**Offline (Windows, bez Dockera): Fleet Server + prywatny EPR + konfiguracja w Kibanie**

**0) Założenia, zmienne i przygotowanie offline**

**Zmienne (ustaw pod siebie; użyj w poleceniach poniżej):**

* STACK\_VER – wersja agenta (np. 8.13.2; zmień jeśli inna)
* ES\_URL – adres Elasticsearch, np. https://es.moje.lan:9200 **lub** http://es.moje.lan:9200
* KIBANA\_URL – adres Kibany, np. https://kibana.moje.lan:5601
* FLEET\_HOST – adres/hostname serwera Windows, na którym uruchomisz Fleet Server, np. fleet01.moje.lan
* FLEET\_PORT – port Fleet Server, domyślnie 8220
* EPR\_HOST i EPR\_PORT – host/port prywatnego EPR (Package Registry), np. fleet01.moje.lan:8080

**Co przygotować na *komputerze z Internetem* (przenieś potem na serwer offline np. pendrive’em):**

1. **Elastic Agent (ZIP, Windows x86\_64)**  
   Plik: elastic-agent-<STACK\_VER>-windows-x86\_64.zip
2. **Paczki integracji (ZIP) do EPR / lub do późniejszego „uploadu” do Kibany**  
   Na start minimum:
   * elastic\_agent-<ver>.zip (pakiet bazowy)
   * fleet\_server-<ver>.zip (aby Fleet Server był rozpoznany)
   * system-<ver>.zip (monitoring systemu)
   * windows-<ver>.zip (eventlog, perfmon itd.)

**Skąd pobrać wersje paczek:**  
Na maszynie online można sprawdzić dostępne wersje przez EPR (np. https://epr.elastic.co/search?package=windows&kibana.version=<twoja\_wersja>), a następnie pobrać ZIP danej paczki (/epr/windows/windows-<ver>.zip). API EPR jest opisane w repozytorium „package-registry”. ([okteto.com](https://www.okteto.com/docs/self-hosted/manage/air-gapped/?utm_source=chatgpt.com), [GitHub](https://github.com/elastic/package-registry))

1. (Opcjonalnie) **Go + Mage** (jeśli chcesz zbudować binarkę EPR dla Windows samodzielnie – sekcja 2A).

**1) Instalacja Elastic Agent jako Fleet Server (Windows, offline, bez Dockera)**

Ten rozdział zakłada, że **Fleet Server** będzie działał na Windowsie i będzie się łączył do ES po ES\_URL. Ponieważ nie używasz CA, użyjemy trybów --insecure / --fleet-server-es-insecure, zgodnie z dokumentacją poleceń agenta. ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))

**1.1. Skopiuj pliki i otwórz port w zaporze**

1. Skopiuj na serwer Windows:
   * elastic-agent-<STACK\_VER>-windows-x86\_64.zip → np. do C:\Install\elastic-agent.zip
2. PowerShell (administrator):

$STACK\_VER = "8.13.2" # zmień jeśli inna

$ES\_URL = "https://es.moje.lan:9200" # lub http://...

$FLEET\_HOST= "fleet01.moje.lan"

$FLEET\_PORT= 8220

New-Item -ItemType Directory -Force -Path "C:\Elastic\Agent" | Out-Null

Expand-Archive "C:\Install\elastic-agent.zip" "C:\Elastic\Agent" -Force

# Otwórz port 8220 (Fleet Server) w Windows Firewall:

netsh advfirewall firewall add rule name="Fleet Server 8220" dir=in action=allow protocol=TCP localport=$FLEET\_PORT

**1.2. Przygotuj tokeny i politykę w Kibanie (ona może być online lub wewnętrzna)**

Wejdź do **Kibana → Management → Fleet** i kliknij **Fleet Settings / Add Fleet Server** („Dodaj Fleet Server”). Kreator:

* utworzy **Fleet Server policy** (politykę dla hosta Fleet Server),
* **wygeneruje service token** dla Fleet Server (lub zrób to z API),
* poda gotowy przykład polecenia elastic-agent install.

Alternatywnie możesz tworzyć tokeny / enrollment keys i polityki przez Fleet API (REST), m.in. **service tokeny** i **enrollment tokens**. Zob. „Kibana Fleet APIs” → „Fleet service tokens”, „Fleet enrollment API keys”, „Install a package by upload”, „Update settings/outputs”. ([Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-agent-policies-delete))

**Uwaga o tokenach i trybie bez CA:**

* Do **Fleet Server** używamy **service tokenu** (--fleet-server-service-token), a do agentów końcowych zwykle **enrollment tokenu**. Mechanika tokenów i API-keys jest opisana w dokumentacji Fleet. ([Elastic](https://www.elastic.co/docs/reference/fleet/fleet-enrollment-tokens?utm_source=chatgpt.com))

**1.3. Instalacja agenta jako usługi z włączonym Fleet Server**

W PowerShell (administrator) – **wstaw tokeny/politykę z kreatora**:

# Przykład: HTTPS do ES bez zaufanego CA

# - --fleet-server-es-insecure : wyłącza weryfikację certyfikatu po stronie ES (albo pozwala na HTTP)

# - bez --url/--enrollment-token dla Fleet Server (używamy service tokenu)

# - jeśli NIE podasz --fleet-server-cert/--fleet-server-cert-key, agent wygeneruje samopodpisany cert z hostname;

# klienci (inne agenty) będą się do niego wpisywać z --insecure (patrz dokumentacja).

$SERVICE\_TOKEN = "<WSTAW\_FLEET\_SERVER\_SERVICE\_TOKEN>"

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

Set-Location "C:\Elastic\Agent\elastic-agent-$STACK\_VER-windows-x86\_64"

.\elastic-agent.exe install `

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

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

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

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

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

--fleet-server-es-insecure # pozwala na HTTP albo ignoruje weryfikację łańcucha certów do ES

**Dlaczego te flagi?**

* --fleet-server-es-insecure — pozwala Fleet Serverowi łączyć się z ES po HTTP **albo** po HTTPS bez weryfikacji łańcucha (Twoje „bez CA”).
* Jeśli agenta będziesz wpisywać do Fleet Servera z samopodpisanym certem (autogenerowanym), **agenty końcowe** podczas enroll muszą użyć --insecure. To wynika bezpośrednio z **Elastic Agent command reference**. ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))

**Tip (częsty błąd):** samo --insecure dotyczy połączenia **Agenta z Fleet Serverem**; aby Fleet Server akceptował **samopodpisany/HTTP** po stronie **Elasticsearch**, potrzebny jest **--fleet-server-es-insecure** *oraz* w **Fleet Output** należy ustawić weryfikację TLS na „none” (patrz rozdz. 3). ([Elastic](https://www.elastic.co/docs/troubleshoot/ingest/fleet/common-problems?utm_source=chatgpt.com))

Po instalacji sprawdź status:

# Status usługi

Get-Service elastic-agent

# Logi:

Get-Content "C:\Program Files\Elastic\Agent\data\elastic-agent-\*\logs\elastic-agent.ndjson" -Tail 200 -Wait

**2) Prywatny Elastic Package Registry (EPR) na Windows, offline, bez Dockera**

Masz dwie stabilne drogi:

**2A) EPR jako binarka „package-registry.exe” (Windows, bez Dockera)**

1. **Zbuduj EPR na maszynie z Internetem** (Windows lub Linux):
   * Zainstaluj **Go** i **Mage**.
   * Sklonuj repozytorium: git clone https://github.com/elastic/package-registry.git
   * Zbuduj: mage build → powinien powstać build/package-registry.exe  
     (Repo opisuje też API: /search, /categories, /package/<name>/<version>, /epr/....) ([GitHub](https://github.com/elastic/package-registry))
2. **Przygotuj „magazyn” paczek** (na maszynie online):
   * Utwórz katalog np. .\epr-storage\
   * Wrzuć do niego ZIP-y integracji, które pobrałeś w punkcie 0 (np. windows-<ver>.zip, system-<ver>.zip, fleet\_server-<ver>.zip, elastic\_agent-<ver>.zip).
3. **Skopiuj na serwer offline**:
   * package-registry.exe → C:\EPR\package-registry.exe
   * katalog paczek → C:\EPR\storage\
   * plik konfiguracyjny C:\EPR\config.yml (przykład):

server:

host: "0.0.0.0"

port: 8080

# file-system indexer: EPR będzie serwował paczki wprost z katalogu

paths:

- "C:\\EPR\\storage"

cache:

time: "10m"

1. **Uruchom EPR** (PowerShell administrator):

# Reguła zapory dla portu EPR (8080)

netsh advfirewall firewall add rule name="EPR 8080" dir=in action=allow protocol=TCP localport=8080

# Start w oknie (do testu):

Set-Location C:\EPR

.\package-registry.exe -c C:\EPR\config.yml

Jeśli chcesz, aby EPR startował po reboocie, najprościej utwórz **Zadanie Harmonogramu Zadań** („At startup”, „Run with highest privileges”) uruchamiające package-registry.exe -c C:\EPR\config.yml. (Aplikacja nie jest natywną usługą Windows – sc.exe create nie zadziała bez wrappera typu NSSM).

1. **Test**: z innego hosta w sieci otwórz  
   http://<EPR\_HOST>:8080/search?package=windows → powinieneś zobaczyć metadane paczki. API EPR jest opisane w repo (sekcja „API”). ([GitHub](https://github.com/elastic/package-registry))

**2B) Bez EPR: wgrywanie paczek bezpośrednio do Kibany (air-gapped)**

Od Kibany 8.x możesz **zainstalować paczkę z pliku ZIP** przez API (nie potrzebujesz EPR). To bywa najprostsze, jeśli **nie możesz** zmienić kibana.yml. Endpoint: ***Install a package by upload***. ([Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-epm-packages" \o ))

**Przykład (na maszynie, która widzi Kibanę):**

curl -u user:password -k \

-H "kbn-xsrf: true" \

-F "file=@windows-<ver>.zip" \

https://kibana.moje.lan:5601/api/fleet/epm/packages

W ten sposób „wszczepisz” potrzebne paczki (windows, system, elastic\_agent, fleet\_server) do instancji Kibany – bez konieczności uruchamiania EPR.

**3) Wymagane działania w Kibanie, aby dane zaczęły płynąć (bez CA)**

Ten rozdział jest kluczowy przy pracy „bez CA”. Dwa kroki: **(A) Fleet Settings/Outputs** i **(B) Integracje/Polityki**.

**3A) Fleet → Settings**

1. **Fleet Server hosts**  
   Dodaj hosta: https://<FLEET\_HOST>:8220 (jeśli Fleet Server działa na HTTPS z certem) **albo** http://<FLEET\_HOST>:8220 (jeśli akceptujesz HTTP w LAN).  
   Upewnij się, że adres jest osiągalny z hostów, gdzie zainstalujesz agenta.
2. **Outputs** (domyślne wyjście dla Integrations i Monitoring)
   * Dodaj/edytuj **Elasticsearch Output** wskazujący na ES\_URL.
   * W sekcji **SSL / Advanced YAML** ustaw **wyłączenie weryfikacji** certyfikatu (bo nie masz CA):
   * ssl.verification\_mode: none

To wymagane przy samopodpisanych certach lub HTTP i jest wskazane w oficjalnych poradnikach/FAQ. ([Elastic](https://www.elastic.co/docs/troubleshoot/ingest/fleet/common-problems?utm_source=chatgpt.com), [Discuss the Elastic Stack](https://discuss.elastic.co/t/is-there-a-way-to-ease-installing-fleet-server-to-a-elasticsearch-server-secured-by-self-signed-certificate/281583?utm_source=chatgpt.com))

1. **(Opcjonalnie) Agent binary download sources**  
   Jeśli chcesz umożliwić **aktualizacje agentów w trybie air-gapped**, hostuj ZIP-y agenta na swoim http(s) i dodaj **Download source** przez API „Elastic Agent binary download sources” (GET/POST/PUT/DELETE) – wtedy Fleet nie będzie korzystał z Internetu. ([Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-agent-policies-delete))
2. **(Jeśli używasz EPR 2A)** – wskaż Kibanie prywatny rejestr:  
   W pliku kibana.yml (na hoście Kibany):
3. xpack.fleet.registryUrl: "http://<EPR\_HOST>:<EPR\_PORT>"

Zrestartuj Kibanę. To oficjalny sposób na środowiska air-gapped. ([Elastic](https://www.elastic.co/docs/reference/fleet/air-gapped?utm_source=chatgpt.com" \o "Air-gapped environments | Elastic Docs), [Elastic Docs](https://elastic.ac.cn/guide/en/fleet/current/air-gapped.html?utm_source=chatgpt.com))

**Jeśli nie możesz edytować kibana.yml**, skorzystaj z wariantu **2B** (upload ZIP paczek do Kibany) – nie wymaga zmiany registryUrl. ([Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-epm-packages))

**3B) Fleet → Integrations & Policies (polityki)**

1. **Fleet Server policy**  
   Tworzy ją kreator „Add Fleet Server” – *nic nie dopinaj* tu poza integracją „Fleet Server”.
2. **Default (albo nowa) Agent Policy** dla hostów Windows
   * **Add integration**:
     + Windows (eventlog, security, sysmon – jeśli używasz),
     + System (CPU, mem, disk, system logs).
   * **Save & deploy**.
3. **Enrollment agenta końcowego (Windows)**  
   Na hostach Windows, które mają wysyłać dane:
   * skopiuj ZIP agenta,
   * **Add agent** w Kibanie → wybierz tę politykę, skopiuj polecenie **elastic-agent install ... --url=https://<FLEET\_HOST>:8220 --enrollment-token=<...>**
   * **ponieważ Fleet Server ma cert samopodpisany / brak CA**, **dodaj --insecure** przy enrollu (zob. command reference). ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))
4. **Weryfikacja**
   * Fleet → **Agents**: oba byty powinny mieć **Healthy** (najpierw Fleet Server, potem agenty).
   * W Discover/Logs/hosts zobaczysz indeksy logs-... i metrics-....

**Najczęstsze problemy (bez CA):**

* **x509: cannot validate certificate** – przy samopodpisanych certach:
  + Fleet Server → ES: dodaj --fleet-server-es-insecure przy instalacji Fleet Server. ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))
  + Agenty → Fleet Server: do komendy **enroll** dodaj --insecure. ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))
  + W **Output (Fleet Settings)** dodaj ssl.verification\_mode: none. ([Elastic](https://www.elastic.co/docs/troubleshoot/ingest/fleet/common-problems?utm_source=chatgpt.com))
* **Brak danych po integracji** – sprawdź **Fleet → Settings → Outputs** (adresy, YAML, spacje/format). To częsty drobiazg. ([gooksu.com](https://www.gooksu.com/2022/06/elastic-fleet-server-elastic-agent-common-troubleshooting/?utm_source=chatgpt.com))

**4) Alternatywa dla EPR: „upload paczek” do Kibany (air-gapped, *bez* zmian kibana.yml)**

Jeżeli nie chcesz/nie możesz stawiać EPR:

1. Zainstaluj paczki („windows”, „system”, „elastic\_agent”, „fleet\_server”) przez **Kibana API** POST /api/fleet/epm/packages z parametrem file=@...zip.  
   Endpoint: **Install a package by upload**. ([Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-epm-packages))
2. W Integrations → zobaczysz paczki jako „Installed”; twórz polityki jak w 3B.

**5) Checklista sieciowo-systemowa**

* **Porty**:
  + Fleet Server: TCP **8220** (inbound z sieci)
  + Do ES: TCP **9200** (outbound z hosta Fleet Server)
  + Do Kibany (UI i API Fleet): TCP **5601** (z przeglądarki admina / automatyzacji)
  + EPR (jeśli używany): TCP **8080** (inbound z hosta Kibany)
* **Uprawnienia**: PowerShell „Run as Administrator”.
* **Ścieżki/logi (Windows)** – agenta:  
  C:\Program Files\Elastic\Agent\... (layout i pliki zgodnie z dokumentacją; logi w data\elastic-agent-\*\logs\...). ([DevOps School](https://www.devopsschool.com/blog/elastic-agent-installation-configuration/?utm_source=chatgpt.com))

**6) Bezpieczeństwo (ważne)**

* --insecure i ssl.verification\_mode: none **obniżają** poziom bezpieczeństwa (brak weryfikacji certów). To jest dopuszczalne w odciętym od Internetu labie/PoC, ale **zalecane** jest później wdrożenie własnego CA i prawidłowych certyfikatów oraz usunięcie tych wyjątków. (Flagi i konsekwencje opisane w oficjalnej dokumentacji agenta). ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))

**Źródła (kluczowe fragmenty)**

* **Elastic Agent – command reference**: składnia install/enroll, --fleet-server-es-insecure, --insecure, przykłady. ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))
* **Kibana Fleet APIs**: upload paczek (EPM), outputs, fleet settings, service/enrollment tokens, agent download sources. ([Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-agent-policies-delete))
* **Air-gapped / registryUrl**: konfiguracja prywatnego rejestru paczek (xpack.fleet.registryUrl) i praca bez Internetu. ([Elastic](https://www.elastic.co/docs/reference/fleet/air-gapped?utm_source=chatgpt.com), [Elastic Docs](https://elastic.ac.cn/guide/en/fleet/current/air-gapped.html?utm_source=chatgpt.com))
* **Package Registry (EPR) – repo i API**: sposób działania, endpointy /search, /package, /epr/.... ([GitHub](https://github.com/elastic/package-registry))
* **Weryfikacja TLS „none” w Output** (częsty wymóg przy braku CA). ([Elastic](https://www.elastic.co/docs/troubleshoot/ingest/fleet/common-problems?utm_source=chatgpt.com), [Discuss the Elastic Stack](https://discuss.elastic.co/t/is-there-a-way-to-ease-installing-fleet-server-to-a-elasticsearch-server-secured-by-self-signed-certificate/281583?utm_source=chatgpt.com))

**Krótki plan w punktach (TL;DR)**

1. **Fleet Server (Windows):** rozpakuj ZIP agenta → elastic-agent.exe install ... --fleet-server-es=<ES\_URL> --fleet-server-service-token=<token> --fleet-server-policy=<id> --fleet-server-port=8220 --fleet-server-es-insecure. ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))
2. **EPR (opcjonalnie):** uruchom package-registry.exe z config.yml i katalogiem paczek; albo **wgraj paczki ZIP do Kibany** przez POST /api/fleet/epm/packages. ([GitHub](https://github.com/elastic/package-registry), [Elastic](https://www.elastic.co/docs/api/doc/kibana/operation/operation-post-fleet-epm-packages))
3. **Kibana / Fleet Settings:** ustaw **Outputs** na ES\_URL i w **Advanced YAML** dodaj ssl.verification\_mode: none; dodaj **Fleet Server host** http(s)://<FLEET\_HOST>:8220; jeśli używasz EPR – ustaw xpack.fleet.registryUrl. ([Elastic](https://www.elastic.co/docs/troubleshoot/ingest/fleet/common-problems?utm_source=chatgpt.com))
4. **Polityki & Integracje:** w polityce dla Windows dodaj Windows + System; **Add agent** na hostach – komenda enroll z --insecure (bo Fleet Server ma samopodpisany cert). ([Elastic](https://www.elastic.co/docs/reference/fleet/agent-command-reference))