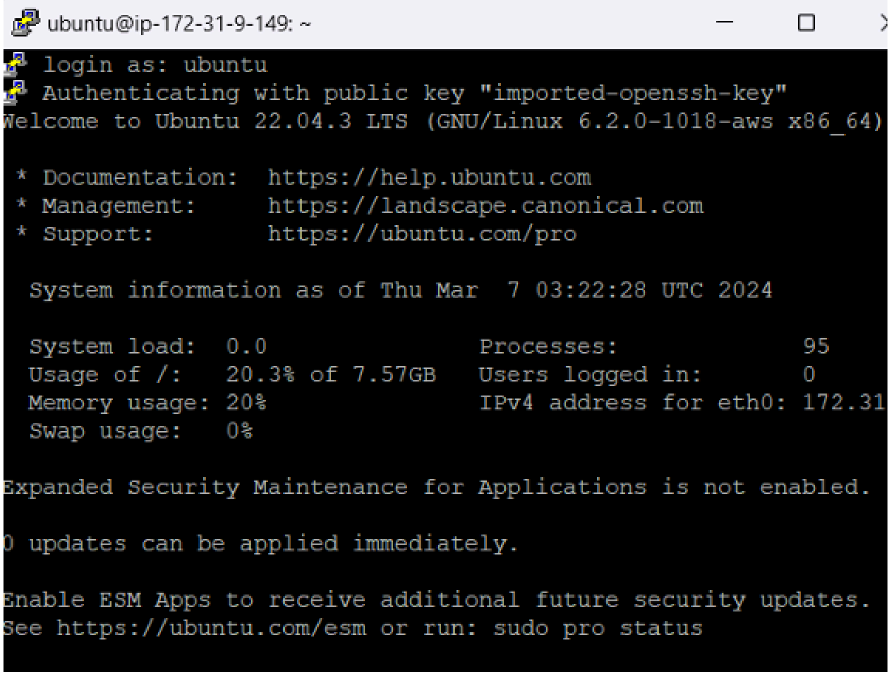
Create an ec2 instance to host TheHIVE

- TheHive is a resource-intensive application, especially if it handles large volumes of data.
- A minimum of 2 vCPUs and 4 GB of RAM is recommended for small to medium deployments.
    - ***t3.medium**: 2 vCPUs, 4 GB RAM*

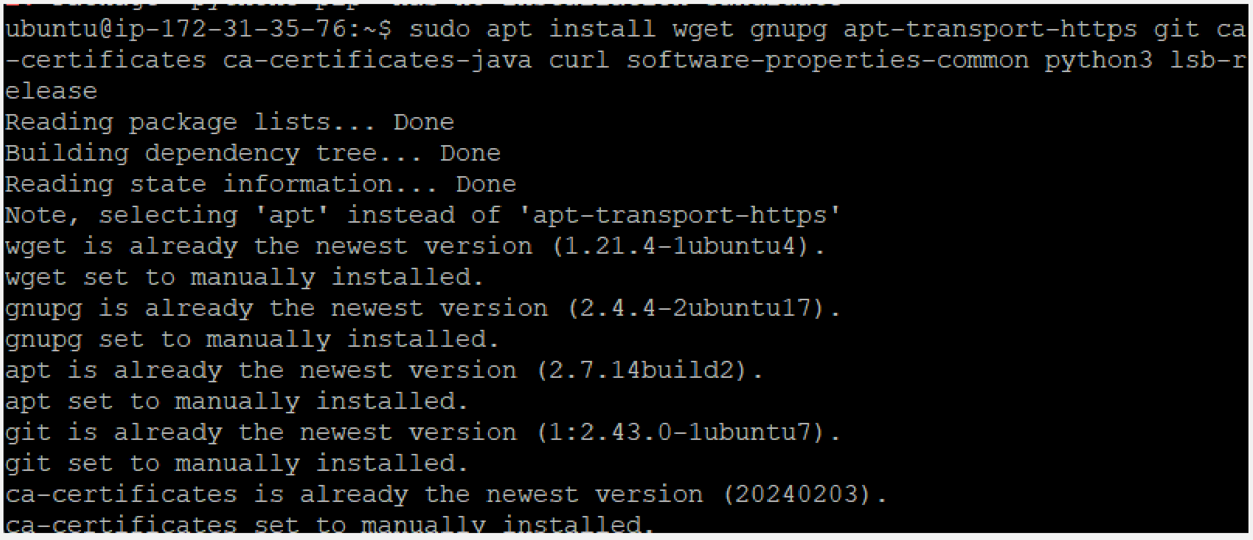
Connect to the instance via ssh



```
 login as: ubuntu
 Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Thu Mar  7 03:22:28 UTC 2024

  System load:  0.0               Processes:             95
  Usage of /:   20.3% of 7.57GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 172.31
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

Installing Dependencies

sudo apt install wget gnupg apt-transport-https git ca-certificates ca-certificates-java curl software-properties-common python3 lsb-release



```
ubuntu@ip-172-31-35-76:~$ sudo apt install wget gnupg apt-transport-https git ca
-certificates ca-certificates-java curl software-properties-common python3 lsb-r
elease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'apt' instead of 'apt-transport-https'
wget is already the newest version (1.21.4-1ubuntu4).
wget set to manually installed.
gnupg is already the newest version (2.4.4-2ubuntu17).
gnupg set to manually installed.
apt is already the newest version (2.7.14build2).
apt set to manually installed.
git is already the newest version (1:2.43.0-1ubuntu7).
git set to manually installed.
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
```

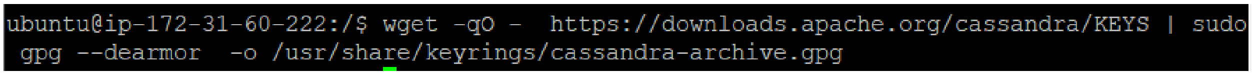
Java Installation

wget -qO- https://apt.corretto.aws/corretto.key | sudo gpg --dearmor -o /usr/share/keyrings/corretto.gpg
echo "deb [signed-by=/usr/share/keyrings/corretto.gpg] https://apt.corretto.aws stable main" | sudo tee -a /etc/apt/sources.list.d/corretto.sources.list
sudo apt update
sudo apt install java-common java-11-amazon-corretto-jdk
echo JAVA_HOME="/usr/lib/jvm/java-11-amazon-corretto" | sudo tee -a /etc/environment
export JAVA_HOME="/usr/lib/jvm/java-11-amazon-corretto"

Apache Cassandra Installation

- Download Apache Cassandra repository keys

wget -qO - https://downloads.apache.org/cassandra/KEYS | sudo gpg --dearmor -o /usr/share/keyrings/cassandra-archive.gpg



```
ubuntu@ip-172-31-60-222:/$ wget -qO -  https://downloads.apache.org/cassandra/KEYS | sudo
 gpg --dearmor  -o /usr/share/keyrings/cassandra-archive.gpg
```

- Add the repository to your system

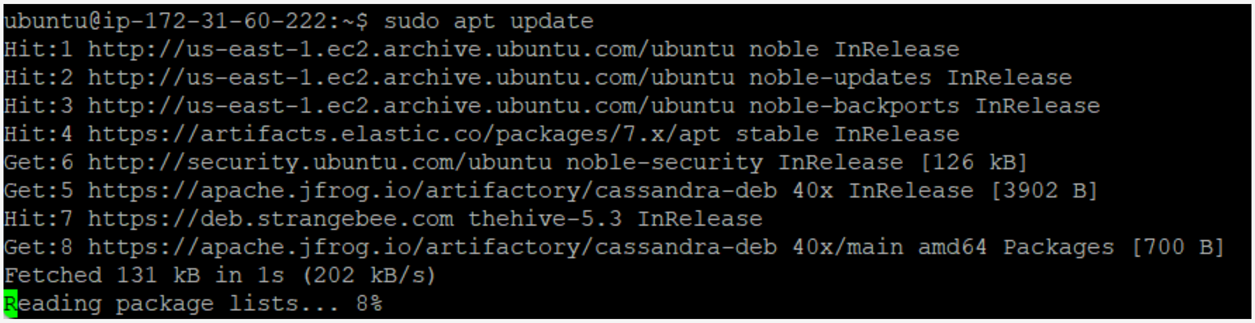
/etc/apt/sources.list.d/cassandra.sources.list

This file may not exist, and you may need to create it.

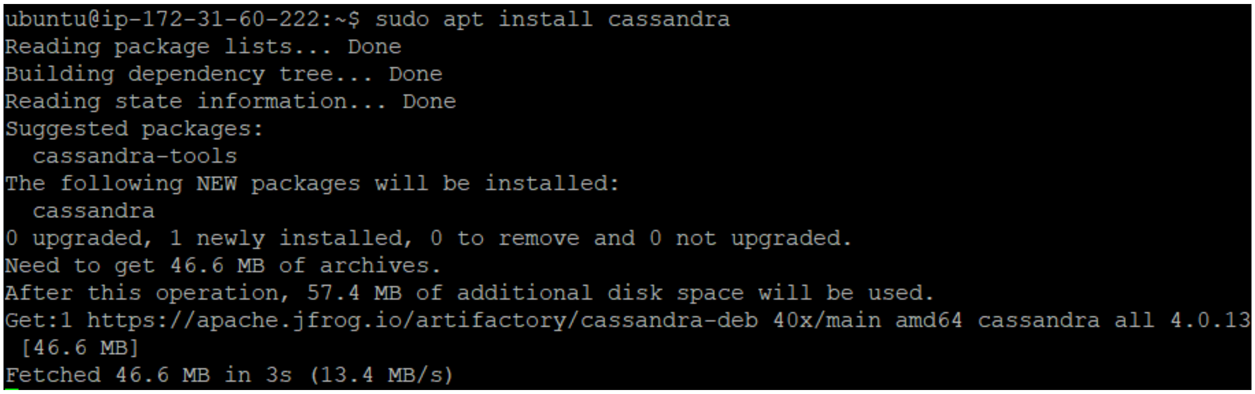
- *echo "deb [signed-by=/usr/share/keyrings/cassandra-archive.gpg] https://debian.cassandra.apache.org 40x main" | sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list*

- Install the package.
- Once the repository references are added, update your package index and install Cassandra.

sudo apt update
sudo apt install cassandra



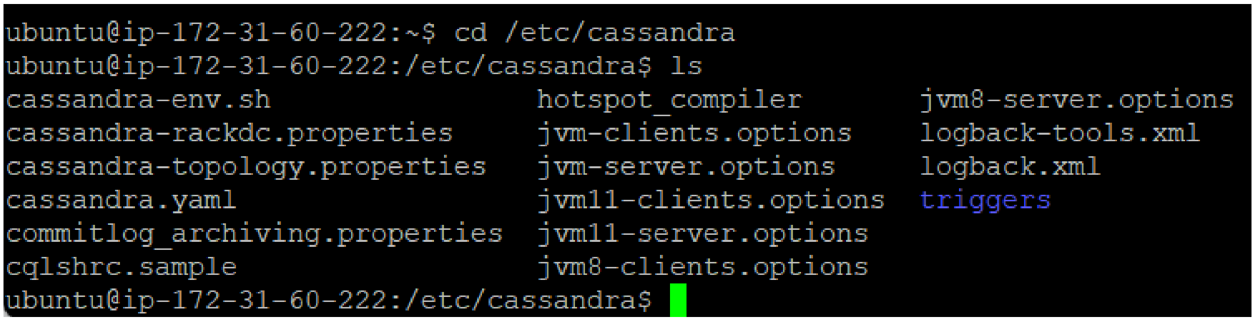
```
ubuntu@ip-172-31-60-222:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Get:6 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 https://apache.jfrog.io/artifactory/cassandra-deb 40x InRelease [3902 B]
Hit:7 https://deb.strangebee.com thehive-5.3 InRelease
Get:8 https://apache.jfrog.io/artifactory/cassandra-deb 40x/main amd64 Packages [700 B]
Fetched 131 kB in 1s (202 kB/s)
Reading package lists... 8%
```



```
ubuntu@ip-172-31-60-222:~$ sudo apt install cassandra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  cassandra-tools
The following NEW packages will be installed:
  cassandra
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 46.6 MB of archives.
After this operation, 57.4 MB of additional disk space will be used.
Get:1 https://apache.jfrog.io/artifactory/cassandra-deb 40x/main amd64 cassandra all 4.0.13
 [46.6 MB]
Fetched 46.6 MB in 3s (13.4 MB/s)
```

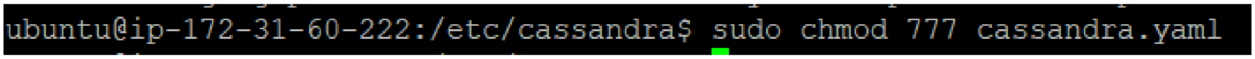
Cassandra Configuration

You can configure Cassandra by modifying settings within the */etc/cassandra/cassandra.yaml file.*

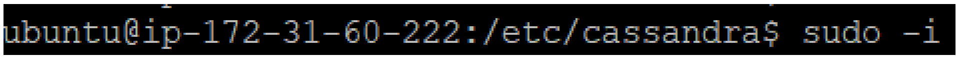


```
ubuntu@ip-172-31-60-222:~$ cd /etc/cassandra
ubuntu@ip-172-31-60-222:/etc/cassandra$ ls
cassandra-env.sh                 hotspot_compiler       jvm8-server.options
cassandra-rackdc.properties      jvm-clients.options    logback-tools.xml
cassandra-topology.properties    jvm-server.options     logback.xml
cassandra.yaml                   jvm11-clients.options  triggers
commitlog_archiving.properties   jvm11-server.options
cqlshrc.sample                   jvm8-clients.options
ubuntu@ip-172-31-60-222:/etc/cassandra$
```

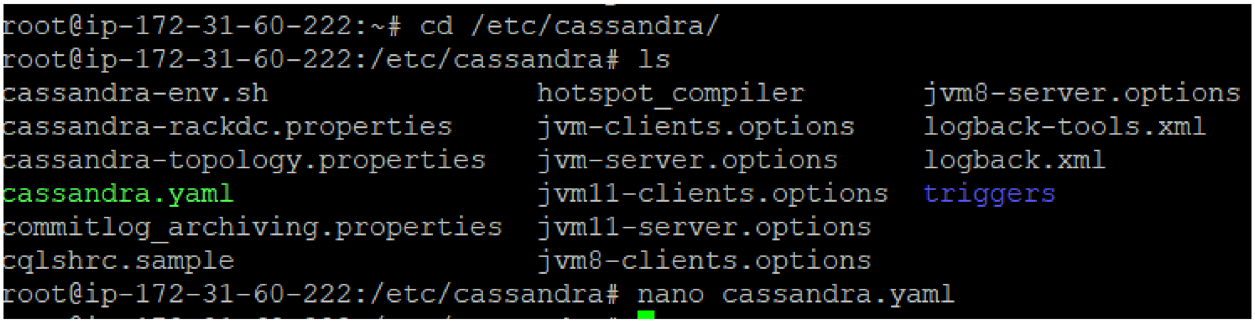
- Set appropriate permissions



```
ubuntu@ip-172-31-60-222:/etc/cassandra$ sudo chmod 777 cassandra.yaml
```

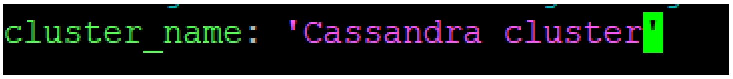


```
ubuntu@ip-172-31-60-222:/etc/cassandra$ sudo -i
```



```
root@ip-172-31-60-222:~# cd /etc/cassandra/
root@ip-172-31-60-222:/etc/cassandra# ls
cassandra-env.sh                 hotspot_compiler       jvm8-server.options
cassandra-rackdc.properties      jvm-clients.options    logback-tools.xml
cassandra-topology.properties    jvm-server.options     logback.xml
cassandra.yaml                   jvm11-clients.options  triggers
commitlog_archiving.properties   jvm11-server.options
cqlshrc.sample                   jvm8-clients.options
root@ip-172-31-60-222:/etc/cassandra# nano cassandra.yaml
```

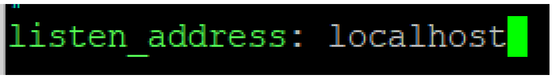
- Set the `cluster_name` parameter to the desired name. This name helps identify the Cassandra cluster.



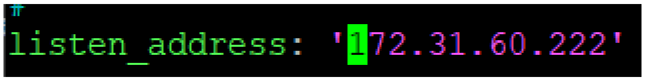
```
cluster_name: 'Cassandra cluster'
```

- Set the `listen_address` parameter to the IP address of the node within the cluster. This address is used by other nodes within the cluster to communicate.
- Set the `rpc_address` parameter to the IP address of the node to enable clients to connect to the Cassandra cluster.
- Ensure the `seed_provider` section is properly configured. The `seeds` parameter should contain the IP address(es) of the seed node(s) in the cluster.
- Set the directories for data storage, commit logs, saved caches, and hints as per your requirements. Ensure that the specified directories exist and have appropriate permissions.
- After making the necessary configurations, save the changes to the `cassandra.yaml` file.

```
cluster_name: 'Cassandra cluster'
listen_address: 'YOUR_PRIVATE_IP'
```

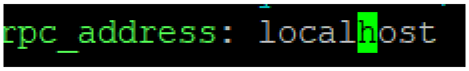


```
listen_address: localhost
```

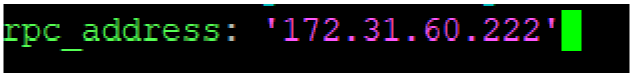


```
listen_address: '172.31.60.222'
```

```
rpc_address: 'YOUR_PRIVATE_IP'
```

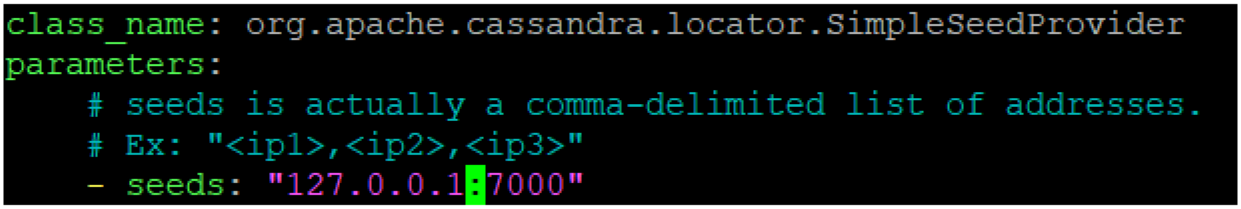


```
rpc_address: localhost
```



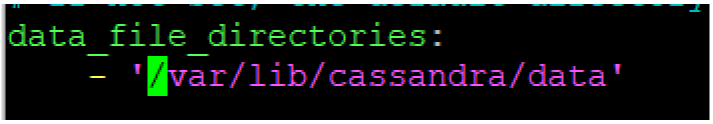
```
rpc_address: '172.31.60.222'
```

```
seed_provider:
  - class_name: org.apache.cassandra.locator.SimpleSeedProvider
    parameters:
      - seeds: 'YOUR_PRIVATE_IP'
```



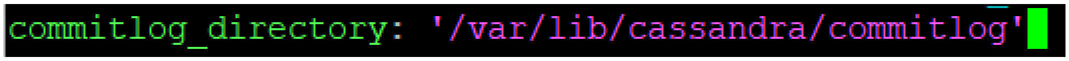
```
class_name: org.apache.cassandra.locator.SimpleSeedProvider
parameters:
    # seeds is actually a comma-delimited list of addresses.
    # Ex: "<ip1>,<ip2>,<ip3>"
    - seeds: "127.0.0.1:7000"
```

```
data_file_directories:
  - '/var/lib/cassandra/data'
```



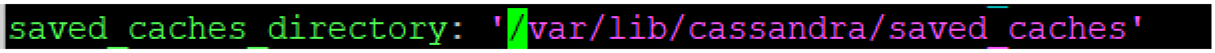
```
data_file_directories:
    - '/var/lib/cassandra/data'
```

commitlog_directory: '/var/lib/cassandra/commitlog'



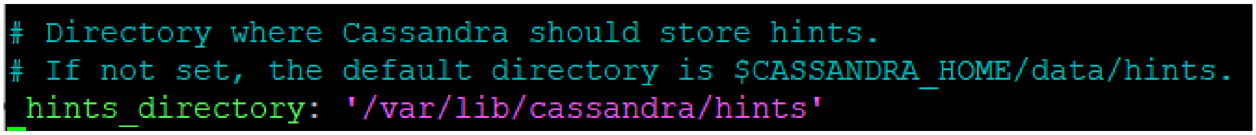
```
commitlog_directory: '/var/lib/cassandra/commitlog'
```

saved_caches_directory: '/var/lib/cassandra/saved_caches'



```
saved_caches_directory: '/var/lib/cassandra/saved_caches'
```

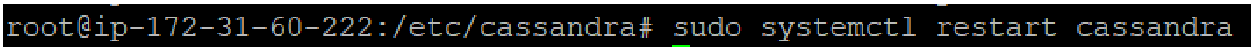
hints_directory:
- '/var/lib/cassandra/hints'



```
# Directory where Cassandra should store hints.
# If not set, the default directory is $CASSANDRA_HOME/data/hints.
 hints_directory: '/var/lib/cassandra/hints'
```

Restart Cassandra

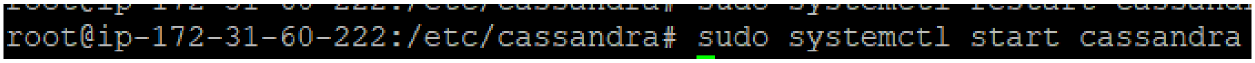
sudo systemctl restart cassandra



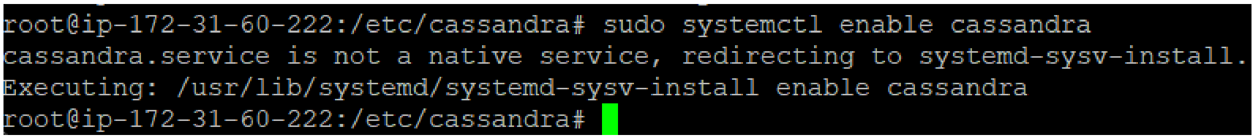
```
root@ip-172-31-60-222:/etc/cassandra# sudo systemctl restart cassandra
```

Start and Enable Cassandra

sudo systemctl start cassandra
sudo systemctl enable cassandra



```
root@ip-172-31-60-222:/etc/cassandra# sudo systemctl start cassandra
```

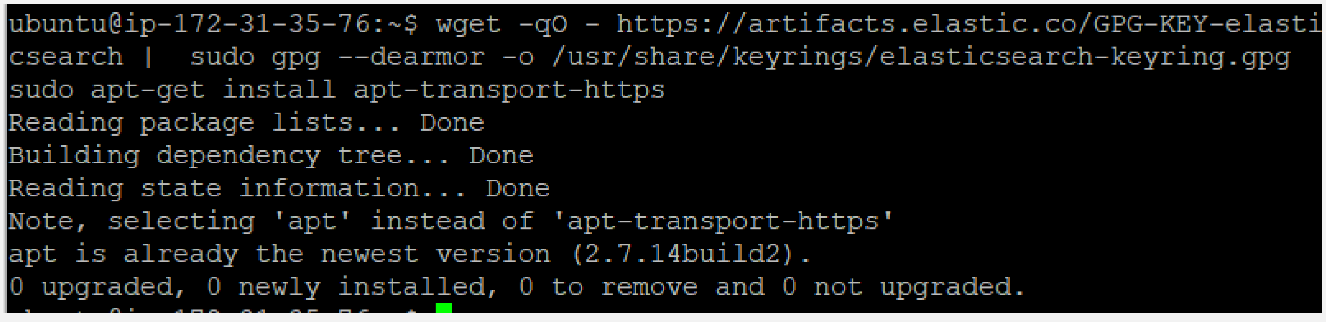


```
root@ip-172-31-60-222:/etc/cassandra# sudo systemctl enable cassandra
cassandra.service is not a native service, redirecting to systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable cassandra
root@ip-172-31-60-222:/etc/cassandra#
```

Executing Command to add Elasticsearch repository keys

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

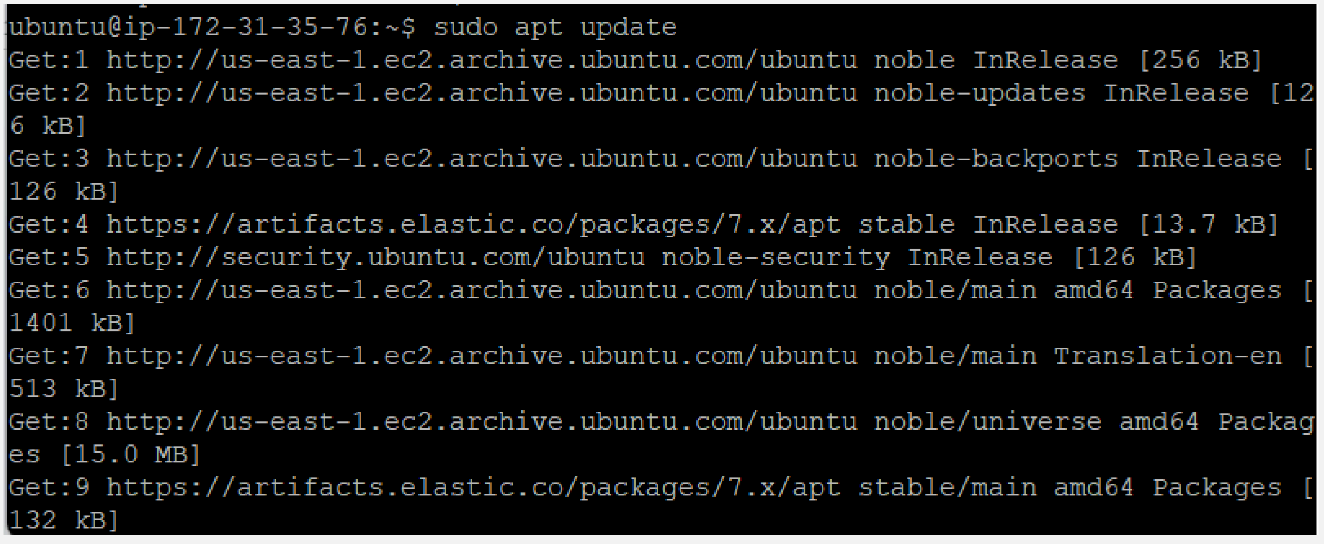
sudo apt-get install apt-transport-https



```
ubuntu@ip-172-31-35-76:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasti
csearch |  sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'apt' instead of 'apt-transport-https'
apt is already the newest version (2.7.14build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Update

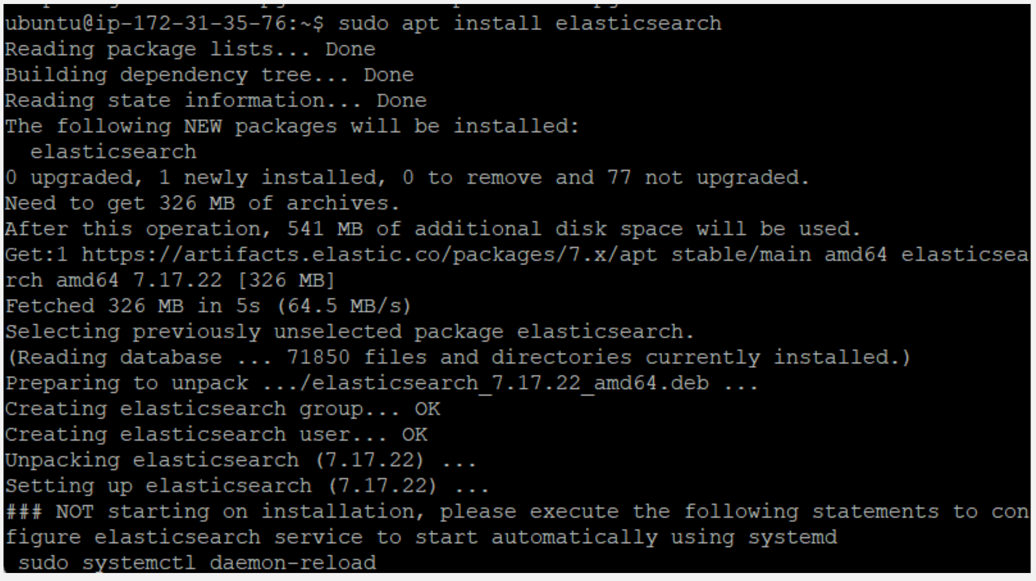
sudo apt update



```
ubuntu@ip-172-31-35-76:~$ sudo apt update
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease [256 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [12
6 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [
126 kB]
Get:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 Packages [
1401 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main Translation-en [
513 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packag
es [15.0 MB]
Get:9 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [
132 kB]
```

Install Elasticsearch

sudo apt install elasticsearch



```
ubuntu@ip-172-31-35-76:~$ sudo apt install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 77 not upgraded.
Need to get 326 MB of archives.
After this operation, 541 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsea
rch amd64 7.17.22 [326 MB]
Fetched 326 MB in 5s (64.5 MB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 71850 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.22_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.17.22) ...
Setting up elasticsearch (7.17.22) ...
### NOT starting on installation, please execute the following statements to con
figure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
```

If those commands don't allow you to install elasticsearch, try these.

- *sudo apt-get update*
- *sudo apt-get upgrade*
- *sudo apt-get install apt-transport-https ca-certificates curl software-properties-common*
- *curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg*
- *echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list*
- *sudo apt-get update*
- *sudo apt-get install elasticsearch*

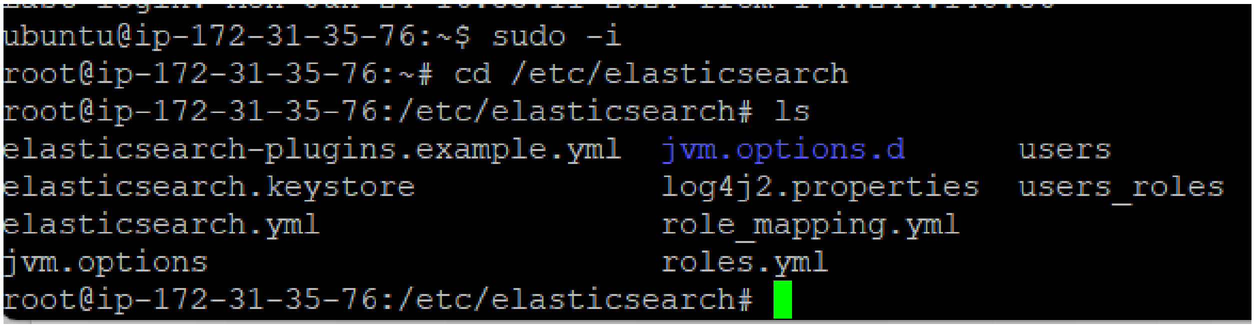
Configuring the /etc/elasticsearch/elastic.yml

- Navigate to the directory containing the Elasticsearch config file

sudo -i

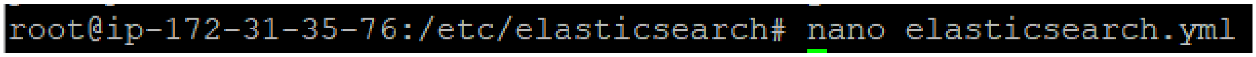
root@ip-172-31-35-76: *cd /etc/elasticsearch*

root@ip-172-31-35-76: */etc/elasticsearch then ls*



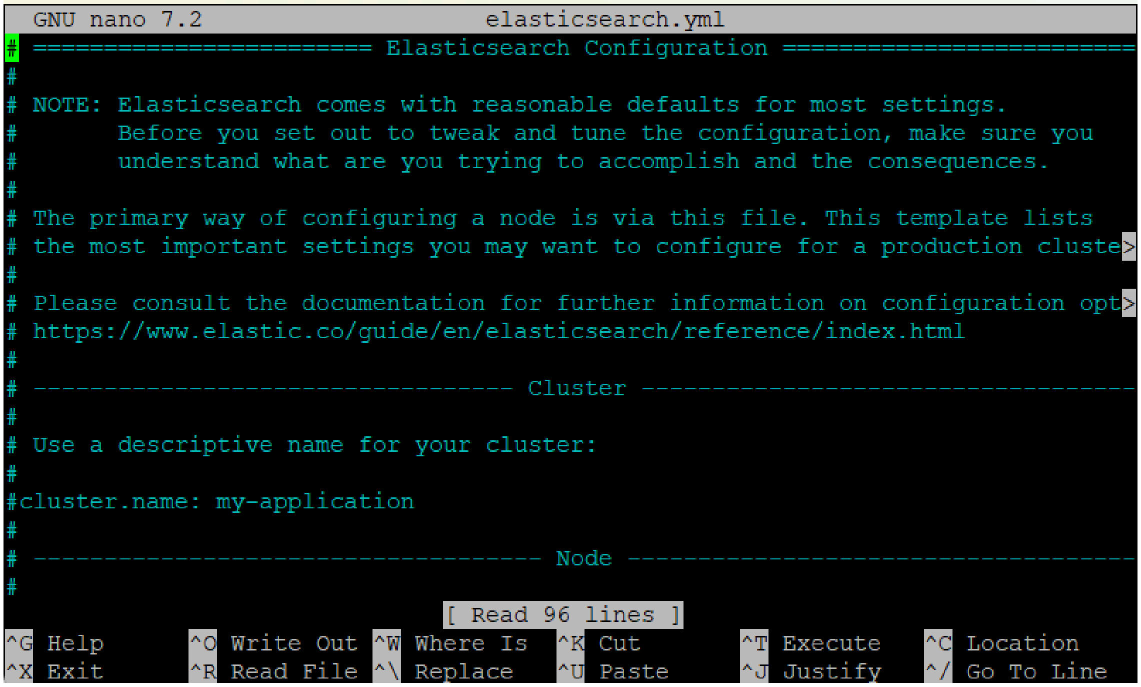
```
ubuntu@ip-172-31-35-76:~$ sudo -i
root@ip-172-31-35-76:~# cd /etc/elasticsearch
root@ip-172-31-35-76:/etc/elasticsearch# ls
elasticsearch-plugins.example.yml  jvm.options.d      users
elasticsearch.keystore             log4j2.properties  users_roles
elasticsearch.yml                  role_mapping.yml
jvm.options                        roles.yml
root@ip-172-31-35-76:/etc/elasticsearch#
```

- Open the `elasticsearch.yml` file in a text editor with appropriate permissions.

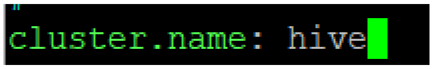


```
root@ip-172-31-35-76:/etc/elasticsearch# nano elasticsearch.yml
```

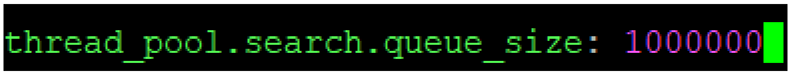
- Configure the `elasticsearch.yml` file and Save changes



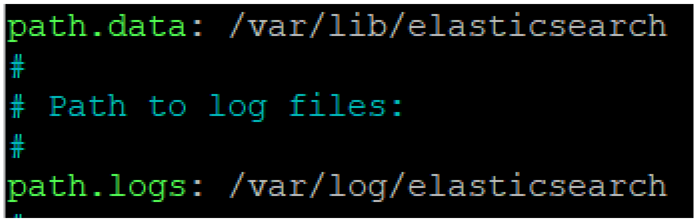
```
  GNU nano 7.2                       elasticsearch.yml
# ======================== Elasticsearch Configuration =========================
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
#       Before you set out to tweak and tune the configuration, make sure you
#       understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluste>
#
# Please consult the documentation for further information on configuration opt>
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
#cluster.name: my-application
#
# ------------------------------------ Node ------------------------------------
#
                              [ Read 96 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```



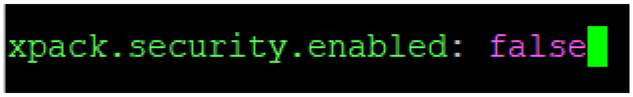
```
cluster.name: hive
```



```
thread_pool.search.queue_size: 1000000
```



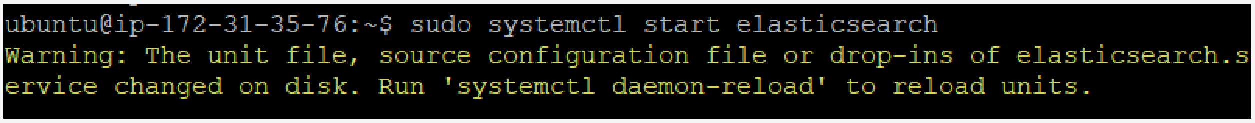
```
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
```



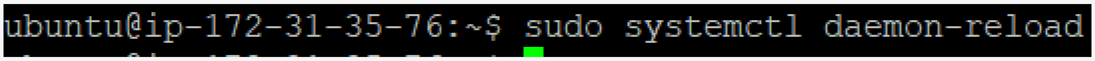
```
xpack.security.enabled: false
```

Start and enable the Elasticsearch service

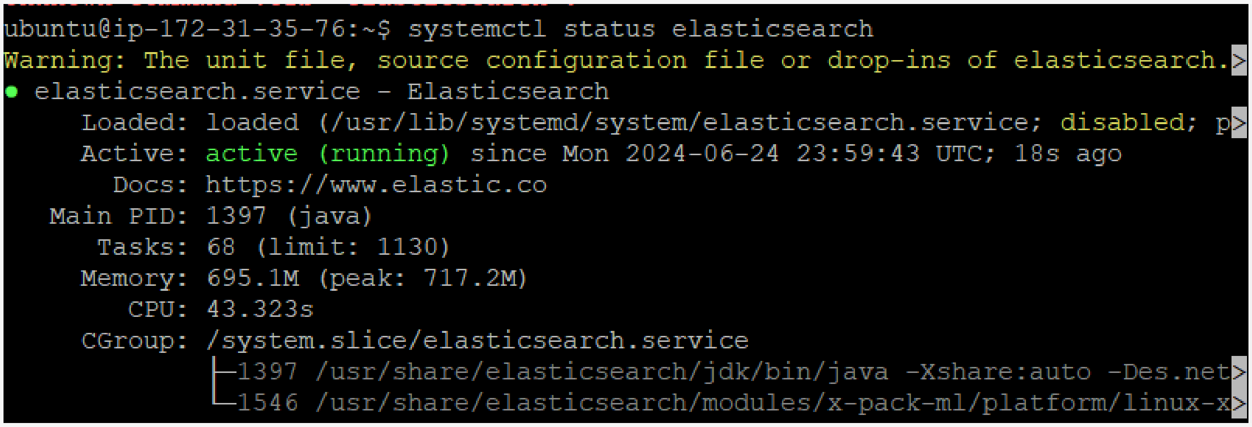
sudo systemctl start elasticsearch



```
ubuntu@ip-172-31-35-76:~$ sudo systemctl start elasticsearch
Warning: The unit file, source configuration file or drop-ins of elasticsearch.s
ervice changed on disk. Run 'systemctl daemon-reload' to reload units.
```

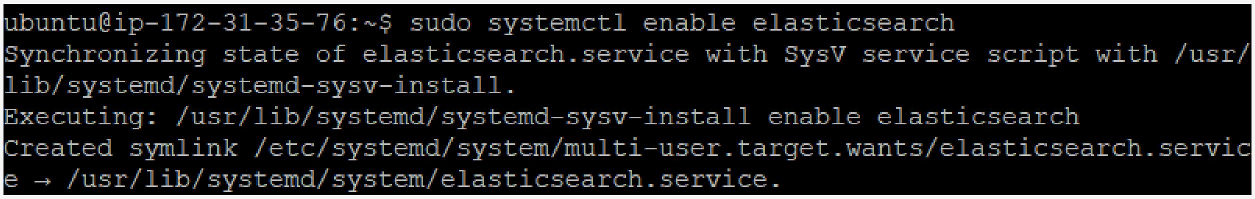


```
ubuntu@ip-172-31-35-76:~$ sudo systemctl daemon-reload
```

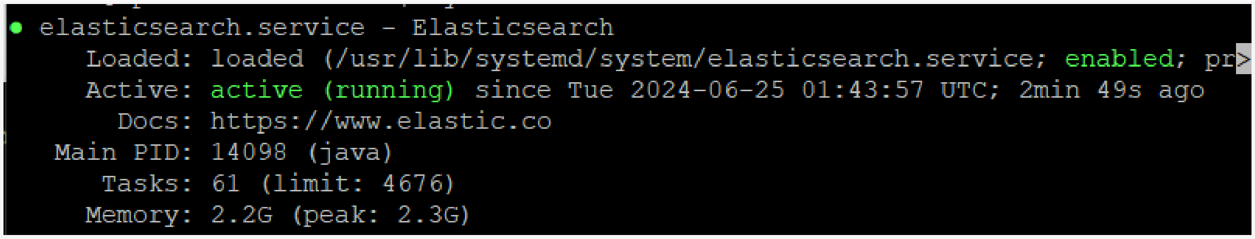


```
ubuntu@ip-172-31-35-76:~$ systemctl status elasticsearch
Warning: The unit file, source configuration file or drop-ins of elasticsearch.>
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; p>
     Active: active (running) since Mon 2024-06-24 23:59:43 UTC; 18s ago
       Docs: https://www.elastic.co
   Main PID: 1397 (java)
      Tasks: 68 (limit: 1130)
     Memory: 695.1M (peak: 717.2M)
        CPU: 43.323s
     CGroup: /system.slice/elasticsearch.service
             ├─1397 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net>
             └─1546 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>
```

sudo systemctl enable elasticsearch



```
ubuntu@ip-172-31-35-76:~$ sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /usr/
lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.servic
e → /usr/lib/systemd/system/elasticsearch.service.
```

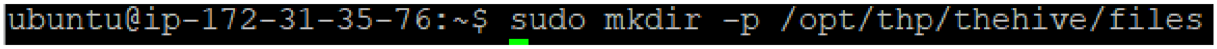


```
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr>
     Active: active (running) since Tue 2024-06-25 01:43:57 UTC; 2min 49s ago
       Docs: https://www.elastic.co
   Main PID: 14098 (java)
      Tasks: 61 (limit: 4676)
     Memory: 2.2G (peak: 2.3G)
```

File Storage

- To utilize the local filesystem for file storage, begin by selecting a dedicated folder. By default, this folder is located at `/opt/thp/thehive/files`:

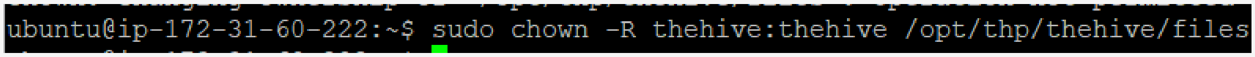
sudo mkdir -p /opt/thp/thehive/files



```
ubuntu@ip-172-31-35-76:~$ sudo mkdir -p /opt/thp/thehive/files
```

- This path will be utilized in the configuration of TheHive. After installing TheHive, it's important to ensure that the user TheHive owns the chosen path for storing files:

chown -R thehive:thehive /opt/thp/thehive/files

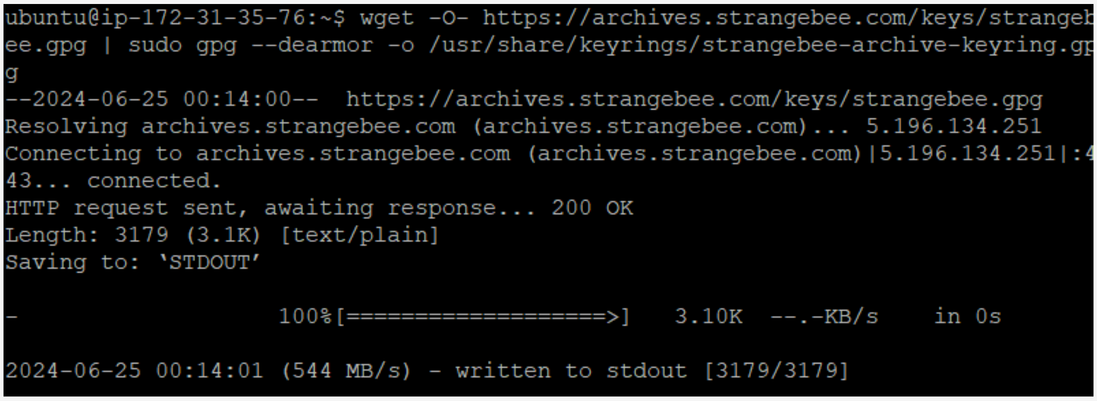


```
ubuntu@ip-172-31-60-222:~$ sudo chown -R thehive:thehive /opt/thp/thehive/files
```

Installation and configuration of TheHive

- For Debian systems, use the following commands:

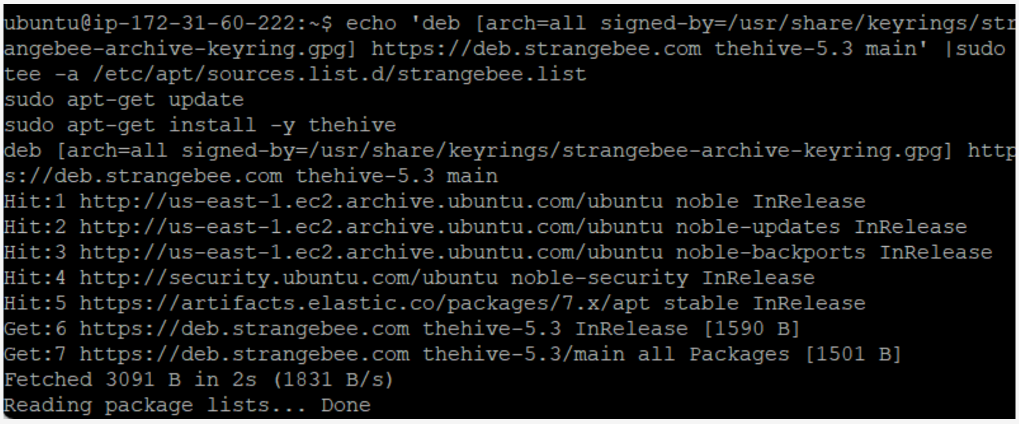
wget -O- https://archives.strangebee.com/keys/strangebee.gpg | sudo gpg --dearmor -o /usr/share/keyrings/strangebee-archive-keyring.gpg



```
ubuntu@ip-172-31-35-76:~$ wget -O- https://archives.strangebee.com/keys/strangeb
ee.gpg | sudo gpg --dearmor -o /usr/share/keyrings/strangebee-archive-keyring.gp
g
--2024-06-25 00:14:00--  https://archives.strangebee.com/keys/strangebee.gpg
Resolving archives.strangebee.com (archives.strangebee.com)... 5.196.134.251
Connecting to archives.strangebee.com (archives.strangebee.com)|5.196.134.251|:4
43... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3179 (3.1K) [text/plain]
Saving to: 'STDOUT'

-                   100%[===================>]   3.10K  --.-KB/s    in 0s

2024-06-25 00:14:01 (544 MB/s) - written to stdout [3179/3179]
```

- Install TheHive package by using the following commands

echo 'deb [arch=all signed-by=/usr/share/keyrings/strangebee-archive-keyring.gpg] https://deb.strangebee.com thehive-5.3 main' |sudo tee -a /etc/apt/sources.list.d/strangebee.list
sudo apt-get update
sudo apt-get install -y thehive



```
ubuntu@ip-172-31-60-222:~$ echo 'deb [arch=all signed-by=/usr/share/keyrings/str
angebee-archive-keyring.gpg] https://deb.strangebee.com thehive-5.3 main' |sudo
tee -a /etc/apt/sources.list.d/strangebee.list
sudo apt-get update
sudo apt-get install -y thehive
deb [arch=all signed-by=/usr/share/keyrings/strangebee-archive-keyring.gpg] http
s://deb.strangebee.com thehive-5.3 main
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Get:6 https://deb.strangebee.com thehive-5.3 InRelease [1590 B]
Get:7 https://deb.strangebee.com thehive-5.3/main all Packages [1501 B]
Fetched 3091 B in 2s (1831 B/s)
Reading package lists... Done
```

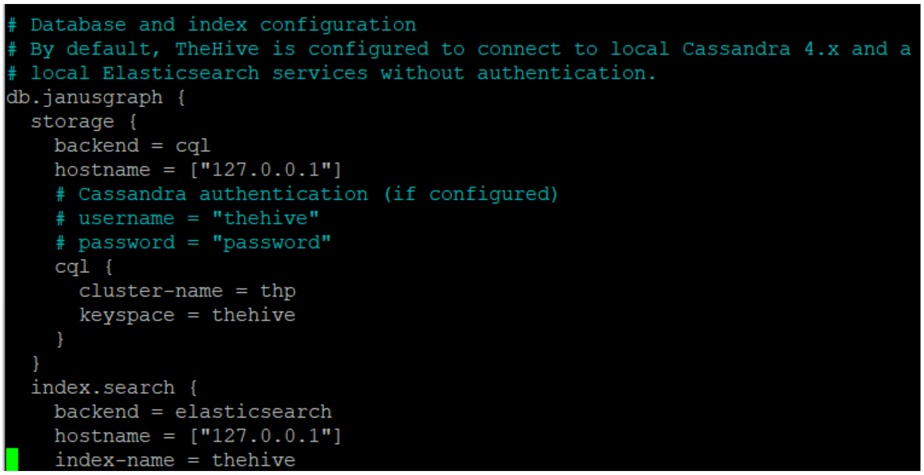
- The following configurations are necessary for successful initiation of TheHive:

Secret key configuration

- The secret key is automatically generated and stored in /etc/thehive/secret.conf during package installation.

Database configuration

- By default, TheHive is configured to connect to local Cassandra and Elasticsearch databases.



```
# Database and index configuration
# By default, TheHive is configured to connect to local Cassandra 4.x and a
# local Elasticsearch services without authentication.
db.janusgraph {
  storage {
    backend = cql
    hostname = ["127.0.0.1"]
    # Cassandra authentication (if configured)
    # username = "thehive"
    # password = "password"
    cql {
      cluster-name = thp
      keyspace = thehive
    }
  }
  index.search {
    backend = elasticsearch
    hostname = ["127.0.0.1"]
    index-name = thehive
```

-

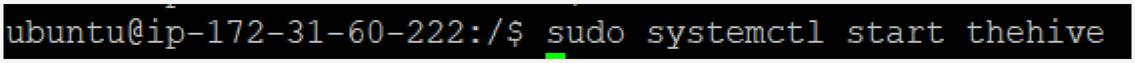
File storage configuration

- The default file storage location of TheHive is `/opt/thp/thehive/files`.

Run TheHive

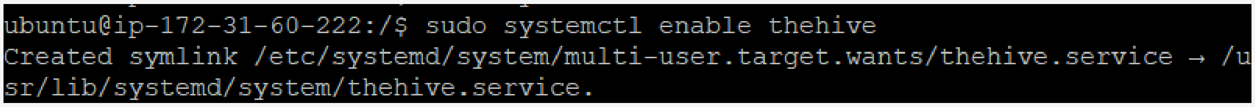
- To start TheHive service and enable it to run on system boot, execute the following commands in your terminal:

sudo systemctl start thehive

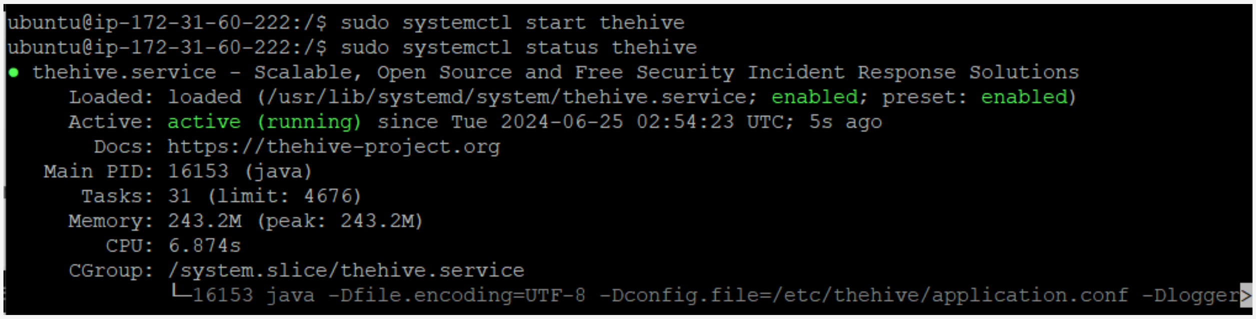


```
ubuntu@ip-172-31-60-222:/$ sudo systemctl start thehive
```

sudo systemctl enable thehive



```
ubuntu@ip-172-31-60-222:/$ sudo systemctl enable thehive
Created symlink /etc/systemd/system/multi-user.target.wants/thehive.service → /u
sr/lib/systemd/system/thehive.service.
```



```
ubuntu@ip-172-31-60-222:/$ sudo systemctl start thehive
ubuntu@ip-172-31-60-222:/$ sudo systemctl status thehive
● thehive.service - Scalable, Open Source and Free Security Incident Response Solutions
     Loaded: loaded (/usr/lib/systemd/system/thehive.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-06-25 02:54:23 UTC; 5s ago
       Docs: https://thehive-project.org
   Main PID: 16153 (java)
      Tasks: 31 (limit: 4676)
     Memory: 243.2M (peak: 243.2M)
        CPU: 6.874s
     CGroup: /system.slice/thehive.service
             └─16153 java -Dfile.encoding=UTF-8 -Dconfig.file=/etc/thehive/application.conf -Dlogger>
```