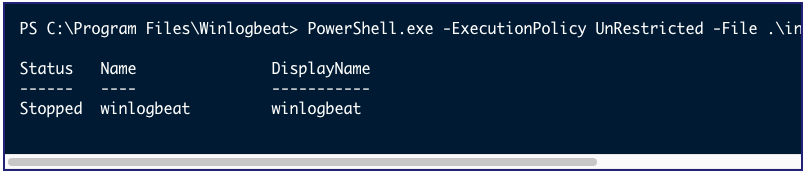
### How to **Install Winlogbeat on Windows**

1. Download Winlogbeat: [download page](https://www.elastic.co/downloads/beats/winlogbeat)
2. Giải nén
3. Copy vào thư mục Program Files
4. Mở terminal với quyền administrator và thay đổi tới thư mục Winlogbeat bằng câu lệnh sau:  
   **cd C:\Program Files\Winlogbeat**
5. Cài đặt Winlogbeat bằng câu lệnh sau:

**C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1**

1. Thực thi tệp lệnh Winlogbeat với chính sách không hạn chế bằng lệnh sau:  
   **C:\Program Files\Winlogbeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1**
2. Sửa file cấu hình của Winlogbeat C:\Program Files\Winlogbeat\winlogbeat.yml. Sử dụng notepad++ hoặc các công cụ khác để sửa file winlogbeat.yml  
     
   # ================== Winlogbeat specific options =================  
   **winlogbeat.event\_logs:**

- name: Application

ignore\_older: 72h

- name: System

- name: Security

event\_id: 4624, 4625, 4634

- name: Microsoft-Windows-Sysmon/Operational

event\_id: 4608, 4609, 4610

- name: Windows PowerShell

event\_id: 400, 403, 600, 800

- name: Microsoft-Windows-PowerShell/Operational

event\_id: 4103, 4104, 4105, 4106

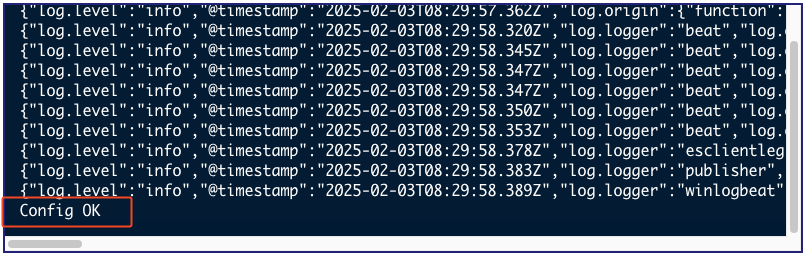
- name: ForwardedEvents

tags: [forwarded]  
  
# ------------------------------ Logstash Output -------------------------------

**output.logstash:**

# The Logstash hosts

hosts: ["**logstash08-anhpt8.citigo.com.vn:31544**"]  
  
Chú Ý: các event\_id mình sẽ lấy ở trong Event Viewer

1. Kiểm tra cấu hình  
   C:\'Program Files'\Winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml -e  
   
2. Start service winlogbeat

# Start Service

**C:\Program Files\Winlogbeat> Start-Service winlogbeat**

# Stop Service

**C:\Program Files\Winlogbeat> Stop-Service winlogbeat**

# Service Status  
**C:\Program Files\Winlogbeat> Get-Service winlogbeat**