TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN, ĐHQG-HCM

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO ĐỒ ÁN MÔN HỌC

ĐỀ TÀI: TRIỂN KHAI VÀ GIÁM SÁT HỆ THỐNG MẠNG VỚI SPLUNK

Môn học: NT531.P21 – Đánh giá hiệu năng hệ thống mạng máy tính

Giảng viên hướng dẫn: Đặng Lê Bảo Chương

Thực hiện bởi nhóm 10, bao gồm:

STT	Họ và Tên	MSSV
1	Lương Cao Thắng	22521328
2	Phạm Hữu Thắng	22521340
3	Phạm Xuân Tuấn Anh	22520071

Thời gian thực hiện: 30/3/2025 – 5/4/2025

MỤC LỤC

TÓM TẮT

Đồ án triển khai hệ thống giám sát mạng với Splunk nhằm thu thập, phân tích log và phát hiện sự kiện bất thường, nâng cao bảo mật. Mô hình gồm Firewall SOPHOS bảo vệ mạng, DMZ chứa Web Server, LAN có Domain Controller, Client PC và Splunk Server. Splunk giám sát log từ firewall, server, thiết bị mạng để phát hiện truy cập trái phép, tấn công và hỗ trợ quản trị viên xử lý sự cố nhanh chóng, đảm bảo an toàn hệ thống.

Chương I. TỔNG QUAN

1. Giới thiệu đề tài:

1.1. Nội dung chính của đề tài:

Đề tài "Triển khai và giám sát hệ thống mạng với Splunk" tập trung vào việc thiết lập một hệ thống mạng có tích hợp giải pháp giám sát an ninh Splunk. Hệ thống giúp thu thập, phân tích log từ các thiết bị mạng như firewall, máy chủ, domain controller và phát hiện các sự kiện bất thường nhằm nâng cao tính bảo mật.

1.2. Lý do chọn đề tài:

- Tăng cường bảo mật hệ thống: Việc giám sát log giúp phát hiện và xử lý sớm các mối đe dọa, giảm thiểu rủi ro tấn công mạng.
- Tối ưu hóa quản trị hệ thống: Hỗ trợ quản trị viên theo dõi hoạt động mạng, xác định lỗi và cải thiện hiệu suất.
- Ứng dụng thực tiễn cao: Splunk là công cụ mạnh mẽ được sử dụng rộng rãi trong các doanh nghiệp để giám sát và phân tích log.
- Mở rộng kiến thức chuyên môn: Giúp nhóm tiếp cận với các công nghệ bảo mật và quản trị hệ thống thực tế.

1.3. Liên quan đến nội dung môn học:

Đề tài liên quan trực tiếp đến các kiến thức trong các môn học về Mạng máy tính, An toàn thông tin, Hệ điều hành, Quản trị hệ thống. Cụ thể:

- Mạng máy tính: Cấu hình và quản lý hệ thống mạng với các thành phần như firewall, domain controller, server.
- An toàn thông tin: Ứng dụng Splunk để giám sát, phân tích log và phát hiện xâm nhập.
- Hệ điều hành & Quản trị hệ thống: Cấu hình và vận hành Splunk trên hệ thống mạng doanh nghiệp.

2. Cơ sở lý thuyết:

2.1. Giới thiệu về Splunk:

Splunk là một nền tảng phân tích dữ liệu và log mạnh mẽ, giúp thu thập, xử lý và trực quan hóa dữ liệu từ nhiều nguồn khác nhau để phát hiện sự kiện bất thường và tối ưu hóa hệ thống.

2.2. Firewall SOPHOS:

SOPHOS là tường lửa giúp bảo vệ hệ thống khỏi các cuộc tấn công từ bên ngoài, kiểm soát truy cập và ghi nhận log về lưu lượng mạng.

2.3. Cấu trúc mạng với DMZ:

DMZ (Demilitarized Zone) là vùng trung lập chứa Web Server, giúp cô lập các dịch vụ công khai với mạng nội bộ, giảm rủi ro tấn công trực tiếp.

2.4. Domain Controller:

Domain Controller là máy chủ quản lý xác thực người dùng và tài nguyên trong mạng nội bộ, đóng vai trò quan trọng trong bảo mật và quản lý hệ thống.

2.5. Các phương pháp giám sát log:

- Thu thập log từ nhiều nguồn: Firewall, máy chủ, thiết bị mạng.
- Phân tích log: Xác định hành vi bất thường, tấn công mạng.
- Cảnh báo và phản hồi: Tạo cảnh báo tự động khi phát hiện nguy cơ bảo mật.

2.6. Ứng dụng thực tế của hệ thống:

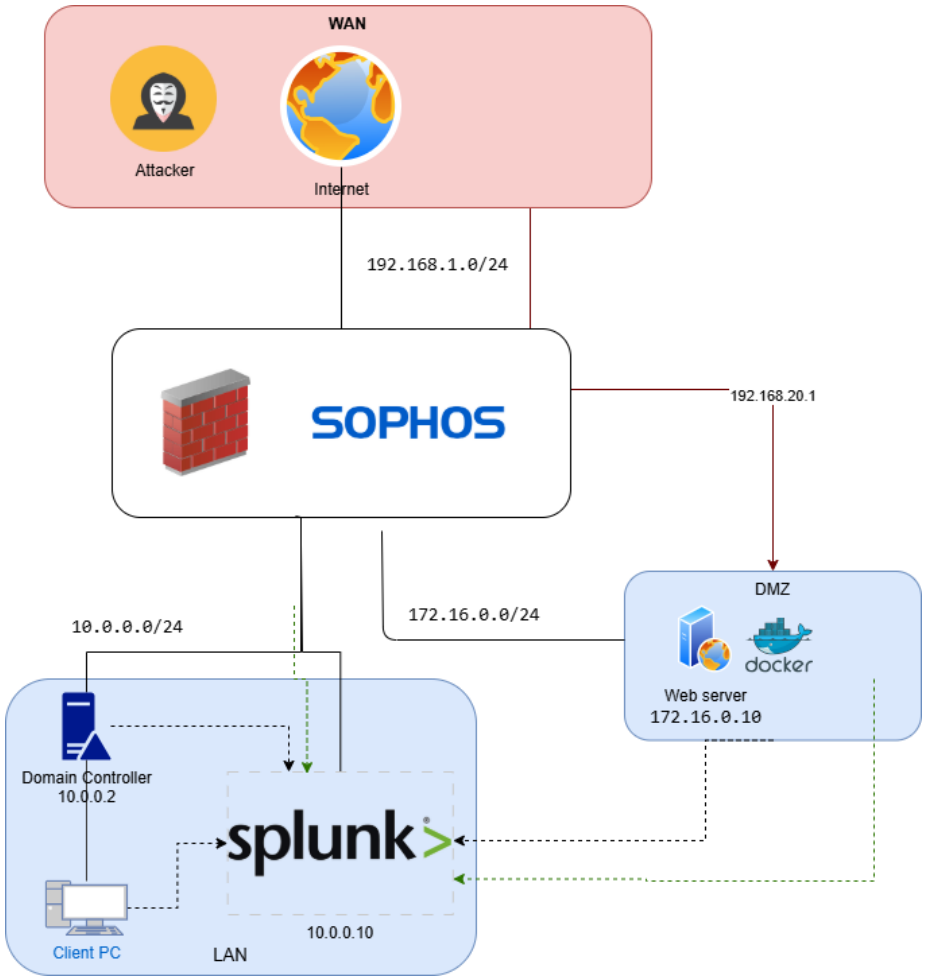
- Giám sát an ninh hệ thống doanh nghiệp.
- Phát hiện truy cập trái phép và cảnh báo tấn công.
- Hỗ trợ điều tra sự cố bảo mật nhanh chóng.

Chương II. THIẾT KẾ HỆ THỐNG:

1. Kiến trúc hệ thống:

Hệ thống giám sát mạng sử dụng Splunk được thiết kế với mô hình ba vùng chính: WAN (Internet), DMZ, và LAN. Firewall SOPHOS đóng vai trò bảo vệ hệ thống khỏi các cuộc tấn công từ bên ngoài, trong khi Splunk giám sát và phân tích log từ các thiết bị quan trọng.

1.1. Biểu đồ kiến trúc hệ thống



Mô hình hệ thống

Hệ thống gồm các thành phần chính:

- WAN (Internet): Kết nối từ bên ngoài, có thể xuất hiện các mối đe dọa như hacker, mã độc, tấn công DDoS.
- Firewall SOPHOS: Đóng vai trò kiểm soát lưu lượng vào/ra giữa WAN, DMZ và LAN. Firewall này giúp lọc các truy cập trái phép, ghi nhận log bảo mật và gửi dữ liệu này đến Splunk để phân tích.
- DMZ (Demilitarized Zone): Chứa Web Server phục vụ các dịch vụ công khai.
- LAN (Mạng nội bộ): Gồm các thành phần quan trọng:
    - Domain Controller (DC - 10.0.0.2): Quản lý xác thực và tài nguyên mạng.
    - Client PC: Máy tính người dùng trong hệ thống.
    - Splunk Server (10.0.0.10): Nhận, xử lý và phân tích log từ firewall, DC, web server và các thiết bị khác.

2. Luồng xử lý và tương tác giữa các thành phần:

2.1. Luồng dữ liệu trong hệ thống:

- Người dùng hoặc hacker truy cập vào Web Server (172.16.0.10) qua Internet. Firewall SOPHOS kiểm soát luồng truy cập này, chặn các kết nối nguy hiểm và cho phép kết nối hợp lệ.
- Web Server phản hồi yêu cầu và thực hiện giao tiếp với các dịch vụ nội bộ nếu cần.
- Domain Controller xử lý xác thực người dùng trong hệ thống LAN, quản lý quyền truy cập tài nguyên.
- Splunk Server thu thập log từ các nguồn:
    - Firewall SOPHOS gửi log về các gói dữ liệu đến/đi.
    - Web Server gửi log về hoạt động HTTP, đăng nhập thất bại, lỗi hệ thống.
    - Domain Controller gửi log về hoạt động người dùng, xác thực thành công/thất bại.
    - Máy trạm (Client PC) có thể gửi log về hoạt động truy cập và ứng dụng.
- Splunk phân tích dữ liệu và phát hiện sự kiện bất thường như truy cập trái phép, tấn công DDoS, lỗi hệ thống.
- Cảnh báo và hiển thị kết quả trên Dashboard: Nếu phát hiện mối đe dọa, Splunk có thể gửi cảnh báo qua email hoặc hệ thống giám sát để quản trị viên kịp thời xử lý.

2.2. Mô hình tương tác giữa các thành phần

- Firewall SOPHOS ↔ Splunk: Firewall gửi log về lưu lượng mạng, truy cập bị chặn, các cuộc tấn công nghi ngờ.
- Web Server ↔ Splunk: Gửi log về hoạt động HTTP, lỗi hệ thống, truy cập đáng ngờ.

- Domain Controller ↔ Splunk: Gửi log về xác thực người dùng, thay đổi quyền truy cập.
- Client PC ↔ Splunk: (Tùy chọn) Gửi log về hoạt động đăng nhập, truy cập file quan trọng.

3. Biểu đồ chi tiết:

3.1. Biểu đồ luồng dữ liệu (Data Flow Diagram - DFD)

- Mức 0 (DFD Level 0):
  - Người dùng → Web Server → Firewall → Splunk → Quản trị viên
  - Người dùng → Domain Controller → Splunk
- Mức 1 (DFD Level 1):
  - Firewall lọc và gửi log đến Splunk
  - Splunk phân tích log từ Web Server và Domain Controller
  - Splunk tạo cảnh báo nếu phát hiện bất thường

3.2. Biểu đồ luồng sự kiện (Event Flow Diagram)

1. Người dùng truy cập Web Server
2. Firewall kiểm tra gói tin, cho phép hoặc từ chối truy cập
3. Web Server xử lý yêu cầu và phản hồi
4. Domain Controller xác thực người dùng nội bộ
5. Splunk nhận log từ Firewall, Web Server, Domain Controller
6. Splunk phân tích và phát hiện sự kiện bất thường
7. Gửi cảnh báo đến quản trị viên nếu phát hiện nguy cơ

4. Phương án triển khai:

4.1. Cấu hình Splunk để thu thập log

- Tích hợp với Firewall SOPHOS để lấy log về các gói dữ liệu
- Cấu hình Web Server và Domain Controller để gửi log về Splunk
- Xây dựng Dashboard hiển thị dữ liệu giám sát

4.2. Chính sách bảo mật

- Quản lý quyền truy cập Splunk để chỉ cho phép quản trị viên xem dữ liệu
- Bảo vệ Splunk Server khỏi tấn công bằng firewall nội bộ
- Mã hóa log gửi giữa các thiết bị và Splunk

Chương III. TRIỂN KHAI HỆ THỐNG.

Hostname	**IP**
SOPHOS	10.0.0.1(Vmnet1), 172.16.0.1 (Vmnet2), 192.168.1.3 (NAT hoặc Bridge)
Domain Controller, ClientPC	10.0.0.2 (Vmnet1)
DMZ	172.16.0.10 (Vmnet2)
Splunk	10.0.0.10 (Vmnet1)

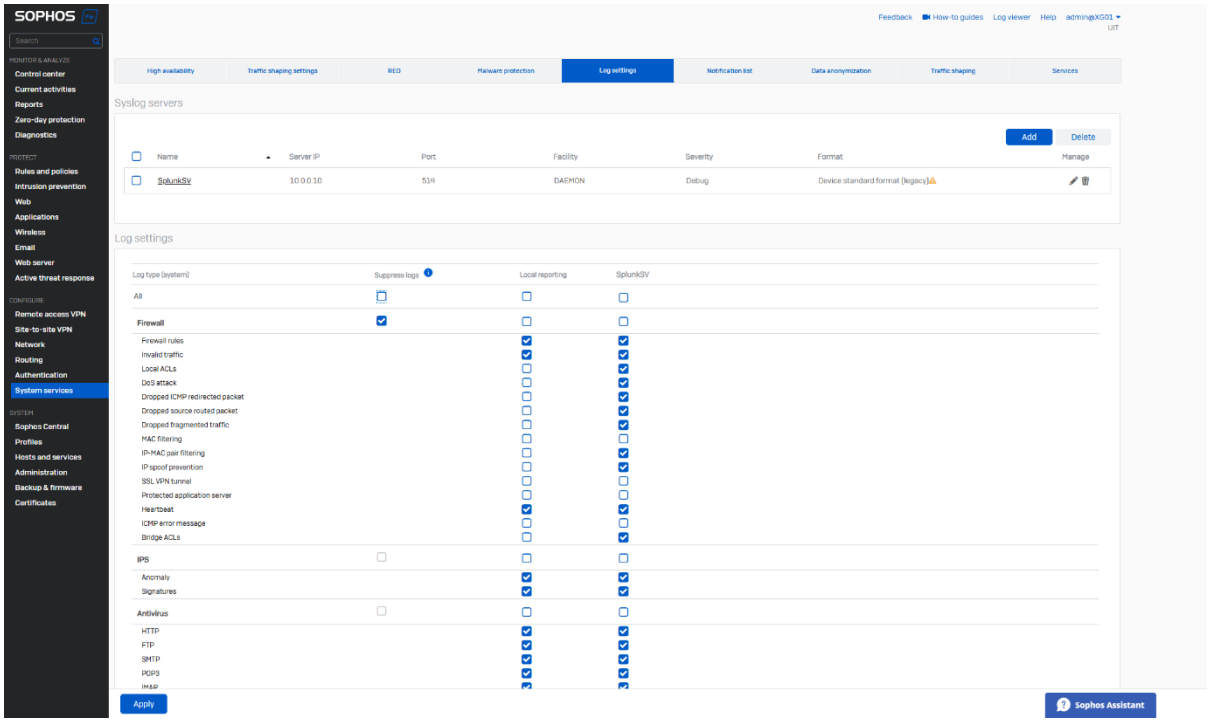
Hostname, IP của các máy thành phần.

Đây là phần nội dung mô tả chi tiết về quá trình tìm hiểu, xây dựng và triển khai hệ thống mà nhóm đã thực hiện.

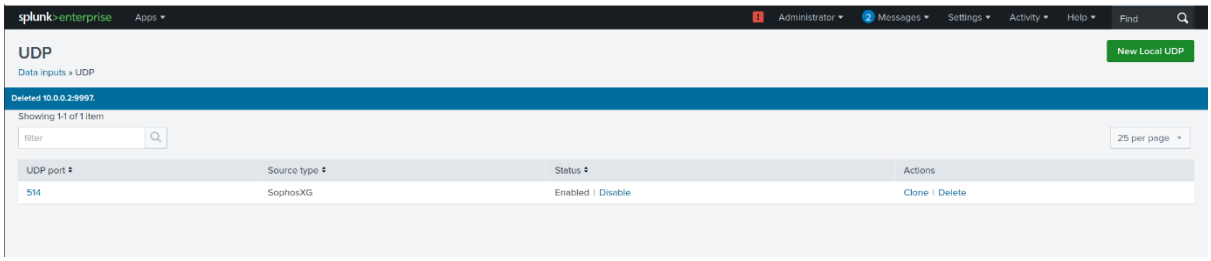
1. Logs từ SOPHOS:

1.1 Đẩy logs (Syslog) sophos về splunk:

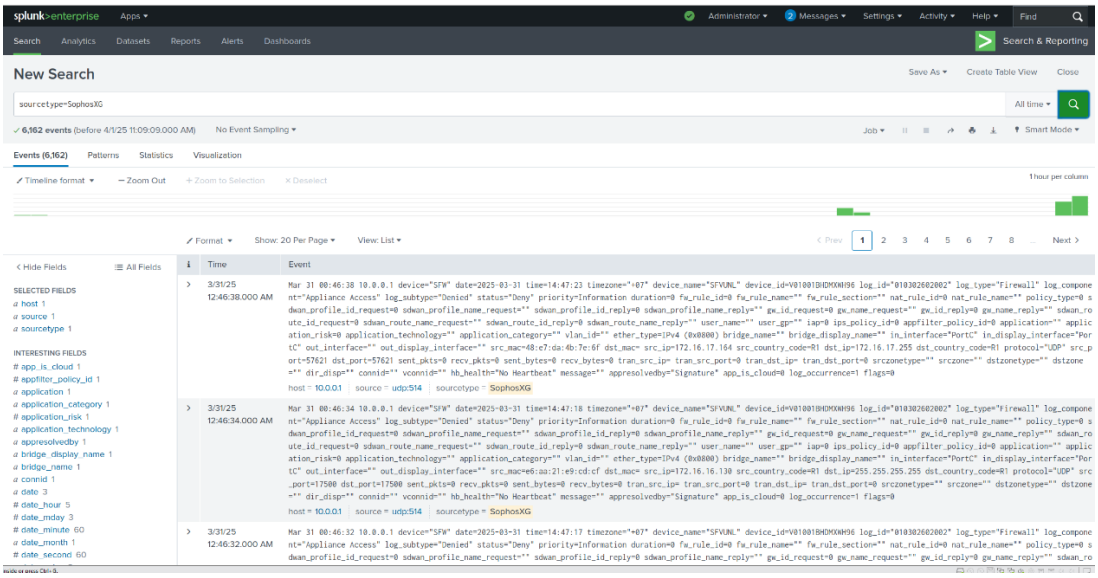
- Vào log setting sau đó tạo syslog server và setting như sau:



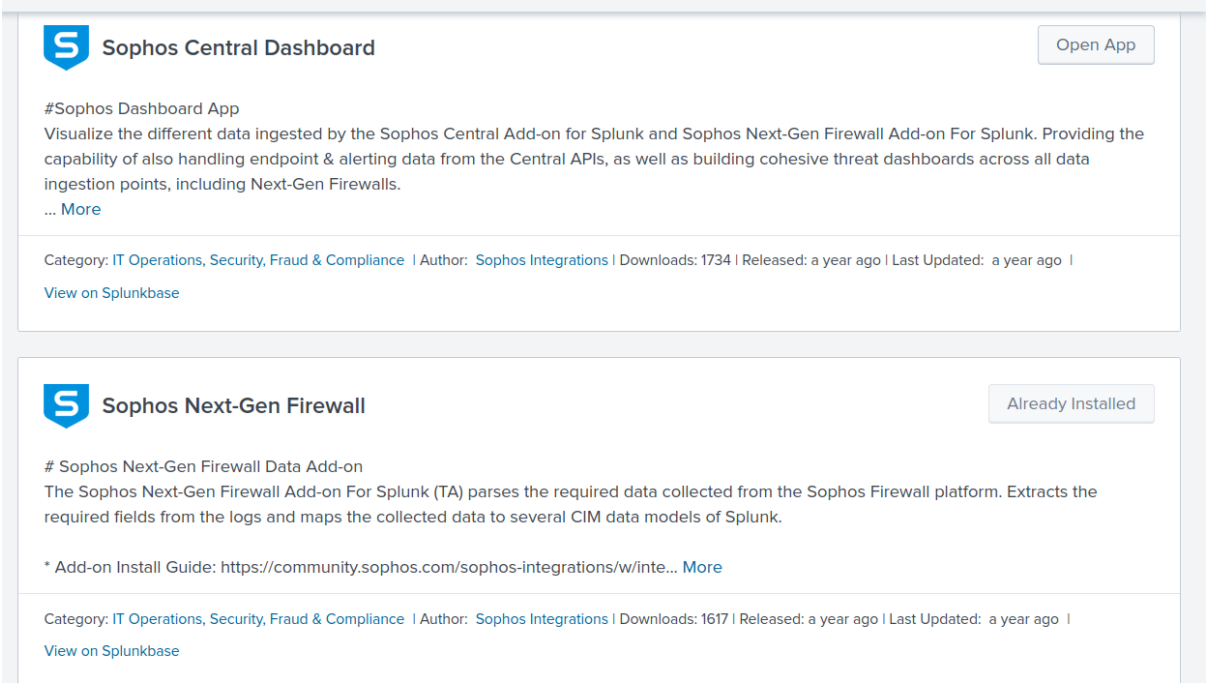
- Cấu hình nhận log tại port 514 trên Splunk: **Setting → Data Inputs → UDP** và tạo như sau:
  - Tạo mới một UDP input:
  - Port: 514.
  - Source Type: Chọn syslog hoặc một source type cụ thể cho SOPHOS (nếu đã cài add-on, chọn sophos:firewall).
  - Index: Chọn index phù hợp (ví dụ: sophos_logs).
  - Host: Đặt là IP của SOPHOS (10.0.0.1, 172.16.0.1, hoặc 192.168.1.3 tùy thuộc vào giao diện gửi log).

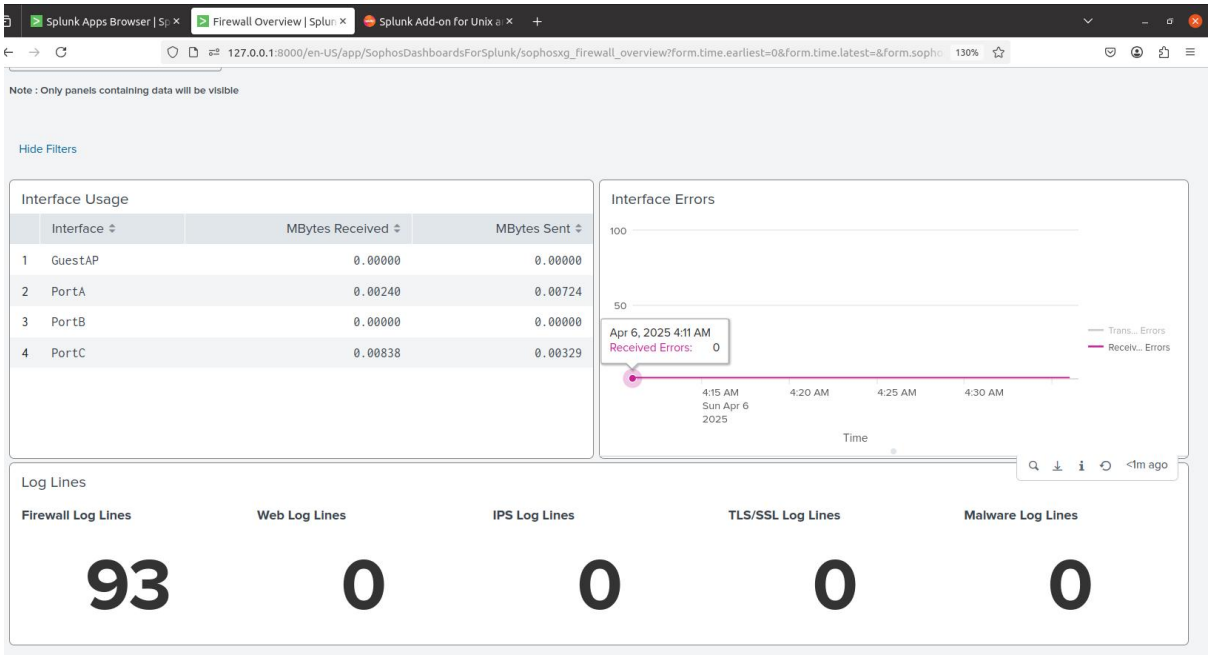


- Sau khi lưu, kiểm tra log trong Splunk bằng cách tìm kiếm:
  - ❖ Kết quả:



1.2 Cài plugin:

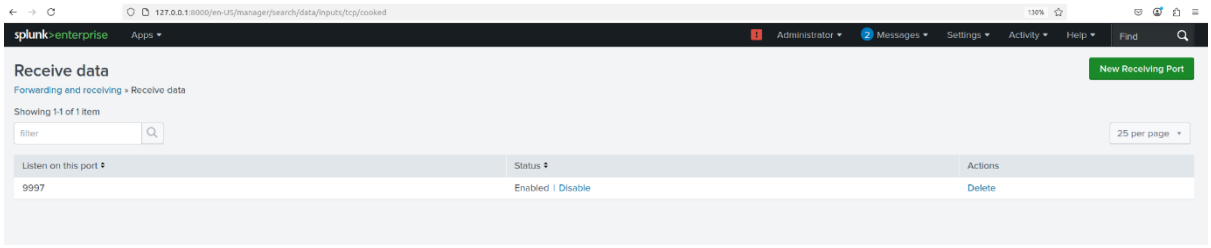




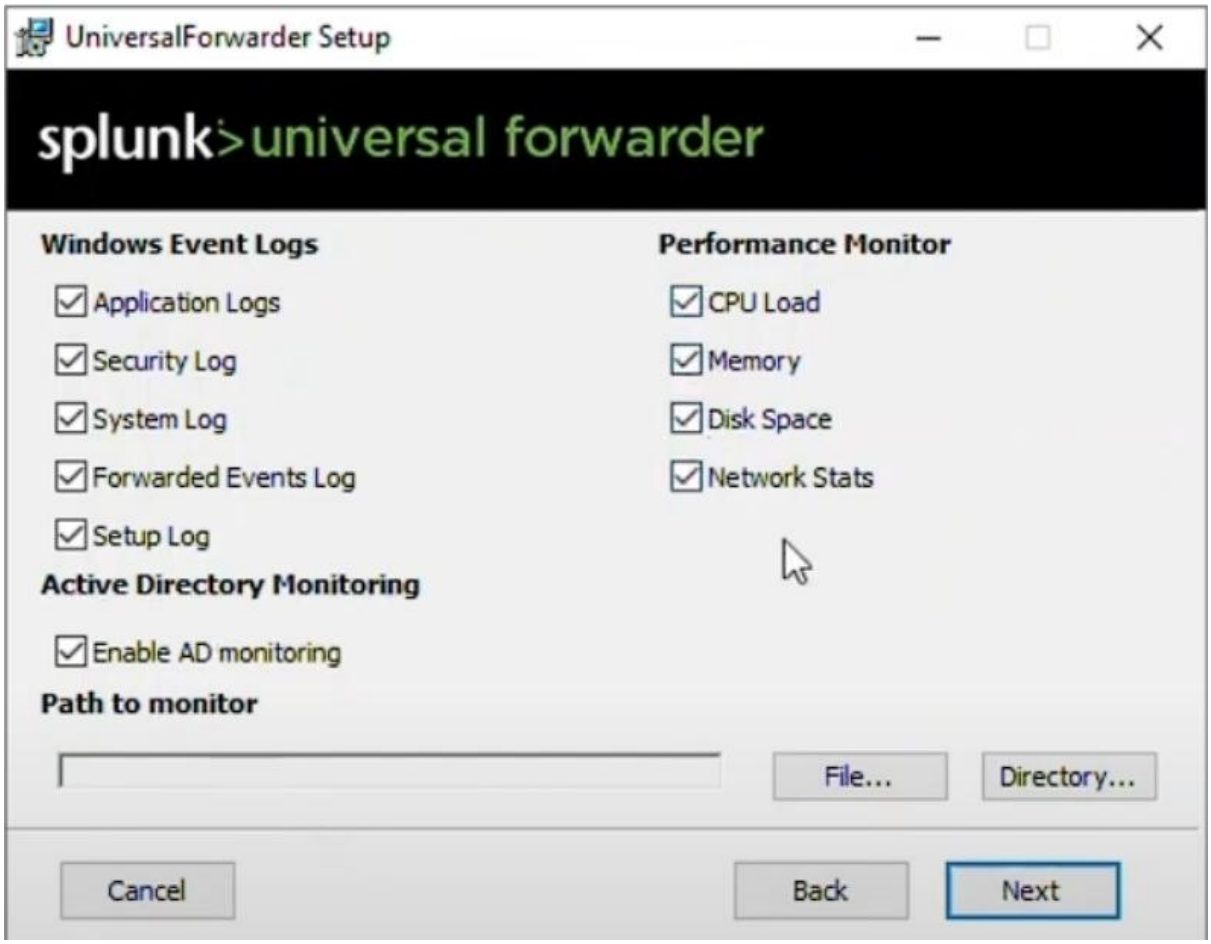
- Tải add-on theo hướng dẫn theo đường link https://community.sophos.com/sophos-integrations/w/integrations/106/splunk-add-on-for-sophos-next-gen-firewall
  - ❖ Lưu ý: Add-on cần được cài trên Splunk Server (Search Head và Indexer) và có thể cần cài trên Universal Forwarder nếu SOPHOS gửi log qua Forwarder.

2. Logs từ Domain Controller (Windows):

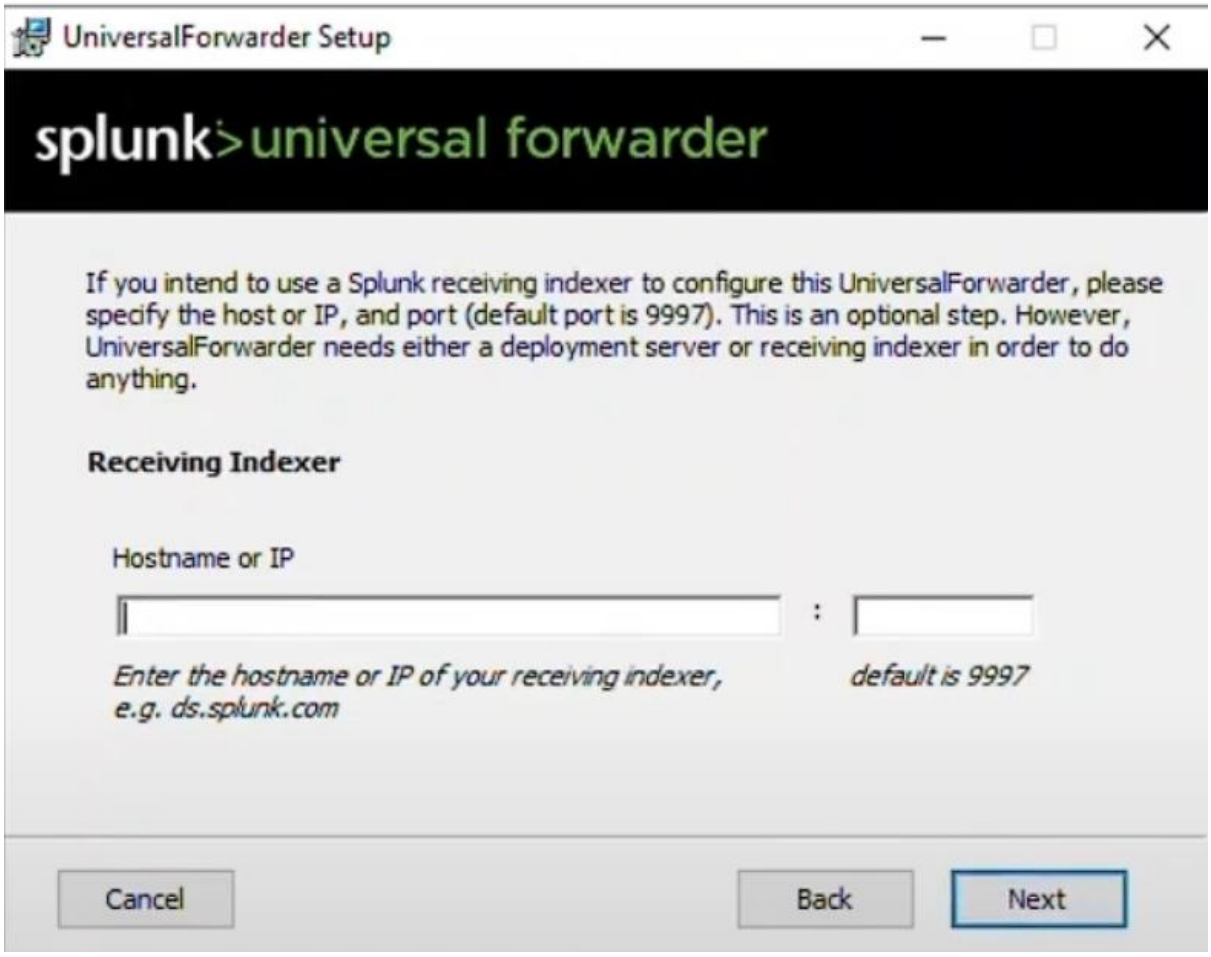
- Logs từ Domain Controller về Splunk: Mở listening port 9997 tại **Settings → Forwarding and receiving → Receive data.**



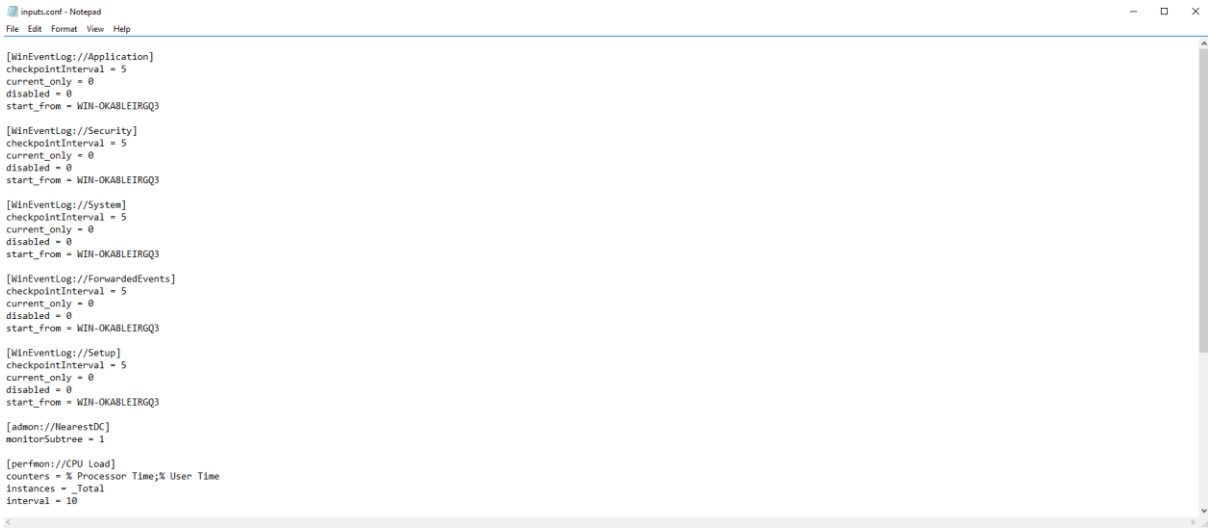
- Cài Forwarder trên DC(tìm logo Splunk forwarder), đăng nhập bằng tên Domain**.**
- Chọn những sự kiện muốn theo dõi



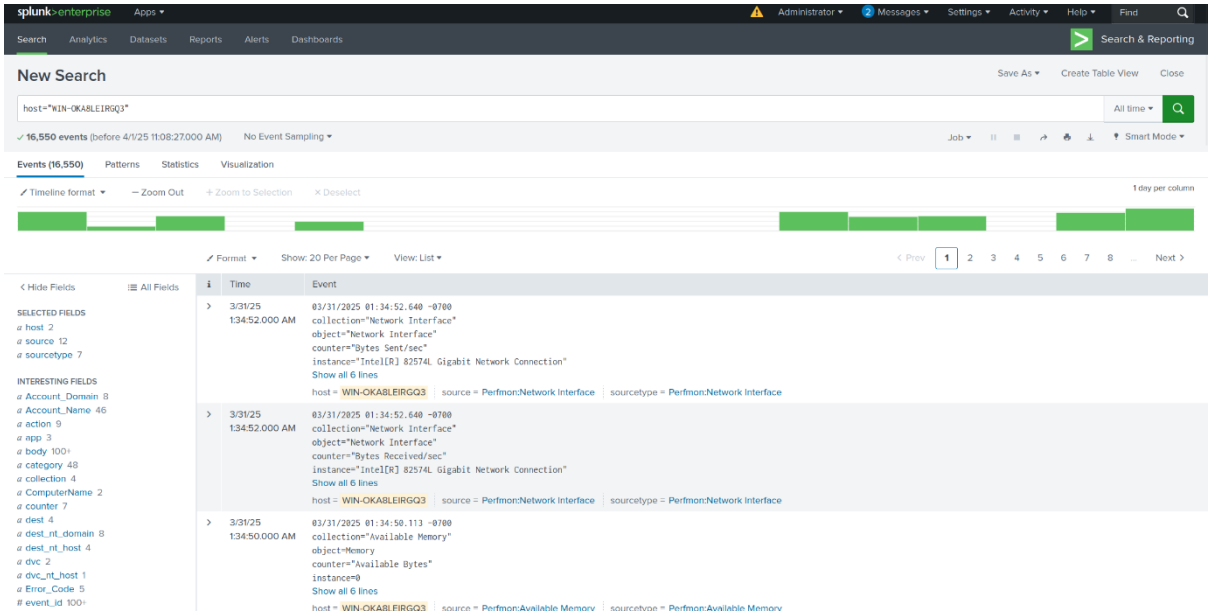
- Cấu hình receiver là IP của máy Splunk & port là 9997:



- Vào "*C:\ProgramFiles\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local*" chỉnh sửa file inputs.conf: thay tất cả sau *start_from=<tên máy>*.



❖ Kết quả (cột bên trái là các trường liên quan):



- Tải thêm Add-on để quản lí và giám sát dành cho Domain Controller là hệ điều hành Windows

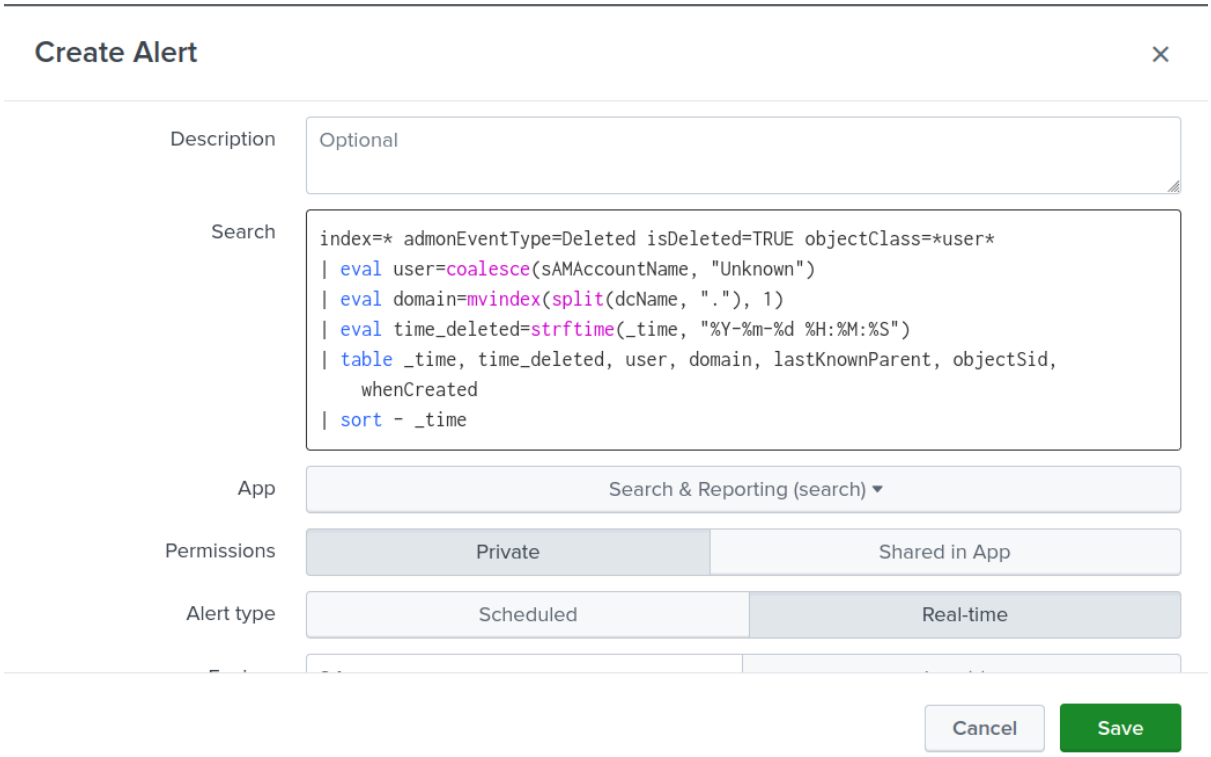
- Mẫu Rule Alert để phát hiện tài khoản bị xóa:

```
index=* admonEventType=Deleted isDeleted=TRUE objectClass=*user*
| eval user=coalesce(sAMAccountName, "Unknown")
| eval domain=mvindex(split(dcName, "."), 1)
| eval time_deleted=strftime(_time, "%Y-%m-%d %H:%M:%S")
| table _time, time_deleted, user, domain, lastKnownParent, objectSid, whenCreated
| sort - _time
```

Giải thích:

- index=*: Tìm kiếm trên tất cả các index (nên giới hạn thành index=windows để tối ưu).
- admonEventType=Deleted isDeleted=TRUE objectClass=*user*: Tìm các sự kiện liên quan đến việc xóa tài khoản người dùng trong Active Directory.
- eval user=coalesce(sAMAccountName, "Unknown"): Gán giá trị sAMAccountName cho trường user, nếu không có thì gán là "Unknown".
- eval domain=mvindex(split(dcName, "."), 1): Tách tên domain từ dcName (ví dụ: dc.company.local → company).

- eval time_deleted=strftime(_time, "%Y-%m-%d %H:%M:%S"): Định dạng thời gian xóa tài khoản.
- table và sort: Hiển thị kết quả theo bảng và sắp xếp theo thời gian giảm dần

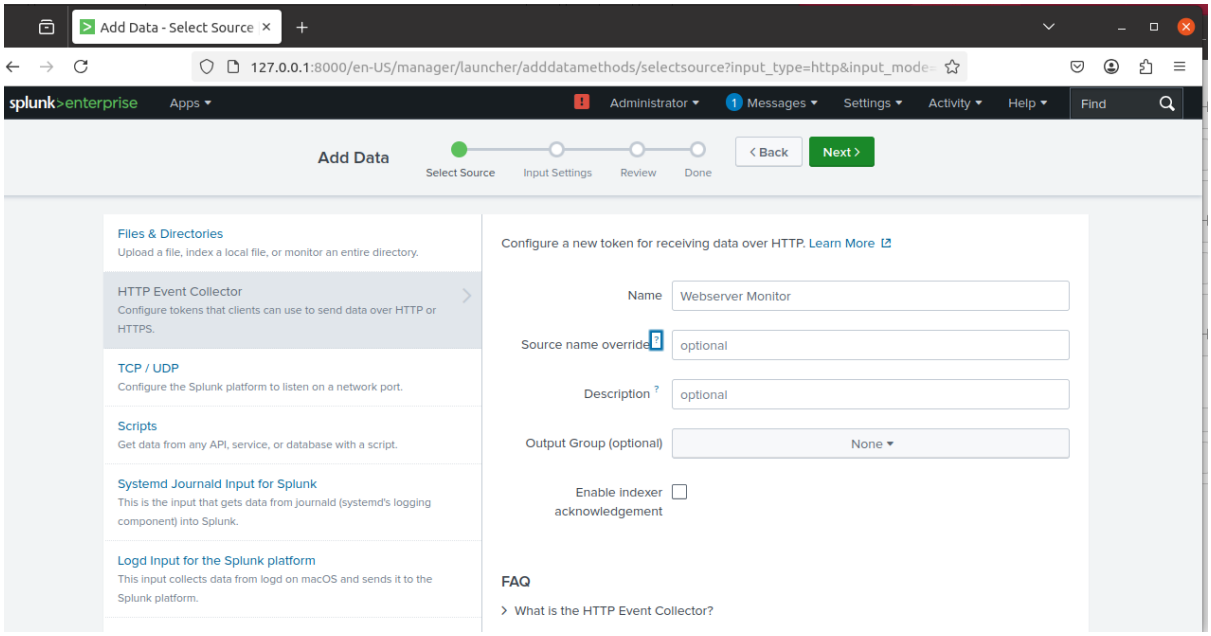


- Truy cập Splunk Web: Search & Reporting > Alerts > Create Alert, nhập câu lệnh SPL trên. Khi xóa một user trên Domain Controller, sẽ có cảnh báo.

3. Lấy logs từ Ubuntu chạy Web Server (thông qua docker container):

3.1 Nhận logs HTTP bằng HEC:

- Truy cập Splunk Web: Settings > Data Inputs > HTTP Event Collector.
- Tạo một HEC token mới:
  - Name: Ví dụ: webserver_hec.
  - Index: Chọn index (ví dụ: docker_logs).
  - Enable SSL: Nên bật để mã hóa dữ liệu (yêu cầu chứng chỉ SSL trên Splunk Server).
  - Token: Lưu lại token.



- Cấu hình Web Server gửi log qua HEC:
  - URL: https://10.0.0.10:8088/services/collector/event.
  - Token: Sử dụng token vừa tạo.
  - Kiểm tra log trong Splunk: index=docker_logs sourcetype=httpevent.
  - ❖ Lưu ý: Đảm bảo port 8088 được mở trên Splunk Server và firewall không chặn

3.2 Plugin lấy log từ Docker:
https://www.outcoldsolutions.com/docs/monitoring-docker/v5/installation/

```
docker run --net=host -d \
   --name collectorfordocker  \
   --volume /sys/fs/cgroup:/rootfs/sys/fs/cgroup:ro \
   --volume /proc:/rootfs/proc:ro \
   --volume /var/log:/rootfs/var/log:ro \
   --volume /var/lib/docker:/rootfs/var/lib/docker:ro \
   --volume /var/run/docker.sock:/rootfs/var/run/docker.sock:ro \
   --volume collector_data:/data/ \
   --cpu-shares=204 \
   --cpus=1 \
   --memory=256M \
   --restart=always \
   --env
"COLLECTOR__SPLUNK_URL=output.splunk__url=https://10.0.0.10:8088/services
/collector/event/1.0" \
   --env        "COLLECTOR__SPLUNK_TOKEN=output.splunk__token=ac8bb585-
b5d9-4a09-b26f-1a0f8bc16199" \
   --env "COLLECTOR__SPLUNK_INSECURE=output.splunk__insecure=true" \
   --env "COLLECTOR__ACCEPTLICENSE=general__acceptLicense=true" \
   --env "COLLECTOR__LICENSE=general__license= <your license key> " \
   --env  "COLLECTOR__STATS_INDEX=input.system_stats__index=docker_stats"
\
   --env "COLLECTOR__STATS_INDEX=input.mount_stats__index=docker_stats" \
   --env "COLLECTOR__STATS_INDEX=input.net_stats__index=docker_stats" \
   --env
"COLLECTOR__STATS_INDEX=input.net_socket_table__index=docker_stats" \
   --env
"COLLECTOR__PROCSTATS_INDEX=input.proc_stats__index=docker_stats" \
   --env
"COLLECTOR__CONTAINERLOGS_INDEX=input.files__index=docker_logs" \
   --env
"COLLECTOR__APPLICATIONLOGS_INDEX=input.app_logs__index=docker_lo
gs" \
   --env
"COLLECTOR__SYSLOG_INDEX=input.files::syslog__index=docker_logs" \
   --env
"COLLECTOR__HOSTLOGS_INDEX=input.files::logs__index=docker_logs" \
   --env "COLLECTOR__EVENTS_INDEX=input.files__index=docker_logs" \
   --privileged \
```

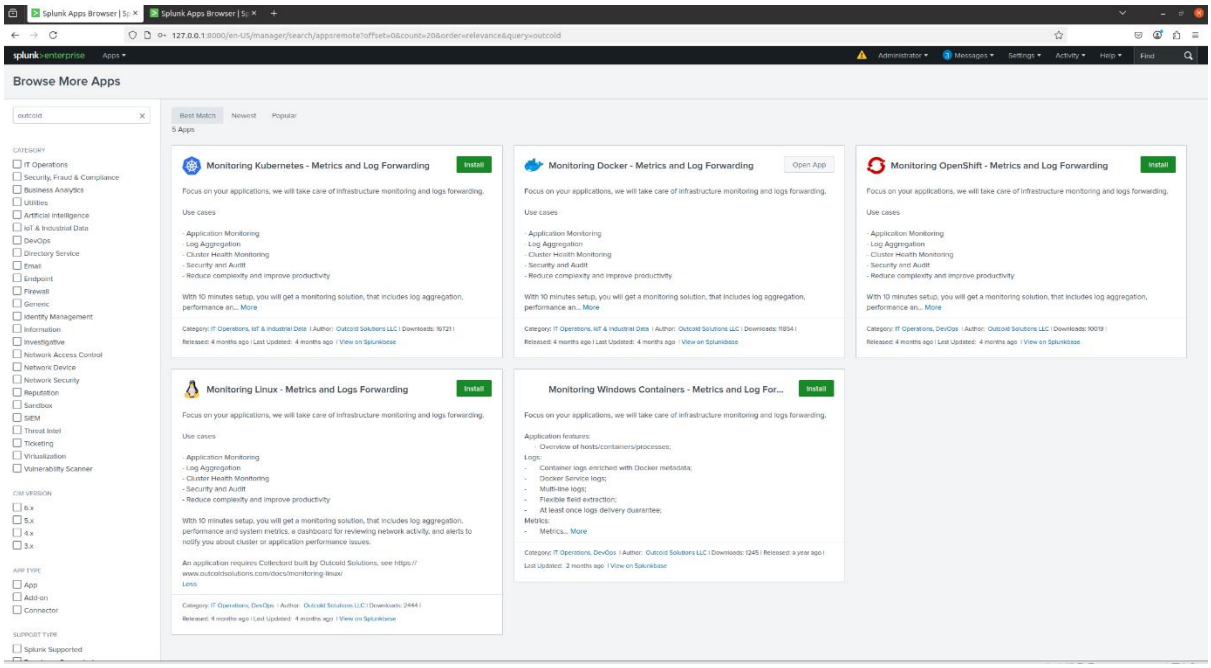
```
outcoldsolutions/collectorfordocker:5.23.432
```

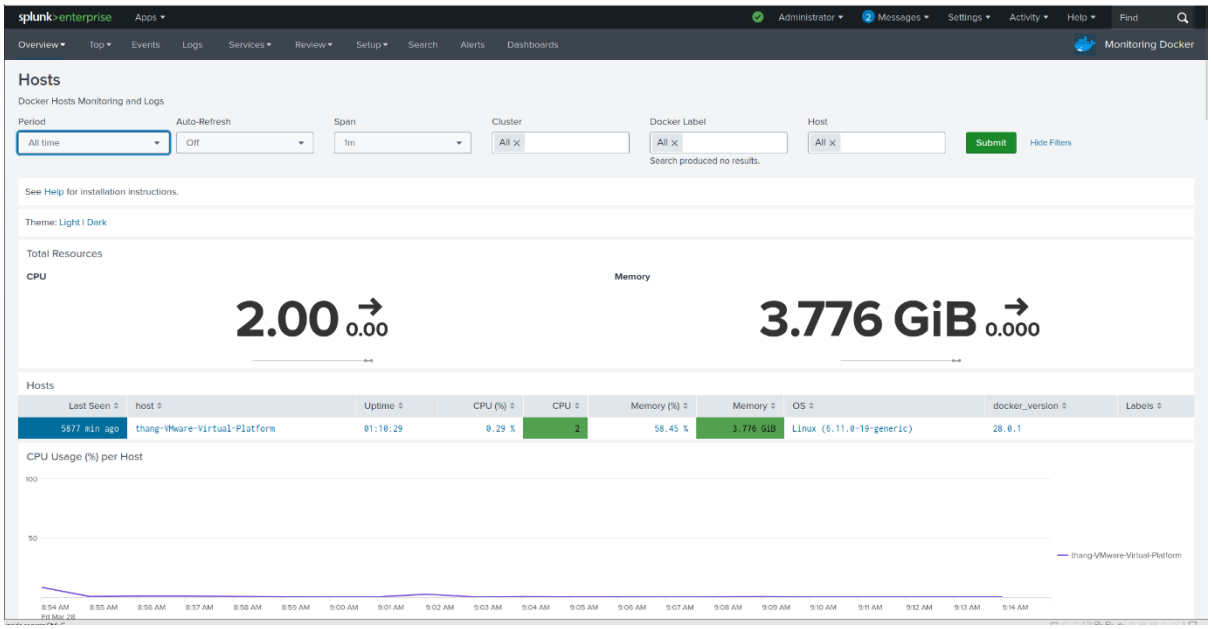
- Chạy Web Server với lệnh:

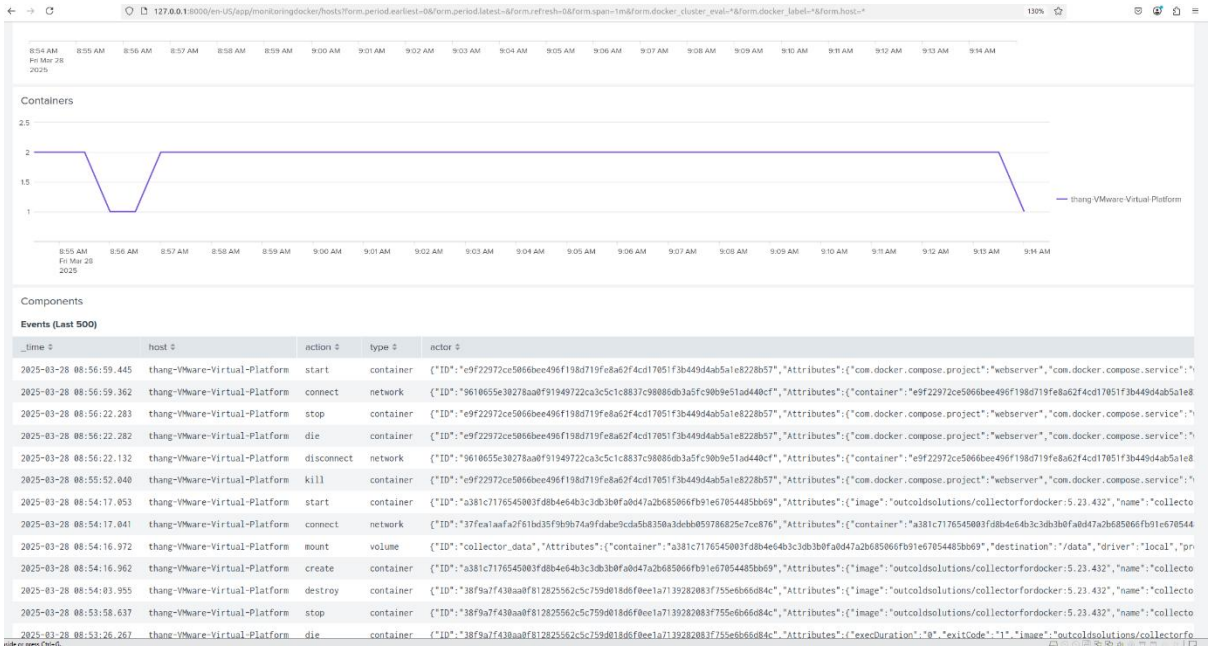
```
sudo docker run -d -p 8080:80 --log-driver=splunk \
  --log-opt splunk-url=https://10.0.0.10:8088 \
  --log-opt splunk-token=ac8bb585-b5d9-4a09-b26f-1a0f8bc16199 \
  --log-opt splunk-insecureskipverify=true \
  webserver-webserver
```

- Với các trường:
  - --log-driver=splunk: Sử dụng Splunk log driver để gửi log trực tiếp đến Splunk qua HEC.
  - --log-opt: Cung cấp URL và token của HEC.
  - splunk-insecureskipverify=true: Bỏ qua kiểm tra chứng chỉ SSL (chỉ dùng trong môi trường thử nghiệm)

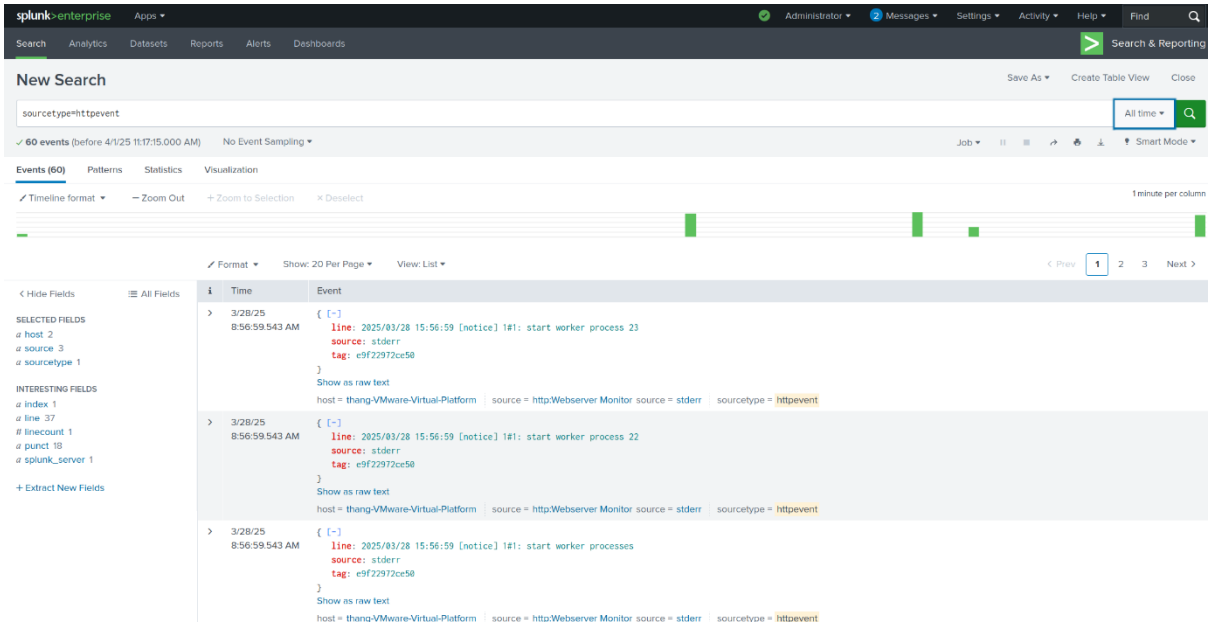
3.3 Plugin cho Docker:

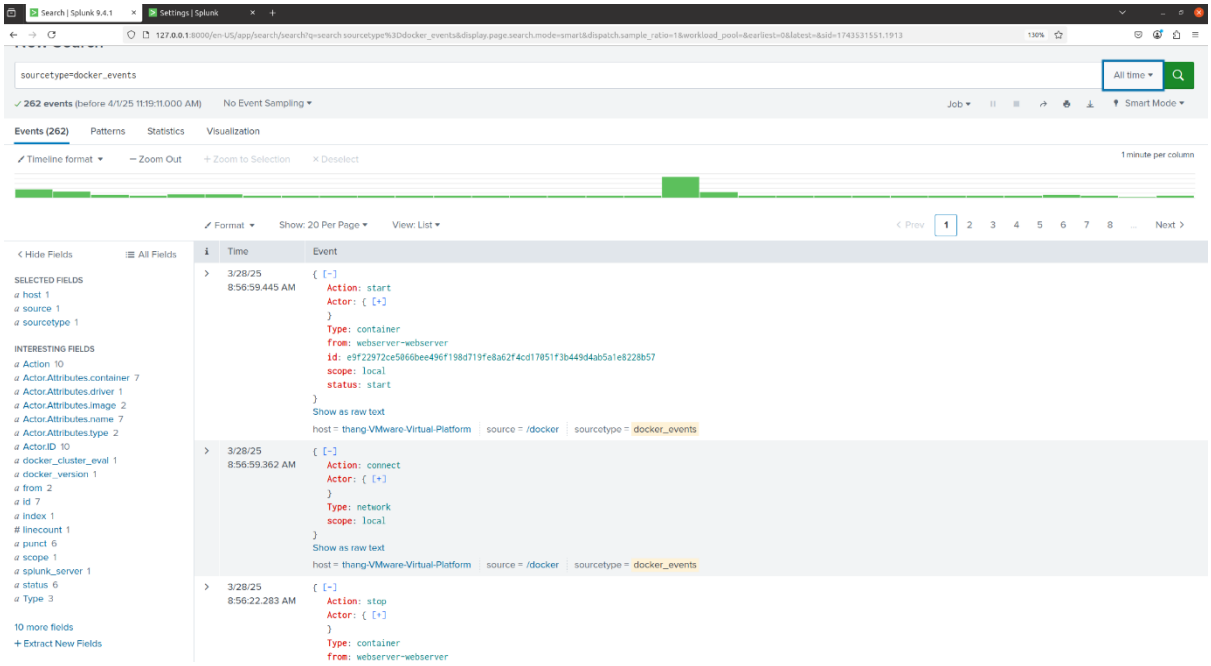


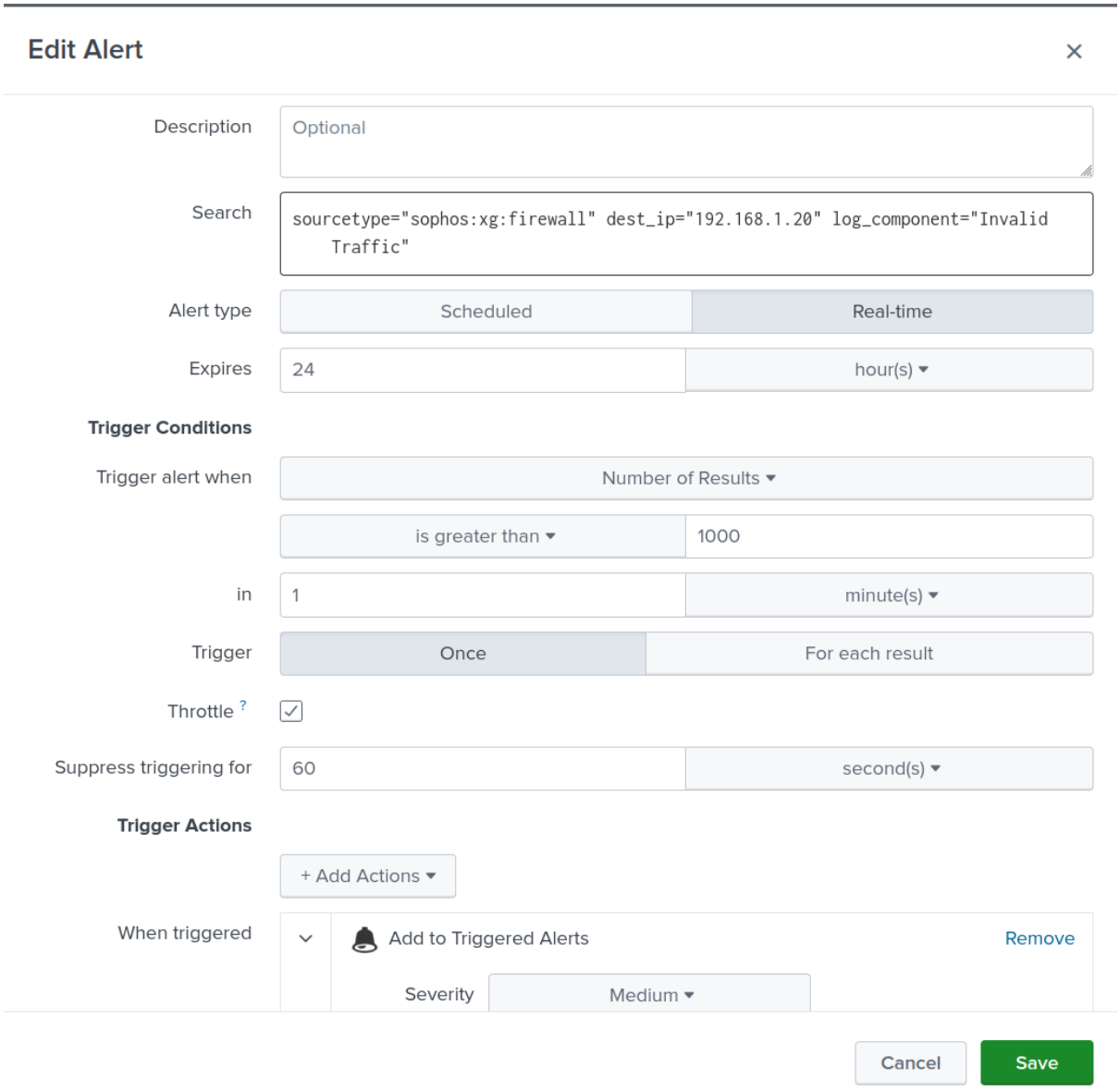




❖ Kết quả trả ra sau khi triển khai:

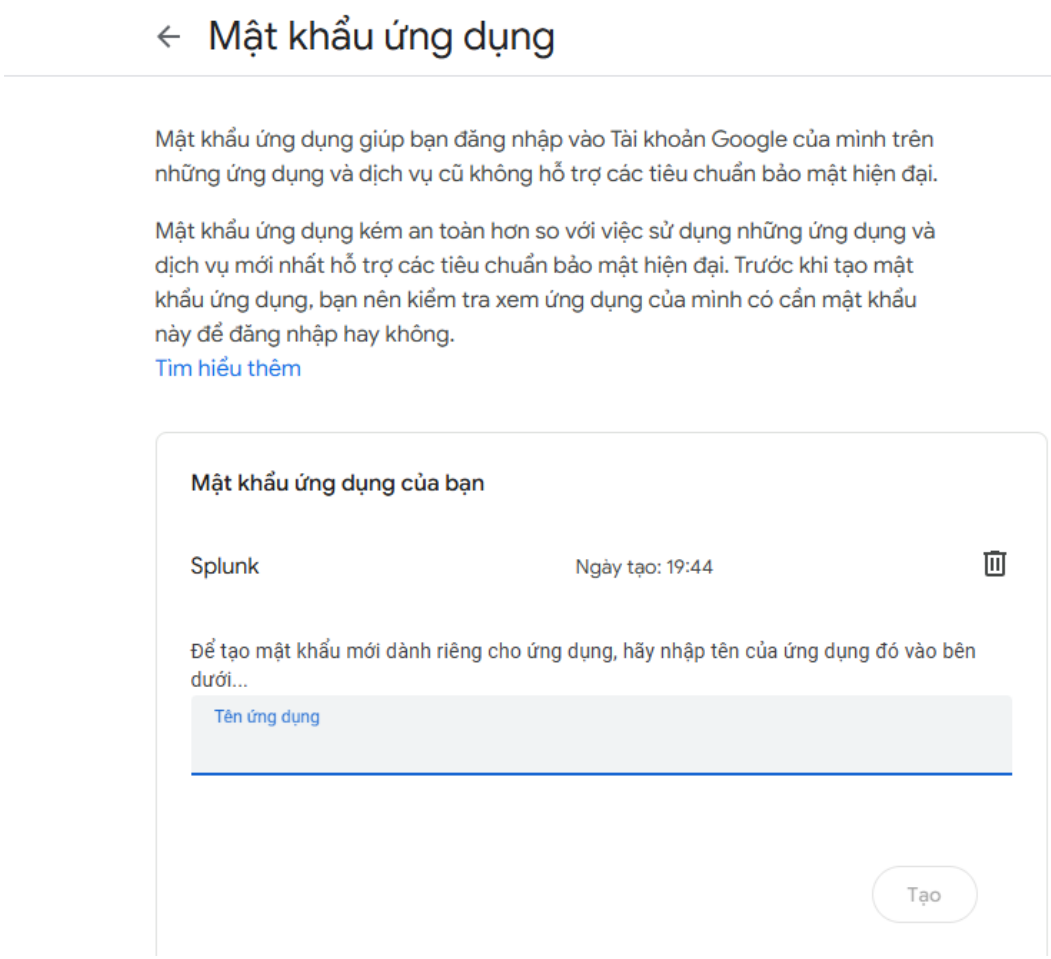

splunk>enterprise
New Search
sourcetype=httpevent
60 events (before 4/1/25 11:17:15.000 AM)
Events (60)
Patterns
Statistics
Visualization
SELECTED FIELDS
a host 2
a source 3
a sourcetype 1
INTERESTING FIELDS
a index 1
a line 37
linecount 1
a punct 18
a splunk_server 1
3/28/25 8:56:59.543 AM
line: 2025/03/28 15:56:59 [notice] 1#1: start worker process 23
source: stderr
tag: e9f22972ce50
Show as raw text
host = thang-VMware-Virtual-Platform source = http:Webserver Monitor source = stderr sourcetype = httpevent
3/28/25 8:56:59.543 AM
line: 2025/03/28 15:56:59 [notice] 1#1: start worker process 22
source: stderr
tag: e9f22972ce50
Show as raw text
host = thang-VMware-Virtual-Platform source = http:Webserver Monitor source = stderr sourcetype = httpevent
3/28/25 8:56:59.543 AM
line: 2025/03/28 15:56:59 [notice] 1#1: start worker processes
source: stderr
tag: e9f22972ce50
Show as raw text
host = thang-VMware-Virtual-Platform source = http:Webserver Monitor source = stderr sourcetype = httpevent


sourcetype=docker_events
262 events (before 4/1/25 11:19:11.000 AM)
Events (262)
Patterns
Statistics
Visualization
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Action 10
a Actor.Attributes.container 7
a Actor.Attributes.driver 1
a Actor.Attributes.image 2
a Actor.Attributes.name 7
a Actor.Attributes.type 2
a Actor.ID 10
a docker_cluster_eval 1
a docker_version 1
a from 2
a id 7
a index 1
linecount 1
a punct 6
a scope 1
a splunk_server 1
a status 6
a Type 3
10 more fields
3/28/25 8:56:59.445 AM
Action: start
Actor: { [+]
Type: container
from: webserver-webserver
id: e9f22972ce5066bee496f198d719fe8a62f4cd17051f3b449d4ab5a1e8228b57
scope: local
status: start
Show as raw text
host = thang-VMware-Virtual-Platform source = /docker sourcetype = docker_events
3/28/25 8:56:59.362 AM
Action: connect
Actor: { [+]
Type: network
scope: local
Show as raw text
host = thang-VMware-Virtual-Platform source = /docker sourcetype = docker_events
3/28/25 8:56:22.283 AM
Action: stop
Actor: { [+]
Type: container
from: webserver-webserver

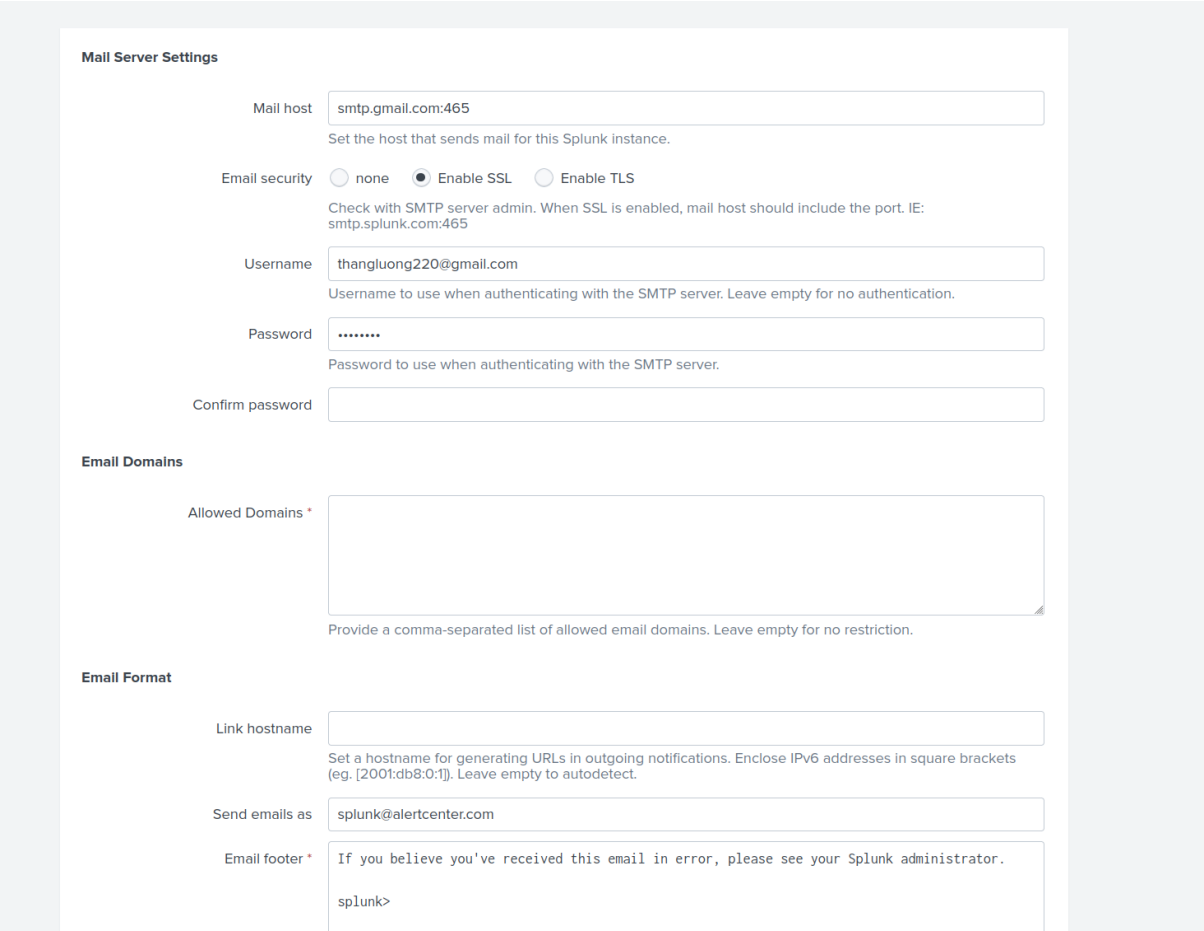


4. Tạo cảnh báo qua Gmail:

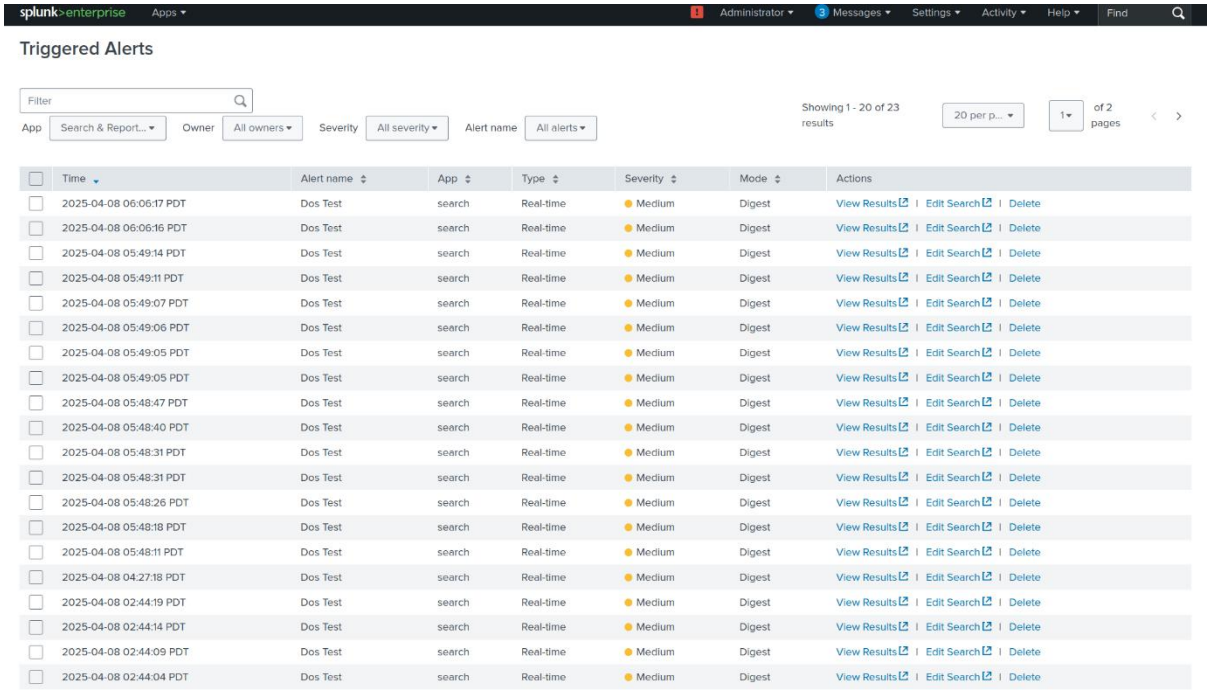
- Tạo App Password trên Gmail:
  - Đăng nhập vào tài khoản Google: Account Settings > Security > 2-Step Verification.
  - Tạo App Password:
    - Chọn App > Mail, Device > Other (Custom name), ví dụ: Splunk.
    - Sao chép App Password.


Mật khẩu ứng dụng
Mật khẩu ứng dụng giúp bạn đăng nhập vào Tài khoản Google của mình trên những ứng dụng và dịch vụ cũ không hỗ trợ các tiêu chuẩn bảo mật hiện đại.
Mật khẩu ứng dụng kém an toàn hơn so với việc sử dụng những ứng dụng và dịch vụ mới nhất hỗ trợ các tiêu chuẩn bảo mật hiện đại. Trước khi tạo mật khẩu ứng dụng, bạn nên kiểm tra xem ứng dụng của mình có cần mật khẩu này để đăng nhập hay không.
Tìm hiểu thêm
Mật khẩu ứng dụng của bạn
Splunk
Ngày tạo: 19:44
Để tạo mật khẩu mới dành riêng cho ứng dụng, hãy nhập tên của ứng dụng đó vào bên dưới...
Tên ứng dụng
Tạo

- Cài Mail server với App Pass được tạo ở trên :



- Truy cập Splunk Web: Settings > Server Settings > Email Settings.
- Cấu hình:
  - Mail Host: smtp.gmail.com:465.
  - Email Security: Chọn SSL.
  - Username: Địa chỉ email Gmail.
  - Password: App Password vừa tạo.
  - Send emails as: Địa chỉ email gửi cảnh báo.



5. Lấy Logs cho Web Server (Ubuntu):

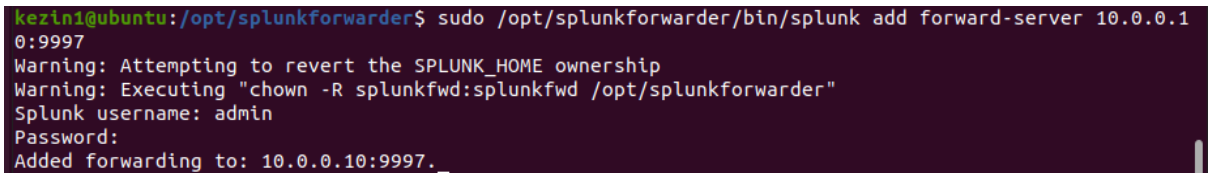
- Sử dụng lệnh dưới đây để lấy logs cho Web Server:

wget -O splunkforwarder.deb https://download.splunk.com/products/universalforwarder/releases/latest/linux/splunkforwarder-<VERSION>-Linux-x86_64.deb

sudo dpkg -i splunkforwarder.deb

#Chạy lệnh để chấp nhận điều khoản và bật Splunk sau khi cài đặt:
sudo /opt/splunkforwarder/bin/splunk start --accept-license

#Cấu hình Splunk Server nhận log
sudo /opt/splunkforwarder/bin/splunk add forward-server 10.0.0.10:9997



```
# Tạo thư mục inputs.conf
sudo mkdir -p /opt/splunkforwarder/etc/system/local/
# Tạo file cấu hình inputs.conf
sudo nano /opt/splunkforwarder/etc/apps/Splunk_TA_nix/local/inputs.conf
[default]
host = Agent1
##
## SPDX-FileCopyrightText: 2024 Splunk, Inc.
## SPDX-License-Identifier: LicenseRef-Splunk-8-2021
##
##

[script://./bin/vmstat_metric.sh]
sourcetype = vmstat_metric
source = vmstat
interval = 60
disabled = 1

[script://./bin/iostat_metric.sh]
sourcetype = iostat_metric
source = iostat
interval = 60
disabled = 1

[script://./bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 30
disabled = 1

[script://./bin/df_metric.sh]
sourcetype = df_metric
source = df
interval = 300
disabled = 1

[script://./bin/interfaces_metric.sh]
sourcetype = interfaces_metric
source = interfaces
interval = 60
```

```
disabled = 1

[script://./bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
interval = 30
disabled = 1

########################################################
############### Event Inputs ###################
########################################################

[script://./bin/vmstat.sh]
interval = 60
sourcetype = vmstat
source = vmstat
disabled = 1

[script://./bin/iostat.sh]
interval = 60
sourcetype = iostat
source = iostat
disabled = 1

[script://./bin/nfsiostat.sh]
interval = 60
sourcetype = nfsiostat
source = nfsiostat
disabled = 1

[script://./bin/ps.sh]
interval = 30
sourcetype = ps
source = ps
disabled = 1

[script://./bin/top.sh]
interval = 60
sourcetype = top
source = top
```

```
disabled = 1

[script://./bin/netstat.sh]
interval = 60
sourcetype = netstat
source = netstat
disabled = 1

[script://./bin/bandwidth.sh]
interval = 60
sourcetype = bandwidth
source = bandwidth
disabled = 1

[script://./bin/protocol.sh]
interval = 60
sourcetype = protocol
source = protocol
disabled = 1

[script://./bin/openPorts.sh]
interval = 300
sourcetype = openPorts
source = openPorts
disabled = 1

[script://./bin/time.sh]
interval = 21600
sourcetype = time
source = time
disabled = 1

[script://./bin/lsof.sh]
interval = 600
sourcetype = lsof
source = lsof
disabled = 1

[script://./bin/df.sh]
interval = 300
```

```
sourcetype = df
source = df
disabled = 1

# Shows current user sessions
[script://./bin/who.sh]
sourcetype = who
source = who
interval = 150
disabled = 1

# Lists users who could login (i.e., they are assigned a login shell)
[script://./bin/usersWithLoginPrivs.sh]
sourcetype = usersWithLoginPrivs
source = usersWithLoginPrivs
interval = 3600
disabled = 1

# Shows last login time for users who have ever logged in
[script://./bin/lastlog.sh]
sourcetype = lastlog
source = lastlog
interval = 300
disabled = 1

# Shows stats per link-level Etherner interface (simply, NIC)
[script://./bin/interfaces.sh]
sourcetype = interfaces
source = interfaces
interval = 60
disabled = 1

# Shows stats per CPU (useful for SMP machines)
[script://./bin/cpu.sh]
sourcetype = cpu
source = cpu
interval = 30
disabled = 1

# This script reads the auditd logs translated with ausearch
```

```
[script://./bin/rlog.sh]
sourcetype = auditd
source = auditd
interval = 60
disabled = 1

# Run package management tool collect installed packages
[script://./bin/package.sh]
sourcetype = package
source = package
interval = 3600
disabled = 1

[script://./bin/hardware.sh]
sourcetype = hardware
source = hardware
interval = 36000
disabled = 1

[monitor:///Library/Logs]
disabled = 1

[monitor:///var/log]
whitelist=(\.log|log$|messages|secure|auth|mesg$|cron$|acpid$|\.out)
blacklist=(lastlog|anaconda\.syslog)
disabled = 1

[monitor:///var/adm]
whitelist=(\.log$|messages)
disabled = 1

[monitor:///etc]
whitelist=(\.(conf|cfg|ini|init|cf|cnf|profile|rc|rules|tab|login)$|(config|shrc|tab|policy)$|
^ifcfg)
disabled = 1

### bash history
[monitor:///root/.bash_history]
disabled = true
sourcetype = bash_history
```

```
[monitor:///home/*/.bash_history]
disabled = true
sourcetype = bash_history



##### Added for ES support
# Note that because the UNIX app uses a single script to retrieve information
# from multiple OS flavors, and is intended to run on Universal Forwarders,
# it is not possible to differentiate between OS flavors by assigning
# different sourcetypes for each OS flavor (e.g. Linux:SSHDConfig), as was
# the practice in the older deployment-apps included with ES. Instead,
# sourcetypes are prefixed with the generic "Unix".

# May require Splunk forwarder to run as root on some platforms.
[script://./bin/openPortsEnhanced.sh]
disabled = true
interval = 3600
source = Unix:ListeningPorts
sourcetype = Unix:ListeningPorts

[script://./bin/passwd.sh]
disabled = true
interval = 3600
source = Unix:UserAccounts
sourcetype = Unix:UserAccounts

# Only applicable to Linux
[script://./bin/selinuxChecker.sh]
disabled = true
interval = 3600
source = Linux:SELinuxConfig
sourcetype = Linux:SELinuxConfig

# Currently only supports SunOS, Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://./bin/service.sh]
disabled = true
interval = 3600
```

```
source = Unix:Service
sourcetype = Unix:Service

# Currently only supports SunOS, Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://./bin/sshdChecker.sh]
disabled = true
interval = 3600
source = Unix:SSHDConfig
sourcetype = Unix:SSHDConfig

# Currently only supports Linux, OSX.
# May require Splunk forwarder to run as root on some platforms.
[script://./bin/update.sh]
disabled = true
interval = 86400
source = Unix:Update
sourcetype = Unix:Update

[script://./bin/uptime.sh]
disabled = true
interval = 86400
source = Unix:Uptime
sourcetype = Unix:Uptime

[script://./bin/version.sh]
disabled = true
interval = 86400
source = Unix:Version
sourcetype = Unix:Version

# This script may need to be modified to point to the VSFTPD configuration file.
[script://./bin/vsftpdChecker.sh]
disabled = true
interval = 86400
source = Unix:VSFTPDConfig
sourcetype = Unix:VSFTPDConfig
```

6. Cài plugin trên Windows Server:

- Cài Splunk Add-on for Microsoft Windows cho splunk và cả máy Domain Controller: giải nén vào C:\Program Files\SplunkUniversalForwarder\etc\apps\ . Sau đó chỉnh file inputs.conf trên Windows Universal Forwarder.

```
# Đường dẫn:
C:\Program
Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\inputs.conf
# Thêm cấu hình sau để lấy dữ liệu CPU, RAM, Disk:
[perfmon://CPU]
object = Processor
counters = % Processor Time
instances = _Total
interval = 10
index = windows
disabled = 0

[perfmon://Memory]
object = Memory
counters = Available MBytes
interval = 10
index = windows
disabled = 0

[perfmon://Disk]
object = LogicalDisk
counters = % Free Space, Disk Read Bytes/sec, Disk Write Bytes/sec
instances = C:
interval = 10
index = windows
disabled = 0
```

❖ **Lưu ý:**

- Nếu chưa có thư mục local/, hãy tạo nó trước.
- Sau đó, khởi động lại Splunk Universal Forwarder trên Windows Server: C:\Program Files\SplunkUniversalForwarder\bin\splunk restart
- Dashboard → Microsoft Windows Monitoring Dashboard để xem dashboard

Chương IV. KẾT LUẬN.

1. Tổng quát:

Trong đồ án môn học "Triển khai và giám sát hệ thống mạng với Splunk", nhóm đã thành công trong việc thiết kế và triển khai một hệ thống giám sát mạng tích hợp Splunk để thu thập, phân tích log và phát hiện các sự kiện bất thường nhằm nâng cao bảo mật và hiệu suất hệ thống. Các công việc chính bao gồm:

- Thiết kế kiến trúc hệ thống: Xây dựng mô hình mạng gồm ba vùng chính (WAN, DMZ, LAN) với các thành phần như Firewall SOPHOS, Web Server, Domain Controller, Client PC, và Splunk Server. Mô hình này đảm bảo cô lập các dịch vụ công khai và bảo vệ mạng nội bộ.
- Triển khai thu thập log:
  - Từ Firewall SOPHOS: Cấu hình Syslog để gửi log về Splunk qua port 514, tích hợp Splunk Add-on for Sophos Next-Gen Firewall để phân tích dữ liệu hiệu quả.
  - Từ Domain Controller: Cài đặt Splunk Universal Forwarder trên Windows Server, thu thập Windows Event Logs (Security, System, Application) và thiết lập rule alert để phát hiện tài khoản người dùng bị xóa.
  - Từ Web Server: Sử dụng HTTP Event Collector (HEC) và Splunk log driver trong Docker để thu thập log HTTP, đồng thời triển khai Splunk Add-on for Unix and Linux để giám sát hiệu suất hệ thống.
  - Cấu hình cảnh báo: Thiết lập cảnh báo qua email (sử dụng SMTP Gmail) để thông báo cho quản trị viên khi phát hiện các sự kiện bất thường, như xóa tài khoản người dùng hoặc truy cập trái phép.
  - Tạo dashboard: Xây dựng dashboard giám sát để trực quan hóa dữ liệu từ các nguồn, hỗ trợ quản trị viên theo dõi và phân tích hoạt động mạng.

❖ Hệ thống đã được kiểm tra và hoạt động ổn định, cho phép phát hiện các sự kiện bất thường, giám sát hiệu suất mạng, và cung cấp thông tin chi tiết để xử lý sự cố nhanh chóng.

2. Kết quả và hạn chế:

2.1 Kết quả:

- Hệ thống giám sát mạng với Splunk được triển khai thành công, đáp ứng các yêu cầu về thu thập, phân tích log và phát hiện sự kiện bất thường.
- Nâng cao bảo mật: Việc tích hợp Splunk với Firewall SOPHOS, Domain Controller, và Web Server giúp phát hiện các mối đe dọa như truy cập trái phép, tấn công DDoS, hoặc lỗi hệ thống, từ đó tăng cường khả năng bảo vệ mạng.

2.2 Hạn chế:

Đồ án vẫn tồn tại một số hạn chế:

- Hiệu suất hệ thống: Splunk Server có thể gặp tình trạng quá tải khi thu thập và phân tích khối lượng log lớn, đặc biệt trong môi trường mạng có lưu lượng cao.

- Bảo mật chưa tối ưu: Việc sử dụng tùy chọn insecure=true trong HEC và không bật mã hóa SSL cho Syslog có thể gây rủi ro bảo mật trong môi trường thực tế.
- Thiếu tài liệu chi tiết: Một số bước cấu hình, như chỉnh sửa file inputs.conf hoặc xử lý lỗi, chưa được mô tả đầy đủ, gây khó khăn khi triển khai lại hệ thống.
- Hạn chế về dashboard: Dashboard hiện tại chỉ hiển thị các thông tin cơ bản, chưa khai thác hết khả năng trực quan hóa của Splunk để hỗ trợ phân tích sâu hơn.

3. Hướng phát triển trong tương lai:

Để cải thiện và mở rộng hệ thống:

- Tối ưu hóa hiệu suất Splunk: Triển khai Splunk trong môi trường phân tán (Distributed Deployment) với Search Head, Indexer, và Forwarder riêng biệt để xử lý khối lượng log lớn hơn.
- Tăng cường bảo mật:
  - Bật SSL/TLS cho HEC và Syslog để mã hóa dữ liệu truyền tải.
  - Cấu hình role-based access control trong Splunk để hạn chế quyền truy cập.
  - Sử dụng chứng chỉ số hợp lệ thay vì tùy chọn insecure=true.

Mở rộng khả năng giám sát:

- Tích hợp thêm các nguồn log, như log từ thiết bị IoT hoặc ứng dụng…..
- Phát triển các dashboard nâng cao để hiển thị các chỉ số như thời gian phản hồi của Web Server, tỷ lệ tấn công bị chặn bởi SOPHOS, hoặc hoạt động người dùng trên Domain Controller.
- Tự động hóa phản hồi: Thiết lập các hành động tự động (như chặn IP độc hại trên SOPHOS) khi Splunk phát hiện sự kiện bất thường, thay vì chỉ gửi cảnh báo qua email.

4. Kết luận:

Đồ án “Triển khai và giám sát hệ thống mạng với Splunk” đã cung cấp một giải pháp giám sát hiệu quả và có tính ứng dụng cao. Mặc dù còn một số hạn chế, nhưng những kinh nghiệm và bài học rút ra từ quá trình thực hiện là nền tảng quý giá để nhóm tiếp tục phát triển kỹ năng trong lĩnh vực an ninh mạng và quản trị hệ thống. Hệ thống này không chỉ đáp ứng yêu cầu học thuật mà còn có tiềm năng áp dụng thực tế trong các doanh nghiệp, góp phần nâng cao khả năng bảo vệ và tối ưu hóa hệ thống mạng.

LINK DEMO: Danh Gia hieu nang

LINK SLIDE: https://www.canva.com/design/DAGjdlP4NJc/3dnMAuGPKyj8wSHn-RsJXg/edit?utm_content=DAGjdlP4NJc&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

NGUỒN THAM KHẢO

1. Sophos. (n.d.). *How to configure Syslog in Sophos Firewall to send logs to Splunk* [Video]. YouTube. Truy cập từ https://www.youtube.com/watch?v=dvy7F7I2Kiw
2. Splunk. (n.d.). *How to configure Splunk Universal Forwarder for Windows Event Logs* [Video]. YouTube. Truy cập từ https://www.youtube.com/watch?v=oTeCOe4LQNY
3. Outcold Solutions. (n.d.). *Monitoring Docker with Splunk: Installation guide*. Truy cập từ https://www.outcoldsolutions.com/docs/monitoring-docker/v5/installation/
4. Sophos Community. (n.d.). *Splunk Add-on for Sophos Next-Gen Firewall*. Truy cập từ https://community.sophos.com/sophos-integrations/w/integrations/106/splunk-add-on-for-sophos-next-gen-firewall
5. Splunk. (n.d.). Splunk Add-on for Unix and Linux. Truy cập từ https://splunk.github.io/splunk-add-on-for-unix-and-linux/