Elastic Beats — Instalacja (Windows, ZIP/offline) z dashboardami Kibany

Komponenty: Filebeat, Winlogbeat, Packetbeat  
*Data: 2025-08-20 12:16*

# Wspólne wymagania

- Adresy: https://<ES\_HOST>:9200 i https://<KIBANA\_HOST>:5601; uprawnienia do Saved Objects i indeksów.

- TLS: własne CA w konfiguracji; 'ssl.verification\_mode: none' tylko testowo.

- Po imporcie dashboardów sprawdź Timepicker (np. Last 15 minutes) i właściwą Space.

# FILEBEAT — instalacja + dashboardy

1) Rozpakuj ZIP do C:\Elastic\filebeat.

2) Minimalny filebeat.yml:

filebeat.inputs:  
 - type: filestream  
 id: app-logs  
 enabled: true  
 paths: ["C:/Logs/\*.log"]  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<user>"  
 password: "<pass>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<user>"  
 password: "<pass>"

3) Instalacja usługi i start:

cd C:\Elastic\filebeat  
.\install-service-filebeat.ps1  
Start-Service filebeat

Dashboardy — wybierz jedną ścieżkę:

A) Auto-import:

C:\Elastic\filebeat\filebeat.exe setup --dashboards ^  
 -E setup.kibana.host=https://<KIBANA\_HOST>:5601 ^  
 -E setup.kibana.username=<user> ^  
 -E setup.kibana.password=<pass> ^  
 -E output.elasticsearch.hosts=["https://<ES\_HOST>:9200"] ^  
 -E output.elasticsearch.username=<user> ^  
 -E output.elasticsearch.password=<pass>

B) Ręczny import: Kibana → Stack Management → Saved Objects → Import → pliki .ndjson z katalogu kibana/ w paczce Filebeat.

Po imporcie: Analytics → Dashboard („Filebeat …”), Discover (filebeat-\* lub logs-\*).

# WINLOGBEAT — instalacja + dashboardy

1) Rozpakuj ZIP do C:\Elastic\winlogbeat.

2) Minimalny winlogbeat.yml:

winlogbeat.event\_logs:  
 - name: Security  
 level: Information  
 - name: System  
 - name: Application  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<user>"  
 password: "<pass>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<user>"  
 password: "<pass>"

3) Instalacja usługi i start:

cd C:\Elastic\winlogbeat  
.\install-service-winlogbeat.ps1  
Start-Service winlogbeat

Dashboardy — wybierz jedną ścieżkę:

A) Auto-import:

C:\Elastic\winlogbeat\winlogbeat.exe setup --dashboards ^  
 -E setup.kibana.host=https://<KIBANA\_HOST>:5601 ^  
 -E setup.kibana.username=<user> ^  
 -E setup.kibana.password=<pass> ^  
 -E output.elasticsearch.hosts=["https://<ES\_HOST>:9200"] ^  
 -E output.elasticsearch.username=<user> ^  
 -E output.elasticsearch.password=<pass>

B) Ręczny import: Kibana → Saved Objects → Import → pliki z katalogu kibana/ (np. module\windows\\_meta\kibana\dashboard).

Po imporcie: Analytics → Dashboard („Winlogbeat …”), Discover (winlog.\*).

# PACKETBEAT — instalacja + dashboardy

Wymóg: Npcap (WinPcap-compatible). Przy offline przygotuj instalator wcześniej.

1) Rozpakuj ZIP do C:\Elastic\packetbeat.

2) Minimalny packetbeat.yml:

packetbeat.interfaces.device: 0 # lub nazwa interfejsu (Get-NetAdapter)  
  
packetbeat.protocols:  
 - type: http  
 ports: [80, 8080, 8000, 5000, 8002]  
 - type: tls  
 ports: [443, 8443]  
 - type: dns  
 ports: [53]  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<user>"  
 password: "<pass>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<user>"  
 password: "<pass>"

3) Instalacja usługi i start:

cd C:\Elastic\packetbeat  
.\install-service-packetbeat.ps1  
Start-Service packetbeat

Dashboardy — wybierz jedną ścieżkę:

A) Auto-import:

C:\Elastic\packetbeat\packetbeat.exe setup --dashboards ^  
 -E setup.kibana.host=https://<KIBANA\_HOST>:5601 ^  
 -E setup.kibana.username=<user> ^  
 -E setup.kibana.password=<pass> ^  
 -E output.elasticsearch.hosts=["https://<ES\_HOST>:9200"] ^  
 -E output.elasticsearch.username=<user> ^  
 -E output.elasticsearch.password=<pass>

B) Ręczny import: Kibana → Saved Objects → Import → pliki z katalogu kibana/ w paczce Packetbeat.

Po imporcie: Analytics → Dashboard („Packetbeat …”), Discover (network.\*, http.\*, dns.\*, tls.\*).

# Weryfikacja po imporcie

1) Analytics → Dashboard: wyszukaj „Filebeat” / „Winlogbeat” / „Packetbeat”.

2) Saved Objects: sprawdź, czy przybyło dashboardów/wizualizacji.

3) Data Views: filebeat-\*, winlogbeat-\*, packetbeat-\* (lub logs-\*).

4) Timepicker: Last 15 minutes.

# Najczęstsze problemy

- 403 podczas importu: brak uprawnień do Saved Objects/Space.

- TLS: dodaj CA w setup.kibana.ssl.certificate\_authorities i output.elasticsearch.ssl.certificate\_authorities.

- Pusty dashboard: zły zakres czasu lub brak dopasowanego Data View.

- Packetbeat nie widzi interfejsu: zainstaluj Npcap, uruchom usługę jako Administrator.