# Packetbeat quick start: installation and configuratione:

### To install Packetbeat Oss version 7.10.2 RPM execute bellow command

## Install libpcap packet library

RPM

sudo yum install libpcap

DEB

sudo apt-get install libpcap0.8

Linux: You probably do not need to install libpcap.

## Step 1: Install Packetbeat

RPM

curl -L -O https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-oss-7.10.2-x86\_64.rpm

## Step 2: Setup Packetbeat

sudo rpm -vi packetbeat-oss-7.10.2-x86\_64.rpm

## Step 3: Connect to the elasticsearch

cd /etc/packetbeat/

vi packetbeat.yml

# ================================== Outputs ===================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------

output.elasticsearch:

# Array of hosts to connect to.

hosts: ["http://10.30.150.74:9200/"]

# Protocol - either `http` (default) or `https`.

#protocol: "https"

# Authentication credentials - either API key or username/password.

#api\_key: "id:api\_key"

username: "\*\*\*\*\*"

password: "\*\*\*\*\*"

## For more detail about configure the Sniffing refer :

<https://www.elastic.co/guide/en/beats/packetbeat/current/packetbeat-installation-configuration.html#packetbeat-installation-configuration>

l

### Step 3: Configure sniffing

In packetbeat.yml, configure the network devices and protocols to capture traffic from.

Set the sniffer type. By default, Packetbeat uses pcap, which uses the libpcap library and works on most platforms.

On Linux, set the sniffer type to af\_packet to use memory-mapped sniffing. This option is faster than libpcap and doesn’t require a kernel module, but it’s Linux-specific:

packetbeat.interfaces.type: af\_packet

Specify the network device to capture traffic from. For example:

packetbeat.interfaces.device: eth0

On Linux, specify packetbeat.interfaces.device: any to capture all messages sent or received by the server where Packetbeat is installed. The any setting does not work on macOS.

To see a list of available devices, run:

packetbeat devices

For more information about these settings, see [Traffic sniffing](https://www.elastic.co/guide/en/beats/packetbeat/current/configuration-interfaces.html" \o "Configure traffic capturing options).

In the protocols section, configure the ports where Packetbeat can find each protocol. If you use any non-standard ports, add them here. Otherwise, use the default values.

packetbeat.protocols:- type: dhcpv4

ports: [67, 68]

- type: dns

ports: [53]

- type: http

ports: [80, 8080, 8081, 5000, 8002]

- type: memcache

ports: [11211]

- type: mysql

ports: [3306,3307]

- type: pgsql

ports: [5432]

- type: redis

ports: [6379]

- type: thrift

ports: [9090]

- type: mongodb

ports: [27017]

- type: cassandra

ports: [9042]

- type: tls

ports: [443, 993, 995, 5223, 8443, 8883, 9243]

To test your configuration file, change to the directory where the Packetbeat binary is installed, and run Packetbeat in the foreground with the following options specified: sudo ./packetbeat test config -e. Make sure your config files are in the path expected by Packetbeat (see [Directory layout](https://www.elastic.co/guide/en/beats/packetbeat/current/directory-layout.html" \o "Directory layout)), or use the -c flag to specify the path to the config file. Depending on your OS, you might run into file ownership issues when you run this test. See [Config File Ownership and Permissions](https://www.elastic.co/guide/en/beats/libbeat/8.5/config-file-permissions.html" \t "https://www.elastic.co/guide/en/beats/packetbeat/current/_top) for more information.

For more information about configuring Packetbeat, also see:

[Configure Packetbeat](https://www.elastic.co/guide/en/beats/packetbeat/current/configuring-howto-packetbeat.html" \o "Configure Packetbeat)

[Config file format](https://www.elastic.co/guide/en/beats/libbeat/8.5/config-file-format.html" \t "https://www.elastic.co/guide/en/beats/packetbeat/current/_top)

[packetbeat.reference.yml](https://www.elastic.co/guide/en/beats/packetbeat/current/packetbeat-reference-yml.html" \o "packetbeat.reference.yml): This reference configuration file shows all non-deprecated options. You’ll find it in the same location as packetbeat.yml.

Step 4: Set up assets[edit](https://github.com/elastic/beats/edit/8.5/packetbeat/docs/getting-started.asciidoc" \o "Edit this page on GitHub)

Packetbeat comes with predefined assets for parsing, indexing, and visualizing your data. To load these assets:

Make sure the user specified in packetbeat.yml is [authorized to set up Packetbeat](https://www.elastic.co/guide/en/beats/packetbeat/current/privileges-to-setup-beats.html" \o "Grant privileges and roles needed for setup).

From the installation directory, run:

packetbeat setup -e

-e is optional and sends output to standard error instead of the configured log output.

This step loads the recommended [index template](https://www.elastic.co/guide/en/elasticsearch/reference/8.5/index-templates.html" \t "https://www.elastic.co/guide/en/beats/packetbeat/current/_top) for writing to Elasticsearch and deploys the sample dashboards for visualizing the data in Kibana.

A connection to Elasticsearch (or Elasticsearch Service) is required to set up the initial environment. If you’re using a different output, such as Logstash, see [Load the index template manually](https://www.elastic.co/guide/en/beats/packetbeat/current/packetbeat-template.html" \l "load-template-manually" \o "Load the index template manually) and [Load Kibana dashboards](https://www.elastic.co/guide/en/beats/packetbeat/current/load-kibana-dashboards.html" \o "Load Kibana dashboards).

## Step 4: Start Packetbeat

service packetbeat start

Check the status

systemctl status packetbeat -l

To check the configuration file of packetbeat --> rpm -qc packetbeat

To check the version --> packetbeat version

To find the help --> packetbeat help

To check the config validation--> packetbeat test config (If ok means its valid)

To check the output--> packetbeat test output

elasticsearch: http://10.30.150.216:9200/...

parse url... OK

connection...

parse host... OK

dns lookup... OK

addresses: 10.30.150.216

dial up... OK

TLS... WARN secure connection disabled

talk to server... OK

version: 7.10.2

To setup packetbeat --> packetbeat setup