

ELK INSTALLATION IN DEBIAN

Step 1: Install Dependencies & Import GPG Key

First, update your package lists and install the necessary tools to handle HTTPS repositories.

```
sudo apt update
sudo apt install -y apt-transport-https software-properties-common wget curl gnupg
```

Next, import the official Elastic public signing key. This ensures the packages you download are genuine.

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

Step 2: Add the Elastic Repository

Add the Elastic 8.x repository to your system's source list.

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

Update your repository index to recognize the new packages:

```
sudo apt update
```

```
root@vbox:/home/elk# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
root@vbox:/home/elk# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo t
ee /etc/apt/sources.list.d/elasticsearch-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
root@vbox:/home/elk# sudo apt update
Hit:1 http://deb.debian.org/debian trixie InRelease
Hit:2 http://security.debian.org/debian-security trixie-security InRelease
Hit:3 http://deb.debian.org/debian trixie-updates InRelease
Get:4 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [3,248 B]
Get:5 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [98.7 kB]
Fetched 102 kB in 0s (289 kB/s)
All packages are up to date.
root@vbox:/home/elk# |
```

Step 3: Install Elasticsearch 8.13.1

To install the specific version **8.13.1**, we use the = operator

```
sudo apt install elasticsearch=8.13.1
```

```
root@vbox:/home/elk# sudo apt install elasticsearch=8.13.1
Installing:
  elasticsearch

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 574 MB
  Space needed: 1,133 MB / 111 GB available

Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.13.1 [574 MB]
1% [1 elasticsearch 7,968 kB/574 MB 1%]|
```

Step 4: Enable and Start Elasticsearch

```
sudo systemctl daemon-reload
sudo systemctl enable --now elasticsearch
```

```
root@vbox:/home/elk# nano token.txt
root@vbox:/home/elk# sudo systemctl daemon-reload
root@vbox:/home/elk# systemctl enable elasticsearch
Created symlink '/etc/systemd/system/multi-user.target.wants/elasticsearch.service' → '/usr/lib/systemd/system/elasticsearch.service'.
root@vbox:/home/elk# |
```

Step 5 : open a elasticsearch yml file and uncomment the line

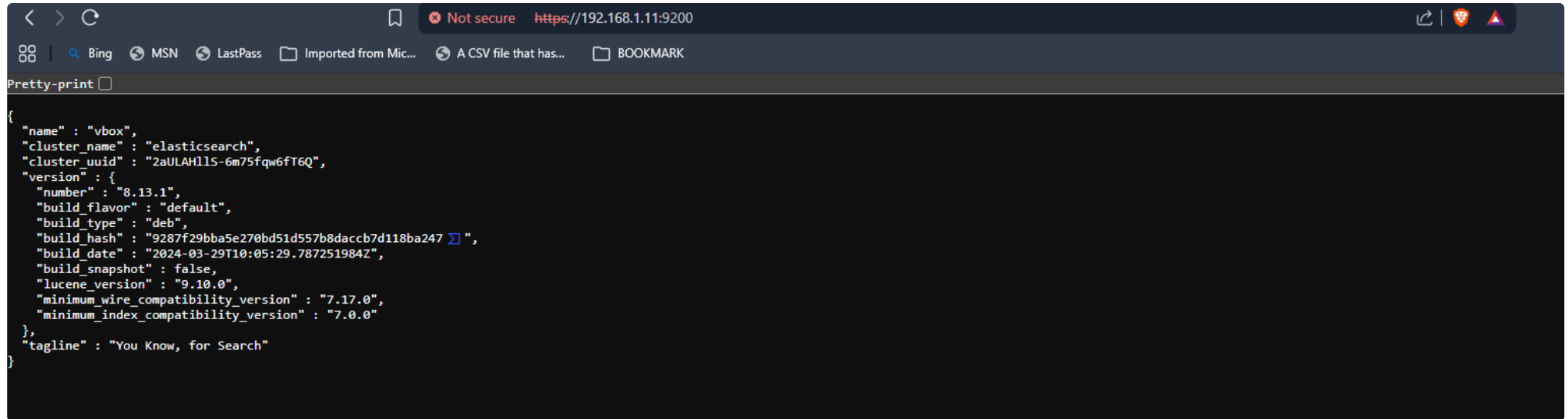
```
nano /etc/elasticsearch/elasticsearch.yml
```

```
#
# Use a descriptive name for your cluster:
#
cluster.name: my-application
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
#node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----- Paths -----
#
# Path to directory where to store the data (separate multiple locations by comma):
#
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
#
# ----- Memory -----
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
```

```
#  
http.port: 9200  
#  
# For more information, consult the network module documentation.
```

```
systemctl start elasticsearch
```

after change the config file start elasticsearch services



```
{  
  "name" : "vbox",  
  "cluster_name" : "elasticsearch",  
  "cluster_uuid" : "2aULAH1lS-6m75fqw6fT6Q",  
  "version" : {  
    "number" : "8.13.1",  
    "build_flavor" : "default",  
    "build_type" : "deb",  
    "build_hash" : "9287f29bba5e270bd51d557b8daccb7d118ba247",  
    "build_date" : "2024-03-29T10:05:29.787251984Z",  
    "build_snapshot" : false,  
    "lucene_version" : "9.10.0",  
    "minimum_wire_compatibility_version" : "7.17.0",  
    "minimum_index_compatibility_version" : "7.0.0"  
  },  
  "tagline" : "You Know, for Search"  
}
```

install kibana

```
sudo apt install kibana=8.13.1
```

```
root@vbox:/home/elk# sudo apt install kibana=8.13.1
Installing:
  kibana

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1
  Download size: 321 MB
  Space needed: 938 MB / 109 GB available

Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.13.1 [321 MB]
1% [1 kibana 3,827 kB/321 MB 1%]
```

Configure Kibana

Enable and start the service:

```
sudo systemctl enable --now kibana
```

Access the Setup: Open your web browser and go to `http://:5601`

```
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ===== System: Kibana Server =====
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.1.11"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# 'server.basePath' or require that they are rewritten by your reverse proxy.
# Defaults to 'false'.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# 'server.basePath' is configured this URL should end with the same basePath.
server.publicBaseUrl: "http://192.168.1.11:5601"

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"
```

open config file of kibana

```
nano /etc/kibana/kibana.yml
```

changes uper screenshot in config file



Configure Elastic to get started

Enrollment token

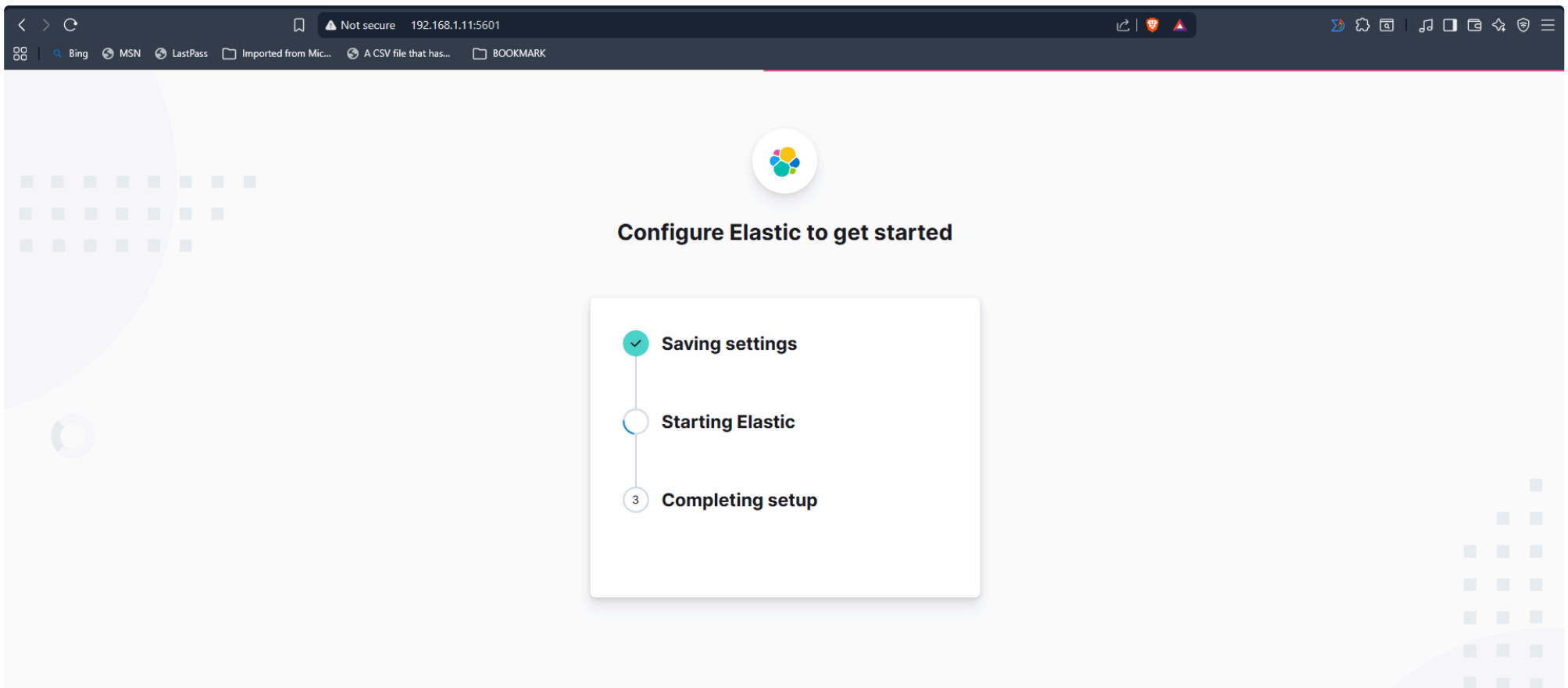
Paste enrollment token from terminal.

Where do I find this?

 [Configure manually](#)

[Configure Elastic](#)

```
Generate an enrollment token for Kibana instances with  
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```



```
New value: PaJYtMLNFFTbnggMuQCC
root@vbox:/usr/share/elasticsearch# nano pass.txt
root@vbox:/usr/share/elasticsearch# nano pass.txt
root@vbox:/usr/share/elasticsearch# sudo /usr/share/kibana/bin/kibana-verification-code
Your verification code is: 682 796
root@vbox:/usr/share/elasticsearch#
```


```
sudo /usr/share/kibana/bin/kibana-verification-code
```

elastic

Find apps, content, and more.


Home

Welcome home




Search

Create search experiences with a refined set of APIs and tools.




Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.



Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.




Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

[Add integrations](#)[Try sample data](#)[Upload a file](#)




Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.


[Move to Elastic Cloud](#)

Management




Manage permissions

Control who has access and what tasks they can perform.




Monitor the stack

Track the real-time health and performance of your stack.



Back up and restore

Save snapshots to a backup repository, and restore to a new or existing index.



Manage index lifecycles

Define lifecycle policies to automatically perform actions on indices.

[Dev Tools](#)[Stack Management](#)

install logstash

```
root@vbox:~# sudo apt install logstash=1:8.13.1-1
Installing:
  logstash

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2
  Download size: 404 MB
  Space needed: 668 MB / 107 GB available

Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.13.1-1 [404 MB]
Fetched 404 MB in 44s (9,230 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 226941 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.13.1-1_amd64.deb ...
Unpacking logstash (1:8.13.1-1) ...
Setting up logstash (1:8.13.1-1) ...
root@vbox:~# sudo systemctl enable --now logstash
Created symlink '/etc/systemd/system/multi-user.target.wants/logstash.service' → '/usr/lib/systemd/system/logstash.service'.
root@vbox:~# sudo systemctl start logstash
root@vbox:~# |
```

Install Logstash with the matching version.

```
sudo apt install logstash=8.13.1
```

nable and start Logstash:

```
sudo systemctl enable --now logstash
```

```
sudo systemctl start logstash
```