What are Beats in the ELK ecosystem?

🔷 **What are Beats in the ELK ecosystem?**

Think of **Beats** as **tiny agents (lightweight shippers)** that sit on your servers, applications, or containers and **collect data/logs/metrics** → then send them to **Logstash** or **Elasticsearch**.

🔷 **Why do we use Beats?**

- They are **lightweight**, so they don't consume much system resources.
- Specialized: Each Beat is designed for a **specific type of data** (logs, metrics, network traffic, etc.).
- Easy to install and configure.

🔷 **Types of Beats (Most Common)**

1. **Filebeat** 📜
    - Collects **log files** from servers (e.g., Nginx logs, Apache logs, application logs).
    - Most commonly used Beat in production.
    - Example: Reading /var/log/nginx/access.log and shipping logs to Elasticsearch.
2. **Metricbeat** 📊
    - Collects **system and service metrics** (CPU, memory, disk usage, Nginx/Apache/DB performance).
    - Example: "CPU usage is 80% on Server A."
3. **Packetbeat** 🌐
    - Captures **network traffic** like TCP, UDP, HTTP, DNS, etc.
    - Example: Detecting slow HTTP requests between services.
4. **Winlogbeat** 🪟
    - Collects **Windows event logs**.
    - Example: Monitoring failed login attempts in Windows Server.
5. **Auditbeat** 🔒
    - Collects **security-related events** (who accessed files, who changed permissions).
    - Example: Detect unauthorized access to sensitive files.
6. **Heartbeat** ❤️
    - Checks **uptime/availability** of services.
    - Example: Ping your website every 30 seconds → alert if it goes down.

🔷 **Beats Flow (Simple Pipeline)**

[Filebeat / Metricbeat / Packetbeat] ---> [Logstash (optional)] ---> [Elasticsearch] ---> [Kibana]

- If you want **just logs → ES → Kibana**, Beats can send data **directly to Elasticsearch**.
- If you need **data transformation/cleaning**, you send Beats → Logstash → ES.

🔷 **Use Case in DevOps**

- **Filebeat**: Collect app logs from Kubernetes pods → send to Elasticsearch → view in Kibana.
- **Metricbeat**: Monitor EC2 CPU/Memory without CloudWatch.
- **Heartbeat**: Monitor if your APIs/URLs are up and running.

👉 So in short:

Beats = lightweight data shippers that bring data (logs, metrics, traffic, events) from your systems → into the ELK stack for storage, search, and visualization.

What are **Beats** in the ELK ecosystem?

A) Visualization tools like Kibana
B) Lightweight data shippers that collect logs/metrics/events
C) Database clusters in Elasticsearch
D) Plugins inside Logstash
Answer: B) Lightweight data shippers that collect logs/metrics/events

---

Which Beat is most commonly used to **collect log files** like Nginx, Apache, or application logs?

A) Metricbeat
B) Filebeat
C) Packetbeat
D) Auditbeat
Answer: B) Filebeat

Which Beat would you use to monitor **CPU, memory, and disk usage** on servers?

A) Packetbeat
B) Auditbeat
C) Metricbeat
D) Heartbeat
Answer: C) Metricbeat

What is the main purpose of **Packetbeat**?

A) Collecting Windows event logs
B) Capturing network traffic (TCP, UDP, HTTP, DNS)
C) Monitoring service uptime
D) Auditing file access
Answer: B) Capturing network traffic (TCP, UDP, HTTP, DNS)

Which Beat is specifically designed for **Windows event logs**?
A) Metricbeat
B) Winlogbeat
C) Filebeat
D) Auditbeat
Answer: B) Winlogbeat

Which Beat helps with **security auditing**, such as tracking file access or permission changes?
A) Filebeat
B) Auditbeat
C) Heartbeat
D) Packetbeat
Answer: B) Auditbeat

If you want to **monitor uptime/availability** of your APIs or websites, which Beat would you use?
A) Heartbeat
B) Packetbeat
C) Metricbeat
D) Winlogbeat
Answer: A) Heartbeat

Why might you send Beats data to **Logstash before Elasticsearch**?
A) To store raw data directly
B) To transform/clean/parse data before indexing
C) To visualize data in dashboards
D) To replace Kibana
Answer: B) To transform/clean/parse data before indexing