**0) Założenia (wstaw swoje, jeśli inne)**

* **Elasticsearch:** https://es.internal.local:9200
* **Kibana:** https://kibana.internal.local:5601
* **Fleet Server URL (8220/TCP):** https://fleet.internal.local:8220
* **Namespace:** default
* **CA (PEM) ES/Fleet/EPR:** posiadasz i dodałeś w Kibanie tam, gdzie trzeba

**1) Fleet → Settings (jednorazowo)**

1. **Fleet Server hosts** → **Add/Edit** → wpisz https://fleet.internal.local:8220.
2. **Outputs → Default output (Elasticsearch)** → **Edit** → wklej **CA** (PEM), zapisz.
3. **Download sources (offline)** → dodaj URL do **wewnętrznego EPR** i jego **CA** → zapisz.

Jeżeli nie masz on-prem EPR: integracje mogą wisieć na *pending download*. Wtedy dodawaj tylko te, które masz lokalnie zapewnione przez źródło.

**2) Polityki (Agent policies)**

**2.1 Fleet Server policy (już jest)**

* **Add integration** → **System**
  + Metrics: CPU/Memory/Network/Filesystem (domyślne)
* **Add integration** → **Windows**
  + Channels: *Application*, *Security*, *System* (domyślnie)  
    Zapisz. Dzięki temu Fleet Server **sam też** wysyła swoje logi/metryki.

**2.2 Windows Base policy (dla zwykłych hostów)**

**Fleet → Agent policies → Create agent policy**

* **Name:** Windows Base policy
* **Namespace:** default
* **Add integration → Windows**
  + *Windows Logs:* zaznacz Application, Security, System
  + (opcjonalnie) ForwardedEvents, Setup
* **Add integration → System**
  + CPU/Memory/Network/Filesystem (domyślnie)
* **Add integration → IIS** *(jeśli masz IIS)*
  + Log path: pozostaw domyślne (Agent znajdzie standardowe ścieżki)

Zapisz. Polityka gotowa.

*(Opcjonalnie później)*

* **APM policy** (jeśli chcesz endpoint /intake na osobnym hoście): *Create agent policy → Add integration → Elastic APM* → zapisz.
* **Synthetics/Uptime** (Private locations): *Add integration → Synthetics* i przypnij do hosta/hostów, które będą wykonywać monitory.

**3) Enrollment tokens**

**Fleet → Enrollment tokens**

* Sprawdź, że jest token dla Windows Base policy.
* Jeśli nie: **Create enrollment token** → wybierz Windows Base policy → **Copy**.

**4) Dodawanie hostów (Windows) do Fleet**

Na **każdym** serwerze Windows (PowerShell jako Admin), użyj komendy podanej przez Kibana → *Agents → Add agent*. Przykład (offline, z CA):

cd C:\Elastic\elastic-agent

.\elastic-agent.exe install `

--url=https://fleet.internal.local:8220 `

--enrollment-token=<WSTAW\_TOKEN\_Z\_KIBANY> `

--certificate-authorities="C:\Elastic\elastic-agent\certs\ca.crt" `

--background

Uwaga: na **jednym** hoście działa **jedna** usługa Elastic Agent. Jeśli host ma też być **Private Location** dla Synthetics, dodasz integrację do jego polityki.

**5) Data Streams / Data Views**

**Stack Management → Data Views → Create data view**

* logs-\*-\* → Name logs → @timestamp
* metrics-\*-\* → Name metrics → @timestamp  
  *(jeśli używasz APM/Synthetics, dodaj później traces-\*-\*, synthetics-\*-\*)*

**6) Szybka walidacja danych**

**Discover → View: logs**

* KQL:
  + Winlogi: data\_stream.dataset : "winlog.security" OR "winlog.system" OR "winlog.application"
  + IIS: data\_stream.dataset : "iis.access"  
    **Discover → View: metrics**
* KQL: data\_stream.dataset : "system.cpu" OR "system.memory" OR "system.network" OR "system.filesystem"

W **Integrations → Windows/System/IIS → Dashboards** otwórz gotowe pulpity i sprawdź wykresy.

**7) Alerty (dwa szybkie przykłady)**

**Alerting → Create rule**

1. **Logs threshold** (nieudane logowanie):

* Rule type: *Logs threshold*
* Data view: logs-\*-\*
* Filter (KQL): data\_stream.dataset : "winlog.security" AND event.code : 4625
* Condition: Count > 0 w 5 min → dodaj Action (np. e-mail)

1. **Metric threshold** (CPU > 90%):

* Rule type: *Metric threshold*
* Data view: metrics-\*-\*
* Aggregation: *Average* of system.cpu.total.norm.pct
* Condition: > 0.9 przez 5 min → Action

**8) (Opcjonalnie) ILM / szablony**

**Index Lifecycle Policies**

* ilm-logs-30d: *Delete after 30 days*
* ilm-metrics-14d: *Delete after 14 days*

**Index Templates → Create template**

* tmpl-logs (patterns: logs-\*) → Settings:
* { "index.lifecycle.name": "ilm-logs-30d" }
* tmpl-metrics (patterns: metrics-\*) → Settings:
* { "index.lifecycle.name": "ilm-metrics-14d" }

Integracje mają własne domyślne ustawienia; te szablony służą do **nadpisania globalnie** retencji, jeśli chcesz.

**9) Najczęstsze problemy i szybkie fixy**

* **Agent „Pending” / integracja „Pending download”** → brak dostępu Kibany do pakietów integracji. Skonfiguruj **Download source** (on-prem EPR) + CA.
* **TLS x509** (mismatch hosta) → używaj tego samego FQDN w certyfikacie i w Fleet Server hosts.
* **Brak danych w Discover** → sprawdź Fleet → Agents (status), oraz log na hoście: C:\Program Files\Elastic\Agent\data\logs\elastic-agent.log.
* **Brak uprawnień do indeksów** → użytkownik musi mieć read/view\_index\_metadata do logs-\*, metrics-\*.

**Mini-skrypt do szybkiej instalacji na wielu Windowsach (opcjonalnie)**

Zapisz jako enroll.ps1, uzupełnij token i ścieżkę CA, skopiuj na hosty:

param(

[Parameter(Mandatory=$true)][string]$EnrollmentToken,

[string]$FleetUrl = "https://fleet.internal.local:8220",

[string]$CaPath = "C:\Elastic\elastic-agent\certs\ca.crt"

)

$ErrorActionPreference = "Stop"

if (-not (Test-Path $CaPath)) { throw "Brak CA pod: $CaPath" }

& "C:\Elastic\elastic-agent\elastic-agent.exe" install `

--url=$FleetUrl `

--enrollment-token=$EnrollmentToken `

--certificate-authorities=$CaPath `

--background

Write-Host "OK: Agent zainstalowany i zarejestrowany."

**Podsumowanie (co dziś zrobiłeś w Kibanie)**

* Upewniłeś się, że **Fleet Server hosts / Output / Download source** są ustawione.
* Stworzyłeś politykę **Windows Base policy** z **Windows + System (+ IIS)**.
* Wygenerowałeś **Enrollment token** i dodałeś hosty.
* Zbudowałeś **Data Views**, sprawdziłeś dane w **Discover** i **dashboardach**.
* Włączyłeś 2 **alerty** i (opcjonalnie) **ILM**.