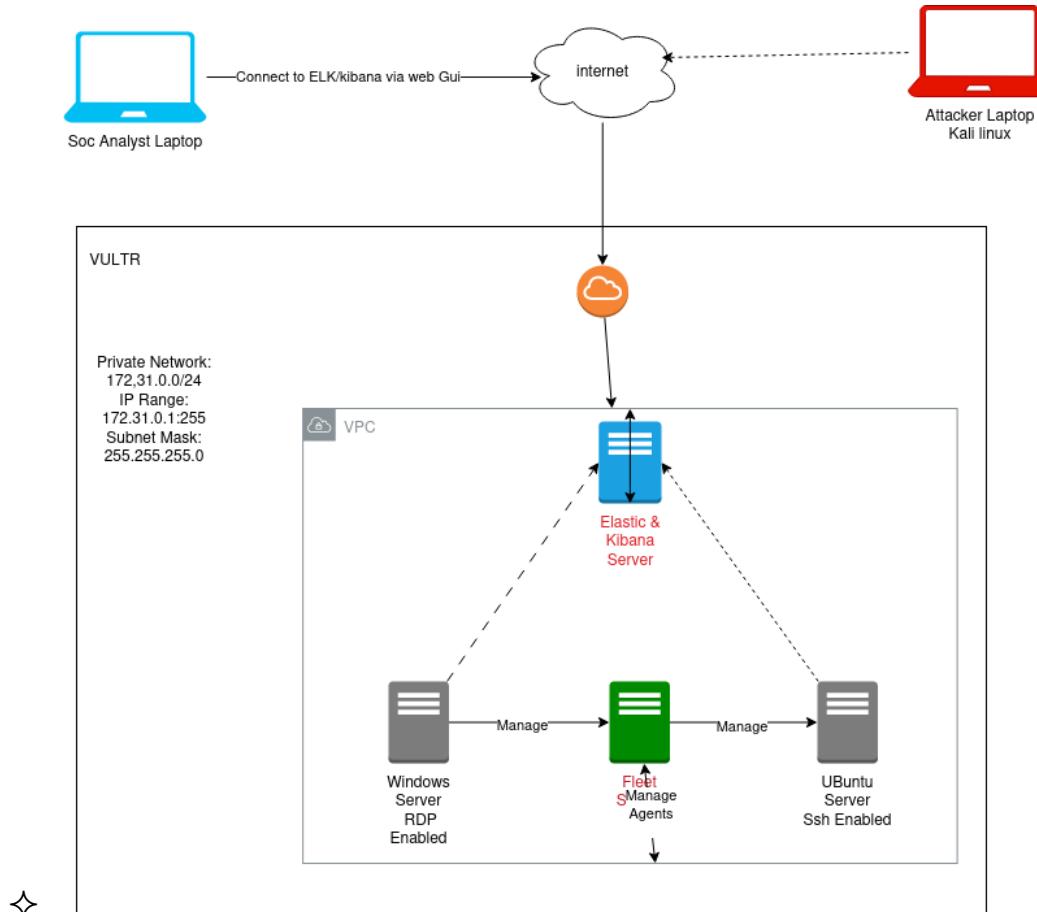


HASSAN MAZHAR_243293_PROJECT_REPORT

❖ LOGICAL DIAGRAM OF PROJECT IS:



❖ I FOLLOW THE ABOVE IMAGE IN THE BELOW STEPS

first of all setup the vultr account by giving any credit card number which are not in use like in my case I am using Sadapay.

after that the dashboard looks like in the below image, and then create an VPC(virtual private network first)

<https://my.vultr.com/vpc2/add>

The screenshot shows the 'Add VPC 2.0 Network' page. On the left, there's a sidebar with 'Products' expanded, showing options like Compute, Cloud Storage, Kubernetes, Serverless, Container Registry, Databases, Load Balancers, CDN, and Network. Under Network, 'VPC 2.0' is selected. The main area is titled 'Network Location' with a grid of 24 locations. The first row includes Tokyo (Japan), Bangalore (India), Delhi NCR (India), and Mumbai (India). The second row includes Osaka (Japan), Seoul (Korea, Republic of), Singapore (Singapore), and Tel Aviv (Israel). The third row includes Amsterdam (Netherlands), Paris (France), Frankfurt (Germany), and London (United Kingdom). The fourth row includes Madrid (Spain), Manchester (United Kingdom), Stockholm (Sweden), and Warsaw (Poland). The fifth row includes Atlanta (United States), New York (NJ) (United States), Chicago (United States), and Dallas (United States).

Now Configure an ip address manually by assigning an ipaddress in the below image:

Configure IP Range

Choose if you would like to generate an IP range automatically or configure this manually by yourself. We recommend using the automatic method.

Be careful if you create VPCs with overlapping IP blocks, whether an original VPC or a VPC 2.0. If you attach a VPS to multiple VPCs with overlapping IP blocks, it may cause connectivity issues.

Auto-Assign IP Range (Automatic - Recommended)

Configure IPv4 Range (Manual - Advanced)

Set IP Range

IPv4 Subnet Calculator

Network Address: 172.31.0.0

Network Prefix: 20

VPC 2.0 Network Description

Give the network a name.

Name: MY-VPC

◆ **configure a server:**

- choosing the location like i choose tornoto
- assigning the memory

The screenshot shows the Vultr web interface for deploying a server. On the left, there's a sidebar with a 'Deploy a Server' section and a 'Choose Type' dropdown. The 'Dedicated CPU' option is selected, with a brief description of what it offers. Below this are 'Shared CPU' and 'Bare Metal' options. To the right, a 'Location' dropdown is set to 'Toronto, CA'. Under 'Available Services', 'Dedicated CPU' is highlighted. Other options include 'Shared CPU', 'Bare Metal', 'VPC Network', 'DDoS Protection', 'Block Storage', and 'Load Balancers'. A 'Kubernetes Engine' button is also present. The 'Compliance' section lists 'SOC 2 Type 1', 'SOC 2 Type 2', 'ISO 27001', 'PCI-DSS', and 'NIST 800-53'. On the far right, a 'Deploy Summary' panel shows the location as 'Toronto, CA', 'Cores' as '1 vCPU', 'Memory' as '2 GB', 'Storage' as '25 GB', and 'Total Price' as '\$33.60/mo (\$0.050/hr)'. A 'Configure Software' button is at the bottom.

- ❖ choose machine:
 - i choose ubuntu where i install my elastic search

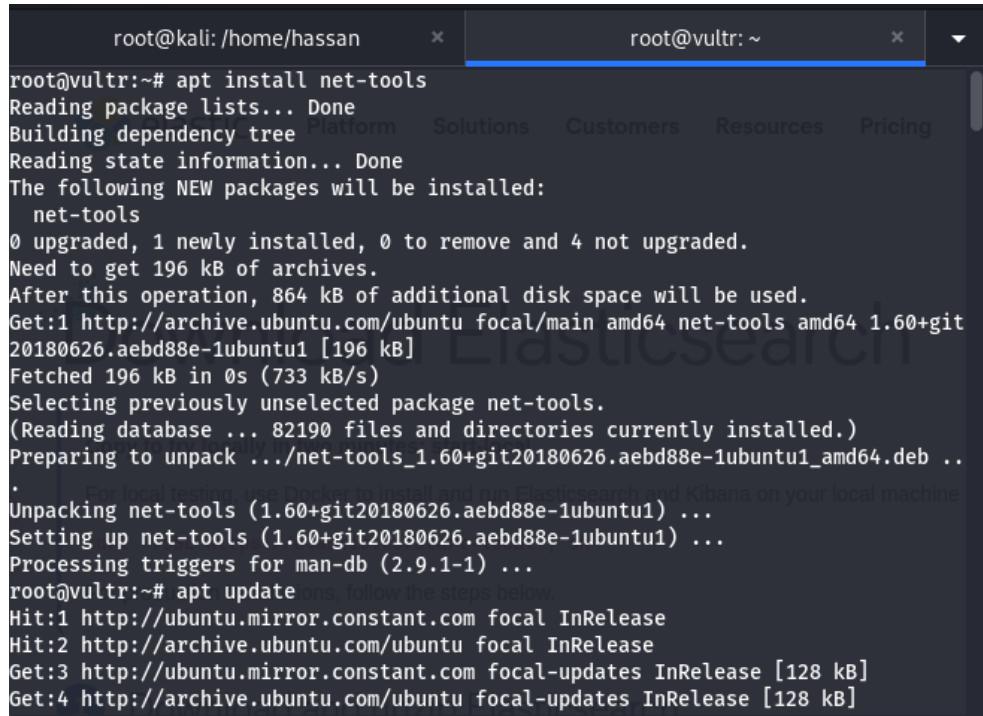
This screenshot shows the 'Select Version' step for Ubuntu. It features two main sections: 'Fedora CoreOS' and 'Flatcar Container Linux'. The 'Ubuntu' section is highlighted with a blue border. It contains the Ubuntu logo, the word 'Ubuntu', and the version '20.04 x64'. Below the logo is a checkmark icon. The 'Flatcar Container Linux' section has its own logo and version 'Leap 15 x64'. There are also 'X' and 'Y' buttons on the left side of the screen.

now you can see that the our server is running
and you can change its setting.
you can view its in the console.

This screenshot shows the Vultr server management interface. At the top, there's a browser window titled 'noVNC - ID 3670c618-51ab-4f51-9f85-886d40470c35 - Mozilla Firefox' showing a terminal session. The terminal shows the command 'curl 20.04.1 LTS vultr 111'. Below the browser is a search bar and a 'Deploy' button. The main area displays a table of servers with columns for 'OS', 'Location', 'Charges', and 'Status'. One server entry shows 'Ubuntu' OS, 'Toronto' location, '\$0.06' charges, and 'Running' status. To the right of the table is a vertical menu with options: 'Server Details', 'View Console', 'Server Stop', 'Server Restart', 'Server Reinstall', and 'Server Destroy'. A small star icon is visible on the left side of the screen.

Or you can run in the locally by using ssh:

- ✧ now do ssh root@ipaddress and enter password in the localmachine to use this, so now install some common tools and update and upgrade it:

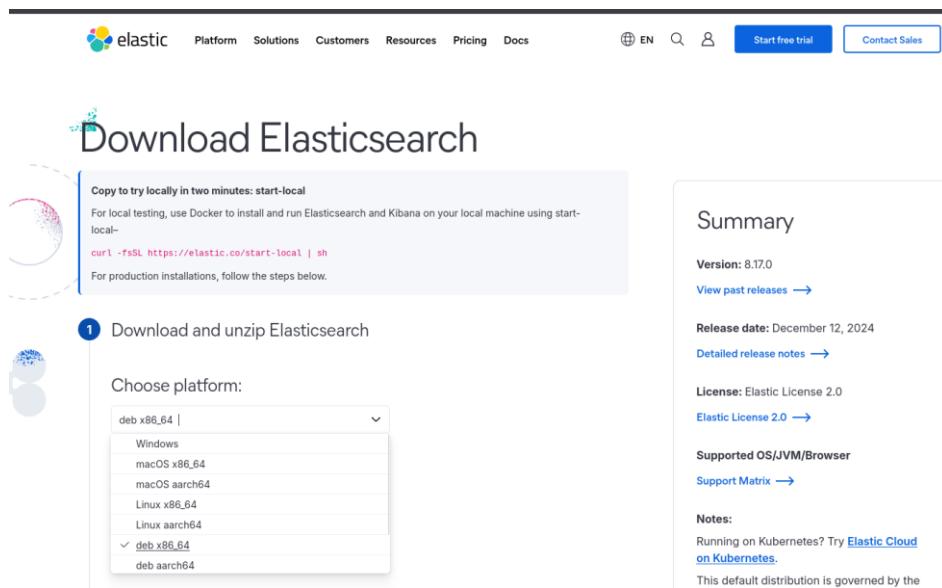


```

root@vultr:~# apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 0s (733 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 82190 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
.
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
root@vultr:~# apt update
Hit:1 http://ubuntu.mirror.constant.com focal InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://ubuntu.mirror.constant.com focal-updates InRelease [128 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]

```

- ✧ now install elastic search in it:



The screenshot shows the Elasticsearch download page. On the left, there's a section titled "Copy to try locally in two minutes: start-local" with a curl command. Below it, a step-by-step guide starts with "1 Download and unzip Elasticsearch". A dropdown menu for "Choose platform:" is open, showing options like Windows, macOS x86_64, macOS arm64, Linux x86_64, Linux arm64, deb x86_64, and deb arm64. On the right, there's a "Summary" box with details: Version 8.17.0, Release date December 12, 2024, License Elastic License 2.0, and Notes about running on Kubernetes.

- ✧ installation in the ubuntu server of elastic server:

```
(root@kali)-[~/home/hassan]
# ssh root@155.138.142.160
root@155.138.142.160's password:  elastic
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-200-generic x86_64)

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

System information as of Sat 28 Dec 2024 08:33:43 AM UTC

System load:  0.0          Processes:           141
Usage of /:   28.4% of 22.88GB  Users logged in:   1
Memory usage: 16%          IPv4 address for enp1s0: 155.138.142.160  lrt-local
Swap usage:   0%          For local testing, use Docker to install and run Elasticsearch and Kibana on your local
                         [local] platform:
                         curl -fsSL https://elastic.co/start-local | sh

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.  For production installations, follow the steps below.
2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it. ① Download and unzip Elasticsearch

*** System restart required ***
Last login: Sat Dec 28 07:55:28 2024 from 103.137.24.149
root@vultr:~# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.17.0-amd64.deb
--2024-12-28 08:33:55-- https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.17.0-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7:::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 636179540 (607M) [application/vnd.debian.binary-package]
Saving to: 'elasticsearch-8.17.0-amd64.deb'

elasticsearch-8.17.0-amd64.deb      4%[=====]>
elasticsearch-8.17.0-amd64.deb      8%[=====]>
Package managers:
 deb x86_64  sha  asc
 yum, dnf or zypper  apt-get
```

```
root@vultr:~# ls
elasticsearch-8.17.0-amd64.deb  snap
root@vultr:~# 
```

❖ now run command to install and configure this:

```
root@vultr:~# dpkg -i elasticsearch-8.17.0-amd64.deb
Selecting previously unselected package elasticsearch.
(Reading database ... 118841 files and directories currently installed.)
Preparing to unpack elasticsearch-8.17.0-amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.17.0) ...
Setting up elasticsearch (8.17.0) ...
----- 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 : TZGlJhVMSbn*rvw3Gop

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'.

### 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
root@vultr:~#
```

❖ this contains an important file where the username and the password is there so stored this file in .txt as well:

```
root@vultr:~# cat elastic-configure.txt
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 : TZGlJhVMSbn*rvw3Gop

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. root@vultr:~# 

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'.

### 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
root@vultr:~#
```

❖ now run this commands to update the status:

```
root@vultr:~# sudo systemctl daemon-reload
root@vultr:~# sudo systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@vultr:~#
root@vultr:~# sudo systemctl start elasticsearch.service
root@vultr:~# sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-12-28 08:37:59 UTC; 1min 6s ago
       Docs: https://www.elastic.co
     Main PID: 24814 (java)
        Tasks: 83 (limit: 2248)
      Memory: 1.4G
         CPU: 0.000 CPU(s) since start
        CGroup: /system.slice/elasticsearch.service
                └─24814 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token TZGlJhVMSbn*rvw3Gop
                  ├─24887 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch
                  └─24906 /usr/share/elasticsearch/modules/x-pack/ml/platform/linux-x86_64/bin/controller

Dec 28 08:37:29 vultr systemd[1]: Starting Elasticsearch...
Dec 28 08:37:32 vultr systemd-entrypoint[24887]: CompileCommand: dontinline java/lang/invoke/MethodHandle.setAsTypeCache bool dontinline = true
Dec 28 08:37:32 vultr systemd-entrypoint[24887]: CompileCommand: dontinline java/lang/invoke/MethodHandle.asTypeUncached bool dontinline = true
Dec 28 08:37:59 vultr systemd[1]: Started Elasticsearch.
lines 1-16 (END)
```

- ❖ so the elastic service is running, but there is an directory /etc/elastic where all the important files are there, and most important is elasticsearch.yml
 - ❖ where we need to configue:

```
root@vultr:/etc/elasticsearch# ls
certs  elasticsearch.keystore  elasticsearch-plugins.example.yml  elasticsearch.yml
root@vultr:/etc/elasticsearch# 
```

- ❖ this is the bydefault ipaddress and the portno is :

```

# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 192.168.0.1
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
```

✧ **use this ipaddress to paste in the above:**

```

root@vultr:/etc/elasticsearch# ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 155.138.142.160 brd 155.138.143.255 netmask 255.255.254.0
        broadcast 155.138.143.255
        inet6 fe80::5400:5ff:fe39:883d brd ff02::1 prefixlen 64 scopeid 0x20<link>
        ether 56:00:05:39:88:3d txqueuelen 1000 (Ethernet)
        RX packets 78805 bytes 849419038 (849.4 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 51490 bytes 3683397 (3.6 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

✧ **like this:**

```

# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 155.138.142.160
#
# 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

```

✧ **NOW MANAGE FIREWALL GROUPS SO TO OPEN AND ACESS THE ELASTIC SEARCH FROM ANYWHERR:**

Manage Firewall Group

Group ID: Bb03f4aa-e327-46fb-8bcd-1b015c455faa | Created: 2024-12-28 08:44:51 | Updated: 2024-12-28 08:44:51

Description

Group Rules

Linked Instances

IPv4 Rules

Inbound IPv4 Rules

This firewall ruleset will not be active until at least one rule is added.

Action	Protocol	Port (or range)	Source	Notes	Action
accept	SSH	22	Anywhere	0.0.0.0/0	Add note +

IPv6 Rules

Linked Instances

✿ after the above changings restart the elasticsearch.service:

```
root@vultr:/etc/elasticsearch# sudo systemctl restart elasticsearch.service
root@vultr:/etc/elasticsearch# sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
    Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
    Active: active (running) since Sat 2024-12-28 08:47:00 UTC; 13s ago
      Docs: https://www.elastic.co/
   Main PID: 25013 (java)
     Tasks: 76 (limit: 2248)
    Memory: 1.4G
       CGroup: /system.slice/elasticsearch.service
               ├─25013 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server
               ├─25088 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=60
               └─25107 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Dec 28 08:46:31 vultr systemd[1]: Stopped Elasticsearch.
Dec 28 08:46:31 vultr systemd[1]: Starting Elasticsearch...
Dec 28 08:46:34 vultr systemd-entrypoint[25088]: CompileCommand: dontinline java/lang/InvokeMethodHandle
Dec 28 08:46:34 vultr systemd-entrypoint[25088]: CompileCommand: dontinline java/lang/InvokeMethodHandle
Dec 28 08:47:00 vultr systemd[1]: Started Elasticsearch.
[lines 1-17/17 (END)]
```

➤ SETUP THE KIBANA

Download Kibana

Kibana builds for macOS x86_64 are ending with version 8.17. Future versions of Kibana can be run in Docker on this architecture.

1 Download and unzip Kibana

Choose platform:

DEB x86_64

↳ DEB x86_64

↳ sha

↳ asc



Package managers:

✧ installed kibana:

```
root@vultr:~# wget https://artifacts.elastic.co/downloads/kibana/kibana-8.17.0-amd64.deb
--2024-12-28 08:50:14-- https://artifacts.elastic.co/downloads/kibana/kibana-8.17.0-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::1
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345323288 (329M) [application/vnd.debian.binary-package]
Saving to: 'kibana-8.17.0-amd64.deb' [345323288/345323288]

2024-12-28 08:50:36 (15.4 MB/s) - 'kibana-8.17.0-amd64.deb' saved [345323288/345323288]
root@vultr:~# ls
elastic-configure.txt  elasticsearch-8.17.0-amd64.deb  kibana-8.17.0-amd64.deb  snap
```

```
root@vultr:~# dpkg -i kibana-8.17.0-amd64.deb
Selecting previously unselected package kibana.
(Reading database ... 120318 files and directories currently installed.)
Preparing to unpack kibana-8.17.0-amd64.deb ...
Unpacking kibana (8.17.0) ...
Setting up kibana (8.17.0) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For security reasons, consider switching to the modern providers.
Created Kibana keystore in /etc/kibana/kibana.keystore
root@vultr:~#
```

Installed kibana

✧ now access this file:

```
root@vultr:/etc/kibana#  
root@vultr:/etc/kibana# ls  
kibana.keystore kibana.yml node.options  
root@vultr:/etc/kibana# nano kibana.yml
```

GNU nano 6.2

✧ **configure like this:**

```
# ----- System: Kibana Server  
# Kibana is served by a back end server. This  
server.port: 5601  
# Specifies the address to which the Kibana  
# The default is 'localhost', which usually  
# To allow connections from remote users, set  
server.host: 155.138.142.160  
# Enables you to specify a path to mount Kibana  
# Use the `server.rewriteBasePath` setting to
```

✧ **now save this and start the services for kibana:**

```
root@vultr:~# systemctl daemon-reload  
root@vultr:~# systemctl enable kibana.service  
Unknown operation enable.  
root@vultr:~# systemctl enable kibana.service  
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /lib/systemd/system/kibana.service.  
root@vultr:~# systemctl start kibana.service  
root@vultr:~# systemctl status kibana.service  
● kibana.service - Kibana  
   Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)  
   Active: active (running) since Sat 2024-12-28 08:56:20 UTC; 7s ago  
     Docs: https://www.elastic.co  
     Main PID: 25380 (node)  
        Tasks: 11 (limit: 2248)  
       Memory: 321.5M  
         CPU: 321.5M  
        CGrou... /system.slice/kibana.service  
             └─25380 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist  
  
Dec 28 08:56:20 vultr systemd[1]: Started Kibana.  
Dec 28 08:56:21 vultr kibana[25380]: Kibana is currently running with legacy OpenSSL providers enabled! For details and in...  
Dec 28 08:56:21 vultr kibana[25380]: {"log.level":"info","@timestamp":"2024-12-28T08:56:21.657Z","log.logger":"elastic-apm-...  
Dec 28 08:56:21 vultr kibana[25380]: Native global console methods have been overridden in production environment.  
Dec 28 08:56:22 vultr kibana[25380]: [2024-12-28T08:56:22.944+00:00][INFO ][root] Kibana is starting.  
Dec 28 08:56:22 vultr kibana[25380]: [2024-12-28T08:56:22.998+00:00][INFO ][node] Kibana process configured with roles: [b  
lines 1-16 (END)]
```

✧ **before running its gui, generate an token:**

```
root@kali:~/home/hassan  
root@vultr:/usr/share/elasticsearch/bin# ls  
elasticsearch      elasticsearch-cli      elasticsearch-env      elasticsearch-keystore      elasticsearch-re...  
elasticsearch-certgen  elasticsearch-create-enrollment-token  elasticsearch-env-from-file  elasticsearch-node  elasticsearch-res...  
elasticsearch-certutil  elasticsearch-croneval  elasticsearch-geoip  elasticsearch-plugin  elasticsearch-sa...  
root@vultr:/usr/share/elasticsearch/bin# ./elasticsearch-create-enrollment-token --scope kibana  
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiolsiMTU1LjEzOC4XNDU0MTY0jyMDAiXSwiZmdyIjo1NTQ0OWNkZWJmZTljZDBkMjRhNmUwMGZhZG14YmZlYzlkYTcwNTE2ZGNjZTY2  
root@vultr:/usr/share/elasticsearch/bin#
```

2.895 169.9ms 3 minutes

✧ **now save this enrollment token in an file:**

```
root@vultr:~# nano elastic-enrollment-token
root@vultr:~# cat elastic-enrollment-token
eyJ2ZXIiOiI4LjE0LjAiLCJhZHMiolsiMTU1LjEzOC4xNDIuMTYwOjkyMDAiXSwiZmdyIjoINTQ0OWN
root@vultr:~#
```

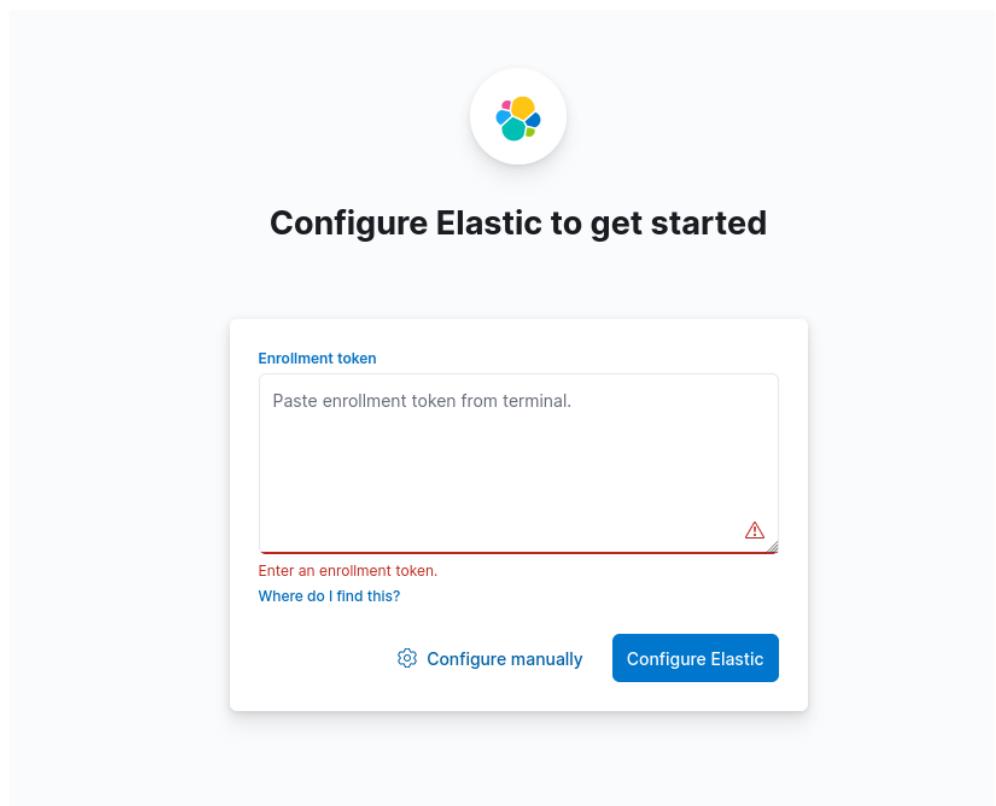
configure like this:

server.port: 5601

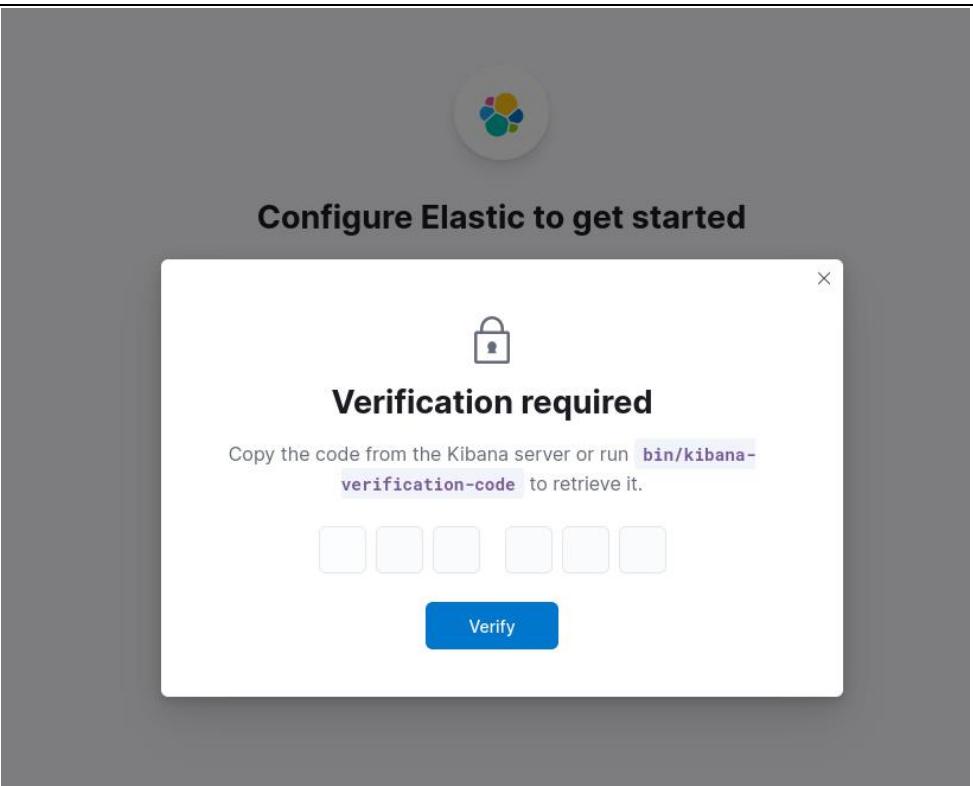
Specifies the address



- ❖ now access the elastic search through web gui:



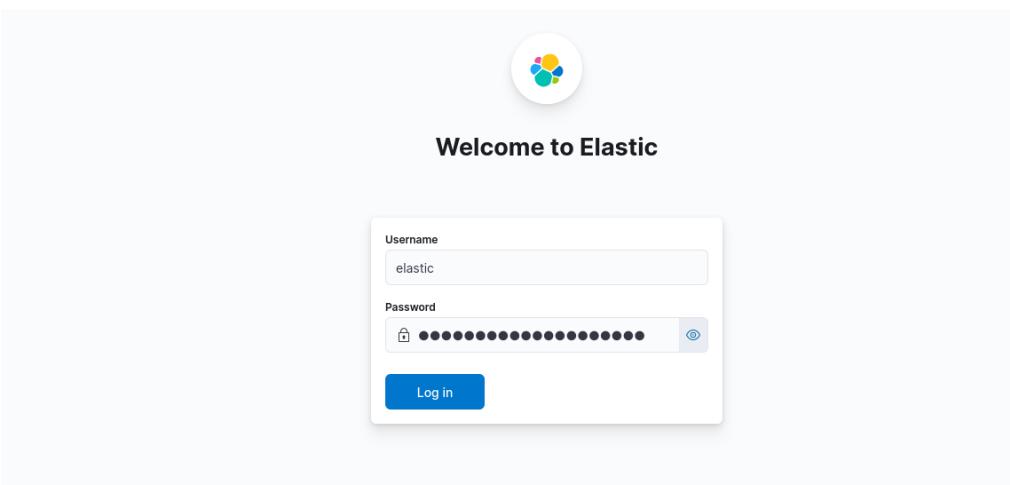
- ❖ now add that token



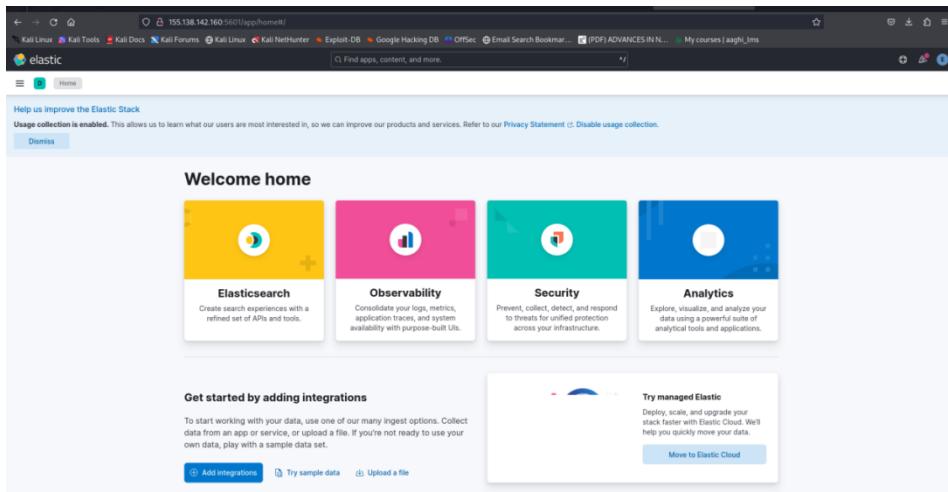
- ❖ now verification the code by runnin this command and paste here:

```
root@kali: /home/hassan
root@vultr:/usr/share/kibana/bin# ls
kibana kibana-encryption-keys kibana-health-gateway kibana-keystore kibana-plugin kibana-setup kibana-verification-code
root@vultr:/usr/share/kibana/bin# ./kibana-verification-code
Your verification code is: 604 930
root@vultr:/usr/share/kibana/bin#
```

- ❖ now enter the otp and now the dashboard look like this:



✧ now enter:



✧ so the dashboard looks like this

✧

✧ <http://155.138.142.160:5601/app>

➤ SETUP FLEET SERVER AND ELSTIC AGENT

✧ now setup and fleet server and elastic agent:

A screenshot of a web-based server deployment interface. At the top, it says 'Deploy a Server [Beta]' and 'Switch back to the old experience for a limited time ». The interface is divided into several sections: 'Operating System' (with options for My ISOs, Upload ISO, iPXE, and PXE Custom Script), 'Server Settings' (SSH Keys, Firewall Group), 'Server Hostname and Label' (Server 1 Hostname: My-Fleet-Server, Server 1 Label: My-Fleet-Server), 'Additional Features' (Step 1: Select Location & Plan, Step 2: Configure Software & Deploy Instance), and a 'Deploy Summary' sidebar on the right. The sidebar shows details like Location (Toronto, CA), Dedicated CPU (voc-0-1c-2gb-25s), Cores (1 vCPU), Memory (2 GB), Storage (25 GB), Automatic Backups (Enabled (\$5.60/mo)), Public IPv4 (Enabled), and Total Price (\$33.60/mo (\$0.050/hr)). At the bottom right are 'Back' and 'Deploy' buttons.

✧ now add this

The screenshot shows the 'Add a Fleet Server' wizard in the Fleet UI. The top navigation bar includes icons for search, refresh, and user profile, along with a 'Send feedback' button. The main title is 'Add a Fleet Server'. A sub-instruction states: 'A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#)'.

The wizard has three tabs: 'Quick Start' (selected) and 'Advanced'. The first step, 'Get started with Fleet Server', is highlighted with a blue circle containing the number 1. It contains fields for 'Name' (My-fleet-server) and 'URL' (https://149.248.62.254), with a link to 'Add another URL'. A blue button labeled 'Generate Fleet Server policy' is present. The next steps are 'Install Fleet Server to a centralized host' (step 2) and 'Confirm connection' (step 3). A sidebar on the left lists 'Fleet', 'Agents', 'Metrics', 'Logs', and 'Metrics & Logs'. A note at the bottom left says 'Paste this in the fleet server:' followed by a copy icon.

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#).

Quick Start **Advanced**

<https://149.248.62.254:443>. You can edit your Fleet Server hosts in [Fleet Settings](#).

2 Install Fleet Server to a centralized host

Install Fleet Server 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. For additional guidance, see our [installation docs](#).

Linux Tar **Mac** **Windows** **RPM** **DEB**

```
curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elast
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install \
--fleet-server-es=https://155.138.142.160:9200 \
--fleet-server-service-token=AAEAAWVsYXN0aNMvZmx1ZXQtc2VydMVyL3Rva2VuLTE3
--fleet-server-policy=fleet-server-policy \
--fleet-server-es-ca-trusted-fingerprint=5449cdebfe9cd0d24a6e00fad8bfec9
--fleet-server-port=8220
```

3 Confirm connection

root@My-Fleet-Server:~# curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 377M 100 377M 0 0 28.1M 0 0:00:13 0:00:13 --:-- 14.7M
root@My-Fleet-Server:~# tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
elastic-agent-8.17.0-linux-x86_64/README.md
elastic-agent-8.17.0-linux-x86_64/otel_samples/
elastic-agent-8.17.0-linux-x86_64/otel_samples/logs_metrics_traces.yml
elastic-agent-8.17.0-linux-x86_64/otel_samples/platform_logs.yml
elastic-agent-8.17.0-linux-x86_64/otel_samples/platform_logs_hostmetrics.yml
elastic-agent-8.17.0-linux-x86_64/elastic-agent-reference.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/.build_hash.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/LICENSE.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE_pf-elastic-collector.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE_pf-elastic-symbolizer.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE_pf-host-agent.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/README.md
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/agentbeat
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/agentbeat.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/apm-server
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/apm-server.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/bundle.tar.gz
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/certs/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/certs/certs.pem
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/checksum.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/cloudbeat
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/cloudbeat.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/endpoint-security
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/endpoint-security-resources.zip
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/endpoint-security.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/fleet-server
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/fleet-server.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/java-attacher.jar
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/lenses/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/lenses/COPYING
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/lenses/access.aug

root@My-Fleet-Server:~# curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 377M 100 377M 0 0 28.1M 0 0:00:13 0:00:13 --:-- 14.7M
root@My-Fleet-Server:~# tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
elastic-agent-8.17.0-linux-x86_64/README.md
elastic-agent-8.17.0-linux-x86_64/otel_samples/
elastic-agent-8.17.0-linux-x86_64/otel_samples/logs_metrics_traces.yml
elastic-agent-8.17.0-linux-x86_64/otel_samples/platform_logs.yml
elastic-agent-8.17.0-linux-x86_64/otel_samples/platform_logs_hostmetrics.yml
elastic-agent-8.17.0-linux-x86_64/elastic-agent-reference.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/.build_hash.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/LICENSE.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE_pf-elastic-collector.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE_pf-elastic-symbolizer.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE_pf-host-agent.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/NOTICE.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/README.md
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/agentbeat
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/agentbeat.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/apm-server
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/apm-server.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/bundle.tar.gz
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/certs/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/certs/certs.pem
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/checksum.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/cloudbeat
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/cloudbeat.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/endpoint-security
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/endpoint-security-resources.zip
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/endpoint-security.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/fleet-server
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/fleet-server.spec.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/java-attacher.jar
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/lenses/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/lenses/COPYING
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b0/components/lenses/access.aug

- ✧ and run this command first:

```
root@My-Fleet-Server:~# ufw allow 9200
Rule added
Rule added (v6)
root@My-Fleet-Server:~# ufw allow 8220
Rule added
Rule added (v6)
```

- ✧ now you can see we have an fleet server sucessfully connected:

The screenshot shows the Elastic Stack Fleet interface. On the left, there's a sidebar with 'Fleet' selected. The main area displays a table of agents. One row is highlighted in green, showing 'My-Fleet-Server' as the host, 'Fleet Server Policy' as the agent policy, and 'N/A' for CPU and Memory usage. To the right, a modal window titled 'Add agent' is open, showing the configuration for the enrolled host.

- ✧ see in the terminal as well:

```
> --fleet-server-port=8220
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:y
[== ] Service Started [2s] Elastic Agent successfully installed, starting enrollment.
[== ] Waiting For Enroll... [4s] {"log.level": "info", "@timestamp": "2024-12-28T14:12:08.934Z", "log.origin": {"func": "file.line":437}, "message": "Generating self-signed certificate for Fleet Server", "ecs.version": "1.6.0"}
[== ] Waiting For Enroll... [5s] {"log.level": "info", "@timestamp": "2024-12-28T14:12:09.465Z", "log.origin": {"func": "cmd.go", "file.line":483}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
[== ] Waiting For Enroll... [7s] {"log.level": "info", "@timestamp": "2024-12-28T14:12:11.470Z", "log.origin": {"func": "file.line":826}, "message": "Fleet Server - Starting", "ecs.version": "1.6.0"}
[== ] Waiting For Enroll... [11s] {"log.level": "info", "@timestamp": "2024-12-28T14:12:15.474Z", "log.origin": {"func": "file.line":807}, "message": "Fleet Server - Running on policy with Fleet Server integration: fleet-server-policy; mis": "[= ] Waiting For Enroll... [11s] {"log.level": "info", "@timestamp": "2024-12-28T14:12:16.213Z", "log.origin": {"func": "file.line":520}, "message": "Starting enrollment to URL: https://My-Fleet-Server:8220/", "ecs.version": "1.6.0"}}
[== ] Waiting For Enroll... [13s] {"log.level": "info", "@timestamp": "2024-12-28T14:12:17.321Z", "log.origin": {"func": "cmd.go", "file.line":483}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
{"log.level": "info", "@timestamp": "2024-12-28T14:12:17.323Z", "log.origin": {"function": "github.com/elastic/elastic-agent", "file.line": 100}, "message": "Successfully restarted the Elastic Agent."}
[ ==] Done [13s]
Elastic Agent has been successfully installed.
root@My-Fleet-Server:~/elastic-agent-8.17.0-linux-x86_64#
```

- ✧ now add an windows server as elastic agent, which we will need to monitor.

1 What type of host do you want to monitor?

Settings for the monitored host are configured in the [agent policy](#). Create a new agent policy to get started.

windows-agent

Create policy

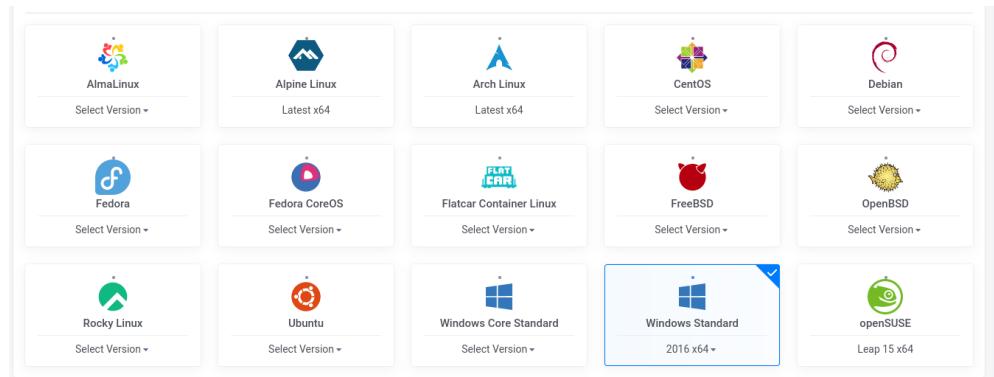
Collect system logs and metrics ⓘ

› Advanced options

2 Install Elastic Agent on your host



✧ and use the windows server int the vultr:



✧ 3 servers:

Cloud Compute

Name	OS	Location	Charges	Status	...
Cloud Instance 2048.00 MB Regular Cloud Compute - 216.128.178.236	Windows	Toronto	\$0.03	Running	...
Cloud Instance 2048.00 MB CPU Optimized Cloud - 155.138.142.160	Windows	Toronto	\$0.41	Running	...
My-Fleet-Server 2048.00 MB CPU Optimized Cloud - 149.248.62.254	Windows	Toronto	\$0.06	Running	...



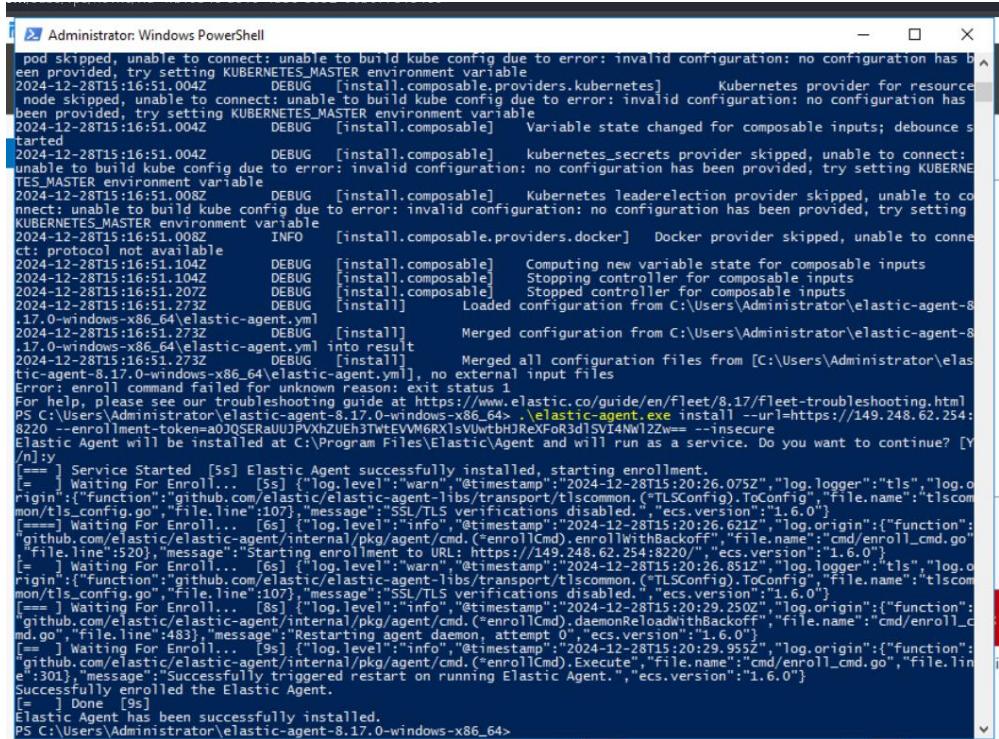
✧ this is windows:

The screenshot shows the Windows Server Manager Dashboard. A command prompt window is open, displaying a log of system events from December 28, 2024, at 14:56:34. The log includes various system configurations and administrative tasks such as changing power plans, executing PowerShell commands to set pagefile sizes, and running setup scripts for Intel QAT and NVIDIA drivers.

```
2024-12-28 14:56:34: Select Administrator: C:\Windows\System32\cmd.exe
2024-12-28 14:56:34: Changing power plan.
2024-12-28 14:56:34: =====
2024-12-28 14:56:34: Executing: powercfg -setactive 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c
2024-12-28 14:56:34:
2024-12-28 14:56:34:
2024-12-28 14:56:34: Updating pagefile maximum size.
2024-12-28 14:56:35: =====
2024-12-28 14:56:35: Executing: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command "Set-CimInstance -Query 'SELECT * FROM Win32_PageFileSetting WHERE Name LIKE ''%pagefile.sys''' -Property @{[MaximumSize=12288]}"
2024-12-28 14:56:51:
2024-12-28 14:56:51: Setting Administrator password.
2024-12-28 14:56:51: =====
2024-12-28 14:56:51: Changing password.
2024-12-28 14:56:52: The command completed successfully.
2024-12-28 14:56:52:
2024-12-28 14:56:52: Running Intel QAT setup!
2024-12-28 14:56:52: =====
2024-12-28 14:56:52: Cleaning up Nvidia files!
2024-12-28 14:56:52: =====
2024-12-28 14:56:52: Opening firewall ports.
2024-12-28 14:56:52: =====
2024-12-28 14:56:52: Updating firewall for remote desktop.
```



✧ so the agent is successfully installed:



```

Administrator: Windows PowerShell
pod skipped, unable to connect; unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2024-12-28T15:16:51.004Z DEBUG [install.composable.providers.kubernetes] Kubernetes provider for resource been skipped, unable to connect; unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2024-12-28T15:16:51.004Z DEBUG [install.composable] Variable state changed for composable inputs; debounce started
2024-12-28T15:16:51.004Z DEBUG [install.composable] kubernetes_secrets provider skipped, unable to connect; unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2024-12-28T15:16:51.008Z DEBUG [install.composable] Kubernetes leadelection provider skipped, unable to connect; unable to build kube config due to error: invalid configuration: no configuration has been provided, try setting KUBERNETES_MASTER environment variable
2024-12-28T15:16:51.008Z INFO [install.composable.providers.docker] Docker provider skipped, unable to connect; protocol not available
2024-12-28T15:16:51.104Z DEBUG [install.composable] Computing new variable state for composable inputs
2024-12-28T15:16:51.104Z DEBUG [install.composable] Stopping controller for composable inputs
2024-12-28T15:16:51.207Z DEBUG [install.composable] Stopped controller for composable inputs
2024-12-28T15:16:51.273Z DEBUG [install] Loaded configuration from C:\Users\Administrator\elastic-agent-8.17.0-windows-x86_64\elastic-agent.yml
2024-12-28T15:16:51.273Z DEBUG [install] Merged configuration from C:\Users\Administrator\elastic-agent-8.17.0-windows-x86_64\elastic-agent.yml into result
2024-12-28T15:16:51.273Z DEBUG [install] Merged all configuration files from [C:\Users\Administrator\elastic-agent-8.17.0-windows-x86_64\elastic-agent.yml], no external input files
Error: enroll command failed for unknown reason: exit status 1
For help, please see our troubleshooting guide at https://www.elastic.co/guide/en/fleet/8.17/fleet-troubleshooting.html
PS C:\Users\Administrator\elastic-agent-8.17.0-windows-x86_64> ./elastic-agent.exe install --url=https://149.248.62.254:8220 --enrollment-token=a0QSERauUJPVXNUeh3tWtEVm6RxIsV0wEbjReXfOr3dISVi4NwIZZw== --insecure
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
[==>] Service Started [5s] Elastic Agent successfully installed, starting enrollment.
[= ] Waiting For Enroll... [5s] {"log.level": "warn", "@timestamp": "2024-12-28T15:20:26.075Z", "log.logger": "tls", "log.origin": {"function": "github.com/elastic/elastic-agent-labs/transport/tlscommon.(*TLSConfig).ToConfig", "file.name": "tlscommon/tls_config.go", "file.line": "107"}, "message": "SSL/TLS verifications disabled", "ecs.version": "1.6.0"}
[= ] Waiting For Enroll... [6s] {"log.level": "info", "@timestamp": "2024-12-28T15:20:26.620Z", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.{enroll|enroll|cmd}.WithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "520"}, "message": "Starting enrollment to URL: https://149.248.62.254:8220", "ecs.version": "1.6.0"}
[= ] Waiting For Enroll... [6s] {"log.level": "warn", "@timestamp": "2024-12-28T15:20:26.851Z", "log.logger": "tls", "log.origin": {"function": "github.com/elastic/elastic-agent-labs/transport/tlscommon.(*TLSConfig).ToConfig", "file.name": "tlscommon/tls_config.go", "file.line": "107"}, "message": "SSL/TLS verifications disabled", "ecs.version": "1.6.0"}
[= ] Waiting For Enroll... [8s] {"log.level": "info", "@timestamp": "2024-12-28T15:20:29.250Z", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.{enroll|enroll|cmd}.daemonOnReloadWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "483"}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
[= ] Waiting For Enroll... [8s] {"log.level": "info", "@timestamp": "2024-12-28T15:20:29.955Z", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.{enroll|Cmd}.Execute", "file.name": "cmd/enroll_cmd.go", "file.line": "301"}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
[= ] Done [9s]
Elastic Agent has been successfully installed.
PS C:\Users\Administrator\elastic-agent-8.17.0-windows-x86_64>

```



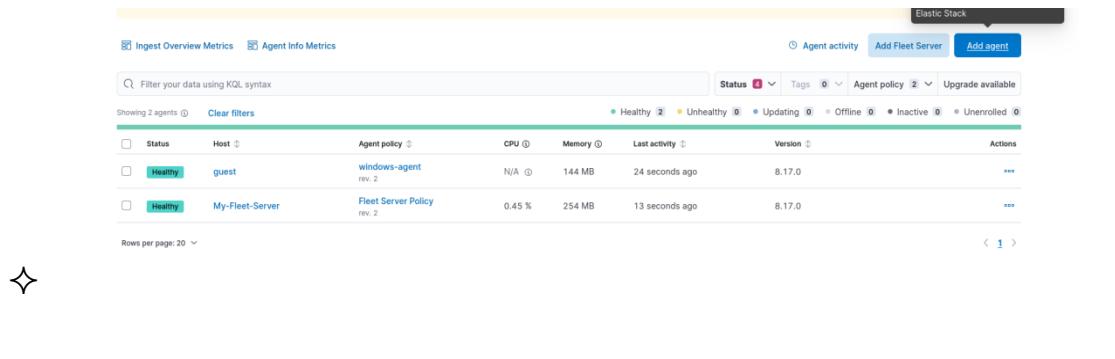
Agent enrollment confirmed



✓ 1 agent has been enrolled.

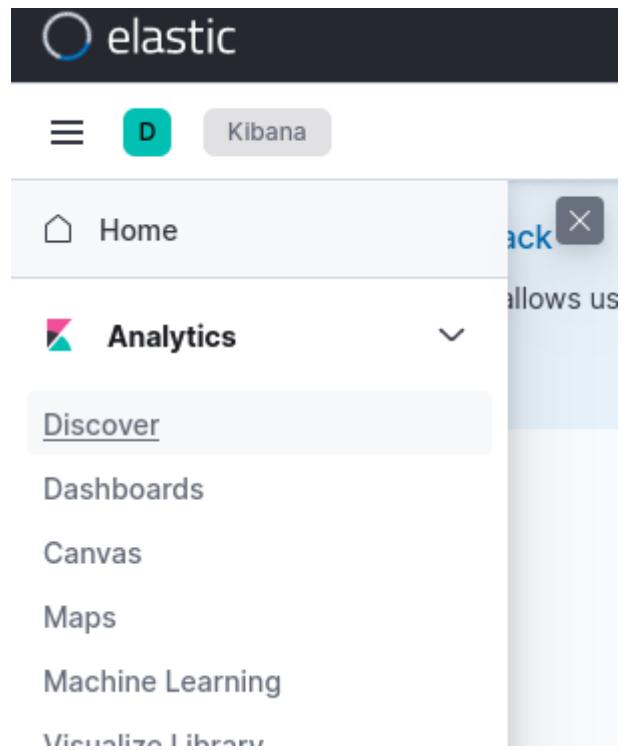
[View enrolled agents](#)

✧ so the windows agent and the fleet server is successfully installed:

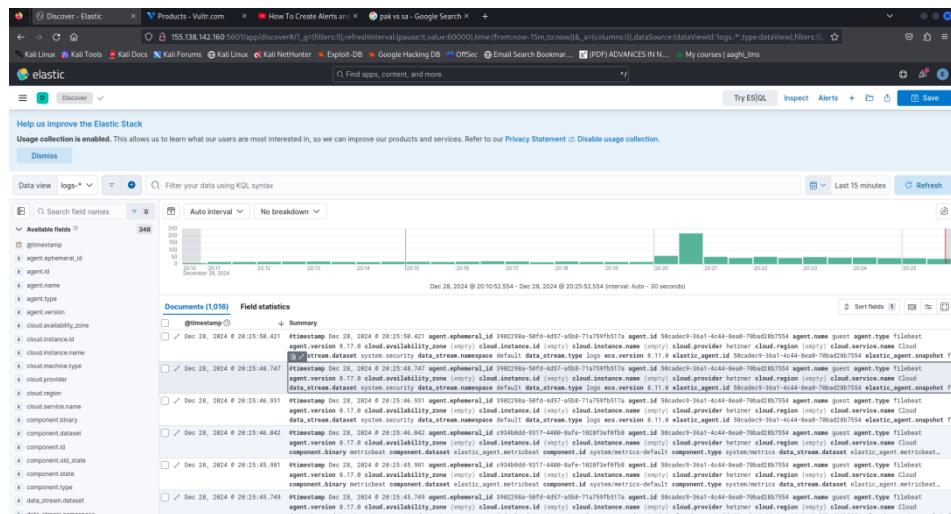


Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	guest	windows-agent rev. 2	N/A	144 MB	24 seconds ago	8.17.0	...
Healthy	My-Fleet-Server	Fleet Server Policy rev. 2	0.45 %	254 MB	13 seconds ago	8.17.0	...

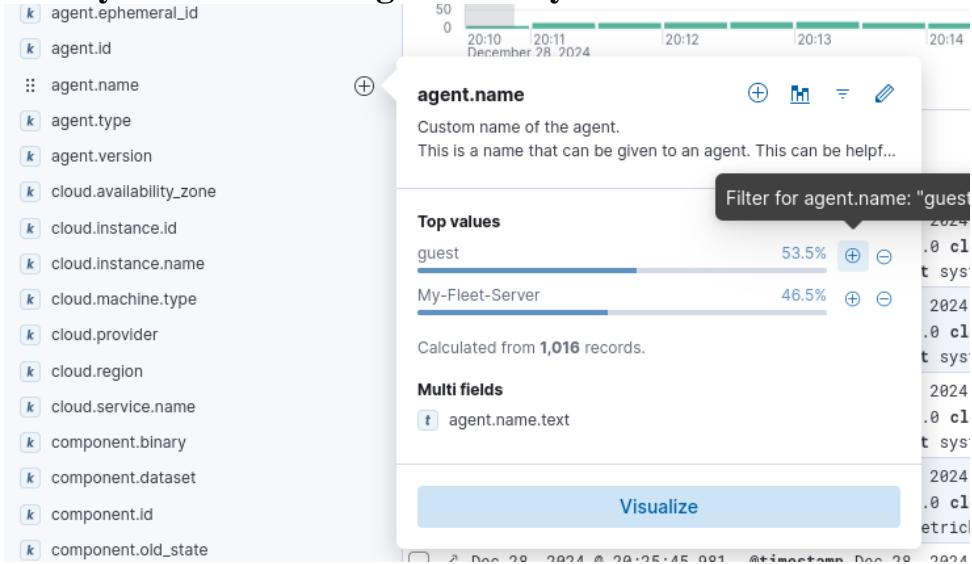
✧ now click on discover:



✧ these are the logs we can see:

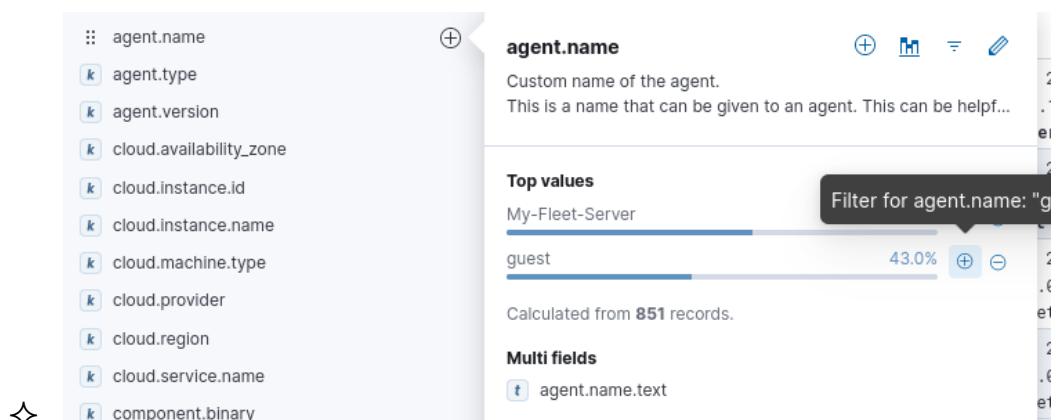


- ✧ when you click on the agent name you can see this:



- ✧ so you can monitor this as well

- ✧ now perform create an alerts in the elasticsearch ELK and perform attack on the windows server..



- ✧ so monitor only the “guest” which is our windows server:

- ✧ and this is the event id which tells us that whoever try to login into the system.

Event ID 4625 (viewed in Windows Event Viewer) documents every failed attempt at logging on to a local computer. This event is generated on the computer from where the logon attempt was made. A related event, Event ID 4624 documents successful logons.

- ✧ when search for this id “4625” in the filter tab:



➤ RDP AUTHENTICATION DETECTION

- ✧ you can see some logs as well. and you can search like this as well:



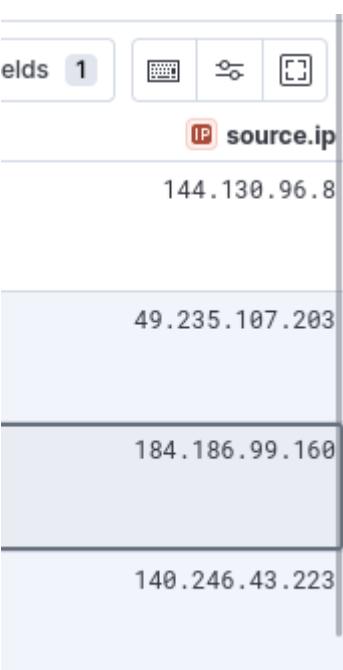
- ✧ apply this filter to know what is the source ip:

The screenshot shows the Kibana search interface. At the top, there is a search bar with the query "source.ip". Below the search bar, under "Available fields", there are two results: "source.ip" and "source.port". Under "Meta fields", there are zero results. To the right of the search interface, there is a sidebar with some icons.

✧ you can see the source ip:

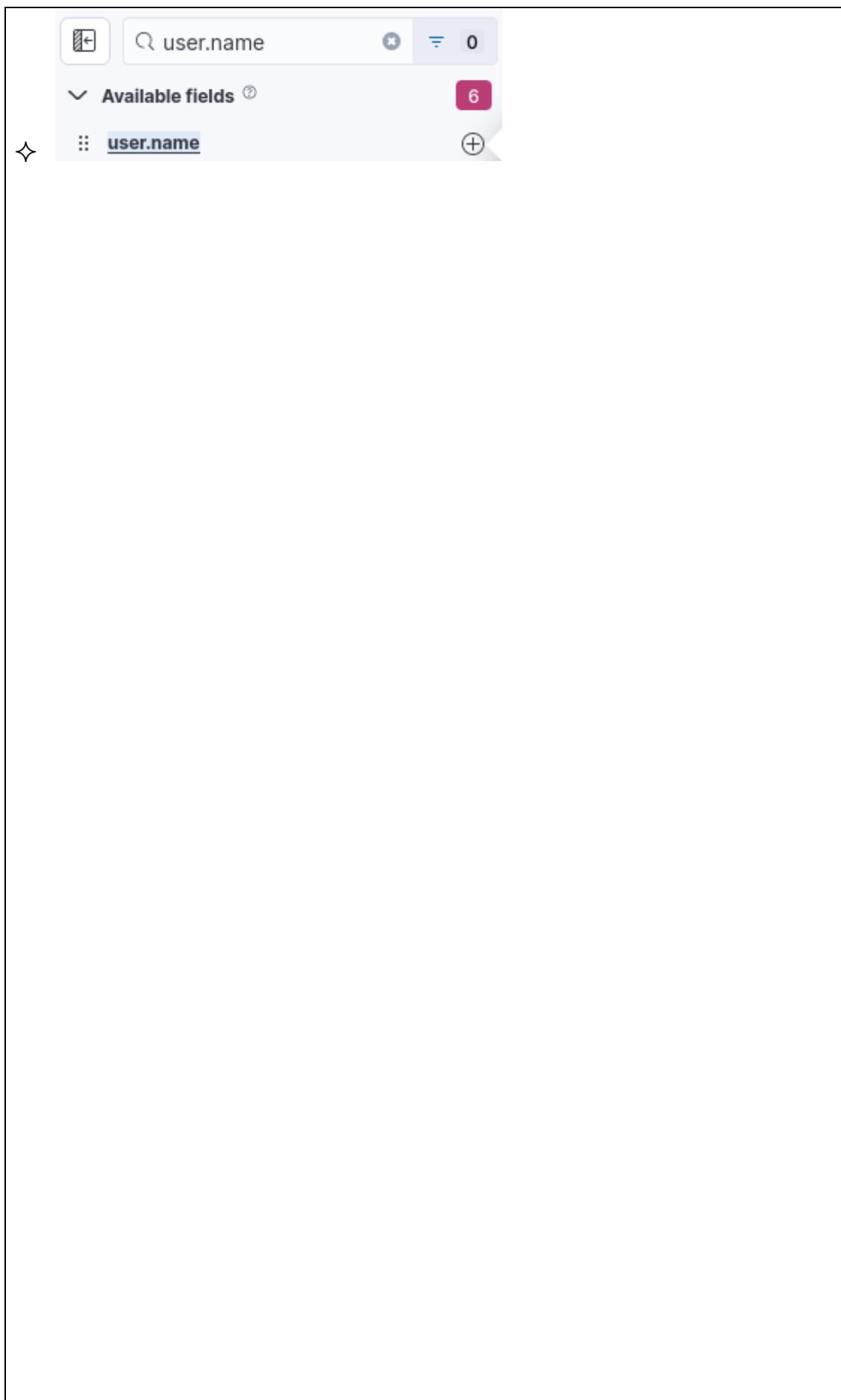


✧



✧

✧ now we have username as well so filter that also:



- ✧ so this is the some steps:

	source.ip	user.name
	144.130.96.8	admin
	49.235.107.203	Admin
	184.186.99.160	admin
	140.246.43.223	Admin

✧

- ✧ when open any event:

Documents (4) Field statistics		Columns 3
<input type="checkbox"/> @timestamp	Dec 29, 2024 @ 12:47:53.575	source.ip user.name
<input type="checkbox"/>		144.130.96.8 admin

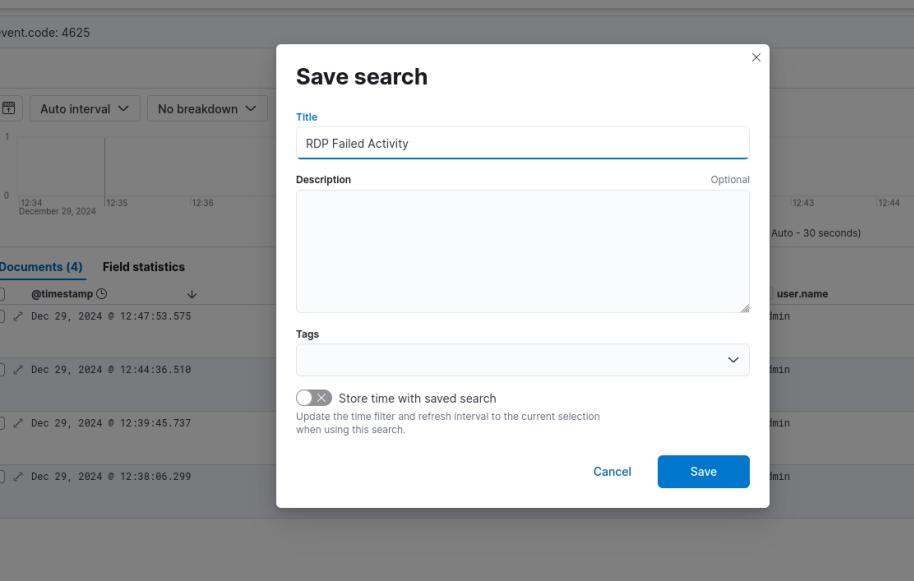
✧

- ✧ see the message:

Table JSON	
<input type="text"/> message	
Field	Value
<input type="text"/> message	<input type="button"/> An account failed to log on.
	Subject: Security ID: S-1-0-0 Account Name: - Account Domain: -

✧

- ✧ now save this activity as “RDP failed actity”:



- ❖ now perform an RDP login using the attacker laptop which is my host computer and try to login

Server Information

216.128.178.236 Toronto Created 17 hours ago

Add Tag +

Overview Usage Graphs Settings Snapshots Backups User-Data Tags DDOS

Bandwidth Usage: 0.07GB

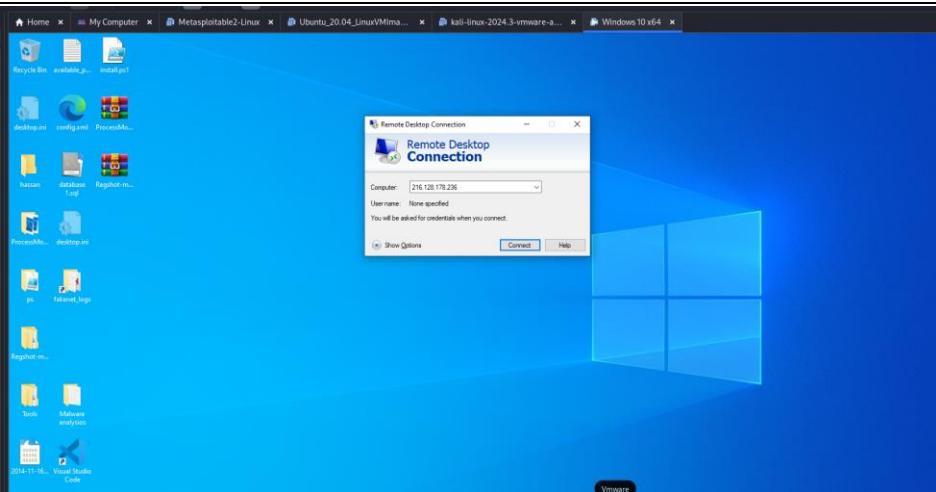
vCPU Usage: 2%

Cur \$

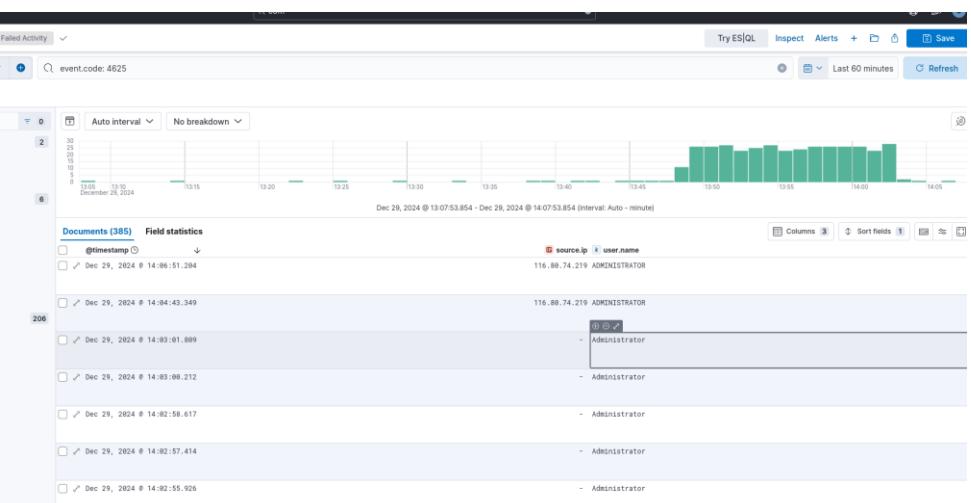
Location:	Toronto	Copy IP Address
IP Address:	216.128.178.236	
Username:	Administrator	
Password:	
vCPU/s:	1 vCPU	Label:
RAM:	2048.00 MB	OS:
Storage:	55 GB SSD	Auto B:
Bandwidth:	0.07 GB	

Vultr Recommendations

- ❖ copy this ipaddress and try to login using the attacker laptop:



❖ logs are created like this:



❖ so these are the logs when trying RDP to access the windows server

✧ **ssh brute force attack:**

✧ choose this:

system.auth.ssh.event

The SSH event as found in the logs (Accepted, Invalid, Failed, etc.)

No field data for the current search.

◆ add this column

Documents (363) Field statistics

	@timestamp	system.auth.ssh.event
<input type="checkbox"/>	Dec 29, 2024 @ 13:17:46.163	-
<input type="checkbox"/>	Dec 29, 2024 @ 13:17:46.163	-
<input type="checkbox"/>	Dec 29, 2024 @ 13:17:46.146	-
<input type="checkbox"/>	Dec 29, 2024 @ 13:17:46.084	-
<input type="checkbox"/>	Dec 29, 2024 @ 13:17:36.172	-
<input type="checkbox"/>	Dec 29, 2024 @ 13:17:36.172	-

◆ track the usernames as well:

user.name    

Short name or login of the user.

Top values



Calculated from 366 records.

Multi fields

 user.name.text

Visualize



✧ **so add this into the column:**



The screenshot shows a log viewer interface with two columns: "system.auth.ssh.event" and "user.name". The "user.name" column contains several rows of data. A dropdown menu is open over the first row of the "user.name" column, showing options for adding (+), deleting (-), and editing (edit icon) the field.

✧ **also we have to see the source ip:**

source.ip



IP address of the source (IPv4 or IPv6).

Top values

118.26.111.118	33.3%		
198.71.79.202	33.3%		
203.33.207.66	33.3%		

Calculated from **366** records.

Visualize



◆ **also add country name:**

source.geo.country_name



Country name.

Top values

China	33.3%		
Singapore	33.3%		
United States	33.3%		

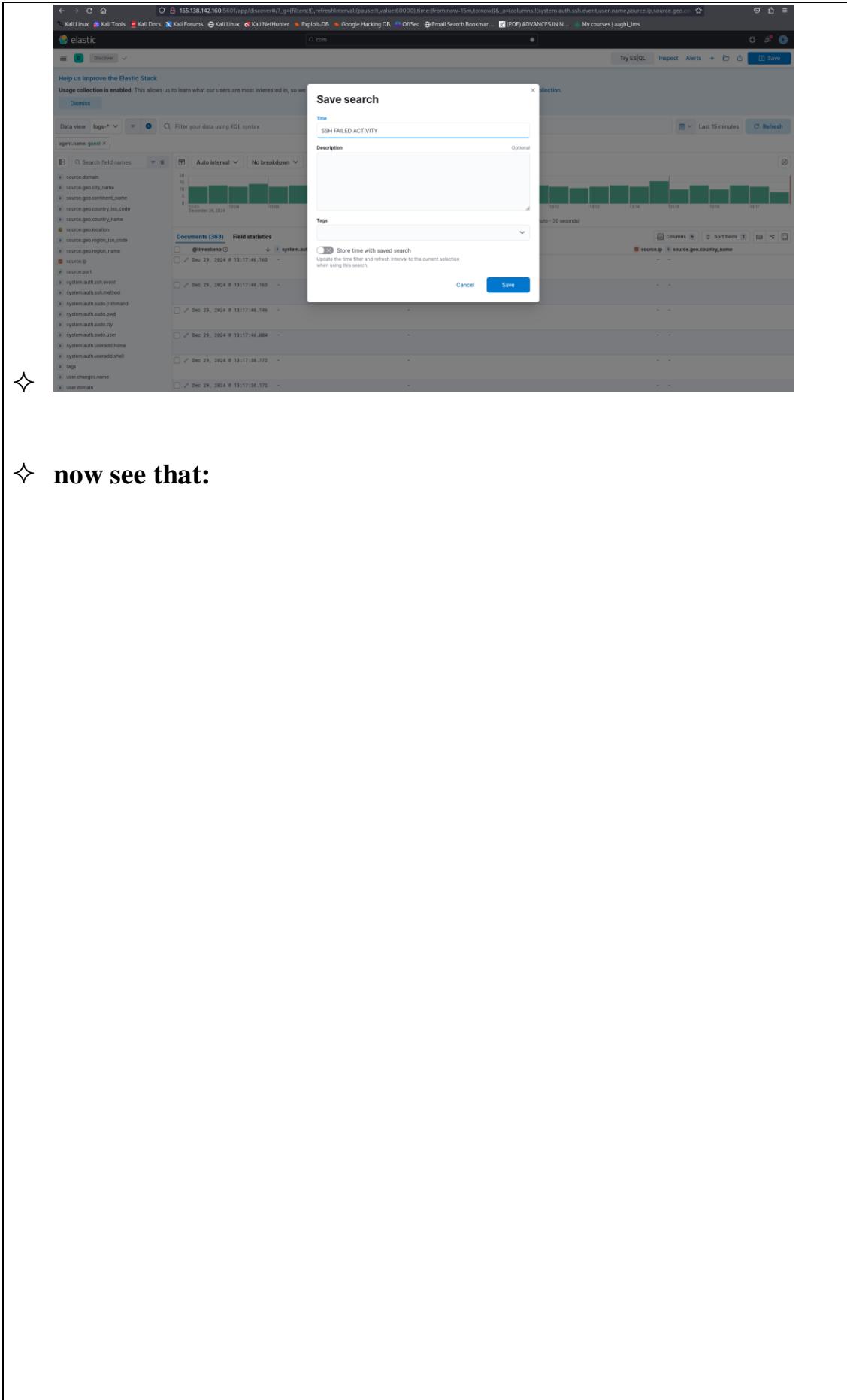
Calculated from **366** records.

Visualize



◆ **add this into the column and the final look like this:**

◆ **Save it as “SSH FAILED ACTIVITY”:**



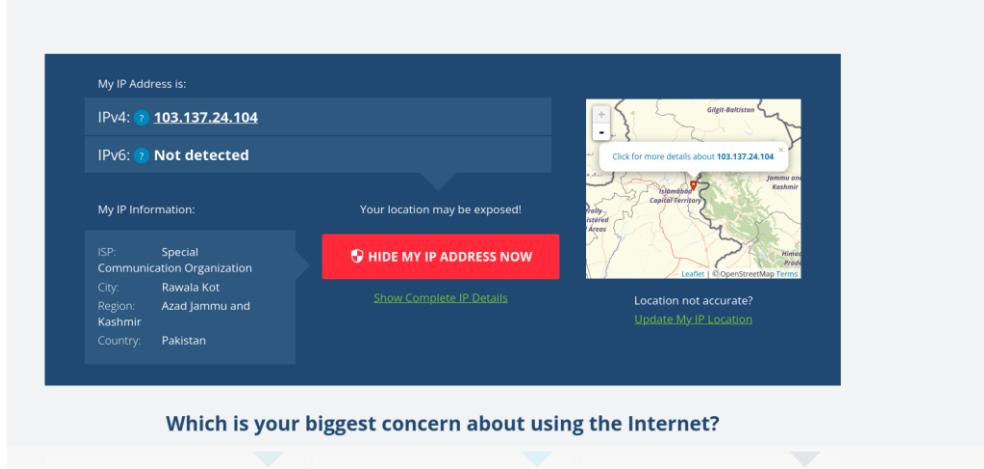
- ✧ from attacker machine use hydra to brute force:

```
[*] hydra -l /usr/share/wordlists/maass/all.txt -P /usr/share/wordlists/maass/all.txt ssh://149.248.62.254
Hydra v9.5 (c) 2023 by van Hauser / The Davi Mac Caw
[*] Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

[!] [HYDRA] https://github.com/anbanus/therc-hydra starting at 2024-12-29 13:32:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 36 tasks, 240112 login tries (l:1/p:428112), -26257 tries per task
[*] attack@149.248.62.254:22
[*] Session file "/hydra.restore" was written. Type "hydra -R" to resume session.
```

- ❖ this is the logs:

- ❖ so you can see that the logs ipaddress is the attacker machine:
 - ❖ and we can identify it through google its location as well:



- ❖ as i am using cloud so you can see someone trying from other countries as well:

Documents (97) Field statistics		Columns 5	Sort fields 1
		source.ip	source.geo.country_name
<input type="checkbox"/>	@timestamp	system.auth.ssh.event	user.name
<input checked="" type="checkbox"/>	Dec 29, 2024 0 13:34:43.000	Failed	hujj
			195.178.110.17 Bulgaria
<input type="checkbox"/>	Dec 29, 2024 0 13:34:41.000	Invalid	hujj
			195.178.110.17 Bulgaria

- ### ❖ **create an alert:**

Try ES|QL **Inspect** Alerts +

[Create search threshold rule](#)

[Manage rules and connectors](#)

Set the group, threshold, and time window

```
WHEN count()
OVER all documents
IS ABOVE 5
FOR THE LAST 5 days
```

Set the number of documents to send

```
SIZE 100
```

Exclude matches from previous runs

Add more fields to alert details

container.id × host.hostname × host.id × host.name ×

[Test query](#) [Copy query](#)

Query matched 749 documents in the last 5d.

Check every 1 minute

[Advanced options](#)

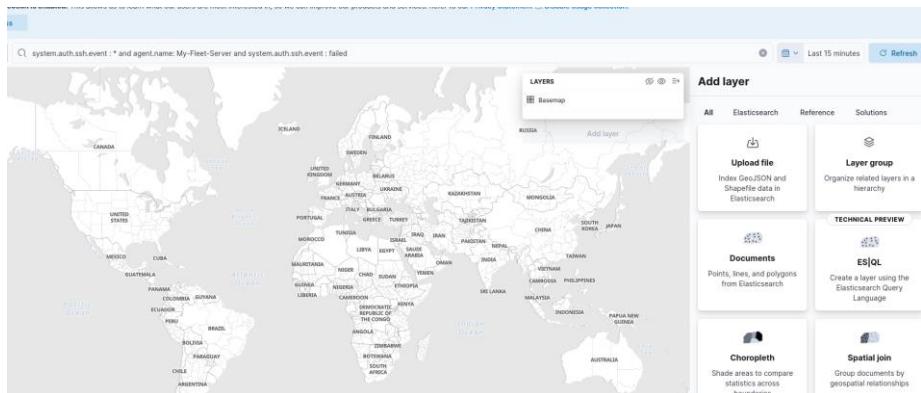
Role visibility

✧ now go to maps:

The screenshot shows the Kibana interface. At the top, there's a sidebar titled "Recently viewed" with items: "SSH FAILED ACTIVITY" and "RDP Failed Activity". Below this is the main navigation bar titled "Analytics" with options: "Discover", "Dashboards", "Canvas", "Maps", "Machine Learning", and "Visualize Library".

✧

✧ now add an layer:

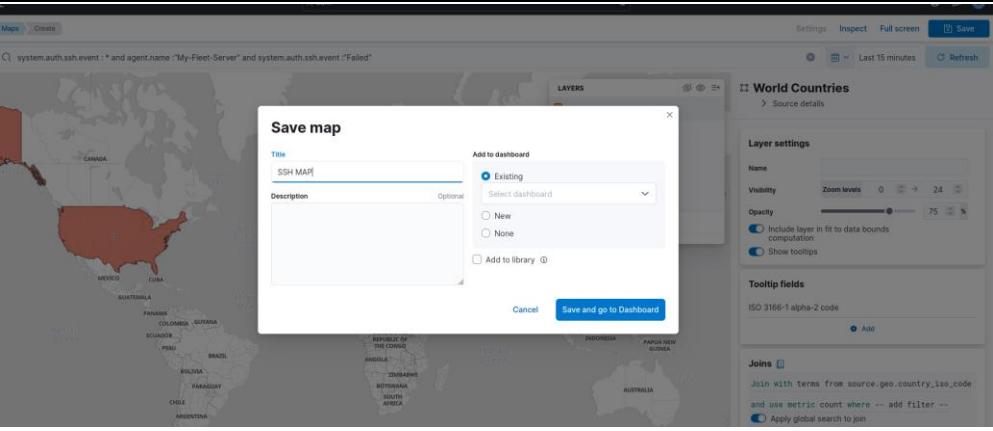


✧

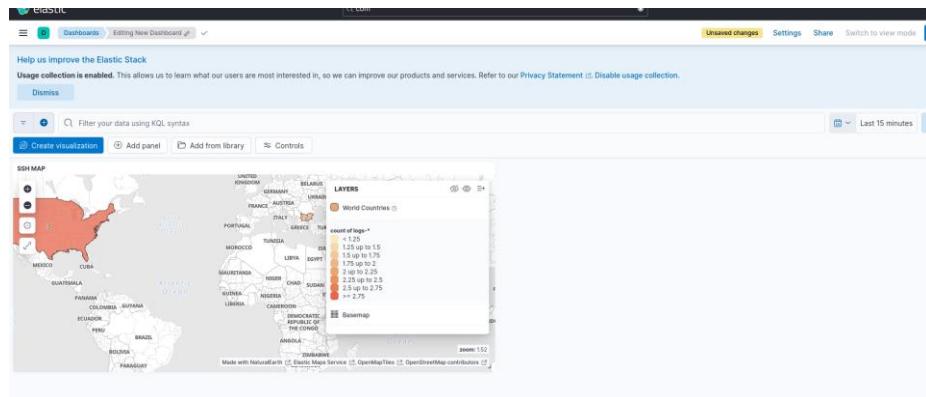
✧ so the location like this:



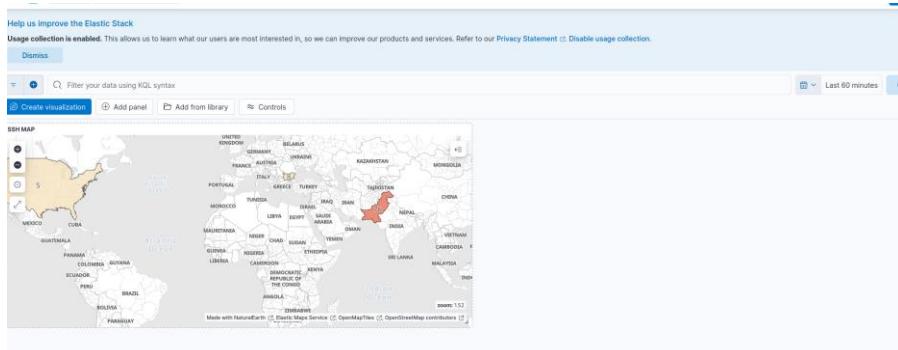
✧ NOW SAVE AS SSH MAP:



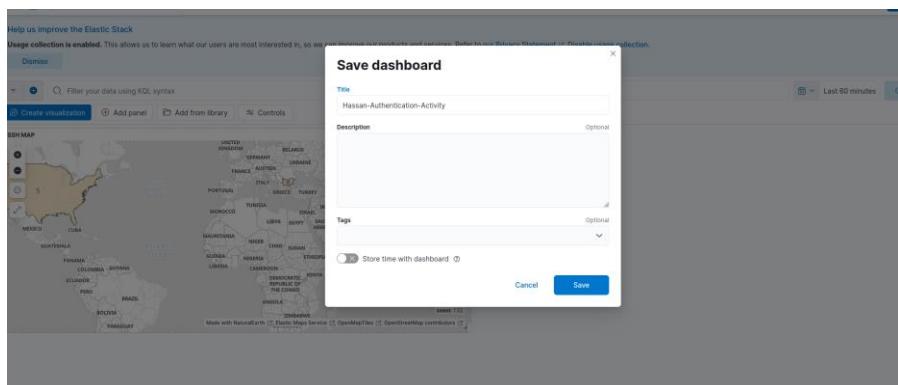
✧ NOW THE DASHBOARD LOOKS LIKE THIS:



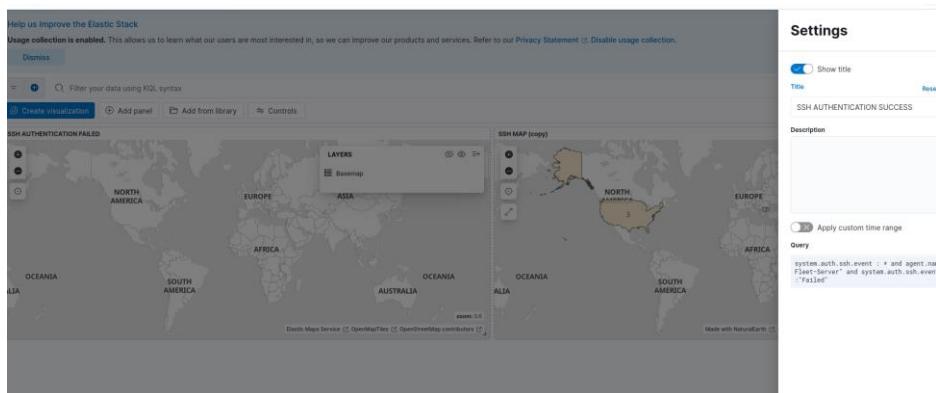
✧ LAST 60 MINUTES YOU CAN SEE:



✧ now save dashboard :



✧ NOW MAKE A COPY OF THE MAP AND CHANGE THE SETTING AS ONE IS FAILED AND OTHER IS SUCCES:



✧ as accepted is like this:

Help us improve the Elastic Stack
Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement [Disable usage collection](#).

[Dismiss](#)

Data view logs+ [Logs](#) system.auth.ssh.event : * and agent.name : "My-Fleet-Server" and system.auth.event : "Accepted"

agent.name: My-Fleet-Server system.auth.event: Accepted

Search field names Auto interval No breakdown

0 13:00 13:05 13:10 13:15 13:20 13:25 13:30 13:35 13:40 13:45 13:50 13:55

Dec 29, 2024 - Dec 29, 2024 @ 13:02:49.785 - Dec 29, 2024 @ 14:02:49.785 (interval: Auto - minute)

Documents (1) Field statistics

@timestamp user.name source.ip source.geo.country.name

Dec 29, 2024 @ 14:00:10.000 root 183.137.24.184 Pakistan

Columns Sort fields

SSH AUTHENTICATION SUCCESS

Made with NaturalEarth [Elastic Maps Service](#) [OpenMapTiles](#) [OpenStreetMap](#)

◆ SO this is our project to setup and ELK and ubuntu and windows server also using fleet server to detect the attacks, and using the VULTR cloud provider to host the server in the internet.