**Słownik pojęć Kibany – Beats + APM/RUM**

*Oddzielny dokument z definicjami w kontekście poprzedniego mini‑słownika*

*Data: 21 sierpnia 2025*

# Definicje

**Beat –** lekki agent (shipper) instalowany na hoście do wysyłania danych do Elasticsearch (np. Filebeat, Metricbeat, Winlogbeat, Packetbeat, Heartbeat). W polach danych widać go zwykle jako wartość pola agent.type.

Przykład: agent.type : "filebeat"

**logs-\* –** wzorzec (data view / nazwa strumienia) pasujący do wszystkich strumieni dzienników, np. logs-system.syslog-default, logs-nginx.access-prod.

Przykład: Data view: logs-\* → pasuje do logs-\*-\*

**Automatyczny rollover –** mechanizm data streams/ILM: gdy bieżący indeks zapisujący („write index”) osiągnie próg (rozmiar/wiek/liczbę dokumentów), tworzony jest kolejny indeks zapasowy (…-000002, …-000003), a zapis płynnie się przełącza. Zapewnia stabilną wydajność i kontrolę retencji.

**Korelacja logów / metryk / śladów –** łączenie informacji z różnych źródeł dzięki wspólnemu schematowi ECS (np. service.name, host.name, trace.id), aby przechodzić od błędu w logach do śladu APM i metryk hosta z tego samego czasu.

**Agent –** proces zbierający dane. Może to być Elastic Agent (zarządzany centralnie we Fleet i obsługujący wiele integracji) albo pojedynczy Beat konfigurowany lokalnie w YAML.

**Integracja centralna –** pakiet we Fleet (Integration), który centralnie dostarcza gotowe pipeline’y, dashboardy i konfiguracje dla grup agentów (np. Windows, System, APM, Synthetics).

Uwaga: Dotyczy Elastic Agent + Fleet; Beats bez Fleet konfigurujesz per‑host.

**Log rate –** widżet w Logs → Stream pokazujący tempo napływu logów (liczbę zdarzeń w czasie). Pomaga wykryć nagłe „burze” logów.

**windows.sysmon –** wartość pola event.dataset dla danych z Sysmon (Windows). Ułatwia filtrowanie/alertowanie logów Sysmon.

Uwaga: W pytaniu: „windows,sysmon” – poprawna notacja to „windows.sysmon”.

Przykład: event.dataset : "windows.sysmon"

**Pods / Container –** byty uruchomieniowe w Kubernetes/Docker. Pod to jednostka K8s (zawiera 1+ kontenery), Container to proces aplikacji z obrazem. W Kibanie widoczne w Infrastructure → Inventory/Pods/Containers.

**Klaster –** grupa węzłów pracujących razem. Najczęściej: klaster Elasticsearch (przechowuje/indeksuje dane) lub klaster Kubernetes (źródło metryk/podów).

Uwaga: W pytaniu zapis w cudzysłowie – tutaj używamy zwykłej formy: klaster.

**p95 –** 95. percentyl wartości (np. czasu odpowiedzi). „p95 latency = 400 ms” oznacza, że 95% operacji zakończyło się szybciej niż 400 ms (5% było wolniejszych).

**ICMP –** protokół używany m.in. przez polecenie ping; w Heartbeat monitor typu icmp sprawdza osiągalność hosta.

Przykład: monitor.type : "icmp"

**TCP –** protokół połączeniowy (np. port 443). W Heartbeat monitor typu tcp sprawdza, czy port przyjmuje połączenia; w Packetbeat analizujesz ruch TCP.

Przykład: network.transport : "tcp"

**Synthetic journey –** scenariusz testów przeglądarkowych w Synthetics/Heartbeat (Browser), odtwarzający kolejne kroki użytkownika; w UI widoczne są „steps” i wykres „waterfall”.

**Latency –** czas trwania/odpowiedzi transakcji/żądania. W APM prezentowana jako średnia i percentyle (p95/p99).

Przykład: transaction.duration.us > 4000000 // >4 s

**Throughput –** przepustowość – liczba transakcji/żądań w jednostce czasu (np. RPS).

Uwaga: W pytaniu literówka: „Troughput”.

**Failed transaction rate –** odsetek transakcji zakończonych niepowodzeniem. W APM zwykle bazuje na event.outcome:"failure" lub kodach 5xx.

Przykład: service.name : "orders-api" and event.outcome : "failure"

**Dependencies –** zależności usługi (DB, usługi HTTP, kolejki), widoczne w APM (karta Dependencies/Service map). Pomagają znaleźć wąskie gardła poza samą usługą.

**Instances –** instancje raportujące danej usługi (procesy/pody). W APM zobaczysz ich rozkład opóźnień i anomalii (np. jeden pod wolniejszy od pozostałych).

**page-load –** typ transakcji RUM dla pierwszego załadowania strony (zwłaszcza dla SPA – Single Page Application).

**route-change –** typ transakcji RUM oznaczający nawigację wewnątrz SPA bez pełnego przeładowania strony (np. Angular Router).

**Core Web Vitals –** kluczowe metryki UX dla frontendu: LCP (Largest Contentful Paint), INP (Interaction to Next Paint – responsywność), CLS (Cumulative Layout Shift – stabilność układu); często analizuje się też TTFB.

**Log Threshold –** typ reguły alertowej w Observability: wyzwala alert, gdy liczba logów spełniających warunek KQL przekroczy zadany próg w oknie czasu.

Przykład: Kondycja: log.level : "error" + Count ≥ 50 w 5 min

**Polityka rollover –** zestaw zasad ILM określających warunki wykonania rollover (progi rozmiaru, wieku, liczby dokumentów) oraz dalsze etapy cyklu życia (warm/cold/delete).

Uwaga: W pytaniu: „ppolityka rollover” – poprawiono literówkę.

# Aneks – szybkie przykłady KQL

event.dataset : "windows.sysmon"

agent.type != "filebeat"

monitor.type : "tcp" and monitor.status : "down"

service.name : "orders-api" and event.outcome : "failure"

transaction.type : "page-load" and transaction.duration.us > 4000000

network.transport : "tcp" and http.response.status\_code >= 500