**File beat Installation Script for Ubuntu**

Save this script as install\_filebeat.sh and run it.

sh

#!/bin/bash

# Update package list

sudo apt update -y

# Download and install the Elastic GPG Key

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo tee /usr/share/keyrings/elasticsearch-keyring.asc

# Add the Elastic APT repository

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.asc] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

# Update package list again

sudo apt update -y

# Install Filebeat version 8.17.0

sudo apt install -y filebeat=8.17.0

# Enable and start Filebeat service

sudo systemctl enable filebeat

sudo systemctl start filebeat

# Check Filebeat status

sudo systemctl status filebeat --no-pager

# Print installation success message

echo "Filebeat 8.17.0 installation completed successfully!"

**How to Run the Script**

1. Save the script as install\_filebeat.sh.
2. Give execution permissions:

chmod +x install\_filebeat.sh

1. Run the script:

./install\_filebeat.sh

This will install **Filebeat 8.17.0**, enable the service, and check its status. Let me know if you need additional configurations!

**Logstash Installation Script for Ubuntu**

Here are the steps to install Logstash on the latest Ubuntu version:

### ****Step 1: Update System Packages****

sh

sudo apt update && sudo apt upgrade -y

### ****Step 2: Install Java (if not installed)****

Logstash requires Java. Install OpenJDK:

sh

sudo apt install -y openjdk-17-jdk

Verify Java installation:

sh

java -version

### ****Step 3: Add Elasticsearch Repository****

sh

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo tee /usr/share/keyrings/elasticsearch-keyring.asc

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.asc] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

### ****Step 4: Install Logstash****

sh

sudo apt update

sudo apt install -y logstash

### ****Step 5: Configure Logstash****

Edit the main configuration file:

sh

sudo nano /etc/logstash/logstash.yml

Modify settings as needed (e.g., pipeline configurations).

### ****Step 6: Configure Logstash Pipeline****

Create a sample pipeline:

sh

sudo nano /etc/logstash/conf.d/sample.conf

Add an example pipeline configuration:

plaintext

input {

beats {

port => 5044

}

}

filter {

mutate {

add\_field => { "example\_field" => "Hello Logstash" }

}

}

output {

elasticsearch {

hosts => ["http://localhost:9200"]

index => "logstash-test"

}

stdout { codec => rubydebug }

}

Save and exit.

### ****Step 7: Enable and Start Logstash****

sh

sudo systemctl enable logstash

sudo systemctl start logstash

Check service status:

sh

sudo systemctl status logstash

### ****Step 8: Verify Logstash****

Test Logstash manually:

sh

echo '{"message": "Hello, Logstash!"}' | /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/sample.conf

### ****Step 9: Allow Ports in Firewall (If Required)****

sh

sudo ufw allow 5044/tcp

sudo ufw reload

### ****Step 10: Monitor Logstash Logs****

sh

sudo journalctl -u logstash -f

Let me know if you need further customization!