Filebeat — dokumentacja wdrożeniowa (PL)

Wersja: Windows (ZIP/offline), integracja z Kibana Dashboards  
*Data: 2025-08-21 06:34*

# 1) Cel i korzyści

* Zbieranie logów aplikacyjnych i systemowych z plików (rotowanych/podzielonych).
* Parsowanie JSON/NDJSON, wsparcie multiline (np. stack trace).
* Wysyłka do Elasticsearch (lub Logstash), mapowanie do ECS, gotowe dashboardy modułów (np. IIS).

# 2) Wymagania i przygotowanie

* Windows x64, dostęp do ścieżek logów (uprawnienia odczytu).
* Kibana/Elasticsearch: adresy, konto z uprawnieniami do Saved Objects i indeksów.
* TLS: jeśli własne CA — wskaż plik CA w konfiguracji (nie wyłączaj weryfikacji w produkcji).

# 3) Instalacja (ZIP/offline) — Windows

1) Rozpakuj paczkę ZIP do katalogu, np. C:\Elastic\filebeat.

2) Zainstaluj usługę i uruchom:

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

# 4) Konfiguracja minimalna (przykłady)

## 4A) Logi aplikacji w NDJSON (rekomendowane)

filebeat.inputs:  
 - type: filestream  
 id: app-json  
 enabled: true  
 paths: ["C:/Logs/MyApp/\*.log"]  
 parsers:  
 - ndjson:  
 target: ""  
 add\_error\_key: true  
  
processors:  
 - add\_fields:  
 target: "app"  
 fields:  
 name: "myapp"  
 env: "prod"  
 - drop\_fields:  
 fields: ["log.offset"]  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<USER>"  
 password: "<PASS>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<USER>"  
 password: "<PASS>"

## 4B) Logi tekstowe z multiline (np. Java stack trace)

filebeat.inputs:  
 - type: filestream  
 id: app-text  
 enabled: true  
 paths: ["C:/Logs/MyApp/\*.txt"]  
 parsers:  
 - multiline:  
 type: pattern  
 pattern: '^[ \t]'  
 negate: false  
 match: after  
processors:  
 - add\_fields:  
 target: "app"  
 fields: { name: "myapp", env: "prod" }  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<USER>"  
 password: "<PASS>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<USER>"  
 password: "<PASS>"

# 5) Dashboardy w Kibanie (auto-import lub ręcznie)

A) Auto-import (rekomendowane):

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>

(Jeśli używasz Spaces: dodaj -E setup.kibana.space.id=<SPACE\_ID>)

B) Ręczny import: Kibana → Stack Management → Saved Objects → Import → wybierz pliki z katalogu 'kibana/' w paczce Filebeat (lub w modułach).

Po imporcie: Analytics → Dashboard → wyszukaj „Filebeat …”. Discover: data view `filebeat-\*` (ew. `logs-\*`).

# 6) Moduły — przykłady

Włączanie modułu (PowerShell, w katalogu Filebeat):

.\filebeat.exe modules enable iis

Przykładowa konfiguracja modułu IIS (pliki access/error):

filebeat.modules:  
 - module: iis  
 access:  
 enabled: true  
 var.paths: ["C:/inetpub/logs/LogFiles/\*/\*.log"]  
 error:  
 enabled: true  
 var.paths: ["C:/Windows/System32/LogFiles/HTTPERR/\*.log"]

Ogólne filtry wejściowe (exclude/include w filestream):

filebeat.inputs:  
 - type: filestream  
 id: app-text  
 paths: ["C:/Logs/MyApp/\*.log"]  
 exclude\_lines: ['^DEBUG']  
 include\_lines: ['ERROR','FATAL']

# 7) Kibana — gdzie patrzeć i jak wyciągać wnioski

* Dashboards: „Filebeat Overview” / modułowe (np. „[Filebeat] IIS logs”).
* Discover: filtruj `log.level`, `message`, `host.name`, `app.name` (jeśli dodane przez add\_fields).
* Lens: Twórz wykresy błędów po hostach/usługach; trend `log.level: error` w czasie.

# 8) KQL — gotowe filtry

log.level : ("error" or "critical") and @timestamp >= now-24h

host.name : "api-01" and log.level : "error"

app.name : "myapp" and not agent.type : "filebeat"

# 9) Alerty — wzorce reguł

* Skok błędów: KQL `log.level: (error or critical)`; okno 5 min; Group by `host.name`, `app.name`.
* IIS 5xx: KQL `event.dataset: "iis.access" and http.response.status\_code >= 500`; warunek procentowy > X%.
* Cisza w logach (brak zdarzeń): monitor „Less than 1 match” dla `app.name`/`host.name` w 10–15 min.

# 10) Dobre praktyki

* Preferuj NDJSON — łatwiejsze parsowanie i mniej błędów multiline.
* Ustal `fields.env` (prod/stage/dev) i `fields.role` (web/api/worker) dla łatwiejszych filtrów.
* Zadbaj o rotację logów po rozmiarze/czasie (IIS/serwisy).
* TLS: użyj `output.elasticsearch.ssl.certificate\_authorities` i odpowiednika w `setup.kibana` dla własnego CA.
* ILM/retencja: zaplanuj okresy przechowywania; dashboardy mogą używać data streams `logs-\*`.

# 11) Troubleshooting

* Brak danych: sprawdź usługę (`Get-Service filebeat`), logi w `logs\`, połączenie do ES/Kibany, Timepicker w Kibanie.
* Duże eventy lub błędy JSON: upewnij się, że źródło loguje NDJSON i nie miesza formatów.
* Multiline 'zalewa' indeks: dostosuj wzorzec `pattern` i `match: after` do konkretnego formatu.
* TLS/403: dodaj CA w `ssl.certificate\_authorities`; sprawdź uprawnienia Saved Objects dla `setup --dashboards`.
* Puste dashboardy: brak dopasowanego data view (`filebeat-\*`) lub zły zakres czasu.

# 12) Szybki checklist (TL;DR)

* Rozpakuj ZIP → `install-service-filebeat.ps1` → `Start-Service filebeat`.
* Skonfiguruj `filebeat.inputs` (NDJSON lub multiline) + `output.elasticsearch` + `setup.kibana`.
* Wgraj dashboardy: `filebeat.exe setup --dashboards` lub import ręczny.
* Sprawdź w Kibanie: Dashboards + Discover; ustaw Timepicker.
* Dodaj alerty (błędy, 5xx, cisza w logach) i retencję/ILM.