Metricbeat — dokumentacja wdrożeniowa (PL)

Wersja: Windows (ZIP/offline), integracja z Kibana Dashboards  
*Data: 2025-08-21 06:36*

# 1) Cel i korzyści

* Zbieranie metryk hostów i usług (CPU, pamięć, dyski, sieć, procesy, usługi Windows).
* Gotowe moduły (system, windows, mssql, i inne) mapujące dane do ECS.
* Wizualizacja w Kibanie (Dashboards, Lens), alerty na progi i anomalie.

# 2) Wymagania i przygotowanie

* Windows x64; uprawnienia usługi do odczytu PerfMon/WMI oraz statusów usług.
* Kibana/Elasticsearch: adresy oraz konto z uprawnieniami do Saved Objects i indeksów.
* TLS: jeśli własne CA — wskaż plik CA; nie wyłączaj weryfikacji w produkcji.

# 3) Instalacja (ZIP/offline) — Windows

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

2) Zainstaluj usługę i uruchom:

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

# 4) Konfiguracja minimalna (przykłady)

## 4A) Moduł system — podstawowe metryki hosta

metricbeat.modules:  
 - module: system  
 metricsets: [cpu, memory, network, diskio, filesystem, process]  
 period: 10s  
 processes: ['.\*']  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<USER>"  
 password: "<PASS>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<USER>"  
 password: "<PASS>"

## 4B) Moduł windows — status usług itp.

metricbeat.modules:  
 - module: windows  
 metricsets: [service] # możesz dodać perfmon itp.  
 period: 30s  
  
output.elasticsearch:  
 hosts: ["https://<ES\_HOST>:9200"]  
 username: "<USER>"  
 password: "<PASS>"  
  
setup.kibana:  
 host: "https://<KIBANA\_HOST>:5601"  
 username: "<USER>"  
 password: "<PASS>"

## 4C) Włączenie modułów (PowerShell)

.\metricbeat.exe modules enable system windows

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

A) Auto-import (rekomendowane):

C:\Elastic\metricbeat\metricbeat.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 Metricbeat (lub w modułach).

Po imporcie: Analytics → Dashboard → wyszukaj „Metricbeat …”. Discover: data view `metricbeat-\*` (ew. `metrics-\*`).

# 6) Kibana — gdzie patrzeć i jak wyciągać wnioski

* Dashboards: „Metricbeat System Overview”, „Host metrics”, modułowe (np. MSSQL).
* Discover: kluczowe pola: host.name, event.dataset, metricset.name, system.\*, windows.service.\*.
* Lens: trendy CPU% per host, wolne miejsce per dysk, usługi Windows w czasie.

# 7) KQL — gotowe filtry

event.dataset : "system.cpu" and system.cpu.total.norm.pct >= 0.9 and @timestamp >= now-15m # CPU > 90%

event.dataset : "system.filesystem" and system.filesystem.used.pct >= 0.9 # dyski <10% wolnego

event.dataset : "windows.service" and windows.service.state : "stopped" # zatrzymane usługi

event.dataset : "system.network" and system.network.in.bytes > 104857600 # >100 MB/s (przykład)

# 8) Alerty — wzorce reguł

* CPU przeciążone: KQL powyżej; okno 5 min; Group by host.name.
* Mało miejsca na dysku: `system.filesystem.used.pct >= 0.9`; Group by host.name i mount\_point.
* Usługa zatrzymana: `windows.service.state: "stopped"`; Group by host.name i windows.service.name.
* Cisza metryk (host down): Less than 1 match dla hosta w 5–10 min.

# 9) Dobre praktyki

* Ustal `host.name` spójnie z CMDB; dodaj fields.env (prod/stage/dev) i fields.role (db/web/app).
* Dostosuj `period` (10–30s) do wymagań i skali; wyłącz zbędne metricsety dla mniejszego narzutu.
* TLS: wskaż CA w output.elasticsearch.ssl.certificate\_authorities oraz w setup.kibana.ssl.certificate\_authorities.
* ILM/retencja: skonfiguruj polityki przechowywania metryk (gorąca→ciepła→kasowanie).

# 10) Troubleshooting

* Brak danych: sprawdź usługę (`Get-Service metricbeat`), logi w `logs\`, połączenie do ES/Kibany, Timepicker w Kibanie.
* Brak `windows.service.\*`: upewnij się, że moduł windows jest włączony, a konto usługi ma dostęp do WMI/PerfMon.
* TLS/403: dodaj CA i sprawdź uprawnienia do Saved Objects (setup --dashboards).
* Puste dashboardy: brak dopasowanego data view (`metricbeat-\*`) lub zły zakres czasu.
* Wysokie zużycie: podnieś `period`, ogranicz `processes`, wyłącz zbędne metricsety.

# 11) Szybki checklist (TL;DR)

* Rozpakuj ZIP → `install-service-metricbeat.ps1` → `Start-Service metricbeat`.
* Włącz `system` i (opcjonalnie) `windows`: `metricbeat.exe modules enable system windows`.
* Skonfiguruj output do ES i setup.kibana; wgraj dashboardy `metricbeat.exe setup --dashboards`.
* Sprawdź w Kibanie: Dashboards + Discover; ustaw Timepicker i dodaj alerty.