**0) Założenia**

* Windows Server **bez dostępu do Internetu**.
* Łączność do **Elasticsearch (HTTPS/9200)** i (opcjonalnie) do **Kibany (HTTPS/5601)**.
* Masz plik **CA** (lub łańcuch CA), którym podpisane są certy ES/Kibany.
* Instalator: **ZIP Elastic Agent (windows-x86\_64)** skopiowany offline (pendrive/SMB).

**1) Rozpakowanie ZIP i przygotowanie katalogów**

Uruchom **PowerShell jako Administrator**:

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

# Skopiuj ZIP wcześniej na serwer, np. do C:\Elastic\

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

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

Set-Location C:\Elastic\elastic-agent

# Katalog na certyfikat(y) CA

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

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

(Opcjonalnie) weryfikacja sumy:  
Get-FileHash C:\Elastic\elastic-agent-<wersja>-windows-x86\_64.zip -Algorithm SHA256

**2) Konfiguracja Standalone: elastic-agent.yml**

Utwórz plik C:\Elastic\elastic-agent\elastic-agent.yml. **Uwaga:** w YAML na Windows używaj **ukośników /** w ścieżkach.

Minimalny, bezpieczny start (Winlog + metryki systemowe + opcjonalnie logi IIS):

outputs:

default:

type: elasticsearch

hosts: ["https://es.internal.local:9200"]

username: "elastic"

password: "${ES\_PWD}" # hasło trzymamy w keystore (patrz krok 3)

ssl:

certificate\_authorities: ["C:/Elastic/elastic-agent/certs/ca.crt"]

verification\_mode: full # CN/SAN certu musi pasować do hosts

agent:

monitoring:

enabled: true

logs: true

metrics: true

inputs:

# 2.1 Winlogi (zastępuje Winlogbeat)

- type: winlog

use\_output: default

streams:

- winlog.channel: Application

- winlog.channel: Security

- winlog.channel: System

# 2.2 Metryki systemowe (zastępuje Metricbeat/system)

- type: system/metrics

use\_output: default

streams:

- metricset: cpu

period: 10s

- metricset: memory

period: 10s

- metricset: network

period: 10s

- metricset: filesystem

period: 1m

# 2.3 (Opcjonalnie) logi IIS z plików

- type: logfile

use\_output: default

vars:

paths:

- "C:/inetpub/logs/LogFiles/W3SVC\*/u\_ex\*.log"

preserve\_original\_event: true

data\_stream:

dataset: iis.access

namespace: default

Chcesz inne źródła (np. dodatkowe kanały winlog, własne ścieżki logów, SQL/MSSQL metryki)? Dorzucimy kolejne inputs – zacznij od powyższego, upewnij się, że dane płyną.

**3) Keystore: sekrety poza YAML (polecane)**

Zamiast trzymać hasło w pliku, zapisz je w keystore Agenta i używaj ${ES\_PWD}:

# Utworzenie keystore (jeśli nie istnieje)

.\elastic-agent.exe keystore create

# Dodanie hasła do Elasticsearch

$sec = Read-Host -AsSecureString "Podaj hasło do Elasticsearch"

$plain = [Runtime.InteropServices.Marshal]::PtrToStringAuto(

[Runtime.InteropServices.Marshal]::SecureStringToBSTR($sec))

.\elastic-agent.exe keystore add ES\_PWD --stdin <<< $plain

# Podgląd kluczy (nazw) – bez ujawniania wartości

.\elastic-agent.exe keystore list

**4) Instalacja jako usługa i start**

# Instalacja w tle na podstawie lokalnej konfiguracji

.\elastic-agent.exe install -c "C:\Elastic\elastic-agent\elastic-agent.yml" --background

# Weryfikacja działania

.\elastic-agent.exe status

sc query "Elastic Agent"

**Logi Agenta:**  
C:\Program Files\Elastic\Agent\data\logs\elastic-agent.log

**Restart po zmianach YAML:**

Restart-Service "Elastic Agent"

**5) Zapora (Windows Firewall)**

Wyjście z hosta Agenta do:

* **Elasticsearch**: TCP **9200** (HTTPS)

*(Kibana 5601 nie jest endpointem ingest; potrzebna tylko do podglądu danych.)*

Jeśli później uruchomisz dodatkowe wejścia, które **nasłuchują portów** (np. APM intake, syslog odbierany lokalnie), otwórz odpowiednie **przychodzące** reguły dla tych portów.

**6) Weryfikacja w Kibanie**

Na stacji z dostępem do Kibany:

1. **Discover** → data view logs-\*-\* (logi) i metrics-\*-\* (metryki).  
   Jeśli data views nie istnieją, utwórz: logs-\*-\* i metrics-\*-\*.
2. Przykładowe KQL:
   * Winlogi: data\_stream.dataset : "winlog.security" OR "winlog.system" OR "winlog.application"
   * Metryki: data\_stream.dataset : "system.cpu" OR "system.memory" OR "system.network"
   * IIS: data\_stream.dataset : "iis.access"

**7) Aktualizacja / diagnostyka / deinstalacja**

**Aktualizacja (offline):**

1. Stop-Service "Elastic Agent"
2. Zrób kopię elastic-agent.yml
3. Rozpakuj nową wersję ZIP nad C:\Elastic\elastic-agent\ albo użyj .\elastic-agent.exe upgrade (jeśli masz lokalne artefakty).
4. Start-Service "Elastic Agent"

**Diagnostyka:**

.\elastic-agent.exe status

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

Test-NetConnection es.internal.local -Port 9200

**Odinstalowanie:**

.\elastic-agent.exe uninstall

**8) Najczęstsze problemy (i szybkie fixy)**

* **TLS/x509**: błąd weryfikacji certu → FQDN w outputs.elasticsearch.hosts musi odpowiadać **CN/SAN** certyfikatu ES; ca.crt musi być właściwy.
* **Brak danych w Discover**: sprawdź elastic-agent.log, łączność do 9200, ścieżki w YAML (używaj /).
* **401/403**: konto nie ma uprawnień do logs-\*/metrics-\* → sprawdź użytkownika/rolę; hasło w keystore pod nazwą zgodną z ${ES\_PWD}.