**1) „Could not start service” – szybka diagnostyka (Windows)**

Najczęstsze powody: zła składnia YAML, brak uprawnień konta usługi, współdzielone katalogi path.data/path.logs, albo parametry startowe wskazują na nieistniejący plik.

**Kroki naprawcze (w tej kolejności):**

1. **Uruchom w konsoli, żeby zobaczyć prawdziwy błąd**

cd "C:\Program Files\Winlogbeat"

.\winlogbeat.exe test config -e -c .\winlogbeat.yml -strict.perms=false

.\winlogbeat.exe -e -c .\winlogbeat.yml -strict.perms=false

Jeśli config OK, a w trybie -e wyskoczy błąd, zobaczysz dokładną przyczynę (linia, klucz, TLS, itp.).

1. **Sprawdź dziennik aplikacji Windows**

* eventvwr.msc → Windows Logs → **Application** → filtruj po **Source: winlogbeat** (lub nazwa Twojej usługi, jeśli custom).

1. **Zweryfikuj, na jakim koncie działa usługa**

* Domyślnie **Local System** jest OK (ma dostęp do dzienników).
* Jeśli podmieniałeś konto, dodaj je do **Event Log Readers** lub wróć do Local System.

1. **Usuń i zainstaluj usługę ponownie** (gdy parametry/ścieżki się rozjechały)

# w katalogu Winlogbeat

powershell -ExecutionPolicy Bypass -File .\uninstall-service-winlogbeat.ps1

powershell -ExecutionPolicy Bypass -File .\install-service-winlogbeat.ps1

Start-Service winlogbeat

1. **Jeśli używasz kilku instalacji na tym samym hoście** – upewnij się, że **nie współdzielą** path.data i path.logs. Współdzielenie = częsty „Could not start service”.

**2) Dwie instancje Winlogbeat na jednym PC – tak, ale z izolacją**

Możesz uruchomić **dwie (lub więcej) instancje** równocześnie, o ile każda ma:

* **osobny katalog instalacyjny** (np. C:\Program Files\Winlogbeat-01 i -02),
* **osobny plik konfiguracyjny**,
* **osobne ścieżki** path.data i path.logs,
* **unikalną nazwę usługi** w Windows.

Uwaga: jeśli obie instancje czytają **te same** kanały Event Logów, będziesz miał **duplikaty zdarzeń**. Zwykle lepiej 1 instancja z wieloma event\_logs. Druga instancja ma sens, gdy **musisz wysyłać do dwóch różnych outputów** (Beats mają tylko **jeden aktywny output** na instancję).

**Przykładowa procedura (druga instancja)**

1. **Sklonuj folder programu**

* Skopiuj C:\Program Files\Winlogbeat → C:\Program Files\Winlogbeat-02.

1. **Stwórz osobny config**, np. C:\Program Files\Winlogbeat-02\winlogbeat-02.yml  
   W nim dodaj izolację ścieżek i unikalną nazwę agenta (ułatwia rozróżnianie):

name: winlogbeat-02

winlogbeat.event\_logs:

- name: Security

- name: Application

# (lub inny zestaw niż w instancji 01, aby uniknąć duplikatów)

# ...reszta Twojej konfiguracji (procesory, output itd.)

path.data: "C:/ProgramData/winlogbeat-02"

path.logs: "C:/ProgramData/winlogbeat-02/logs"

logging.files:

name: winlogbeat-02

1. **Sprawdź config i uruchom testowo w konsoli**

cd "C:\Program Files\Winlogbeat-02"

.\winlogbeat.exe test config -e -c .\winlogbeat-02.yml -strict.perms=false

.\winlogbeat.exe -e -c .\winlogbeat-02.yml -strict.perms=false

1. **Zainstaluj drugą usługę z unikalną nazwą**

Jeśli skrypt instalacyjny w Twojej wersji nie wspiera parametru nazwy, użyj sc.exe:

sc.exe create "winlogbeat-02" binPath= "\"C:\Program Files\Winlogbeat-02\winlogbeat.exe\" -c \"C:\Program Files\Winlogbeat-02\winlogbeat-02.yml\" -path.home \"C:\Program Files\Winlogbeat-02\" -path.data \"C:\ProgramData\winlogbeat-02\" -path.logs \"C:\ProgramData\winlogbeat-02\logs\"" start= auto

Start-Service winlogbeat-02

Jeśli Twój install-service-winlogbeat.ps1 **obsługuje** nazwę/ścieżki, możesz zamiast sc.exe użyć odpowiednich parametrów (różne wersje skryptu mają różny zestaw parametrów – dlatego powyżej daję wariant „pewny” z sc.exe).

1. **Weryfikacja**

Get-Service winlogbeat, winlogbeat-02

* Obie powinny mieć Status : Running.

**Wskazówki, żeby nie wpaść w duplikaty i bałagan**

* Rozdziel kanały: np. instancja 01 → System, Application; instancja 02 → Security (lub inne filtry).
* Jeśli **musisz** czytać te same kanały dwoma instancjami (np. dwa różne outputy), oznacz eventy tagami:
* tags: ["source:winlogbeat-02"]

i/lub zmień **index/prefix**, żeby łatwo filtrować:

output.elasticsearch:

indices:

- index: "winlogbeat-02-%{+yyyy.MM.dd}"

when.equals:

tags: "source:winlogbeat-02"

(albo najprościej: w drugiej instancji ustaw output.elasticsearch.index: "winlogbeat-02-%{+yyyy.MM.dd}" w zależności od wersji Beats).

**TL;DR**

* „**Could not start service**” → odpal Winlogbeat w konsoli -e i sprawdź Event Viewer; zwykle to **błąd w YAML** albo **złe ścieżki/ uprawnienia**.
* **Dwie instancje** na jednym hoście są **OK**, ale każda musi mieć **osobny**: folder, path.data, path.logs, **nazwę usługi** i najlepiej **nie czytać tych samych kanałów** (chyba że świadomie dublujesz do różnych odbiorców).