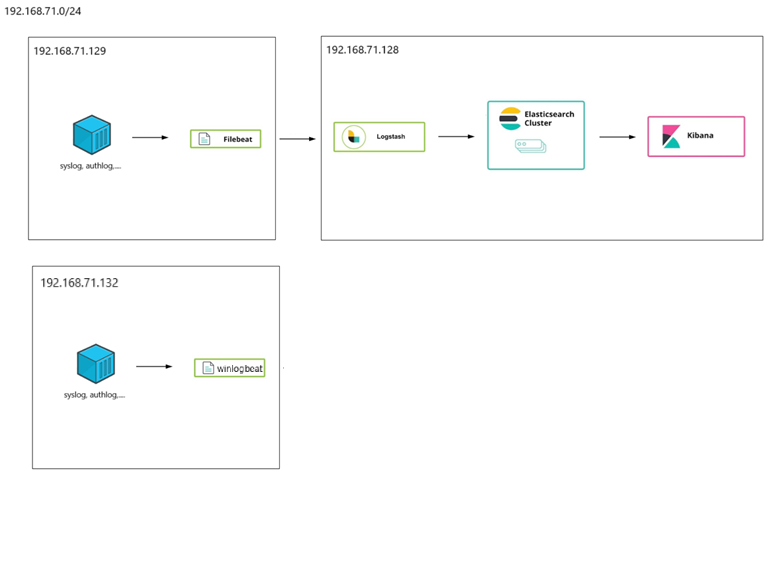
**ĐẨY LOGS VÀ PHÂN TÍCH LOGS**



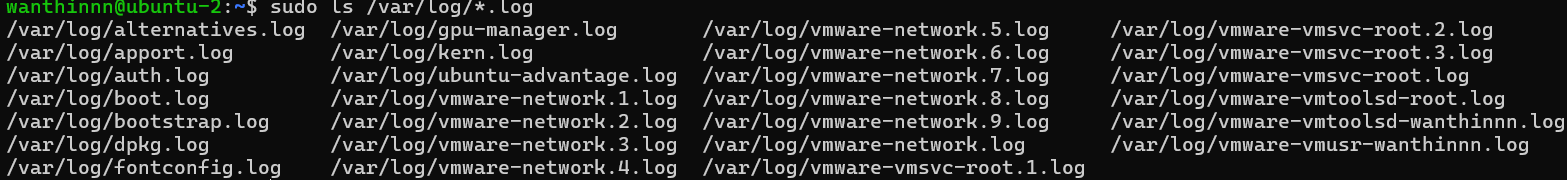
Windows logs

**Hình 1. Mô hình triển khai**

# 1. Đẩy các Logs về ELK

## 1.1. Cấu hình Phía Filebeat Linux

**-** Xác định 1 số log có trên máy 192.168.71.129:

****

**-** Bước 1: Cấu hình file .yml trong Filebeat:

|  |
| --- |
| **wanthinnn@ubuntu-2:~$** sudo cat /etc/filebeat/filebeat.yml  [sudo] password for wanthinnn:  # Cấu hình các input để Filebeat đọc log files từ hệ thống  filebeat.inputs:  - type: log  enabled: true  # Các file log cần thu thập (điều chỉnh theo nhu cầu: ví dụ /var/log/\*.log hoặc đường dẫn khác)  paths:  - /var/log/\*.log  # Các thiết lập chung cho Filebeat  filebeat.config.modules:  path: ${path.config}/modules.d/\*.yml  reload.enabled: false  # Định dạng output cho Filebeat  # 1. Nếu bạn muốn đẩy trực tiếp tới Elasticsearch (ví dụ: dùng Elasticsearch tích hợp sẵn trong ELK)  #output.elasticsearch:  # Thay đổi host và port cho phù hợp, thường Elasticsearch lắng nghe trên 9200  # hosts: ["192.168.71.128:9200"]  # Nếu cần xác thực, bạn có thể thêm các thông số dưới đây  # username: "elastic"  # password: "your\_password"  # 2. Nếu bạn muốn đẩy log qua Logstash (trong trường hợp ELK của bạn có Logstash để xử lý logs)  output.logstash:  hosts: ["192.168.71.128:5044"]  # Các thiết lập logging cho Filebeat (có thể tuỳ chỉnh mức độ log, định dạng, v.v.)  logging.level: info  logging.to\_files: true  logging.files:  path: /var/log/filebeat  name: filebeat  keepfiles: 7  permissions: 0644  # Đảm bảo Filebeat tự động tải lại cấu hình (nếu cần) khi có thay đổi, tuy nhiên thường đặt reload.enabled thành false cho môi trường sản xuất  # reload.enabled: false |

- Bước 2: Restart Filebeat, ta hoàn thành việc cấu hình để hệ thống sẽ đẩy Logs về cho Server.

## 1.2. Cấu hình phía Winlogbeat Windows

- Bước 1: Tải Winlogbeat theo hướng dẫn của ELK [Download Winlogbeat | Ship Windows Event Logs | Elastic | Elastic](https://www.elastic.co/downloads/beats/winlogbeat)

- Bước 2: Ta cấu hình file winlogbeat.yml như sau:

|  |
| --- |
| ###################### Winlogbeat Configuration Example ########################  winlogbeat.event\_logs:  - name: Application  #ignore\_older: 72h  - name: System  - name: Security  - name: Microsoft-Windows-Sysmon/Operational  - name: Windows PowerShell  event\_id: 400, 403, 600, 800  - name: Microsoft-Windows-PowerShell/Operational  event\_id: 4103, 4104, 4105, 4106  - name: ForwardedEvents  tags: [forwarded]  # ================================== Outputs ===================================  # ------------------------------ Logstash Output -------------------------------  output.logstash:  #The Logstash hosts  hosts: ["192.168.71.128:5044"]  # Optional SSL. By default is off.  # List of root certificates for HTTPS server verifications  #ssl.certificate\_authorities: ["/etc/pki/root/ca.pem"]  # Certificate for SSL client authentication  #ssl.certificate: "/etc/pki/client/cert.pem"  # Client Certificate Key  #ssl.key: "/etc/pki/client/cert.key"  # ================================= Processors =================================  processors:  - add\_host\_metadata:  when.not.contains.tags: forwarded  - add\_cloud\_metadata: ~  # ================================= Migration ==================================  # This allows to enable 6.7 migration aliases  #migration.6\_to\_7.enabled: true |

- Bước 3: lưu file và chạy dịch vụ Winlogbeat theo hướng dẫn [Winlogbeat quick start: installation and configuration | Winlogbeat Reference [8.17] | Elastic](https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-installation-configuration.html)

## 1.3. Cấu hình Logstash Server

- Bước 1: Ta chỉnh lại file /etc/logstash/conf.d/sys-logs.conf như sau:

|  |
| --- |
| **root@ubuntu-1**:/home/wanthinnn# cat /etc/logstash/conf.d/sys-logs.conf  input {  beats {  port => 5044  ssl => false  }  }  filter {  if [agent][type] == "winlogbeat" {  if [winlog][channel] == "Security" {  prune {  whitelist\_names => [  "^@timestamp$",  "^winlog\.event\_id$",  "^winlog\.event\_data\.SubjectLogonId$",  "^winlog\.provider\_guid$",  "^winlog\.provider\_name$",  "^host\.name$",  "^host\.hostname$",  "^host\.ip$",  "^winlog\.event\_data\.SubjectUserName$",  "^event\.code$",  "^winlog\.event\_data\.TargetUserName$",  "^winlog\.keywords$",  "^event\.outcome$",  "^event\.action$",  "^message$"  ]  }  } else {  #drop { }  }  }  else if [agent][type] == "filebeat" {  prune {  whitelist\_names => [  "^@timestamp$",  "^syslog\_timestamp$",  "^host$",  "^program$",  "^log\_message$",  "^message$"  ]  }  }  }  output {  elasticsearch {  index => "system\_logs"  hosts => ["192.168.71.128:9200"]  user => "elastic"  password => "\_K0mCKP=\_7Y7y=TU4gTI"  ssl => true  ssl\_certificate\_verification => false  }  # Thêm output debug  stdout { codec => rubydebug }  } |

- Bước 2: Lưu file và khởi động lại Logstash

## 1.4. Kết quả

A screenshot of a computer

AI-generated content may be incorrect.

Hình 2. Logs bên Windows

A screenshot of a text message

AI-generated content may be incorrect.

Hình 3. Logs bên Linux

# 2. Phân tích Logs

## 2.1. Windows Logs

Ta phân tích logs sau:

|  |
| --- |
| {  "@timestamp": [  "2025-03-25T18:07:40.705Z"  ],  "@version": [  "1"  ],  "@version.keyword": [  "1"  ],  "agent.ephemeral\_id": [  "876b9c19-be24-4144-af1c-ae57a29f7f33"  ],  "agent.ephemeral\_id.keyword": [  "876b9c19-be24-4144-af1c-ae57a29f7f33"  ],  "agent.id": [  "c8fafb59-94ab-49f9-8c63-73457b109489"  ],  "agent.id.keyword": [  "c8fafb59-94ab-49f9-8c63-73457b109489"  ],  "agent.name": [  "DESKTOP-DDGUTK5"  ],  "agent.name.keyword": [  "DESKTOP-DDGUTK5"  ],  "agent.type": [  "winlogbeat"  ],  "agent.type.keyword": [  "winlogbeat"  ],  "agent.version": [  "8.17.3"  ],  "agent.version.keyword": [  "8.17.3"  ],  "ecs.version": [  "8.0.0"  ],  "ecs.version.keyword": [  "8.0.0"  ],  "event.action": [  "None"  ],  "event.action.keyword": [  "None"  ],  "event.code": [  "15"  ],  "event.code.keyword": [  "15"  ],  "event.created": [  "2025-03-25T18:07:41.413Z"  ],  "event.kind": [  "event"  ],  "event.kind.keyword": [  "event"  ],  "event.original": [  "Updated Windows Defender status successfully to SECURITY\_PRODUCT\_STATE\_ON."  ],  "event.original.keyword": [  "Updated Windows Defender status successfully to SECURITY\_PRODUCT\_STATE\_ON."  ],  "event.provider": [  "SecurityCenter"  ],  "event.provider.keyword": [  "SecurityCenter"  ],  "host.architecture": [  "x86\_64"  ],  "host.architecture.keyword": [  "x86\_64"  ],  "host.hostname": [  "DESKTOP-DDGUTK5"  ],  "host.hostname.keyword": [  "DESKTOP-DDGUTK5"  ],  "host.id": [  "cc9deadc-7c54-4c4b-8104-9fec22b6a922"  ],  "host.id.keyword": [  "cc9deadc-7c54-4c4b-8104-9fec22b6a922"  ],  "host.ip": [  "fe80::8529:3bf3:a045:a448",  "192.168.71.132"  ],  "host.ip.keyword": [  "fe80::8529:3bf3:a045:a448",  "192.168.71.132"  ],  "host.mac": [  "00-0C-29-C2-3B-2B"  ],  "host.mac.keyword": [  "00-0C-29-C2-3B-2B"  ],  "host.name": [  "desktop-ddgutk5"  ],  "host.name.keyword": [  "desktop-ddgutk5"  ],  "host.os.build": [  "19045.5608"  ],  "host.os.build.keyword": [  "19045.5608"  ],  "host.os.family": [  "windows"  ],  "host.os.family.keyword": [  "windows"  ],  "host.os.kernel": [  "10.0.19041.5607 (WinBuild.160101.0800)"  ],  "host.os.kernel.keyword": [  "10.0.19041.5607 (WinBuild.160101.0800)"  ],  "host.os.name": [  "Windows 10 Pro"  ],  "host.os.name.keyword": [  "Windows 10 Pro"  ],  "host.os.platform": [  "windows"  ],  "host.os.platform.keyword": [  "windows"  ],  "host.os.type": [  "windows"  ],  "host.os.type.keyword": [  "windows"  ],  "host.os.version": [  "10.0"  ],  "host.os.version.keyword": [  "10.0"  ],  "log.level": [  "information"  ],  "log.level.keyword": [  "information"  ],  "message": [  "Updated Windows Defender status successfully to SECURITY\_PRODUCT\_STATE\_ON."  ],  "message.keyword": [  "Updated Windows Defender status successfully to SECURITY\_PRODUCT\_STATE\_ON."  ],  "tags": [  "beats\_input\_codec\_plain\_applied"  ],  "tags.keyword": [  "beats\_input\_codec\_plain\_applied"  ],  "winlog.api": [  "wineventlog"  ],  "winlog.api.keyword": [  "wineventlog"  ],  "winlog.channel": [  "Application"  ],  "winlog.channel.keyword": [  "Application"  ],  "winlog.computer\_name": [  "DESKTOP-DDGUTK5"  ],  "winlog.computer\_name.keyword": [  "DESKTOP-DDGUTK5"  ],  "winlog.event\_data.param1": [  "Windows Defender"  ],  "winlog.event\_data.param1.keyword": [  "Windows Defender"  ],  "winlog.event\_data.param2": [  "SECURITY\_PRODUCT\_STATE\_ON"  ],  "winlog.event\_data.param2.keyword": [  "SECURITY\_PRODUCT\_STATE\_ON"  ],  "winlog.event\_id": [  "15"  ],  "winlog.event\_id.keyword": [  "15"  ],  "winlog.keywords": [  "Classic"  ],  "winlog.keywords.keyword": [  "Classic"  ],  "winlog.opcode": [  "Info"  ],  "winlog.opcode.keyword": [  "Info"  ],  "winlog.provider\_name": [  "SecurityCenter"  ],  "winlog.provider\_name.keyword": [  "SecurityCenter"  ],  "winlog.record\_id": [  1849  ],  "winlog.task": [  "None"  ],  "winlog.task.keyword": [  "None"  ],  "\_id": "QMd9zpUBt1k2K1aFTacx",  "\_index": "system\_logs",  "\_score": null  } |

**Thông tin chung và định danh**

**- @timestamp:** "2025-03-25T18:07:40.705Z" → Đây là thời điểm mà sự kiện được ghi nhận (theo giờ UTC).

- **agent:**agent.type là "winlogbeat", phiên bản "8.17.3" và tên máy "DESKTOP-DDGUTK5". Điều này cho biết log được thu thập bởi winlogbeat trên máy Windows có tên DESKTOP-DDGUTK5.

- **host:**

* + host.os.name: "Windows 10 Pro" và host.os.version: "10.0"
  + host.architecture: "x86\_64"
  + host.hostname và host.name: "DESKTOP-DDGUTK5" (có sự nhất quán giữa các trường).
  + host.ip liệt kê địa chỉ IPv6 và IPv4 (192.168.71.132).

**Thông tin sự kiện (Event details)**

- **event.code / winlog.event\_id:** "15" → Đây là mã sự kiện do Windows ghi lại; mã 15 trong ngữ cảnh của Windows Defender thường liên quan đến việc cập nhật trạng thái bảo mật.

**- event.provider / winlog.provider\_name:** "SecurityCenter" → Sự kiện được tạo ra bởi SecurityCenter – thành phần giám sát của Windows (thường liên quan đến trạng thái của các sản phẩm bảo mật như Windows Defender).

**- log.level:** "information" → Sự kiện có mức độ thông tin, không phải cảnh báo hay lỗi.

**Nội dung sự kiện và ý nghĩa**

**- message / event.original:** "Updated Windows Defender status successfully to SECURITY\_PRODUCT\_STATE\_ON." → Log cho biết rằng trạng thái của Windows Defender đã được cập nhật thành công và đang ở trạng thái “SECURITY\_PRODUCT\_STATE\_ON” (tức là sản phẩm bảo mật đang được bật).

- **winlog.event\_data.param1 và param2:**

* + param1: "Windows Defender"
  + param2: "SECURITY\_PRODUCT\_STATE\_ON"  
    → Các tham số này xác nhận rõ ràng rằng log liên quan đến việc cập nhật trạng thái của Windows Defender và trạng thái mới là ON.

**Các trường bổ sung khác**

- **winlog.channel:** "Application" → Mặc dù Windows Security events thường được ghi vào kênh “Security”, log này lại được đưa vào kênh “Application”. Tuy nhiên, bởi provider là SecurityCenter nên đây vẫn là sự kiện liên quan đến bảo mật.

- **winlog.opcode:** "Info" và **winlog.keywords:** "Classic" → Các trường này củng cố thông tin rằng đây là sự kiện thông tin (informational event) chứ không phải cảnh báo hay lỗi nghiêm trọng.

**event.action:** "None" → Không có hành động cụ thể nào được báo cáo ngoài việc cập nhật trạng thái.

**Ý nghĩa tổng thể**

- Sự kiện cho thấy Windows Defender trên máy DESKTOP-DDGUTK5 đã được cập nhật trạng thái thành công và đang ở chế độ bảo vệ (ON). Đây là một log thông tin, nhằm thông báo rằng sản phẩm bảo mật của Windows đang hoạt động đúng như mong đợi.

- Với mức độ log "information", sự kiện này không đòi hỏi hành động can thiệp mà có thể được dùng để giám sát sức khỏe của hệ thống bảo mật.

**Tóm lại:** Log này là một thông báo thông tin cho biết Windows Defender đã cập nhật trạng thái thành công lên SECURITY\_PRODUCT\_STATE\_ON. Đây là một phần trong chuỗi các sự kiện bảo mật được ghi lại nhằm giám sát trạng thái của các sản phẩm bảo mật của Windows và đảm bảo rằng hệ thống đang được bảo vệ.

## 2.2. Linux Logs

Ta phân tích log sau:

|  |
| --- |
| {  "@timestamp": [  "2025-03-25T18:01:10.840Z"  ],  "@version": [  "1"  ],  "@version.keyword": [  "1"  ],  "agent.ephemeral\_id": [  "8ae8a223-15f8-4909-a4d4-756d917c514b"  ],  "agent.ephemeral\_id.keyword": [  "8ae8a223-15f8-4909-a4d4-756d917c514b"  ],  "agent.id": [  "66168684-adf4-407c-8211-8d97194c00cf"  ],  "agent.id.keyword": [  "66168684-adf4-407c-8211-8d97194c00cf"  ],  "agent.name": [  "ubuntu-2"  ],  "agent.name.keyword": [  "ubuntu-2"  ],  "agent.type": [  "filebeat"  ],  "agent.type.keyword": [  "filebeat"  ],  "agent.version": [  "8.17.3"  ],  "agent.version.keyword": [  "8.17.3"  ],  "ecs.version": [  "8.0.0"  ],  "ecs.version.keyword": [  "8.0.0"  ],  "event.original": [  "Mar 26 01:01:07 ubuntu-2 su: (to root) root on pts/6"  ],  "event.original.keyword": [  "Mar 26 01:01:07 ubuntu-2 su: (to root) root on pts/6"  ],  "host.name": [  "ubuntu-2"  ],  "host.name.keyword": [  "ubuntu-2"  ],  "input.type": [  "filestream"  ],  "input.type.keyword": [  "filestream"  ],  "log.file.device\_id": [  "2051"  ],  "log.file.device\_id.keyword": [  "2051"  ],  "log.file.inode": [  "5507122"  ],  "log.file.inode.keyword": [  "5507122"  ],  "log.file.path": [  "/var/log/auth.log"  ],  "log.file.path.keyword": [  "/var/log/auth.log"  ],  "log.offset": [  3497  ],  "message": [  "Mar 26 01:01:07 ubuntu-2 su: (to root) root on pts/6"  ],  "message.keyword": [  "Mar 26 01:01:07 ubuntu-2 su: (to root) root on pts/6"  ],  "tags": [  "beats\_input\_codec\_plain\_applied"  ],  "tags.keyword": [  "beats\_input\_codec\_plain\_applied"  ],  "\_id": "LMd4zpUBt1k2K1aFw6fT",  "\_index": "system\_logs",  "\_score": null  } |

**Thông tin chung và nguồn log**

- **@timestamp:** "2025-03-25T18:01:10.840Z" → Thời điểm log được ghi nhận theo định dạng UTC. (Lưu ý rằng thời gian hiển thị trong message là "Mar 26 01:01:07", điều này có thể do múi giờ của hệ thống khác với UTC.)

- **agent.type:** "filebeat" → Log này được thu thập bởi filebeat, một agent dùng để giám sát các file log trên Linux.

- **agent.name:** "ubuntu-2" → Tên của máy chủ hoặc host nơi log được ghi nhận, ở đây là "ubuntu-2".

**Thông tin file log và input**

- **input.type:** "filestream" → Cho biết filebeat đang đọc log theo dạng stream từ tệp.

- **log.file.path:** "/var/log/auth.log" → Log này được lấy từ tệp /var/log/auth.log – tệp log chuyên dùng cho các sự kiện xác thực, bao gồm các thao tác đăng nhập, sử dụng lệnh su, sudo,…

- **log.offset:** 3497 → Vị trí offset trong tệp log tại thời điểm log được thu thập.

**Nội dung sự kiện (message và event.original)**

- **message / event.original:** "Mar 26 01:01:07 ubuntu-2 su: (to root) root on pts/6" → Đây là dòng log thực tế được ghi nhận từ hệ thống.

- **Thời gian:** "Mar 26 01:01:07" cho biết thời điểm sự kiện xảy ra theo định dạng của hệ thống (theo giờ địa phương).

- **Host:** "ubuntu-2" xác nhận rằng log đến từ máy chủ này.

- **Thành phần "su":** Dòng log cho biết lệnh su đã được thực thi. Trong trường hợp này, log cho thấy thao tác chuyển đổi quyền (switch user) đến tài khoản root.

- **(to root) root on pts/6:** Phần này giải thích rằng người dùng đã chuyển sang tài khoản root và phiên làm việc được mở trên terminal ảo (pseudo-terminal) pts/6.

**Ý nghĩa tổng thể của log**

- Log này nằm trong /var/log/auth.log nên liên quan đến các hoạt động xác thực trên hệ thống Linux.

- Cụ thể, nó báo cáo rằng vào lúc "Mar 26 01:01:07", một thao tác su được thực hiện trên máy "ubuntu-2", với mục đích chuyển đổi quyền sang tài khoản root trên terminal pts/6.

- Đây là một sự kiện bình thường trong quá trình quản trị hệ thống (nếu được thực hiện bởi người quản trị) nhưng cũng có thể là dấu hiệu cần theo dõi nếu xuất hiện bất thường (ví dụ, nếu có thao tác không được ủy quyền).

**Khuyến nghị khi phân tích log**

- **Kiểm tra lịch sử thao tác su:** Đối với mục đích bảo mật, bạn nên theo dõi xem thao tác chuyển đổi quyền (su) có được thực hiện bởi người quản trị hợp lệ không.

- **Đối chiếu với các log khác:** So sánh với các dòng log khác trong /var/log/auth.log để phát hiện các mẫu truy cập bất thường.

- **Múi giờ:** Lưu ý sự chênh lệch giữa thời gian ghi nhận log (UTC trong @timestamp và thời gian hiển thị trong message) để đảm bảo hiểu đúng thời điểm của sự kiện.

**Tóm lại,** log Linux này cho biết một thao tác su được thực hiện trên máy "ubuntu-2" nhằm chuyển sang tài khoản root, được ghi nhận trong tệp /var/log/auth.log – một thông tin quan trọng để giám sát các sự kiện xác thực và quản trị hệ thống.