**MỤC LỤC**

[1. Tìm hiểu các loại Logs của Windows và Linux 2](#_Toc192005353)

[1.1. Windows Event Logs 2](#_Toc192005354)

[1.1.1. Vị trí 2](#_Toc192005355)

[1.1.2. Định dạng Log 3](#_Toc192005356)

[1.1.3. Phân loại Events 4](#_Toc192005357)

[1.1.4. Các loại Logs 5](#_Toc192005358)

[1.2. Linux Logs 7](#_Toc192005359)

[1.2.1. Sơ Lược 7](#_Toc192005360)

[1.2.2. Các file log quan trọng 7](#_Toc192005361)

[1.3. Kết luận 9](#_Toc192005362)

[2. Cài đặt và triển khai ELK Stack 9](#_Toc192005363)

[2.1. Cài đặt và cấu hình ELK trên Server 9](#_Toc192005364)

[2.1.1. Cài đặt thông qua CLI 9](#_Toc192005365)

[2.1.2. Kết nối Kibana và Elastic Search 11](#_Toc192005366)

[2.1.3. Cấu hình Logstash 13](#_Toc192005367)

[2.2. Cài đặt và cấu hình Filebeat trên Client 13](#_Toc192005368)

[2.3. Sử dụng ELK với giao diện Kibana 15](#_Toc192005369)

[DANH MỤC TÀI LIỆU THAM KHẢO 18](#_Toc192005370)

**ELASTICSEARCH SIEM: TRIỂN KHAI**

# 1. Tìm hiểu các loại Logs của Windows và Linux

## 1.1. Windows Event Logs

Trong điều tra số, một trong những vị trí đem đến những thông tin vô cùng hữu ích cho người điều tra là Windows Event Logs.

Windows Event Logs gồm những sự kiện liên quan đến software, hardware, OS, security. Service Windows Event Log chịu trách nhiệm quản lý các sự kiện, nhật ký sự kiện; nó thu thập các sự kiện từ nhiều nguồn khác nhau và lưu trự tập chung tại một thư mục.

Các sự kiện này có thể giúp người điều tra biết được chuyện gì đã xảy ra trên hệ thống, chúng xảy ra vào thời gian nào, tham chiếu đến người dùng cụ thể liên quan đến những hành vi đó hay các thông tin của các hệ thống, tài nguyên truy cập từ xa.

### 1.1.1. Vị trí

Ban đầu, ở những phiên bản hệ điều hành cũ (trước Windows Vista) event log sẽ được lưu trữ tập chung tại ***systemroot%\System32\config*** ở định dạng nhị phân và với phần mở rộng đuôi ***.evt***.

Nhưng bắt đầu từ Windows Server 2008 và Windows Vista thì đã có sự thay đổi về định dạng log và vị trí lưu trữ của chúng. Event log được chuyển sang định dạng XML và với phần mở rộng ***.evtx*** và chúng được lưu trữ tại  ***%systemroot%\System32\winevt\logs***.

A screenshot of a computer

AI-generated content may be incorrect.

Vị trí lưu của từng loại log có thể tìm thấy trong Registry:

A screenshot of a computer

AI-generated content may be incorrect.

Chẳng hạn như trong hình trên với các event liên quan đến Application sẽ được lưu trữ trong ***%systemroot%\System32\winevt\Logs\Application.evtx***

Và người quản trị có thể thay đổi được vị trí này bằng cách thay đổi data value của registry key.

### 1.1.2. Định dạng Log

Với Windows 2008 trở về trước toàn bộ tệp log sẽ được ánh xạ vào bộ nhớ và điều này thực sự là một vấn đề với việc quản lý bộ nhớ, bộ nhớ luôn phải dành một không gian tối đa tới 300MB để cấp phát chỉ cho Event Log và tất nhiên hiệu suất sẽ bị giảm nhất là đối với thời điểm đó khi mà dung lượng bộ nhớ thực sự không lớn. Và đôi khi có thể dẫn đến vấn đề là người dùng sẽ tắt logging đi để nâng cao hiệu suất.

Nhưng với các bản indows OS mới hơn thì điều này đã được khắc phục, service Windows Event Log quản lý các event và event logs (logging events, querying events, subscribing to events, archiving event logs, and managing event metadata). Trong bộ nhớ lúc này chỉ chứa hững header nhỏ với các đoạn mã 64KB nằm trong bộ nhớ và nó thực sự đã giải quyết được vấn đề quản lý bộ nhớ mà không làm giảm hiệu suất.

A screenshot of a computer

AI-generated content may be incorrect.

Định dạng của event log cũng thay đổi với extension là .EVTX và được lưu trữ ở định dạng XML, giúp việc giải mã cấu trúc nhật ký trở nên trực quan hơn và cũng dễ dàng để tạo bộ lọc hỗ trợ việc tìm kiếm. Ví dụ với 1 event dưới đây:

A screenshot of a computer program

AI-generated content may be incorrect.

Số lượng log đã tăng lên rất nhiều và cũng có các tùy chọn ghi log chi tiết hơn với sự tùy chỉnh của Advanced Audit Policy Configuration.

### 1.1.3. Phân loại Events

Có năm loại sự kiện có thể được ghi lại. Mỗi sự kiện phải thuộc một loại nào đó trong 5 loại này và mỗi loại sẽ có một t biểu tượng khác nhau. VD như hình dưới:

A number of numbers on a white background

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

#### a. Information (Thông tin):

- Ghi lại các hoạt động bình thường, các thông báo hệ thống và ứng dụng.

- Ví dụ: Khởi động thành công của một dịch vụ, thông báo hoàn thành tác vụ, báo cáo trạng thái hệ thống…

- Mức độ thấp, chủ yếu để theo dõi hoạt động thông thường.

#### b. Warning (Cảnh báo):

- Đánh dấu các sự kiện không mong đợi nhưng không gây lỗi nghiêm trọng.

- Ví dụ: Một ứng dụng có thể gặp vấn đề về hiệu suất, một dịch vụ chậm khởi động, hoặc một cảnh báo về tài nguyên hệ thống sắp cạn kiệt.

- Cho phép team SOC cảnh báo và theo dõi để phòng tránh các vấn đề có thể trở nên nghiêm trọng.

#### c. Error (Lỗi):

- Ghi lại các sự kiện báo lỗi, chỉ ra sự cố đã xảy ra ảnh hưởng đến chức năng hoặc hiệu suất của hệ thống, ứng dụng.

- Ví dụ: Dịch vụ không khởi động được, lỗi khi kết nối cơ sở dữ liệu, lỗi ứng dụng…

- Đây là loại sự kiện mà team SOC cần phản ứng nhanh để khắc phục sự cố.

#### d. Critical (Nghiêm trọng):

- Một số phiên bản Windows (và các ứng dụng) có thể phân loại sự kiện với mức độ Critical để chỉ ra những lỗi cực kỳ nghiêm trọng, thường liên quan đến sự cố hệ thống không mong đợi hoặc sự cố bảo mật nghiêm trọng.

- Những sự kiện này đòi hỏi sự can thiệp khẩn cấp.

#### e. Audit Success và Audit Failure (Sự kiện bảo mật thành công/thất bại):

**- Audit Success:** Ghi lại các hoạt động bảo mật đã thành công, như đăng nhập, truy cập tài nguyên, thay đổi quyền…

- **Audit Failure:** Ghi lại các hoạt động bảo mật không thành công, ví dụ như đăng nhập thất bại, truy cập bị từ chối, hành vi đáng ngờ của người dùng…

- Các sự kiện này rất quan trọng trong việc theo dõi và điều tra các hoạt động bảo mật, giúp SOC phát hiện sớm các hành vi truy cập trái phép hoặc tấn công.

### 1.1.4. Các loại Logs

Event log gồm các nhật ký tiêu chuẩn (Security, System và Application) ngoài ra còn có các bản additional logs đã được thêm vào log chuyên biệt (Custom log) chẳng hạn như PowerShell, Task Scheduler,…

#### a. Application Log (Log Ứng Dụng)

**- Mô tả:** Ghi lại các sự kiện liên quan đến các ứng dụng chạy trên Windows.

- **Nội dung:** Lỗi, cảnh báo, thông tin từ các ứng dụng; ví dụ như lỗi phần mềm, thông báo từ trình duyệt, và các ứng dụng bên thứ ba.

- **Ứng dụng SOC:** Giúp phát hiện các lỗi hoặc hành vi bất thường từ các ứng dụng có thể là dấu hiệu của tấn công hoặc phần mềm độc hại.

#### b. System Log (Log Hệ Thống)

**- Mô tả:** Ghi lại các sự kiện của hệ thống Windows, liên quan đến hoạt động của hệ điều hành và các thành phần phần cứng.

- **Nội dung:** Thông báo từ driver, dịch vụ hệ thống, các sự kiện liên quan đến khởi động, tắt máy, cảnh báo lỗi phần cứng…

- **Ứng dụng SOC:** Giúp theo dõi tình trạng hoạt động của hệ thống, từ đó phát hiện sớm các dấu hiệu của tấn công hệ thống hoặc sự cố hệ thống.

#### c. Security Log (Log Bảo Mật)

**- Mô tả:** Ghi lại các sự kiện liên quan đến an ninh, đặc biệt là các hoạt động liên quan đến đăng nhập, truy cập, thay đổi chính sách bảo mật…

**- Nội dung:** Sự kiện đăng nhập thành công hoặc thất bại, thay đổi chính sách, audit các hành động của người dùng, hành vi truy cập không hợp lệ, sử dụng tài khoản đặc quyền.

**- Ứng dụng SOC:** Là nguồn quan trọng giúp phát hiện các hành vi đáng ngờ, tấn công brute-force, truy cập trái phép, và các cuộc tấn công từ bên ngoài.

#### d. Setup Log (Log Cài Đặt)

**- Mô tả:** Ghi lại các sự kiện trong quá trình cài đặt hệ điều hành và các bản cập nhật quan trọng.

**- Ứng dụng SOC:** Có thể cung cấp thông tin về thay đổi cấu hình, cài đặt phần mềm mới và các sự kiện liên quan đến bảo mật hệ thống.

#### e. Forwarded Events (Sự Kiện Chuyển Tiếp)

**- Mô tả:** Đây là log các sự kiện được chuyển tiếp từ các máy chủ hoặc máy tính khác trong mạng. Windows Audit Collection Service chịu trách nhiệm thu thập và chuyển tiếp log.

- **Ứng dụng SOC:** Giúp tập trung theo dõi các sự kiện bảo mật từ nhiều nguồn trong mạng nội bộ, tạo ra một tổng hợp các sự kiện để phân tích.

## 1.2. Linux Logs

### 1.2.1. Sơ Lược

Linux File log là một tập hợp các bản ghi mà Linux duy trì để các quản trị viên theo dõi các sự kiện quan trọng. Các file log này sẽ chứa các thông báo về máy chủ, bao gồm kernel, dịch vụ và ứng dụng đang chạy trên nó. File log cung cấp thời gian của các sự kiện cho hệ điều hành, ứng dụng và hệ thống Linux và là một công cụ quan trọng giúp chúng ta khắc phục sự cố.

Hệ điều hành Linux cung cấp một kho lưu trữ tập trung các file log trong thư mục /var/log. Hầu hết các file log được chia thành một trong bốn loại:

- Application Logs: Nhật ký ứng dụng

- Event Logs: Nhật ký sự kiện

- Service Logs: Nhật ký dịch vụ

- System Logs: Nhật ký hệ thống

Thông qua việc giám sát các file log chúng ta có thể nắm rõ hơn về hiệu suất của máy chủ, bảo mật, thông báo lỗi và các vấn đề tiềm ẩn. Các file log cho phép chúng ta dự đoán các vấn đề sắp tới trước khi thực sự xảy ra.

### 1.2.2. Các file log quan trọng

#### a. Syslog/Messages

**- Đường dẫn:**

**+ Ubuntu/Debian:** /var/log/syslog

**+ RedHat/CentOS:** /var/log/messages

**- Mô tả:** Ghi lại các sự kiện chung của hệ thống, từ các daemon chạy nền đến các thông báo từ kernel.

- **Ứng dụng SOC:** Là nguồn cung cấp các thông tin tổng hợp về hoạt động hệ thống, cho phép phát hiện lỗi, cảnh báo và hành vi bất thường.

#### b. Kernel Log

**- Đường dẫn:**

+ /var/log/kern.log (Ubuntu)

+ Dmesg (thông qua lệnh dmesg)

**- Mô tả:** Ghi lại các thông báo từ kernel, bao gồm lỗi phần cứng, driver, và các sự kiện khởi động.

- **Ứng dụng SOC:** Giúp theo dõi các vấn đề liên quan đến phần cứng hoặc driver, cũng như dấu hiệu của tấn công ở tầng thấp của hệ thống.

#### c. Authentication Log

**- Đường dẫn:**

**+ Ubuntu/Debian:** /var/log/auth.log

**+ RedHat/CentOS:** /var/log/secure

**- Mô tả:** Ghi lại các sự kiện liên quan đến xác thực như đăng nhập, sudo, và các hành động liên quan đến bảo mật.

- **Ứng dụng SOC:** Rất quan trọng để phát hiện các hành vi đăng nhập không hợp lệ, tấn công brute-force, hoặc các hành vi truy cập trái phép.

#### d. Daemon Log

**- Đường dẫn:** /var/log/daemon.log (Ubuntu)

- **Mô tả:** Ghi lại các sự kiện từ các daemon chạy nền (ví dụ: cron, sshd, và các dịch vụ khác).

- **Ứng dụng SOC:** Theo dõi hoạt động của các dịch vụ hệ thống, từ đó phát hiện các vấn đề hoặc hành vi bất thường.

#### e. Mail Log

**- Đường dẫn:** /var/log/mail.log hoặc /var/log/maillog

- **Mô tả:** Ghi lại các hoạt động liên quan đến hệ thống email, như gửi, nhận thư và các lỗi liên quan.

- **Ứng dụng SOC:** Phân tích lưu lượng email, xác định các hành vi spam hoặc tấn công qua email.

#### f. Audit Log

**- Đường dẫn:** /var/log/audit/audit.log (nếu sử dụng auditd)

- **Mô tả:** Ghi lại các hành động được audit, bao gồm các sự kiện truy cập, thay đổi cấu hình và các hành động quan trọng của hệ thống.

- **Ứng dụng SOC:** Rất quan trọng trong việc kiểm tra, điều tra các hành động của người dùng và phát hiện vi phạm chính sách.

#### g. Application Logs (Các log ứng dụng riêng)

**- Đường dẫn:**

+ **Apache/Nginx:** /var/log/apache2/access.log, /var/log/apache2/error.log, /var/log/nginx/access.log, /var/log/nginx/error.log

+ **MySQL:** /var/log/mysql.log hoặc /var/log/mysql/error.log

+ Các ứng dụng khác: Có thể được cấu hình ghi log vào các đường dẫn tùy chỉnh.

**- Mô tả:** Các log từ ứng dụng cung cấp thông tin chi tiết về hoạt động và lỗi của từng ứng dụng.

- **Ứng dụng SOC:** Giúp phát hiện lỗi ứng dụng, các cuộc tấn công nhắm vào ứng dụng và phân tích hiệu năng.

## 1.3. Kết luận

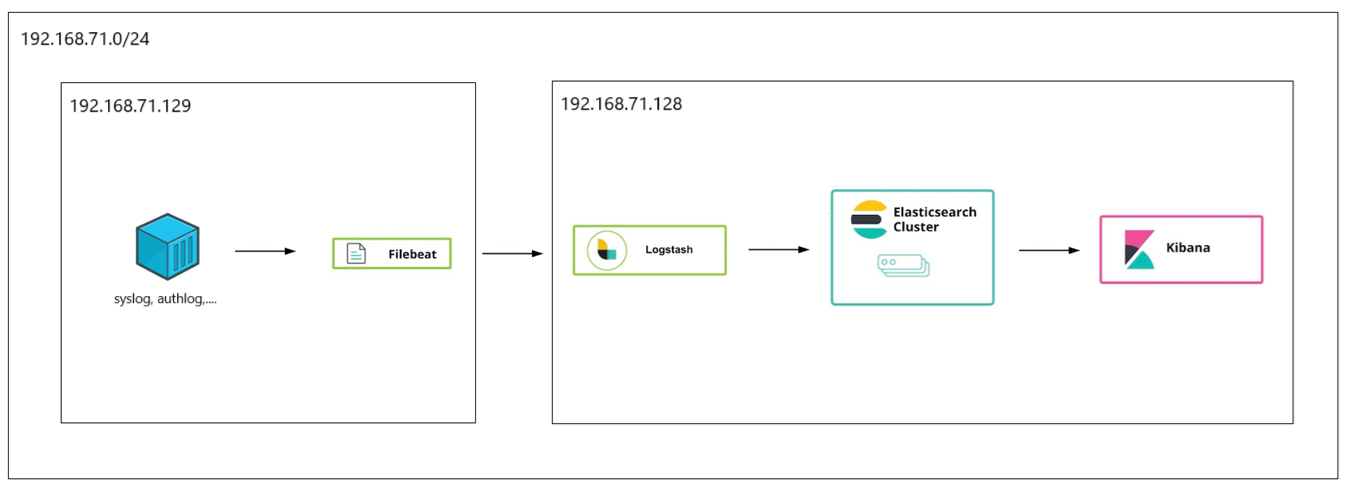
**Windows Logs:** Bao gồm Application, System, Security, Setup và Forwarded Events. Mỗi loại log có vai trò quan trọng trong việc theo dõi các sự kiện ứng dụng, hệ thống và bảo mật.

**Linux Logs:** Bao gồm Syslog/Messages, Kernel log, Authentication log, Daemon log, Mail log, Audit log và các log ứng dụng riêng. Các log này cung cấp thông tin từ hệ thống, kernel, xác thực, và các dịch vụ chạy nền.

**Ứng dụng SOC:** Việc thu thập các log này giúp SOC theo dõi toàn diện hoạt động của hệ thống, phát hiện sớm các hành vi bất thường và tấn công, đồng thời hỗ trợ việc điều tra và phản ứng sự cố.

# 2. Cài đặt và triển khai ELK Stack

Mô hình triển khai:



Trong task này, nhóm sẽ triển khai ELK Stack trên 2 máy ảo Ubuntu 22.04, gồm máy ảo Server là 192.168.71.128 và máy ảo Client đẩy log về Server là 192.168.71.129.

## 2.1. Cài đặt và cấu hình ELK trên Server

### 2.1.1. Cài đặt thông qua CLI

Ta tạo 1 file bash chạy các lệnh cần thiết để cài đặt ELK như sau:

|  |
| --- |
| **#!/bin/bash**  **# Cài đặt Java Development Kit (JDK)**  apt update  apt install -y default-jdk  **# Cài đặt Elasticsearch**  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -  echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-8.x.list  apt update  apt install -y elasticsearch  **# Cấu hình Elasticsearch**  echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml  **# Khởi động Elasticsearch**  systemctl enable elasticsearch  systemctl start elasticsearch  **# Cài đặt Logstash**  echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-8.x.list  apt update  apt install -y logstash  **# Cài đặt Kibana**  echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-8.x.list  apt update  apt install -y kibana  **# Cấu hình Kibana để cho phép truy cập từ tất cả các nguồn**  echo "server.host: 0.0.0.0" >> /etc/kibana/kibana.yml  **# Khởi động Kibana**  systemctl enable kibana  systemctl start kibana  **# Reset mật khẩu elastic search và tạo token cho kibana**  elastic\_password=$(echo "y" | /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic | grep -o "New value: .\*" | cut -d ' ' -f 3-)  kibana\_token=$(/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana)  **# Di chuyển và mở verification code**  cd /usr/share/kibana && verification\_code=$(bin/kibana-verification-code)  **# Hiển thị thông tin đăng nhập**  echo "Thông tin đăng nhập:"  echo "-------------------"  echo "Elasticsearch:"  echo " Tài khoản: elastic"  echo " Mật khẩu: $elastic\_password"  echo ""  echo "Kibana:"  echo " Token: $kibana\_token"  echo ""  echo "Mã xác minh Kibana:"  echo "$verification\_code" |

Kết quả quá trình cài đặt:

A screenshot of a computer

AI-generated content may be incorrect.

Trong hình trên, lỗi không in ra được mã xác minh, do đó ta cần chạy lệnh: sudo systemctl status kibana để lấy mã xác minh của Kibana sau khi cài đặt xong.

|  |
| --- |
| Thg 3 02 14:44:32 ubuntu kibana[10478]: Your verification code is: 789 119 |

### 2.1.2. Kết nối Kibana và Elastic Search

Tiến hành truy cập: [**http://192.168.71.128:9200**](http://192.168.71.128:9200)để xem trạng thái của elasticsearch, nhập tài khoản mật khẩu elasticsearch ở trên:

A screenshot of a computer

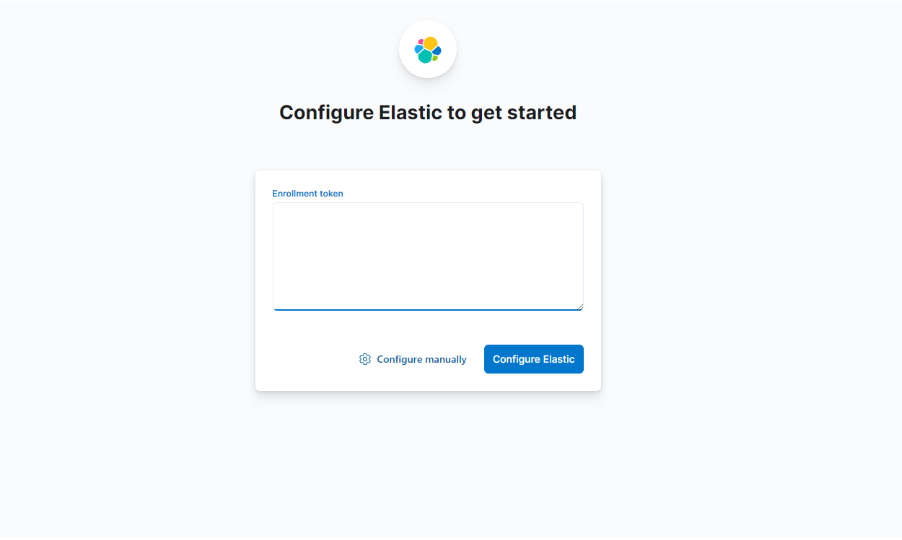
AI-generated content may be incorrect.

Và được kết quả thành công cấu hình và cài đặt elastic search

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp tục truy cập **http://192.168.71.128:5601** cấu hình kibana, nhập token ở trên vào:



Tiếp tục nhập mã xác nhận ở trên vào:

A screenshot of a computer

AI-generated content may be incorrect.

Sau khi ta nhập mã xác nhận, đợi một chút cho kibana khởi động. Vậy là chúng ta đã cài đặt thành công Kibana kết nối bảo mật với Elastic Search.

### 2.1.3. Cấu hình Logstash

Tiếp theo chúng ta sẽ cấu hình logstash để nhận log từ Webserver như đã nói ở trên. Trong logstash chúng ta có 3 khối chính input, filter, output (tuy nhiên ở đây nhóm chỉ sử dụng 2 khối input và output cho dễ hiểu) filter có thể hiểu là giúp chúng ta lọc dữ liệu thô.

|  |
| --- |
| **wanthinnn@ubuntu:~$** sudo nano /etc/logstash/conf.d/sys-logs.conf  input {  beats {  port => 5044  }  }  output {  elasticsearch {  index => "system\_logs"  hosts => ["192.168.71.128:9200"]  user => "elastic"  password => "p6mZPYjvHPnzUDds4MCf"  ssl => true  ssl\_certificate\_verification => false  }  # Thêm output debug  stdout { codec => rubydebug }  } |

Ta sử dụng lệnh sudo ufw allow 5044/tcp mở port để cho logstash sử dụng (và mở các port tương ứng cho elastic, kibana, ssh,..).

Sau đó ta dừng và khởi động lại logstash: sudo systemctl stop logstash && sudo systemctl start logstash

## 2.2. Cài đặt và cấu hình Filebeat trên Client

Tạo file bash script cài đặt filebeat có nội dung sau:

|  |
| --- |
| **#!/bin/bash**  **# Cập nhật hệ thống**  sudo apt update  **# Cài đặt các gói cần thiết**  sudo apt install -y apt-transport-https wget  **# Tải xuống và cài đặt GPG key của Elastic**  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -  **# Thêm kho lưu trữ Elastic vào danh sách nguồn**  echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list  **# Cập nhật hệ thống để áp dụng thay đổi mới**  sudo apt update  **# Cài đặt Filebeat**  sudo apt install -y filebeat  **# Sao chép file cấu hình mẫu**  sudo cp /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml.bak  **# Bật dịch vụ Filebeat**  sudo systemctl enable filebeat  sudo systemctl start filebeat |

Được kết quả cài đặt thành công:

A screenshot of a computer program

AI-generated content may be incorrect.

Ta tạo file cấu hình filebeat mới với nội dung sau:

|  |
| --- |
| **wanthinnn@ubuntu-2**:~/elk$ sudo nano /etc/filebeat/filebeat.yml  filebeat.inputs:  - type: filestream  enabled: true  paths:  #- /var/log/\*.log  #- /var/log/encrypted\_syslog.log  #- /var/log/encrypted\_auth.log  - /var/log/auth.log  output.logstash:  hosts: ["192.168.71.128:5044"] |

Chạy lệnh sudo filebeat test output để kiểm tra kết nối:

A screen shot of a computer

AI-generated content may be incorrect.

Khởi động lại Filebeat:  sudo systemctl stop filebeat && sudo systemctl start filebeat

## 2.3. Sử dụng ELK với giao diện Kibana

Chọn **Stack Management**

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp theo chúng ta sẽ tạo data view để xem dữ liệu từ index đó, chọn **Discover** **->** C**reate data view**

A screenshot of a computer

AI-generated content may be incorrect.

Nhập những thông tin dưới đây:

A screenshot of a computer

AI-generated content may be incorrect.

Tạo data view thành công và chọn **View all matches**. Cuối cùng, ta xem dữ liệu của auth logs:

A screenshot of a computer

AI-generated content may be incorrect.

# DANH MỤC TÀI LIỆU THAM KHẢO

[1] SOC\_Team *,“****[Windows Forensic] [Part1] Windows Event Logs****”*, T4fi, RE Team.

<https://sec.vnpt.vn/2022/03/windows-event-logs-1/> [Truy cập ngày 03/3/2025].

[2] SOC\_Team *,“****[Windows Forensic] [Part2] Windows Event Logs****”*, T4fi, RE Team.

<https://sec.vnpt.vn/2023/01/windows-forensicpart2-windows-event-logs/> [Truy cập ngày 03/3/2025].

[3] Đang Nguyễn *,“****Các file log quan trọng trên Linux****”*, Blogd.Net.

<https://blogd.net/linux/cac-file-log-quan-trong-tren-linux/> [Truy cập ngày 03/3/2025].

[4] Lê Văn Phú *,“* ***Tìm hiểu cơ bản về các loại log trên Linux - Unix****”*, levanphu.info.

<https://levanphu.info/tim-hieu-co-ban-ve-cac-loai-log-tren-linux-unix> [Truy cập ngày 03/3/2025].

[5] Elroydevops*,“****Cách sử dụng ELK Stack****”*, Elroydevops.Tech.

<https://elroydevops.tech/cach-su-dung-elk-stack/> [Truy cập ngày 02/3/2025].