Project Report: Elastic Stack Deployment & Security Monitoring

Submitted by: Ganesh Chandrabhan Shelke
Submitted to: CyberNX Technologies Pvt. Ltd.
Date of Submission: 28-03-2025

As per the assignment guidelines provided by CyberNX Technologies, I am pleased to submit my project report on **"Deployment of Elastic Stack for Security Monitoring"**. This report documents the successful completion of the following tasks:

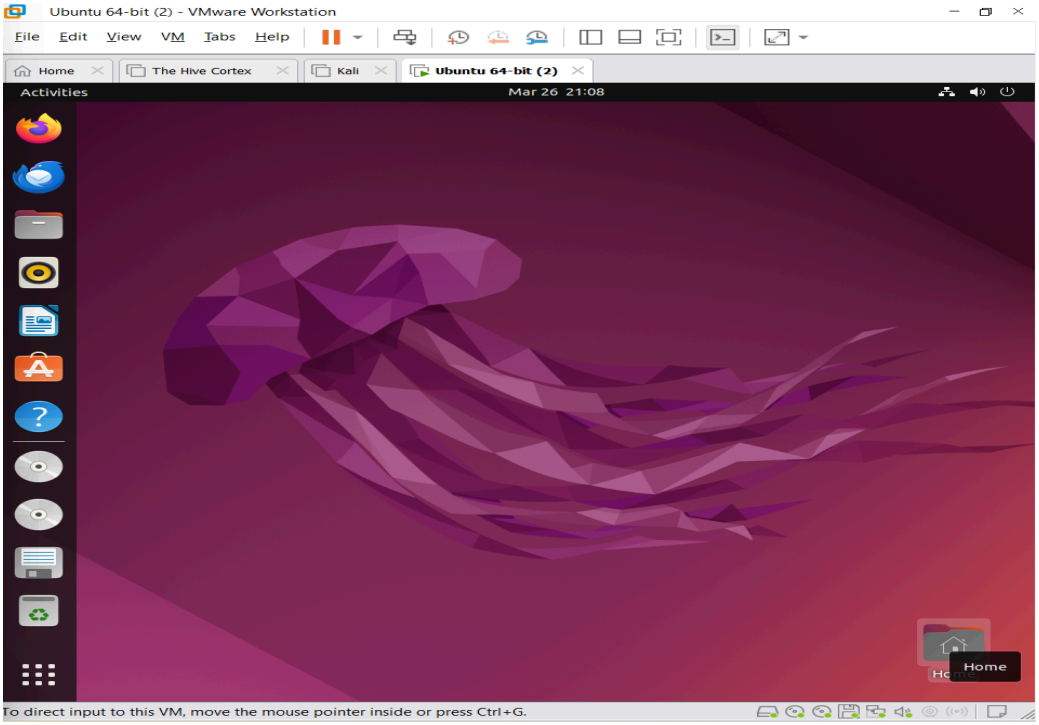
1. **Single-node Elasticsearch deployment** on a local VM.
2. **Kibana installation and integration** with Elasticsearch.
3. **Fleet Server deployment** for centralized agent management.
4. **Windows system log collection** using Fleet-managed Elastic Agents.
5. **System metrics monitoring** (CPU, Memory, Storage) for Windows/Linux.
6. **Detection rule creation** for monitoring Windows logon events (successful/failed).

Technical Environment

Component	Details
Elasticsearch	Single-node v8.x (on Ubuntu VM)
Kibana	v8.x (Elasticsearch)
Fleet Server	Deployed on the same VM
Agents	Fleet-managed (Windows host)
Detection Rules	Custom KQL queries for Event IDs

Installing Ubuntu OS for ELK Installation

Before installing the ELK stack, ensure you have a fresh installation of Ubuntu. Version of Ubuntu 20.04

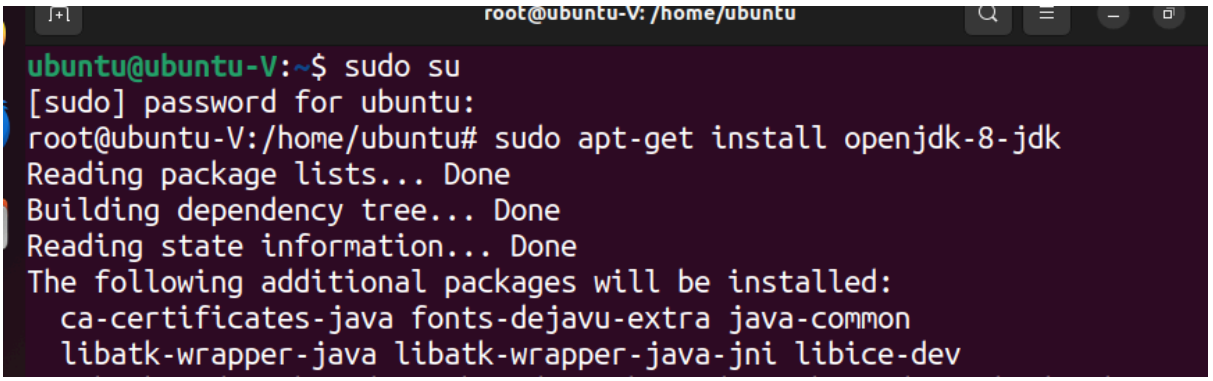


Installing Dependencies

Java for the ELK Stack

The ELK stack requires Java to function correctly. Install OpenJDK 17 using the command:

sudo apt-get install openjdk-17-jdk



Installing NGINX

NGINX acts as a web server and a proxy server. It helps set up password-protected access to the Kibana dashboard.
Command:
sudo apt-get install nginx

```
Setting up libxt-dev:amd64 (1:1.2.1-1) ...
root@ubuntu-V:/home/ubuntu# sudo apt-get install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream
  libnginx-mod-stream-geoip2 nginx-common nginx-core
```

Elasticsearch Setup

Adding Elastic Library

The ELK Stack components are available through official Elastic repositories. These repositories provide access to the latest packages and updates.

Import the GPG key

wget -qO — https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

```
root@ubuntu-V:/home/ubuntu# wget -qO - https://artifacts.elastic.co/GPG-
KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsea
rch-keyring.gpg
root@ubuntu-V:/home/ubuntu#
```

Installing the apt-transport-https package

sudo apt-get install apt-transport-https

```
root@ubuntu-V:/home/ubuntu# sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Help ing state information... Done
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,510 B of archives.
After this operation, 170 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 a
pt-transport-https all 2.4.13 [1,510 B]
```

Add the Elastic repository to your system

echo “deb https://artifacts.elastic.co/packages/7.x/apt stable main” | sudo tee –a /etc/apt/sources.list.d/elastic-7.x.list

```
Setting up apt-transport-https (2.4.13) ...
root@ubuntu-V:/home/ubuntu# echo “deb https://artifacts.elastic.co/packa
ges/7.x/apt stable main” | sudo tee -a /etc/apt/sources.list.d/elastic-7
.x.list
“deb https://artifacts.elastic.co/packages/7.x/apt stable main”
Show Applications V:/home/ubuntu#
```

Install Elasticsearch

sudo apt-get update

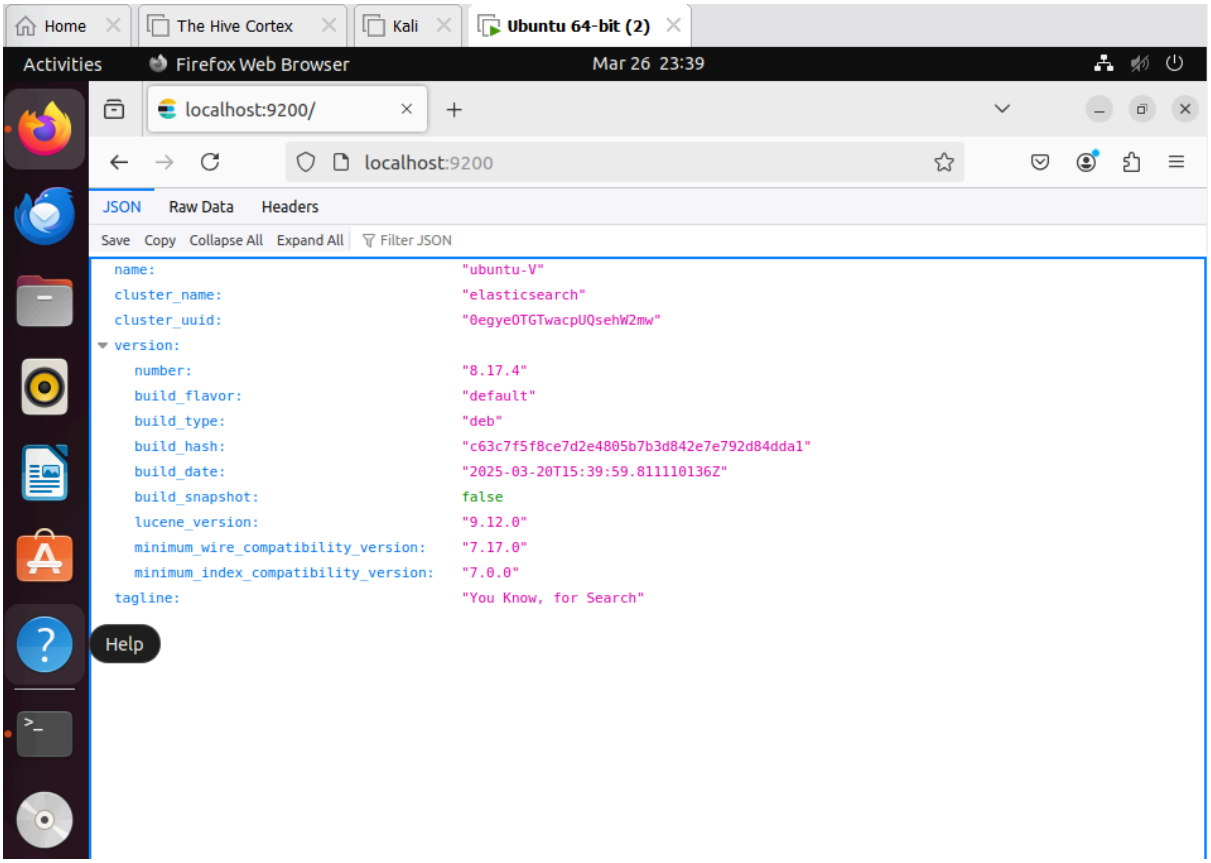
Install Elasticsearch using command

sudo apt-get install elasticsearch

```
tifacts.elastic.co/packages/8.x/apt stable main
root@ubuntu-V:/home/ubuntu# sudo apt-get update && sudo apt-get install
elasticsearch
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13
.7 kB]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [3,
248 B]
Hit:3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Err:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
  The following signatures couldn't be verified because the public key i
```

Elasticsearch service using this systemctl

sudo systemctl start elasticsearch.service
sudo systemctl enable elasticsearch.service



Install Kibana

Kibana serves as a user-friendly interface for analyzing and visualizing data.

Install Kibana

sudo apt-get install kibana

```
root@ubuntu-V: /home/ubuntu
root@ubuntu-V:/home/ubuntu# sudo apt-get install kibana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 343 MB of archives.
After this operation, 1,047 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 ki
bana amd64 8.17.4 [343 MB]
Fetched 343 MB in 1min 6s (5,160 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 205055 files and directories currently installed.)
Preparing to unpack .../kibana_8.17.4_amd64.deb ...
Unpacking kibana (8.17.4) ...
Setting up kibana (8.17.4) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For d
etails and instructions on how to disable see https://www.elastic.co/gui
de/en/kibana/8.17/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
root@ubuntu-V:/home/ubuntu#
```

```
root@ubuntu-VM:/home/ubuntu# /usr/share/elasticsearch/bin/elasticsearch-c
reate-enrollment-token -s kibana
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC4yMzguMTMxOjkyMDAiXSwiZmdyIjoiM
TQ2OTM3MzQ0ZGIxNDVkMDcxMWQ0MTUwNTcwNWEwZGRjNmE0MTllN2M2YzU1ZjM1ZjQ3YTFkOD
A0NGU5ODY0MyIsImtleSI6ImxCS2cxcFVCOURvUy1RT1BOcWZ1Ok00b3pIQmlzUkd5dlNrbld
vRFRSTVEifQ==
root@ubuntu-VM:/home/ubuntu# /usr/share/kibana/bin/kibana-setup
Native global console methods have been overridden in production environm
ent.
? Enter enrollment token: eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC4yMz
guMTMxOjkyMDAiXSwiZmdyIjoiMTQ2OTM3MzQ0ZGIxNDVkMDcxMWQ0MTUwNTcwNWEwZGRjNm
E0MTllN2M2YzU1ZjM1ZjQ3YTFkODA0NGU5ODY0MyIsImtleSI6ImxCS2cxcFVCOURvUy1RT1
BOcWZ1Ok00b3pIQmlzUkd5dlNrbldvRFRSTVEifQ==

✓ Kibana configured successfully.
```

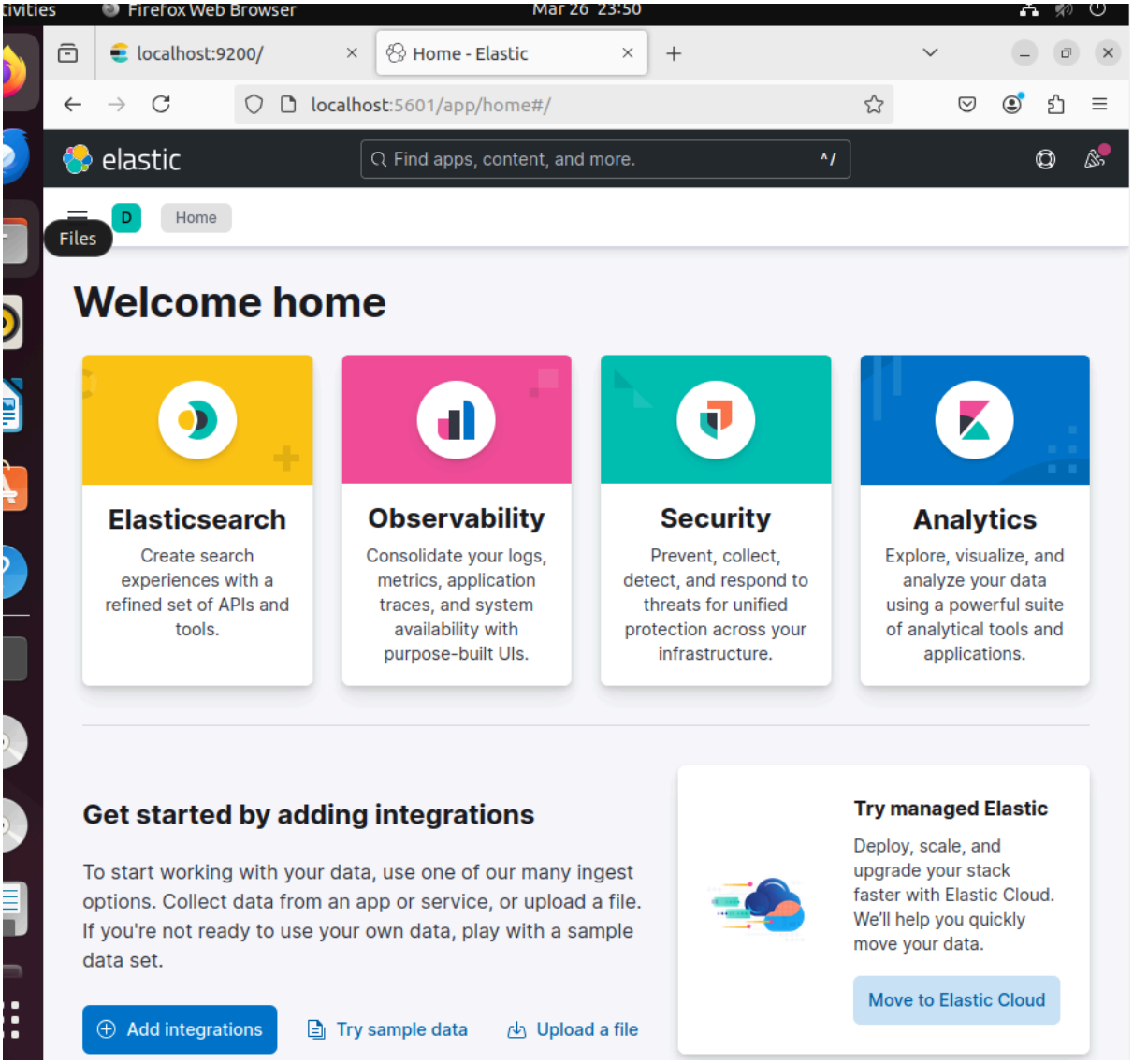
Once you have successfully installed Kibana, you can then configure it. open the kibana.yml file in your preferred text editor or Stay with default settings

sudo nano /etc/kibana/kibana.yml

Next start and enable Kibana.

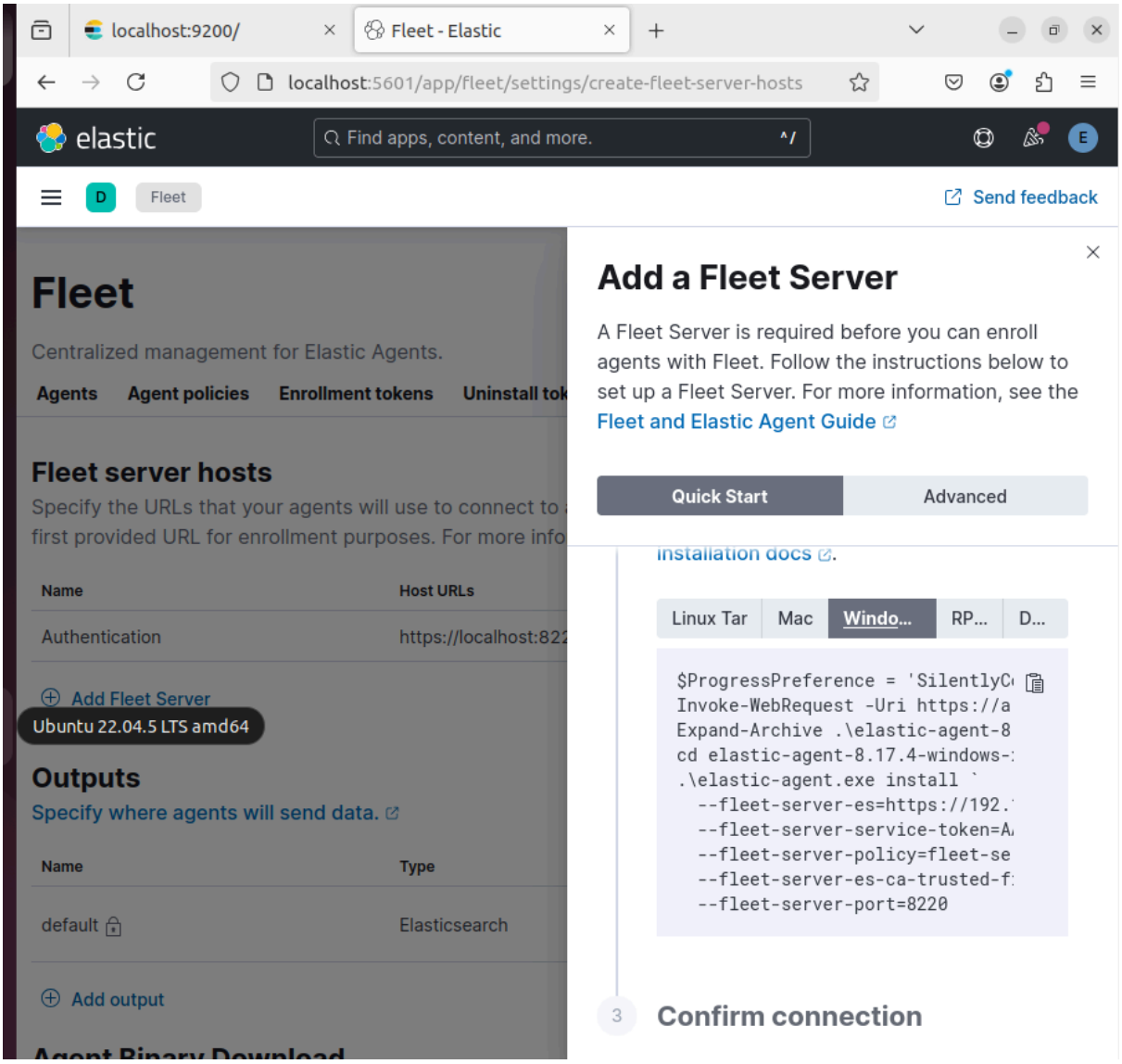
sudo systemctl start kibana
sudo systemctl enable kibana

Now Kibana is running



Adding The Fleet Server Agent

Fleet Server manages Elastic Agents, which collect and send data to Elasticsearch. Ensure that the Fleet Server is installed and running to collect system logs and security data.



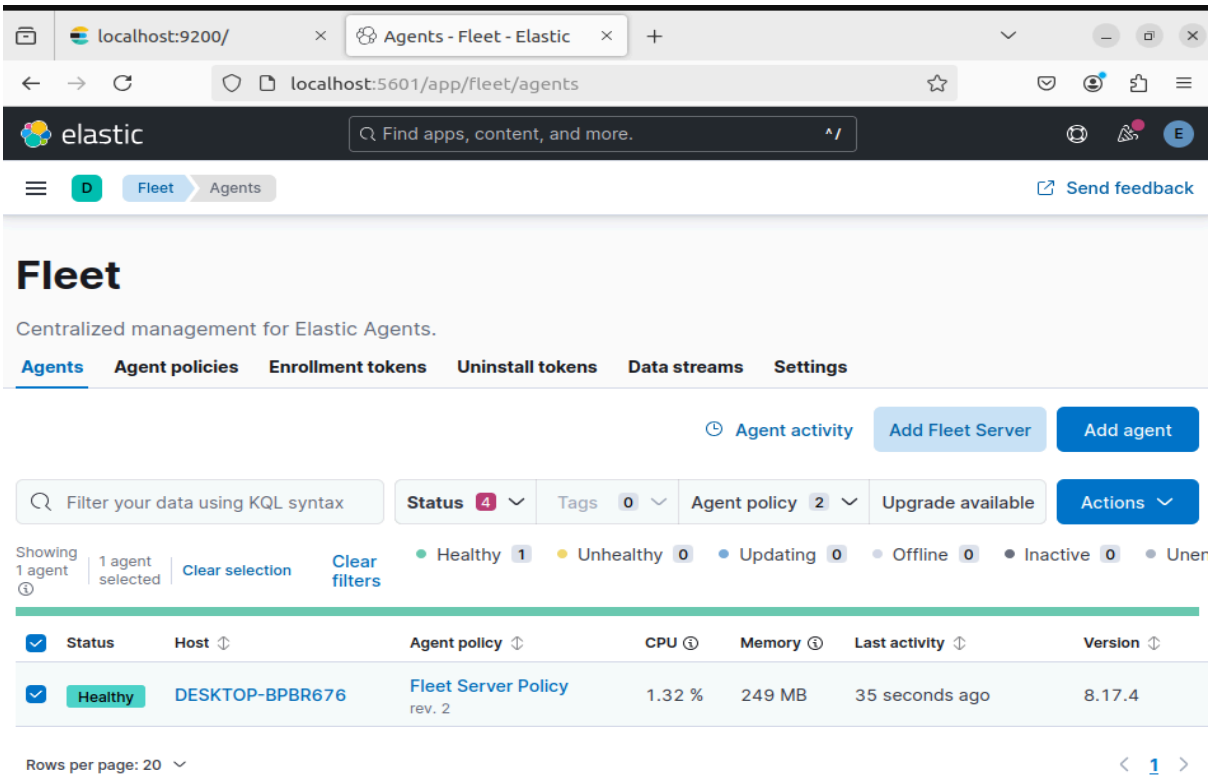
Installing Fleet agent into Windows System to get log in Kibana Dashboard.

Open Powershell in administrator mode and install agent.

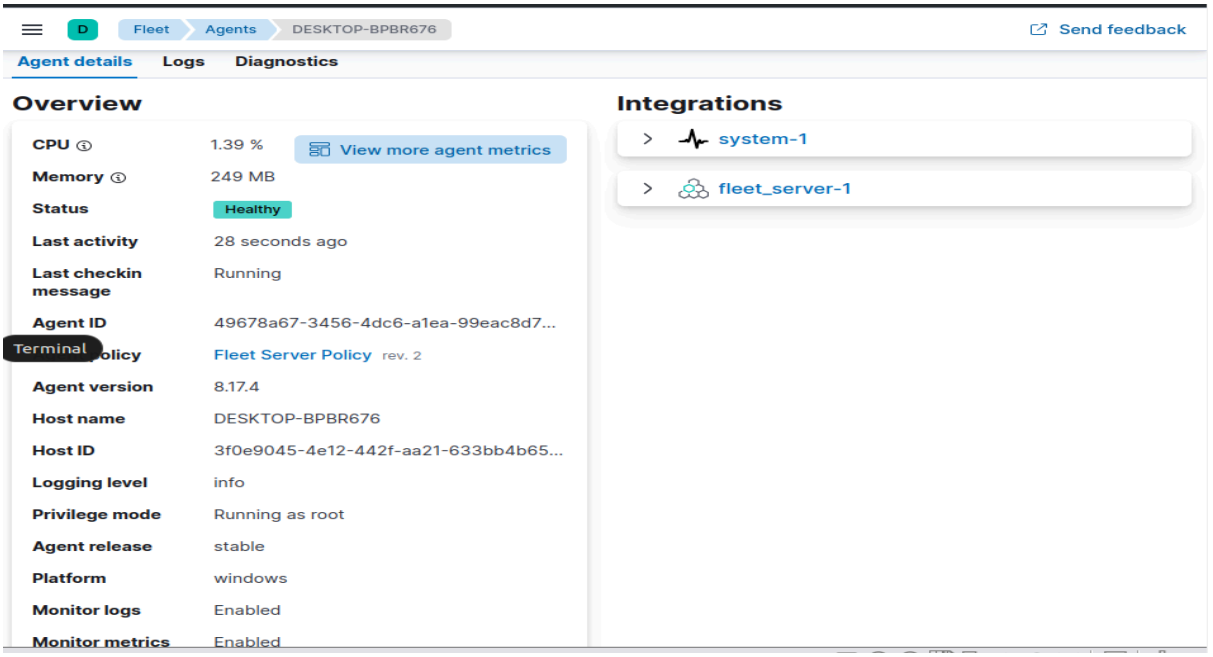
```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri
https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.
4-windows-x86_64.zip -OutFile elastic-agent-8.17.4-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.17.4-windows-x86_64.zip
cd elastic-agent-8.17.4-windows-x86_64
.\elastic-agent.exe install `
  --fleet-server-es=https://192.168.238.131:9200 `
--fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2Vyd
mVyL3Rva2VuLTE3NDMwNjcyMTA3NzM6bzIzSDNqc01RUzI3VHgw
S2VOZU5LUQ `
  --fleet-server-policy=fleet-server-policy `
--fleet-server-es-ca-trusted-fingerprint=146937344db145d0711d41505705
a0ddc6a419e7c6c55f35f47a1d8044e98643 `
  --fleet-server-port=8220
```

```
PS C:\> cd .\Agent\
PS C:\Agent> cd .\elastic-agent-8.17.4-windows-x86_64\
PS C:\Agent\elastic-agent-8.17.4-windows-x86_64> ls


    Directory: C:\Agent\elastic-agent-8.17.4-windows-x86_64


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        27-03-2025     14:32                data
d-----        27-03-2025     14:40                elastic-agent
-a----        27-03-2025     14:30             41 .build_hash.txt
-a----        27-03-2025     14:30             41 .elastic-agent.active.commit
-a----        27-03-2025     14:32       54682992 elastic-agent-8.17.4-windows-x86_64.zip
-a----        27-03-2025     14:30       60347448 elastic-agent.exe
-a----        27-03-2025     14:30          14829 elastic-agent.reference.yml
-a----        27-03-2025     14:30          12306 elastic-agent.yml
-a----        27-03-2025     14:40       71984368 elastic-agent.zip
-a----        27-03-2025     14:33              0 fleet.enc.lock
-a----        27-03-2025     14:30           3860 LICENSE.txt
-a----        27-03-2025     14:30            339 manifest.yaml
-a----        27-03-2025     14:30        5495943 NOTICE.txt
-a----        27-03-2025     14:30            807 otel.yml
-a----        27-03-2025     14:30             88 otelcol.ps1
-a----        27-03-2025     14:30              7 package.version
-a----        27-03-2025     14:30            351 README.md


PS C:\Agent\elastic-agent-8.17.4-windows-x86_64> .\elastic-agent.exe install `
>>   --fleet-server-es=https://192.168.238.131:9200 `
>>   --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3NDMwNjcyMTA3NzM6bzIzSDNqc01RUzI3V
HgwS2VOZU5LUQ `
>>   --fleet-server-policy=fleet-server-policy `
>>   --fleet-server-es-ca-trusted-fingerprint=146937344db145d0711d41505705a0ddc6a419e7c6c55f35f47a1d8044e98643
`
>>   --fleet-server-port=8220
>>
>>
```

Once Install Successfully the Fleet -> Agents status is must be **Healthy**

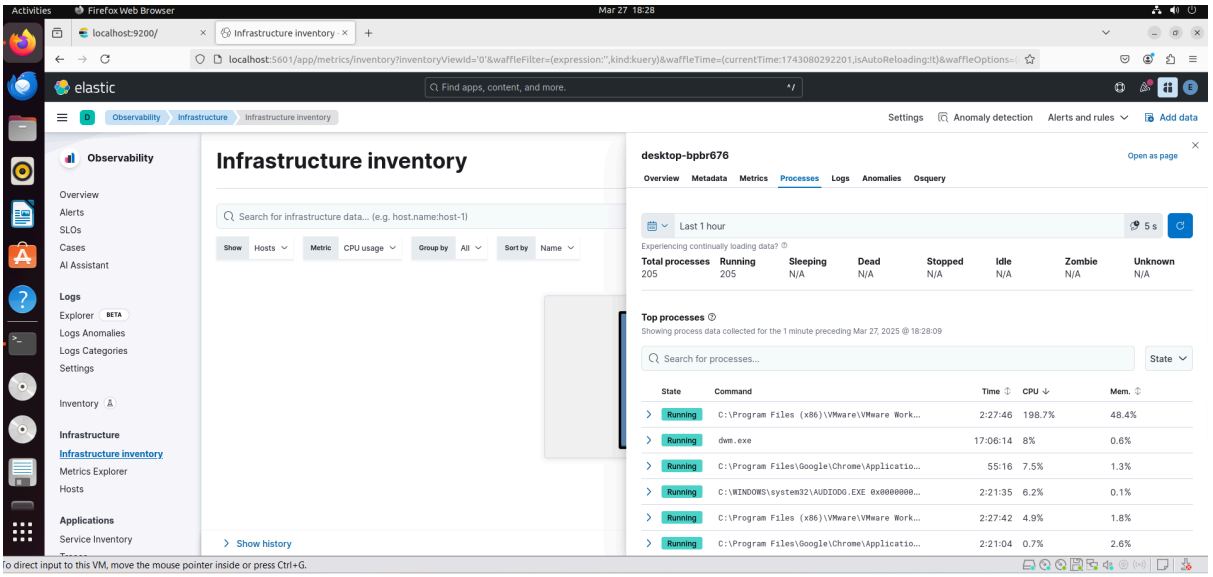


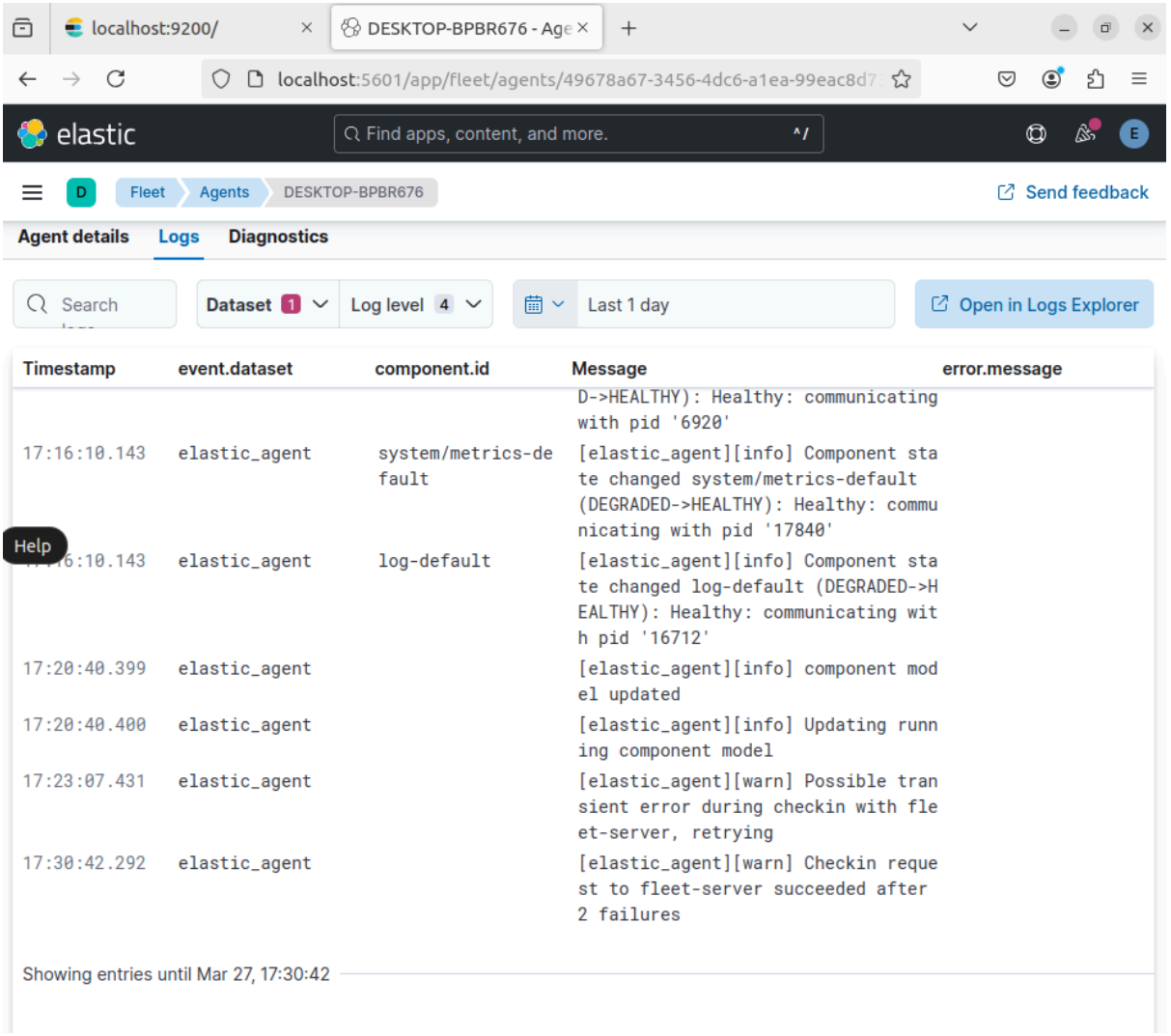
Agent Details



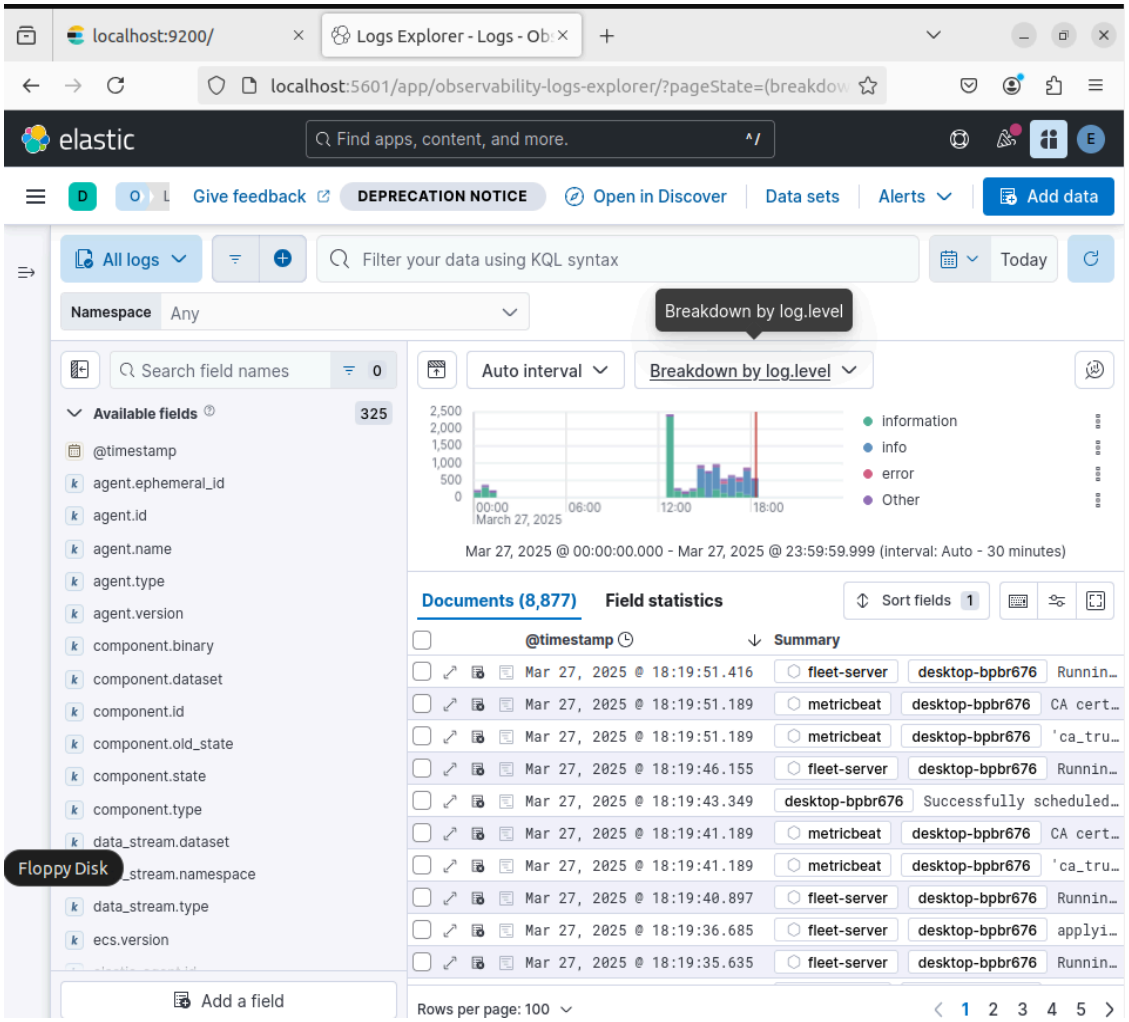
Successful Log Collection

System Logs

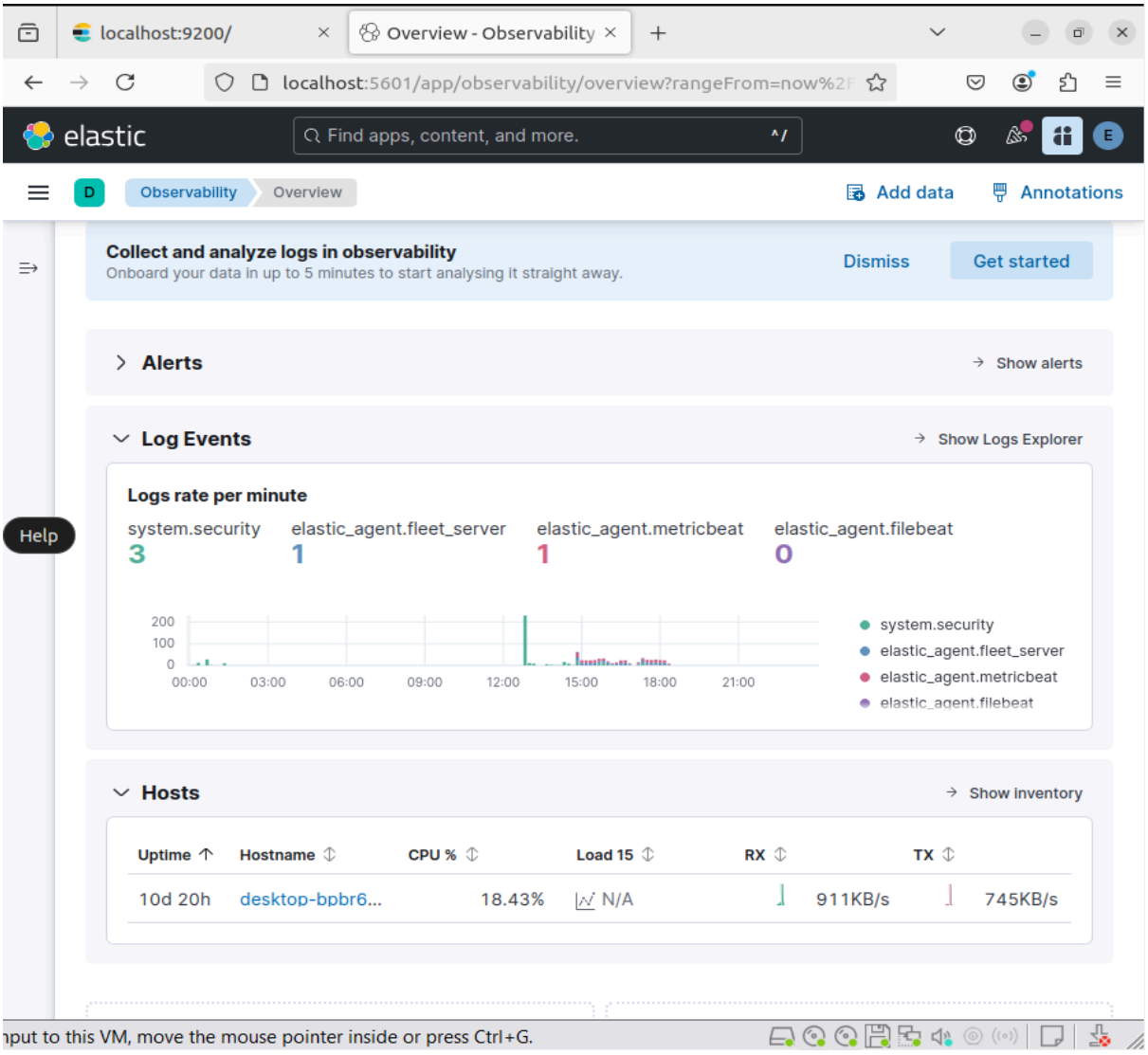




Observability -> Logs

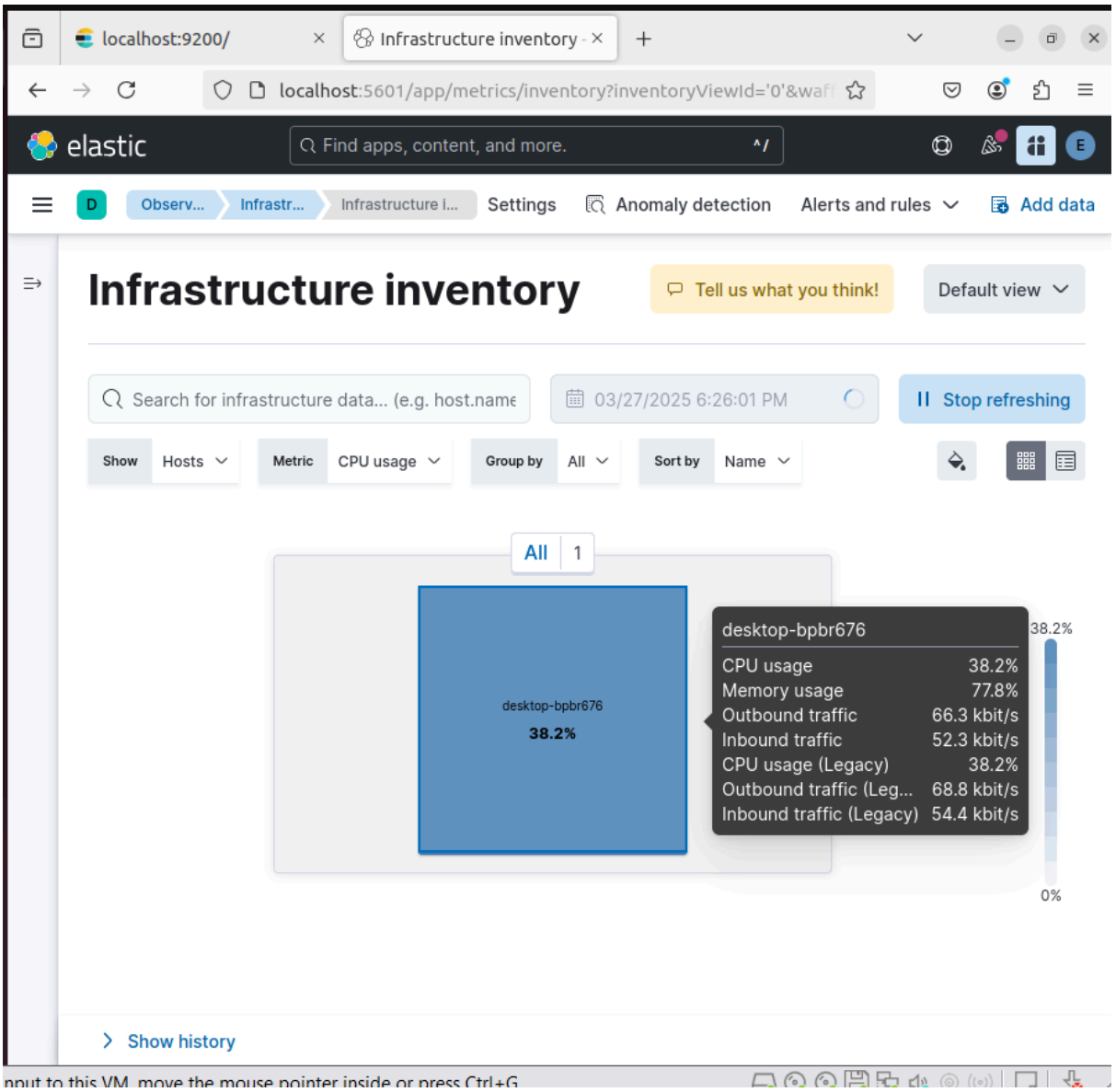


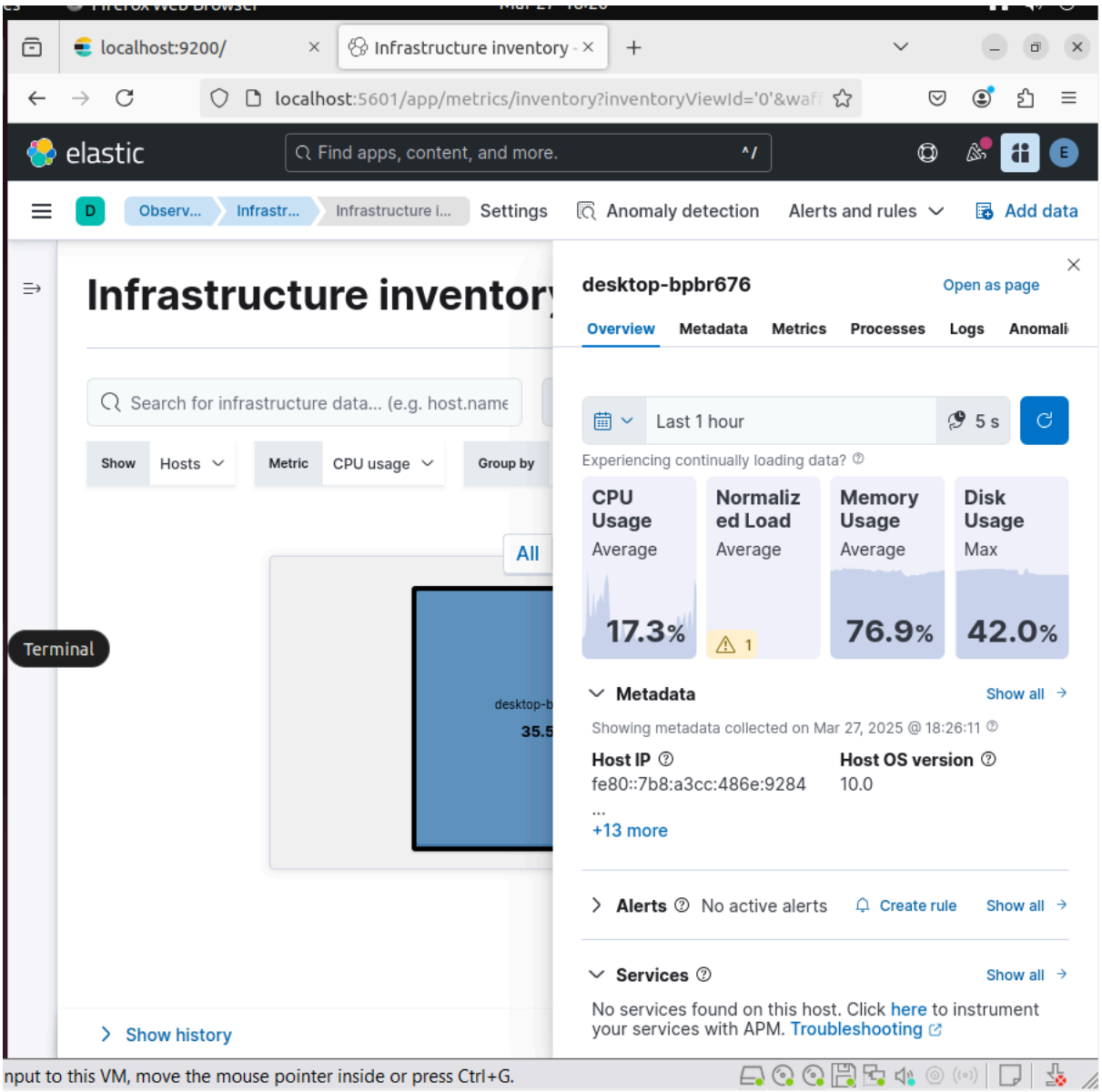
Observability -> Overview



CPU, Memory, Storage Analysis

Observability -> Infrastructure

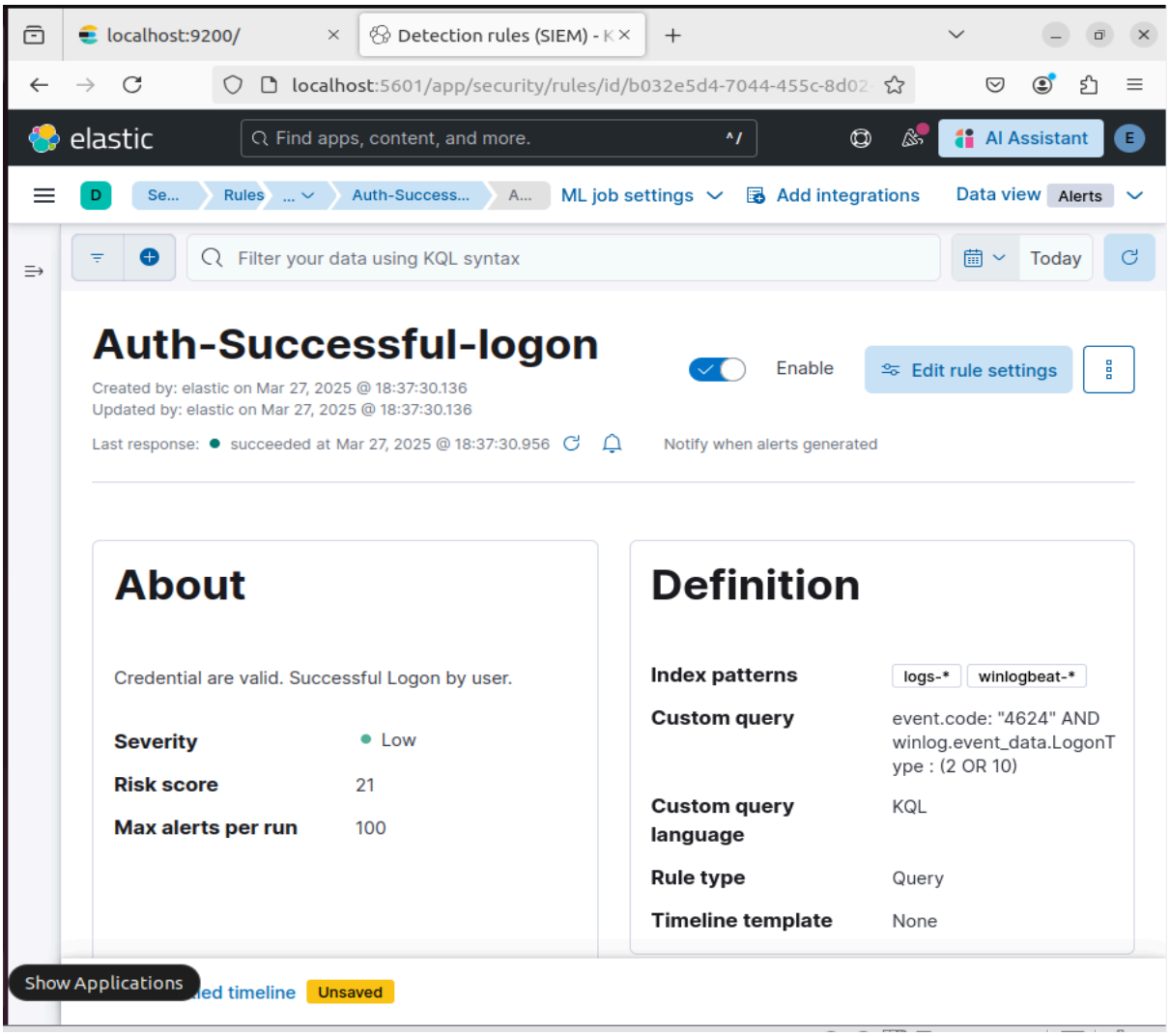



localhost:9200/
Infrastructure inventory
localhost:5601/app/metrics/inventory?inventoryViewId='0'&waf
elastic
Find apps, content, and more.
Observ...
Infrastr...
Infrastructure i...
Settings
Anomaly detection
Alerts and rules
Add data
Infrastructure inventor
Search for infrastructure data... (e.g. host.name
Show
Hosts
Metric
CPU usage
Group by
All
Terminal
desktop-b
35.5
Show history
desktop-bpbr676
Open as page
Overview
Metadata
Metrics
Processes
Logs
Anomali
Last 1 hour
5 s
Experiencing continually loading data?
CPU Usage
Average
17.3%
Normalized Load
Average
1
Memory Usage
Average
76.9%
Disk Usage
Max
42.0%
Metadata
Show all
Showing metadata collected on Mar 27, 2025 @ 18:26:11
Host IP
fe80::7b8:a3cc:486e:9284
...
+13 more
Host OS version
10.0
Alerts
No active alerts
Create rule
Show all
Services
Show all
No services found on this host. Click here to instrument your services with APM. Troubleshooting
nput to this VM, move the mouse pointer inside or press Ctrl+G.

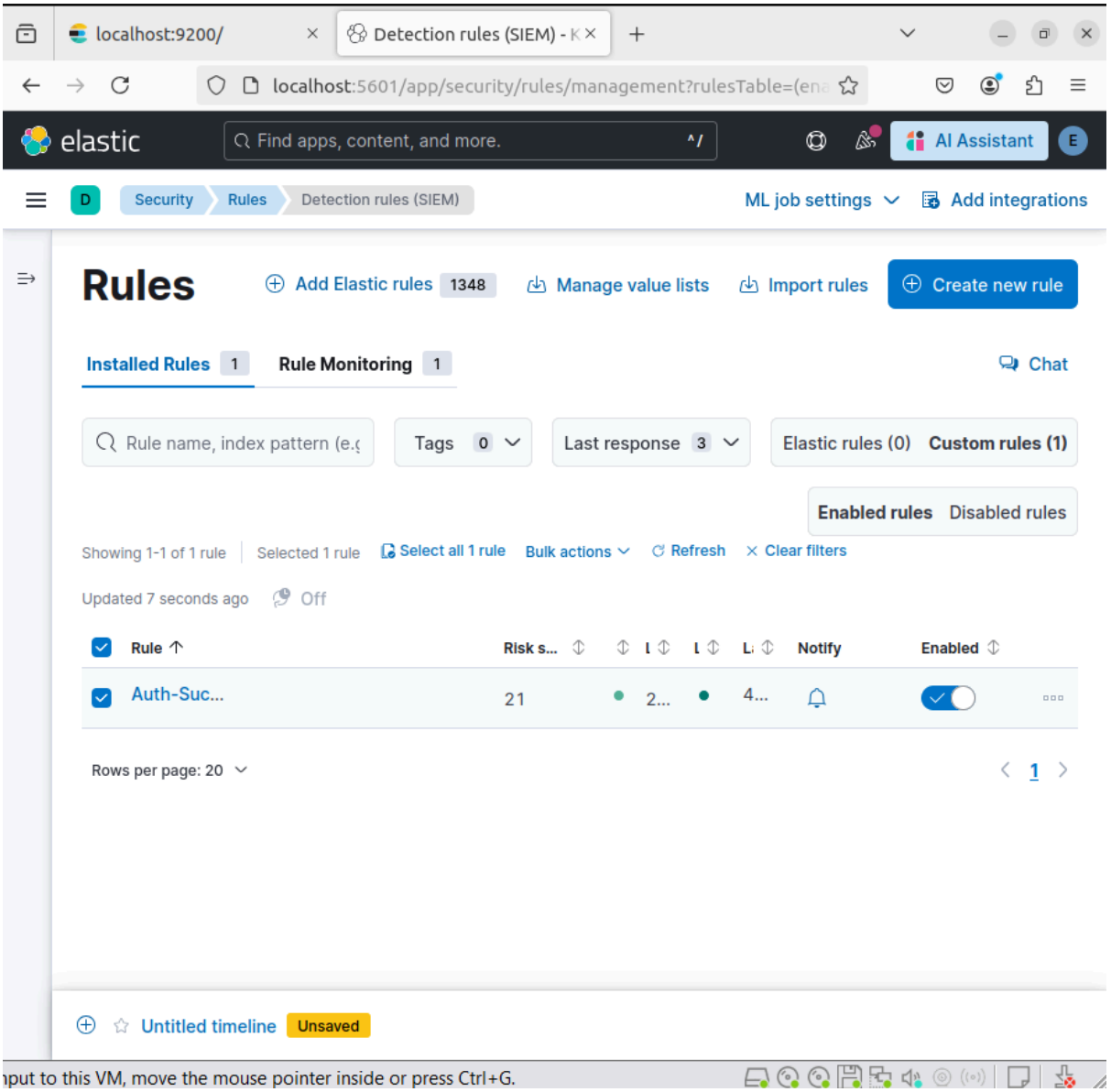
Security Log Rule Creation

Security -> rules -> Detection rules (SIEM)

Rule: 1 Successful Login

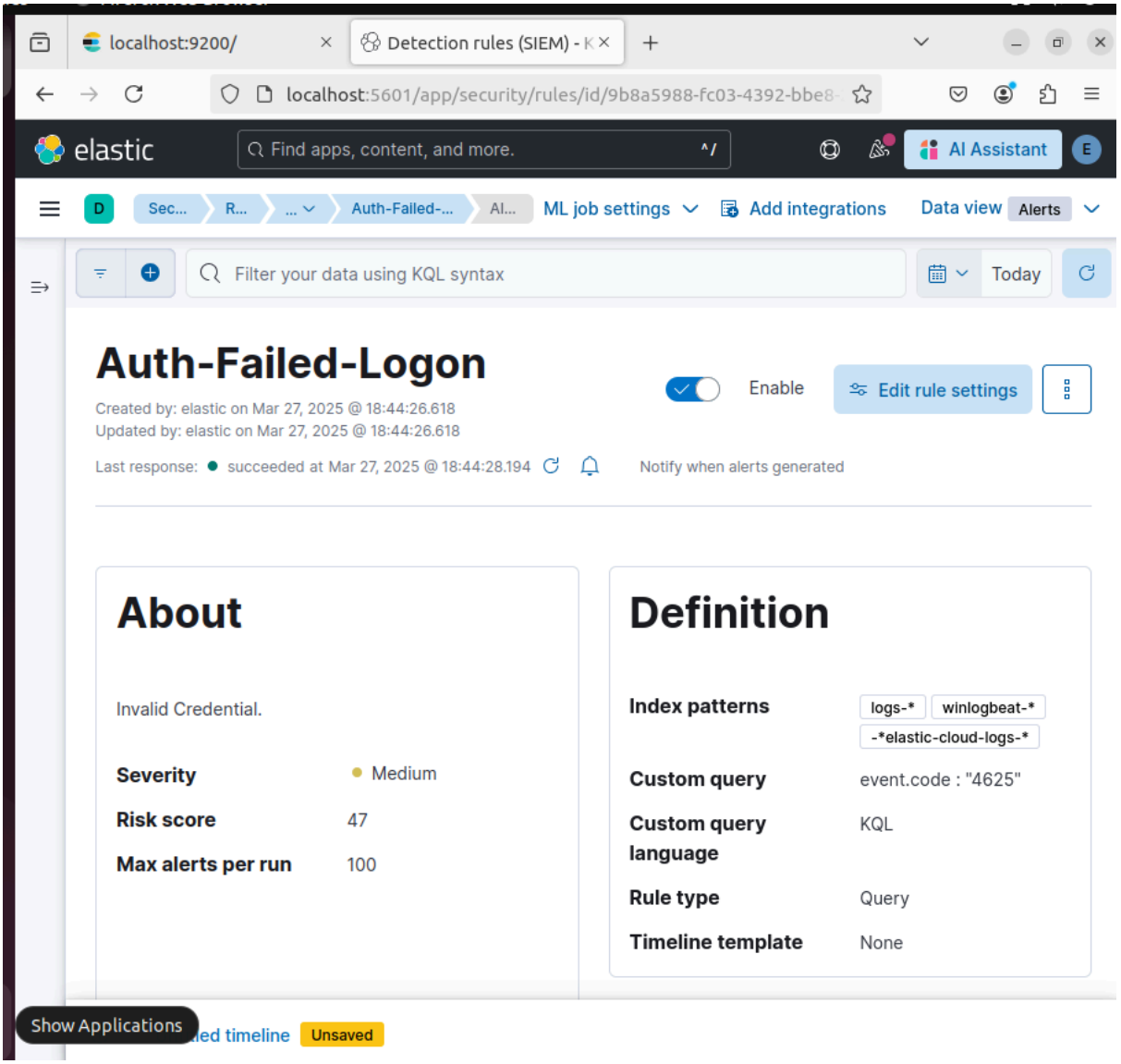


Rule Enabled



Rule: 2 Failed login

Rule Created



Rule Enabled