

# Wykrywanie zagrożeń i reakcja na incydenty

Laboratorium 6

Tomasz Jarząbek 272279  
Wiktoria Migasiewicz 272177

07.05.2025

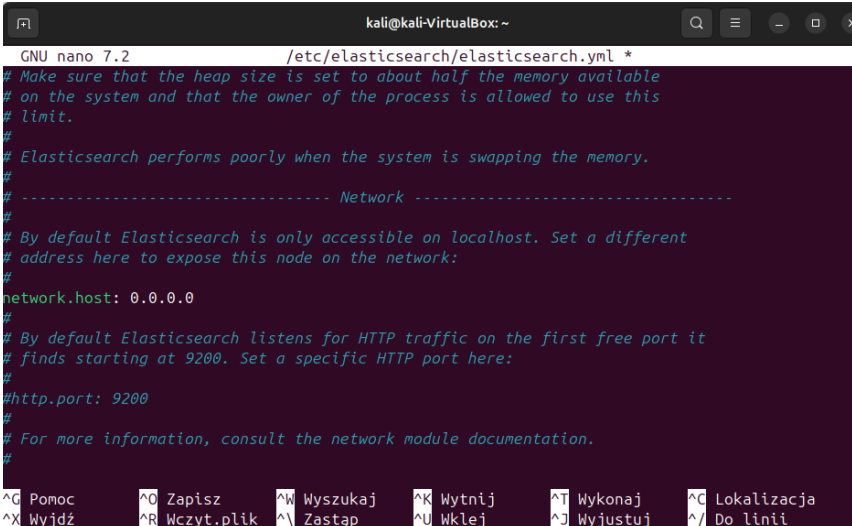
## 5. Konfiguracja usługi Elasticsearch

### Polecenie:

Proszę w ramach zmiennej „network.host” w pliku „/etc/elasticsearch/elasticsearch.yml” ustawić adres IP 0.0.0.0

### Wykorzystana komenda:

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```



```
GNU nano 7.2 /etc/elasticsearch/elasticsearch.yml *
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
^G Pomoc      ^O Zapisz      ^M Wyszukaj    ^K Wytnij    ^T Wykonaj    ^C Lokalizacja
^X Wyjdź      ^R Wczyt.plik ^\ Zastap    ^U Wklej     ^J Wyjustuj  ^/_ Do linii
```

Zrzut ekranu 1. Treść zmodyfikowanego pliku elasticsearch.yml

### Komentarz:

Uruchamia edytor tekstu nano z uprawnieniami administratora w celu edycji pliku konfiguracyjnego Elasticsearch. Ustawienie network.host: 0.0.0.0 pozwala na dostęp do usługi z dowolnego adresu IP.

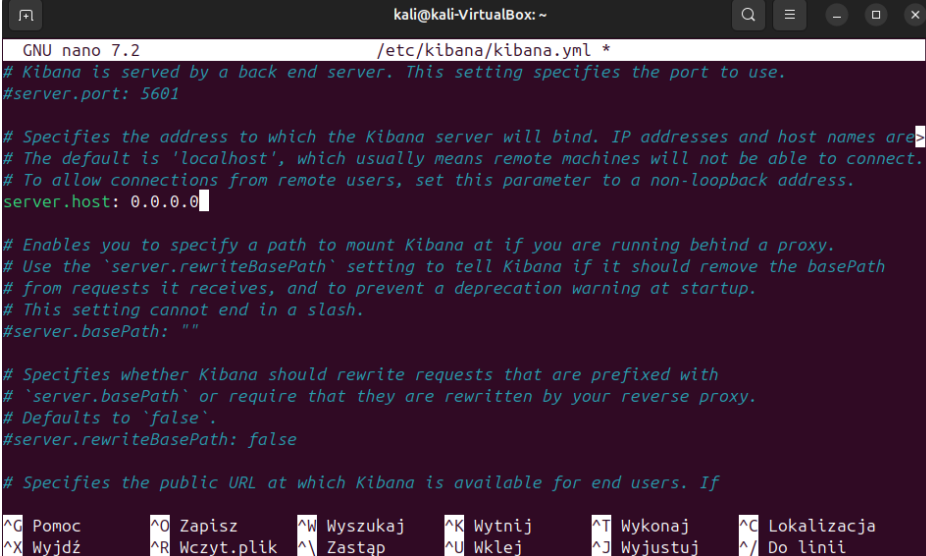
## 5. Konfiguracja usługi Kibana

### Polecenie:

Proszę w ramach zmiennej „server.host” w pliku „/etc/kibana/kibana.yml” ustawić adres IP 0.0.0.0

### Wykorzystana komenda:

sudo nano /etc/kibana/kibana.yml



```
GNU nano 7.2 /etc/kibana/kibana.yml *
# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: 0.0.0.0

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# 'server.basePath' or require that they are rewritten by your reverse proxy.
# Defaults to 'false'.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
```

Zrzut ekranu 2. Treść zmodyfikowanego pliku kibana.yml

#### Komentarz:

Otwiera plik konfiguracyjny Kibany do edycji. Ustawienie server.host: 0.0.0.0 umożliwia dostęp do interfejsu Kibany z innych urządzeń w sieci.

## 7. Uruchomienie usług

#### Wykorzystana komenda:

systemctl start elasticsearch kibana logstash

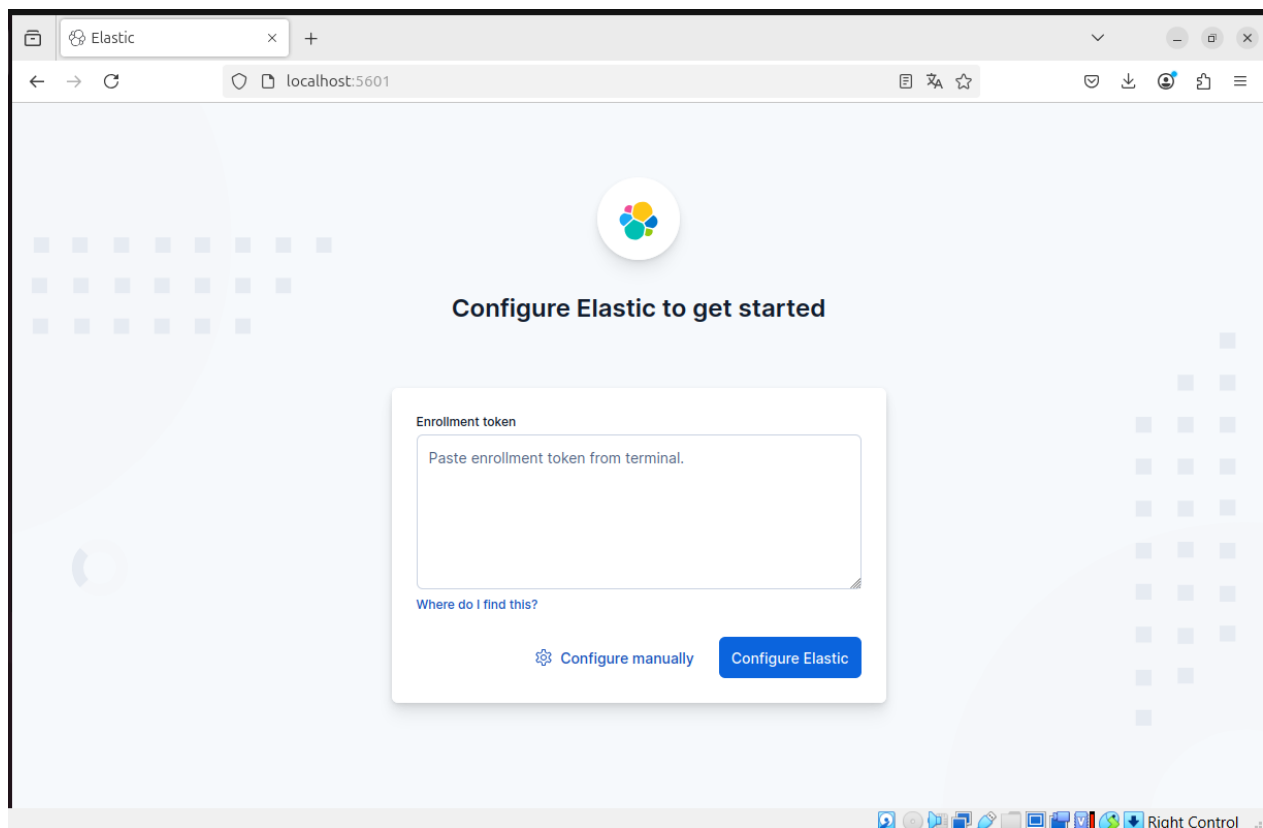
#### Komentarz:

Uruchamia usługi Elasticsearch, Kibana i Logstash przy użyciu menedżera systemd.

## 8. Pierwsze uruchomienie środowiska

#### Polecenie:

Z maszyny z systemem Ubuntu proszę udać się pod adres <http://localhost:5601>.



Zrzut ekranu 3. Widok z przeglądarki na porcie 5601

**Polecenie:**

Proszę wygenerować i wprowadzić „Enrollment token”

**Wykorzystana komenda:**

```
sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token - -scope kibana
```

**Wynik:**

```
kali@kali-VirtualBox:~$ sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token --scope kibana  
eyJzZXI0OiE9LjE0LjAeLCJkZHIwLSMtaUxCMC4zMjQ6OTcwMCBdLCJMzZI0I0IzNTXlxNzRlZmRmM2M5YjFmYTQxOXBvbmVjbWFnZWFrYyZ2  
QyZjRjOWZhMGJlZGJLYjZmMTESVTM3YzMSNmI3IiwiaGVhbnQiOiJkbGlSR1NrTk6a3JKKWFIncyDREFYb1lnNENXWo1USJ9
```

---

```
kali@kali-VirtualBox:~$
```

Zrzut ekranu 4. Wynik komendy generującej “Enrollment token”

**Komentarz:**

Generuje token potrzebny do połączenia Kibany z Elasticsearch podczas początkowej konfiguracji.

**Polecenie:**

Proszę wygenerować “Verification Code”

### Wykorzystana komenda:

```
sudo /usr/share/kibana/bin/kibana-verification-code
```

### Wynik:

```
kali@kali-VirtualBox:~$ sudo /usr/share/kibana/bin/kibana-verification-code
Your verification code is: 043 837
kali@kali-VirtualBox:~$
```

Zrzut ekranu 5. Wynik komendy generującej “Verification Code”

### Komentarz:

Generuje kod weryfikacyjny używany do potwierdzenia poprawności połączenia Kibany z Elasticsearch.

### Polecenie:

Proszę zresetować hasło użytkownika elastic

### Wykorzystana komenda:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic
```

```
kali@kali-VirtualBox:~$ sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic
This tool will reset the password of the [elastic] user to an autogenerated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]y

Password for the [elastic] user successfully reset.
New value: GeOc*bbpNOchJFdawZAn
kali@kali-VirtualBox:~$
```

Zrzut ekranu 6. Wynik komendy resetującej hasło użytkownika elastic

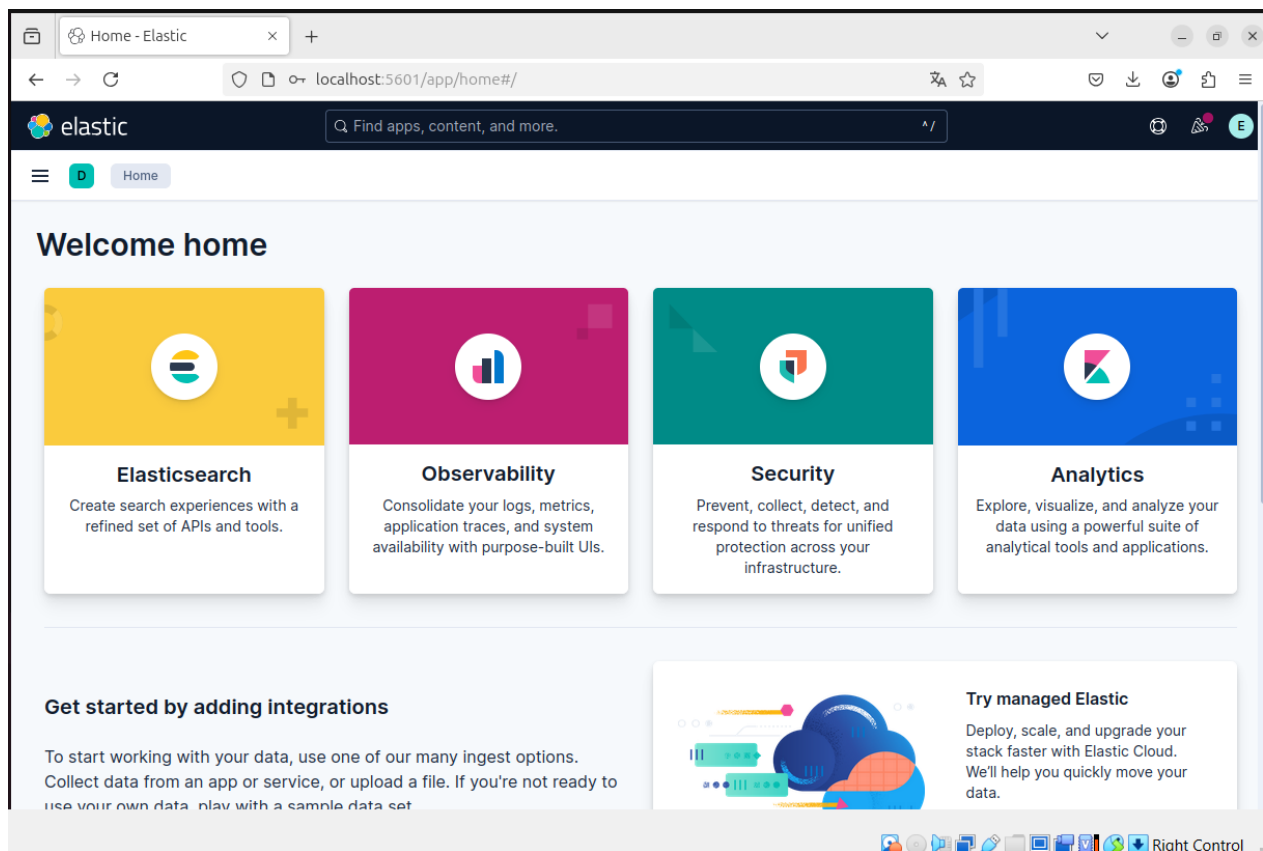
### Komentarz:

Resetuje hasło użytkownika elastic, domyślnego konta administracyjnego Elasticsearch.

### Polecenie:

Proszę zalogować się wygenerowanymi poświadczeniami

### Wynik:



Zrzut ekranu 7. Widok narzędzi Elasticsearch po zalogowaniu

**9. Proszę w ramach VirtualBox zainstalować VM z OS Windows 10**

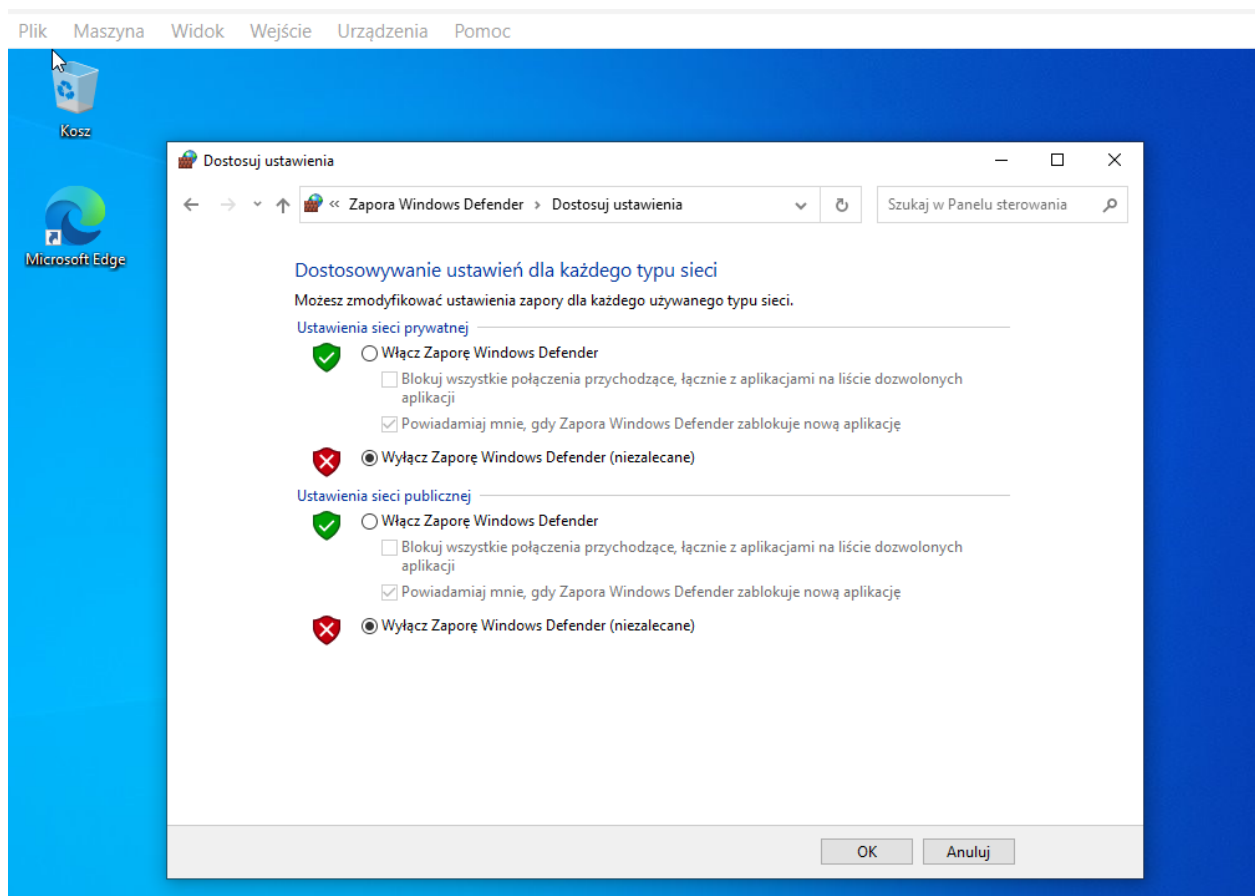
**10. Proszę w ramach VirtualBox zainstalować VM z OS Alma Linux**

## **11. Konfiguracja usług**

**Polecenie:**

Proszę wyłączyć FW w ramach maszyn Windows 10 i Alma Linux

**Wynik:**



Zrzut ekranu 8. Zmiana ustawień zapory dla maszyny Windows

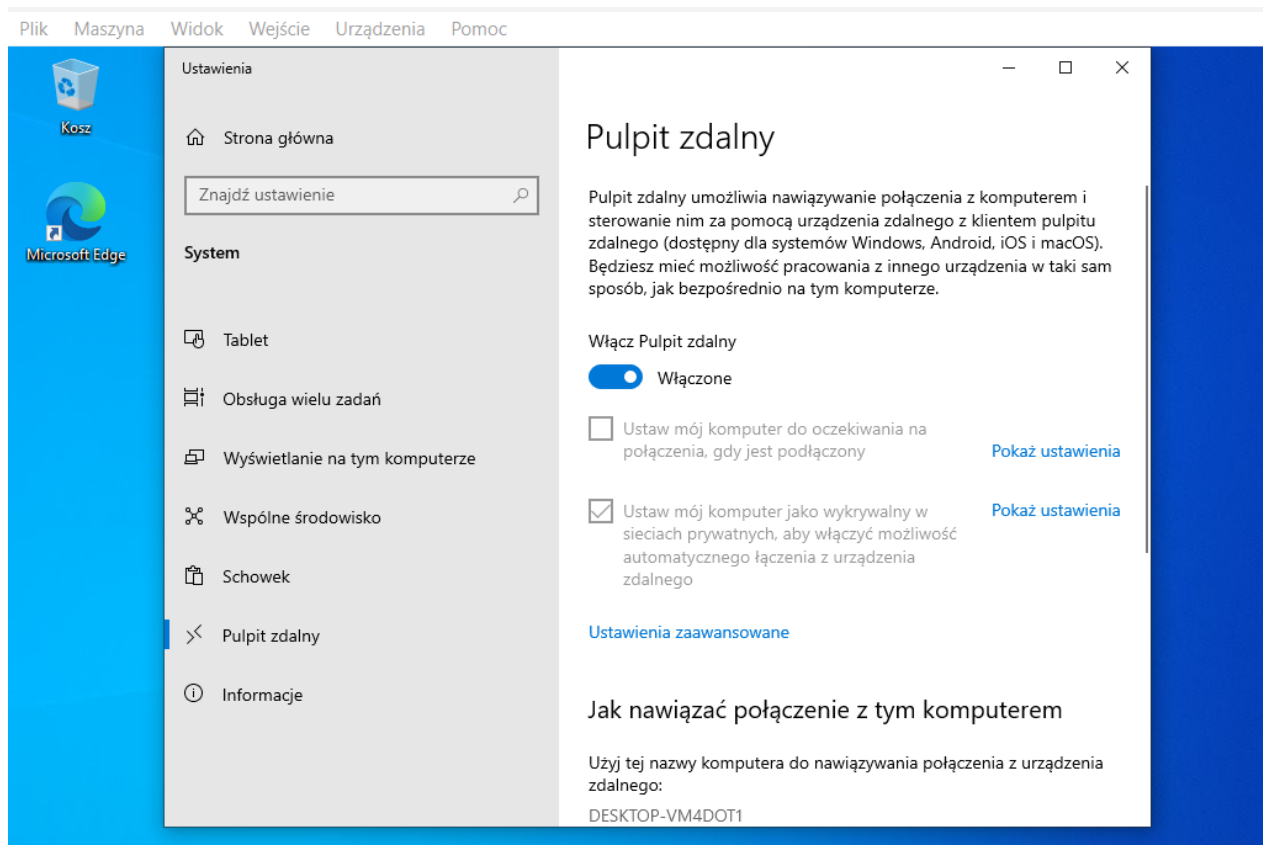
### Komentarz:

Wyłączenie zapory sieciowej umożliwia komunikację między systemami bez ograniczeń sieciowych.

### Polecenie:

Uruchomienie RDP w ramach maszyny z Windows 10

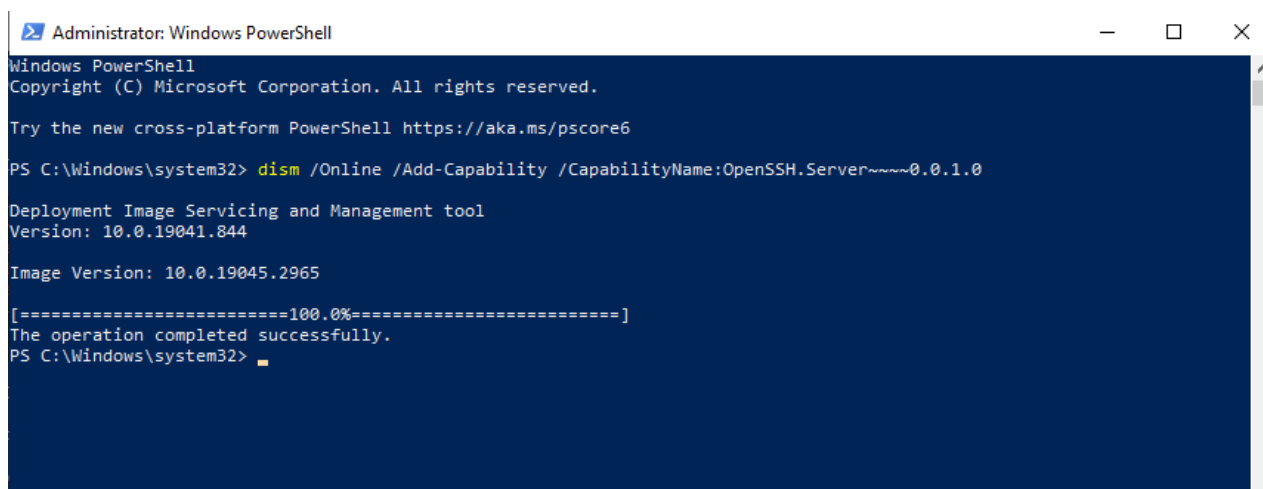
### Wynik:



Zrzut ekranu 9. Uruchomienie pulpitu zdalnego na maszynie Windows

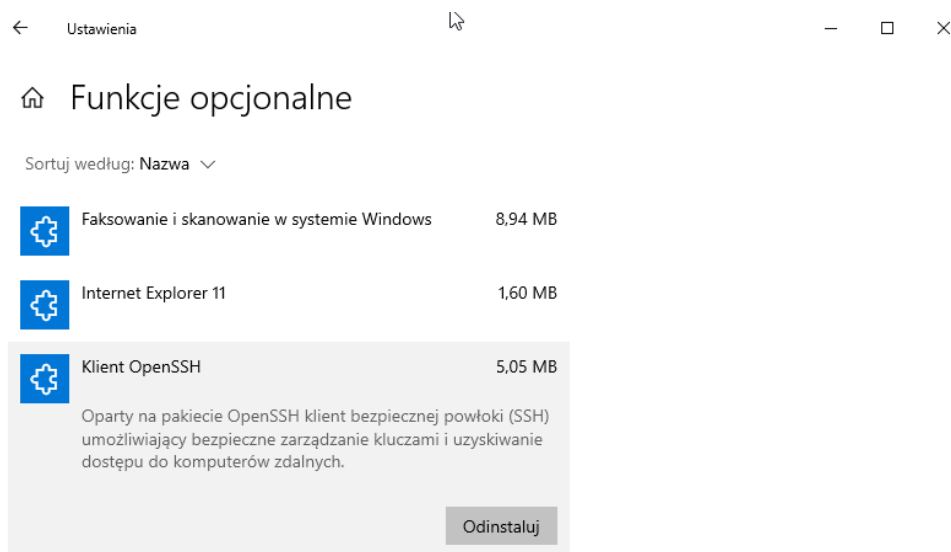
## Polecenie:

Uruchomienie SSH w ramach maszyny z Windows 10



Zrzut ekranu 10. Proces instalacji klienta Open SSH





Zrzut ekranu 10. Weryfikacja poprawnej instalacji kleinta Open SSH

### **Komentarz:**

Włączenie pulpitu zdalnego i instalacja OpenSSH umożliwia zdalny dostęp do systemu Windows 10.

## **12. Instalacja i podłączenie agentów w ramach maszyny Windows 10**

### **Winlogbeat**

#### **Polecenie:**

Instalacja Winlogbeat.

#### **Wynik:**

```

PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1

Status      Name            DisplayName
-----
Stopped     winlogbeat      winlogbeat

PS C:\Program Files\Winlogbeat> Start-Service winlogbeat
PS C:\Program Files\Winlogbeat> Get-Service winlogbeat

Status      Name            DisplayName
-----
Running     winlogbeat      winlogbeat

PS C:\Program Files\Winlogbeat>

```

Zrzut ekranu 11. Proces instalacji Winlogbeat

### Polecenie:

Zmiana adresu Elasticsearch'a i podanie loginu oraz hasła

```

# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.3.4:9200"]

```

Zrzut ekranu 12. Zmiana adresu Elasticsearch w pliku winlogbeat.yml

```

# Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
username: "elastic"
password: "GeOc*bbpNOchJFdawZAn|"

```

Zrzut ekranu 13. Zmiana hasła i użytkownika Elasticsearch w pliku winlogbeat.yml

### Polecenie:

Zmiana adresu Kibany

setup.kibana:

```
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify an additional path, the scheme is required: http://localhost:5601/
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "10.0.3.4:5601"
```

Zrzut ekranu 14. Zmiana adresu Kibany w pliku winlogbeat.yml

## Polecenie:

Dodanie „ssl.verification\_mode: "none"” w konfiguracji

Dodanie „protocol: "https"” w konfiguracji

```
# Protocol - either `http` (default) or `https`.
protocol: "https"
ssl.verification_mode:"none"
```

Zrzut ekranu 15. Dodanie ustawień w pliku winlogbeat.yml

## Polecenie:

Proszę wykonać polecenie “& C:\Program Files\Elastic\Beats\8.7.0\winlogbeat\winlogbeat.exe' -c C:\ProgramData\Elastic\Beats\winlogbeat\winlogbeat.yml setup -e”

```
PS C:\Windows\system32> & 'C:\Program Files\Winlogbeat\winlogbeat.exe' -c 'C:\Program Files\Winlogbeat\winlogbeat.yml'
setup -e
{"log.level":"info","@timestamp":"2025-05-01T13:06:59.819+0200","log.origin":{"function":"github.com/elastic/beats/v7/1
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1080},"message":"Home path: [C:\\Progr
m Files\\Winlogbeat] Config path: [C:\\Program Files\\Winlogbeat] Data path: [C:\\Program Files\\Winlogbeat\\data] Logs
path: [C:\\Program Files\\Winlogbeat\\logs]","service.name":"winlogbeat","ecs.version":"1.6.0"}
```

Zrzut ekranu 16. Uruchomienie komendy konfigurującej Winlogbeat

## Metricbeat

### Polecenie:

Instalacja Metricbeat

```
PS C:\Program Files\Metricbeat> .\install-service-metricbeat.ps1

Status      Name            DisplayName
-----
Stopped     metricbeat      metricbeat

PS C:\Program Files\Metricbeat> █
```

Zrzut ekranu 17. Instalacja narzędzia Metricbeat

## Polecenie:

Zmiana adresu Kibany

```
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify an additional path, the scheme is required: http://localhost:5601/
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "10.0.3.4:5601"
```

Zrzut ekranu 18. Zmiana adresu Kibany w pliku metricbeat.yml

## Polecenie:

Zmiana adresu Elasticsearch'a i podanie loginu oraz hasła

Dodanie „ssl.verification\_mode: \"none\"” w konfiguracji

Dodanie „protocol: \"https\"” w konfiguracji

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.3.4:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  protocol: "https"
  ssl.verification_mode: "none"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "Ge0c*bbpNOchJFdawZAn"
```

Zrzut ekranu 19. Modyfikacja ustawień w pliku metricbeat.yml

```
PS C:\> & 'C:\Program Files\Metricbeat\metricbeat.exe' -c 'C:\Program Files\Metricbeat\metricbeat.yml' setup -e  
{ "log.level": "info", "@timestamp": "2025-05-01T13:24:42.838+0200", "log.origin": { "function": "github.com/elastic/beats/v7/li  
bbeat/cmd/instance.(*Beat).configure", "file.name": "instance/beat.go", "file.line": 1080 }, "message": "Home path: [C:\\Progra  
m Files\\Metricbeat\\ Config_path: [C:\\\\Program Files\\Metricbeat\\ Data_path: [C:\\\\Program Files\\Metricbeat\\data\\logs
```

Zrzut ekranu 20. Uruchomienie komendy konfigurującej Metricbeat

## Auditbeat

### Polecenie:

Instalacja Auditbeat

```
PS C:\Program Files\Auditbeat> .\install-service-auditbeat.ps1  
  
Status      Name      DisplayName  
-----  
Stopped     auditbeat  auditbeat
```

Zrzut ekranu 21. Instalacja narzędzia Auditbeat

### Polecenie:

Zmiana adresu Kibany

```
# Kibana Host  
# Scheme and port can be left out and will be set to the default (http and 5601)  
# In case you specify and additional path, the scheme is required: http://localhost:5601/  
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601  
host: "10.0.3.4:5601"
```

Zrzut ekranu 22. Zmiana adresu Kibany w pliku auditbeat.yml

### Polecenie:

Zmiana adresu Elasticsearch'a i podanie loginu oraz hasła

Dodanie „ssl.verification\_mode: \"none\"” w konfiguracji

Dodanie „protocol: \"https\"” w konfiguracji

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.3.4:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  protocol: "https"
  ssl.verification_mode: "none"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "Ge0c*bbpN0chJFdawZAn"
```

Zrzut ekranu 23. Modyfikacja ustawień w pliku auditbeat.yml

```
PS C:\> & 'C:\Program Files\Auditbeat\auditbeat.exe' -c 'C:\Program Files\Auditbeat\auditbeat.yml' setup -e
{"log.level":"info","@timestamp":"2025-05-01T13:33:10.850+0200","log.origin":{"function":"github.com/elastic/beats/v7/13
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1080},"message":"Home path: [C:\\Progra
m Files\\Auditbeat] Config path: [C:\\Program Files\\Auditbeat] Data path: [C:\\Program Files\\Auditbeat\\data] Logs pat
h: [C:\\Program Files\\Auditbeat\\logs] Service name: Auditbeat\\beat-service-11-6-011"}
```

Zrzut ekranu 24. Uruchomienie komendy konfigurującej Auditbeat

## Packetbeat

### Polecenie:

Instalacja Packetbeat

```
PS C:\Program Files\Packetbeat> .\install-service-packetbeat.ps1

Status      Name             DisplayName
-----
Stopped     packetbeat       packetbeat
```

Zrzut ekranu 25. Instalacja narzędzia Packetbeat

### Polecenie:

## Zmiana adresu Kibany

```
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify an additional path, the scheme is required: http://localhost:5601/
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "10.0.3.4:5601"
```

Zrzut ekranu 26. Zmiana adresu Kibany w pliku packetbeat.yml

## Polecenie:

Zmiana adresu Elasticsearch'a i podanie loginu oraz hasła

Dodanie „ssl.verification\_mode: \"none\"” w konfiguracji

Dodanie „protocol: \"https\"” w konfiguracji

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.3.4:9200"]

  # Protocol - either `http` (default) or `https`.
  protocol: "https"
  ssl.verification_mode: "none"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "GeOc*bbpN0chJFdawZAn"
```

Zrzut ekranu 27. Modyfikacja ustawień w pliku packetbeat.yml

```
PS C:\> & 'C:\Program Files\Packetbeat\packetbeat.exe' -c 'C:\Program Files\Packetbeat\packetbeat.yml' setup -e
{"log.level":"info","@timestamp":"2025-05-01T13:38:50.576+0200","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1080},"message":"Home path: [C:\\Progra
m Files\\Packetbeat] Config path: [C:\\Program Files\\Packetbeat] Data path: [C:\\Program Files\\Packetbeat\\data] Logs
```

Zrzut ekranu 28. Uruchomienie komendy konfigurującej Packetbeat

## Heartbeat

## Polecenie:

Instalacja Heartbeat

```
PS C:\Program Files\Heartbeat> .\install-service-heartbeat.ps1

Status      Name      DisplayName
-----
Stopped heartbeat heartbeat
```

Zrzut ekranu 29. Instalacja narzędzia Heartbeat

## Polecenie:

Zmiana adresu Kibany

```
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify an additional path, the scheme is required: http://localhost:5601/
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "10.0.3.4:5601"
```

Zrzut ekranu 30. Zmiana adresu Kibany w pliku heartbeat.yml

## Polecenie:

Zmiana adresu Elasticsearch'a i podanie loginu oraz hasła

Dodanie „ssl.verification\_mode: "none"” w konfiguracji

Dodanie „protocol: "https"” w konfiguracji

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.3.4:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  protocol: "https"
  ssl.verification_mode: "none"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "Ge0c*bbpN0chJFdawZAn"
```



Zrzut ekranu 31. Modyfikacja ustawień w pliku heartbeat.yml

```
PS C:\> & 'C:\Program Files\Heartbeat\heartbeat.exe' -c 'C:\Program Files\Heartbeat\heartbeat.yml' setup -e
{"log.level":"info","@timestamp":"2025-05-01T13:43:30.426+0200","log.origin":{"function":"github.com/elastic/beats/v7/13
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1080},"message":"Home path: [C:\\Progra
m Files\\Heartbeat] Config path: [C:\\Program Files\\Heartbeat] Data path: [C:\\Program Files\\Heartbeat\\data] Logs pat
h: [C:\\Program Files\\Heartbeat\\logs]","service.name":"heartbeat","ecs.version":"1.6.0"}
```

Zrzut ekranu 32. Uruchomienie komendy konfigurującej Heartbeat

## Polecenie:

Dodanie konfiguracji w heartbeat.monitors

```
- type: icmp # monitor type `icmp` (requires root) uses ICMP Echo Request to ping
  # ID used to uniquely identify this monitor in elasticsearch even if the config changes
  id: icmp-service

  # Human readable display name for this service in Uptime UI and elsewhere
  name: ICMP Service

  # Name of corresponding APM service, if Elastic APM is in use for the monitored service.
  #service.name: my-apm-service-name

  # Enable/Disable monitor
  enabled: true

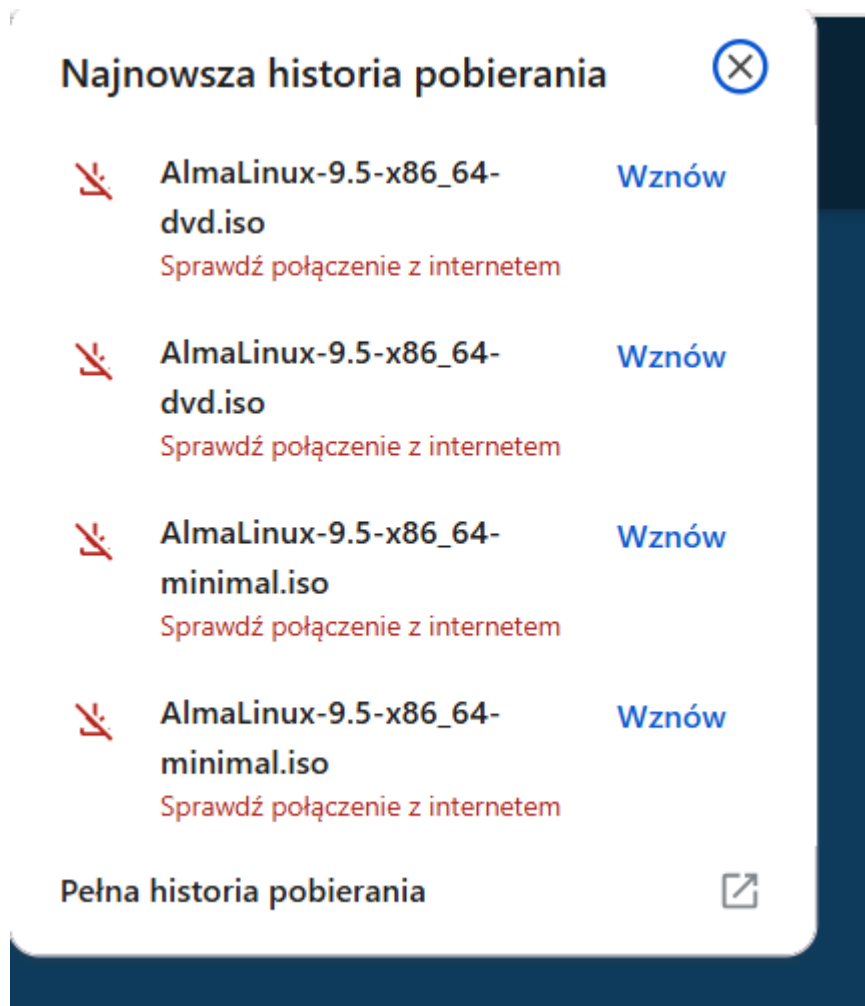
  # Configure task schedule using cron-like syntax
  schedule: '*/*5*****'

  # List of hosts to ping
  hosts: ["localhost"]
```

Zrzut ekranu 33. Modyfikacja ustawień w pliku heartbeat.monitors

## Komentarz:

Wykorzystane koemndy inicjalizują odpowiedniego beata, ładują dashboardsy i sprawdzają konfigurację na podstawie plików YAML.



Passy:

Token:

eyJ2ZXIiOiI4LjE0LjAiLCJhZHliOlsiMTAuMC4zLjQ6OTIwMCJdLCJmZ3IiOiIzNTIxNzRjMzRmM2M5YjFmYTQxOTc1N2VjNWZhMjJhYzFhY2QyZjRjOWZhMGJlZGJIYjZmMTE5YTM3YzM5NmI3Iiwia2V5Ijoic212VWJKWUJCnWNwWGlsR1NnRTk6a3JKWkFINy1DREFYb1lnNENXWVo1USJ9

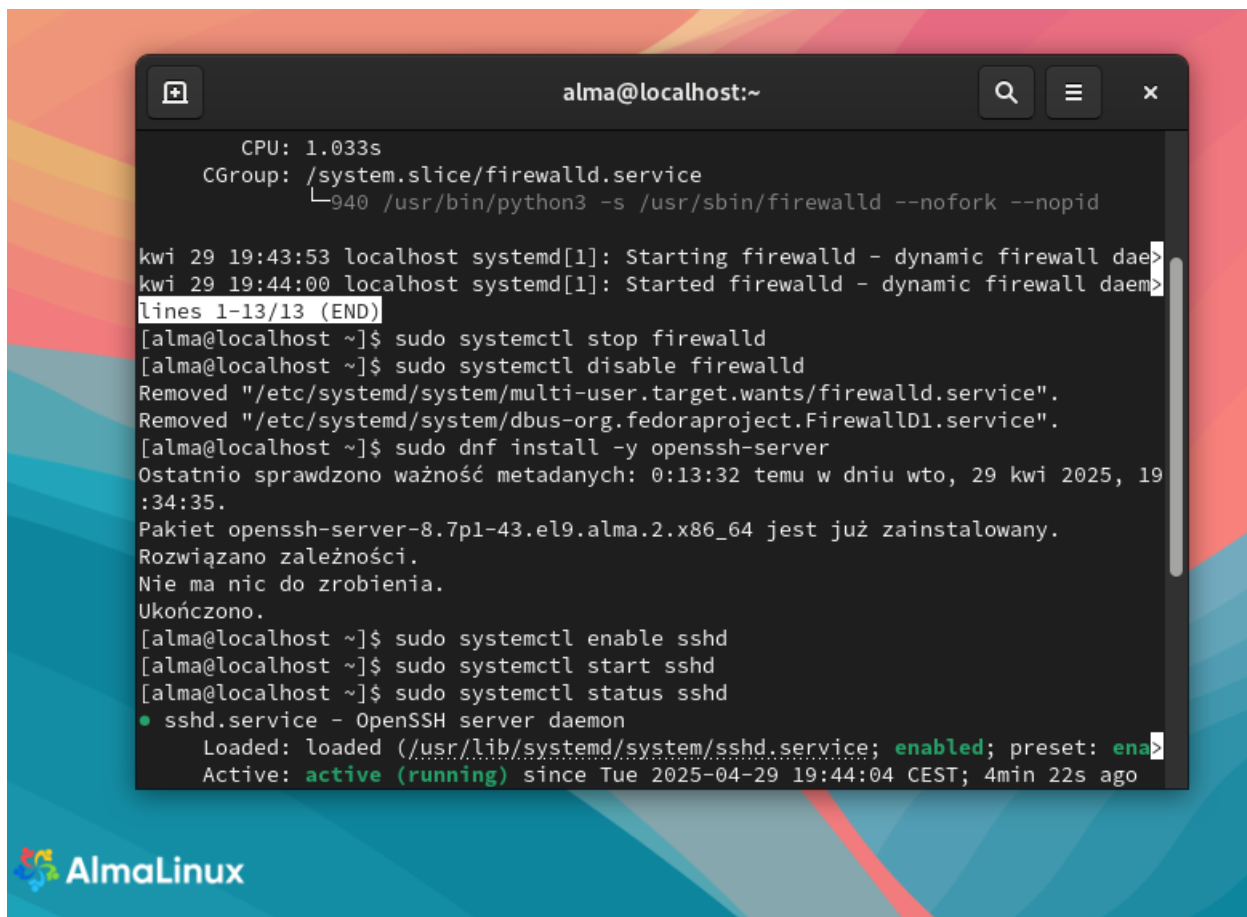
kod: 043 837

hasło: GeOc\*bbpNOchJFdawZAn

# 1 Rozwiązania

## 1.1 Alma

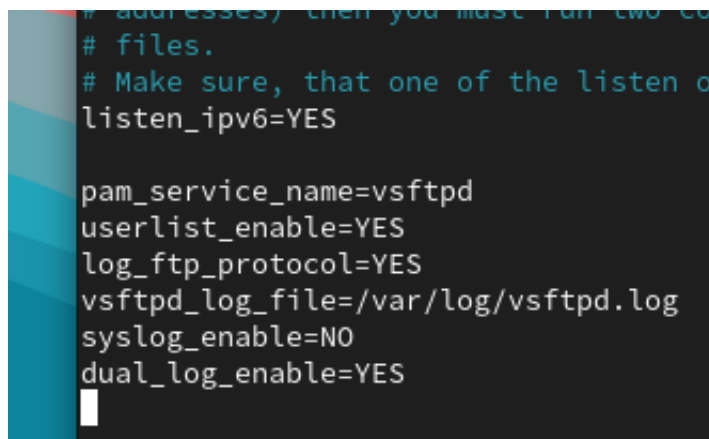
Przygotowano środowisko maszyny wirtualnej Alma Linux. Nadano jej odpowiednie zasoby oraz zainstalowano dodatki gościa. Następnie wyłączono Firewall oraz włączono usługę SSH.



```
alma@localhost:~  
CPU: 1.033s  
CGroup: /system.slice/firewalld.service  
└─940 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid  
kwi 29 19:43:53 localhost systemd[1]: Starting firewalld - dynamic firewall daem>  
kwi 29 19:44:00 localhost systemd[1]: Started firewalld - dynamic firewall daem>  
lines 1-13/13 (END)  
[alma@localhost ~]$ sudo systemctl stop firewalld  
[alma@localhost ~]$ sudo systemctl disable firewalld  
Removed "/etc/systemd/system/multi-user.target.wants/firewalld.service".  
Removed "/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service".  
[alma@localhost ~]$ sudo dnf install -y openssh-server  
Ostatnio sprawdzono ważność metadanych: 0:13:32 temu w dniu wto, 29 kwi 2025, 19:34:35.  
Pakiet openssh-server-8.7p1-43.el9.alma.2.x86_64 jest już zainstalowany.  
Rozwiązano zależności.  
Nie ma nic do zrobienia.  
Ukończono.  
[alma@localhost ~]$ sudo systemctl enable sshd  
[alma@localhost ~]$ sudo systemctl start sshd  
[alma@localhost ~]$ sudo systemctl status sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: ena>  
   Active: active (running) since Tue 2025-04-29 19:44:04 CEST; 4min 22s ago
```

Rysunek 1: Wyłączone Firewall oraz włączone SSH.

Następnie w konfiguracji FTP zmieniono konkretne wartości.

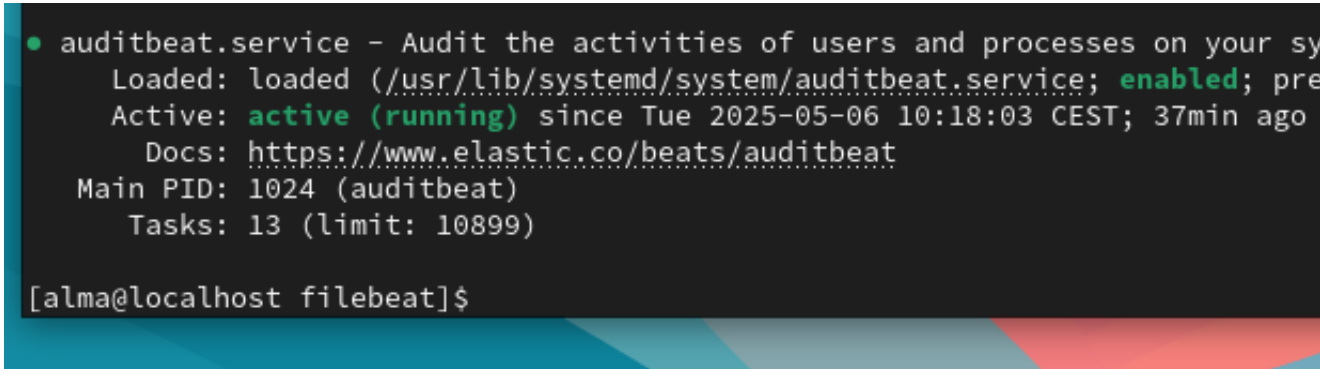


```
# addresses, then you must run two co  
# files.  
# Make sure, that one of the listen o  
listen_ipv6=YES  
  
pam_service_name=vsftpd  
userlist_enable=YES  
log_ftp_protocol=YES  
vsftpd_log_file=/var/log/vsftpd.log  
syslog_enable=NO  
dual_log_enable=YES
```

Rysunek 2: Zmiana konfiguracji FTP.

Następnie sukcesywnie pobierano i instalowano konkretne beaty:

- Filebeat
- Packetbeat
- Metricbeat
- Heartbeat-elastic
- Auditbeat



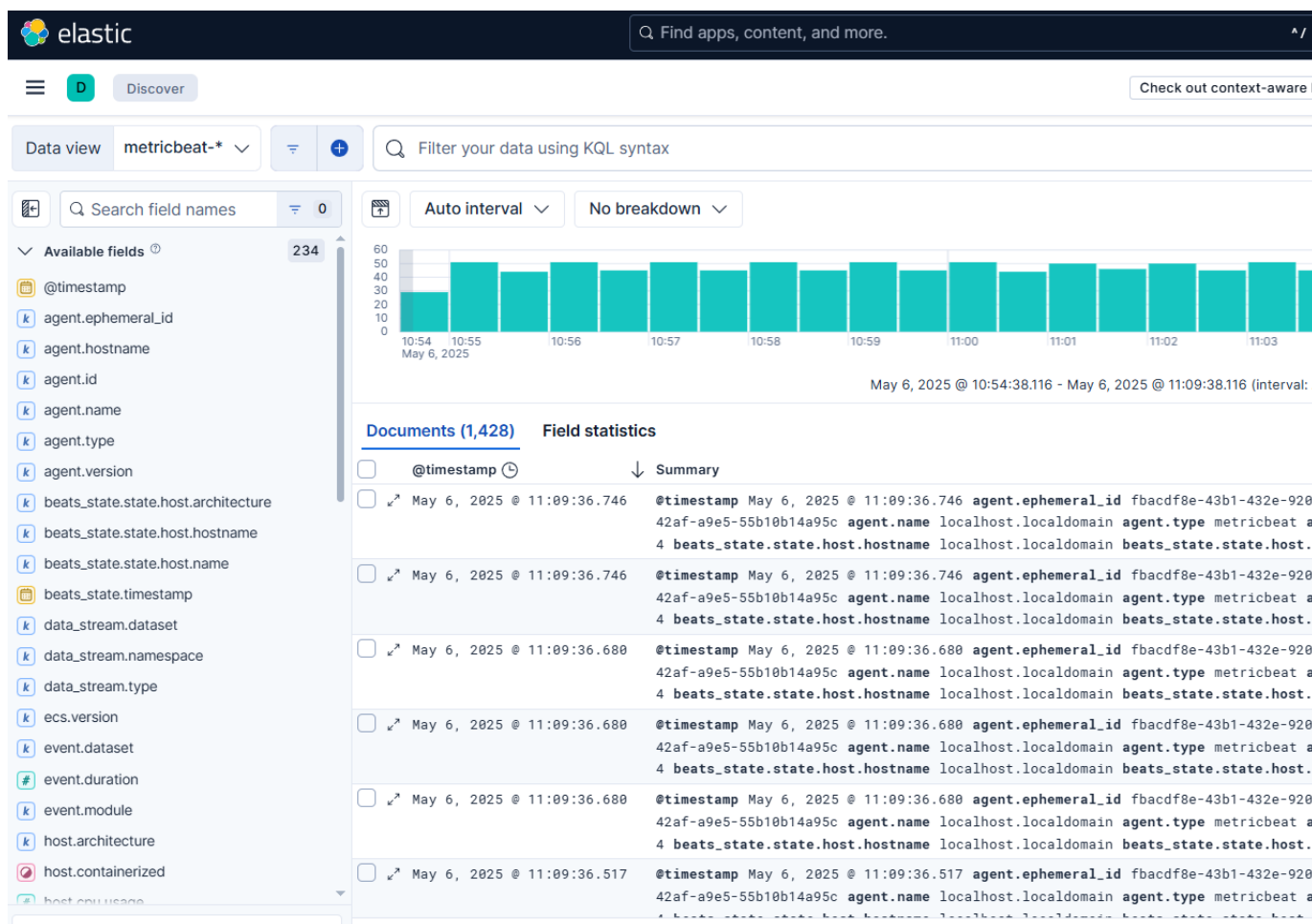
```
• auditbeat.service - Audit the activities of users and processes on your sy
  Loaded: loaded (/usr/lib/systemd/system/auditbeat.service; enabled; pre
  Active: active (running) since Tue 2025-05-06 10:18:03 CEST; 37min ago
  Docs: https://www.elastic.co/beats/auditbeat
  Main PID: 1024 (auditbeat)
  Tasks: 13 (limit: 10899)

[alma@localhost filebeat]$
```

Rysunek 3: Przykład - działający Auditbeat.

## 1.2 Data Views

Po zainstalowaniu zarówno beatów w Almie, jak i Windowsie, wyświetlono w Kibanie widok Data Views.



Rysunek 4: Widok DataView.

Każdy z beatsów zapewne różne typy danych;

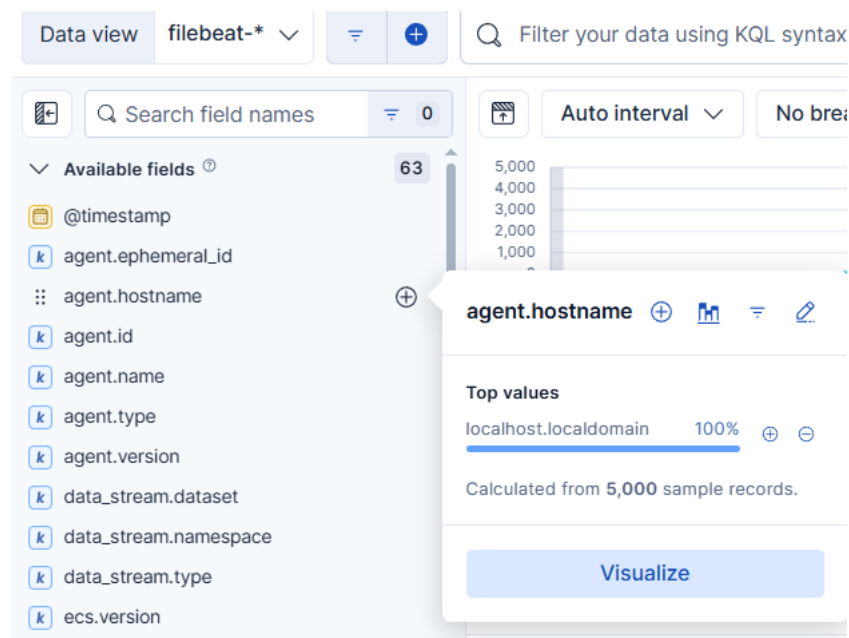
- **Filebeat** – zbiera i przesyła logi z plików logów systemowych i aplikacyjnych.
- **Metricbeat** – monitoruje metryki systemowe i usług (CPU, pamięć, dyski, bazy danych, serwery WWW itp.).
- **Packetbeat** – analizuje ruch sieciowy w czasie rzeczywistym (protokoły, opóźnienia, błędy).
- **Winlogbeat** – zbiera logi zdarzeń z systemu Windows (np. logowania, błędy systemowe).
- **Auditbeat** – śledzi aktywność użytkowników, zdarzenia bezpieczeństwa i zmiany w plikach.
- **Heartbeat** – monitoruje dostępność usług poprzez pingowanie HTTP, TCP lub ICMP.

W **Data Views** możemy zobaczyć różne dane dotyczące zainstalowanych beatsów. Są to m.in.:

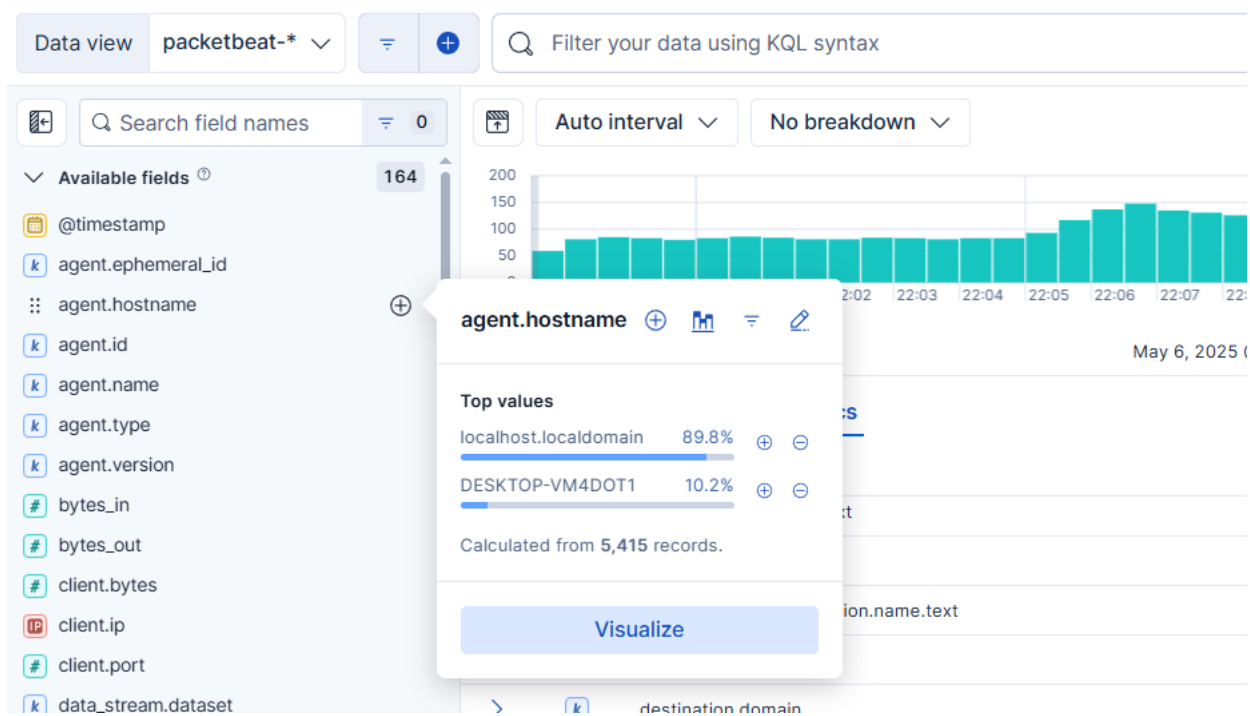
- agent.hostname
- agent.id
- agent.name
- data\_stream.type
- ecs.version
- error.message

- event.code
- event.category

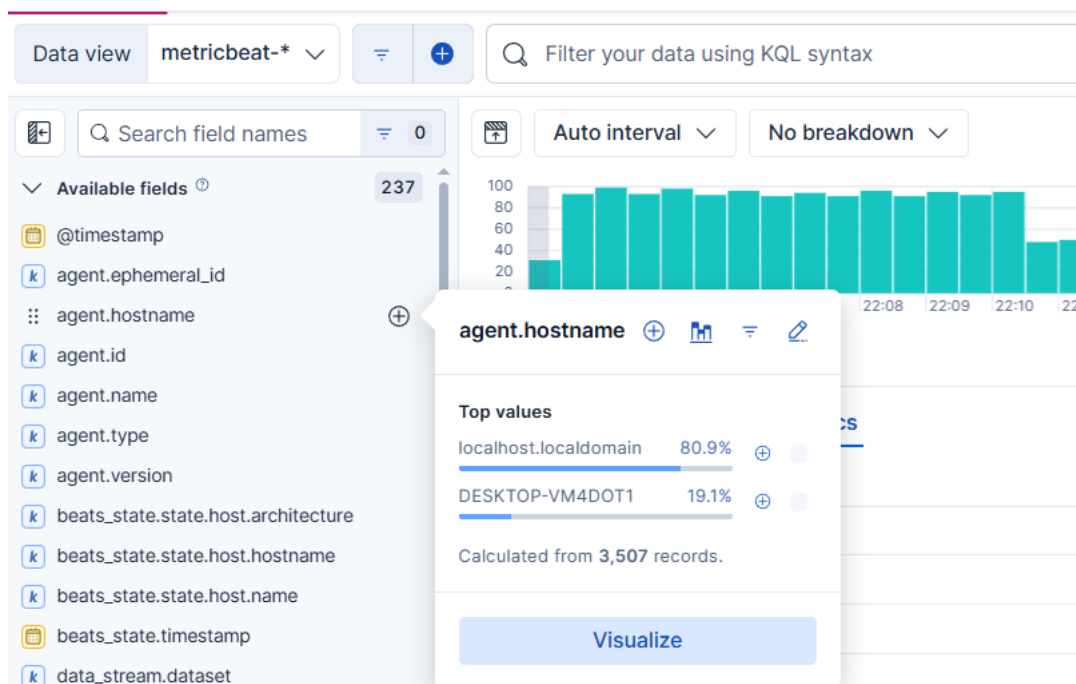
Widoki „data view” w zakładce „Discover” prezentują się następująco:



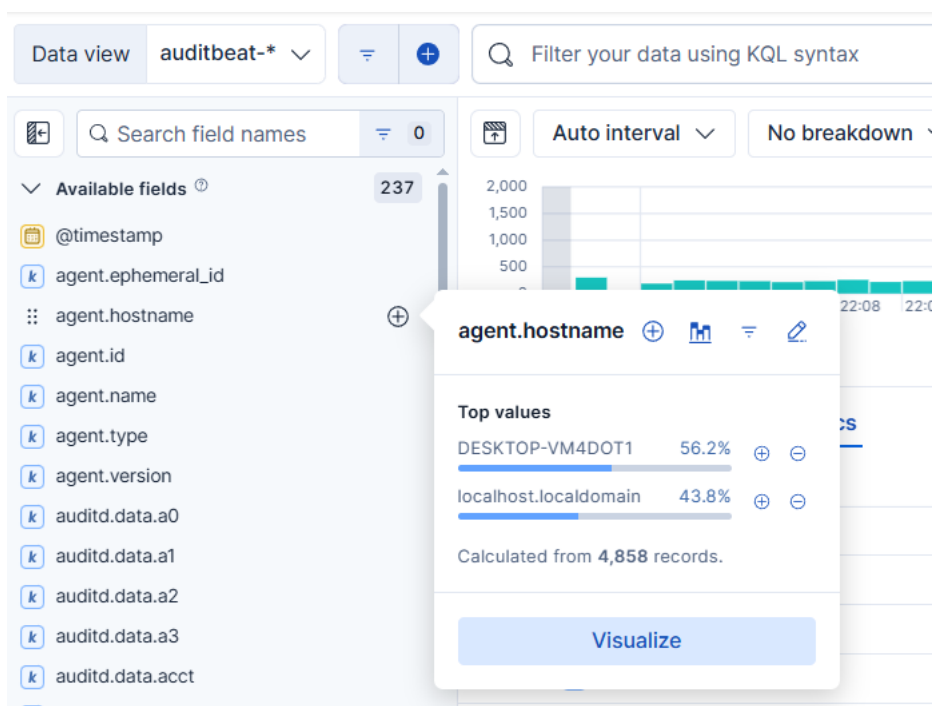
Rysunek 5: Widok DataView Kibany Filebeat.



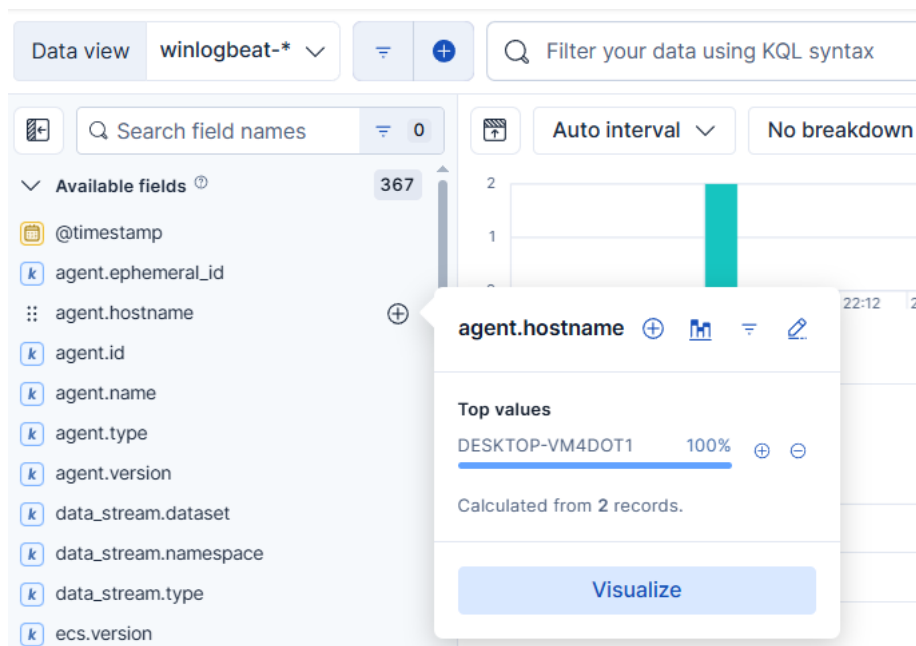
Rysunek 6: Widok DataView Kibany Packetbeat.



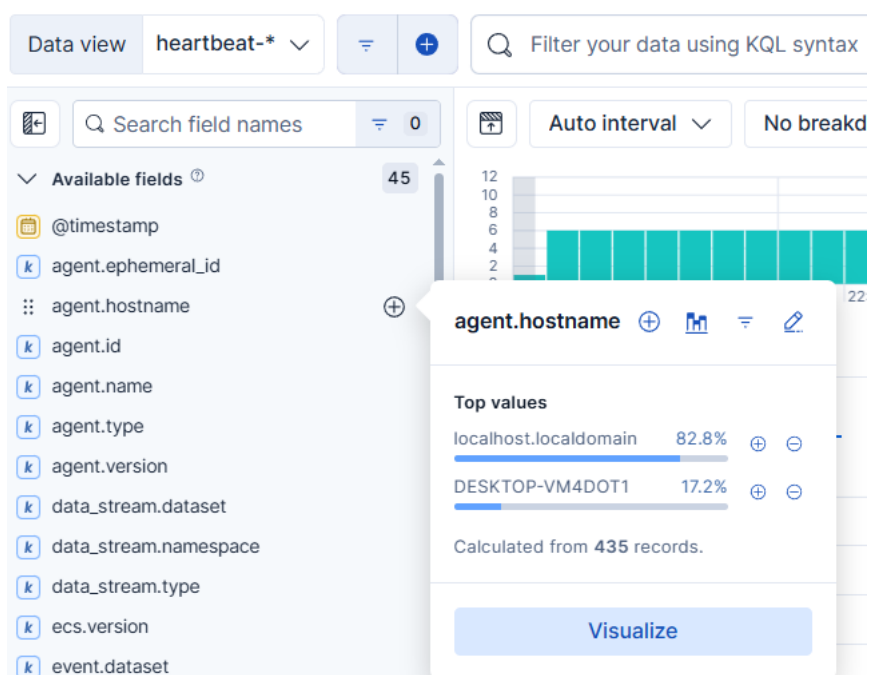
Rysunek 7: Widok DataView Kibany Metricbeat.



Rysunek 8: Widok DataView Kibany Auditbeat.



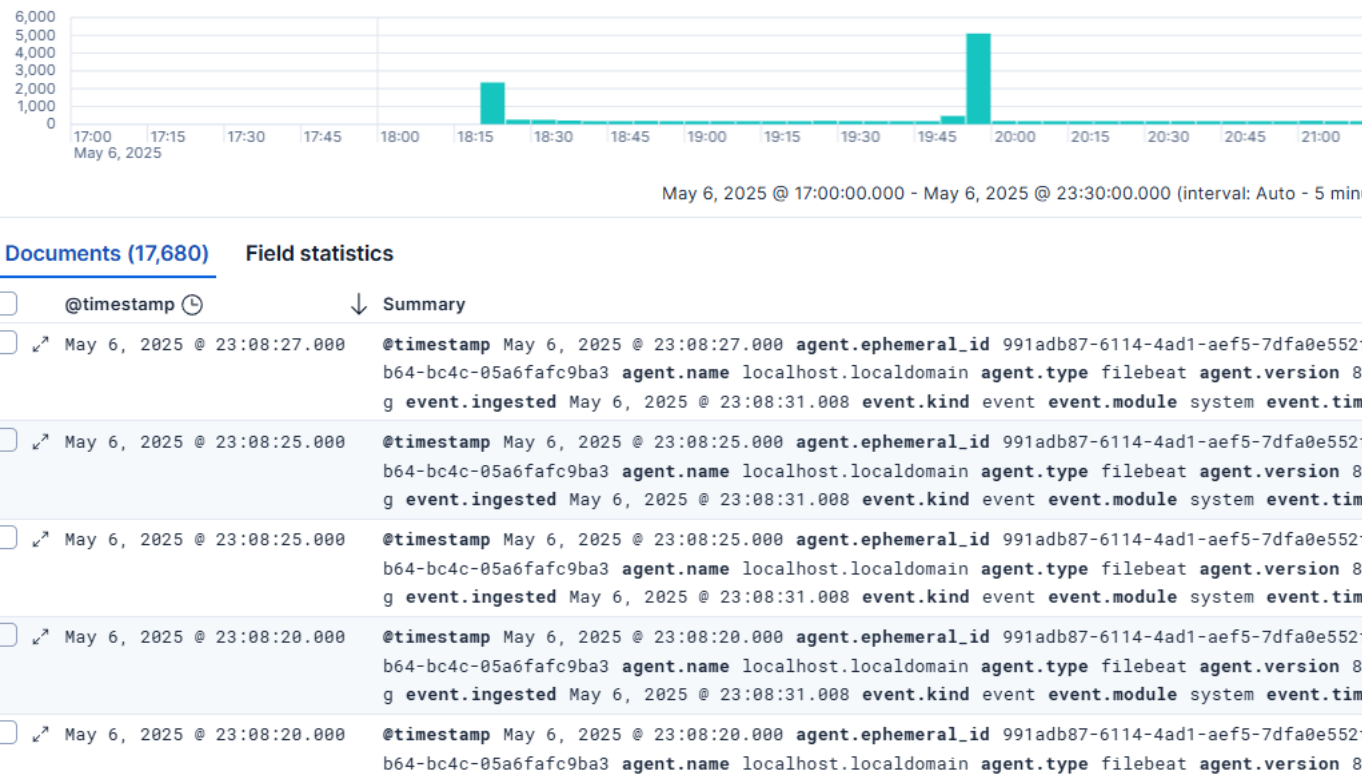
Rysunek 9: Widok DataView Kibany Winlogbeat.



Rysunek 10: Widok DataView Kibany Heartbeat.

Pokazano również fragment strony z logami zarejestrowanymi przez filebeat.

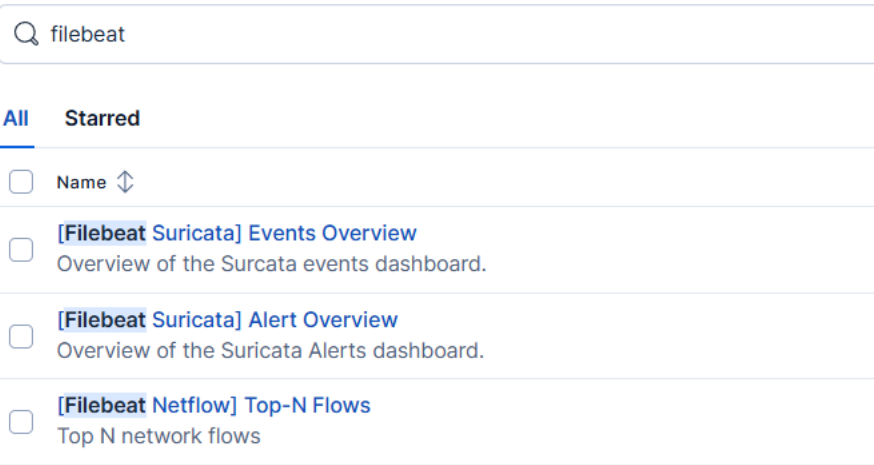




Rysunek 11: Widok DataView Kibany ze wszystkimi logami (fragment).

Każdy z beatsów posiada swoją gamę załadowanych, predefiniowanych dashboardów, oprócz Heartbeata i Winlogbeata, ponieważ stworzone były one ręcznie w Kibanie.

## Dashboards



Rysunek 12: Widok Dashboards Kibany

W sumie jest ich:

- **Filebeat:** 76
- **Packetbeat:** 13

- **Metricbeat:** 113
- **Auditbeat:** 11