**1) Sprawdź zdrowie Fleet Servera**

**Kibana → Fleet → Agents**

1. Na liście powinien być **Fleet Server** (Status: *Healthy* / zielony).
2. Wejdź w jego szczegóły → sprawdź, czy przypięty jest do **Fleet Server policy**.

Jeśli nie jest zielony: najpierw rozwiąż błędy TLS/połączeń (log w hostcie: C:\Program Files\Elastic\Agent\data\logs\elastic-agent.log).

**2) Ustawienia Fleet (adresy, output do ES, źródła paczek)**

**Kibana → Fleet → Settings**

1. **Fleet Server hosts**
   * Kliknij **Edit hosts** → dodaj/zweryfikuj URL(y) Twojego Fleet Servera, np.  
     https://fleet.internal.local:8220
   * (Jeśli masz wiele FS) wprowadź **kilka URL-i** albo URL load balancera.
2. **Elasticsearch outputs**
   * W sekcji **Outputs** upewnij się, że istnieje **Default output** do Twojego ES (HTTPS/9200).
   * Wejdź w **Edit** → dodaj **CA (PEM)**, z którego korzysta ES (w offline to krytyczne).
   * Zapisz.
3. **Download sources (OFFLINE!)**
   * W sekcji **Download sources** dodaj **wewnętrzny Elastic Package Registry (EPR)** (HTTPS) lub proxy, którego używa Kibana do pobierania paczek integracji.
   * (Jeśli Twój EPR ma własne CA) wklej CA/łańcuch zaufania.
   * Zapisz.

Bez tego pakiety integracji będą wisieć w stanie *pending download*.

1. (Opcjonalnie) **Agent binary source**
   * Jeśli używasz własnego mirrora binarek agenta (air-gap), wskaż tu swój serwer.

**3) Polityki agentów (Agent policies)**

**Kibana → Fleet → Agent policies**

1. **Fleet Server policy** (już istnieje):
   * Otwórz → **Add integration** → dodaj **System** oraz **Windows** (zbierzesz metryki/logi z hosta Fleet Servera).
   * Zapisz (Deployment will update).
2. **Utwórz politykę dla zwykłych hostów** (np. „Windows Base policy”):
   * **Create agent policy** → Name: *Windows Base policy*, Namespace: *default*.
   * **Add integration** → dodaj:
     + **Windows** (winlogi: Application/Security/System),
     + **System** (CPU/Memory/Network/Filesystem),
     + (opcjonalnie) **IIS** / inne źródła, których potrzebujesz.
   * Zapisz.
3. (Opcjonalnie) **Polityka APM**
   * **Create agent policy** → Name: *APM policy*.
   * **Add integration → Elastic APM** → włączysz endpoint /intake dla agentów .NET/JS/Java.
   * Tę politykę przypniesz do hosta, który ma przyjmować ruch APM (to może być inny serwer niż Fleet Server).

**4) Tokeny rejestracji (Enrollment tokens)**

**Kibana → Fleet → Enrollment tokens**

1. Sprawdź, czy dla każdej polityki masz token (tworzy się automatycznie).
2. W razie potrzeby **Create enrollment token** → wybierz politykę → skopiuj token (przyda się przy poleceniu elastic-agent.exe install na hostach).

**5) Dodanie kolejnych agentów (zdalne zarządzanie)**

**Kibana → Fleet → Agents → Add agent**

1. Wybierz **Windows Base policy** (albo inną, którą stworzyłeś).
2. Wybierz **Enroll in Fleet**.
3. Kibana wyświetli **gotową komendę** instalacji dla Windows (z Twoim --url=https://fleet.internal.local:8220 i --enrollment-token=...).
4. Uruchom ją na docelowym serwerze (PowerShell jako Admin).
5. Wróć do **Fleet → Agents** i poczekaj, aż nowy agent stanie się *Healthy*.

Na **jednym** hoście możesz łączyć role (Agent zbierający dane + Fleet Server) w **tej samej** instancji, dodając integracje do **Fleet Server policy**. W większych środowiskach rozdzielaj to dla czytelności i wydajności.

**6) Data Streams i Data Views (widoczność danych)**

1. **Kibana → Stack Management → Data Streams**
   * Sprawdź, czy pojawiają się strumienie logs-... i metrics-... z Twoich integracji.
2. **Kibana → Stack Management → Data Views**
   * Jeśli nie masz: **Create data view** →
     + logs-\*-\* (Name: *logs*, Timestamp: @timestamp),
     + metrics-\*-\* (Name: *metrics*, Timestamp: @timestamp),
     + (opcjonalnie) traces-\*-\* (APM), synthetics-\*-\* (Uptime).

**7) Dashboardy „z pudełka” i Discover**

1. **Kibana → Analytics → Discover** → wybierz logs lub metrics i sprawdź napływ danych.
2. **Kibana → Integrations → (np. Windows/System/IIS) → Dashboards** → otwórz gotowe pulpity, zapisz do ulubionych.

**8) Alerty (Rules)**

**Kibana → Alerting (Rules and Connectors) → Create rule**

* **Logs threshold** (np. nieudane logowania):
  + Data view: logs-\*-\*, Filter (KQL): data\_stream.dataset : "winlog.security" AND event.code : 4625
  + Condition: Count > 0 w 5 min → Action: e-mail/Slack (skonfiguruj connector).
* **Metric threshold** (CPU wysokie):
  + Data view: metrics-\*-\*, Metric: Average system.cpu.total.norm.pct > 0.9 przez 5 min.

**9) Retencja (ILM) i szablony indeksów (opcjonalnie)**

**Kibana → Stack Management → Index Lifecycle Policies**

1. Utwórz np. ilm-logs-30d (Delete po 30 dniach), ilm-metrics-14d.  
   **Stack Management → Index Templates → Create template**
2. tmpl-logs dla logs-\* z "index.lifecycle.name": "ilm-logs-30d",  
   tmpl-metrics dla metrics-\* z "index.lifecycle.name": "ilm-metrics-14d".

Integracje mają własne domyślne polityki; powyższe przydaje się, gdy chcesz je **nadpisać** globalnie.

**10) Uprawnienia**

**Kibana → Stack Management → Roles → Create role**

* logs-\*, metrics-\* → read + view\_index\_metadata.
* Przyznaj dostęp do odpowiednich **Spaces** (Discover/Dashboards/Alerts).  
  **Users** → przypisz rolę.

**11) Uptime/Synthetics (jeśli potrzebujesz)**

* **Integrations → Synthetics/Uptime** → *Add monitors*.
* Dla środowisk wewnętrznych ustaw **Private locations** (Fleet Server pełni tu rolę kontrolera; monitory uruchamiasz z hostów-lokacji).
* Zweryfikuj dane w **Uptime** i strumieniach synthetics-\*.

**12) Kontrola stanu i skalowanie**

* **Fleet → Agents**: patrz na **Upgrade available**, **Unhealthy**, **Offline**.
* **Fleet → Settings → Fleet Server hosts**: dodaj drugi/third URL dla HA (lub LB URL).
* W razie zwiększenia ruchu (np. APM/Synthetics) dołóż **kolejny Fleet Server** i dopisz jego URL.