**ELASTICSEARCH Setup**

**What Does the ELK Stack Stand For?**

ELK stands for Elasticsearch, Logstash, and Kibana. They are the three components of the [ELK stack](https://phoenixnap.com/kb/elk-stack).

**Elasticsearch** (indexes data) – This is the core of the Elastic software. Elasticsearch is a search and analytics engine used to sort through data.

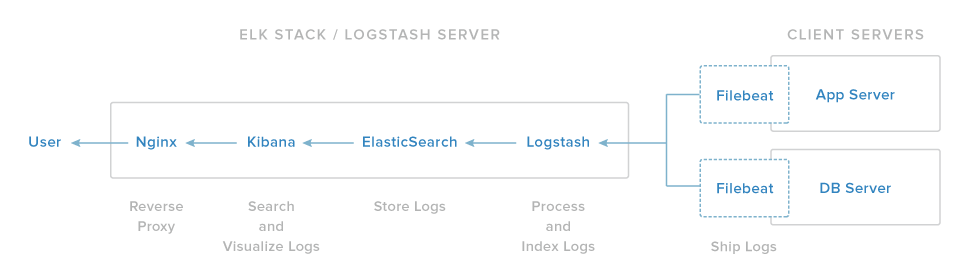
**Logstash** (collects data) – This package connects to various data sources, collates it, and directs it to storage. As its name suggests, it collects and “stashes” your log files.

**Kibana**(visualizes data) – [Kibana](https://phoenixnap.com/kb/kibana-nginx-proxy) is a graphical tool for visualizing data. Use it to generate charts and graphs to make sense of the raw data in your databases.

**---------------------------------------**

Our ELK stack setup has four main components:

* **Logstash**: The server component of Logstash that processes incoming logs
* **Elasticsearch**: Stores all of the logs
* **Kibana**: Web interface for searching and visualizing logs, which will be proxied through Nginx
* **Filebeat**: Installed on client servers that will send their logs to Logstash, Filebeat serves as a log shipping agent that utilizes the *lumberjack* networking protocol to communicate with Logstash



**Installation**

<https://phoenixnap.com/kb/install-elk-stack-centos-8>

**Step 1: Install OpenJDK 8 Java**

sudo yum install java-1.8.0-openjdk

## Step 2: Add Elasticsearch Repositories

### Import the Elasticsearch PGP Key

sudo rpm ––import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

### Add the Elasticsearch RPM Repository

cd /etc/yum.repos.d/  
sudo vim elasticsearch.repo  
[elasticstack]  
name=Elastic repository for 7.x packages  
baseurl=https://artifacts.elastic.co/packages/7.x/yum  
gpgcheck=1  
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch  
enabled=1  
autorefresh=1  
type=rpm-md

# dnf update

## Step 3: Install and Set Up Elasticsearch

sudo dnf install Elasticsearch

### Configure Elasticsearch

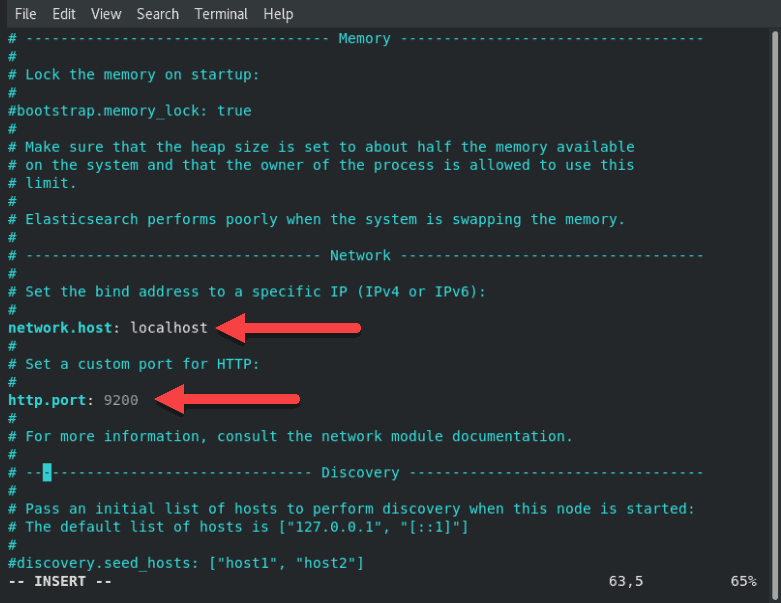
sudo vim /etc/elasticsearch/elasticsearch.yml

# Set the bind address to a specific IP (IPv4 or IPv6):

network.host: localhost

# Set a custom port for HTTP:

http.port: 9200



### Start Elasticsearch

sudo systemctl start Elasticsearch

sudo systemctl enable Elasticsearch

curl -X GET "localhost:9200"

## Step 4: Install and Set Up Kibana

sudo dnf install kibana

### Configure Kibana

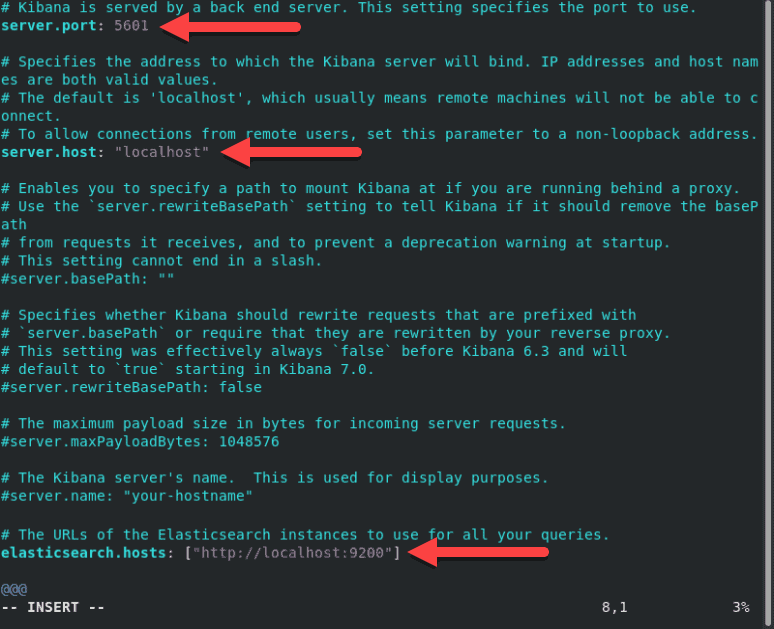
sudo vim /etc/kibana/kibana.yml

The lines should now look as follows:

server.port: 5601

server.host: "localhost"

elasticsearch.hosts: ["http://localhost:9200"]



#### **Start and Enable Kibana**

Next, start and enable the Kibana service:

sudo systemctl start kibana

sudo systemctl enable kibana

## Step 5: Install and Set Up Logstash

sudo dnf install logstash

cp /etc/logstash/config\_sample.conf /etc/logstash/conf.d/config.conf

### Start Logstash

Start and enable the Logstash service:

sudo systemctl start logstash

sudo systemctl enable logstash

config logstash if requirement

<https://www.elastic.co/guide/en/logstash/current/config-examples.html>

<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04>

## Step 6: Install Filebeat

sudo yum install filebeat

Next, add the **system** module, which will examine the local system logs:

sudo filebeat modules enable system

or

sudo filebeat modules enable nginx

or

sudo filebeat modules enable apache

Next, run the Filebeat setup:

sudo filebeat setup

Start the Filebeat service:

sudo service filebeat start

Launch your Kibana dashboard in a browser by visiting the following address:

http://localhost:5601

**FILEBEAT SETUP on AGENT**

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

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.0.0-amd64.deb

sudo dpkg -i filebeat-8.0.0-amd64.deb

#### Enable and configure data collection module

filebeat modules list

filebeat modules enable nginx

1. In the module config under modules.d, enable the desired datasets and change the module settings to match your environment. **Datasets are disabled by default.**

For example, log locations are set based on the OS. If your logs aren’t in default locations, set the paths variable:

- module: nginx

access:

enabled: true

var.paths: ["/var/log/nginx/access.log\*"]

To test your configuration file, change to the directory where the Filebeat binary is installed, and run Filebeat in the foreground with the following options specified: ./filebeat test config -e. Make sure your config files are in the path expected by Filebeat (see [Directory layout](https://www.elastic.co/guide/en/beats/filebeat/current/directory-layout.html)), or use the -c flag to specify the path to the config file.

filebeat setup -e

sudo service filebeat start

### Step 6: View your data in Kibana[edit](https://github.com/elastic/beats/edit/8.0/filebeat/docs/getting-started.asciidoc)

Filebeat comes with pre-built Kibana dashboards and UIs for visualizing log data. You loaded the dashboards earlier when you ran the setup command.

To open the dashboards:

In the side navigation, click **Discover**. To see Filebeat data, make sure the predefined filebeat-\* index pattern is selected.

1. In the side navigation, click **Dashboard**, then select the dashboard that you want to open.

The dashboards are provided as examples. We recommend that you [customize](https://www.elastic.co/guide/en/kibana/8.0/dashboard.html) them to meet your needs.

**Or best article**

[**https://logit.io/sources/configure/ubuntu**](https://logit.io/sources/configure/ubuntu)

**installation**

#### **STEP 2 - ENABLE SYSTEM MODULE**

There are several built in filebeat modules you can use. To enable the system module run.

sudo filebeat modules list

sudo filebeat modules enable system

Additional module configuration can be done using the per module config files located in the modules.d folder, most commonly this would be to read logs from a non-default location

**deb** /etc/filebeat/modules.d/

#### **STEP 3 - LOCATE CONFIGURATION FILE**

/etc/filebeat/filebeat.yml

#### **STEP 4 - CONFIGURE OUTPUT**

We'll be shipping to Logstash so that we have the option to run filters before the data is indexed.  
Comment out the elasticsearch output block.

## Comment out elasticsearch output

#output.elasticsearch:

# hosts: ["localhost:9200"]

Uncomment and change the logstash output to match below.

output.logstash:

hosts: ["your-logstash-host:your-ssl-port"]

loadbalance: true

ssl.enabled: true

#### **STEP 5 - VALIDATE CONFIGURATION**

Let's check the configuration file is syntactically correct by running filebeat directly inside the terminal. If the file is invalid, filebeat will print an error loading config file error message with details on how to correct the problem.

**deb/rpm**

sudo filebeat -e -c /etc/filebeat/filebeat.yml

**macOS**

cd <EXTRACTED\_ARCHIVE>

./filebeat -e -c filebeat.yml

**Windows**

cd <EXTRACTED\_ARCHIVE>

.\filebeat.exe -e -c filebeat.yml

#### **STEP 6 - START FILEBEAT**

Ok, time to start ingesting data!

sudo systemctl enable filebeat

sudo systemctl start filebeat

**filebeat custom path**

[**https://logit.io/sources/configure/apache**](https://logit.io/sources/configure/apache)

**deb/rpm** /etc/filebeat/modules.d/apache.yml  
**mac/win** <EXTRACTED\_ARCHIVE>/modules.d/apache.yml

- module: apache

# Access logs

access:

enabled: true

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

var.paths: ["/custom/path/to/logs"]

# Error logs

error:

enabled: true

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

var.paths: ["/custom/path/to/logs"]

**Password Setup on ELK**

[Set up minimal security for Elasticsearch | Elasticsearch Guide [7.17] | Elastic](https://www.elastic.co/guide/en/elasticsearch/reference/7.17/security-minimal-setup.html)

### Enable Elasticsearch security features

1. On **every** node in your cluster, stop both Kibana and Elasticsearch if they are running.
2. On **every** node in your cluster, add the xpack.security.enabled setting to the $ES\_PATH\_CONF/elasticsearch.yml file and set the value to true:

xpack.security.enabled: true

discovery.type: single-node

* Go to /usr/share/elasticsearch

Using the auto parameter outputs randomly-generated passwords to the console that you can change later if necessary:

./bin/elasticsearch-setup-passwords auto

If you want to use your own passwords, run the command with the interactive parameter instead of the auto parameter. Using this mode steps you through password configuration for all of the built-in users.

./bin/elasticsearch-setup-passwords interactive

Text

Description automatically generated

**LIVE ELK  
  
Changed password for user apm\_system  
PASSWORD apm\_system = 3Fs11zhZ5K7kMxTfTiCP**

**Changed password for user kibana\_system  
PASSWORD kibana\_system = ulPdNnbn3ypQzvHO0WVT**

**Changed password for user kibana  
PASSWORD kibana = ulPdNnbn3ypQzvHO0WVT**

**Changed password for user logstash\_system  
PASSWORD logstash\_system = fc8X0E0D0lQOR6ksvpD1**

**Changed password for user beats\_system  
PASSWORD beats\_system = qU9a9IQzOOHVM362HCfB**

**Changed password for user remote\_monitoring\_user  
PASSWORD remote\_monitoring\_user = PSrXfsgEM00VM38EJFNY**

**Changed password for user elastic  
PASSWORD elastic = En6KiXf7cFDX3QaaslWc**

### Configure Kibana to connect to Elasticsearch with a password

Add the elasticsearch.username setting to the KIB\_PATH\_CONF/kibana.yml file and set the value to the kibana\_system user:

elasticsearch.username: "kibana\_system"

From the directory where you installed Kibana, run the following commands to create the Kibana keystore and add the secure settings:

1. Create the Kibana keystore:

./bin/kibana-keystore create

1. Add the password for the kibana\_system user to the Kibana keystore:

./bin/kibana-keystore add elasticsearch.password

1. Restart Kibana. For example, if you installed Kibana with a .tar.gz package, run the following command from the Kibana directory:

Enter kibana\_system  password

./bin/kibana

1. Log in to Kibana as the elastic user. Use this superuser account to [manage spaces, create new users, and assign roles](https://www.elastic.co/guide/en/kibana/7.17/tutorial-secure-access-to-kibana.html). If you’re running Kibana locally, go to http://localhost:5601 to view the login page.

Text

Description automatically generated

**Changed password for user apm\_system old   
PASSWORD apm\_system = FbDYjM5HUDn8Gld5Sdi0**

**Changed password for user kibana\_system  
PASSWORD kibana\_system = 9QR4rGrHOp1mBXTDZaVz**

**Changed password for user kibana  
PASSWORD kibana = 9QR4rGrHOp1mBXTDZaVz old**

**Changed password for user logstash\_system  
PASSWORD logstash\_system = 3i2gpu0bnN12yCHcxPIf**

**Changed password for user beats\_system  
PASSWORD beats\_system = XIzi24o93wggHS6ufsNY**

**Changed password for user remote\_monitoring\_user  
PASSWORD remote\_monitoring\_user = OdfwSCeMwNI30R4MJMUJ old**

**Changed password for user elastic  
PASSWORD elastic = RmeMr1RsOk008127yn1m**

* **curl --user kibana\_system -X GET "localhost:9200"**
* **Update Password on Logstash**
* Under /etc/logstash/logstash.yml update logstash\_username

xpack.monitoring.elasticsearch.username: logstash\_system

xpack.monitoring.elasticsearch.password: 3i2gpu0bnN12yCHcxPIf

Text

Description automatically generated

**And**

* **Update elastic password   
  vim /etc/logstash/conf.d/logstash.conf**

**user => "elastic"**

**password => "RmeMr1RsOk008127yn1m"**

Text

Description automatically generated

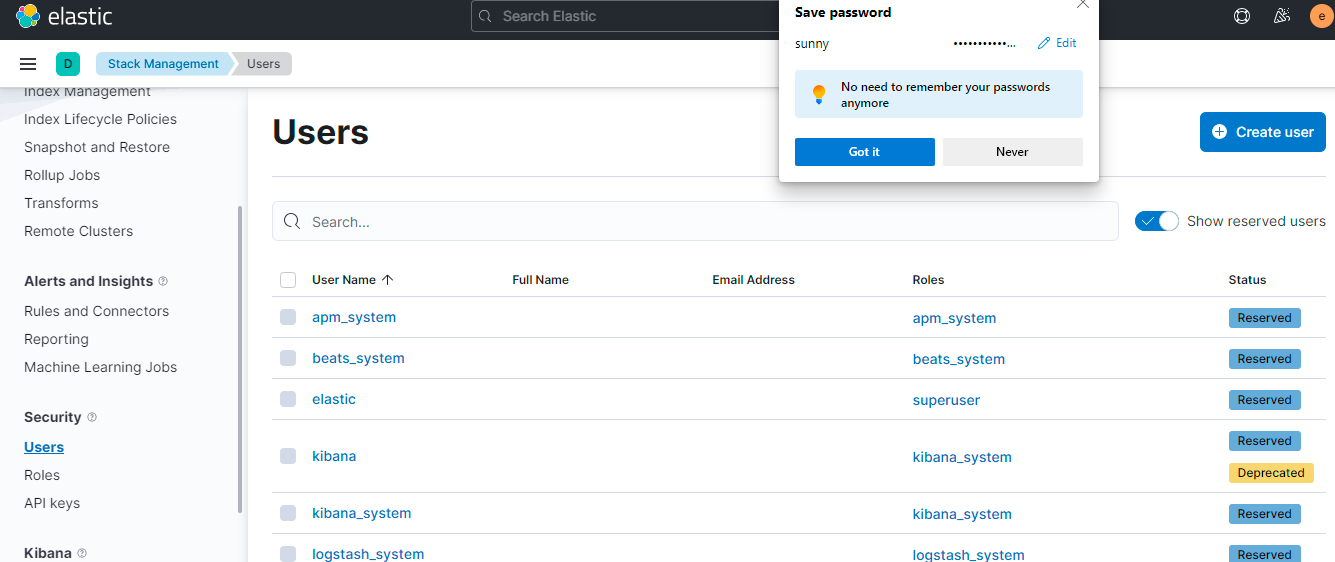
# [How to show multiple servers logs in Kibana separately from each other](https://stackoverflow.com/questions/66006719/how-to-show-mulitple-servers-logs-in-kibana-separatly-from-each-other)

Graphical user interface, text, application, email

Description automatically generated

Create user with different roles

Go to management –> select users under security and create user as per requirement.



Error :

server.publicBaseUrl is missing and should be configured when running in a production environment

Solution :

**MetricBeat SETUP on AGENT**

curl -L -O <https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.17.2-amd64.deb>

curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-8.2.2-amd64.deb

dpkg -i metricbeat-7.17.2-amd64.deb  
  
dpkg -i metricbeat-8.2.2-amd64.deb

cd /etc/metricbeat/

vim metricbeat.yml

output.logstash:

# The Logstash hosts

hosts: ["10.35.0.130:5044"]

output.elasticsearch:

# Array of hosts to connect to.

hosts: ["localhost:9200"]

username: "elastic"

password: "En6KiXf7cFDX3QaaslWc"

- module: elasticsearch

#metricsets:

# - node

# - node\_stats

period: 10s

hosts: ["http://10.35.0.130:9200"]

username: "elastic"

password: "En6KiXf7cFDX3QaaslWc"

- module: kibana

#metricsets:

# - status

period: 10s

hosts: ["localhost:6790"]

#basepath: ""

username: "kibana"

password: "ulPdNnbn3ypQzvHO0WVT"

metricbeat modules enable kibana  
metricbeat modules enable logstash  
metricbeat modules disable elasticsearch  
  
metricbeat setup  
  
systemctl restart metricbeat.service  
systemctl enable metricbeat.service

**FileBeat SETUP on AGENT**

curl -L -O <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.0.0-amd64.deb>  
sudo dpkg -i filebeat-8.0.0-amd64.deb  
filebeat modules list  
filebeat modules enable auditd  
filebeat modules enable system  
filebeat modules enable nginx  
filebeat modules enable crowdstrike  
sudo service filebeat start  
cd /etc/filebeat  
vim filebeat.yml

# filestream is an input for collecting log messages from files.  
- type: log  
  
 paths:

- /var/log/apache2/idace-surbo-access.log  
 - /var/log/\*.log  
  
output.logstash:

# The Logstash hosts  
 hosts: ["10.35.0.130:5044"]  
  
sudo filebeat -e -c /etc/filebeat/filebeat.yml

filebeat setup -e

telnet 10.35.0.130 5044

systemctl restart filebeat.service

var.paths: ["/app-log/\*.log"]