**Uwaga o pakietach integracji (air-gap):** aby potem klikać integracje w Fleet (dashboardy, parsowanie, itp.), Kibana musi mieć dostęp do **Elastic Package Registry (EPR)**. W środowisku offline przygotuj **wewnętrzny EPR** lub proxy i wskaż go w *Kibana → Fleet → Settings → Download sources*. Sam **Fleet Server** uruchomisz i bez tego, ale integracje będą czekały na paczki.

**0) Wymagania i założenia**

* Windows Server (uruchamiasz PowerShell **jako Administrator**).
* Łączność do:
  + **Elasticsearch** (HTTPS/9200),
  + **Kibany** (HTTPS/5601) — do konfiguracji Fleet,
  + Host Fleet Server będzie nasłuchiwał na **8220/TCP** (otwórz w zaporze).
* Certyfikaty:
  + **CA** Twojej organizacji (np. org-ca.crt) — ufa mu Elasticsearch i (opcjonalnie) EPR.
  + **Certyfikat serwera dla Fleet Servera** (**CN/SAN = FQDN Fleet Servera**, np. fleet.internal.local) + **klucz prywatny** (fleet.crt, fleet.key w PEM).
* **ZIP Elastic Agent (windows-x86\_64)** przeniesiony offline na serwer.
* **Service token dla Fleet Servera** oraz **ID polityki Fleet Server** (kroki w §1).

**1) Przygotowanie po stronie Kibany/Elastica (na stacji z dostępem do Kibany)**

1. **Utwórz politykę dla Fleet Servera**  
   Kibana → *Fleet* → *Agent policies* → *Create agent policy*
   * Nazwa: Fleet Server policy
   * (Opcj.) dodaj integrację **System/Windows** (zbiera metryki/logi z hosta Fleet Server).
   * Zanotuj **Policy ID** (widoczne w szczegółach polityki).
2. **Zdefiniuj adres(y) Fleet Servera dla agentów**  
   Kibana → *Fleet* → *Settings* → *Fleet Server hosts* → *Add host*
   * Wpisz np.: https://fleet.internal.local:8220
   * Zapisz.
3. **Utwórz service token dla Fleet Servera**  
   W Kibanie → *Dev Tools* (lub na węźle ES przez CLI), wywołaj:
4. POST /\_security/service/elastic/fleet-server/credential/token/my-fleet-server

Zanotuj wartość value → to **SERVICE\_TOKEN** dla instalatora.

1. *(Air-gap, jeśli używasz wewnętrznego EPR)*  
   Kibana → *Fleet* → *Settings* → sekcja *Download sources*
   * Dodaj URL do **wewnętrznego EPR** (HTTPS), w razie potrzeby dodaj jego CA.
   * (Opcj.) włącz *Only allow default source packages that are signed by Elastic* zgodnie z polityką bezpieczeństwa.

**2) Pliki na serwerze (offline)**

Załóżmy, że ZIP i certy trzymamy w C:\Elastic\elastic-agent\.

# 2.1 Katalogi i rozpakowanie ZIP

New-Item -ItemType Directory -Force -Path C:\Elastic\elastic-agent | Out-Null

Expand-Archive -Path C:\Elastic\elastic-agent-<wersja>-windows-x86\_64.zip `

-DestinationPath C:\Elastic\elastic-agent -Force

Set-Location C:\Elastic\elastic-agent

# 2.2 Katalog na certyfikaty

New-Item -ItemType Directory -Force -Path .\certs | Out-Null

Copy-Item C:\ścieżka\do\org-ca.crt .\certs\ca.crt

Copy-Item C:\ścieżka\do\fleet.crt .\certs\fleet.crt

Copy-Item C:\ścieżka\do\fleet.key .\certs\fleet.key

**Ważne:** fleet.crt musi mieć w **SAN** (albo CN) FQDN, pod którym agenci będą się łączyć (np. fleet.internal.local). Klucz fleet.key w **PEM** (nie PFX).

**3) Otwórz port 8220 w zaporze Windows**

New-NetFirewallRule -DisplayName "Elastic Fleet Server 8220" `

-Direction Inbound -Protocol TCP -LocalPort 8220 -Action Allow

**4) Instalacja Elastic Agenta jako Fleet Server**

Ustal zmienne (dopasuj do środowiska):

$ES\_URL = "https://es.internal.local:9200"

$FLEET\_HOST = "0.0.0.0" # lub konkretny interfejs

$FLEET\_PORT = "8220"

$SERVICE\_TOKEN = "<SERVICE\_TOKEN\_Z\_KIBANY>"

$POLICY\_ID = "<POLICY\_ID\_FLEET\_SERVER>"

$CA\_PATH = "C:\Elastic\elastic-agent\certs\ca.crt"

$FS\_CERT = "C:\Elastic\elastic-agent\certs\fleet.crt"

$FS\_KEY = "C:\Elastic\elastic-agent\certs\fleet.key"

**Instalacja (jedna linia z backtickami dla czytelności):**

.\elastic-agent.exe install `

--fleet-server-es=$ES\_URL `

--fleet-server-service-token=$SERVICE\_TOKEN `

--fleet-server-policy=$POLICY\_ID `

--certificate-authorities="$CA\_PATH" `

--fleet-server-cert="$FS\_CERT" `

--fleet-server-cert-key="$FS\_KEY" `

--fleet-server-host=$FLEET\_HOST `

--fleet-server-port=$FLEET\_PORT `

--background

Co robią kluczowe parametry:

* --fleet-server-es – URL Elasticsearch (z TLS).
* --certificate-authorities – CA, którą Agent ufa **ES** (i opcj. EPR przez Kibana proxy).
* --fleet-server-cert/--fleet-server-cert-key – **cert/klucz serwera** dla **8220/TCP** (to na ten cert będą ufały zwykłe agenty).
* --fleet-server-service-token – uprawnienia Fleet Server → Elasticsearch.
* --fleet-server-policy – przypięcie instancji do stworzonej polityki „Fleet Server policy”.
* --fleet-server-host/port – interfejs i port nasłuchu.

**Weryfikacja:**

.\elastic-agent.exe status

sc query "Elastic Agent"

**5) Rejestracja zwykłych agentów (po udanym starcie Fleet Server)**

Na **innych hostach** (lub nawet na tym samym — jako agent danych w tej samej instancji), w Kibanie → *Fleet* → *Agents* → *Add agent*:

* Wybierz politykę (np. Windows Base policy),
* Skopiuj **Enrollment token** i komendę instalacji dla Windows,
* Na hoście uruchom:
* .\elastic-agent.exe install `
* --url=https://fleet.internal.local:8220 `
* --enrollment-token=<ENROLLMENT\_TOKEN> `
* --certificate-authorities="C:\Elastic\elastic-agent\certs\ca.crt" `
* --background

**Uwaga:** Na **jednym** hoście działa **jedna usługa Elastic Agent**. Ten sam proces może pełnić rolę **Fleet Server** i **zbieracza danych** — dodaj integracje (System/Windows itp.) do **Fleet Server policy**.

**6) Diagnostyka**

* **Logi Fleet Server/Agenta (na hoście):**  
  C:\Program Files\Elastic\Agent\data\logs\elastic-agent.log
* **Szybki health-check:**
* Test-NetConnection es.internal.local -Port 9200
* Test-NetConnection fleet.internal.local -Port 8220
* **Typowe problemy:**
  + *TLS x509 host mismatch* → FQDN użyty przez agentów musi być w SAN certyfikatu fleet.crt.
  + *401/403* przy instalacji → zły **service token** lub brak ról; wygeneruj nowy.
  + *Agenci nie pobierają integracji (pending)* → Kibana nie ma dostępu do paczek; skonfiguruj **wewnętrzny EPR** w *Fleet → Settings → Download sources*.
  + *„Nie widzę Fleet Servera w Kibanie”* → sprawdź elastic-agent.log; upewnij się, że polityka o ID $POLICY\_ID istnieje i ES jest osiągalny.

**7) Utrzymanie**

* **Upgrade (offline):** zatrzymaj usługę, podmień binaria z nowego ZIP, uruchom usługę.
* **Zmiany polityk/integracji:** od teraz robisz **w Kibanie → Fleet → Policies** (agenci pobiorą z Fleet Server).
* **HA/skalowanie:** możesz postawić **kolejne Fleet Servery** (inne hosty) i dodać ich URL-e w *Fleet → Settings → Fleet Server hosts* lub użyć **load balancera** przed 8220.

**Jeśli wolisz bez żadnych zmiennych — jedna komenda**

Wstaw swoje wartości i uruchom w PowerShell (Admin):

cd C:\Elastic\elastic-agent

.\elastic-agent.exe install `

--fleet-server-es=https://es.internal.local:9200 `

--fleet-server-service-token=AAAABBBBCCCCDDDD `

--fleet-server-policy=0f2a3b4c-...-9d8e7f6a `

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

--fleet-server-cert="C:\Elastic\elastic-agent\certs\fleet.crt" `

--fleet-server-cert-key="C:\Elastic\elastic-agent\certs\fleet.key" `

--fleet-server-host=0.0.0.0 `

--fleet-server-port=8220 `

--background

To wszystko. Żadne zmienne nie są wymagane.