

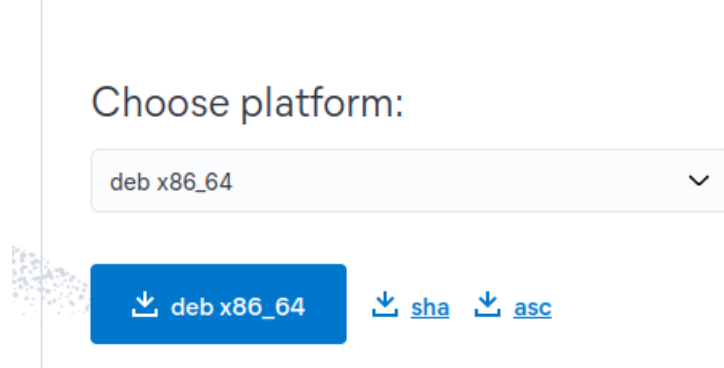
Task1

Installing elasticsearch , kibana , agents

First: Installing elasticsearch

1-

1 Download and unzip Elasticsearch



2- depackage elasticsearch and retrieve the default elastic user password

```
elasticsearch-8.14.3-amd64.deb  opensearch-2.15.0-linux-x64.deb
root@abdelrahman-1-2:/home/abdelrahman/Downloads# dpkg -i elasticsearch-8.14.3-amd64.deb
Selecting previously unselected package elasticsearch.
(Reading database ... 143343 files and directories currently installed.)
Preparing to unpack elasticsearch-8.14.3-amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.14.3) ...
Setting up elasticsearch (8.14.3) ...
----- Security autoconfiguration information -----

Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : xJm=*=02Pln5-U3QQN8s

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

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

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.
```

3- start the service

```

root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl start elasticsearch.service
Command 'systemctl' not found, did you mean:
  command 'systemctl' from deb systemd (253.5-1ubuntu6)
  command 'systemctl' from deb systemctl (1.4.4181-1.1)
Try: apt install <deb name>
root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl start elasticsearch.service
root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-07-23 14:53:29 EEST; 20s ago
     Docs: https://www.elastic.co
   Main PID: 5163 (java)
    Tasks: 87 (limit: 4880)
   Memory: 2.5G
      CPU: 1min 21.760s
   CGroup: /system.slice/elasticsearch.service
           └─5163 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=
           └─5221 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10
           └─5246 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jul 23 14:52:15 abdelrahman-1-2 systemd[1]: Starting elasticsearch.service - Elasticsearch...
Jul 23 14:52:29 abdelrahman-1-2 systemd-entrypoint[5163]: Jul 23, 2024 2:52:29 PM sun.util.locale.provider.LocaleProviderImpl$
Jul 23 14:52:29 abdelrahman-1-2 systemd-entrypoint[5163]: WARNING: COMPAT locale provider will be removed in a future release
Jul 23 14:53:29 abdelrahman-1-2 systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)

```

4- Change default configurations

```

GNU nano 7.2 elasticsearch.yml *
#
# 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: 127.0.0.1
#
# 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 -----

```

```

root@abdelrahman-1-2:/etc/elasticsearch# systemctl restart elasticsearch.service
root@abdelrahman-1-2:/etc/elasticsearch# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-07-23 14:59:00 EEST; 36s ago
     Docs: https://www.elastic.co
   Main PID: 5417 (java)
    Tasks: 80 (limit: 4880)
   Memory: 2.4G
      CPU: 59.187s
   CGroup: /system.slice/elasticsearch.service
           └─5417 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=
           └─5484 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10
           └─5507 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jul 23 14:58:29 abdelrahman-1-2 systemd[1]: Starting elasticsearch.service - Elasticsearch...
Jul 23 14:58:36 abdelrahman-1-2 systemd-entrypoint[5417]: Jul 23, 2024 2:58:36 PM sun.util.locale.provider.LocaleProviderImpl$
Jul 23 14:58:36 abdelrahman-1-2 systemd-entrypoint[5417]: WARNING: COMPAT locale provider will be removed in a future release
Jul 23 14:59:00 abdelrahman-1-2 systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)

```

Second : Installing kibana

1-

1 Download and unzip Kibana

DEB x86_64

↓ DEB x86_64

[↓](#) [sha](#)
[↓](#) [asc](#)

2- start the service

4- changing the default configuration and connect to elasticsearch

```
# ===== 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
# 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: ""

# The maximum payload size in bytes for incoming server requests.
```

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

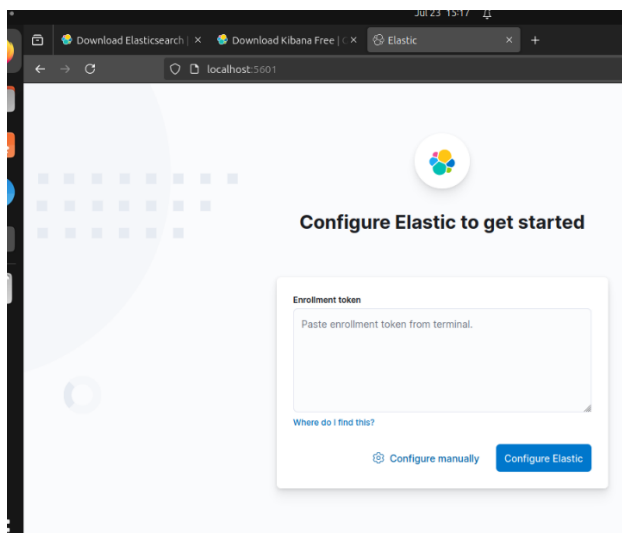
# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
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/
# 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
# the elasticsearch.requestTimeout setting.
elasticsearch.pingTimeout: 1500

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This
```

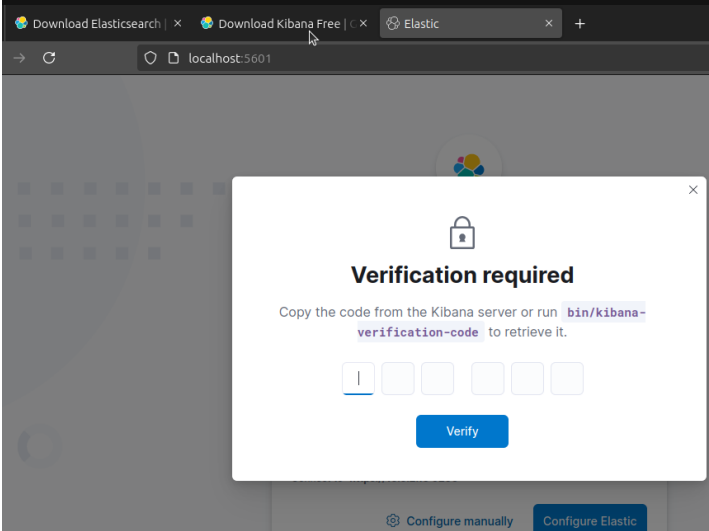
5- Generating an enrollment token to access kibana



The command for generating the token:

```
bash: cd: /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token: not a directory
root@abdelrahman-1-2:/etc/kibana# /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
eyJ2ZXIiOi0lI4JlE0LjAiLCZlZWl0SiMTAUMC4yLEJlOjkyMDAxSwizMdyIjoieTYJTOTQwMWNNkYjZhYXksNDYlZDZkZGFLMzJhVmVtZWVkME3MTlJyZU
3ZDNHMiThMzISMDFmNDQwYWZlTWmQlZSIntleSI6IElnRDS0c8NUFCN09BQLFScm9nWg0KNSjrLUkhukUpHrIdYWGhjeliTwcifQ==
root@abdelrahman-1-2:/etc/kibana#
```

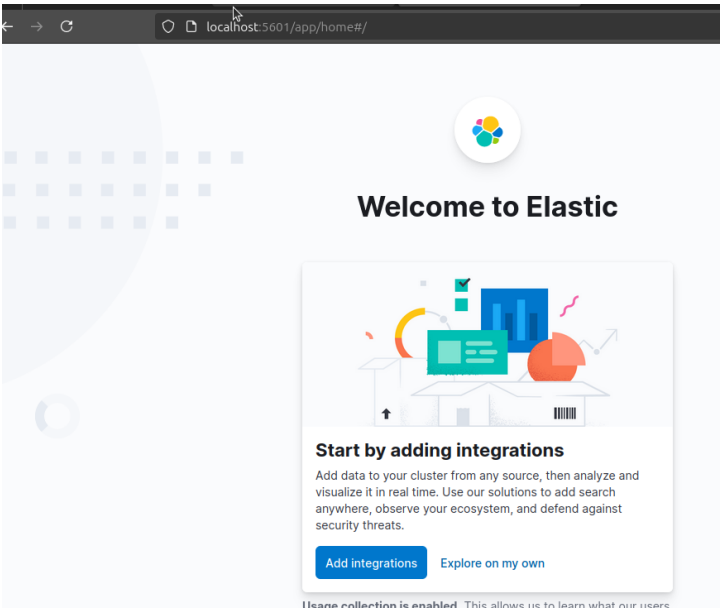
6- retrieving the verification code to log into kibana



Command to get verification code:

```
root@abdelrahman-1-2:/etc/kibana# /usr/share/kibana/bin/kibana-verification-code
Your verification code is: 343 987
root@abdelrahman-1-2:/etc/kibana#
```

Then kibana will work perfectly



Third: Installing stand-alone elastic agent

1-

Install standalone Elastic Agents

To run an Elastic Agent in standalone mode, install the agent and manually configure the agent locally on the system where it's installed. You are responsible for managing and upgrading the agents. This approach is recommended for advanced users only.

We recommend using [Fleet-managed Elastic Agents](#), when possible, because it makes the management and upgrade of your agents considerably easier.



Standalone agents are unable to upgrade to new integration package versions automatically. When you upgrade the integration in Kibana, you'll need to update the standalone policy manually.



You can install only a single Elastic Agent per host.

Elastic Agent can monitor the host where it's deployed, and it can collect and forward data from remote services and hardware where direct deployment is not possible.

To install and run Elastic Agent standalone:

2-

```
root@abdelrahman-1-2: /home/abdelrahman/Downloads
root@abdelrahman-1-2:/home/abdelrahman/Downloads# curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.14.3-and64.deb
root@abdelrahman-1-2:/home/abdelrahman/Downloads# sudo dpkg -i elastic-agent-8.14.3-and64.deb
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Done    0     0     0    0      0      0      0
100 322M 100 322M    0     0 153k      0  0:03:35  0:03:35 --:--:-- 1850k
Selecting previously unselected package elastic-agent.
(Reading database ... 239757 files and directories currently installed.)
Preparing to unpack elastic-agent-8.14.3-and64.deb ...
Unpacking elastic-agent (8.14.3) ...
Setting up elastic-agent (8.14.3) ...
create symlink /usr/share/elastic-agent/bin/elastic-agent to /var/lib/elastic-agent/data/elastic-agent-8.14.3-2df2c1/elastic-agent
root@abdelrahman-1-2:/home/abdelrahman/Downloads#
```

3- Changing configuration to send logs to elasticsearch

```
root@abdelrahman-1-2: /etc/elastic-agent
GNU nano 7.2 elastic-agent.yml
##### Agent Configuration Example #####

# This file is an example configuration file highlighting only the most common
# options. The elastic-agent.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.

#####
# Fleet configuration
#####

outputs:
  default:
    type: elasticsearch
    hosts: [127.0.0.1:9200]
    # api_key: "example-key"
    username: "elastic"
    password: "xJm*=02Pln5-U3QQN8s"
    preset: balanced

# Here you can configure your list of inputs. You can either configure all the inputs at
# once or create an "inputs.d" directory containing your input configurations.
# See https://www.elastic.co/guide/en/fleet/current/elastic-agent-configuration.html for
# more details.
inputs:
  # Collecting system metrics
  - type: system/metrics
    # Each input must have a unique ID.
    id: unique-system-metrics-input
    # Namespace name must conform to the naming conventions for Elasticsearch indices.
    # For index naming restrictions, see https://www.elastic.co/guide/en/elasticsearch/
```

4- starting the service

```

root@abdelrahman-1-2:/etc/elastic-agent# systemctl enable elastic-agent
Synchronizing state of elastic-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elastic-agent
Created symlink /etc/systemd/system/multi-user.target.wants/elastic-agent.service → /lib/systemd/system/elastic-agent.service.
root@abdelrahman-1-2:/etc/elastic-agent# systemctl start elastic-agent
root@abdelrahman-1-2:/etc/elastic-agent# systemctl status elastic-agent
● elastic-agent.service: Agent manages other beats based on configuration provided.
   Loaded: loaded (/lib/systemd/system/elastic-agent.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-07-23 16:27:30 EEST; 10s ago
     Docs: https://www.elastic.co/elastic-agent
   Main PID: 9136 (elastic-agent)
      Tasks: 39 (limit: 4880)
    Memory: 389.4M
       CPU: 3.556s
   CGroup: /system.slice/elastic-agent.service
           └─9136 /usr/share/elastic-agent/bin/elastic-agent --path.home /var/lib/elastic-agent --path.config /etc/e-
           └─9165 /var/lib/elastic-agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat metricbeat -E setup.il-
           └─9167 /var/lib/elastic-agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat filebeat -E setup.il-
           └─9169 /var/lib/elastic-agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat metricbeat -E setup.il-
           └─9170 /var/lib/elastic-agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat metricbeat -E setup.il-

Jul 23 16:27:36 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:36.189+0300","@
Jul 23 16:27:36 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:36.939+0300","@
Jul 23 16:27:36 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:36.939+0300","@
Jul 23 16:27:36 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:36.939+0300","@
Jul 23 16:27:37 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:37.503+0300","@
Jul 23 16:27:37 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:37.503+0300","@
Jul 23 16:27:37 abdelrahman-1-2 elastic-agent[9136]: {"log_level":"info","@timestamp":"2024-07-23T16:27:37.503+0300","@

```

The screenshot shows the Elastic Stack Management UI. The 'Index Management' section is active, with the 'Data Streams' tab selected. The table lists the following data streams:

Name	Health	Indices	Data retention	Actions
kibana-event-log-ds	green	1	90 days	[Icon]
logs-deprecation.elasticsearch-default	green	1	Disabled	[Icon]
ilm-history-7	green	1	90 days	[Icon]

Fourth : installing stand-alone FIM and auditd on linux machine

1- Installing auditd service

```

root@abdelrahman-1-2:/home/abdelrahman/Downloads# apt install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 8 not upgraded.
1 not fully installed or removed.
Need to get 275 kB of archives.
After this operation, 885 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://eg.archive.ubuntu.com/ubuntu mantic/main amd64 libauparse0 amd64 1:3.1.1-1
Get:2 http://eg.archive.ubuntu.com/ubuntu mantic/main amd64 auditd amd64 1:3.1.1-1 [217
Fetched 275 kB in 1s (338 kB/s)
Selecting previously unselected package libauparse0:amd64.
(Reading database ... 240199 files and directories currently installed.)
Preparing to unpack .../libauparse0_1%3a3.1.1-1_amd64.deb ...
Unpacking libauparse0:amd64 (1:3.1.1-1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a3.1.1-1_amd64.deb ...
Unpacking auditd (1:3.1.1-1) ...
Setting up opensearch (2.15.0) ...
Running OpenSearch Post-Installation Script

```


2- Installing auditd from integrations in kibana

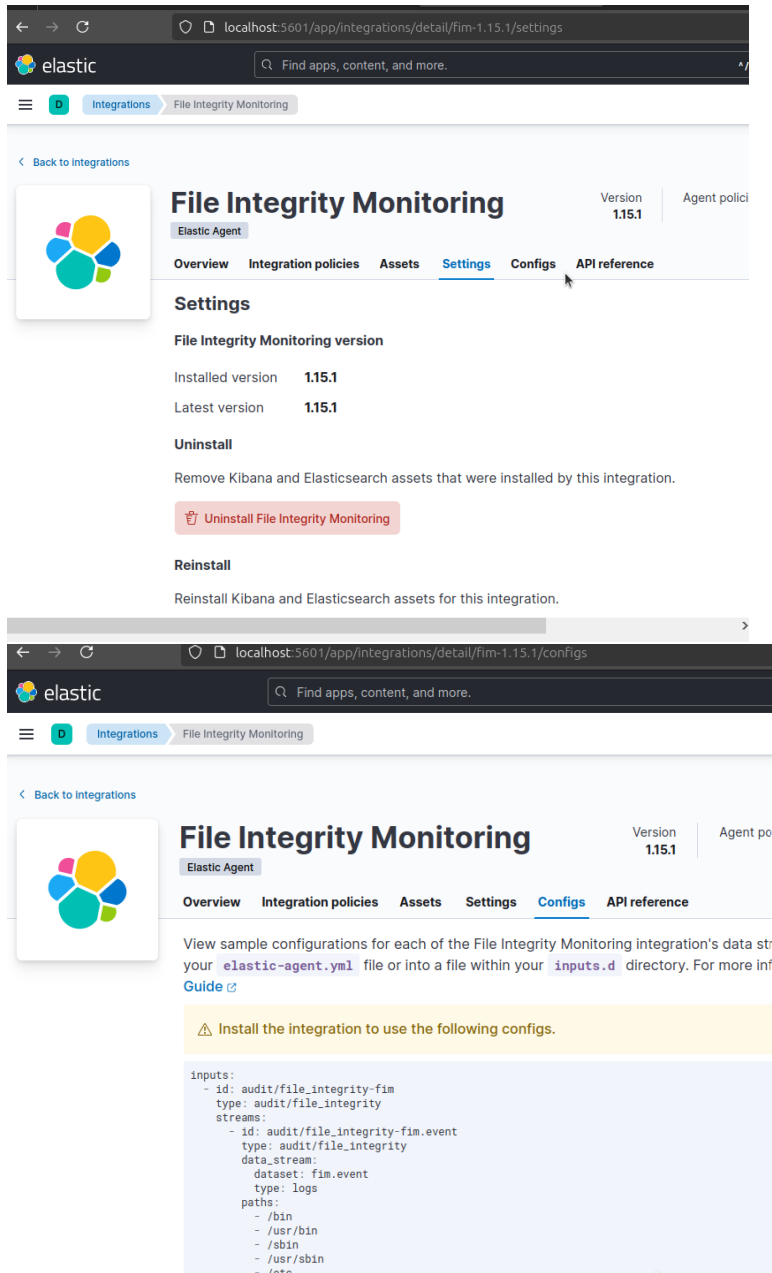
The screenshot shows the Kibana interface for the Auditd Logs integration. The browser address bar indicates the URL: `localhost:5601/app/integrations/detail/auditd-3.19.2/overview`. The page title is "Auditd Logs" under the "Elastic Agent" category. The "Overview" tab is selected, showing a description: "The Auditd Logs integration collects and parses logs from the audit daemon (auditd)." It also lists compatibility: "The integration was tested with logs from auditd on OSes like CentOS 6 and CentOS ; This integration is not available for Windows." An example log entry is shown: `{ "timestamp": "2016-01-03T00:37:51.394Z", ... }`. The "Settings" tab is also visible, showing the "Auditd Logs version" as 3.19.2 and an "Uninstall Auditd Logs" button.

3- Copying auditd configurations into the elastic-agent.yml

The screenshot shows the "Configs" tab for the Auditd Logs integration. It provides sample configurations for the integration's data streams. The configuration is as follows:

```
inputs:
- id: logfile-auditd
  type: logfile
  streams:
  - id: logfile-auditd.log
    data_stream:
      dataset: auditd.log
      type: logs
    paths:
    - /var/log/audit/audit.log*
  tags:
  - auditd-log
  exclude_files:
  - \.gz$
```

4- Installing FIM from kibana integrations and copying its configurations into elastic-agent.yml file



localhost:5601/app/integrations/detail/fim-1.15.1/settings

elastic Find apps, content, and more.

Integrations File Integrity Monitoring

Back to integrations

File Integrity Monitoring

Elastic Agent Version 1.15.1 Agent policy

Overview Integration policies Assets Settings Configs API reference

Settings

File Integrity Monitoring version

Installed version 1.15.1

Latest version 1.15.1

Uninstall

Remove Kibana and Elasticsearch assets that were installed by this integration.

Uninstall File Integrity Monitoring

Reinstall

Reinstall Kibana and Elasticsearch assets for this integration.

localhost:5601/app/integrations/detail/fim-1.15.1/configs

elastic Find apps, content, and more.

Integrations File Integrity Monitoring

Back to integrations

File Integrity Monitoring

Elastic Agent Version 1.15.1 Agent policy

Overview Integration policies Assets Settings Configs API reference

View sample configurations for each of the File Integrity Monitoring integration's data streams. Add the configuration to your `elastic-agent.yml` file or into a file within your `inputs.d` directory. For more information, see the [FIM Guide](#).

Install the integration to use the following configs.

```
inputs:
- id: audit/file_integrity-fim
  type: audit/file_integrity
  streams:
  - id: audit/file_integrity-fim.event
    type: audit/file_integrity
    data_stream:
      dataset: fim.event
      type: logs
    paths:
    - /bin
    - /usr/bin
    - /sbin
    - /usr/sbin
    - /etc
```

5- Audid and FIM:

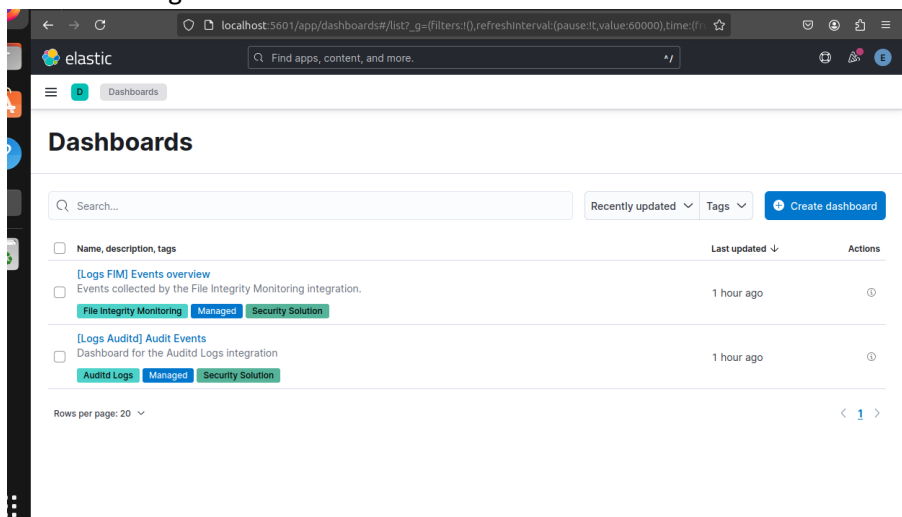
```

root@abdelrahman-1-z:/home/abdelrahman/Downloads
GNU nano 7.2 /etc/elastic-agent/elastic-agent.yml *
max_file_size: 100 MiB
scan_rate_per_sec: 50 MiB
exclude_files:
  - '(?i)\.sw[nop]$'
  - '$'
  - /\.git($|/)/
  - \.tmp$
  - \.log$
  - \.db$
include_files: null
keep_null: false
tags:
  - fin-event
processors:
  - add_host_metadata:
      replace_fields: true

inputs:
  - id: logfile-auditd
    type: logfile
    streams:
      - id: logfile-auditd.log
        data_stream:
          dataset: auditd.log
          type: logs
        paths:
          - /var/log/audit/audit.log

```

6- Review the logs in kibana



7- Install windows log agent from kibana integrations:



8-

```

PS D:\Security courses\security meter intern\summer\t1\windows> # PowerShell 5.0+
PS D:\Security courses\security meter intern\summer\t1\windows> wget https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.14.3-windows-x86_64.zip -OutFile elastic-agent-8.14.3-windows-x86_64.zip
PS D:\Security courses\security meter intern\summer\t1\windows> Expand-Archive .\elastic-agent-8.14.3-windows-x86_64.zip

```

9- Installing the archived agent with administrator privs

```

Administrator: Windows PowerShell
PS D:\Security courses\security meter intern\summer\t1\windows\elastic-agent-8.14.3-windows-x86_64> .\elastic-agent.exe install
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
Do you want to enroll this Agent into Fleet? [Y/n]:n
[== ] Service Started [19s] Elastic Agent successfully installed, starting enrollment.
[== ] Done [19s]
Elastic Agent has been successfully installed.
PS D:\Security courses\security meter intern\summer\t1\windows\elastic-agent-8.14.3-windows-x86_64>

```

10- Modifying the elastic-agent.yml to send logs to elasticsearch

```

elastic-agent.yml X
D: > Security courses > security meter intern > summer > t1 > windows > e
1  ##### Agent Configuration Example
2
3  # This file is an example configuration file highlighting
4  # options. The elastic-agent.reference.yml file for
5  # supported options with more comments. You can use
6
7  #####
8  # Fleet configuration
9  #####
10 outputs:
11   default:
12     type: elasticsearch
13     hosts: [192.168.1.9:9200]
14     #api_key: "example-key"
15     username: "elastic"
16     password: "u=hNzUobNkVUtM2j5Qv5"
17     preset: balanced
18
19
20

```

11- Adding the windows logs configuration from the kibana

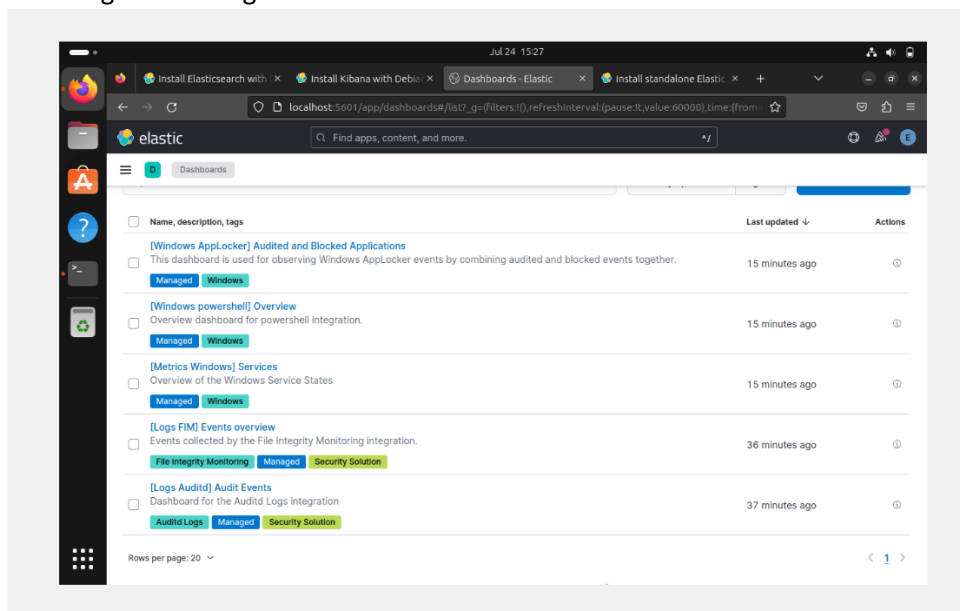
```
Restricted Mode is intended for safe code browsing. Trust this window to enabl... Manage Learn More >

! elastic-agent.yml x

ity meter intern > summer > t1 > windows > elastic-agent-8.14.3-windows-x86_64 > ! elastic-age

308   inputs:
500     - id: httpjson-windows
502       streams:
803         - id: httpjson-windows.forwarded
838         processors:
850           - json.result._cu
851             - json.result._indextime
852             - json.result._raw
853             - json.result._time
854             - json.result.host
855             - json.result.source
856             target_field: '@metadata._id'
857         - drop_fields:
858             fields: message
859         - rename:
860             fields:
861               - from: json.result._raw
862                 to: event.original
863               - from: json.result.host
864                 to: host.name
865               - from: json.result.source
866                 to: event.provider
867             ignore_missing: true
868             fail_on_error: false
869         - drop_fields:
870             fields: json
871         - decode_xml_wineventlog:
```

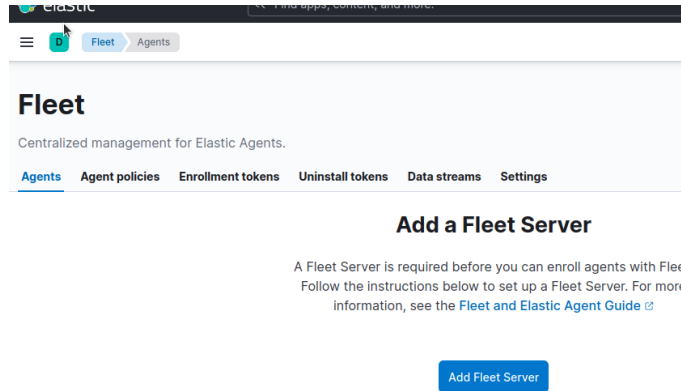
12- Checking for sent logs in kibana



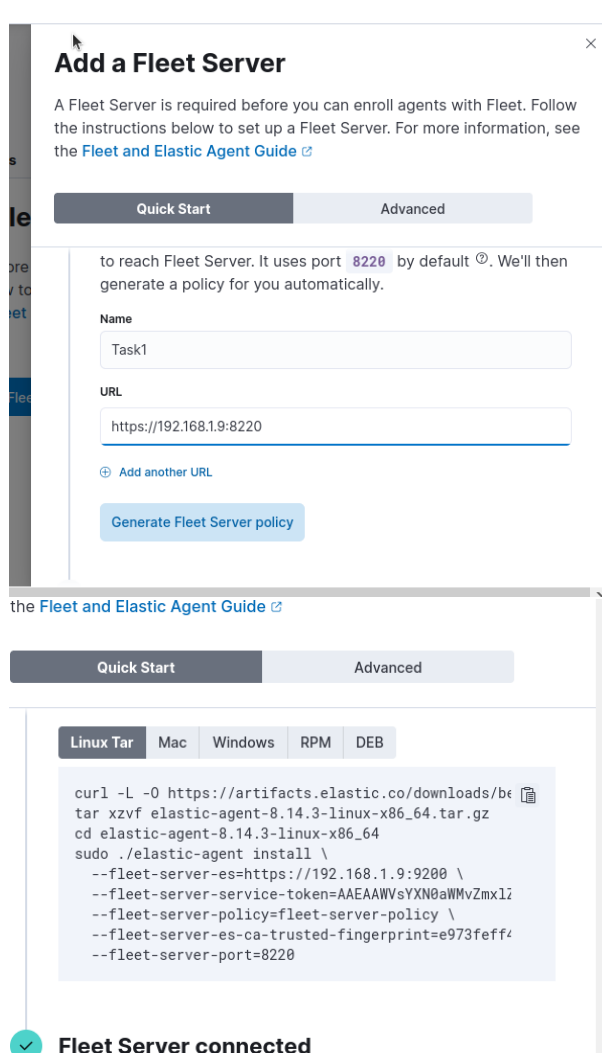
Now we know how to setup a stand-alone agent , but using the best practice we will do it using fleet-server

Fifth: Installing fleet server and FIM agent with it

1- From kibana select fleet



2- Add fleet server



3- Install fleet server

```
root@abdelrahman-1:2:/home/abdelrahman/Downloads# curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent
/elastic-agent-8.14.3-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.14.3-linux-x86_64.tar.gz
cd elastic-agent-8.14.3-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://192.168.1.9:9200 \
  --fleet-server-service-token=AAEAMVSYXN8aMvZmxlZXQtc2VydMvYl3Rva2VulTE3MjE4MzEwMjM4OTk6VmxvYVUNCaipSVVcySVVzNmZzVkhP
UQ \
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=e973feff46e1a2e02d1579009b679a54a4173de09e3c1cd09297df56a2a260d2 \
  --fleet-server-port=8228
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Done   0         0      0     2197k    0      0:02:32  0:02:32  --:--:-- 2171k
elastic-agent-8.14.3-linux-x86_64/manifest.yaml
elastic-agent-8.14.3-linux-x86_64/data/elastic-agent-2df2c1/elastic-agent
elastic-agent-8.14.3-linux-x86_64/LICENSE.txt
elastic-agent-8.14.3-linux-x86_64/elastic-agent.yml
elastic-agent-8.14.3-linux-x86_64/build_hash.txt
elastic-agent-8.14.3-linux-x86_64/NOTICE.txt
elastic-agent-8.14.3-linux-x86_64/elastic-agent.reference.yml
elastic-agent-8.14.3-linux-x86_64/otel.yml
elastic-agent-8.14.3-linux-x86_64/data/elastic-agent-2df2c1/otelcol
elastic-agent-8.14.3-linux-x86_64/README.md
elastic-agent-8.14.3-linux-x86_64/data/elastic-agent-2df2c1/components/
```



Fleet Server connected

You can now continue enrolling agents with Fleet.

[Continue enrolling Elastic Agent](#)

4- Add fleet policy

Name	Description	La
task1 policy rev. 1		Ju
Fleet Server Policy rev. 1	Fleet Server policy generated by Kibana	Ju
Agent policy 1 rev. 3		Ju

5-Adding agents to fleet using FIM

{note : I stood with the default configurations}

Add Fleet Server integration

Fleet Server integration added

To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack.

[Add Elastic Agent later](#) [Add Elastic Agent to your hosts](#)

Integrations > File Integrity Monitoring

File Integrity Monitoring

Version 1.15.1 Agent policies 0 [Add File Integrity Monitoring](#)

[Overview](#) [Integration policies](#) [Assets](#) [Settings](#) [Configs](#) [API reference](#)

File Integrity Monitoring Integration

This integration sends events when a file is changed (created, updated, or deleted) on disk. The events contain file metadata and hashes.

The integration is implemented for Linux, macOS (Darwin), and Windows.

Requirements

Permissions root privileges

Screenshots << 1 of 1 >>

How it works

This integration uses features of the operating system to monitor file changes in realtime.

elastic [localhost:5601/app/fleet/agents](#)

[Fleet](#) [Agents](#) [Send feedback](#)

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

[Set up encryption key](#)

An encryption key will make your environment more secure. Click [here](#) to learn how to set up an encryption key.

[Dismiss](#)

[Agent activity](#) [Add Fleet Server](#) [Add agent](#)

Filter your data using KQL syntax

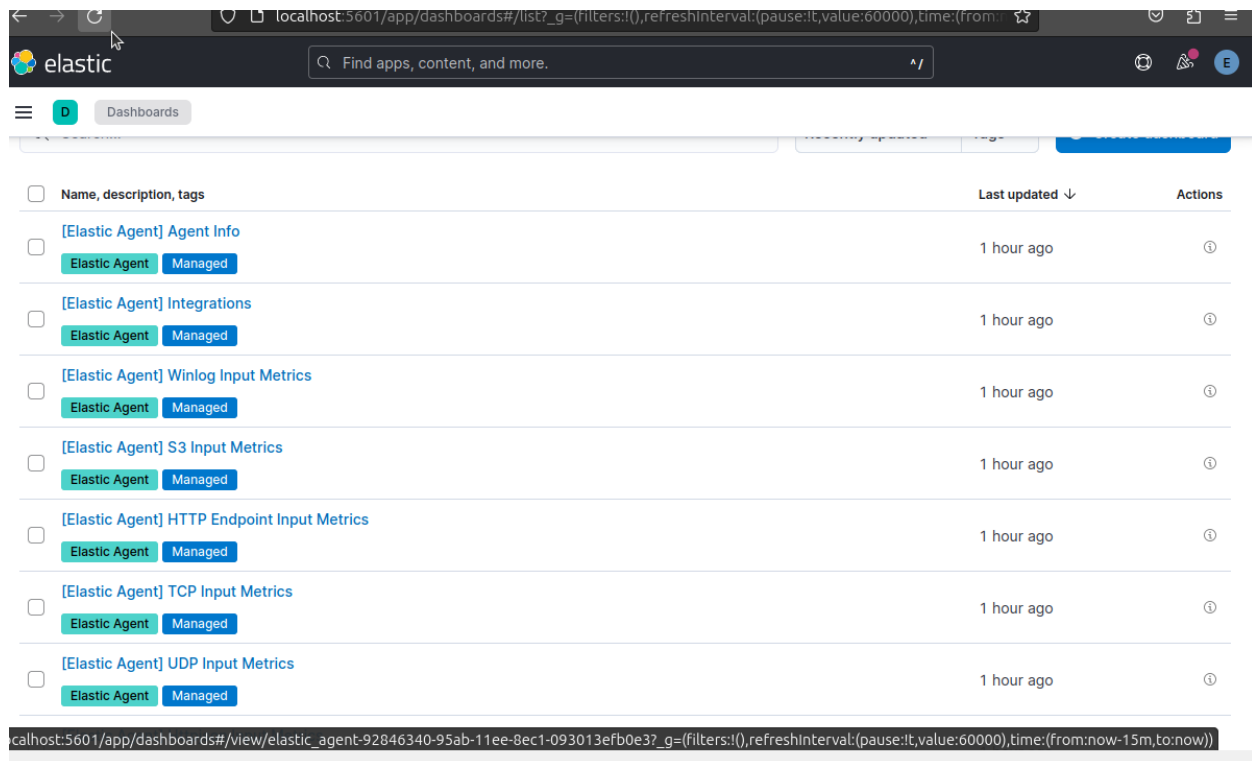
Status [Tags](#) [Agent policy](#) [Upgrade available](#)

Showing 1 agent [Clear filters](#)

Healthy 1 Unhealthy 0 Updating 0 Offline 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	abdelrahman-1-2	Fleet Server Policy rev. 1	3.26 %	231 MB	8 seconds ago	8.14.3	...

Finally all the agents in the dashboard:



Resources:

- 1- <https://www.elastic.co/guide/en/fleet/current/install-fleet-managed-elastic-agent.html>
- 2- <https://www.elastic.co/guide/en/fleet/current/install-standalone-elastic-agent.html>
- 3- <https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html>
- 4- <https://www.elastic.co/guide/en/kibana/current/install.html>

Problems I faced:

- 1- All my services gone died , due changing in the IP address of the machine , so I reinstalled it ,but this time I configured the machine to have a static IP
- 2- The windows machine could not reach the elasticsearch , so I troubleshooted the network configuration until the problem is solved

