## **📌 Logstash Installation on Ubuntu**

### ****1. Update System Packages****

sudo apt update && sudo apt upgrade -y

### ****2. Install Java****

sudo apt install openjdk-11-jdk -y

Verify:

java -version

### ****3. Add Elastic Repository****

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

### ****4. Install Logstash****

sudo apt update

sudo apt install logstash -y

### ****5. Enable and Start Logstash****

sudo systemctl enable logstash

sudo systemctl start logstash

sudo systemctl status logstash

## **📌 Logstash Installation on RHEL/CentOS**

### ****1. Update System****

sudo yum update -y

### ****2. Install Java****

sudo yum install -y java-11-openjdk

Verify:

java -version

### ****3. Add Elastic Repository****

sudo tee /etc/yum.repos.d/logstash.repo <<EOF

[logstash-8.x]

name=Elastic repository for 8.x packages

baseurl=https://artifacts.elastic.co/packages/8.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

EOF

### ****4. Install Logstash****

sudo yum install -y logstash

### ****5. Enable and Start Logstash****

sudo systemctl enable logstash

sudo systemctl start logstash

sudo systemctl status logstash

## **📌 Verify Logstash Installation (Both Ubuntu & RHEL)**

logstash --version

## **📌 Test Logstash with a Simple Pipeline**

Create a config file:

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

Add:

input {

stdin { }

}

output {

stdout { codec => rubydebug }

}

Save and exit.

Run Logstash:

sudo /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/test.conf

**Basic Command**

**Logstash Commands for Ubuntu & RHEL**

## **1. General Commands**

### ****Check Logstash Version****

logstash --version

Displays the installed Logstash version.

### ****Check Logstash Status****

sudo systemctl status logstash

Shows whether Logstash is running, stopped, or has encountered an error.

### ****Start Logstash****

sudo systemctl start logstash

Starts the Logstash service.

### ****Stop Logstash****

sudo systemctl stop logstash

Stops the Logstash service.

### ****Restart Logstash****

sudo systemctl restart logstash

Restarts the Logstash service after making configuration changes.

### ****Enable Logstash on Boot****

sudo systemctl enable logstash

Ensures Logstash starts automatically after a system reboot.

### ****Disable Logstash on Boot****

sudo systemctl disable logstash

Prevents Logstash from starting automatically on system boot.

## **2. Configuration & Plugin Commands**

### ****List Installed Logstash Plugins****

sudo /usr/share/logstash/bin/logstash-plugin list

Displays all installed plugins (inputs, outputs, filters, codecs).

### ****List Logstash Config Files****

ls -l /etc/logstash/conf.d/

Lists all Logstash pipeline configuration files.

### ****View Logstash Main Configuration (logstash.yml)****

cat /etc/logstash/logstash.yml

Displays the Logstash main configuration file.

### ****Edit Logstash Main Configuration****

sudo nano /etc/logstash/logstash.yml

Opens the Logstash config file for editing.

### ****Test Logstash Configuration Syntax****

sudo /usr/share/logstash/bin/logstash --config.test\_and\_exit -f /etc/logstash/conf.d/test.conf

Checks if the Logstash config file syntax is correct before applying changes.

### ****Run Logstash with a Specific Configuration****

sudo /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/test.conf

Starts Logstash using a specific pipeline config file (test.conf).

### ****View Logstash Logs (Real-time)****

sudo journalctl -u logstash -f

Shows real-time Logstash logs for debugging.

### ****View Logstash Logs (Old Logs)****

sudo cat /var/log/logstash/logstash-plain.log

Displays old Logstash logs.

## **3. Additional Commands**

### ****Manually Install a Logstash Plugin****

sudo /usr/share/logstash/bin/logstash-plugin install logstash-output-kafka

Installs a specific Logstash plugin (replace logstash-output-kafka with the desired plugin name).

### ****Remove a Logstash Plugin****

sudo /usr/share/logstash/bin/logstash-plugin remove logstash-output-kafka

Uninstalls a specific Logstash plugin.

### ****Check System Resource Usage by Logstash****

top -p $(pgrep -d',' -x java)

Shows CPU & memory usage of Logstash (which runs as a Java process).

### ****Find Logstash Process ID (PID)****

ps aux | grep logstash

Displays the process ID and running details of Logstash.

### ****Kill Logstash Process (If Stuck)****

sudo kill -9 $(pgrep -f logstash)

Forcefully stops Logstash if it is unresponsive.