**Offline (Windows, bez Dockera, bez EPR): Fleet Server + upload paczek do Kibany + konfiguracja z CA fingerprint**

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

**Zmienne (dopasuj i wklej do poleceń):**

* STACK\_VER – wersja Elastic Agent, np. 8.13.2
* ES\_URL – URL Elasticsearch, np. https://es.twoja.lan:9200 (jeśli ES ma TLS) **lub** http://es.twoja.lan:9200 (jeśli bez TLS)
* KIBANA\_URL – URL Kibany, np. https://kibana.twoja.lan:5601
* FLEET\_HOST / FLEET\_PORT – host/port Fleet Servera, np. fleet01.twoja.lan / 8220
* ES\_CA\_FP – **SHA-256 fingerprint CA Elasticsearch (HEX, bez dwukropków)** — weź go z kreatora **Fleet → Add Fleet Server** w Kibanie (sekcja 2.2)

**Co przygotować na *maszynie z Internetem* (przenieś na serwer offline, np. pendrive):**

1. elastic-agent-<STACK\_VER>-windows-x86\_64.zip
2. Paczki integracji w ZIP (minimum):
   * elastic\_agent-<ver>.zip
   * fleet\_server-<ver>.zip
   * system-<ver>.zip
   * windows-<ver>.zip  
     *(jeśli planujesz inne integracje, pobierz ich ZIP-y też)*

Uwaga: Nie używamy żadnego CA-pliku. Do połączeń **Fleet Server → Elasticsearch** oraz **Agent → Elasticsearch** wykorzystamy **CA fingerprint**.  
Jeśli **Elasticsearch działa po HTTP** (bez TLS), pominiesz krok z fingerprintem i odpowiednie flagi (wskazane niżej).

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

**1.1. Rozpakowanie i firewall**

PowerShell (uruchom **jako Administrator**):

$STACK\_VER = "8.13.2"

$ES\_URL = "https://es.twoja.lan:9200"

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

$FLEET\_PORT= 8220

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

Expand-Archive "C:\Install\elastic-agent-$STACK\_VER-windows-x86\_64.zip" "C:\Elastic\Agent" -Force

# Otwórz port Fleet Server w zaporze

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

**1.2. Token i polityka Fleet Server + fingerprint CA (z Kibany)**

W Kibanie:

* **Management → Fleet → Agents → Add Fleet Server**
* Kreator utworzy **Fleet Server policy** i **service token** (zapisz je).
* **Skopiuj „Elasticsearch CA trusted fingerprint”** (HEX SHA-256, bez dwukropków). To będzie Twój ES\_CA\_FP.

**1.3. Instalacja Fleet Servera jako usługi (z fingerprintem)**

PowerShell (Administrator) — wstaw swoje wartości:

$SERVICE\_TOKEN = "<FLEET\_SERVER\_SERVICE\_TOKEN\_Z\_KIBANY>"

$POLICY\_ID = "<FLEET\_SERVER\_POLICY\_ID\_Z\_KIBANY>"

$ES\_CA\_FP = "<HEX\_SHA256\_BEZ\_DWUKROPKOW>"

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

# Wariant z TLS na Elasticsearch (zalecany):

.\elastic-agent.exe install `

--url="https://$FLEET\_HOST:$FLEET\_PORT" `

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

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

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

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

--fleet-server-es-ca-trusted-fingerprint="$ES\_CA\_FP"

# Jeśli Elasticsearch działa po HTTP (bez TLS) -> użyj zamiast powyższego:

# .\elastic-agent.exe install `

# --url="https://$FLEET\_HOST:$FLEET\_PORT" `

# --fleet-server-es="http://es.twoja.lan:9200" `

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

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

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

Jeśli **nie masz własnego, zaufanego certyfikatu dla samego Fleet Servera**, agent wygeneruje samopodpisany. Wtedy **podczas enrollu agentów końcowych** użyjesz --insecure (sekcja 3.3). To dotyczy *tylko* połączenia **Agent → Fleet Server**. Połączenie do **Elasticsearch** będzie weryfikowane fingerprintem (bez CA-pliku).

**Szybka weryfikacja:**

Get-Service elastic-agent

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

**2) Kibana (Fleet) – konfiguracja bez EPR**

**2.1. Wgraj paczki integracji ZIP do Kibany (air-gapped)**

Na komputerze, który widzi Kibana (może to być ten sam serwer), użyj **curl.exe** (na Windows wywołuj curl.exe, nie alias PowerShella):

# przykład dla system

curl.exe -u user:password -k ^

-H "kbn-xsrf: true" ^

-F "file=@C:\Install\packages\system-<ver>.zip" ^

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

# windows

curl.exe -u user:password -k ^

-H "kbn-xsrf: true" ^

-F "file=@C:\Install\packages\windows-<ver>.zip" ^

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

# fleet\_server

curl.exe -u user:password -k ^

-H "kbn-xsrf: true" ^

-F "file=@C:\Install\packages\fleet\_server-<ver>.zip" ^

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

# elastic\_agent

curl.exe -u user:password -k ^

-H "kbn-xsrf: true" ^

-F "file=@C:\Install\packages\elastic\_agent-<ver>.zip" ^

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

-k pomija weryfikację certyfikatu przy *połączeniu do Kibany* (bo nie używasz CA).  
Po udanym uploadzie paczki pojawią się jako **Installed** w **Fleet → Integrations**.

**2.2. Fleet → Settings**

* **Fleet Server hosts**: dodaj https://<FLEET\_HOST>:8220
* **Outputs → Default Elasticsearch output**:
  + Host: ES\_URL
  + Pole **Elasticsearch CA trusted fingerprint**: wklej **ES\_CA\_FP** (ten sam co w 1.3)  
    Dzięki temu **wszystkie agenty** będą weryfikowały certyfikat ES po fingerprint’cie (bez CA-pliku).

*(Jeśli ES jest po HTTP — podaj http://... i fingerprint nie jest potrzebny.)*

**3) Polityki, integracje i enroll agentów końcowych (Windows)**

**3.1. Fleet Server policy**

* Zostaw integrację **Fleet Server** w polityce Fleet Servera (utworzonej w kreatorze). Nic więcej tu nie dopinaj.

**3.2. Polityka dla hostów Windows**

* **Fleet → Agent policies → Create policy** (np. „Windows-Servers”)
* **Add integration**:
  + Windows (Event Log, ewentualnie Security/Sysmon jeśli używasz),
  + System (CPU, RAM, disk, system logs).
* **Save & deploy**

**3.3. Enroll agentów Windows (na hostach, które mają wysyłać dane)**

Na każdym hoście Windows:

1. Skopiuj ZIP agenta i rozpakuj.
2. W Kibanie → **Fleet → Agents → Add agent** → wybierz politykę „Windows-Servers” i skopiuj komendę install.

**Wariant bez zaufanego certu Fleet Servera (najszybszy):**

# PowerShell jako Administrator, w katalogu rozpakowanego agenta

.\elastic-agent.exe install `

--url=https://<FLEET\_HOST>:8220 `

--enrollment-token <ENROLLMENT\_TOKEN\_Z\_KIBANY> `

--insecure

--insecure jest tu tylko po to, by agent *zaufał samopodpisanemu certowi Fleet Servera*.  
Połączenia do **Elasticsearch** będą już weryfikowane fingerprintem ustawionym w **Outputs**.

**Wariant „PRO” (bez --insecure):**

* Wystaw zaufany cert/CA dla **Fleet Servera** i podaj go agentowi:

.\elastic-agent.exe install `

--url=https://<FLEET\_HOST>:8220 `

--enrollment-token <ENROLLMENT\_TOKEN> `

--certificate-authorities "C:\path\to\fleet-ca.crt"

**4) Weryfikacja i diagnostyka**

* **Fleet → Agents**: najpierw Healthy dla Fleet Servera, potem dla agentów Windows.
* **Observability / Discover**: pojawią się indeksy logs-\* i metrics-\*.
* **Typowe błędy i szybkie fixy:**
  + x509: certificate signed by unknown authority (Fleet Server ↔ ES): sprawdź --fleet-server-es-ca-trusted-fingerprint (HEX bez :).
  + x509 przy **enrolowaniu agenta**: użyj --insecure (jeśli Fleet Server ma samopodpisany cert), albo dostarcz **CA** Fleet Servera (--certificate-authorities).
  + Brak danych: sprawdź **Fleet → Settings → Outputs** (czy jest host ES i fingerprint) oraz czy polityka „Windows-Servers” ma integracje Windows i System.

**Porty do otwarcia (inbound/outbound wg potrzeb):**

* Fleet Server: TCP **8220** (inbound dla agentów)
* Elasticsearch: TCP **9200** (outbound z Fleet Servera)
* Kibana: TCP **5601** (z przeglądarki admina / na upload ZIP)

**5) TL;DR (skrót)**

1. **Fleet Server (Windows)** – z fingerprintem:

.\elastic-agent.exe install `

--url=https://<FLEET\_HOST>:8220 `

--fleet-server-es=<ES\_URL> `

--fleet-server-service-token=<SERVICE\_TOKEN> `

--fleet-server-policy=<POLICY\_ID> `

--fleet-server-port=8220 `

--fleet-server-es-ca-trusted-fingerprint=<ES\_CA\_FP>

1. **Kibana** – **upload ZIP** paczek (system, windows, fleet\_server, elastic\_agent) przez:

curl.exe -u user:password -k -H "kbn-xsrf: true" -F "file=@<pakiet>.zip" https://kibana.twoja.lan:5601/api/fleet/epm/packages

1. **Fleet → Settings → Outputs** – ustaw ES\_URL i **Elasticsearch CA trusted fingerprint = <ES\_CA\_FP>**.
2. **Agenty Windows** – enroll:

# szybki wariant (samopodpisany cert Fleet Servera)

.\elastic-agent.exe install --url=https://<FLEET\_HOST>:8220 --enrollment-token <TOKEN> --insecure