

Report

1. Install elasticsearch.

1. Install elasticsearch from apt (Just search on google).
2. Enable elasticsearch to run as service:

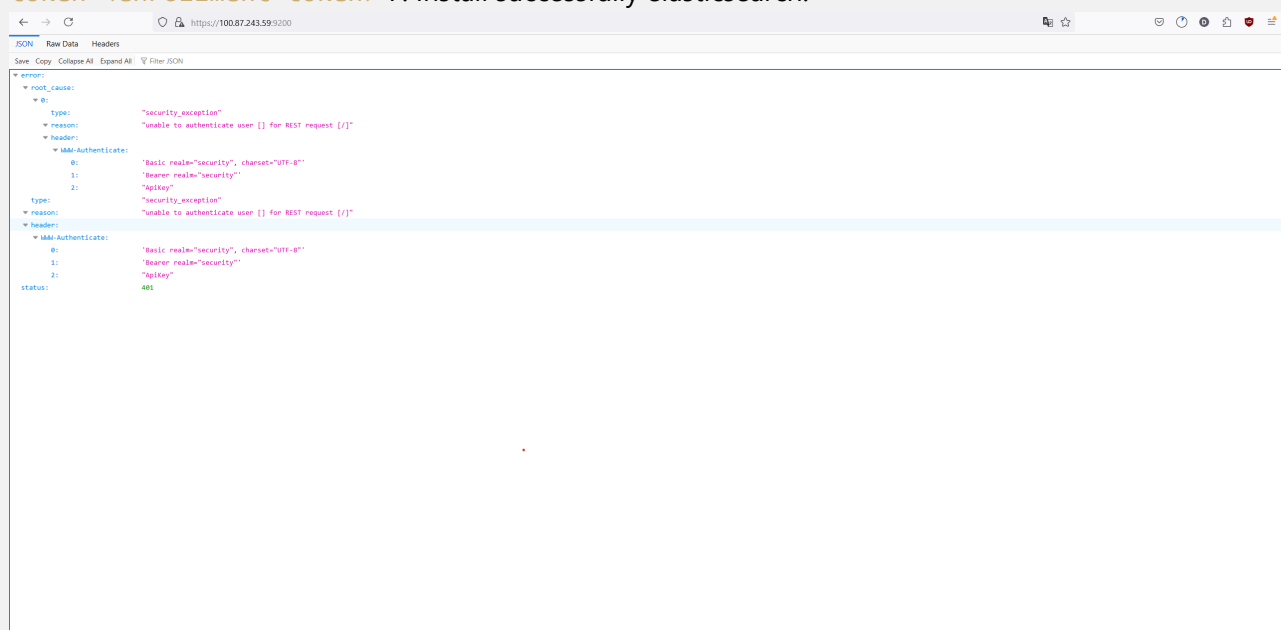
```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
```

3. Locate to `/usr/share/elasticsearch/bin/elasticsearch-create-token -s node` to generate token for node enrollment.
4. Locate to `/usr/share/elasticsearch/bin/elasticsearch-create-token -s kibana` to generate token for kibana enrollment.
5. Edit needed information in the file `/etc/elasticsearch/elasticsearch.yml` (this step maybe require changing file permission of folder or editing under root's right) Change the following varibale:

```
cluster.name: demo
network.host: 100.87.243.59
http.host: 0.0.0.0
transport.host: 0.0.0.0
```

Noted that data and logs are stored in the following file:

`/var/lib/elasticsearch /var/log/elasticsearch` 6. Noted that in the second node need to do this actions
`sudo /usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <enrollment-token>` 7. Install successfully elasticsearch.



Default account:elastic **Password:** tRZfgFvq+6bzGBh+aqAE **Updated: password:** elastic123

2. Install Kibana.

Back to the elasticsearch node and generate token using:

```
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```

The result is:

```
unable to create enrollment token for scope [kibana]
ERROR: Read timed out, with exit code 73
root@duyanhserver:/home/satan# /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
warning: ignoring JAVA_HOME=/usr/lib/jvm/java-21-openjdk-amd64; using bundled JDK
eyJ2ZXI0i0iI4LjE0LjAiLCJhZHII0lsMTAwLjg3LjI0My41OT05MjAwIl0sImZnciI6ImJhYWYyYjg5YTMxNTU2NDQ0YVWQxNzFmODZjYjRmOWRlMGY3NmM2NWVhZjQ3NGJkN2E5Nzk3MDdkMzM5NjBkM2IiLCJrZXkiOiIyYVJxT0pNQkottTWR1eU5FM6xvdjpuPU2F1N3FXdFRlRCZVU1NXktYzA5S0JnIn0=
root@duyanhserver:/home/satan#
```

1. Install kibana as guided through google (Just search installing Kibana)
- 2.

```
sudo systemctl daemon-reload
sudo systemctl enable kibana.service
```

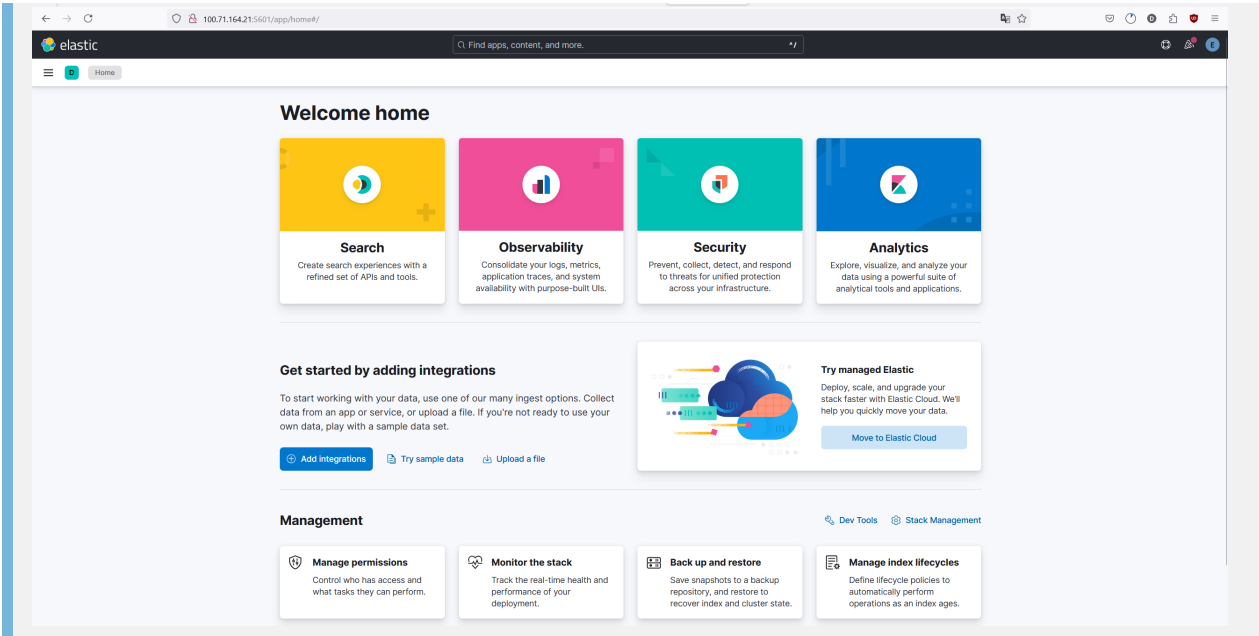
3. Edit `/etc/kibana/kibana.yml`
4. Back to elastic server to generate kibana enrollment token.
5. Enable elasticsearch to run as a service.

```
sudo systemctl daemon-reload
sudo systemctl enable kibana.service
```

6. Edit file `/etc/kibana/kibana.yml` Keys to edit:

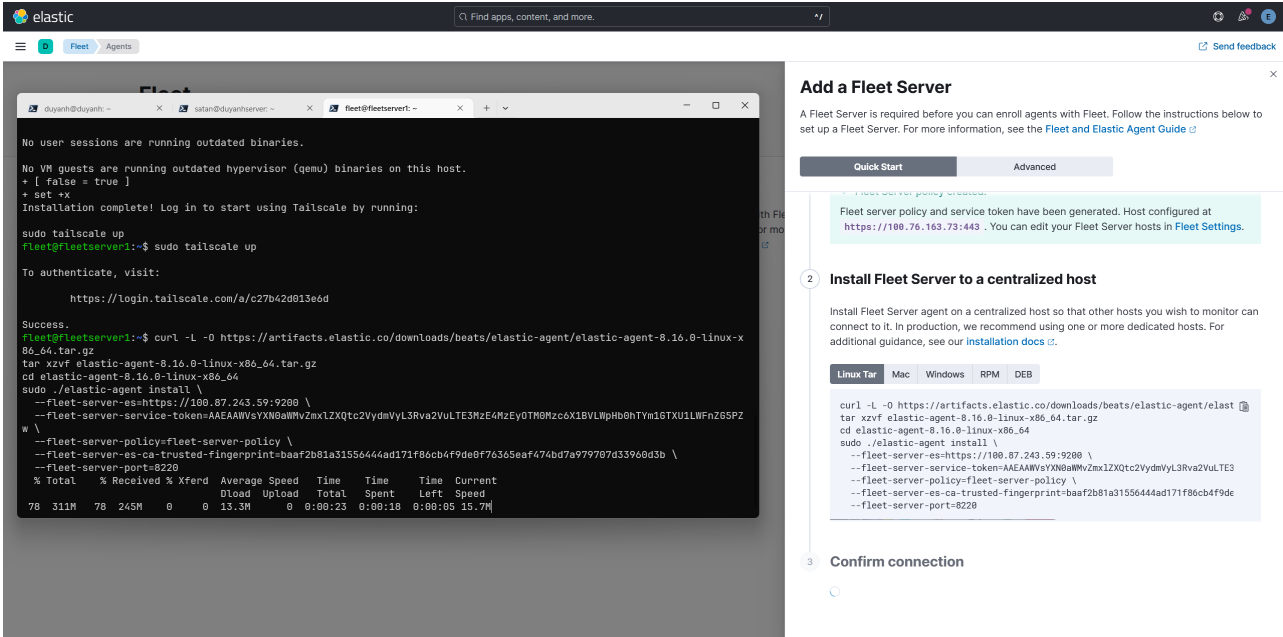
```
server.host: the current ip address of the server
```

7. Start kibana `sudo systemctl start kibana.service`
8. `http://ip_address:5601/code=` (Node that this code get by run `systemctl status`)
`http://100.71.164.21:5601`
9. Result:

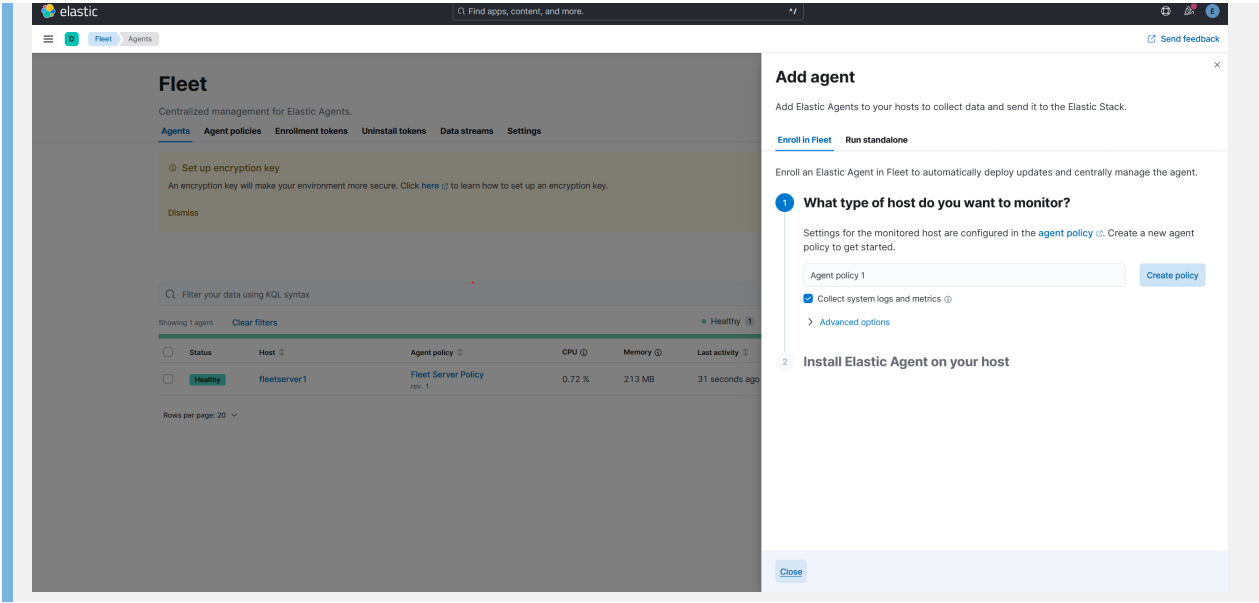


3. Install Fleet Server

- 1. Navigate to fleet in kibana dashboard.
- 2. Do the step as guided in the dashboard.

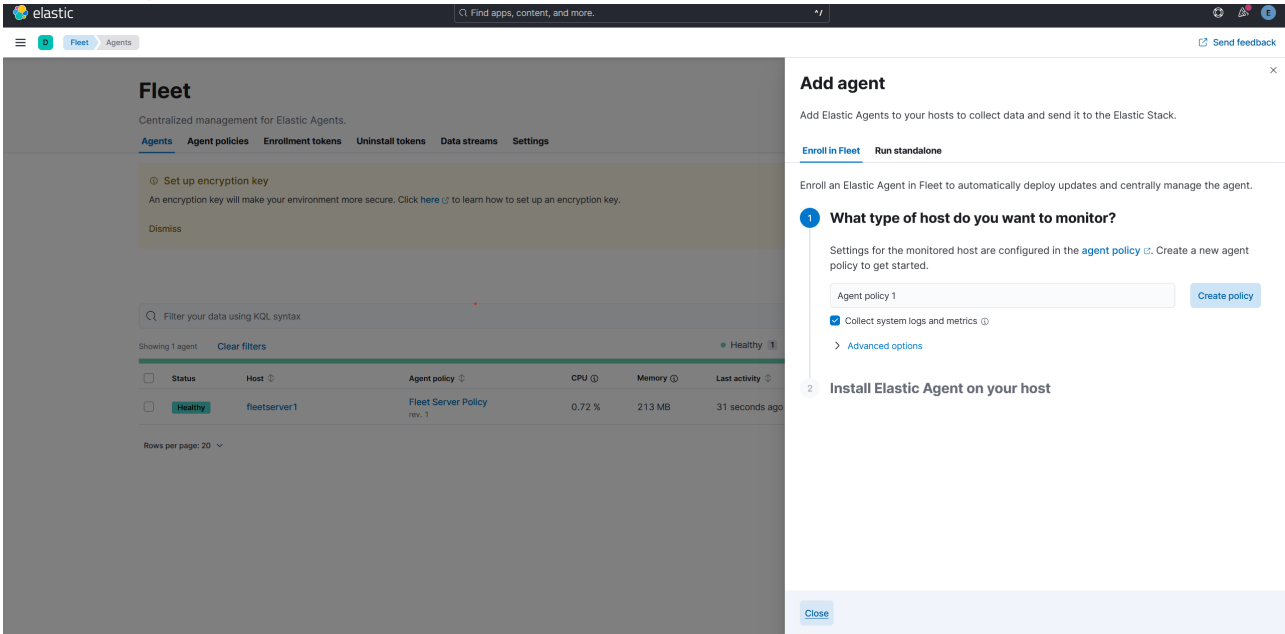


3. Result

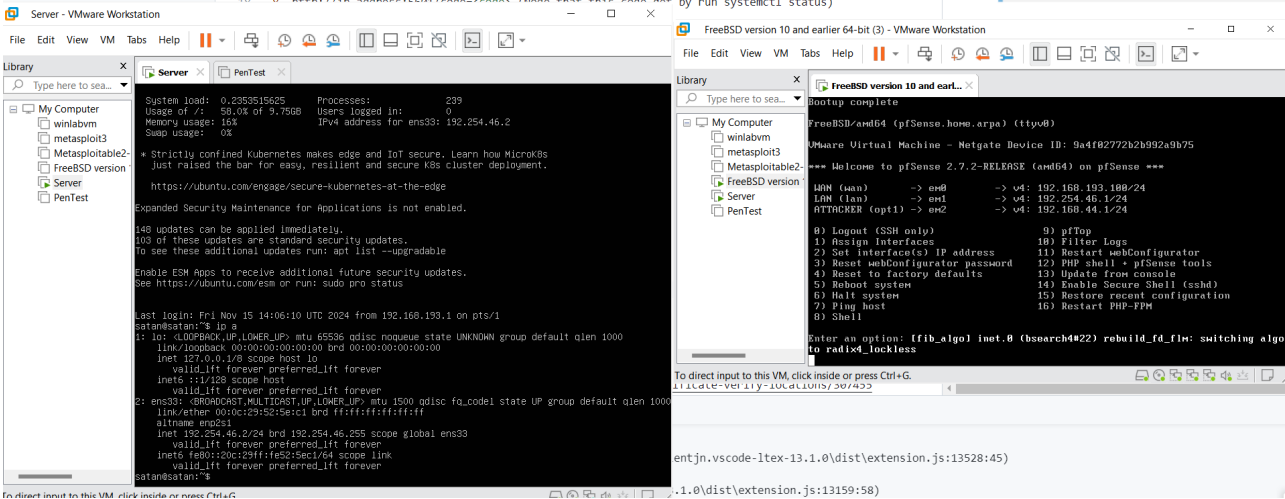


4. Add agent.

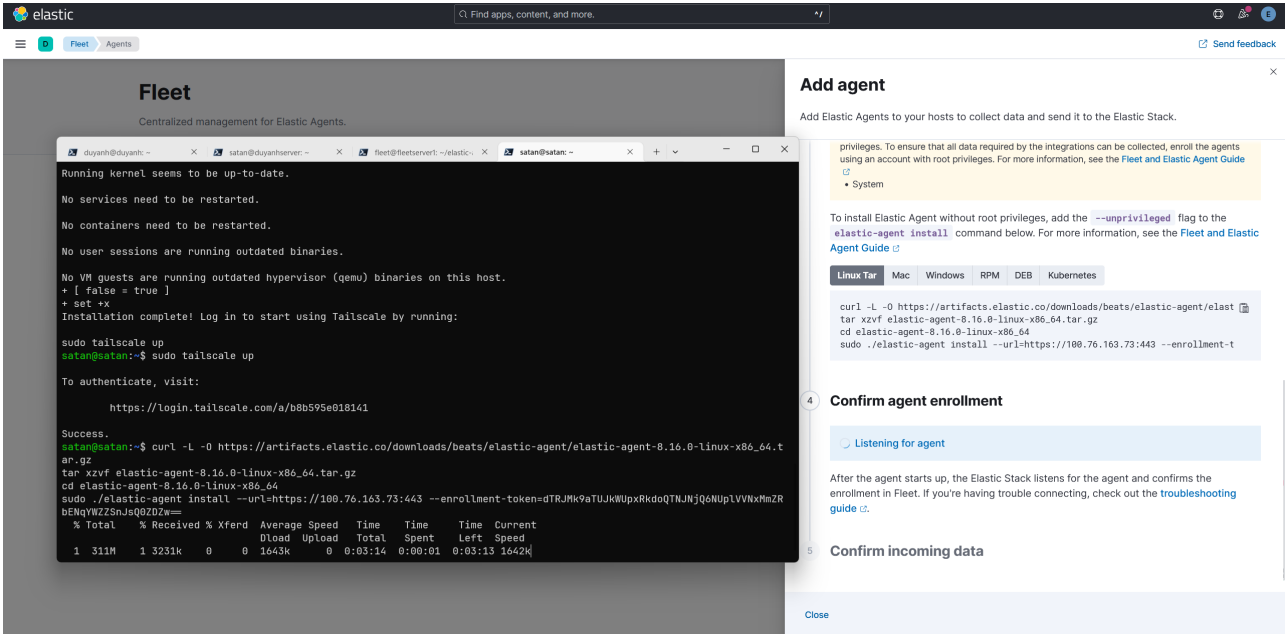
1. Install agent.



2. Turn on pfsense firewall and the server behind it.

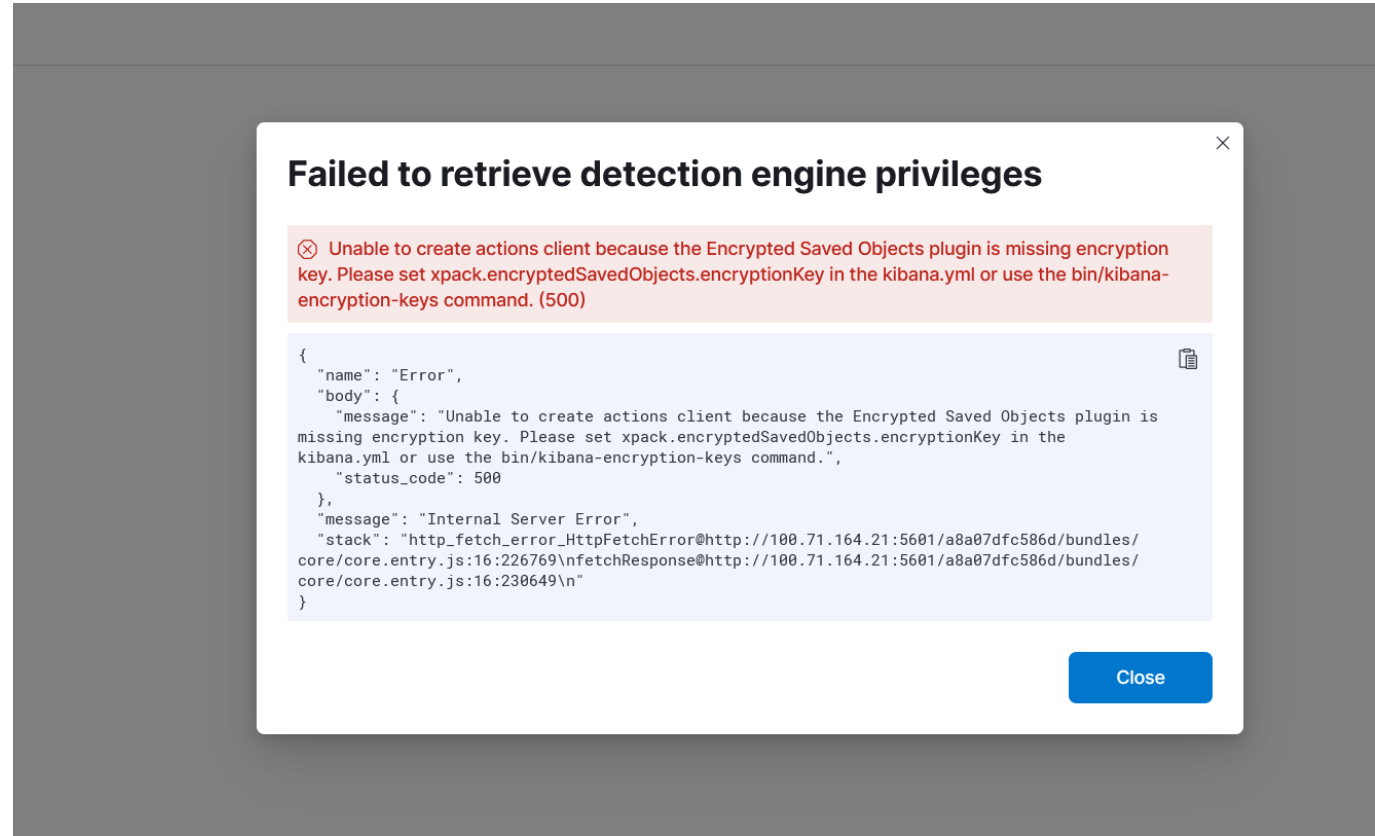


3. Install agent.



5. Add rule.

Engine privileged error.



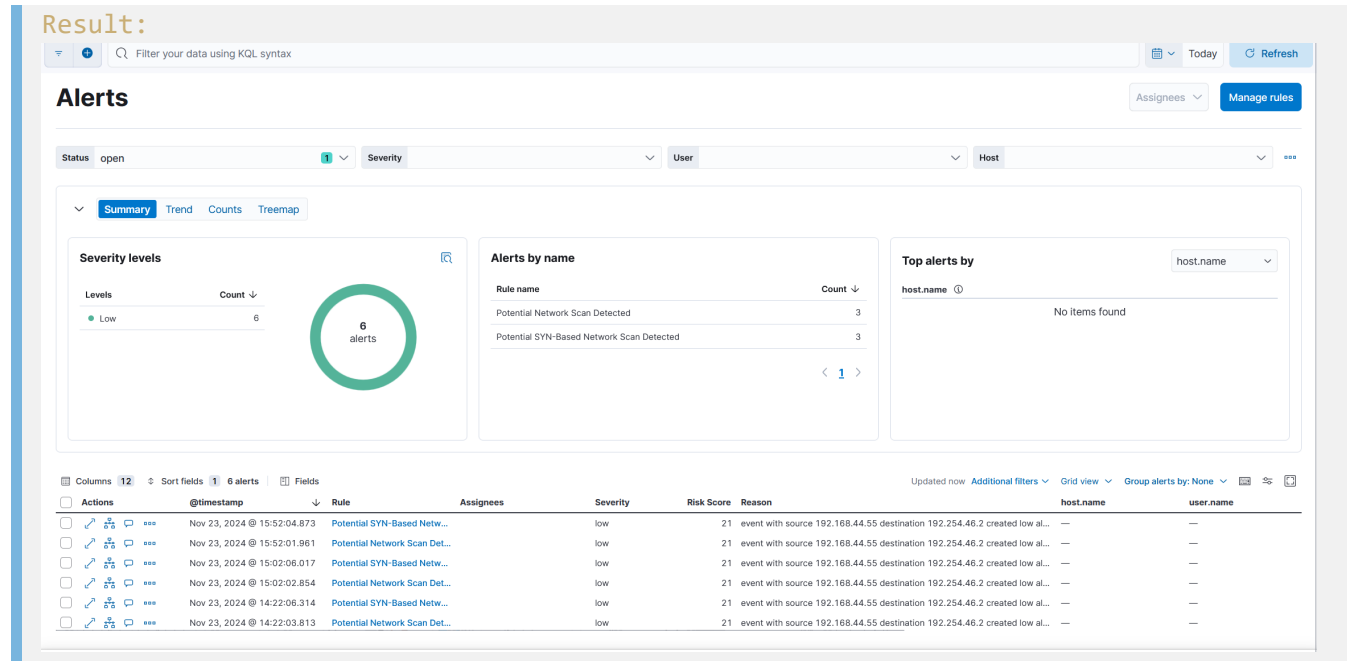
Link to fix: <https://www.elastic.co/guide/en/security/current/detections-permissions-section.html> .

Install and enable two rule "Potential SYN-Based Network Scan detected" and "Potential Network Scan detected"

Demo by pingint from kali linux vm to an ubuntu server:

```
(satan@kali)-[~]
$ sudo nmap 192.254.46.2
[sudo] password for satan:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 00:47 PST
Nmap scan report for 192.254.46.2
Host is up (0.00087s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```



There are some necessary command that I have learn:

```
ss -tuln | grep -E ':443|:9001'
```

to check whether those port is opening or not.

edit file: /etc/rsyslog.conf to open collect log at port 9001

```
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
module(load="imudp") # Load the UDP module
input(type="imudp" port="9001") # Listen on UDP port 9001
```

firewall@forwarder:/var/log\$ tail -n 10 syslog

use this to see newest log

Setup pfsense

1. Install iso disk from the netgate page.
2. Then cofigure vmnet host-only in vmare.
3. The wan interface will receive internet through the real machine. Unable dhcp in all interfaces, we can enable them later.
4. There will be 2 LAN network.
5. From pfsense, send logs to elk.
6. Navigate to Status/System Logs/ Settings.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / System Logs / Settings

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages **Settings**

General Logging Options

Log Message Format syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps)
The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled). Changing this value will only affect new log messages.

Forward/Reverse Display ☒ Show log entries in reverse order (newest entries on top)

GUI Log Entries 500
This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.

Log firewall default blocks ☒ Log packets matched from the default block rules in the ruleset
Log packets that are blocked by the implicit default block rule. - Per-rule logging options are still respected.

☐ Log packets matched from the default pass rules put in the ruleset
Log packets that are allowed by the implicit default pass rule. - Per-rule logging options are still respected.

☒ Log packets blocked by 'Block Bogon Networks' rules

☒ Log packets blocked by 'Block Private Networks' rules

Web Server Log ☒ Log errors from the web server process
If this is checked, errors from the web server process for the GUI or Captive Portal will appear in the main system log.

Raw Logs ☐ Show raw filter logs
If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information, but it is more difficult to read.

Where to show rule descriptions Display as column
Show the applied rule description below or in the firewall log rows. Displaying rule descriptions for all lines in the log might affect performance with large rule sets.

Local Logging ☐ Disable writing log files to the local disk

- Change Log message format to syslog.
- Enable send log to remote syslog server
- Enter ip address of remote syslog host and port, here choose another elastic agent as remote syslog server and ports for sending logs are: 443,9001, 5601 and then select send everything.
- Edit pfsense intergration.

elastic

Integrations > pfSense > pfSense-1

[Cancel](#)

Edit pfSense integration

Modify integration settings and deploy changes to the selected agent policy.

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

Integration name pfSense-1

Description Optional

[Advanced options](#)

☒ **Collect pfSense logs (input: udp)** [Change defaults](#)

☒ pfSense syslog logs [Technical preview](#)
Collect pfSense logs using udp input

Syslog Host 100.127.97.126
The interface to listen to UDP based syslog traffic. Set to 0.0.0.0 to bind to all available interfaces.

Syslog Port 9001
The UDP port to listen for syslog traffic. Ports below 1024 require Filebeat to run as root.

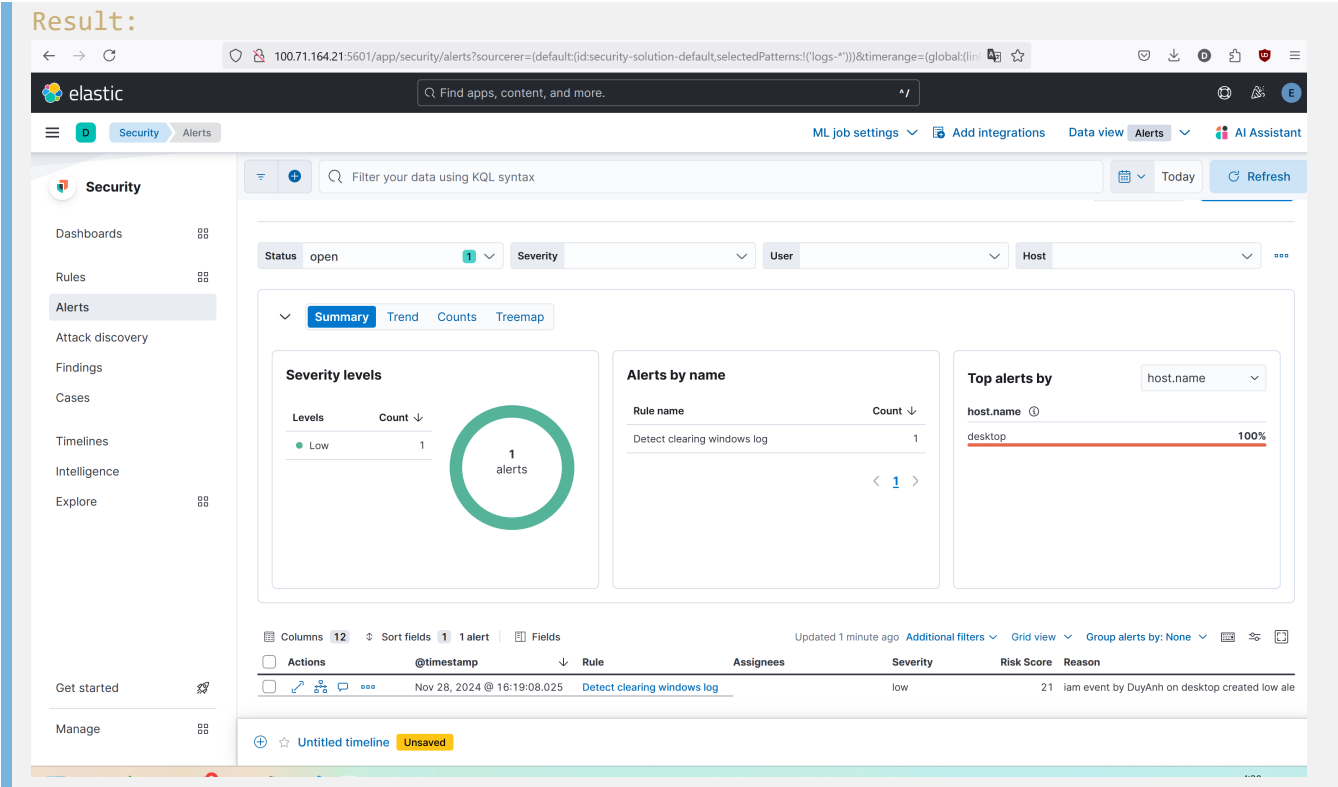
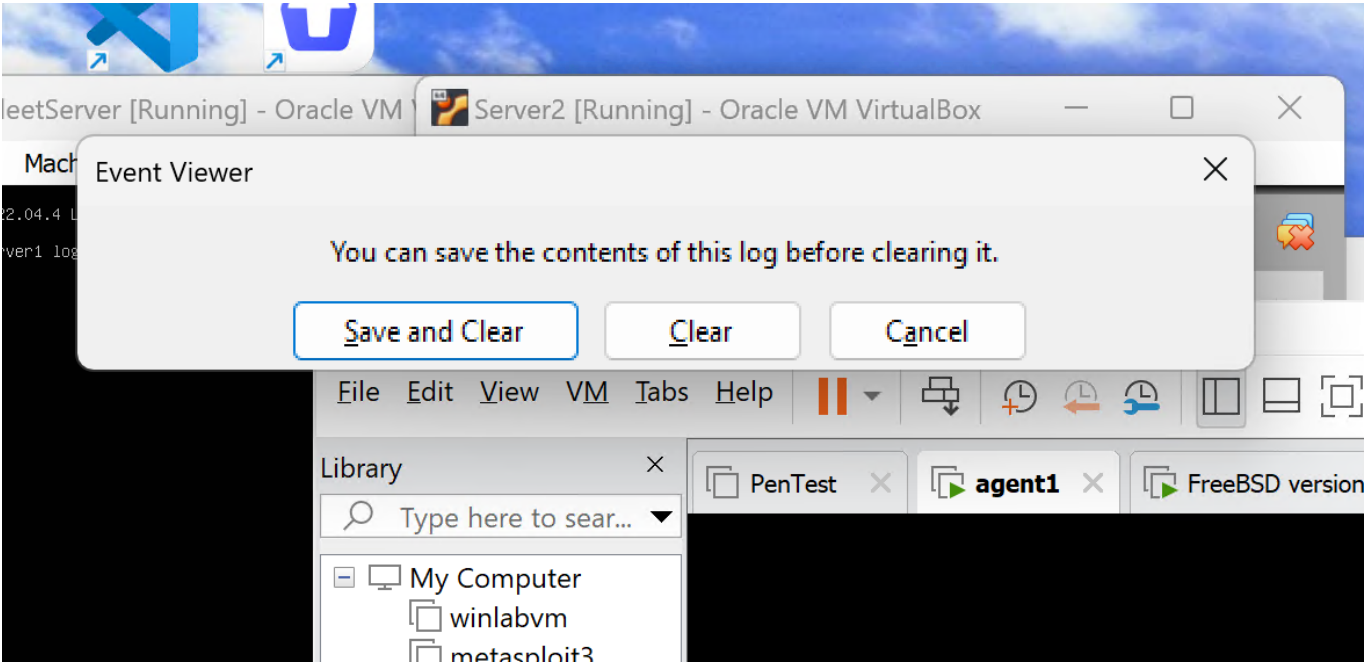
Internal Networks private Optional

[Add row](#)
The internal IP subnet(s) of the network.

Timezone Offset local

Rules detection in some usecases

1. Detect clearing Windows log.



Set the rule so that it will alert when event.log = "1102"

Index patterns

apm-*-transaction* ×

auditbeat-* ×

endgame-* ×

filebeat-* ×

logs-* ×

packetbeat-* ×

traces-apm* ×

winlogbeat-* ×

elastic-cloud-logs- ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query

Import query from saved timeline

+

event.code : "1102" and message : "audit log"

Suppress alerts by

Optional

Select a field

Select field(s) to use for suppressing extra alerts

☒ Per rule execution

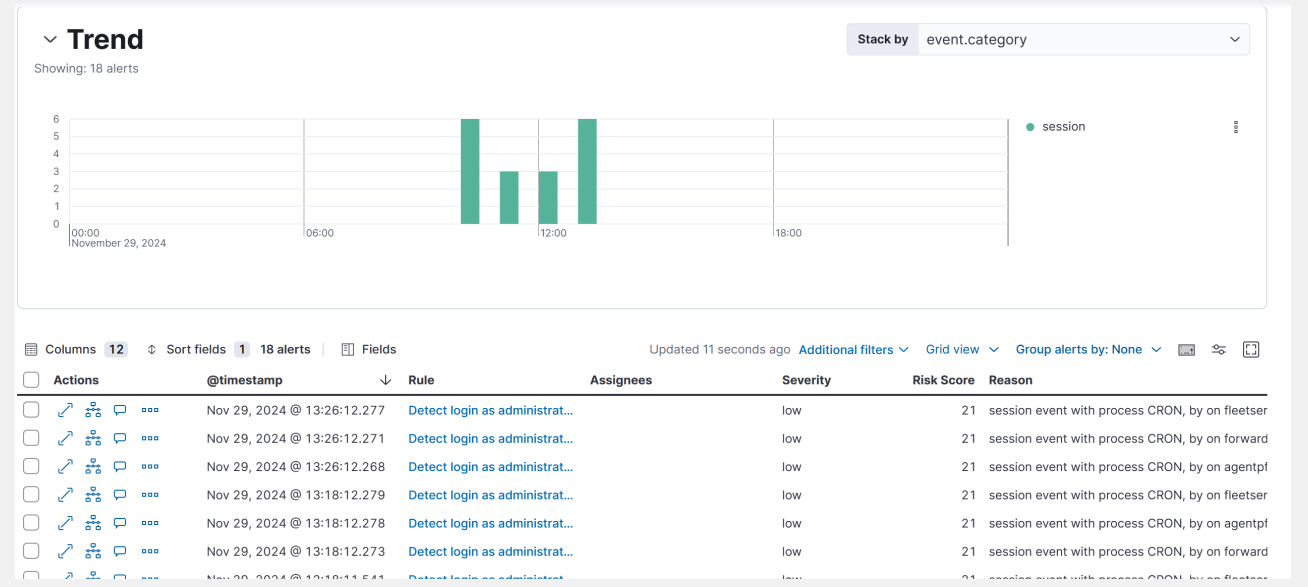
☐ Per time period

- Detect clearing Linux logs. Set the KQL query as: process.name: "rm" and process.args: ("-rf" or "-f" or "/var/log" or "/*.log")

Columns 12 Sort fields 1 1 alert Fields Updated 37 minutes ago Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
<div><input type="checkbox"/></div>	Nov 29, 2024 @ 10:53:21.972	Detect creating new user in...		low	21	iam event by DuyAnh on desktop created low ale

Result:



2. Detect adding new user.

- In Windows. Set rule to detect event ID :

Index Patterns

Data View

Index patterns

apm-*-transaction* ×

auditbeat-* ×

endgame-* ×

filebeat-* ×

logs-* ×

packetbeat-* ×

traces-apm* ×

winlogbeat-* ×

-*elastic-cloud-logs-* ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query

Import query from saved timeline

+

event.code : "4720"

×

Suppress alerts by

Optional

Select a field

Select field(s) to use for suppressing extra alerts

Result:

Columns 12 Sort fields 1 1 alert Fields Updated 37 minutes ago Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
<div>🔗 📄 🗨️ ⋮</div>	Nov 29, 2024 @ 10:53:21.972	Detect creating new user in...		low	21	iam event by DuyAnh on desktop created low ale

- In Linux.

apm-*-transaction* ×

auditbeat-* ×

endgame-* ×

filebeat-* ×

logs-* ×

packetbeat-* ×

traces-apm* ×

winlogbeat-* ×

-*elastic-cloud-logs-* ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query

Import query from saved timeline

+

log.file.path :"/var/log/auth.log" and message : "group added"

×

Set rule to detect log from auth.log file with message : "group added"

Result:

Columns 12 Sort fields 1 2 alerts Fields Updated now Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
<div>🔗 📄 🗨️ ⋮</div>	Nov 28, 2024 @ 17:18:24.877	Detect create new user.		low	21	iam event with process groupadd, on agentpfser
<div>🔗 📄 🗨️ ⋮</div>	Nov 28, 2024 @ 17:18:24.875	Detect create new user.		low	21	iam event with process groupadd, on agentpfser

3. Detect login as administrator.

- In linux
 - Setup the custom query: log.file.path :"/var/log/auth.log" and message : "user root" and message : "opened"

Result:

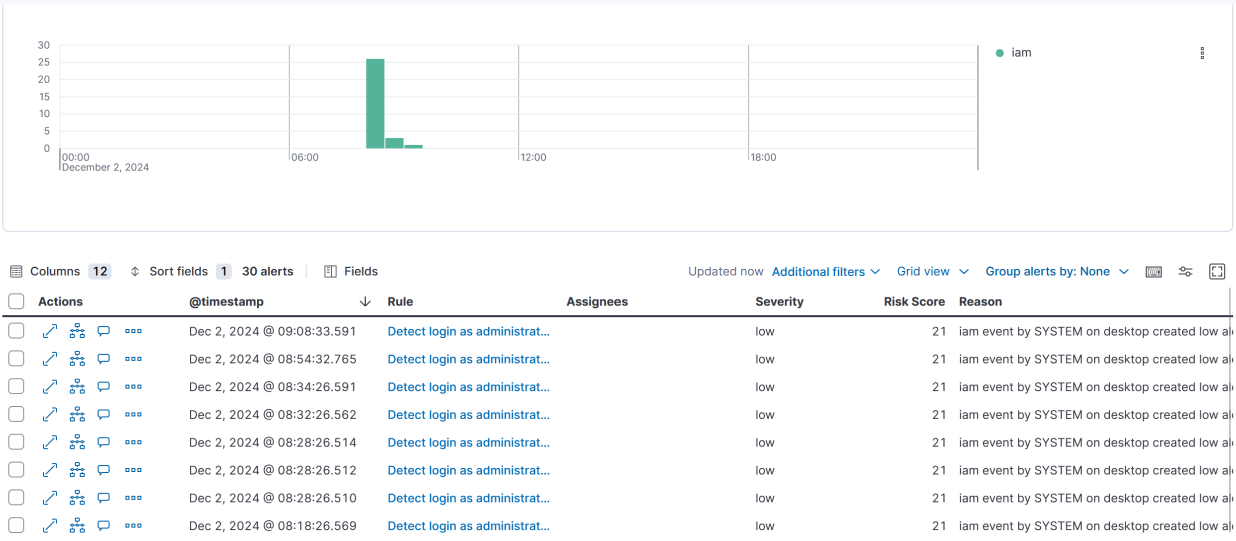
Columns 12 Sort fields 1 1 alert Fields Updated 37 minutes ago Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
<div>🔗 📄 🗨️ ⋮</div>	Nov 29, 2024 @ 10:53:21.972	Detect creating new user in...		low	21	iam event by DuyAnh on desktop created low ale

- In Windows:

- Setup the custom query: event.code : "4672" and message : "Special privileges assigned to new logon"

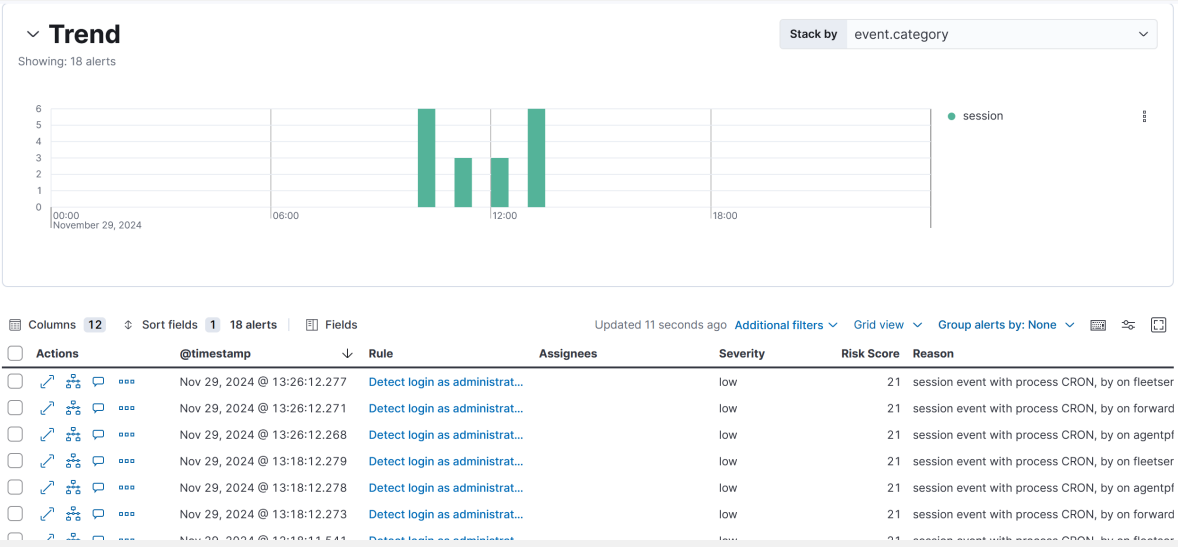
Result:



4. Detect suspicious outbound traffic.

- Setup the custom query: network.protocol : "tls"

Result:



5. Monitor for activities such as brute force by login by malware.

- Set the query: log.file.path : "/var/log/auth.log" and message : "user root" and message : "opened"

▼

Define rule

Edit

Index patterns

apm-*transaction*

auditbeat-*

endgame-*

filebeat-*

logs-*

packetbeat-*

traces-apm*

winlogbeat-*

-*elastic-cloud-logs-*

Custom query

log.file.path :"/var/log/auth.log" and message : "user root" and message : "opened"

Rule type

Threshold

Timeline template

None

Threshold

All results >= 5

This alert will be triggered when there are more than 5 login attempt, here we cannot set during any time period due to lack of license.

Some good reference.

- 1. <https://discuss.elastic.co/t/new-install-error-setting-certificate-verify-locations/307455>
- 2. <https://www.elastic.co/guide/en/elastic-stack/8.13/installing-stack-demo-self.html#install-stack-self-elasticsearch-first>
- 3. PFSENSE - ELASTIC: <https://www.elastic.co/docs/current/integrations/pfsense>
- 4.