කැලණිය විශ්වවිද්‍යාලය
களனி பல்கலைக்கழகம்
UNIVERSITY OF KELANIYA

Bachelor of Information and Communication Technology

CTNT 32051 –

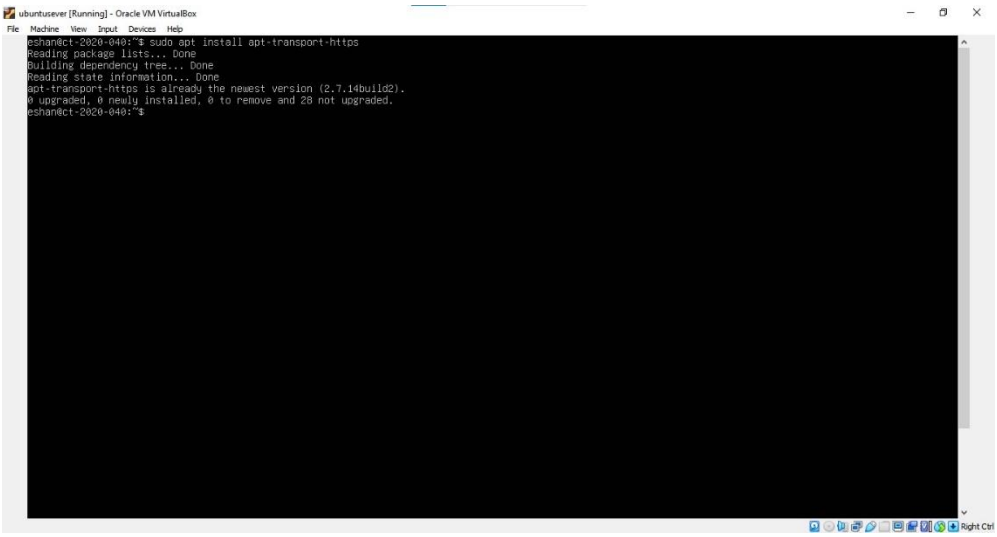
Cyber Security Laboratory (2022/2023)

CT/2020/040 –

WANASINHA W.P.E.M.

Task 1: ELK Stack Installation

Update Packages



Import Elasticsearch PGP Key:

Add Elasticsearch Repository:

Install Elasticsearch:

```
eshan@ct-2020-040:~$ sudo apt-get 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 33 not upgraded.
Need to get 636 MB of archives.
After this operation, 1,210 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.17.2 [636 MB]
3% [1 elasticsearch 21.1 MB/636 MB 3%]                                                                    449 kB/s 22min 51s
```

Enable and Start Elasticsearch:

ubuntusever [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
eshan@ct-2020-040:~$ sudo systemctl start elasticsearch
[sudo] password for eshan:
eshan@ct-2020-040:~$
eshan@ct-2020-040:~$ sudo systemctl start elasticsearch
eshan@ct-2020-040:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
eshan@ct-2020-040:~$ _
```

eshan@ct-2020-040: ~

```
  GNU nano 7.2                                                    /etc/elasticsearch/elasticsearch.yml
# 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: 192.168.1.12
#
# 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]"]
#
```

eshan@ct-2020-040: ~

```
  GNU nano 7.2                                                    /etc/elasticsearch/elasticsearch.yml
#
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 17-03-2025 05:33:56
#
# --------------------------------------------------------------------------

# Enable security features
xpack.security.enabled: true

xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: true
  certificate: certs/elastic/elastic.crt
  key: certs/elastic/elastic.key
  certificate_authorities: certs/ca/ca.crt


# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
cluster.initial_master_nodes: ["ct-2020-040"]

# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0

# Allow other nodes to join the cluster from anywhere
# Connections are encrypted and mutually authenticated
#transport.host: 0.0.0.0

#----------------------- END SECURITY AUTO CONFIGURATION -------------------------
```

eshan@ct-2020-040: ~

```
eshan@ct-2020-040:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-20 16:20:22 UTC; 1h 16min ago
       Docs: https://www.elastic.co
   Main PID: 863 (java)
      Tasks: 103 (limit: 5023)
     Memory: 2.6G (peak: 2.8G swap: 112.8M swap peak: 150.2M)
        CPU: 3min 55.851s
     CGroup: /system.slice/elasticsearch.service
             ├─ 863 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch -Dc
             ├─ 961 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.
             └─1015 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Mar 20 16:19:57 ct-2020-040 systemd[1]: Starting elasticsearch.service - Elasticsearch...
Mar 20 16:20:01 ct-2020-040 systemd-entrypoint[961]: CompileCommand: dontinline java/lang/invoke/MethodHandle.setAsTypeCache bool dontinline = true
Mar 20 16:20:01 ct-2020-040 systemd-entrypoint[961]: CompileCommand: dontinline java/lang/invoke/MethodHandle.asTypeUncached bool dontinline = true
Mar 20 16:20:22 ct-2020-040 systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)
```

eshan@ct-2020-040: ~

```
eshan@ct-2020-040:~$ curl -u elastic:abcd1234 -k -X GET "https://192.168.1.12:9200"
{
  "name" : "ct-2020-040",
  "cluster_name" : "es-demo",
  "cluster_uuid" : "F5fLqcN5SdSfSP-v6fHC4Q",
  "version" : {
    "number" : "8.17.3",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "a091390de485bd4b127884f7e565c0cad59b10d2",
    "build_date" : "2025-02-28T10:07:26.089129809Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
eshan@ct-2020-040:~$
```

Install Logstash

ubuntusever [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
eshan@ct-2020-040:~$ sudo apt-get 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 34 not upgraded.
Need to get 437 MB of archives.
After this operation, 716 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.17.3-1 [437 MB]
Fetched 437 MB in 6min 9s (1,183 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 90649 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.17.3-1_amd64.deb ...
Unpacking logstash (1:8.17.3-1) ...
Setting up logstash (1:8.17.3-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
eshan@ct-2020-040:~$ _
```

ubuntusever [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
eshan@ct-2020-040:~$ sudo systemctl start logstash
[sudo] password for eshan:
eshan@ct-2020-040:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /usr/lib/systemd/system/logstash.service.
eshan@ct-2020-040:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-03-05 00:08:25 UTC; 2s ago
   Main PID: 5261 (java)
      Tasks: 21 (limit: 4609)
     Memory: 205.2M (peak: 205.4M)
        CPU: 4.662s
     CGroup: /system.slice/logstash.service
             └─5261 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -XX:+HeapD>

Mar 05 00:08:25 ct-2020-040 systemd[1]: logstash.service: Scheduled restart job, restart counter is at 2.
Mar 05 00:08:25 ct-2020-040 systemd[1]: Started logstash.service - logstash.
Mar 05 00:08:25 ct-2020-040 logstash[5261]: Using bundled JDK: /usr/share/logstash/jdk
lines 1-13/13 (END)
```

Install Kibana

ubuntusever [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
eshan@ct-2020-040:~$ sudo apt-get install kibana
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 34 not upgraded.
Need to get 343 MB of archives.
After this operation, 1,045 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.17.3 [343 MB]
20% [1 kibana 84.0 MB/343 MB 24%]                                                                    9,917 kB/s 26s
```

eshan@ct-2020-040: ~

```
  GNU nano 7.2                                                    /etc/kibana/kibana.yml
# ==================== 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: "0.0.0.0"

# 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: "https://kibana.198.168.1.12.net: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"

# ==================== System: Kibana Server (Optional) ====================
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
server.ssl.enabled: true
server.ssl.certificateAuthorities: ["/etc/kibana/certs/elastic.192.168.1.12/ca.crt"]
server.ssl.certificate: /etc/kibana/certs/kibana.192.168.1.12/kibana.crt
server.ssl.key: /etc/kibana/certs/kibana.192.168.1.12/kibana.key
```

eshan@ct-2020-040: ~

```
  GNU nano 7.2                                                    /etc/kibana/kibana.yml
# Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.
#elasticsearch.shardTimeout: 30000

# ================== System: Elasticsearch (Optional) ==================
# These files are used to verify the identity of Kibana to Elasticsearch and are required when
# xpack.security.http.ssl.client_authentication in Elasticsearch is set to required.
#elasticsearch.ssl.certificate: /path/to/your/client.crt
#elasticsearch.ssl.key: /path/to/your/client.key

# Enables you to specify a path to the PEM file for the certificate
# authority for your Elasticsearch instance.
elasticsearch.ssl.certificateAuthorities: ["/etc/kibana/certs/elastic.192.168.1.12/ca.crt"]

# To disregard the validity of SSL certificates, change this setting's value to 'none'.
elasticsearch.ssl.verificationMode: full

# ================== System: Logging ==================
# Set the value of this setting to off to suppress all logging output, or to debug to log everything. Defaults to 'info'
#logging.root.level: debug

# Enables you to specify a file where Kibana stores log output.
logging:
  appenders:
    file:
      type: file
      fileName: /var/log/kibana/kibana.log
      layout:
        type: json
  root:
    appenders:
      - default
      - file
#  policy:
#    type: size-limit
#    size: 256mb
#  strategy:
#    type: numeric
#    max: 10
#  layout:
```

eshan@ct-2020-040: ~

```
  GNU nano 7.2                                                    /etc/kibana/kibana.yml

# ================== System: Elasticsearch ==================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["https://192.168.1.12:9200"]

# 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: "kibana_system"
#elasticsearch.password: "pass"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# Service account tokens are Bearer style tokens that replace the traditional username/password based configuration.
# Use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of
# the elasticsearch.requestTimeout setting.
#elasticsearch.pingTimeout: 1500

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This value
# must be a positive integer.
#elasticsearch.requestTimeout: 30000

# The maximum number of sockets that can be used for communications with elasticsearch.
# Defaults to `800`.
#elasticsearch.maxSockets: 1024

# Specifies whether Kibana should use compression for communications with elasticsearch
# Defaults to `false`.
#elasticsearch.compression: false

# List of Kibana client-side headers to send to Elasticsearch. To send *no* client-side
# headers, set this value to [] (an empty list).
#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom headers cannot be overwritten
# by client-side headers, regardless of the elasticsearch.requestHeadersWhitelist configuration.
```

eshan@ct-2020-040: ~

```
eshan@ct-2020-040:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-20 16:19:57 UTC; 1h 36min ago
       Docs: https://www.elastic.co
   Main PID: 865 (node)
      Tasks: 11 (limit: 5023)
     Memory: 740.8M (peak: 1.0G)
        CPU: 3min 29.947s
     CGroup: /system.slice/kibana.service
             └─865 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Mar 20 17:20:38 ct-2020-040 kibana[865]: [2025-03-20T17:20:38.785+00:00][INFO ][plugins.fleet] Running Fleet Usage telemetry send task
Mar 20 17:20:38 ct-2020-040 kibana[865]: [2025-03-20T17:20:38.798+00:00][INFO ][plugins.fleet.fleet:delete-unenrolled-agents-task:1.0.0] [DeleteUnenrolledAgentsTask] r
Mar 20 17:30:36 ct-2020-040 kibana[865]: [2025-03-20T17:30:36.803+00:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.0] [runTask()] started
Mar 20 17:30:36 ct-2020-040 kibana[865]: [2025-03-20T17:30:36.819+00:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.0] [UnenrollInactiveAgentsTask] r
Mar 20 17:35:36 ct-2020-040 kibana[865]: [2025-03-20T17:35:36.900+00:00][INFO ][plugins.fleet] Fleet Usage: {"agents_enabled":true,"agents":{"total_enrolled":0,"health
Mar 20 17:40:36 ct-2020-040 kibana[865]: [2025-03-20T17:40:36.918+00:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.0] [runTask()] started
Mar 20 17:40:36 ct-2020-040 kibana[865]: [2025-03-20T17:40:36.934+00:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.0] [UnenrollInactiveAgentsTask] r
Mar 20 17:50:36 ct-2020-040 kibana[865]: [2025-03-20T17:50:36.986+00:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.0] [runTask()] started
Mar 20 17:50:37 ct-2020-040 kibana[865]: [2025-03-20T17:50:37.009+00:00][INFO ][plugins.fleet.fleet:unenroll-inactive-agents-task:1.0.0] [UnenrollInactiveAgentsTask] r
Mar 20 17:50:37 ct-2020-040 kibana[865]: [2025-03-20T17:50:37.011+00:00][INFO ][plugins.fleet] Fleet Usage: {"agents_enabled":true,"agents":{"total_enrolled":0,"health
lines 1-21/21 (END)
```

http://192.168.1.9:5601 - Search | Assignment 1.pdf | http://192.168.1.9:5601 - Search | Elastic

Not secure | https://192.168.1.12:5601/login?msg=LOGGED_OUT

Welcome to Elastic

You have logged out of Elastic.

Username

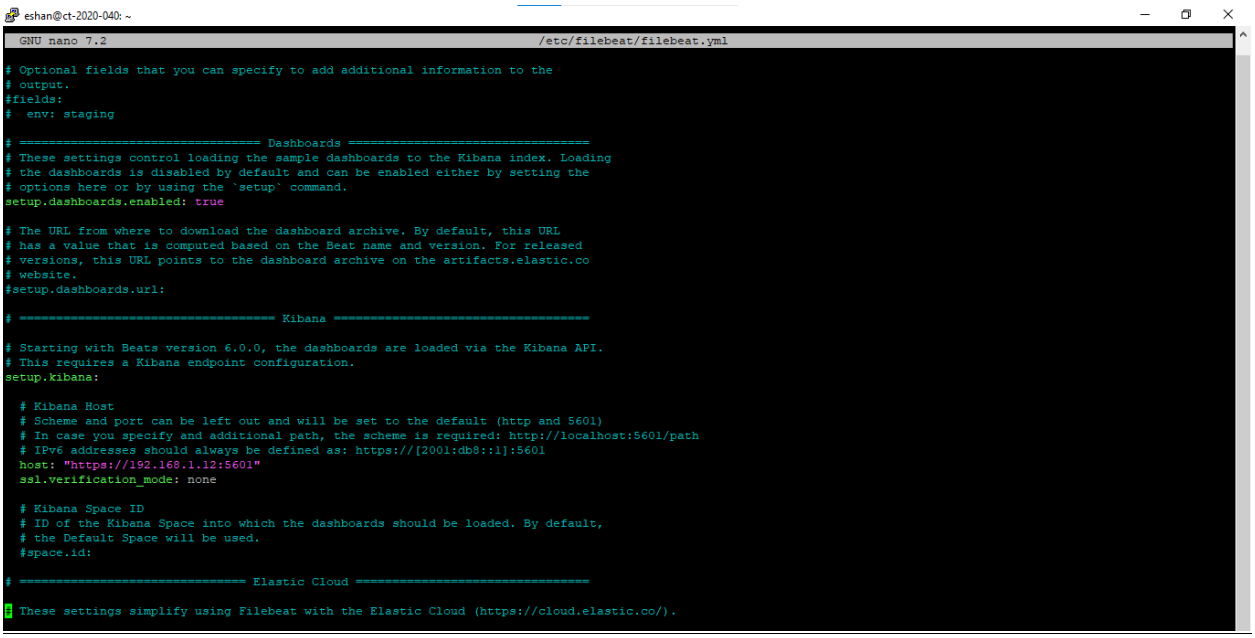
Password

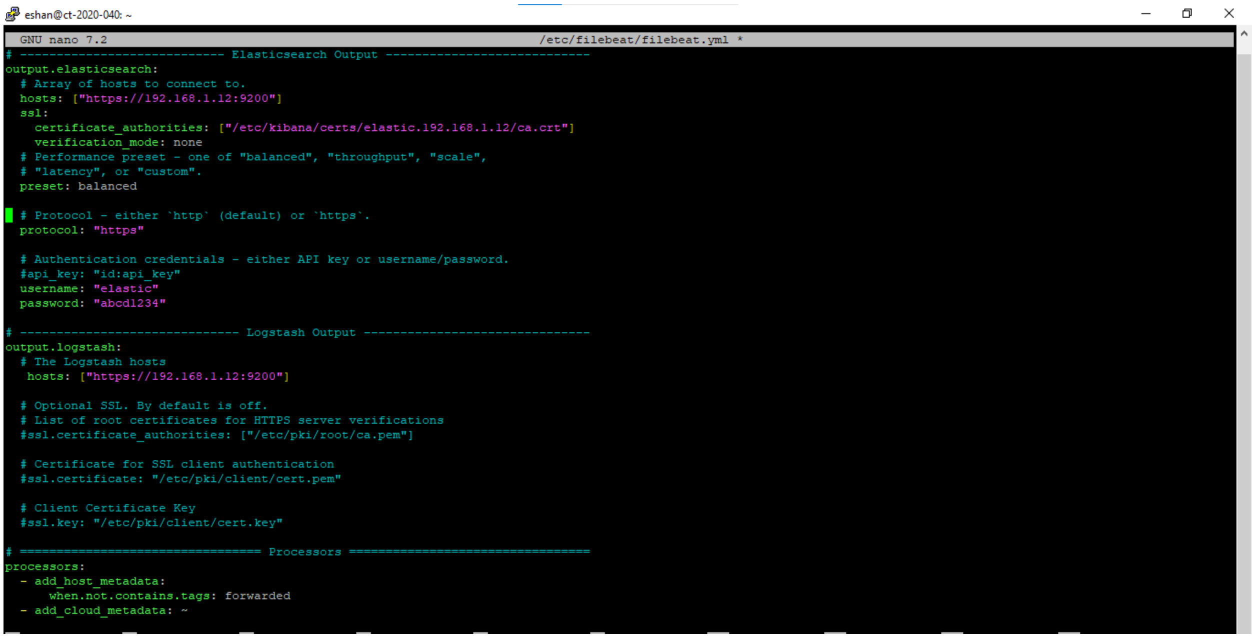
Log in

Install Filebeat

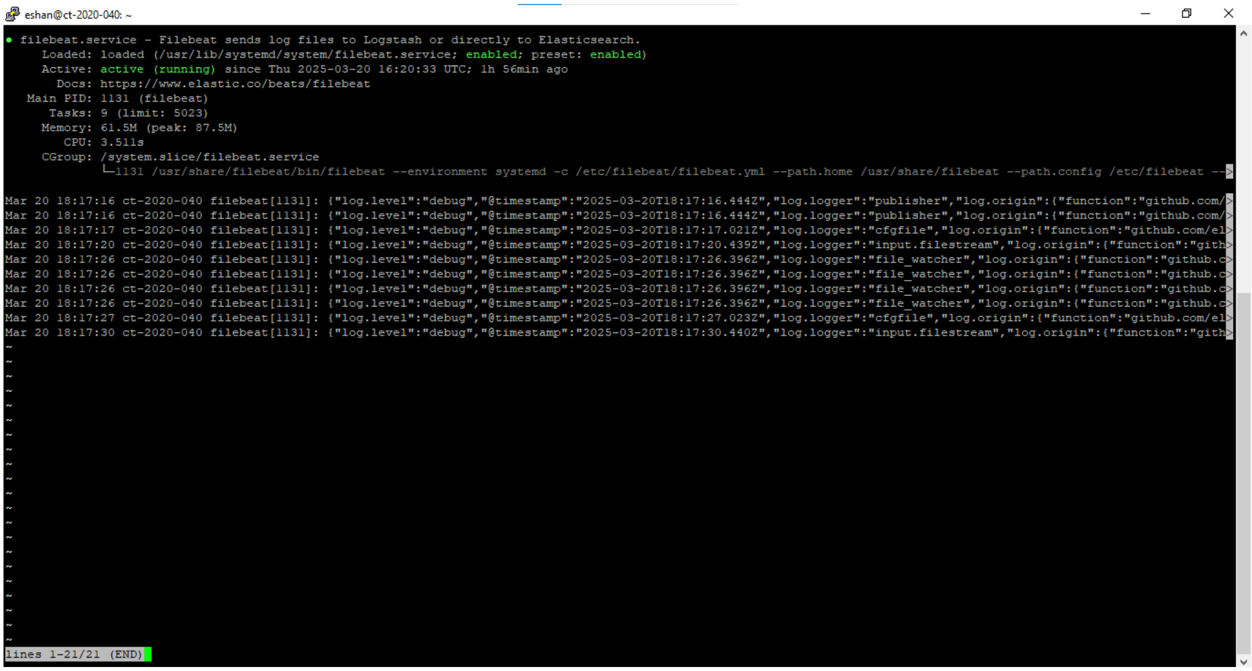
Update package lists and install Filebeat:

sudo apt update && sudo apt install filebeat -y

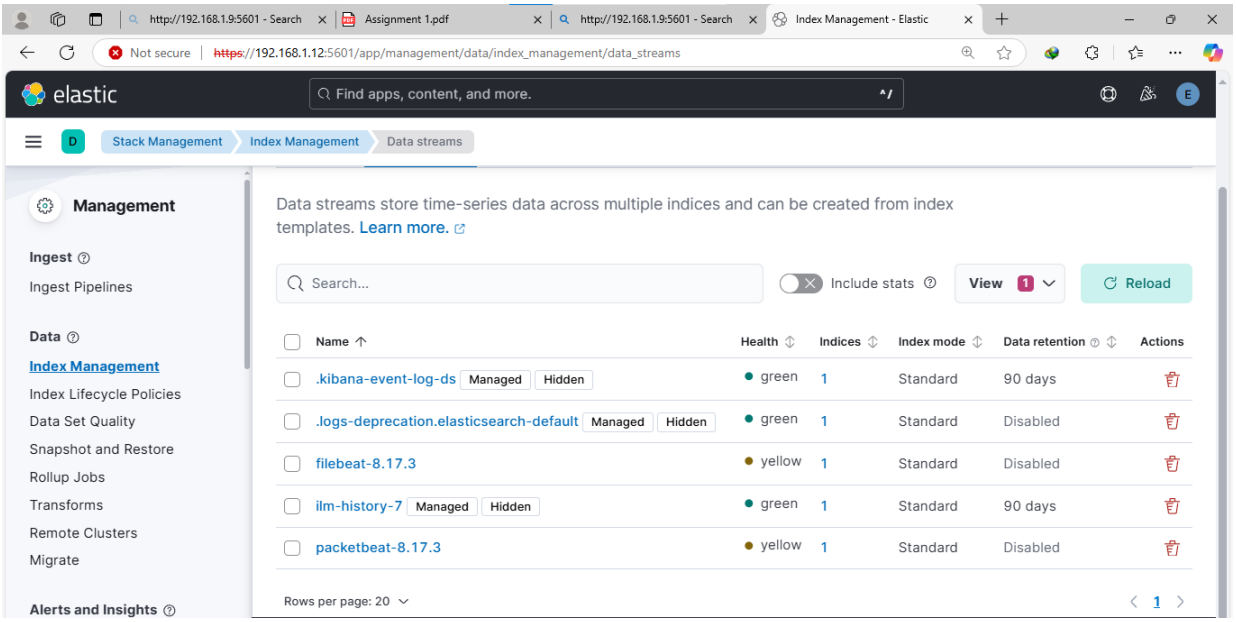


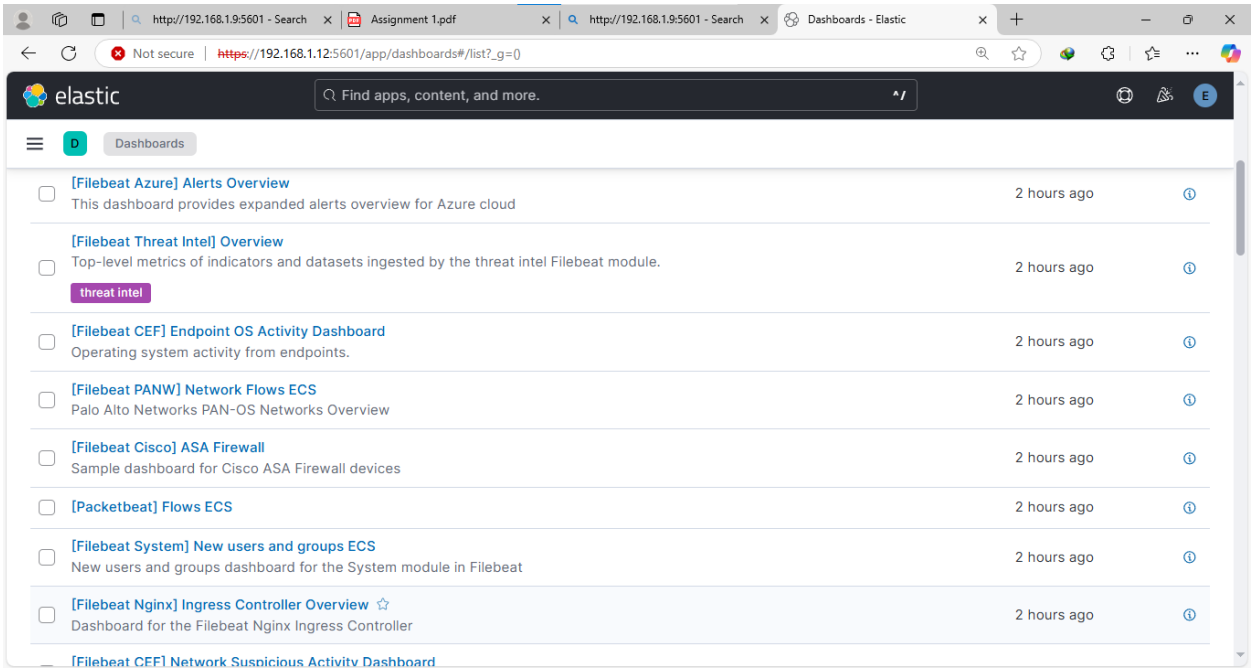


```
  GNU nano 7.2                                    /etc/filebeat/filebeat.yml *
# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://192.168.1.12:9200"]
  ssl:
    certificate_authorities: ["/etc/kibana/certs/elastic.192.168.1.12/ca.crt"]
    verification_mode: none
  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

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

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "abcd1234"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
   hosts: ["https://192.168.1.12:9200"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

# ================================= Processors =================================
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~
```



```
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-20 16:20:33 UTC; 1h 56min ago
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 1131 (filebeat)
      Tasks: 9 (limit: 5023)
     Memory: 61.5M (peak: 87.5M)
        CPU: 3.511s
     CGroup: /system.slice/filebeat.service
             └─1131 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebeat -->

Mar 20 18:17:16 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:16.444Z","log.logger":"publisher","log.origin":{"function":"github.com/>
Mar 20 18:17:16 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:16.444Z","log.logger":"publisher","log.origin":{"function":"github.com/>
Mar 20 18:17:17 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:17.021Z","log.logger":"cfgfile","log.origin":{"function":"github.com/el>
Mar 20 18:17:20 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:20.439Z","log.logger":"input.filestream","log.origin":{"function":"gith>
Mar 20 18:17:26 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:26.396Z","log.logger":"file_watcher","log.origin":{"function":"github.c>
Mar 20 18:17:26 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:26.396Z","log.logger":"file_watcher","log.origin":{"function":"github.c>
Mar 20 18:17:26 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:26.396Z","log.logger":"file_watcher","log.origin":{"function":"github.c>
Mar 20 18:17:26 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:26.396Z","log.logger":"file_watcher","log.origin":{"function":"github.c>
Mar 20 18:17:27 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:27.023Z","log.logger":"cfgfile","log.origin":{"function":"github.com/el>
Mar 20 18:17:30 ct-2020-040 filebeat[1131]: {"log.level":"debug","@timestamp":"2025-03-20T18:17:30.440Z","log.logger":"input.filestream","log.origin":{"function":"gith>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
lines 1-21/21 (END)
```

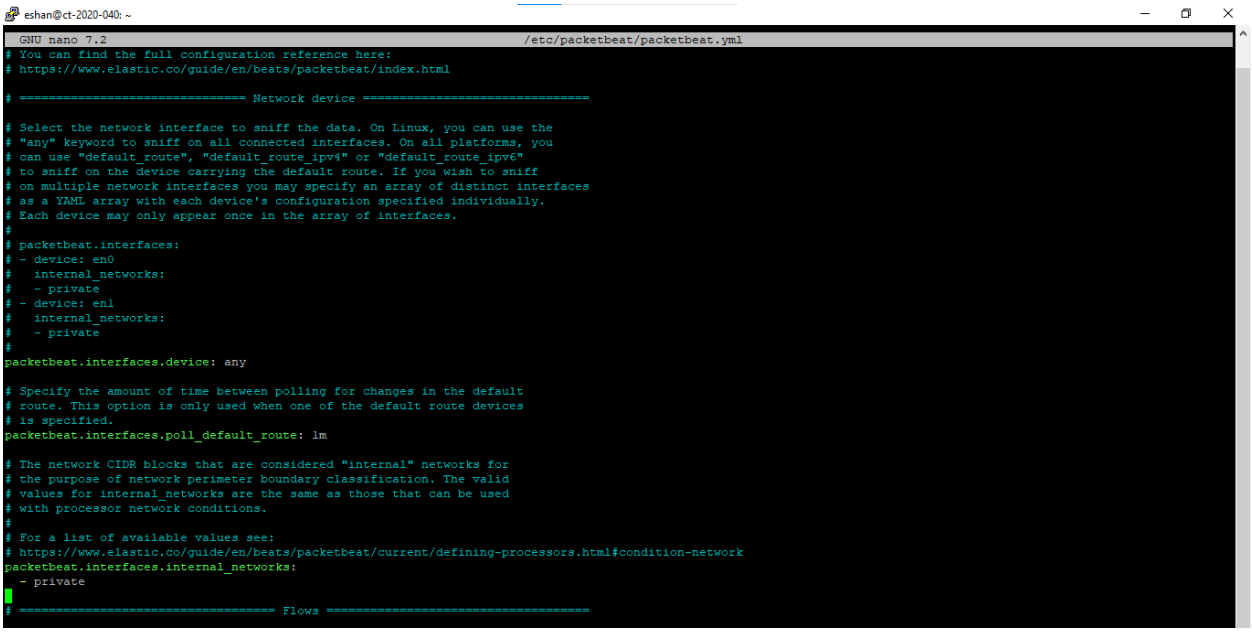

http://192.168.1.9:5601 - Search
Assignment 1.pdf
http://192.168.1.9:5601 - Search
Index Management - Elastic
Not secure
https://192.168.1.12:5601/app/management/data/index_management/data_streams
elastic
Find apps, content, and more.
Stack Management
Index Management
Data streams
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Data Set Quality
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Migrate
Alerts and Insights
Data streams store time-series data across multiple indices and can be created from index templates. Learn more.
Search...
Include stats
View 1
Reload
Name
Health
Indices
Index mode
Data retention
Actions
.kibana-event-log-ds Managed Hidden green 1 Standard 90 days
.logs-deprecation.elasticsearch-default Managed Hidden green 1 Standard Disabled
filebeat-8.17.3 yellow 1 Standard Disabled
ilm-history-7 Managed Hidden green 1 Standard 90 days
packetbeat-8.17.3 yellow 1 Standard Disabled
Rows per page: 20
1

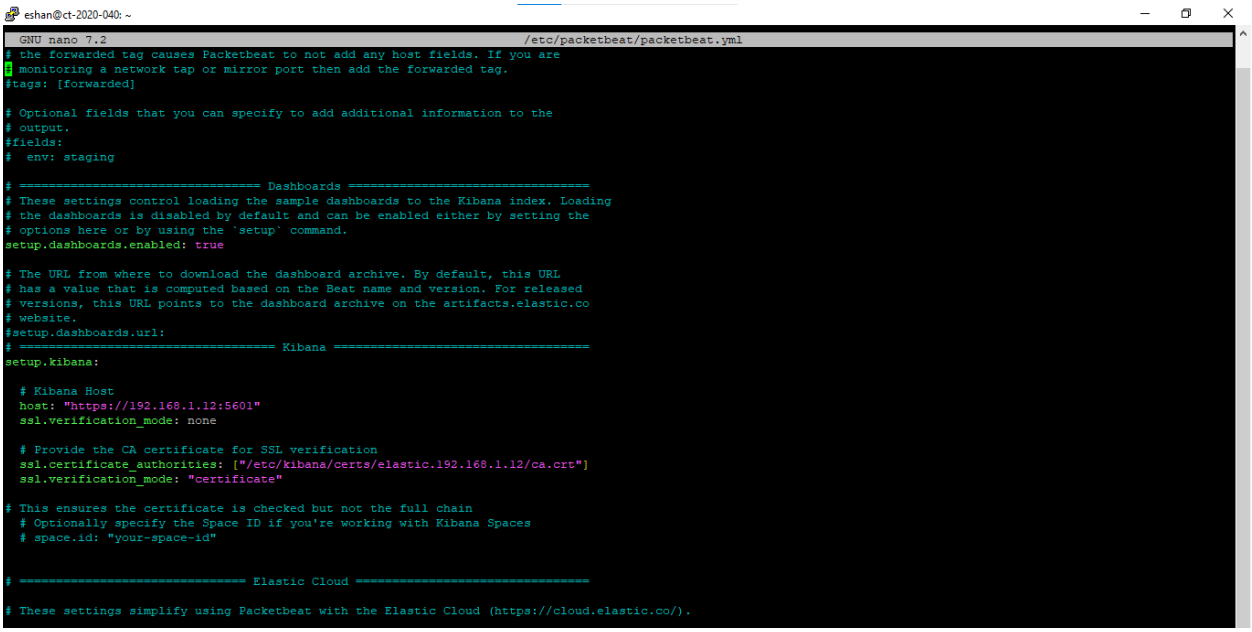

http://192.168.1.9:5601 - Search
Assignment 1.pdf
http://192.168.1.9:5601 - Search
Dashboards - Elastic
Not secure
https://192.168.1.12:5601/app/dashboards#/list?_g=()
elastic
Find apps, content, and more.
Dashboards
[Filebeat Azure] Alerts Overview
This dashboard provides expanded alerts overview for Azure cloud
2 hours ago
[Filebeat Threat Intel] Overview
Top-level metrics of indicators and datasets ingested by the threat intel Filebeat module.
threat intel
2 hours ago
[Filebeat CEF] Endpoint OS Activity Dashboard
Operating system activity from endpoints.
2 hours ago
[Filebeat PANW] Network Flows ECS
Palo Alto Networks PAN-OS Networks Overview
2 hours ago
[Filebeat Cisco] ASA Firewall
Sample dashboard for Cisco ASA Firewall devices
2 hours ago
[Packetbeat] Flows ECS
2 hours ago
[Filebeat System] New users and groups ECS
New users and groups dashboard for the System module in Filebeat
2 hours ago
[Filebeat Nginx] Ingress Controller Overview
Dashboard for the Filebeat Nginx Ingress Controller
2 hours ago
[Filebeat CEF] Network Suspicious Activity Dashboard

install Packetbeat.

Download and Install Packetbeat

sudo apt update && sudo apt install packetbeat -y



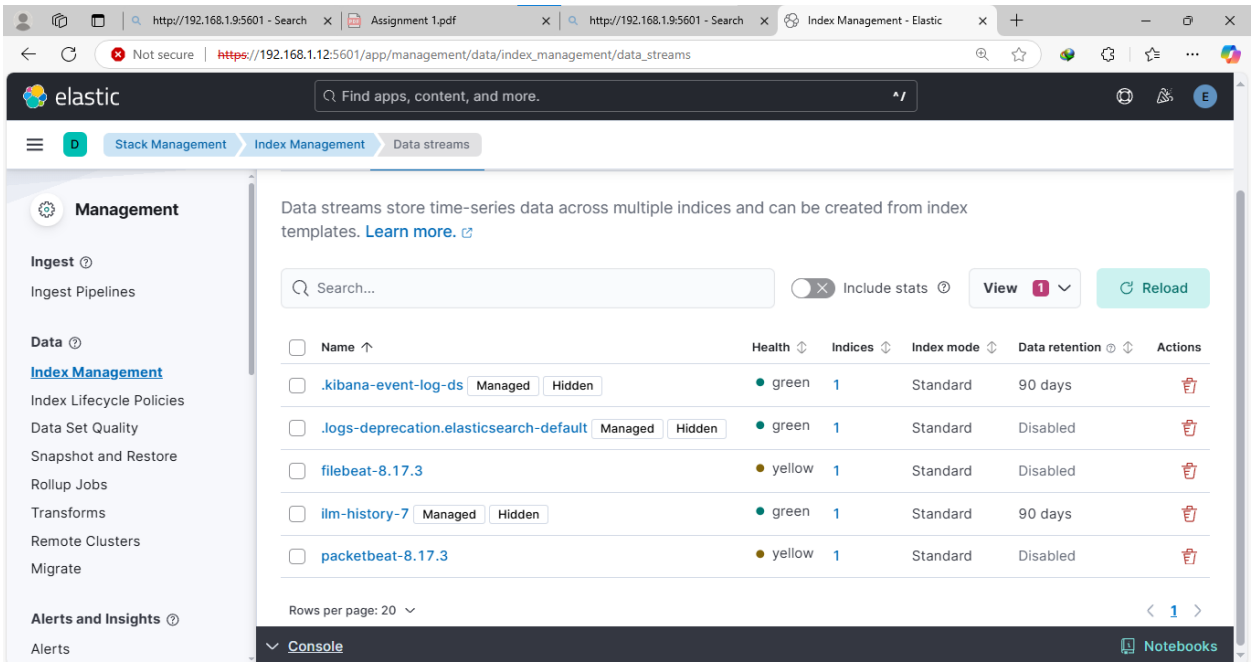


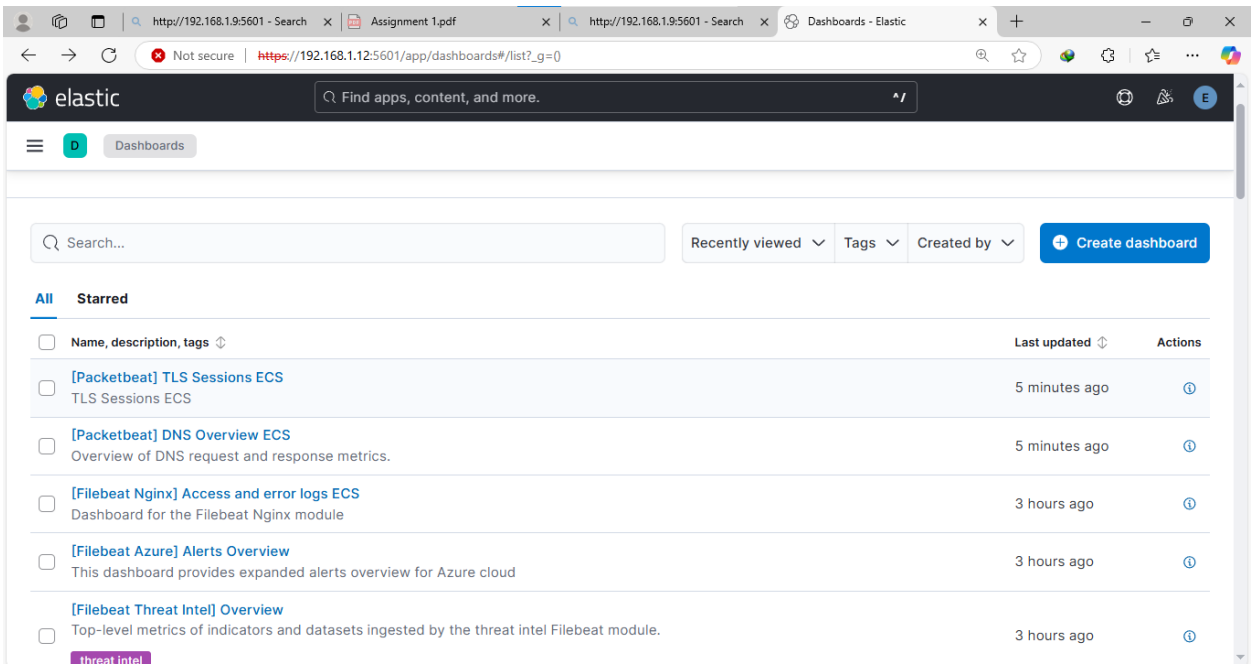
eshan@ct-2020-040: ~

```
  GNU nano 7.2                                                    /etc/packetbeat/packetbeat.yml *

# These settings simplify using Packetbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

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

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

# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  hosts: ["https://192.168.1.12:9200"]
  username: "elastic"
  password: "abcd1234"
  ssl:
    certificate_authorities: ["/etc/kibana/certs/elastic.192.168.1.12/ca.crt"]
    verification_mode: none
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
   hosts: ["https://192.168.1.12:9200"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications

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

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "abcd1234"
```

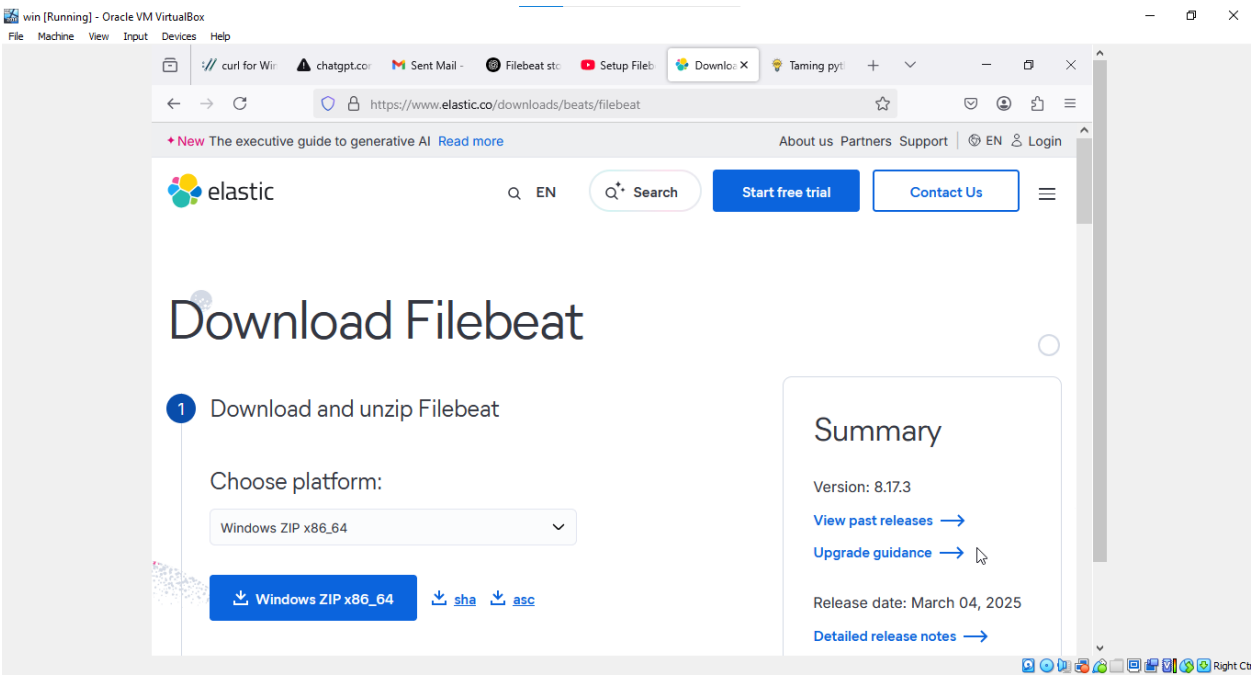
eshan@ct-2020-040: ~

```
eshan@ct-2020-040:~$ sudo systemctl status packetbeat
● packetbeat.service - Packetbeat analyzes network traffic and sends the data to Elasticsearch.
     Loaded: loaded (/usr/lib/systemd/system/packetbeat.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-20 18:56:42 UTC; 2min 18s ago
       Docs: https://www.elastic.co/beats/packetbeat
   Main PID: 2162 (packetbeat)
      Tasks: 9 (limit: 5023)
     Memory: 160.0M (peak: 160.4M)
        CPU: 802ms
     CGroup: /system.slice/packetbeat.service
             └─2162 /usr/share/packetbeat/bin/packetbeat --environment systemd -c /etc/packetbeat/packetbeat.yml --path.home /usr/share/packetbeat --path.config /etc/p

Mar 20 18:57:07 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:07.088Z","log.logger":"index-management","log.origin":{"function":"git
Mar 20 18:57:07 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:07.091Z","log.logger":"index-management.ilm","log.origin":{"function":
Mar 20 18:57:07 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:07.091Z","log.logger":"index-management","log.origin":{"function":"git
Mar 20 18:57:07 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:07.096Z","log.logger":"template_loader","log.origin":{"function":"gith
Mar 20 18:57:07 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:07.096Z","log.logger":"index-management","log.origin":{"function":"git
Mar 20 18:57:07 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:07.114Z","log.logger":"publisher_pipeline_output","log.origin":{"funct
Mar 20 18:57:13 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:13.034Z","log.logger":"monitoring","log.origin":{"function":"github.co
Mar 20 18:57:43 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:57:43.033Z","log.logger":"monitoring","log.origin":{"function":"github.co
Mar 20 18:58:13 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:58:13.033Z","log.logger":"monitoring","log.origin":{"function":"github.co
Mar 20 18:58:43 ct-2020-040 packetbeat[2162]: {"log.level":"info","@timestamp":"2025-03-20T18:58:43.033Z","log.logger":"monitoring","log.origin":{"function":"github.co
lines 1-21/21 (END)
```

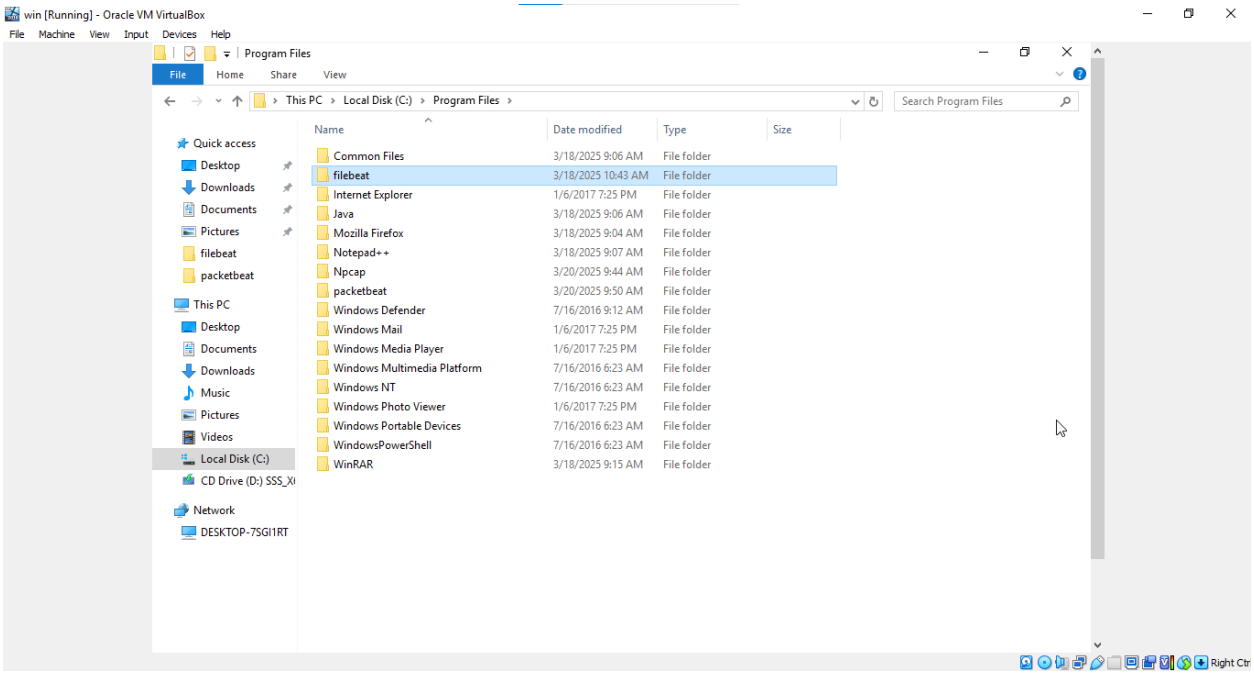

http://192.168.1.9:5601 - Search
Assignment 1.pdf
http://192.168.1.9:5601 - Search
Index Management - Elastic
Not secure
https://192.168.1.12:5601/app/management/data/index_management/data_streams
elastic
Find apps, content, and more.
Stack Management
Index Management
Data streams
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Data Set Quality
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Migrate
Alerts and Insights
Alerts
Data streams store time-series data across multiple indices and can be created from index templates. Learn more.
Search...
Include stats
View 1
Reload
Name
Health
Indices
Index mode
Data retention
Actions
.kibana-event-log-ds Managed Hidden green 1 Standard 90 days
.logs-deprecation.elasticsearch-default Managed Hidden green 1 Standard Disabled
filebeat-8.17.3 yellow 1 Standard Disabled
ilm-history-7 Managed Hidden green 1 Standard 90 days
packetbeat-8.17.3 yellow 1 Standard Disabled
Rows per page: 20
1
Console
Notebooks


http://192.168.1.9:5601 - Search
Assignment 1.pdf
http://192.168.1.9:5601 - Search
Dashboards - Elastic
Not secure
https://192.168.1.12:5601/app/dashboards#/list?_g=()
elastic
Find apps, content, and more.
Dashboards
Search...
Recently viewed
Tags
Created by
Create dashboard
All
Starred
Name, description, tags
Last updated
Actions
[Packetbeat] TLS Sessions ECS
TLS Sessions ECS
5 minutes ago
[Packetbeat] DNS Overview ECS
Overview of DNS request and response metrics.
5 minutes ago
[Filebeat Nginx] Access and error logs ECS
Dashboard for the Filebeat Nginx module
3 hours ago
[Filebeat Azure] Alerts Overview
This dashboard provides expanded alerts overview for Azure cloud
3 hours ago
[Filebeat Threat Intel] Overview
Top-level metrics of indicators and datasets ingested by the threat intel Filebeat module.
3 hours ago
threat intel

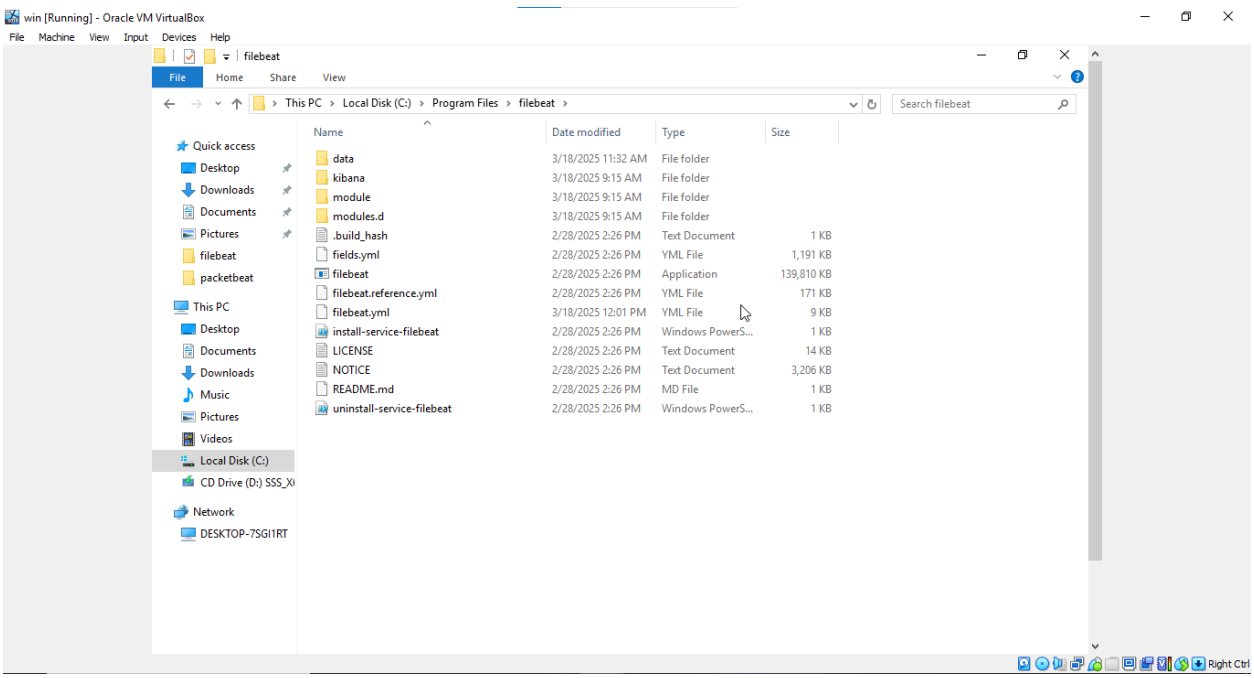
Windows Server

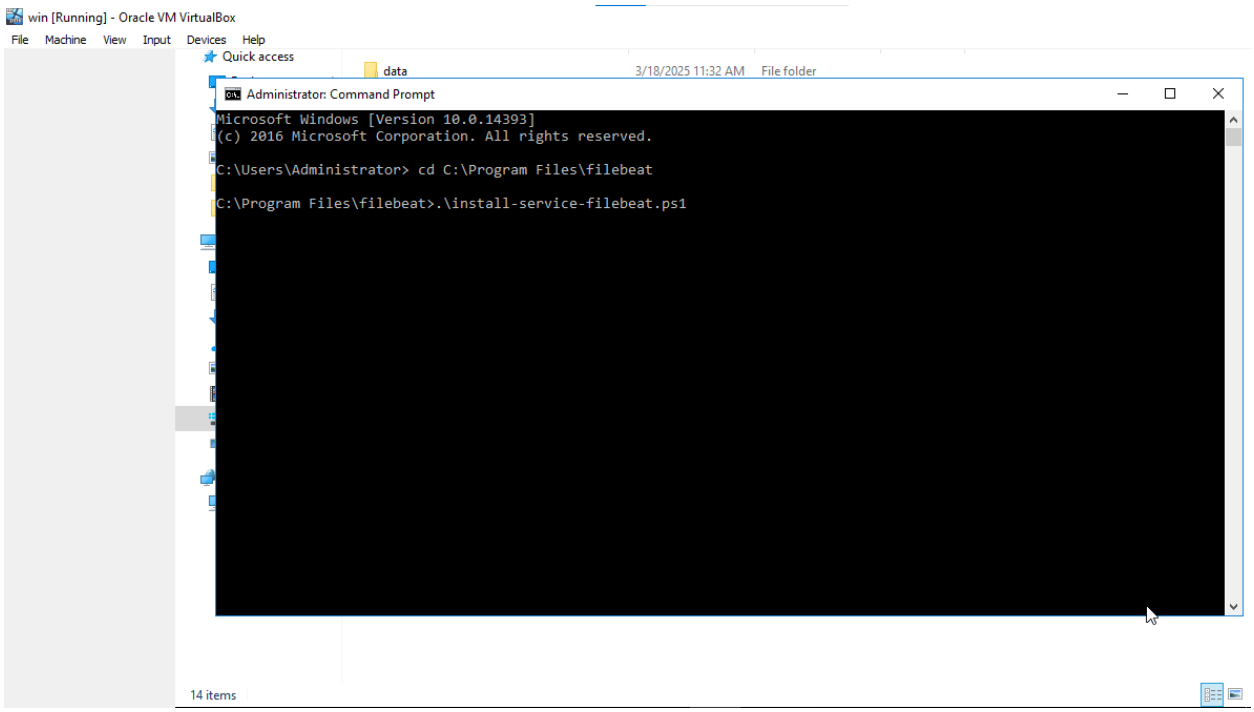


C→program files→filebeat



unzip a Filebeat





win [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

C:\Program Files\filebeat\filebeat.yml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

filebeat.yml | packetbeat.yml

```yaml

# ================================== General ===================================

# The name of the shipper that publishes the network data. It can be used to group
# all the transactions sent by a single shipper in the web interface.
#name:

# The tags of the shipper are included in their field with each
# transaction published.
#tags: ["service-X", "web-tier"]

# Optional fields that you can specify to add additional information to the
# output.
#fields:
#  env: staging

# ================================= Dashboards =================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here or by using the `setup` command.
setup.dashboards.enabled: true

# The URL from where to download the dashboard archive. By default, this URL
# has a value that is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:

# ================================== Kibana ====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
```

win [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

C:\Program Files\filebeat\filebeat.yml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

filebeat.yml | packetbeat.yml

```yaml

# ================================== Kibana ====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "https://192.168.1.12:5601"
  ssl.verification_mode: none

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

# ============================= Elastic Cloud ==================================

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

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

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

Right Ctrl

win [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

*C:\Program Files\filebeat\filebeat.yml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

filebeat.yml | packetbeat.yml

```yaml
# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://192.168.1.12:9200"]
  ssl:
    verification_mode: none
  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

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

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "abcd1234"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
   hosts: ["https://192.168.1.12:9200"]
  ssl:
    verification_mode: none

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

# ================================= Processors =================================
```

vin [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

Services (Local)

filebeat

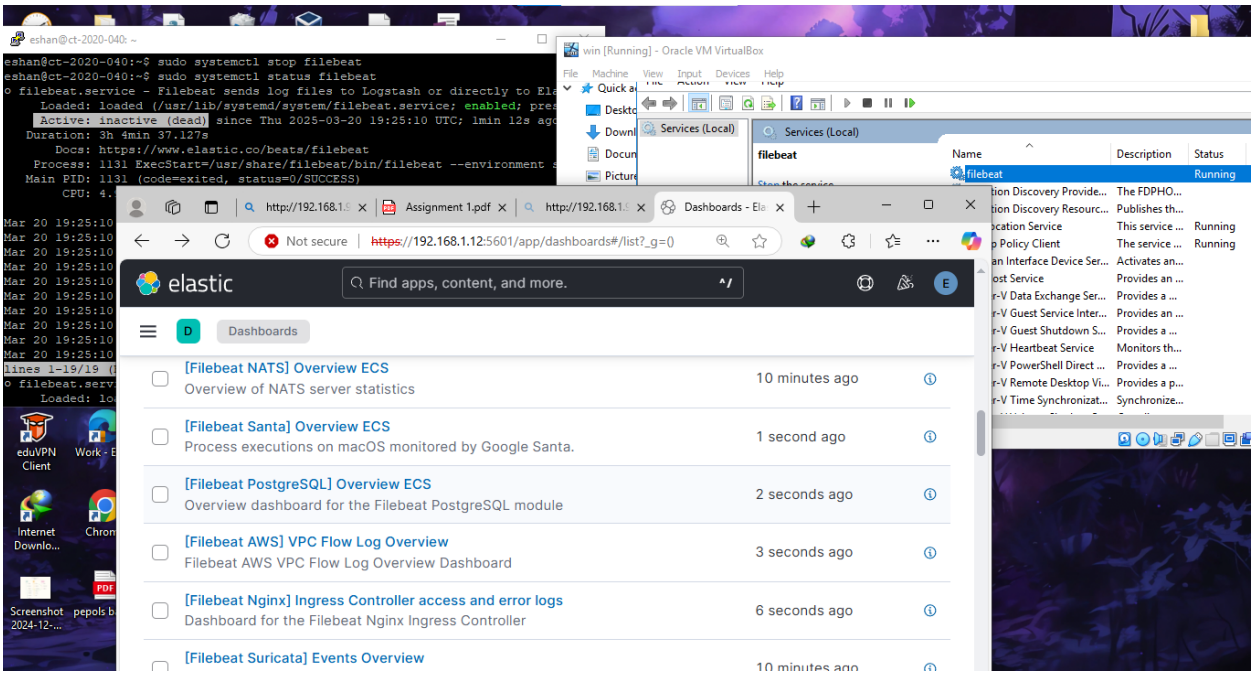
Stop the service
Restart the service

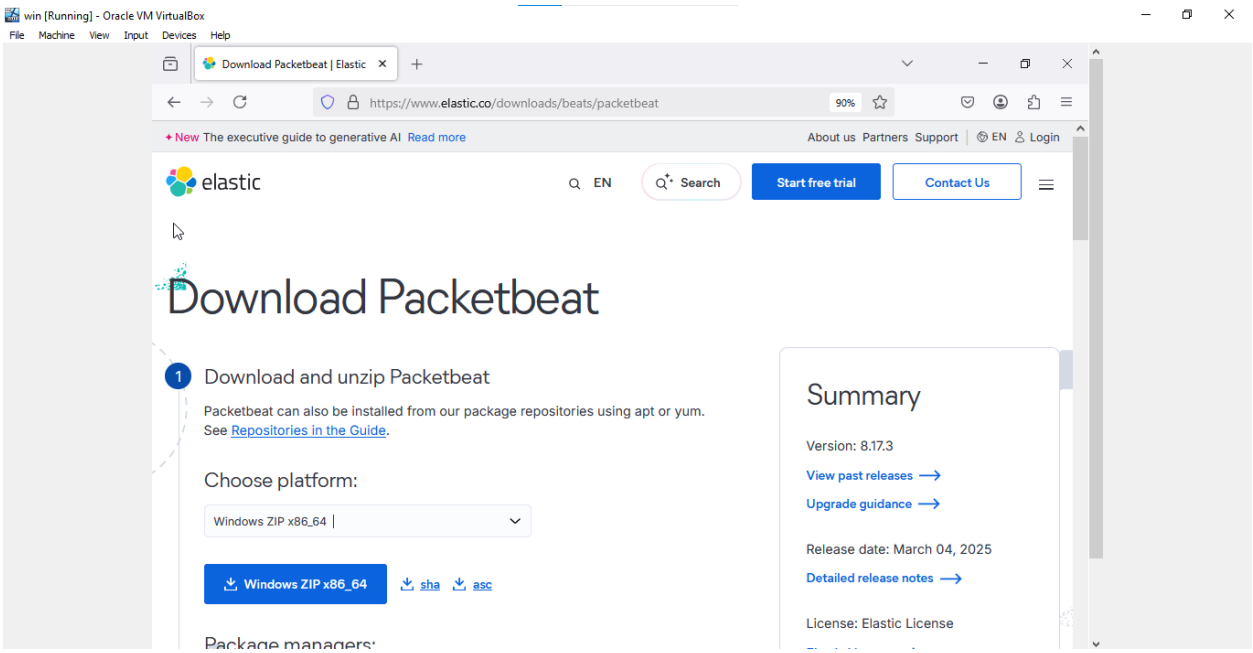
Name	Description	Status	Startup Type	Log On As
filebeat		Running	Automatic (D...	Local Syste...
Function Discovery Provide...	The FDPHO...		Manual	Local Service
Function Discovery Resourc...	Publishes th...		Manual	Local Service
Geolocation Service	This service ...	Running	Manual (Trig...	Local Syste...
Group Policy Client	The service ...	Running	Automatic (T...	Local Syste...
Human Interface Device Ser...	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange Ser...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service Inter...	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Guest Shutdown S...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Heartbeat Service	Monitors th...		Manual (Trig...	Local Syste...
Hyper-V PowerShell Direct ...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Remote Desktop Vi...	Provides a p...		Manual (Trig...	Local Syste...
Hyper-V Time Synchronizat...	Synchronize...		Manual (Trig...	Local Service
Hyper-V Volume Shadow C...	Coordinates...		Manual (Trig...	Local Syste...
IKE and AuthIP IPsec Keying...	The IKEEXT ...		Manual (Trig...	Local Syste...
Interactive Services Detection	Enables use...		Manual	Local Syste...
Internet Connection Sharin...	Provides ne...		Manual (Trig...	Local Syste...
IP Helper	Provides tu...	Running	Automatic	Local Syste...
IPsec Policy Agent	Internet Pro...		Manual (Trig...	Network S...
KDC Proxy Server service (K...	KDC Proxy S...		Manual	Network S...
KtmRm for Distributed Tran...	Coordinates...		Manual (Trig...	Network S...

Extended | Standard

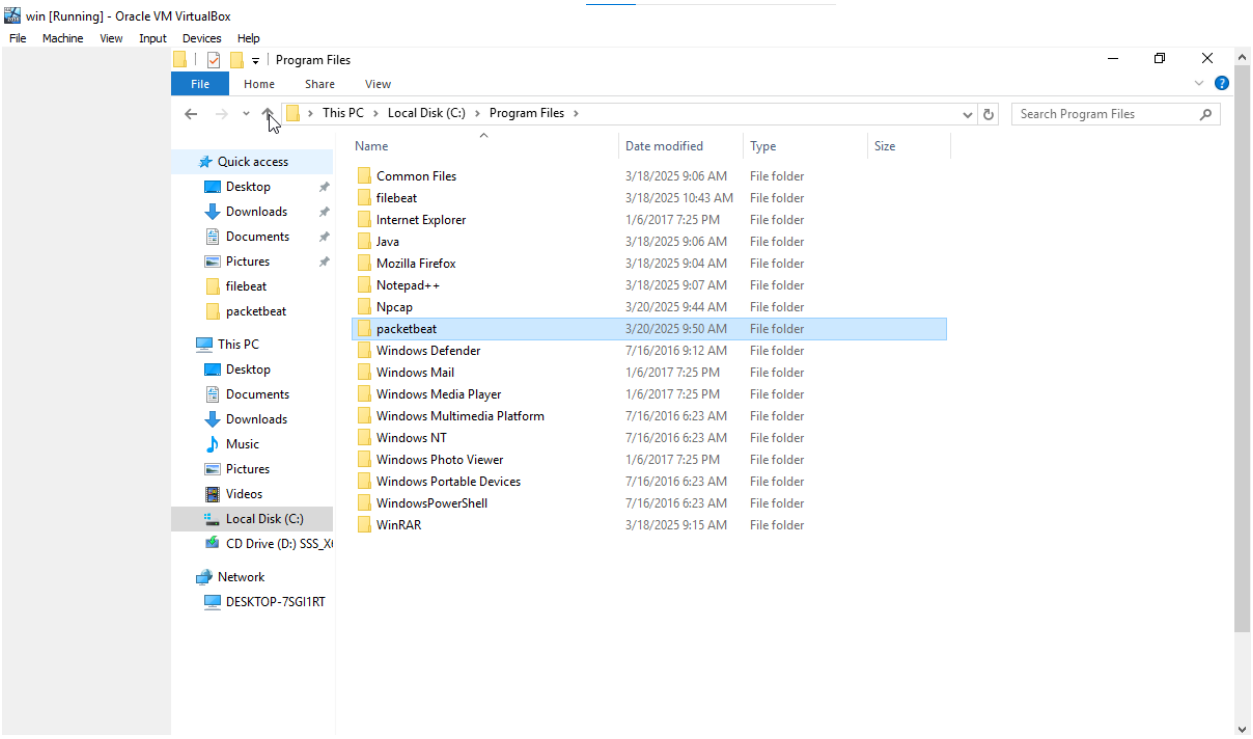
14 items 1 item selected 8.60 KB

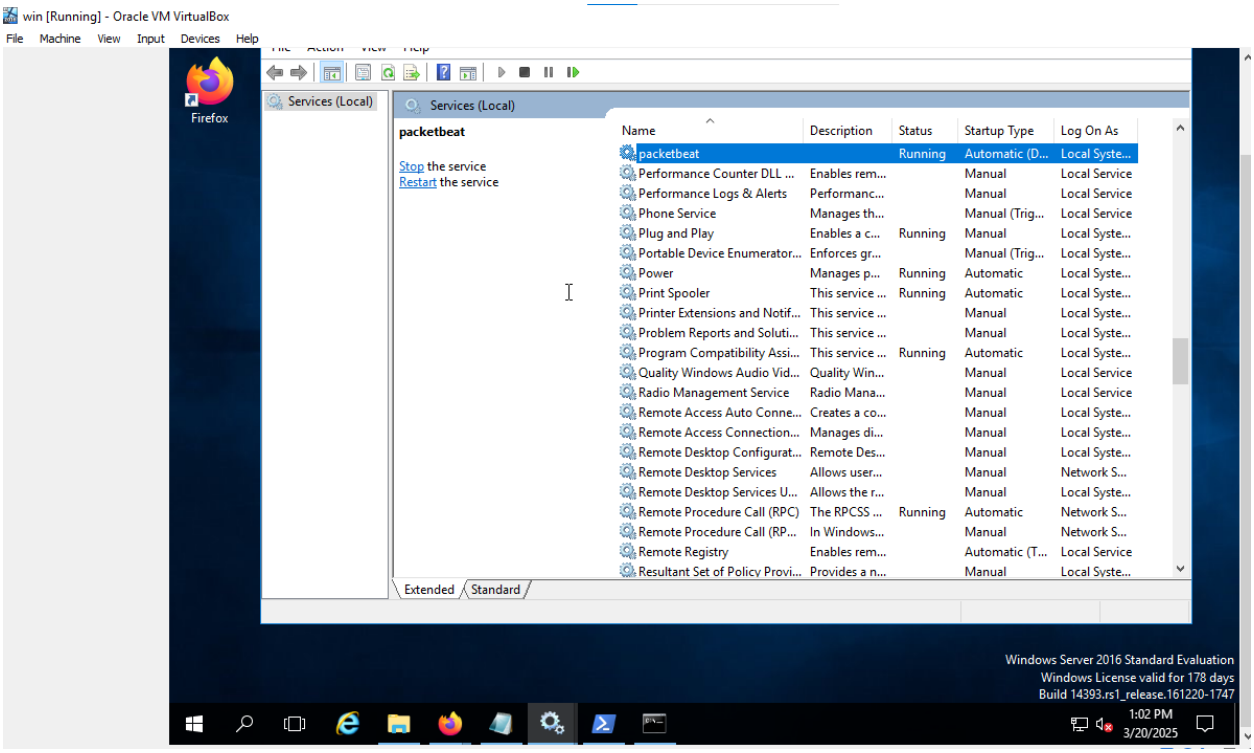
Ubuntu server is stopped, and only the **Windows Server Filebeat service** is running.

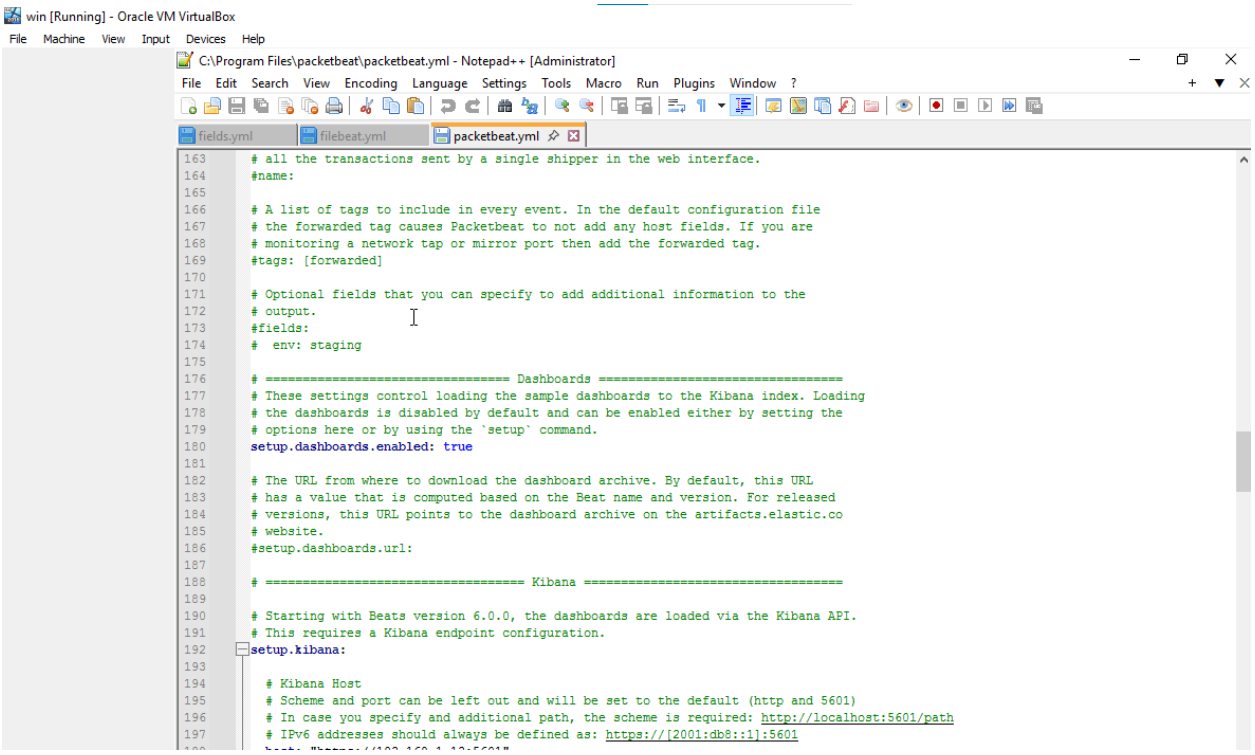




C→program files→packetbeat




win [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox
Services (Local)
packetbeat
Stop the service
Restart the service
Name Description Status Startup Type Log On As
packetbeat Running Automatic (D... Local Syste...
Performance Counter DLL ... Enables rem... Manual Local Service
Performance Logs & Alerts Performanc... Manual Local Service
Phone Service Manages th... Manual (Trig... Local Service
Plug and Play Enables a c... Running Manual Local Syste...
Portable Device Enumerator... Enforces gr... Manual (Trig... Local Syste...
Power Manages p... Running Automatic Local Syste...
Print Spooler This service ... Running Automatic Local Syste...
Printer Extensions and Notif... This service ... Manual Local Syste...
Problem Reports and Soluti... This service ... Manual Local Syste...
Program Compatibility Assi... This service ... Running Automatic Local Syste...
Quality Windows Audio Vid... Quality Win... Manual Local Service
Radio Management Service Radio Mana... Manual Local Service
Remote Access Auto Conne... Creates a co... Manual Local Syste...
Remote Access Connection... Manages di... Manual Local Syste...
Remote Desktop Configurat... Remote Des... Manual Local Syste...
Remote Desktop Services Allows user... Manual Network S...
Remote Desktop Services U... Allows the r... Manual Local Syste...
Remote Procedure Call (RPC) The RPCSS ... Running Automatic Network S...
Remote Procedure Call (RP... In Windows... Manual Network S...
Remote Registry Enables rem... Automatic (T... Local Service
Resultant Set of Policy Provi... Provides a n... Manual Local Syste...
Extended Standard
Windows Server 2016 Standard Evaluation
Windows License valid for 178 days
Build 14393.rs1_release.161220-1747
1:02 PM
3/20/2025


win [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
C:\Program Files\packetbeat\packetbeat.yml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
fields.yml
filebeat.yml
packetbeat.yml
all the transactions sent by a single shipper in the web interface.
#name:
A list of tags to include in every event. In the default configuration file
the forwarded tag causes Packetbeat to not add any host fields. If you are
monitoring a network tap or mirror port then add the forwarded tag.
#tags: [forwarded]
Optional fields that you can specify to add additional information to the
output.
#fields:
env: staging
================================= Dashboards =================================
These settings control loading the sample dashboards to the Kibana index. Loading
the dashboards is disabled by default and can be enabled either by setting the
options here or by using the `setup` command.
setup.dashboards.enabled: true
The URL from where to download the dashboard archive. By default, this URL
has a value that is computed based on the Beat name and version. For released
versions, this URL points to the dashboard archive on the artifacts.elastic.co
website.
#setup.dashboards.url:
================================= Kibana =================================
Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
This requires a Kibana endpoint configuration.
setup.kibana:
Kibana Host
Scheme and port can be left out and will be set to the default (http and 5601)
In case you specify and additional path, the scheme is required: http://localhost:5601/path
IPv6 addresses should always be defined as: https://[2001:db8::1]:5601

win [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

C:\Program Files\packetbeat\packetbeat.yml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

fields.yml | filebeat.yml | packetbeat.yml

```yaml
# ================================== Kibana ===================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "https://192.168.1.12:5601"
  ssl.verification_mode: none

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

# ============================== Elastic Cloud ================================

# These settings simplify using Packetbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

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

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

Right Ctrl

win [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

*C:\Program Files\packetbeat\packetbeat.yml - Notepad++ [Administrator]

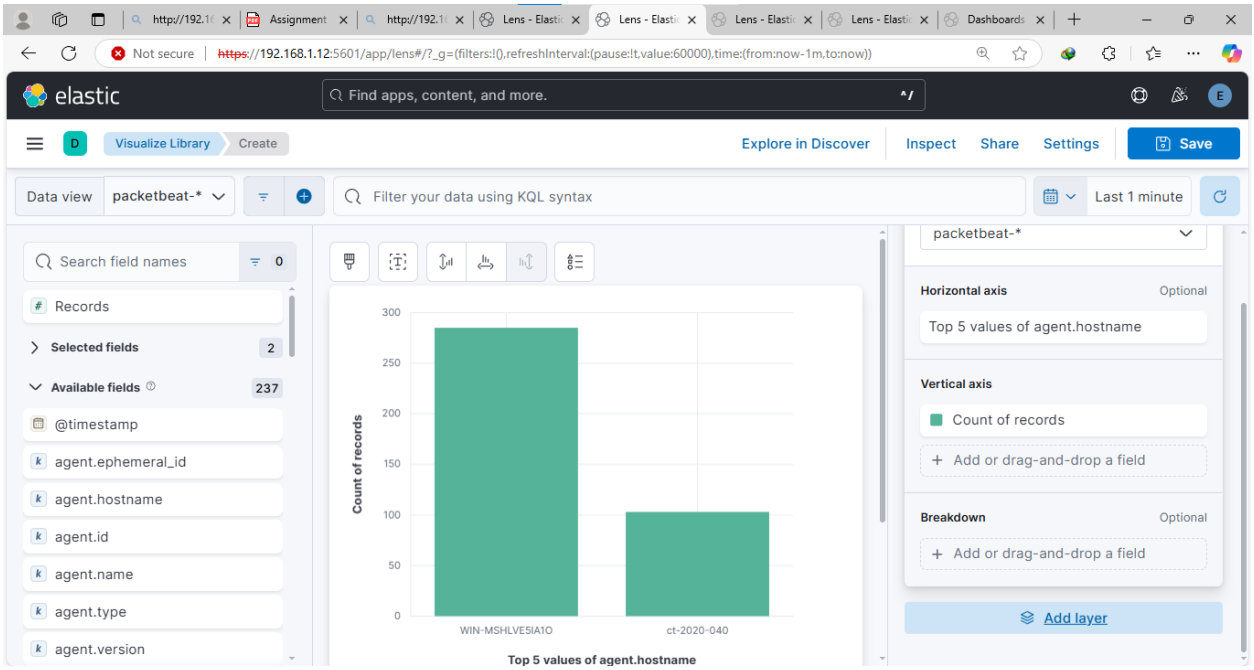
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

fields.yml | filebeat.yml | packetbeat.yml

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

# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://192.168.1.12:9200"]
  ssl:
    verification_mode: none

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

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "abcd1234"

  # Pipeline to route events to protocol pipelines.
  pipeline: "packetbeat-%{[agent.version]}-routing"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
hosts: ["https://192.168.1.12:9200"]
  ssl:
    verification_mode: none

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
```

Windows and Ubuntu machines, Packetbeat is capturing network activity from both systems. The two hostnames visible in the graph:

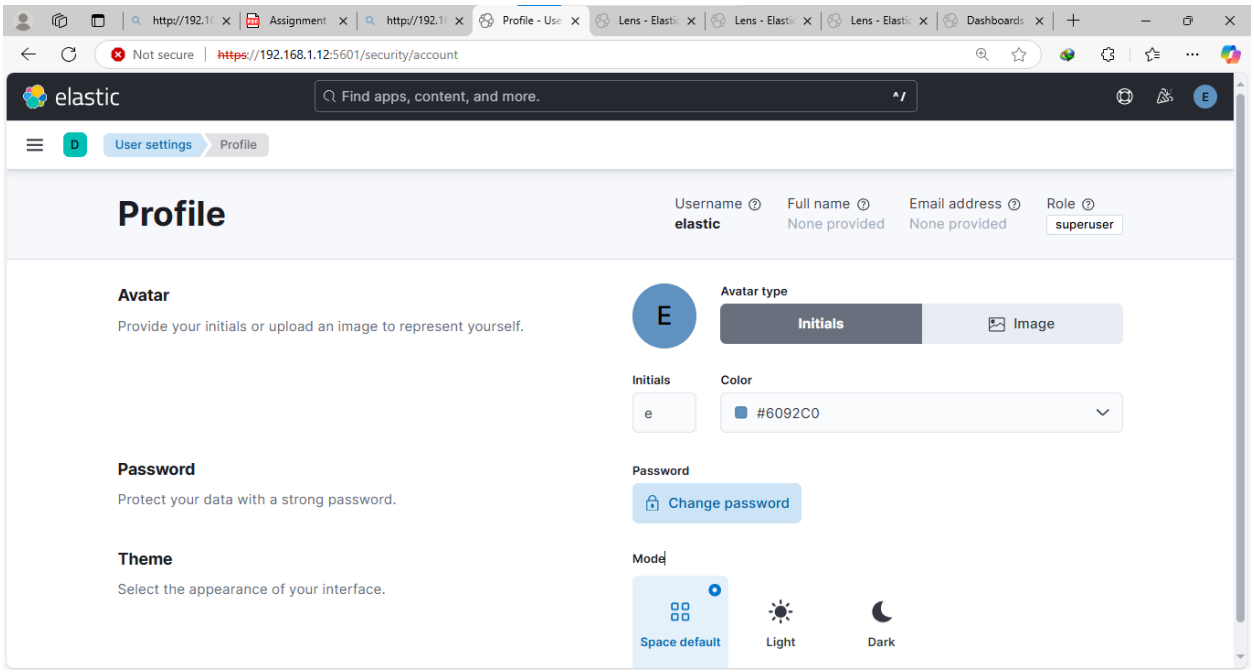
1. WIN-MSHLVE5IA10 (**Windows** machine)
2. ct-2020-040 (**Ubuntu** or Linux machine)



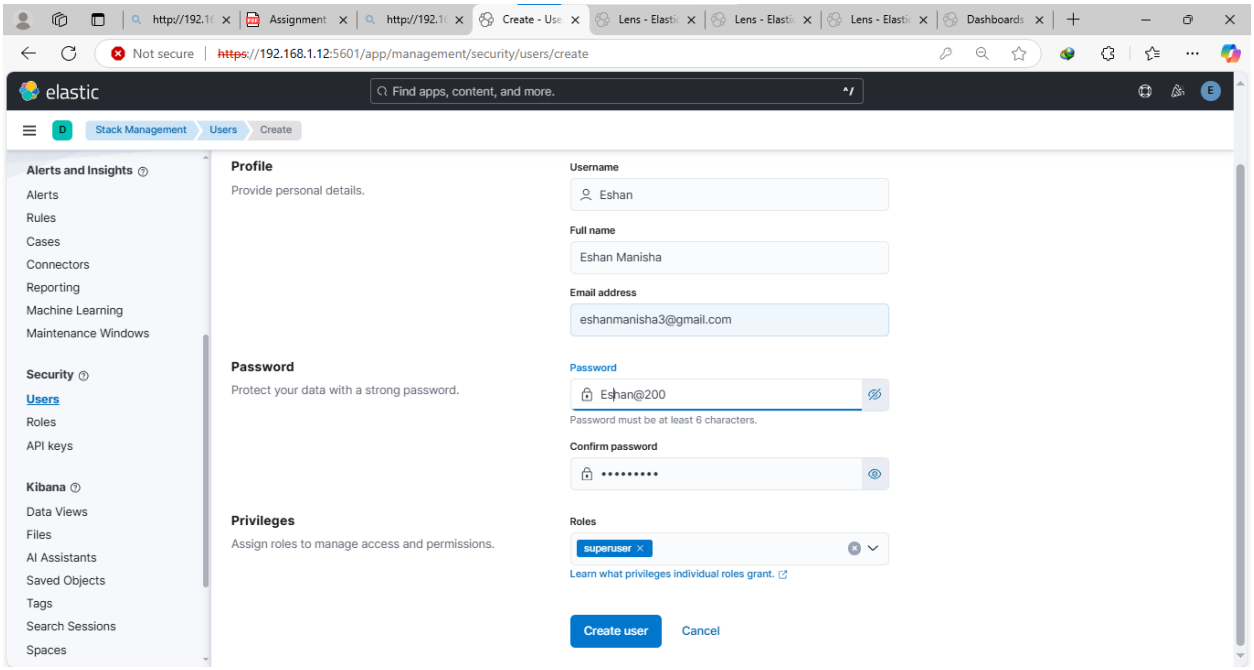
Task 3: User Management in ELK

1. Create default users for ELK access.

elastic user with superuser privileges in Kibana.



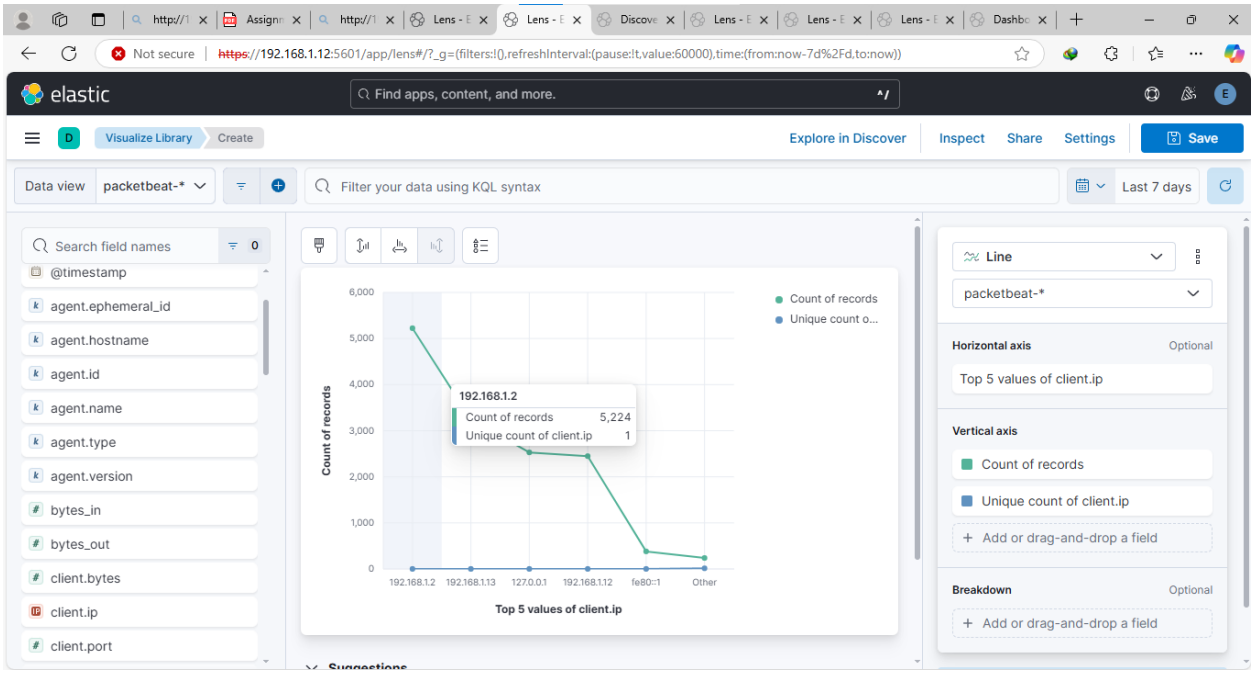
2. Add a custom user with ‘admin’ role and privileges, username should be your name.



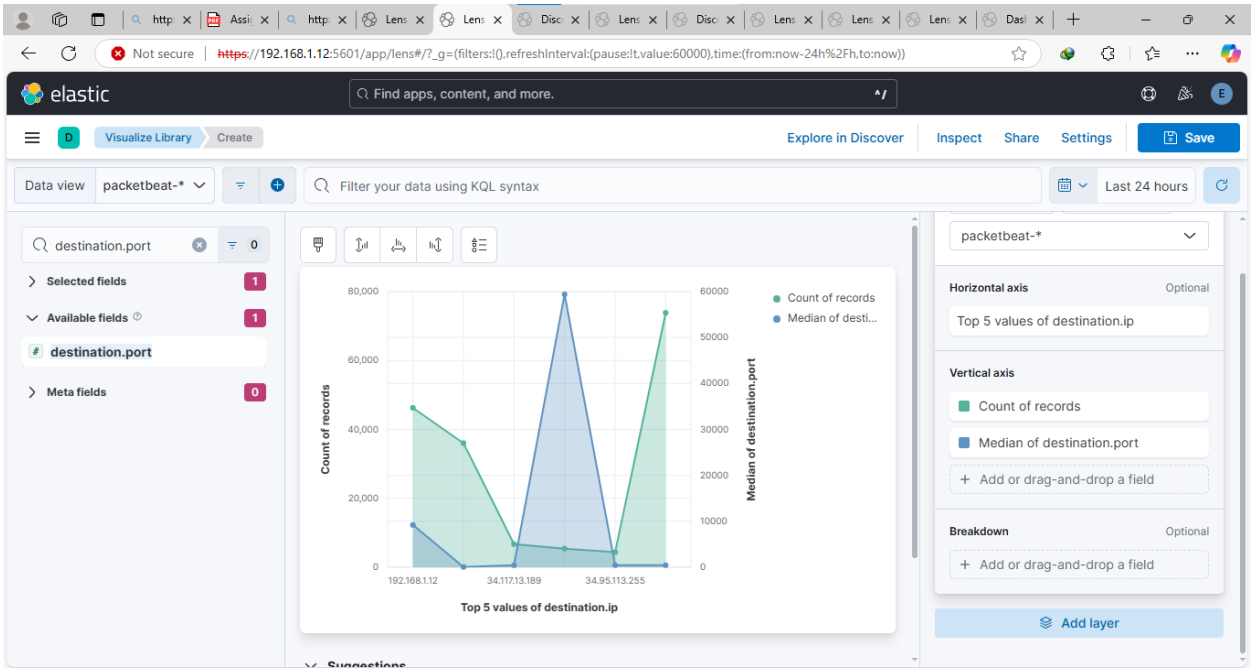
Provide insights into potential security threats observed from the logs.

Key Fields for Network Security Analysis

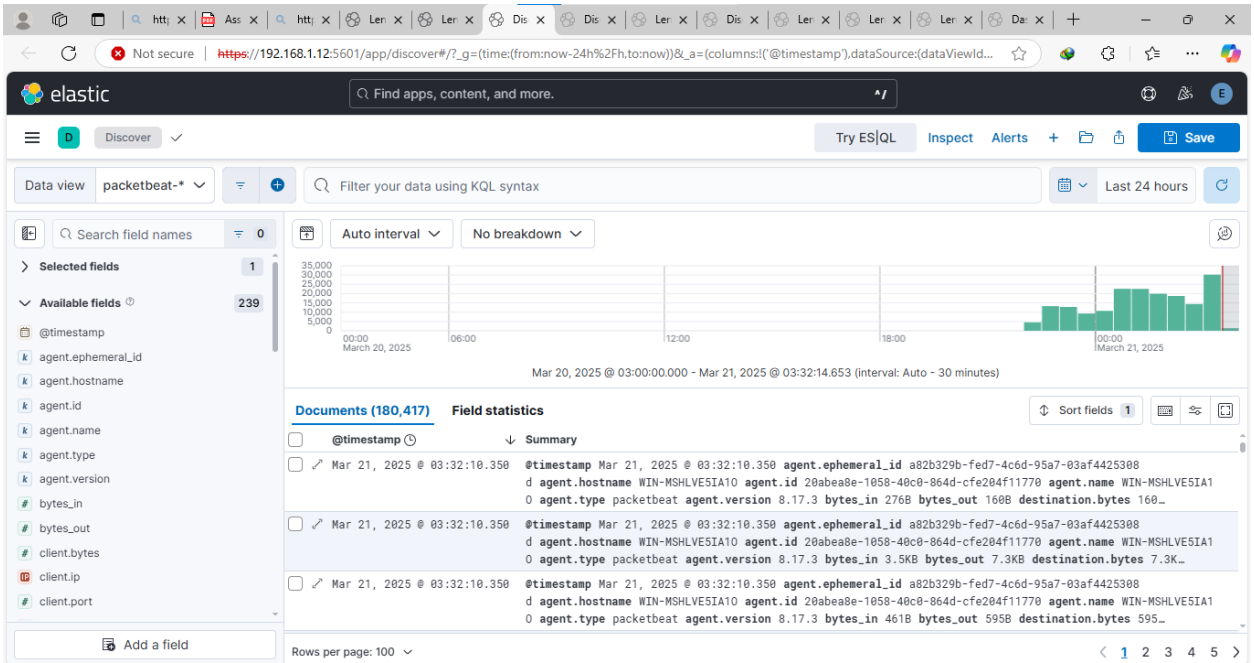
client.ip / client.port → Detect suspicious incoming requests.



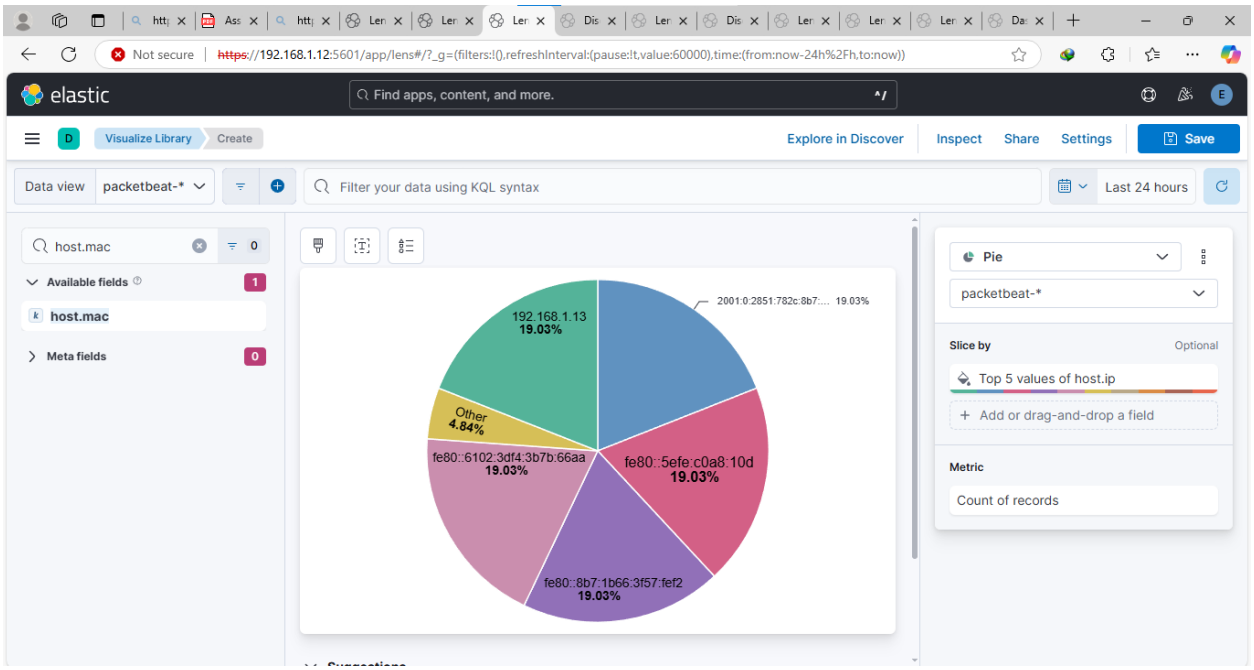
destination.ip / destination.port → Identify unauthorized connections.



@timestamp → Check for unusual activity spikes at specific times.



host.ip / host.mac → Look for unauthorized IPs or MAC addresses.



host.os.platform / host.os.version → Check if there are outdated or vulnerable OS versions.