.org/>
4. <https://github.com/hocchudong/ghichep-graylog/tree/master/docs/graylog-v4>