Name: P.Aashritha

Regno:21BCE7241

CYBER PHYSICAL SYSTEMS-CSE1018 PROJECT REPORT

In the rapidly evolving environment of modern networks, maintaining robust security, optimizing performance, and gaining visibility into network activity are paramount. Network administrators and security experts rely on advanced tools and frameworks to address these challenges. One such powerful synergy results from the integration of the ELK stack (Elasticsearch, Logstash, and Kibana) with Zeek (formerly known as Bro), a high-performance network analysis framework. This integration offers a comprehensive solution for capturing, analyzing and visualizing network data, providing invaluable insights to improve network management, security and decision making.

Zeek:

Zeek, a leading network analytics framework, acts as a passive monitoring system. It dissects network traffic and transforms it into structured logs that detail a wide range of network activities, from protocol interactions to connections and data transfers. Its non-intrusive approach enables real-time analysis without disrupting normal network operations.

ELK stack:

The ELK stack consists of a trio of tools that together deal with data processing, storage and visualization:

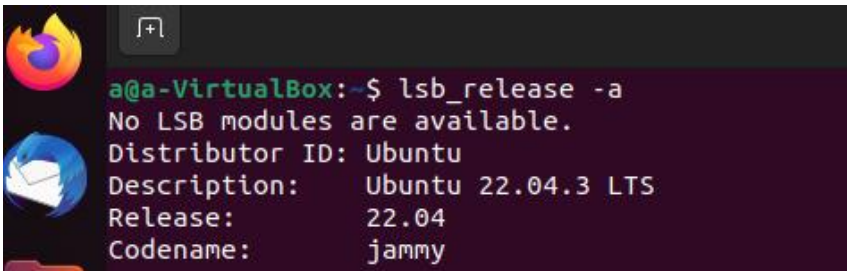
Elasticsearch: This distributed search and analytics engine excels at indexing and storing large volumes of data, enabling lightning-fast searches and comprehensive data analysis.

Logstash: As a versatile data processing pipeline, Logstash ingests, transforms and enriches data from a variety of sources and prepares it for storage and analysis.

Kibana: Kibana's powerful visualization platform works seamlessly with Elasticsearch, allowing users to create customized dashboards, reports, and visualizations that transform raw data into meaningful insights.

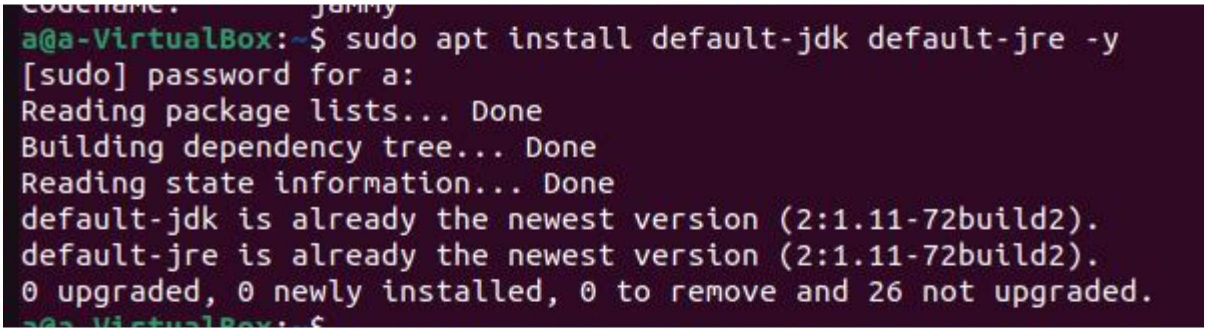
IMPLEMENTATION:

- Before installing ELK, set the required dependencies:
- Check current ubuntu version



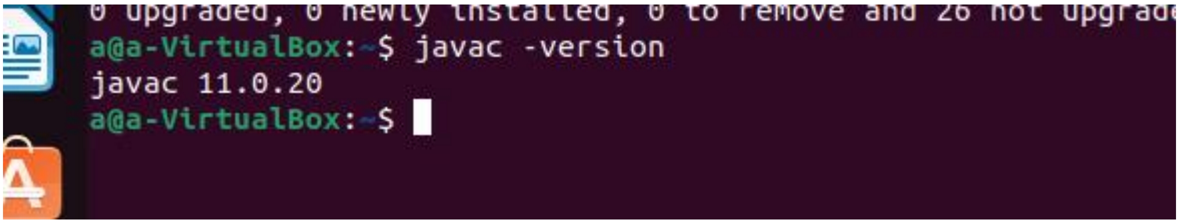
```
a@a-VirtualBox:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.3 LTS
Release:        22.04
Codename:       jammy
```

- Install java Dependencies:



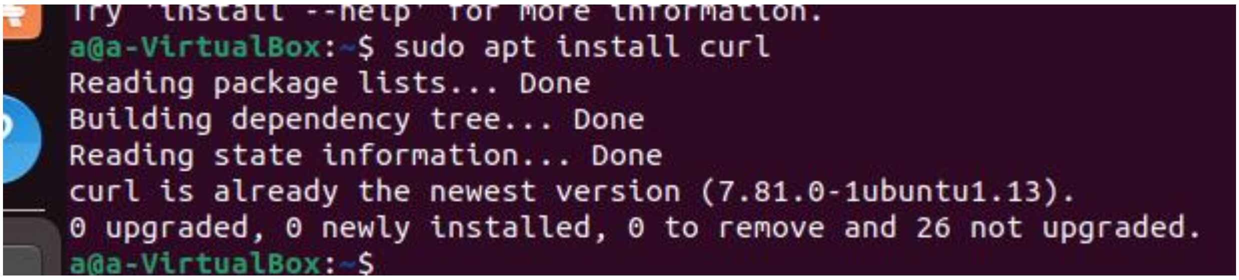
```
Codename:        jammy
a@a-VirtualBox:~$ sudo apt install default-jdk default-jre -y
[sudo] password for a:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
default-jdk is already the newest version (2:1.11-72build2).
default-jre is already the newest version (2:1.11-72build2).
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
a@a-VirtualBox:~$
```

- Check current java version:



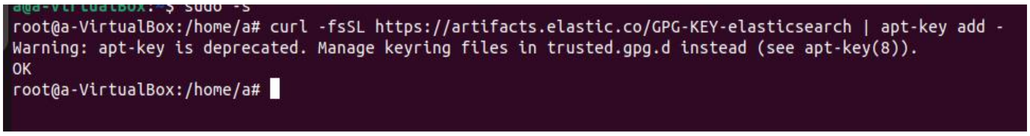
```
0 upgraded, 0 newly installed, 0 to remove and 26 not upgrade
a@a-VirtualBox:~$ javac -version
javac 11.0.20
a@a-VirtualBox:~$ █
```

- Install curl if not installed



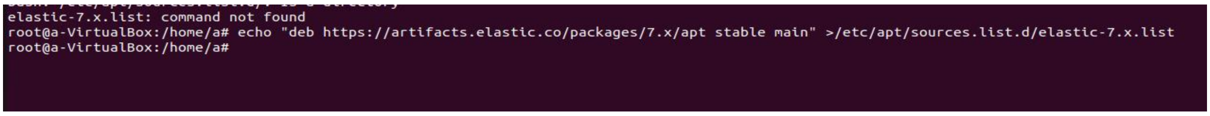
```
Try 'install --help' for more information.
a@a-VirtualBox:~$ sudo apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.81.0-1ubuntu1.13).
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
a@a-VirtualBox:~$
```

- Add elasticsearch APT respository by using below command
  curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -



```
a@a-VirtualBox:~$ sudo -s
root@a-VirtualBox:/home/a# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
root@a-VirtualBox:/home/a# █
```

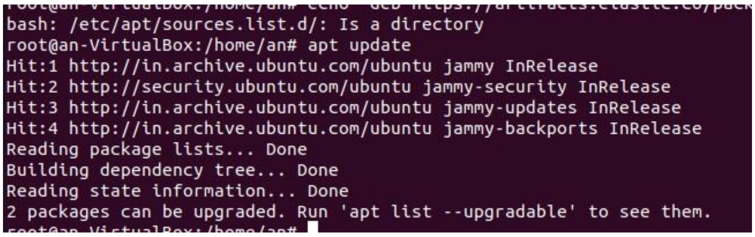
- Add the Elastic Search to the APT source List by using the below command



```
bash: /etc/apt/sources.list.d/: Is a directory
elastic-7.x.list: command not found
root@a-VirtualBox:/home/a# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" >/etc/apt/sources.list.d/elastic-7.x.list
root@a-VirtualBox:/home/a#
```

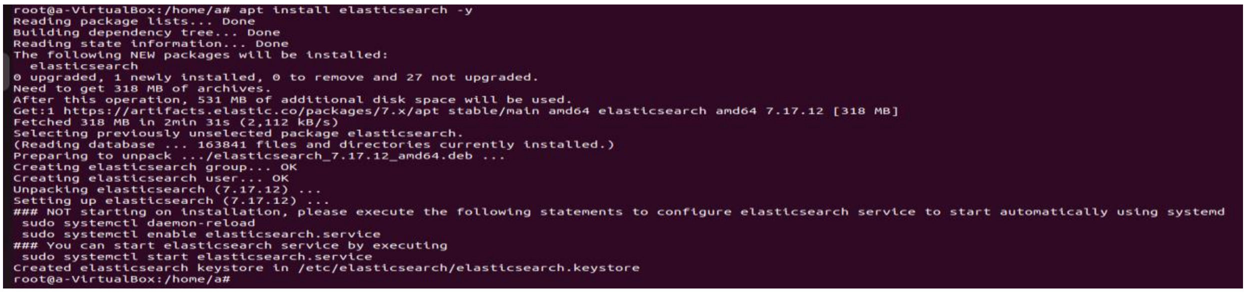
Installation of elastic search:

- Apt update



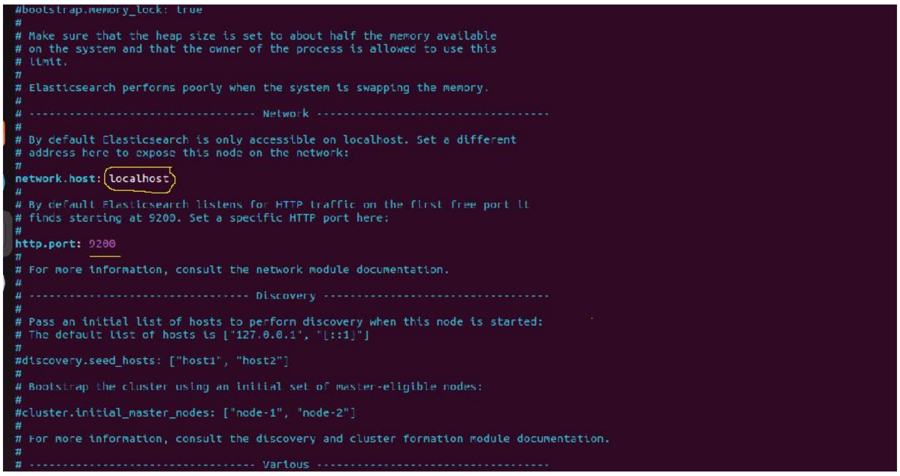
```
root@an-VirtualBox:/home/an# echo "deb https://artifacts.elastic.co/pack
bash: /etc/apt/sources.list.d/: Is a directory
root@an-VirtualBox:/home/an# apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@an-VirtualBox:/home/an#
```

- Install elastic search



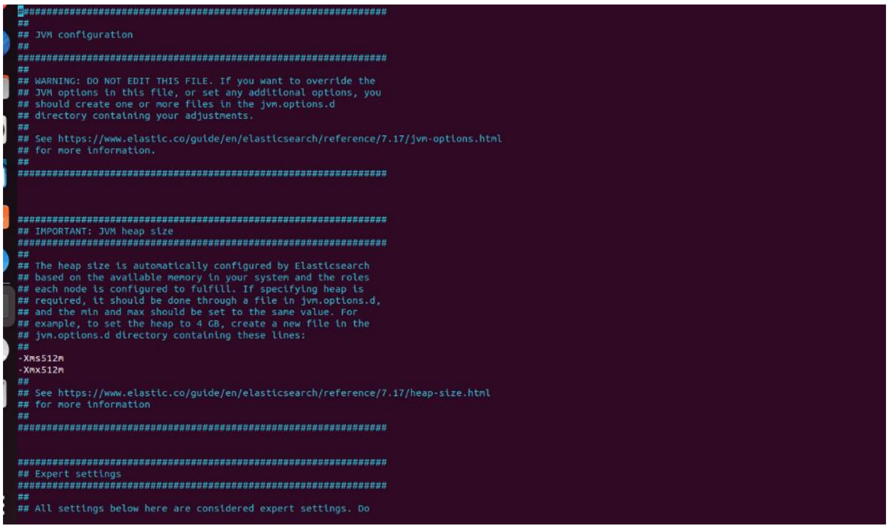
```
root@a-VirtualBox:/home/a# apt install elasticsearch -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 27 not upgraded.
Need to get 318 MB of archives.
After this operation, 531 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17.12 [318 MB]
Fetched 318 MB in 2min 31s (2,112 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 163841 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.12_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.17.12) ...
Setting up elasticsearch (7.17.12) ...
### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
root@a-VirtualBox:/home/a#
```

- Configure Elastic search
  # vim /etc/elasticsearch/elasticsearch.yml



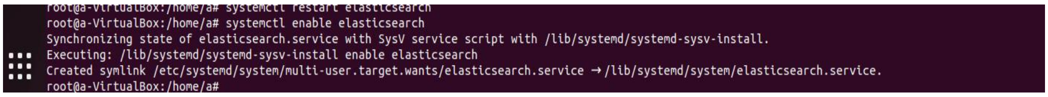
```
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: localhost
#
# 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.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# ---------------------------------- Various -----------------------------------
```

- Configure JVM heap
  vim /etc/elasticsearch/jvm.options



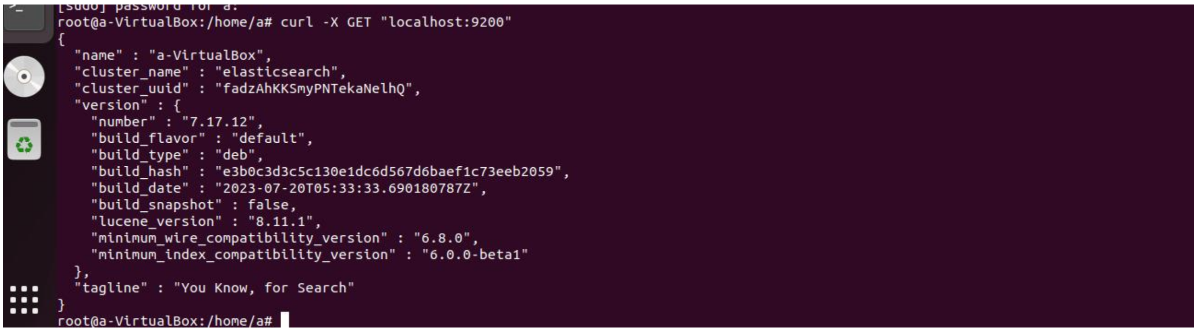
```
################################################################
##
## JVM configuration
##
################################################################
##
## WARNING: DO NOT EDIT THIS FILE. If you want to override the
## JVM options in this file, or set any additional options, you
## should create one or more files in the jvm.options.d
## directory containing your adjustments.
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
## for more information.
##
################################################################



################################################################
## IMPORTANT: JVM heap size
################################################################
##
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
-Xms512m
-Xmx512m
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
## for more information
##
################################################################


################################################################
## Expert settings
################################################################
##
## All settings below here are considered expert settings. Do
```

- Restart elasticsearch
- Enable elasticsearch

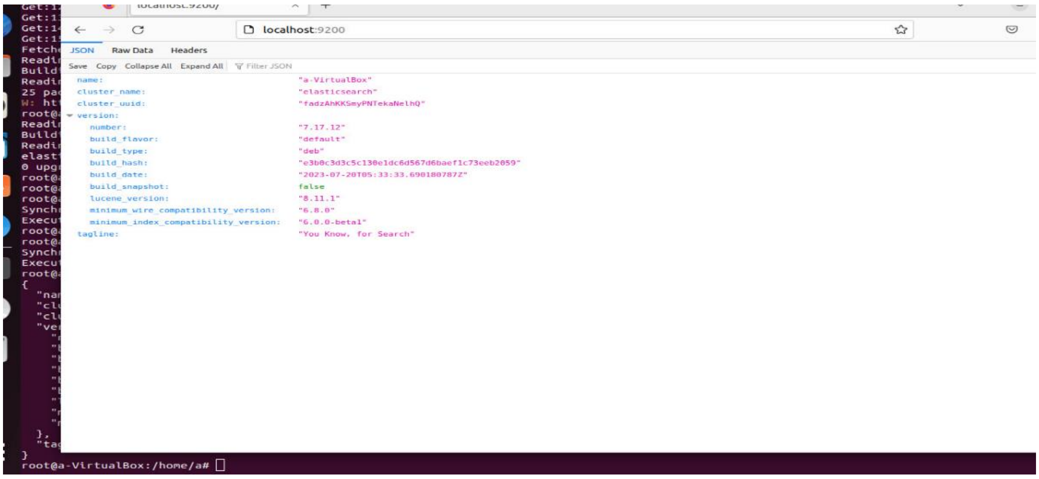


```
root@a-VirtualBox:/home/a# systemctl restart elasticsearch
root@a-VirtualBox:/home/a# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@a-VirtualBox:/home/a#
```

- Ping the Elastic Search to verify installation by using the below command



```
[sudo] password for a:
root@a-VirtualBox:/home/a# curl -X GET "localhost:9200"
{
  "name" : "a-VirtualBox",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "fadzAhKKSmyPNTekaNelhQ",
  "version" : {
    "number" : "7.17.12",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "e3b0c3d3c5c130e1dc6d567d6baef1c73eeb2059",
    "build_date" : "2023-07-20T05:33:33.690180787Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@a-VirtualBox:/home/a#
```

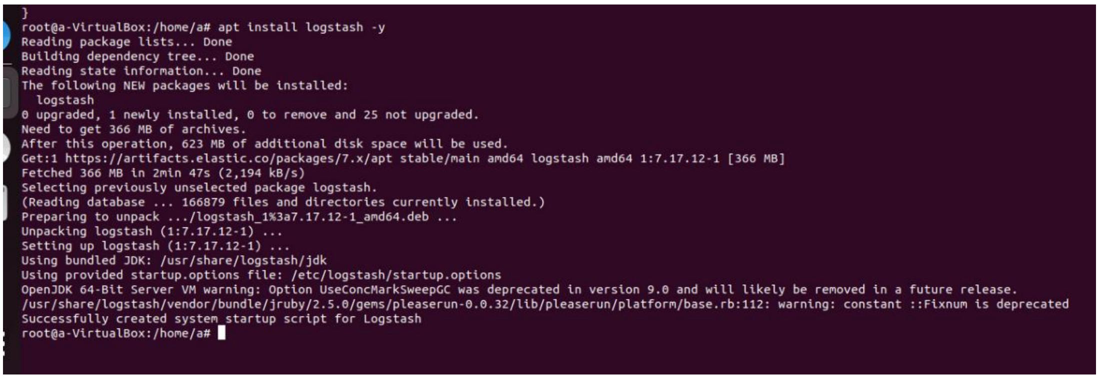


```
name:                                    "a-VirtualBox"
cluster_name:                            "elasticsearch"
cluster_uuid:                            "fadzAhKKSmyPNTekaNelhQ"
version:
  number:                                "7.17.12"
  build_flavor:                          "default"
  build_type:                            "deb"
  build_hash:                            "e3b0c3d3c5c130e1dc6d567d6baef1c73eeb2059"
  build_date:                            "2023-07-20T05:33:33.690180787Z"
  build_snapshot:                        false
  lucene_version:                        "8.11.1"
  minimum_wire_compatibility_version:    "6.8.0"
  minimum_index_compatibility_version:   "6.0.0-beta1"
tagline:                                 "You Know, for Search"
```

```
root@a-VirtualBox:/home/a#
```

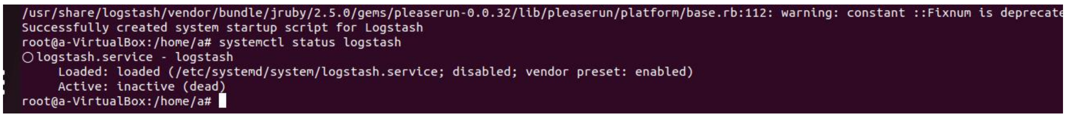
Installation of logstash:

- Install logstash by below command



```
}
root@a-VirtualBox:/home/a# apt install logstash -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 25 not upgraded.
Need to get 366 MB of archives.
After this operation, 623 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash amd64 1:7.17.12-1 [366 MB]
Fetched 366 MB in 2min 47s (2,194 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 166879 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.17.12-1_amd64.deb ...
Unpacking logstash (1:7.17.12-1) ...
Setting up logstash (1:7.17.12-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
root@a-VirtualBox:/home/a#
```

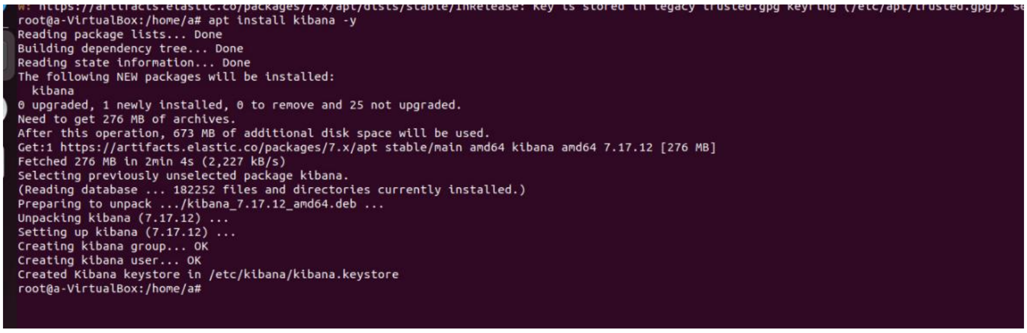
- Check its working and status



```
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/platform/base.rb:112: warning: constant ::Fixnum is deprecate
Successfully created system startup script for Logstash
root@a-VirtualBox:/home/a# systemctl status logstash
○ logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
root@a-VirtualBox:/home/a#
```

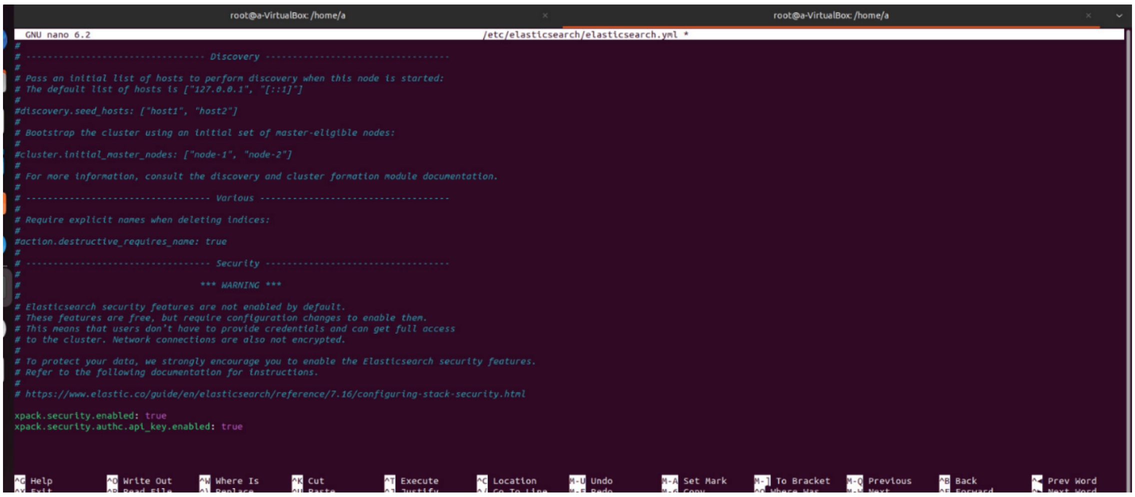
Installation of kibana:

- Install kibana



```
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), se
root@a-VirtualBox:/home/a# apt install kibana -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 25 not upgraded.
Need to get 276 MB of archives.
After this operation, 673 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.12 [276 MB]
Fetched 276 MB in 2min 4s (2,227 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 182252 files and directories currently installed.)
Preparing to unpack .../kibana_7.17.12_amd64.deb ...
Unpacking kibana (7.17.12) ...
Setting up kibana (7.17.12) ...
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
root@a-VirtualBox:/home/a#
```

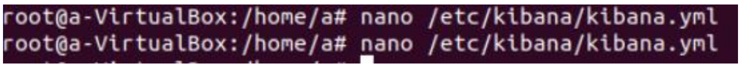
- Configure kibana
  Before configuring stop kibana
  systemctl stop kibana
- Open elasticsearch.yml
- sudo nano /etc/elasticsearch/elasticsearch.yml
- Add to elasticsearch.yml:
  xpack.security.enabled: true
  xpack.security.authc.api_key.enabled: true



```
  GNU nano 6.2                                      /etc/elasticsearch/elasticsearch.yml *
#
# ---------------------------------- Discovery -----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# ---------------------------------- Various -----------------------------------
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
#
# ---------------------------------- Security ----------------------------------
#
#                                 *** WARNING ***
#
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full access
# to the cluster. Network connections are also not encrypted.
#
# To protect your data, we strongly encourage you to enable the Elasticsearch security features.
# Refer to the following documentation for instructions.
#
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html

xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
```

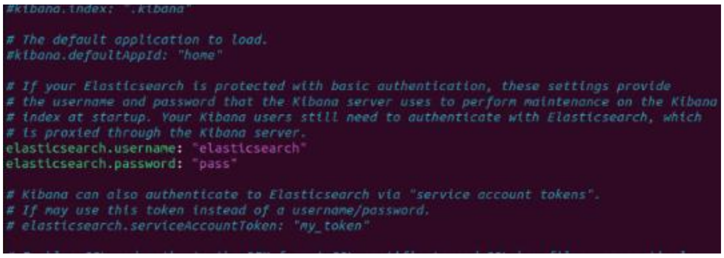
- Restart elasticsearch
  systemctl restart elasticsearch

- Set up default password :
- cd usr/share/elasticsearch/bin
- sudo ./elasticsearch-setup-passwords auto
- Make sure you give elastic user name and password
- Open kibana.yml



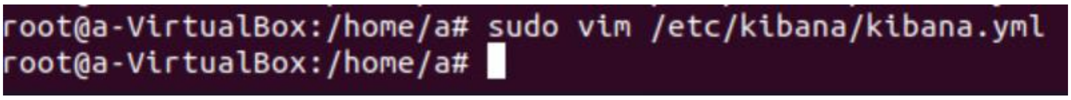
```
root@a-VirtualBox:/home/a# nano /etc/kibana/kibana.yml
root@a-VirtualBox:/home/a# nano /etc/kibana/kibana.yml
```

- Give elasticsearch username and password

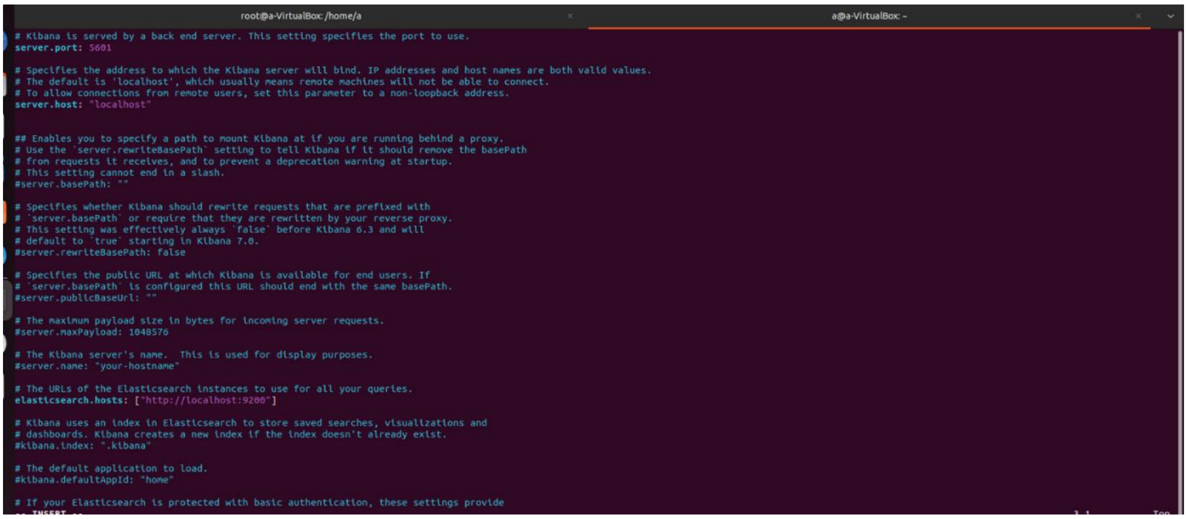


```
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "elasticsearch"
elasticsearch.password: "pass"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# If may use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"
```

- Configure kibana uncomment server port and host

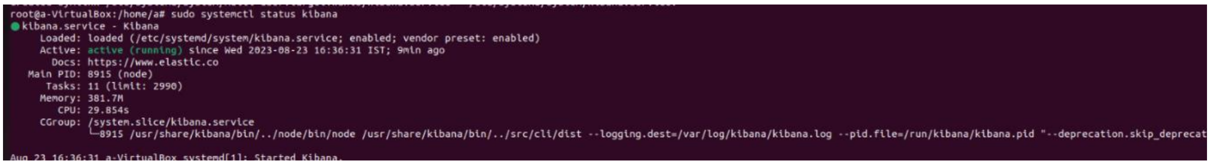


```
root@a-VirtualBox:/home/a# sudo vim /etc/kibana/kibana.yml
root@a-VirtualBox:/home/a#
```



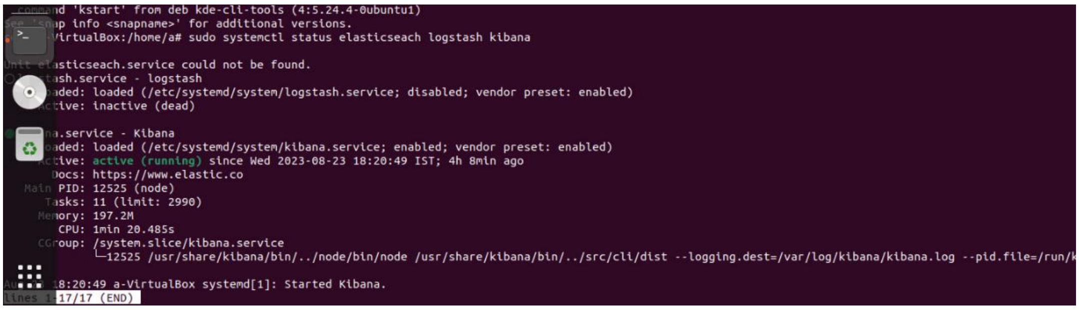
```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# 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: "localhost"


## 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.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#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: ""

# 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"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
-- INSERT --
```

- Save the changes and restart kibana
  Systemctl restart kibana



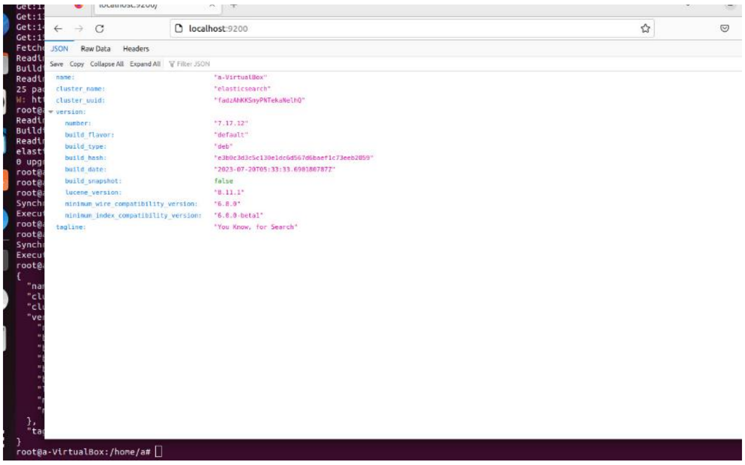
```
root@a-VirtualBox:/home/a# sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-23 16:36:31 IST; 9min ago
       Docs: https://www.elastic.co
   Main PID: 8915 (node)
      Tasks: 11 (limit: 2990)
     Memory: 381.7M
        CPU: 29.854s
     CGroup: /system.slice/kibana.service
             └─8915 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest=/var/log/kibana/kibana.log --pid.file=/run/kibana/kibana.pid "--deprecation.skip_deprecat

Aug 23 16:36:31 a-VirtualBox systemd[1]: Started Kibana.
```

- Give a command sudo systemctl status elasticseach logstash kibana



```
command 'kstart' from deb kde-cli-tools (4:5.24.4-0ubuntu1)
See 'snap info <snapname>' for additional versions.
   VirtualBox:/home/a# sudo systemctl status elasticseach logstash kibana

Unit elasticseach.service could not be found.
○    ash.service - logstash
     aded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset: enabled)
     Active: inactive (dead)

●    na.service - Kibana
     aded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-23 18:20:49 IST; 4h 8min ago
      Docs: https://www.elastic.co
   Main PID: 12525 (node)
      Tasks: 11 (limit: 2990)
     Memory: 197.2M
        CPU: 1min 20.485s
     CGroup: /system.slice/kibana.service
             └─12525 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest=/var/log/kibana/kibana.log --pid.file=/run/k

Au    18:20:49 a-VirtualBox systemd[1]: Started Kibana.
lines 1-17/17 (END)
```

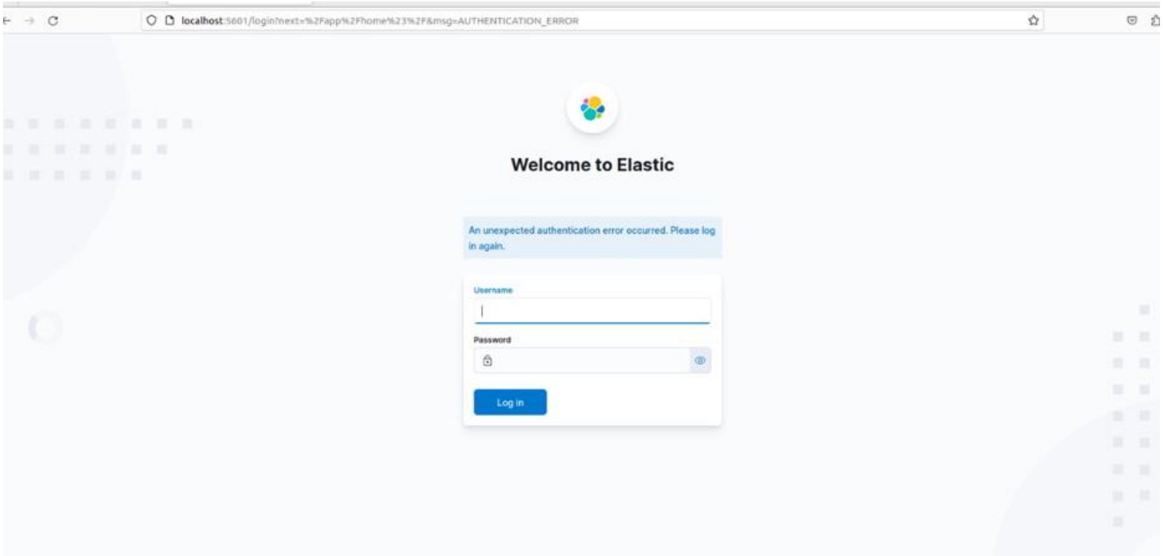
- Open browser on unbutu
  Search localhost:9200



```
name:                                   "a-VirtualBox"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "fadzAhKKSmyPNTekaNelhQ"
▾ version:
  number:                               "7.17.12"
  build_flavor:                         "default"
  build_type:                           "deb"
  build_hash:                           "e3b0c3d3c5c130e1dc6d567d6baef1c73eeb2059"
  build_date:                           "2023-07-20T05:33:33.690180787Z"
  build_snapshot:                       false
  lucene_version:                       "8.11.1"
  minimum_wire_compatibility_version:   "6.8.0"
  minimum_index_compatibility_version:  "6.0.0-beta1"
tagline:                                "You Know, for Search"
```

```
root@a-VirtualBox:/home/a#
```

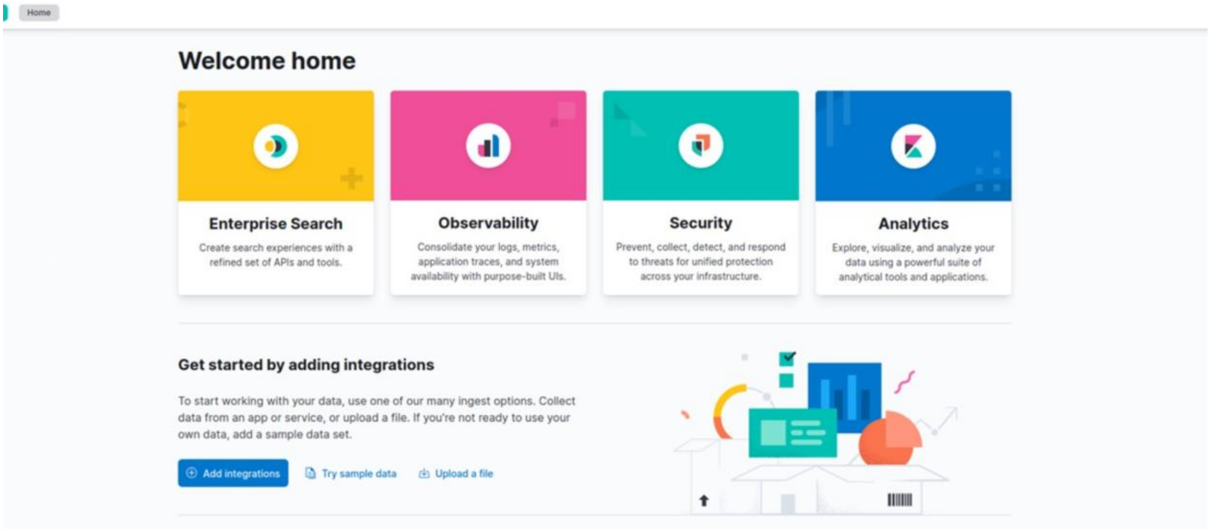
localhost:5200



localhost:5601/login?next=%2Fapp%2Fhome%23%2F&msg=AUTHENTICATION_ERROR

Welcome to Elastic

An unexpected authentication error occurred. Please log in again.



Welcome home

Enterprise 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

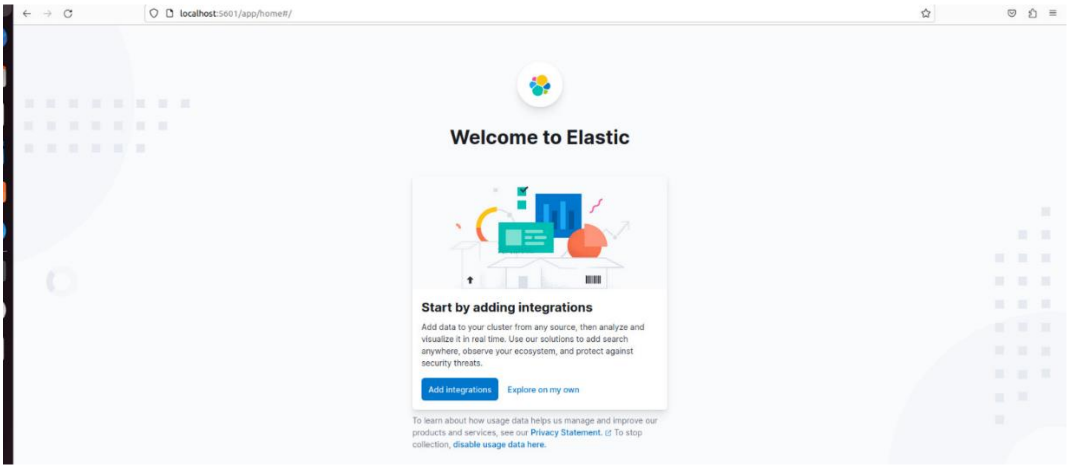
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

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, add a sample data set.



localhost:5601/app/home#/

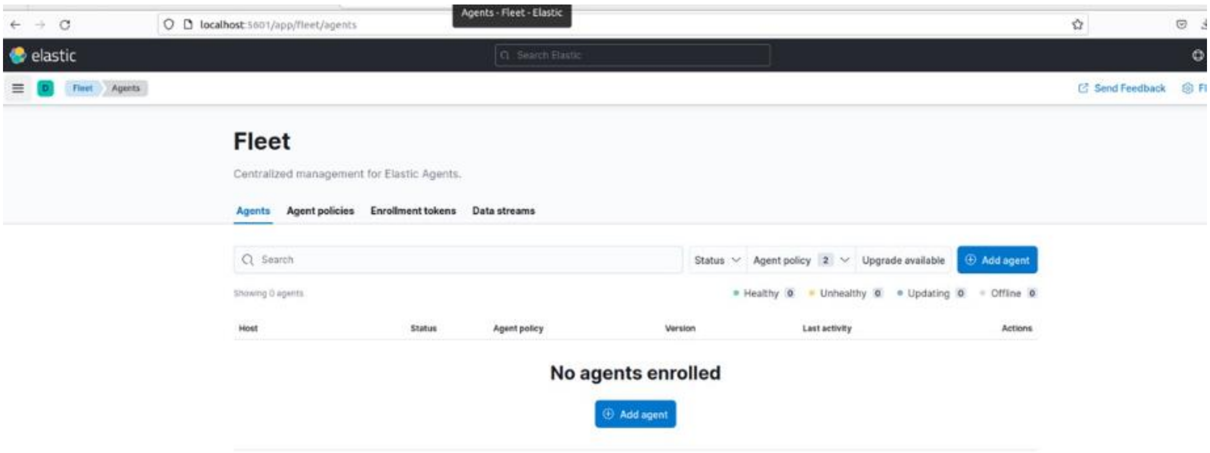
Welcome to Elastic

Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

- Go to management> FLEET

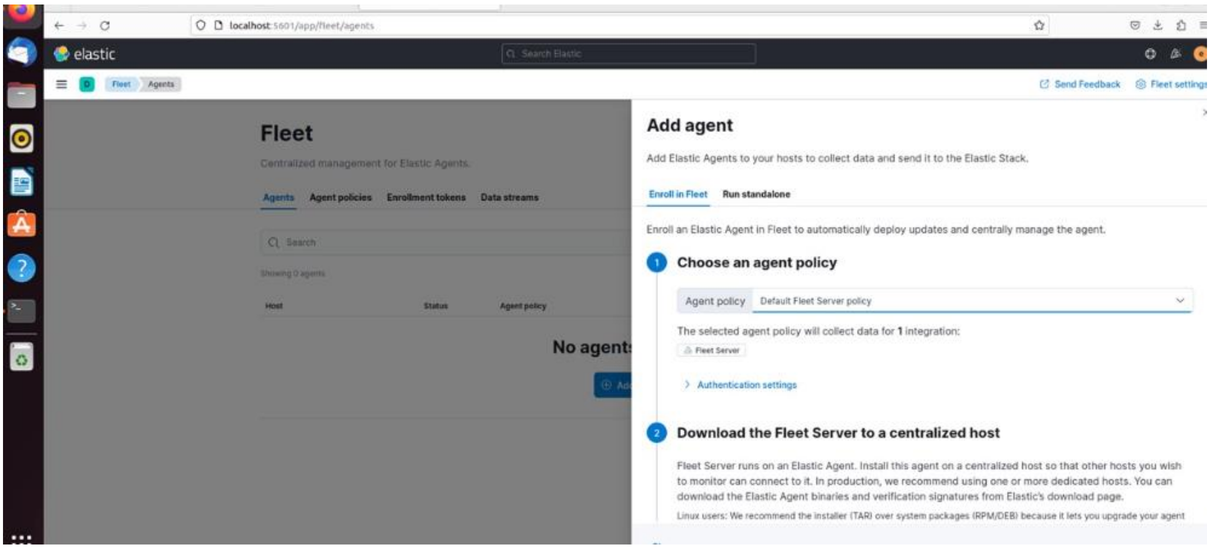


Fleet

Centralized management for Elastic Agents.

No agents enrolled

- Add agent



Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Enroll an Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.

1 Choose an agent policy

Agent policy: Default Fleet Server policy

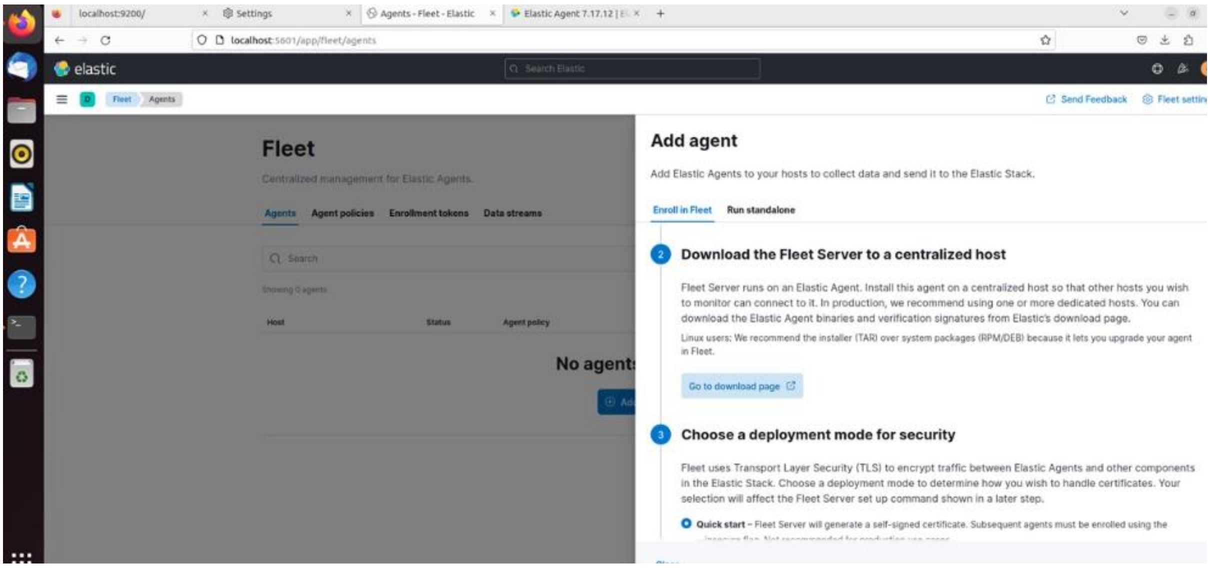
The selected agent policy will collect data for **1** integration:

2 Download the Fleet Server to a centralized host

Fleet Server runs on an Elastic Agent. Install this agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. You can download the Elastic Agent binaries and verification signatures from Elastic's download page.

Linux users: We recommend the installer (TAR) over system packages (RPM/DEB) because it lets you upgrade your agent

- Download fleet centralised host



Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

2 Download the Fleet Server to a centralized host

Fleet Server runs on an Elastic Agent. Install this agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. You can download the Elastic Agent binaries and verification signatures from Elastic's download page.

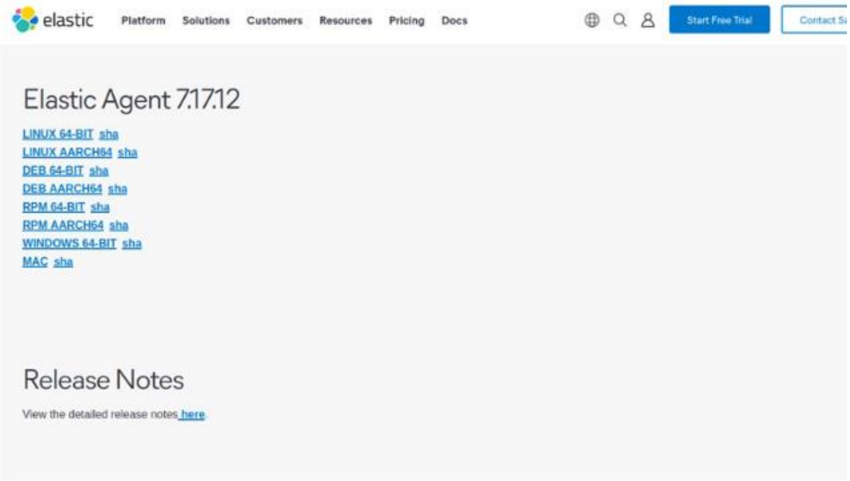
Linux users: We recommend the installer (TAR) over system packages (RPM/DEB) because it lets you upgrade your agent in Fleet.

3 Choose a deployment mode for security

Fleet uses Transport Layer Security (TLS) to encrypt traffic between Elastic Agents and other components in the Elastic Stack. Choose a deployment mode to determine how you wish to handle certificates. Your selection will affect the Fleet Server set up command shown in a later step.

● **Quick start** – Fleet Server will generate a self-signed certificate. Subsequent agents must be enrolled using the

- Click download and Download

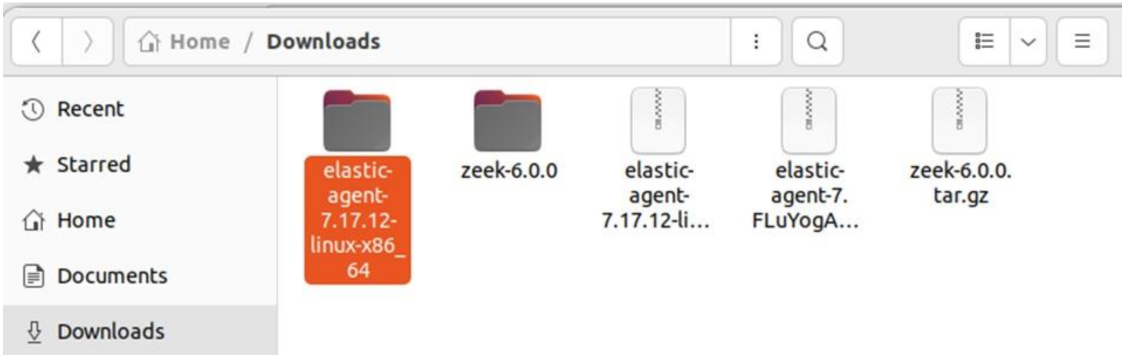


Elastic Agent 7.17.12

- LINUX 64-BIT sha
- LINUX AARCH64 sha
- DEB 64-BIT sha
- DEB AARCH64 sha
- RPM 64-BIT sha
- RPM AARCH64 sha
- WINDOWS 64-BIT sha
- MAC sha

Release Notes

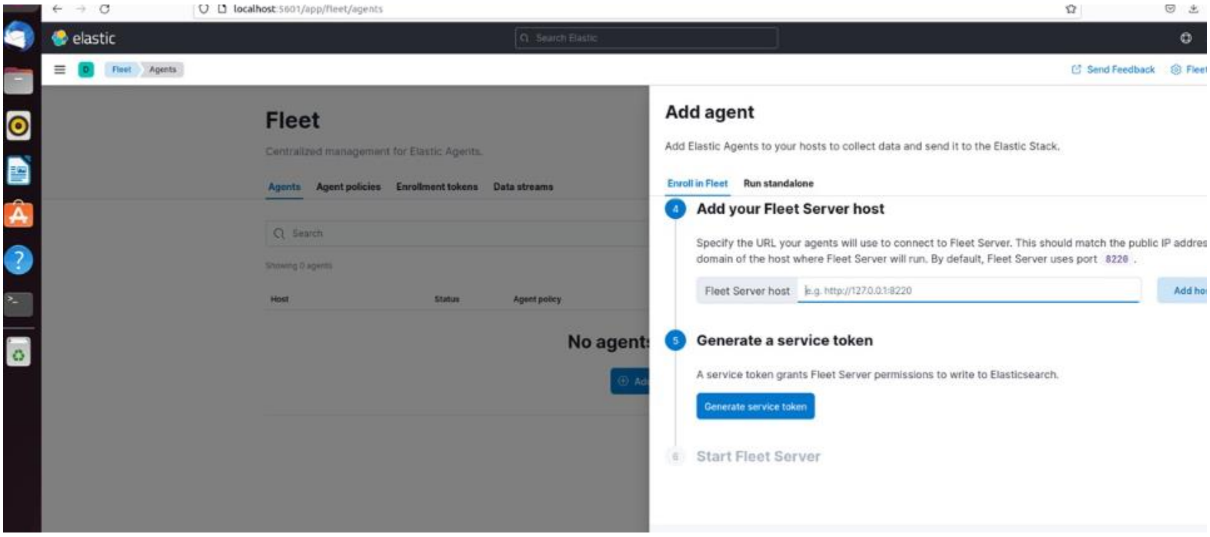
View the detailed release notes here


Home / Downloads
Recent
Starred
Home
Documents
Downloads
elastic-agent-7.17.12-linux-x86_64
zeek-6.0.0
elastic-agent-7.17.12-li…
elastic-agent-7. FLuYogA…
zeek-6.0.0.tar.gz

Add yours fleet host server

Fleet Server host : http://localhost:8220 then click on add host

- Complete the following steps:



Fleet

Centralized management for Elastic Agents.

Showing 0 agents

No agent

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

4 **Add your Fleet Server host**

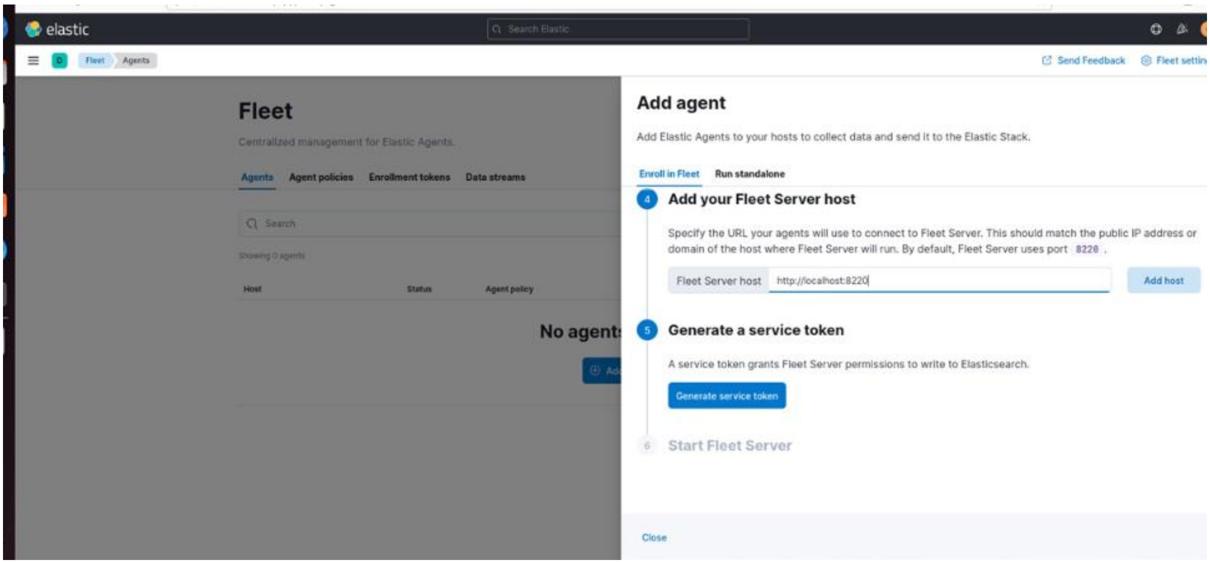
Specify the URL your agents will use to connect to Fleet Server. This should match the public IP addres domain of the host where Fleet Server will run. By default, Fleet Server uses port `8220` .

Fleet Server host: e.g. http://127.0.0.1:8220

5 **Generate a service token**

A service token grants Fleet Server permissions to write to Elasticsearch.

6 Start Fleet Server



Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Enroll in Fleet | Run standalone

4 **Add your Fleet Server host**

Specify the URL your agents will use to connect to Fleet Server. This should match the public IP address or domain of the host where Fleet Server will run. By default, Fleet Server uses port `8220`.

Fleet Server host: http://localhost:8220

Add host

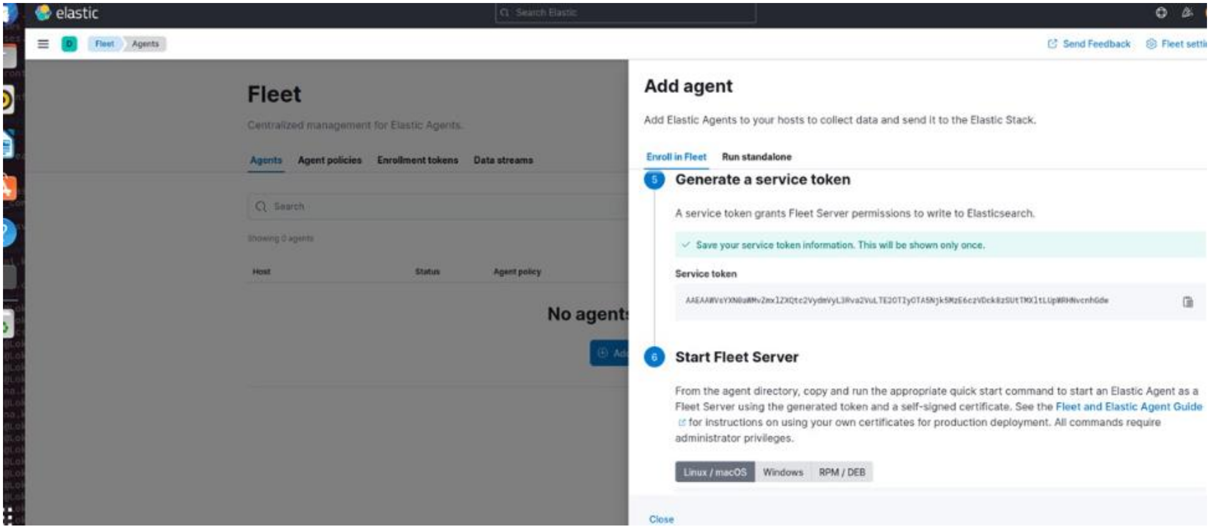
5 **Generate a service token**

A service token grants Fleet Server permissions to write to Elasticsearch.

Generate service token

6 Start Fleet Server

Close



Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Enroll in Fleet | Run standalone

5 **Generate a service token**

A service token grants Fleet Server permissions to write to Elasticsearch.

✓ Save your service token information. This will be shown only once.

Service token

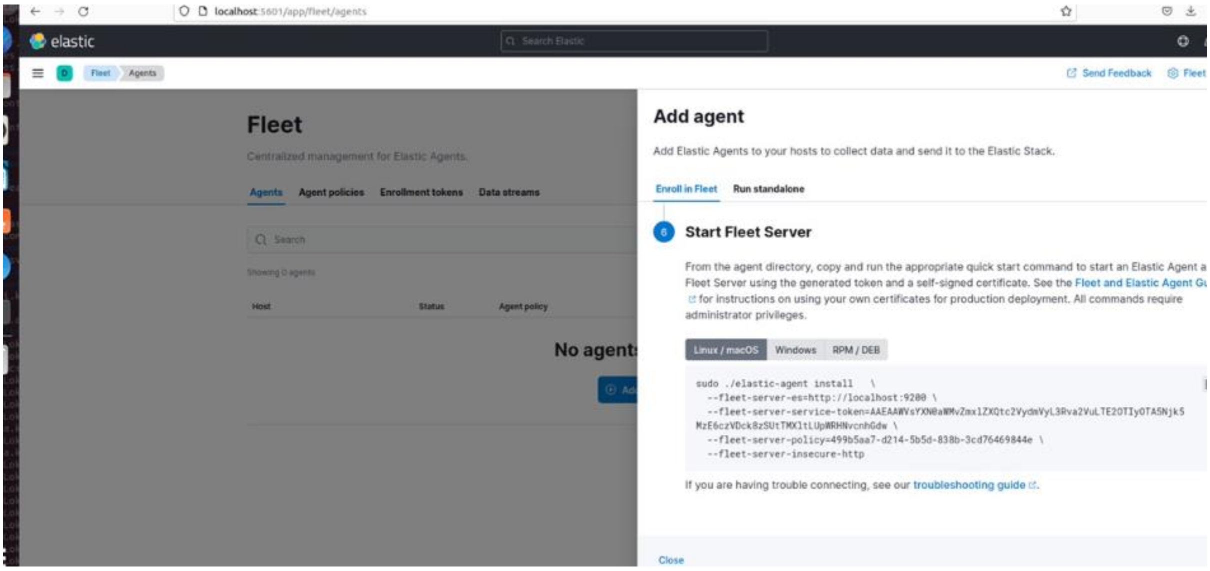
```
AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTIyOTA5Njk5MzE6czVDck8zSUtTMXltLUpWRHNvcnhGdw
```

6 **Start Fleet Server**

From the agent directory, copy and run the appropriate quick start command to start an Elastic Agent as a Fleet Server using the generated token and a self-signed certificate. See the Fleet and Elastic Agent Guide for instructions on using your own certificates for production deployment. All commands require administrator privileges.

Linux / macOS | Windows | RPM / DEB

Close



Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Enroll in Fleet | Run standalone

6 **Start Fleet Server**

From the agent directory, copy and run the appropriate quick start command to start an Elastic Agent a Fleet Server using the generated token and a self-signed certificate. See the Fleet and Elastic Agent Gu for instructions on using your own certificates for production deployment. All commands require administrator privileges.

Linux / macOS | Windows | RPM / DEB

```
sudo ./elastic-agent install   \
  --fleet-server-es=http://localhost:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTIyOTA5Njk5
MzE6czVDck8zSUtTMXltLUpWRHNvcnhGdw \
  --fleet-server-policy=499b5aa7-d214-5b5d-838b-3cd76469844e \
  --fleet-server-insecure-http
```

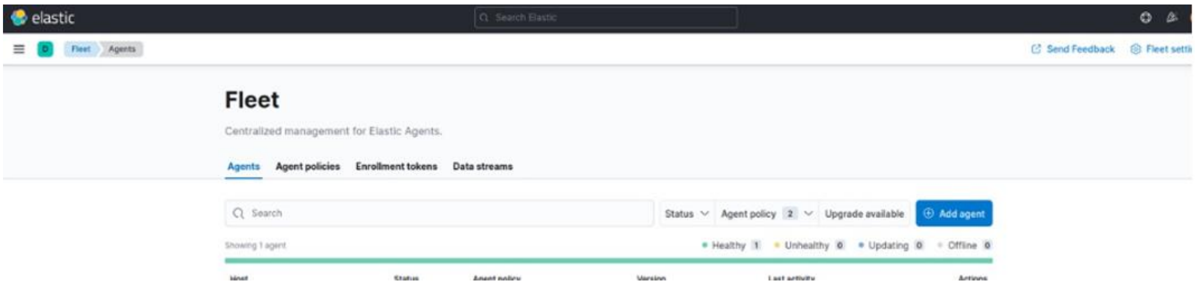
If you are having trouble connecting, see our troubleshooting guide.

Close

- Copy commands and give those command in ubuntu terminal (give commands related to which environment based elastic agent you downloaded)

- Go to the path of elastic agent and paste the fleet server commands

- Fleet server hosted



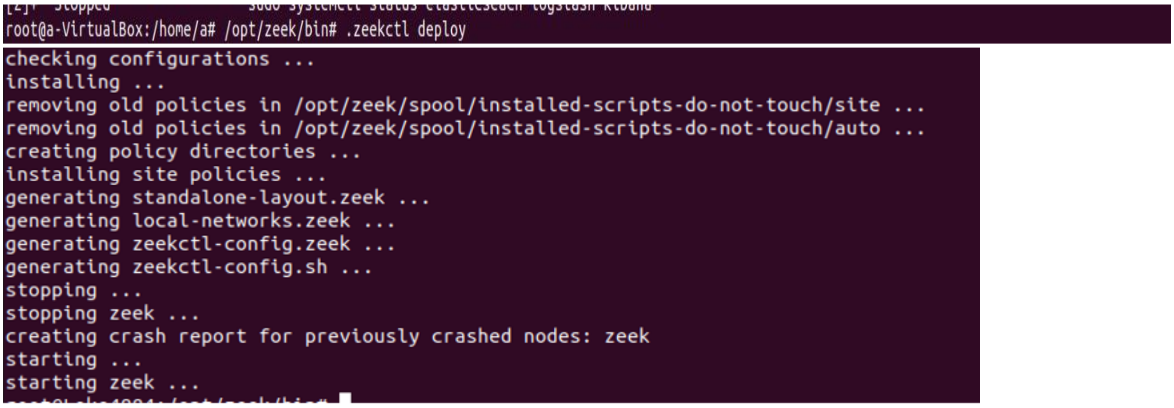
Fleet

Centralized management for Elastic Agents.

Showing 1 agent

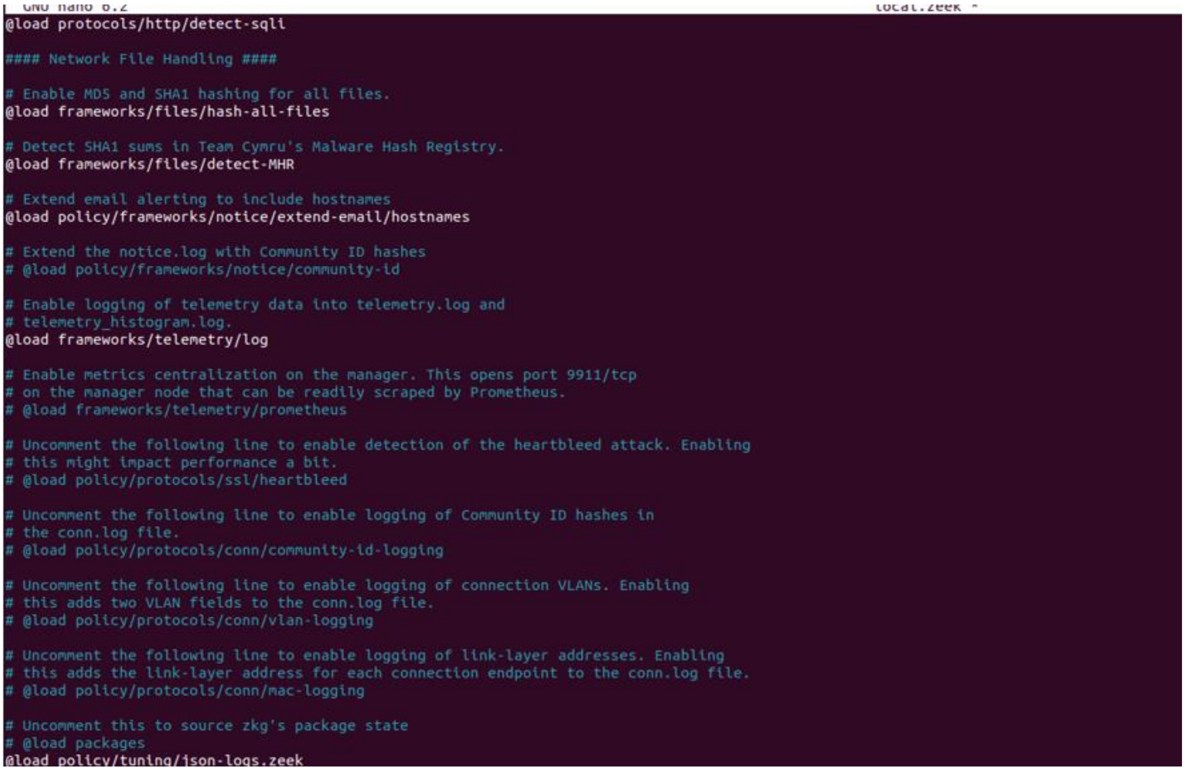
Healthy 1 Unhealthy 0 Updating 0 Offline 0

- Make sure zeek logs are running



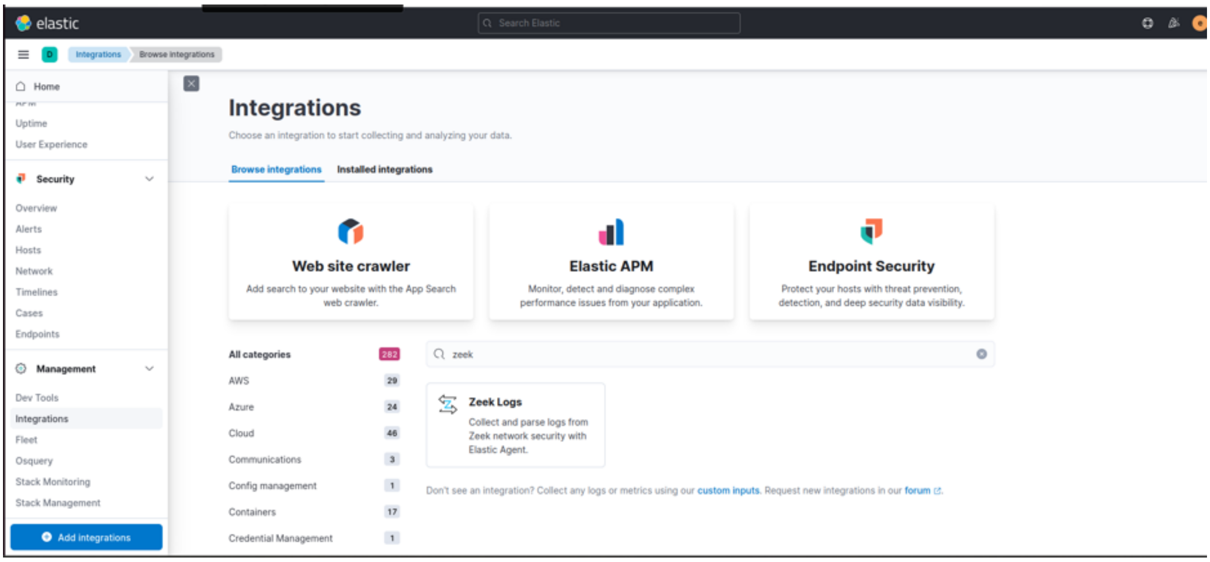
```
[2]+  Stopped                 sudo systemctl status elasticsearch logstash kibana
root@a-VirtualBox:/home/a# /opt/zeek/bin# .zeekctl deploy
checking configurations ...
installing ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
creating crash report for previously crashed nodes: zeek
starting ...
starting zeek ...
```

- Go to local.zeek and add a line @load policy/tuning/json_logs.zeek
- Add at the end of the file @load policy/tuning/json-logs.zeek → to solve error of getting zeek logs



```
GNU nano 6.2                                                    local.zeek *
@load protocols/http/detect-sqli

#### Network File Handling ####

# Enable MD5 and SHA1 hashing for all files.
@load frameworks/files/hash-all-files

# Detect SHA1 sums in Team Cymru's Malware Hash Registry.
@load frameworks/files/detect-MHR

# Extend email alerting to include hostnames
@load policy/frameworks/notice/extend-email/hostnames

# Extend the notice.log with Community ID hashes
# @load policy/frameworks/notice/community-id

# Enable logging of telemetry data into telemetry.log and
# telemetry_histogram.log.
@load frameworks/telemetry/log

# Enable metrics centralization on the manager. This opens port 9911/tcp
# on the manager node that can be readily scraped by Prometheus.
# @load frameworks/telemetry/prometheus

# Uncomment the following line to enable detection of the heartbleed attack. Enabling
# this might impact performance a bit.
# @load policy/protocols/ssl/heartbleed

# Uncomment the following line to enable logging of Community ID hashes in
# the conn.log file.
# @load policy/protocols/conn/community-id-logging

# Uncomment the following line to enable logging of connection VLANs. Enabling
# this adds two VLAN fields to the conn.log file.
# @load policy/protocols/conn/vlan-logging

# Uncomment the following line to enable logging of link-layer addresses. Enabling
# this adds the link-layer address for each connection endpoint to the conn.log file.
# @load policy/protocols/conn/mac-logging

# Uncomment this to source zkg's package state
# @load packages
@load policy/tuning/json-logs.zeek
```

-
- Restart zeek
- Go to integrations>> search zeek logs



Integrations

Choose an integration to start collecting and analyzing your data.

Web site crawler

Add search to your website with the App Search web crawler.

Elastic APM

Monitor, detect and diagnose complex performance issues from your application.

Endpoint Security

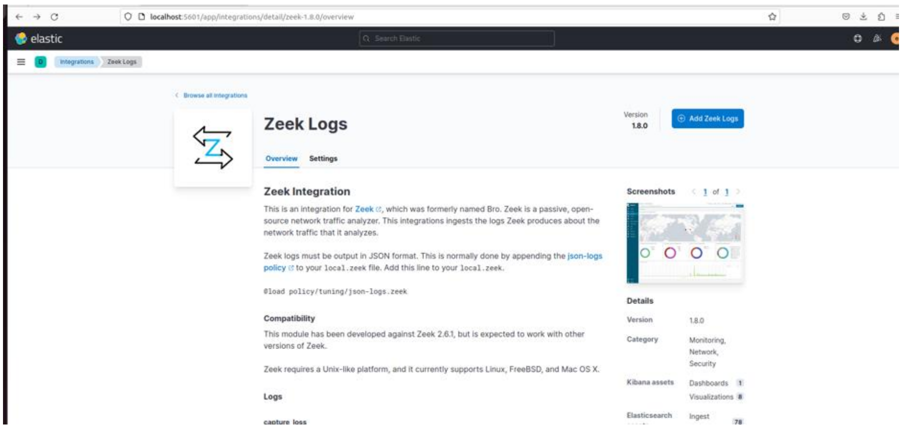
Protect your hosts with threat prevention, detection, and deep security data visibility.

Zeek Logs

Collect and parse logs from Zeek network security with Elastic Agent.

Don't see an integration? Collect any logs or metrics using our custom inputs. Request new integrations in our forum.

- Click on zeek logs



localhost:5601/app/integrations/detail/zeek-1.8.0/overview

elastic

Integrations > Zeek Logs

< Browse all integrations

Zeek Logs

Version 1.8.0

⊕ Add Zeek Logs

Overview | Settings

Zeek Integration

This is an integration for Zeek, which was formerly named Bro. Zeek is a passive, open-source network traffic analyzer. This integrations ingests the logs Zeek produces about the network traffic that it analyzes.

Zeek logs must be output in JSON format. This is normally done by appending the json-logs policy to your `local.zeek` file. Add this line to your `local.zeek`.

```
@load policy/tuning/json-logs.zeek
```

Compatibility

This module has been developed against Zeek 2.6.1, but is expected to work with other versions of Zeek.

Zeek requires a Unix-like platform, and it currently supports Linux, FreeBSD, and Mac OS X.

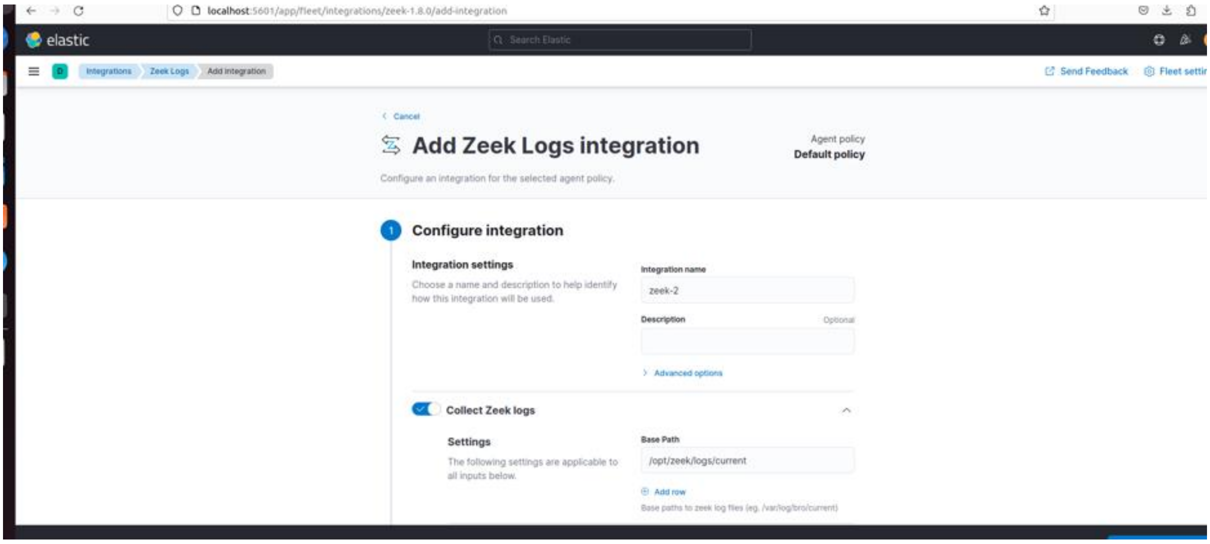
Logs

capture_loss

Screenshots < 1 of 1 >

Details

Version	1.8.0
Category	Monitoring, Network, Security
Kibana assets	Dashboards 1 Visualizations 8
Elasticsearch	Ingest 78



localhost:5601/app/fleet/integrations/zeek-1.8.0/add-integration

elastic

Integrations > Zeek Logs > Add integration

Send Feedback | Fleet settin

< Cancel

Add Zeek Logs integration

Agent policy
Default policy

Configure an integration for the selected agent policy.

1 **Configure integration**

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: zeek-2

Description (Optional):

> Advanced options

☑ Collect Zeek logs

Settings

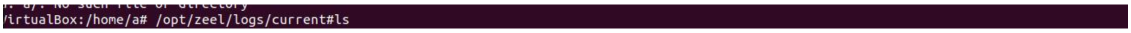
The following settings are applicable to all inputs below.

Base Path: /opt/zeek/logs/current

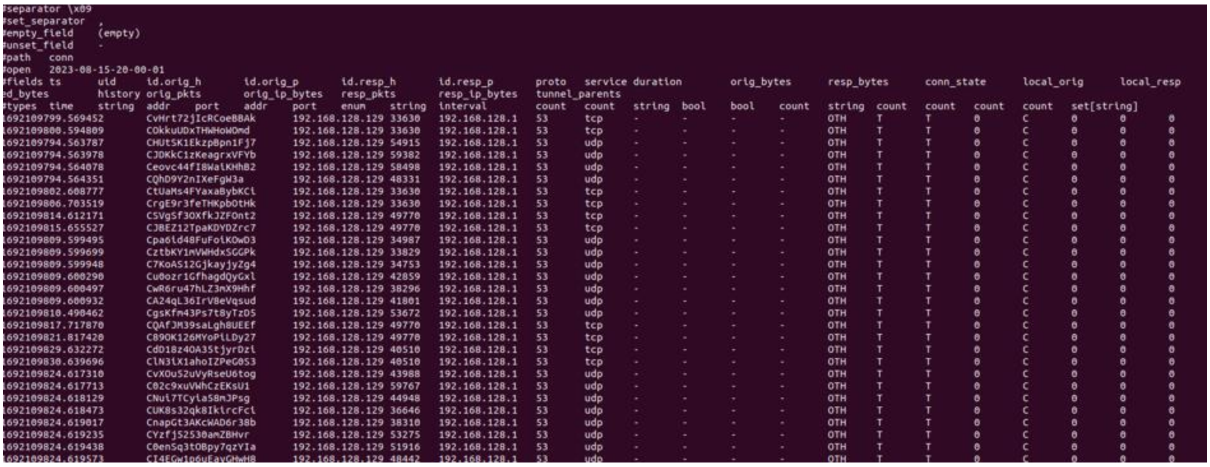
⊕ Add row

Base paths to zeek log files (eg. /var/log/bro/current)

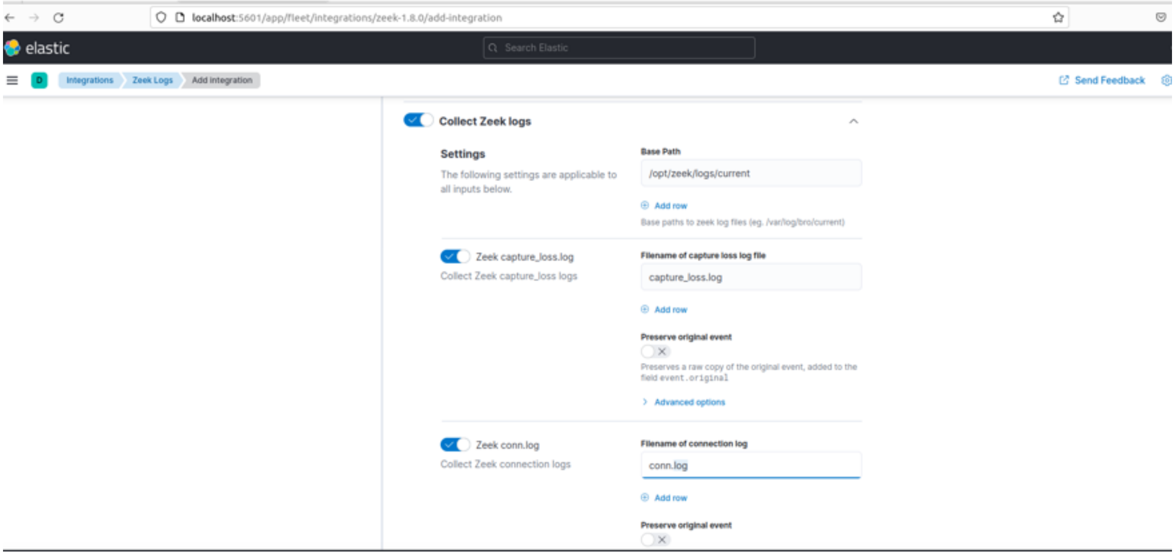
- Give the path where zeek logs stored



```
: a/: No such file or directory
irtualBox:/home/a# /opt/zeel/logs/current#ls
```



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2023-08-15-20-00-01
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_bytes      resp_bytes      conn_state      local_orig      local_resp
ed_bytes        history orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_parents
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool    bool    count   string  count   count   count   count   set[string]
1692109799.569452       CvHrt72jIcRCoeBBAk      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109800.594809       COkkuUDxTHWHoWOmd       192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.563787       CHUtSK1EkzpBpn1Fj7      192.168.128.129 54915   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.563978       CJDKkC1zKeagrxVFYb      192.168.128.129 59382   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.564078       Ceovc44fI8WalKHhB2      192.168.128.129 58498   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.564351       CQhD9Y2nIXeFgW3a        192.168.128.129 48331   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109802.608777       CtUaMs4FYaxaBybKCl      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109806.703519       CrgE9r3feTHKpbOtHk      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109814.612171       CSVgSf3OXfkJZFOnt2      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109815.655527       CJBEZ12TpaKDYDZrc7      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.599495       Cpa6ld48FuFoiKOwD3      192.168.128.129 34987   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.599699       CztbKY1mVWHdxSGGPk      192.168.128.129 33829   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.599948       C7KoAS12GjkayjyZg4      192.168.128.129 34753   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.600290       Cu0ozr1GfhagdQyGxl      192.168.128.129 42859   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.600497       CwR6ru47hLZ3mX9Hhf      192.168.128.129 38296   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.600932       CA24qL36IrV8eVqsud      192.168.128.129 41801   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109810.490462       CgsKfm43Ps7t8yTzD5      192.168.128.129 53672   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109817.717870       CQAfJM39saLgh8UEEf      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109821.817420       CB9OK126MYoPiLDy27      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109829.632272       CdD18z4OA35tjyrDzl      192.168.128.129 40510   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109830.639696       ClN3iX1ahoIZPeG0S3      192.168.128.129 40510   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.617310       CvXOuS2uVyRseU6tog      192.168.128.129 43988   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.617713       C02c9xuVWhCzEKsU1       192.168.128.129 59767   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.618129       CNui7TCyla58mJPsg       192.168.128.129 44948   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.618473       CUK8s32qk8IkircFcl      192.168.128.129 36646   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619017       CnapGt3AKcWAD6r38b      192.168.128.129 38310   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619235       CYzfj52530amZBHvr       192.168.128.129 53275   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619438       C0enSq3tOBpy7qzYIa      192.168.128.129 51916   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619573       CI4EGw1p6uEayGMwH8      192.168.128.129 48442   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
```



Collect Zeek logs

Settings

The following settings are applicable to all inputs below.

Base Path

/opt/zeek/logs/current

Base paths to zeek log files (eg. /var/log/bro/current)

Zeek capture_loss.log

Collect Zeek capture_loss logs

Filename of capture loss log file

capture_loss.log

Preserve original event

Preserves a raw copy of the original event, added to the field `event.original`

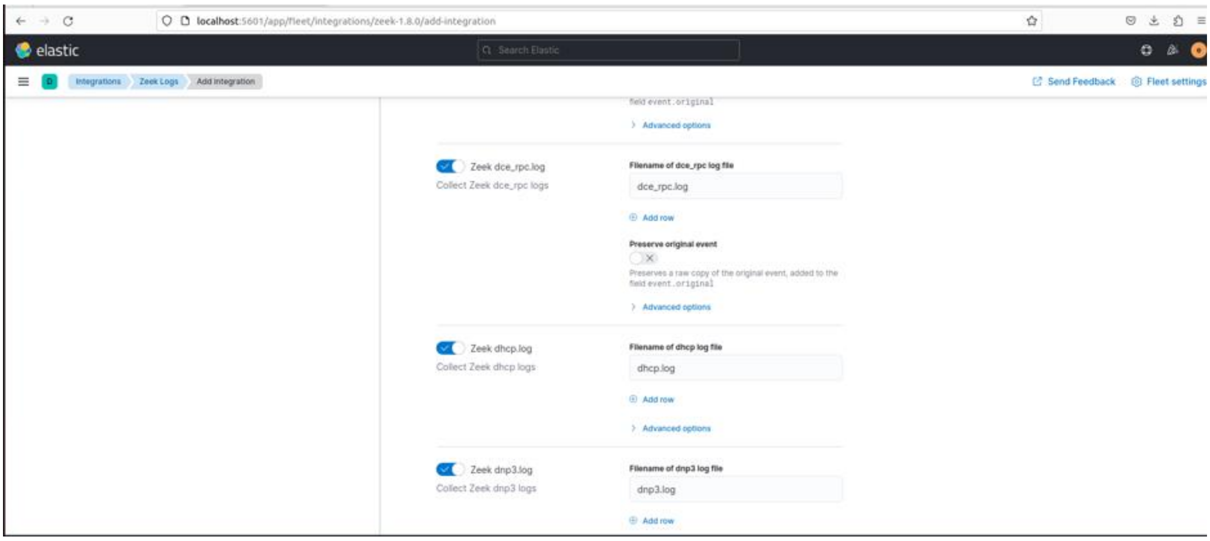
Zeek conn.log

Collect Zeek connection logs

Filename of connection log

conn.log

Preserve original event



field `event.original`

Zeek dce_rpc.log

Collect Zeek dce_rpc logs

Filename of dce_rpc log file

dce_rpc.log

Preserve original event

Preserves a raw copy of the original event, added to the field `event.original`

Zeek dhcp.log

Collect Zeek dhcp logs

Filename of dhcp log file

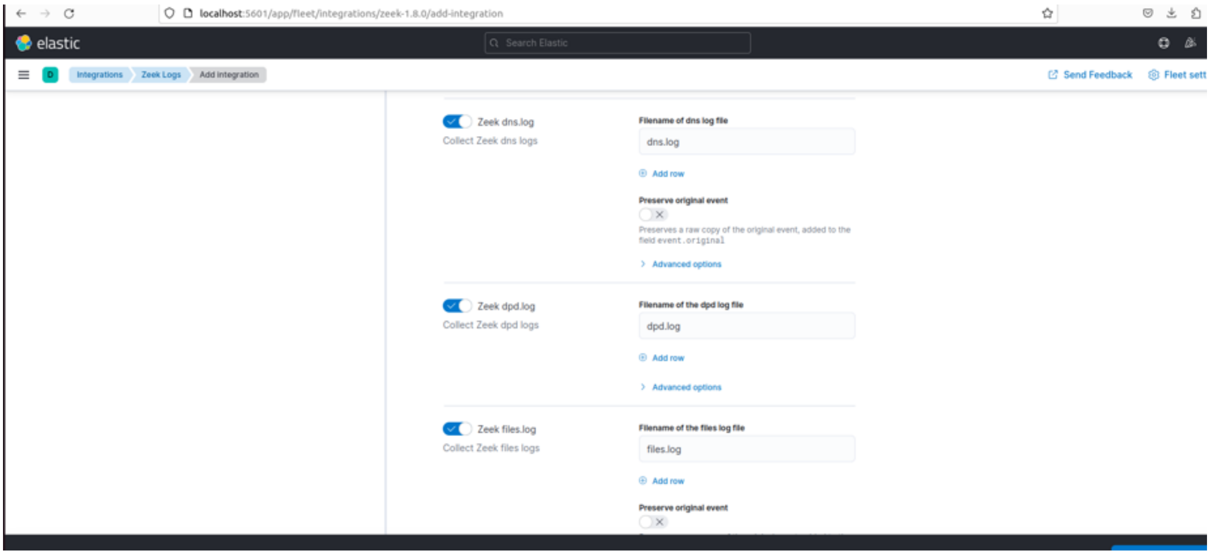
dhcp.log

Zeek dnp3.log

Collect Zeek dnp3 logs

Filename of dnp3 log file

dnp3.log



Zeek dns.log

Collect Zeek dns logs

Filename of dns log file

dns.log

Preserve original event

Preserves a raw copy of the original event, added to the field `event.original`

Zeek dpd.log

Collect Zeek dpd logs

Filename of the dpd log file

dpd.log

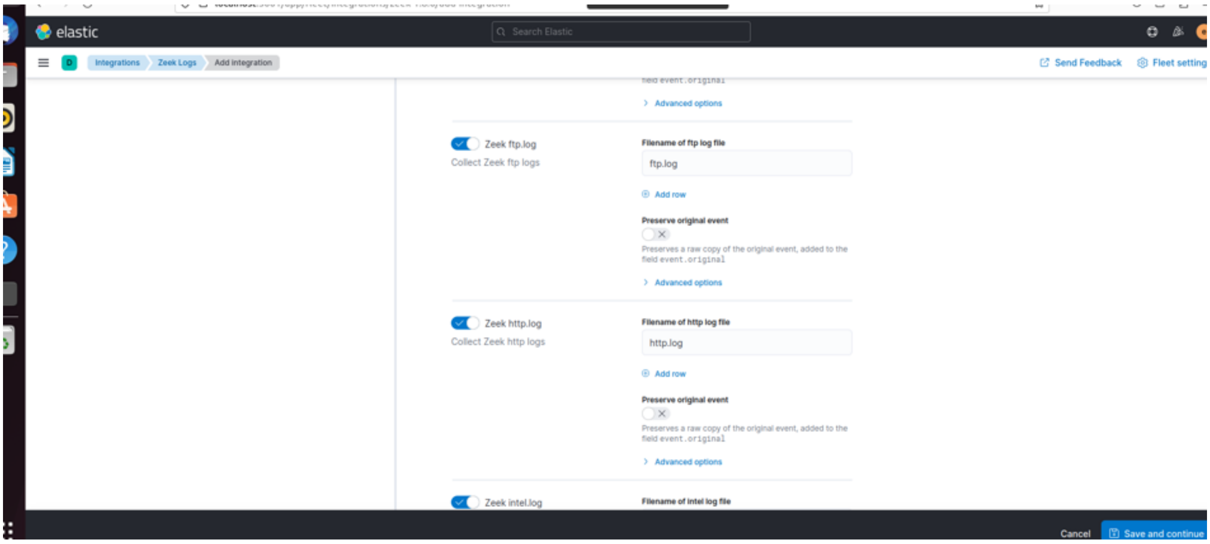
Zeek files.log

Collect Zeek files logs

Filename of the files log file

files.log

Preserve original event



field event.original

› Advanced options

Zeek ftp.log
Collect Zeek ftp logs

Filename of ftp log file
ftp.log

⊕ Add row

Preserve original event
Preserves a raw copy of the original event, added to the field event.original

› Advanced options

Zeek http.log
Collect Zeek http logs

Filename of http log file
http.log

⊕ Add row

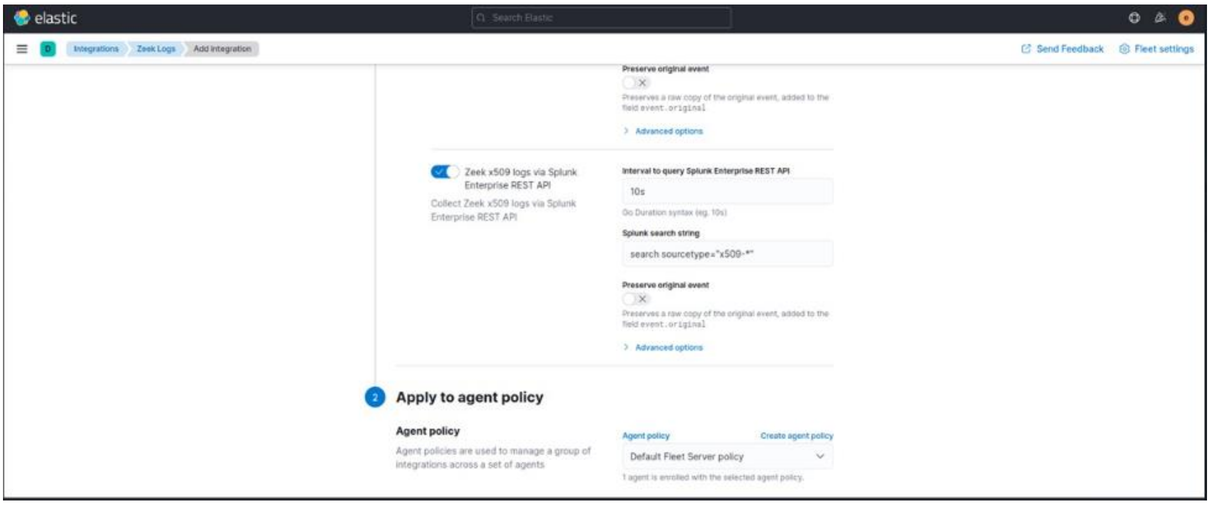
Preserve original event
Preserves a raw copy of the original event, added to the field event.original

› Advanced options

Zeek intel.log

Filename of intel log file

- Leave all by default
- Change Agent policy



Preserve original event
Preserves a raw copy of the original event, added to the field event.original

› Advanced options

Zeek x509 logs via Splunk Enterprise REST API
Collect Zeek x509 logs via Splunk Enterprise REST API

Interval to query Splunk Enterprise REST API
10s
Go Duration syntax (eg. 10s)

Splunk search string
search sourcetype="x509-*"

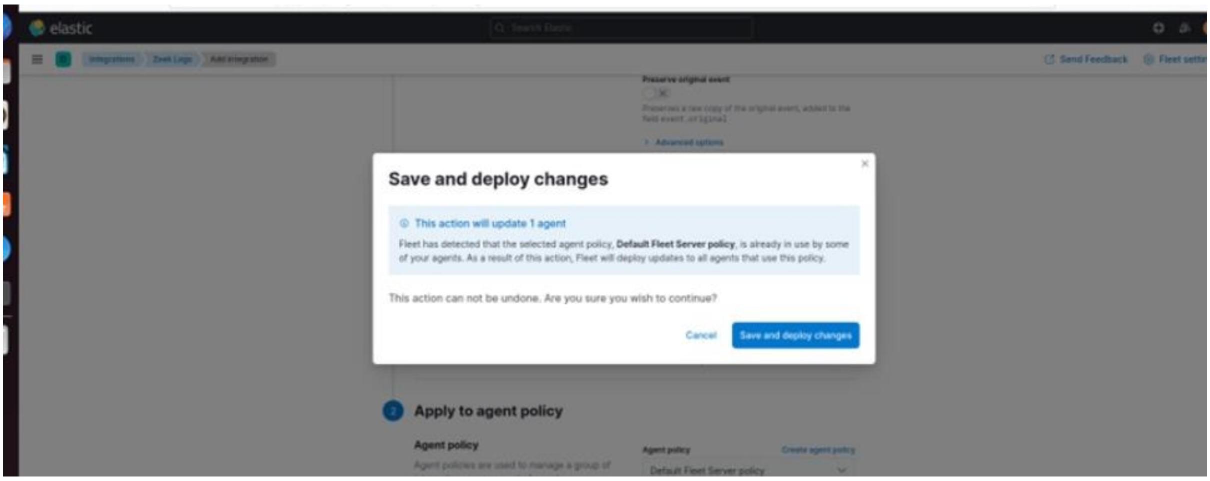
Preserve original event
Preserves a raw copy of the original event, added to the field event.original

› Advanced options

2 Apply to agent policy

Agent policy
Agent policies are used to manage a group of integrations across a set of agents

Agent policy
Create agent policy
Default Fleet Server policy
1 agent is enrolled with the selected agent policy.



Save and deploy changes

This action will update 1 agent

Fleet has detected that the selected agent policy, **Default Fleet Server policy**, is already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use this policy.

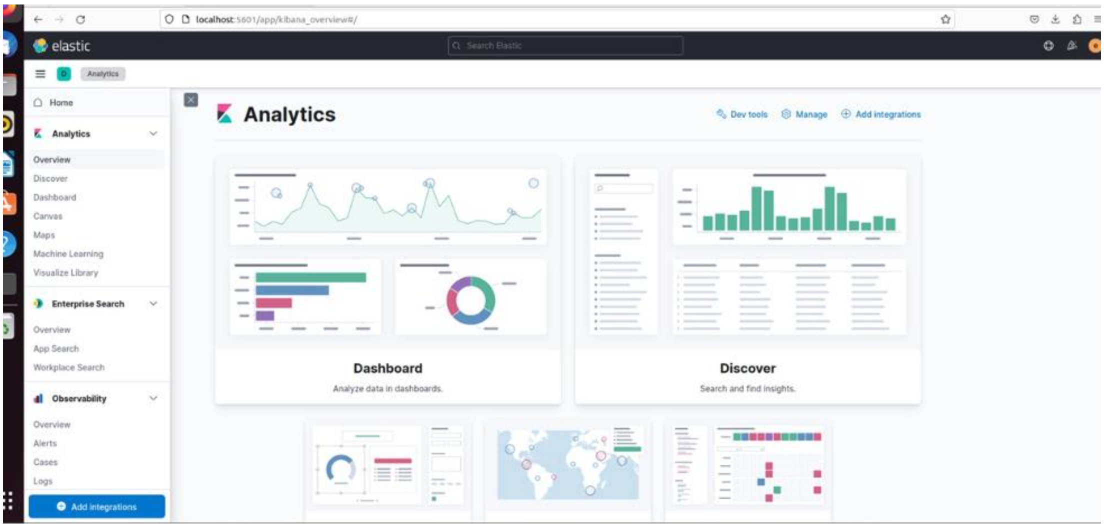
This action can not be undone. Are you sure you wish to continue?

2 Apply to agent policy

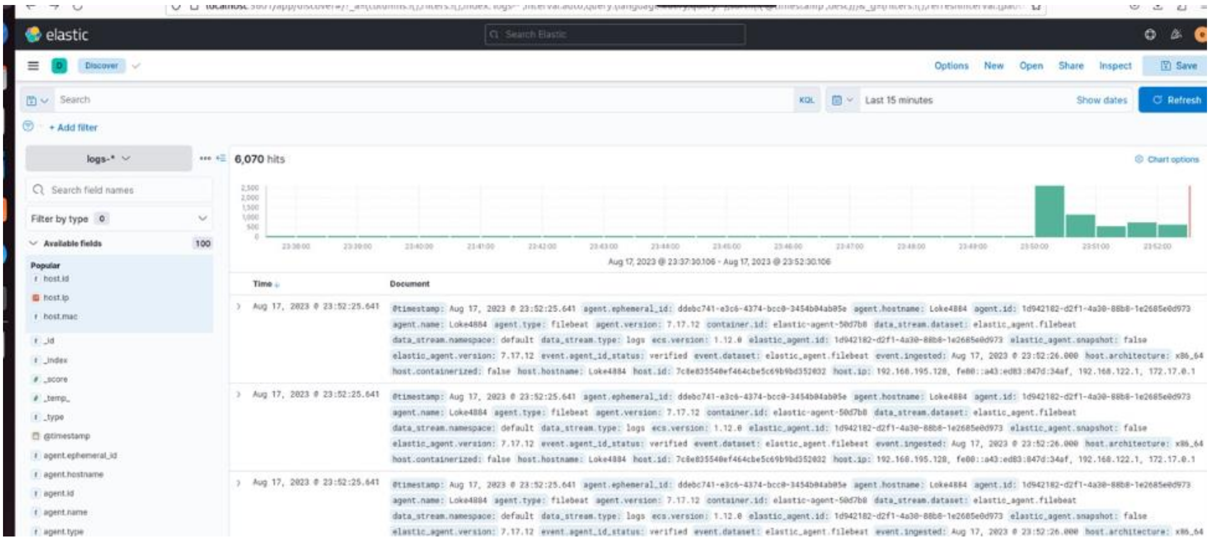
Agent policy
Agent policies are used to manage a group of

Agent policy
Create agent policy
Default Fleet Server policy

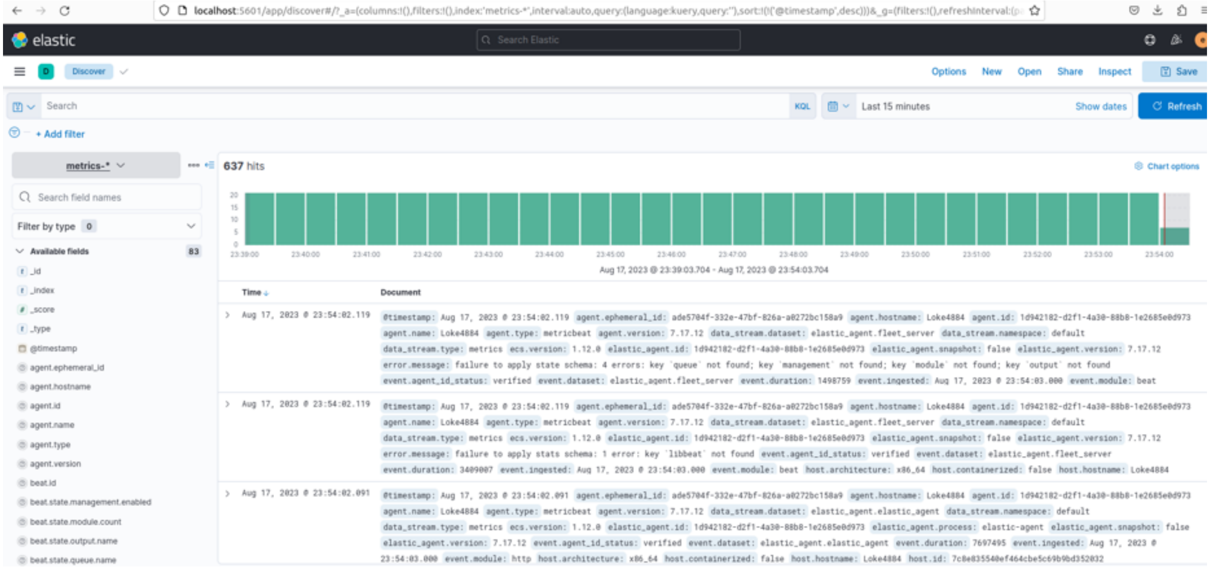
- Go to discover



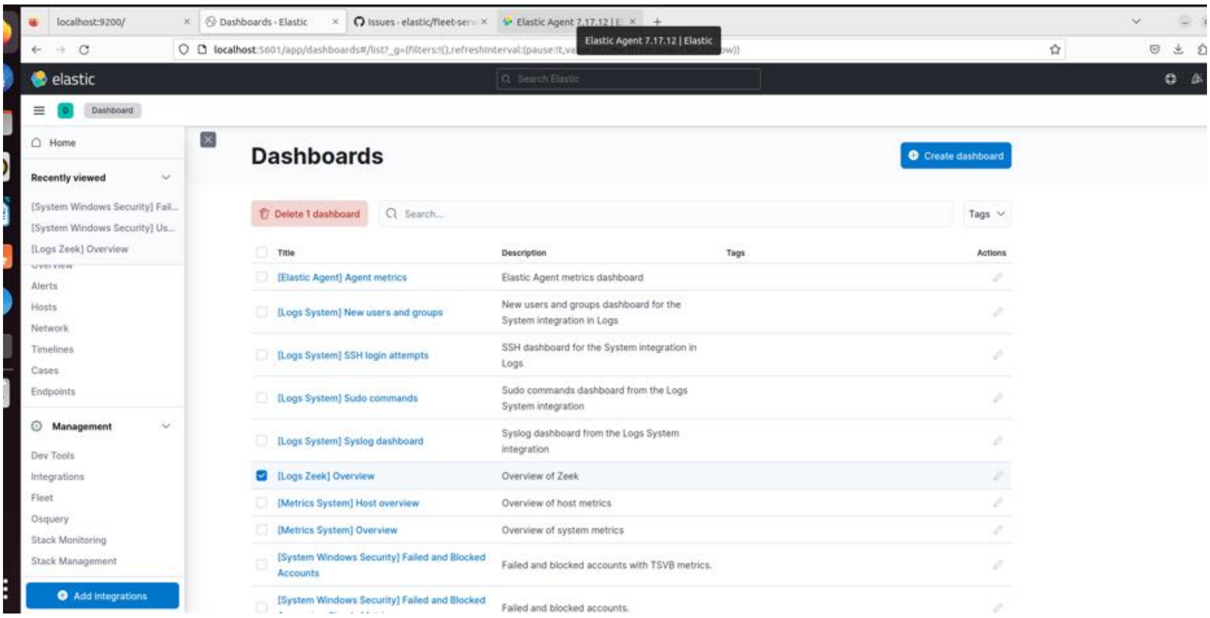
- In the logs



```
Aug 17, 2023 @ 23:52:25.641  @timestamp: Aug 17, 2023 @ 23:52:25.641 agent.ephemeral_id: ddebc741-e3c6-4374-bcc0-3454b04ab05e agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973
                             agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: elastic-agent-50d7b8 data_stream.dataset: elastic_agent.filebeat
                             data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false
                             elastic_agent.version: 7.17.12 event.agent_id_status: verified event.dataset: elastic_agent.filebeat event.ingested: Aug 17, 2023 @ 23:52:26.000 host.architecture: x86_64
                             host.containerized: false host.hostname: Loke4884 host.id: 7c8e835540ef464cbe5c69b9bd352032 host.ip: 192.168.195.128, fe80::a43:ed83:847d:34af, 192.168.122.1, 172.17.0.1
Aug 17, 2023 @ 23:52:25.641  @timestamp: Aug 17, 2023 @ 23:52:25.641 agent.ephemeral_id: ddebc741-e3c6-4374-bcc0-3454b04ab05e agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973
                             agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: elastic-agent-50d7b8 data_stream.dataset: elastic_agent.filebeat
                             data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false
                             elastic_agent.version: 7.17.12 event.agent_id_status: verified event.dataset: elastic_agent.filebeat event.ingested: Aug 17, 2023 @ 23:52:26.000 host.architecture: x86_64
                             host.containerized: false host.hostname: Loke4884 host.id: 7c8e835540ef464cbe5c69b9bd352032 host.ip: 192.168.195.128, fe80::a43:ed83:847d:34af, 192.168.122.1, 172.17.0.1
Aug 17, 2023 @ 23:52:25.641  @timestamp: Aug 17, 2023 @ 23:52:25.641 agent.ephemeral_id: ddebc741-e3c6-4374-bcc0-3454b04ab05e agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973
                             agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: elastic-agent-50d7b8 data_stream.dataset: elastic_agent.filebeat
                             data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false
                             elastic_agent.version: 7.17.12 event.agent_id_status: verified event.dataset: elastic_agent.filebeat event.ingested: Aug 17, 2023 @ 23:52:26.000 host.architecture: x86_64
```



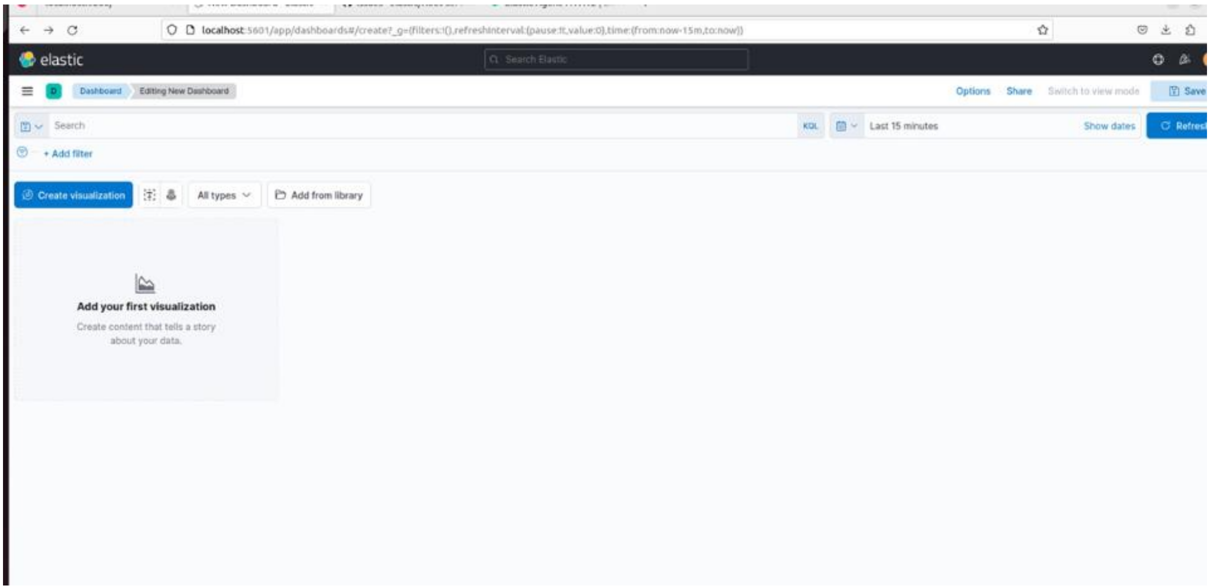
```
Aug 17, 2023 @ 23:54:02.119  @timestamp: Aug 17, 2023 @ 23:54:02.119 agent.ephemeral_id: ade5704f-332e-47bf-826a-a0272bc158a9 agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973
                             agent.name: Loke4884 agent.type: metricbeat agent.version: 7.17.12 data_stream.dataset: elastic_agent.fleet_server data_stream.namespace: default
                             data_stream.type: metrics ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12
                             error.message: failure to apply state schema: 4 errors: key `queue` not found; key `management` not found; key `module` not found; key `output` not found
                             event.agent_id_status: verified event.dataset: elastic_agent.fleet_server event.duration: 1498759 event.ingested: Aug 17, 2023 @ 23:54:03.000 event.module: beat
Aug 17, 2023 @ 23:54:02.119  @timestamp: Aug 17, 2023 @ 23:54:02.119 agent.ephemeral_id: ade5704f-332e-47bf-826a-a0272bc158a9 agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973
                             agent.name: Loke4884 agent.type: metricbeat agent.version: 7.17.12 data_stream.dataset: elastic_agent.fleet_server data_stream.namespace: default
                             data_stream.type: metrics ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12
                             error.message: failure to apply stats schema: 1 error: key `libbeat` not found event.agent_id_status: verified event.dataset: elastic_agent.fleet_server
                             event.duration: 3409007 event.ingested: Aug 17, 2023 @ 23:54:03.000 event.module: beat host.architecture: x86_64 host.containerized: false host.hostname: Loke4884
Aug 17, 2023 @ 23:54:02.091  @timestamp: Aug 17, 2023 @ 23:54:02.091 agent.ephemeral_id: ade5704f-332e-47bf-826a-a0272bc158a9 agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973
                             agent.name: Loke4884 agent.type: metricbeat agent.version: 7.17.12 data_stream.dataset: elastic_agent.elastic_agent data_stream.namespace: default
                             data_stream.type: metrics ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.process: elastic-agent elastic_agent.snapshot: false
                             elastic_agent.version: 7.17.12 event.agent_id_status: verified event.dataset: elastic_agent.elastic_agent event.duration: 7697495 event.ingested: Aug 17, 2023 @
                             23:54:03.000 event.module: http host.architecture: x86_64 host.containerized: false host.hostname: Loke4884 host.id: 7c8e835540ef464cbe5c69b9bd352032
```



localhost:5601/app/dashboards#/list?_g=(filters:!(),refreshInterval:(pause:!t,va ... w))

Dashboards

	Title	Description	Tags	Actions
□	[Elastic Agent] Agent metrics	Elastic Agent metrics dashboard		
□	[Logs System] New users and groups	New users and groups dashboard for the System integration in Logs		
□	[Logs System] SSH login attempts	SSH dashboard for the System integration in Logs		
□	[Logs System] Sudo commands	Sudo commands dashboard from the Logs System integration		
□	[Logs System] Syslog dashboard	Syslog dashboard from the Logs System integration		
☑	[Logs Zeek] Overview	Overview of Zeek		
□	[Metrics System] Host overview	Overview of host metrics		
□	[Metrics System] Overview	Overview of system metrics		
□	[System Windows Security] Failed and Blocked Accounts	Failed and blocked accounts with TSVB metrics.		
□	[System Windows Security] Failed and Blocked	Failed and blocked accounts.		

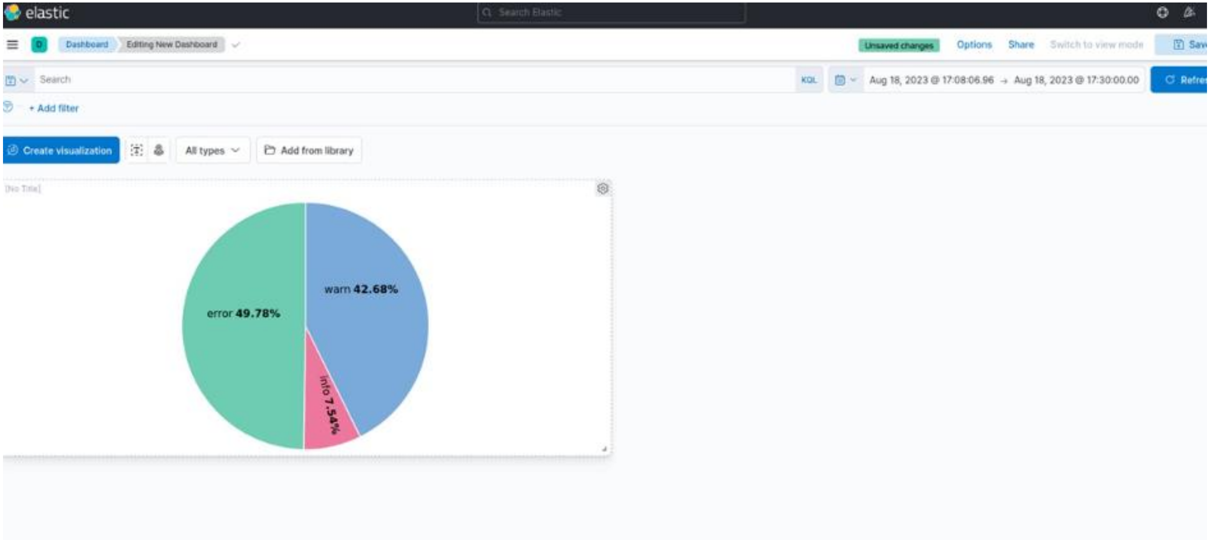


localhost:5601/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))

Last 15 minutes

Add your first visualization

Create content that tells a story about your data.



Aug 18, 2023 @ 17:08:06.96 → Aug 18, 2023 @ 17:30:00.00