

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:

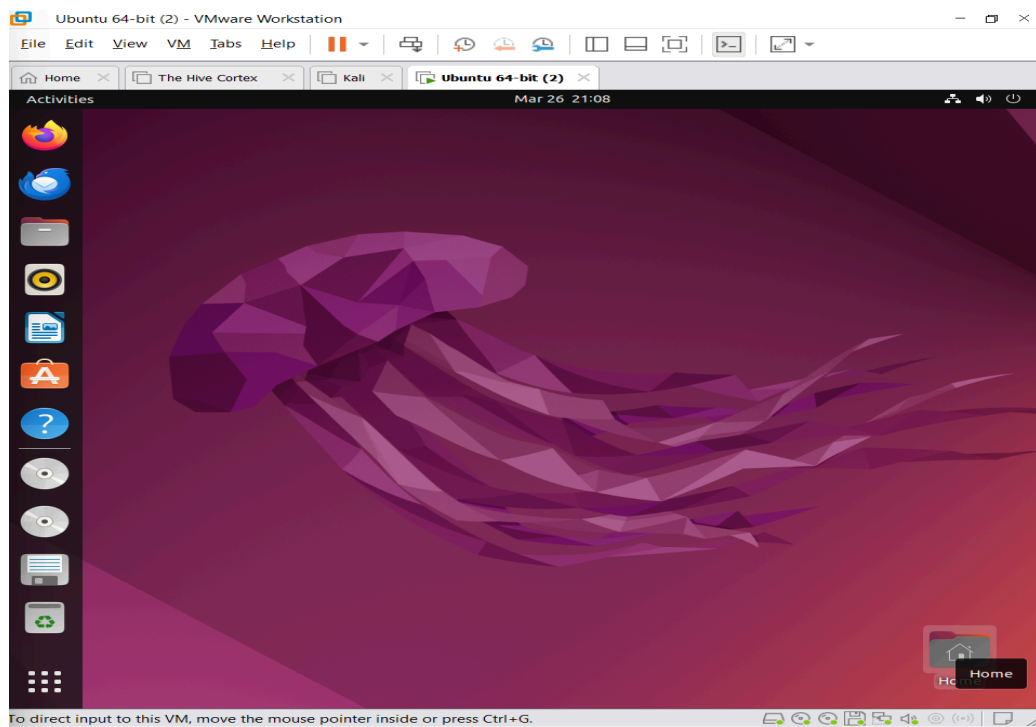
1. **Single-node Elasticsearch deployment** on a local VM.
2. **Kibana installation and integration** with Elasticsearch.
3. **Fleet Server deployment** for centralized agent management.
4. **Windows system log collection** using Fleet-managed Elastic Agents.
5. **System metrics monitoring** (CPU, Memory, 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
```

```
root@ubuntu-V: /home/ubuntu
ubuntu@ubuntu-V:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-V:/home/ubuntu# sudo apt-get install openjdk-8-jdk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-java fonts-dejavu-extra java-common
  libatk-wrapper-java libatk-wrapper-java-jni libice-dev
```

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 ttbxt-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
Reading 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

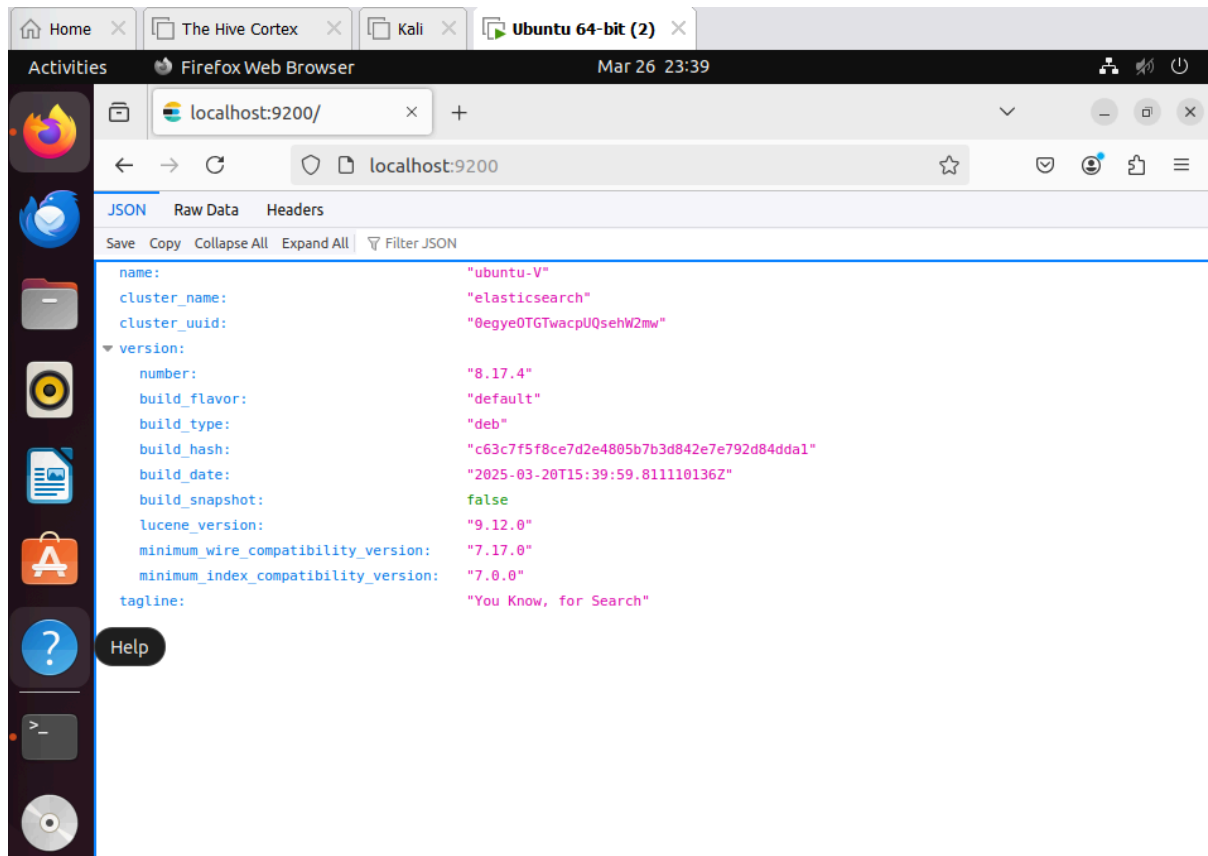
sudo apt-get install elasticsearch

```
https://artifacts.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 is
```

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
create-enrollment-token -s kibana
eyJ2ZXIiOiI4LjE0LjAiaLCJhZHIIoIsImTkyLjE2OC4yMzguMTxOjkyMDAiXSwiZmdyIjoim
TQ2OTM3MzQ0ZGIXNDVkdMDcxMWQ0MTUwNTcwNWEwZGRjNmE0MTlN2M2YzU1ZjM1ZjQ3YTfkOD
A0NGU5ODY0MyIsImtleSI6ImxCS2cxcFVCOURvUy1RT1B0cWZ10k00b3pIQmlzUkd5dlnRblld
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: eyJ2ZXIiOiI4LjE0LjAiaLCJhZHIIoIsImTkyLjE2OC4yMz
guMTxOjkyMDAiXSwiZmdyIjoimTQ2OTM3MzQ0ZGIXNDVkdMDcxMWQ0MTUwNTcwNWEwZGRjNm
E0MTlN2M2YzU1ZjM1ZjQ3YTfkODA0NGU5ODY0MyIsImtleSI6ImxCS2cxcFVCOURvUy1RT1
B0cWZ10k00b3pIQmlzUkd5dlnRblldVRFRSTVEifQ==
✓ 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

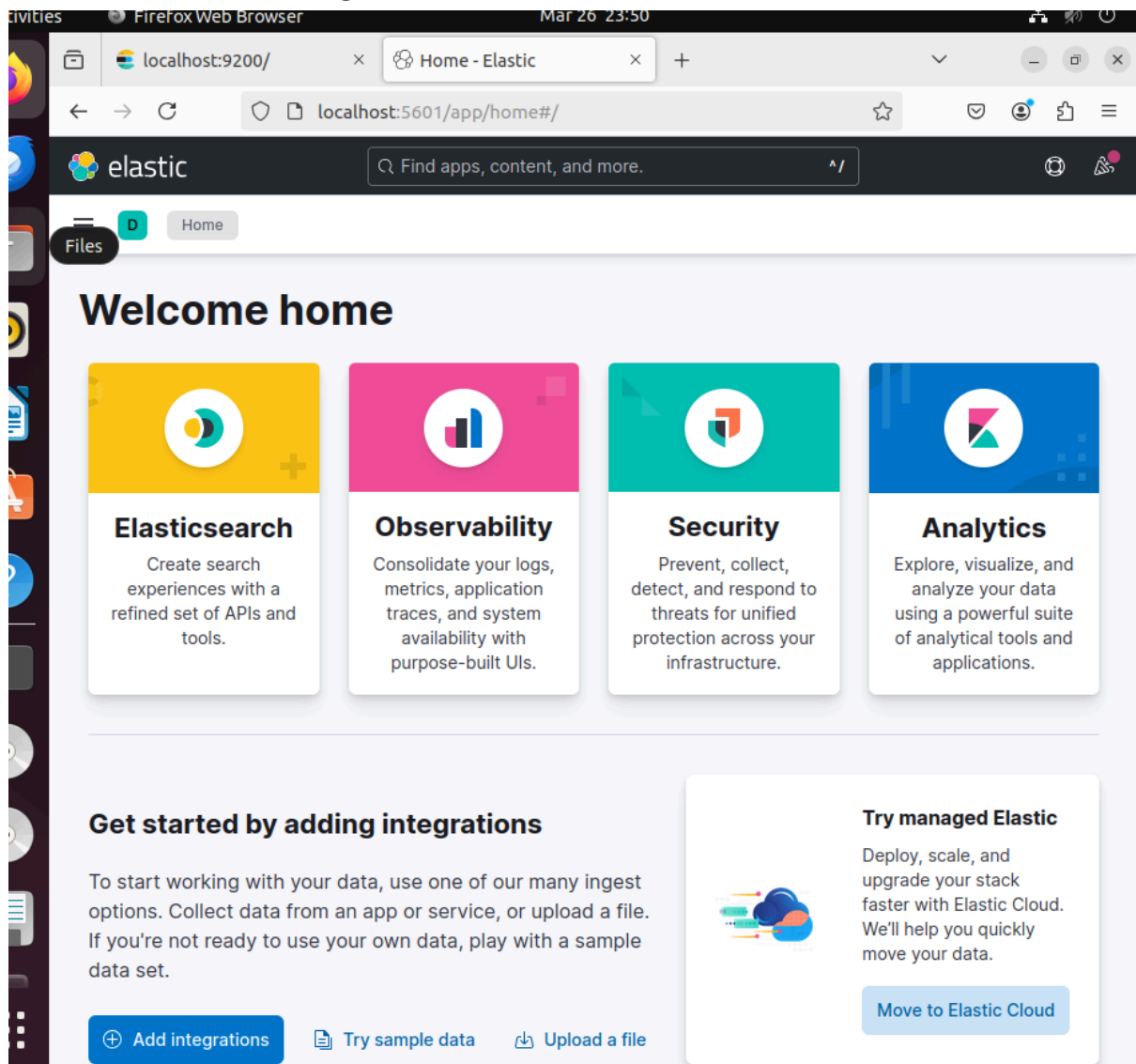
```
# sudo nano /etc/kibana/kibana.yml
```

Next start and enable Kibana.

```
# sudo systemctl start kibana
```

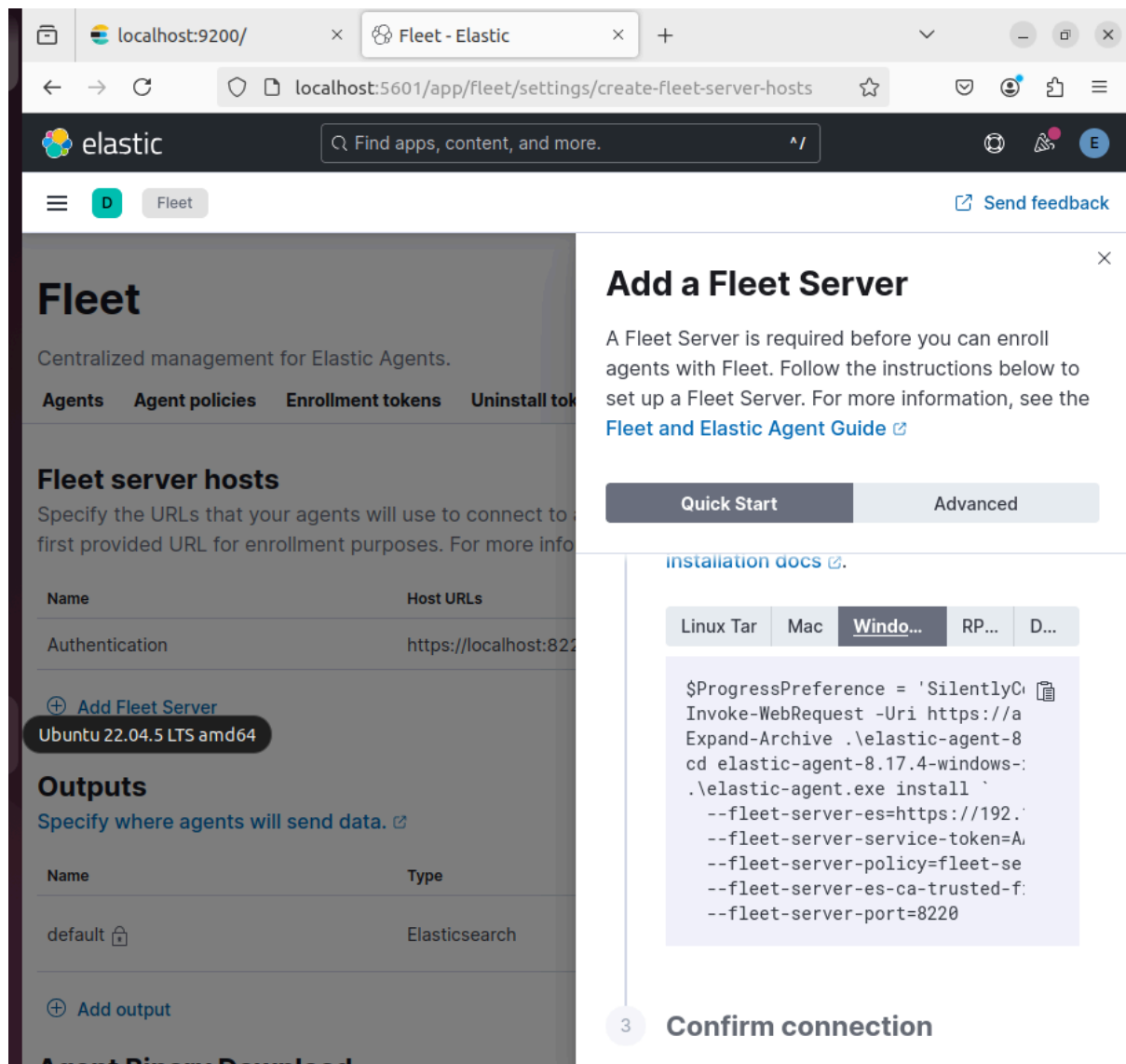
```
# sudo systemctl enable kibana
```

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=AAEAAWVsYXN0aWMvZmxlZXQtc2Vyd
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**

localhost:9200/Agents - Fleet - Elastic

localhost:5601/app/fleet/agents

elasticFind apps, content, and more.

Fleet

Centralized management for Elastic Agents.

AgentsAgent policiesEnrollment tokensUninstall tokensData streamsSettings

Agent activityAdd Fleet ServerAdd agent

Filter your data using KQL syntaxStatus 4Tags 0Agent policy 2Upgrade availableActions

Showing 1 agent1 agent selectedClear selectionClear filters

Healthy 1Unhealthy 0Updating 0Offline 0Inactive 0Unhealthy 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version
Healthy	DESKTOP-BPBR676	Fleet Server Policy rev. 2	1.32 %	249 MB	35 seconds ago	8.17.4

Rows per page: 20

Agent Details

DESKTOP-BPBR676

Send feedback

Agent detailsLogsDiagnostics

Overview

CPU1.39 %View more agent metrics

Memory249 MB

StatusHealthy

Last activity28 seconds ago

Last checkin messageRunning

Agent ID49678a67-3456-4dc6-a1ea-99eac8d7...

TerminalPolicyFleet Server Policy rev. 2

Agent version8.17.4

Host nameDESKTOP-BPBR676

Host ID3f0e9045-4e12-442f-aa21-633bb4b65...

Logging levelinfo

Privilege modeRunning as root

Agent releasestable

Platformwindows

Monitor logsEnabled

Monitor metricsEnabled

Integrations

>system-1

>fleet_server-1

Successful Log Collection

System Logs

elastic

Find apps, content, and more.

Observability

Infrastructure

Infrastructure inventory

Settings

Anomaly detection

Alerts and rules

Add data

Observability

Overview

Alerts

SLOs

Cases

AI Assistant

Logs

Explorer

Logs Anomalies

Logs Categories

Settings

Inventory

Infrastructure

Infrastructure inventory

Metrics Explorer

Hosts

Applications

Service Inventory

Infrastructure inventory

Search for infrastructure data... (e.g. host.name:host-1)

Show Hosts Metric CPU usage Group by All Sort by Name

desktop-bpbr676

Overview Metadata Metrics Processes Logs Anomalies Osquery

Last 1 hour 5 s

Experiencing continually loading data?

Total processes 205 Running 205 Sleeping N/A Dead N/A Stopped N/A Idle N/A Zombie N/A Unknown N/A

Top processes

Showing process data collected for the 1 minute preceding Mar 27, 2025 @ 18:28:09

Search for processes... State

State	Command	Time	CPU	Mem
Running	C:\Program Files (x86)\VMware\VMware Work...	2:27:46	198.7%	48.4%
Running	des.exe	17:06:14	8%	0.6%
Running	C:\Program Files\Google\Chrome\Application...	55:16	7.5%	1.3%
Running	C:\WINDOWS\system32\AUDIODG.EXE 0x00000000...	2:21:35	6.2%	0.1%
Running	C:\Program Files (x86)\VMware\VMware Work...	2:27:42	4.9%	1.8%
Running	C:\Program Files\Google\Chrome\Application...	2:21:04	0.7%	2.6%

localhost:9200/

DESKTOP-BPBR676 - Age

localhost:5601/app/fleet/agents/49678a67-3456-4dc6-a1ea-99eac8d7

elastic

Find apps, content, and more.

Fleet

Agents

DESKTOP-BPBR676

Send feedback

Agent details

Logs

Diagnostics

Search

Dataset 1

Log level 4

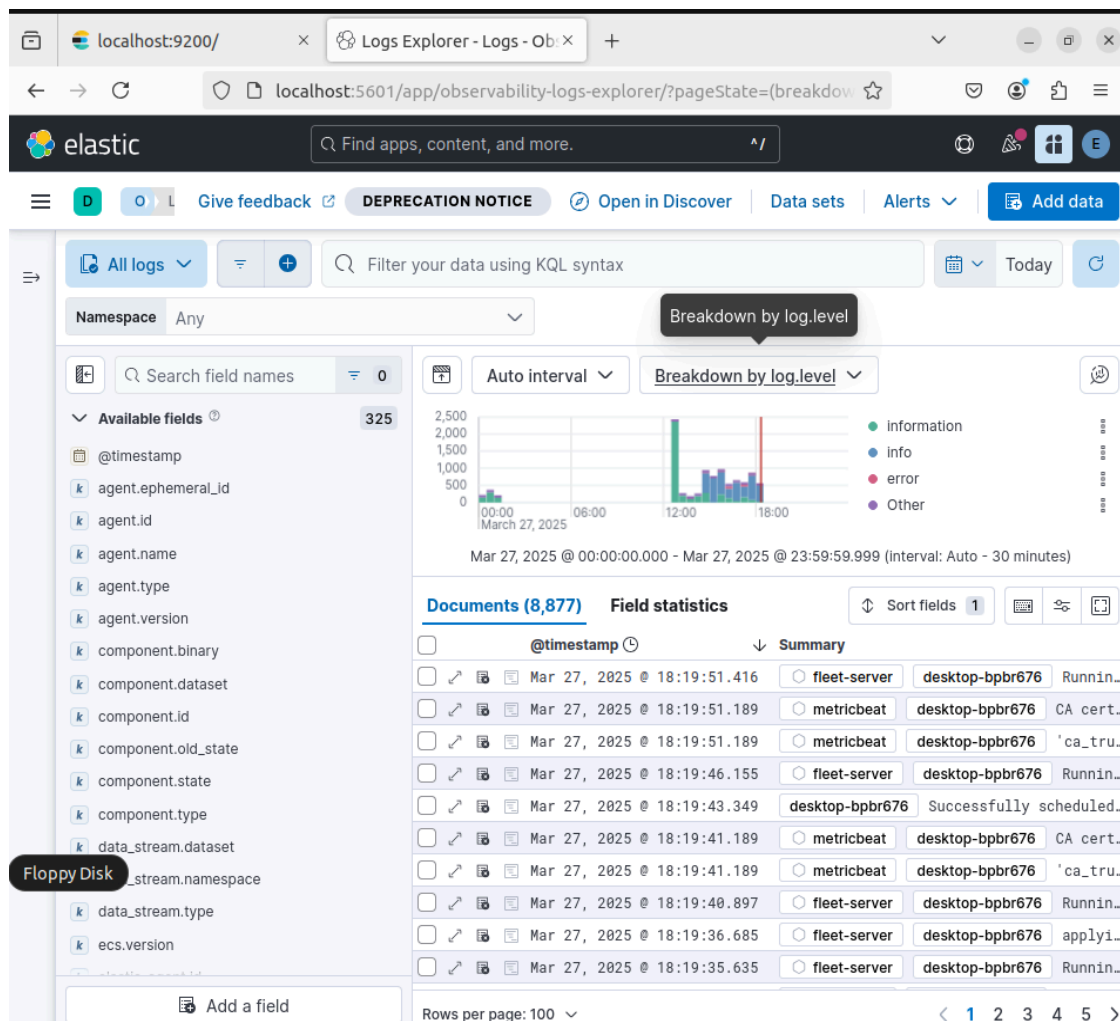
Last 1 day

Open in Logs Explorer

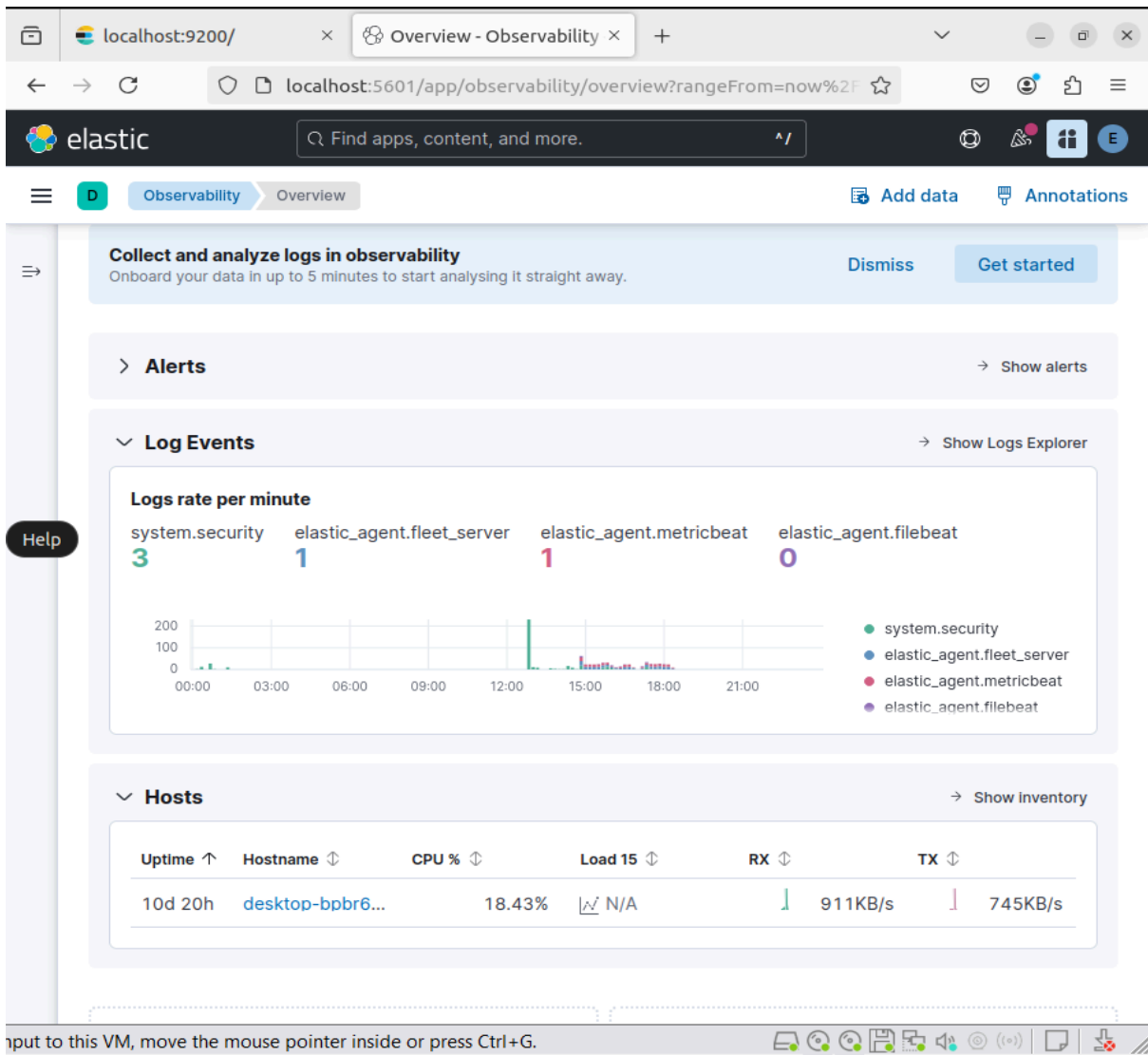
Timestamp	event.dataset	component.id	Message	error.message
17:16:10.143	elastic_agent	system/metrics-de fault	D->HEALTHY): Healthy: communicating with pid '6920'	
17:16:10.143	elastic_agent	log-default	[elastic_agent][info] Component sta te changed system/metrics-default (DEGRADED->HEALTHY): Healthy: commu nicating with pid '17840'	
17:20:40.399	elastic_agent		[elastic_agent][info] Component sta te changed log-default (DEGRADED->H EALTHY): Healthy: communicating wit h pid '16712'	
17:20:40.400	elastic_agent		[elastic_agent][info] component mod el updated	
17:23:07.431	elastic_agent		[elastic_agent][info] Updating runn ing component model	
17:30:42.292	elastic_agent		[elastic_agent][warn] Possible tran sient error during checkin with fle et-server, retrying	
			[elastic_agent][warn] Checkin requ est to fleet-server succeeded after 2 failures	

Showing entries until Mar 27, 17:30:42

Observability -> Logs

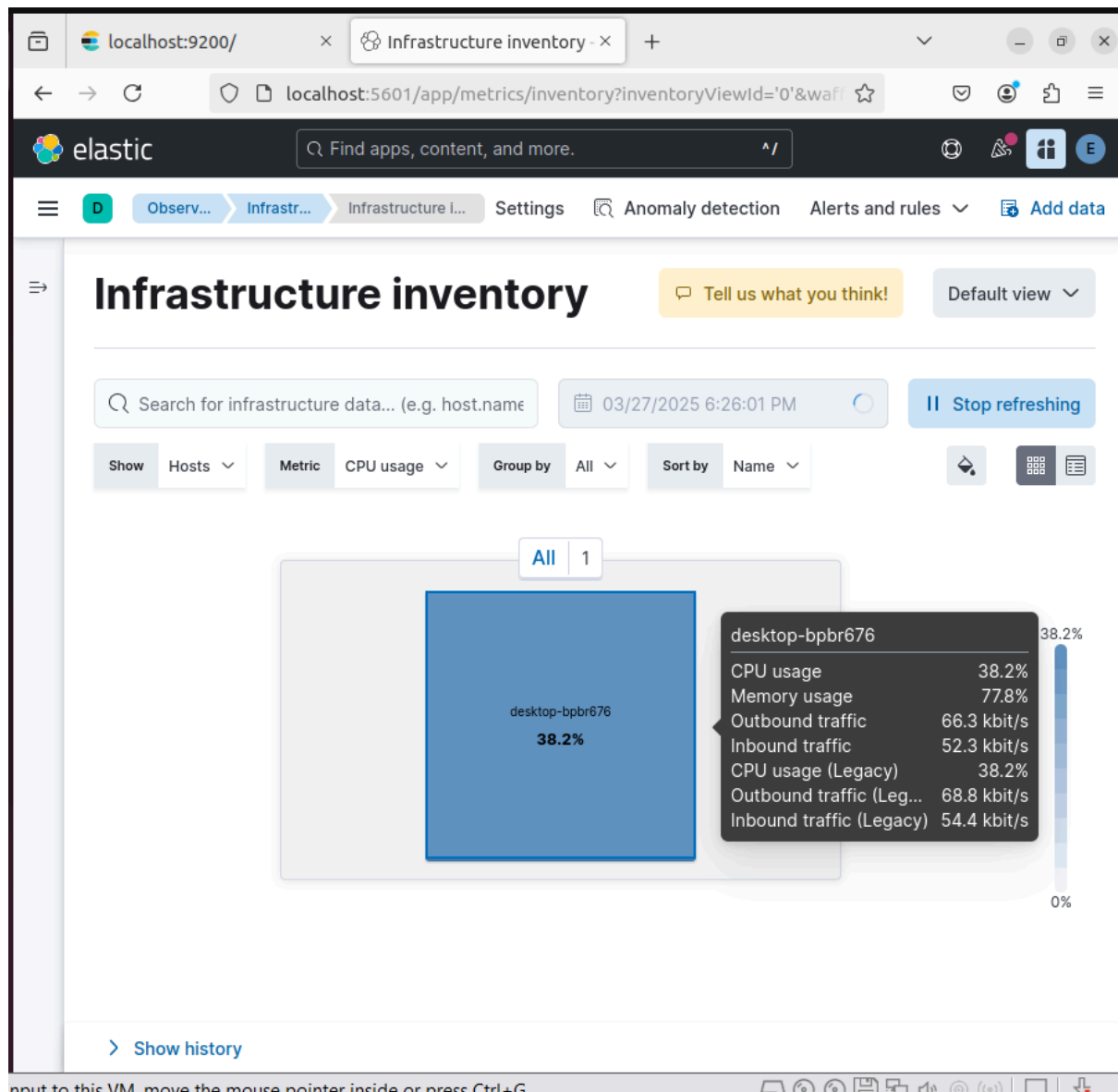


Observability -> Overview



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 inventory

Search for infrastructure data... (e.g. host.name)

Show

Hosts

Metric

CPU usage

Group by

All

Terminal

desktop-bpbr676

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%

Normaliz ed 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

Host OS version

10.0

+13 more

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](#)

input 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

The screenshot displays the Elastic SIEM interface for a rule named 'Auth-Successful-logon'. The interface is divided into several sections:

- Header:** Shows the Elastic logo, a search bar, and navigation tabs for 'Security', 'Rules', 'Auth-Successful-logon', 'Alerts', 'ML job settings', 'Add integrations', 'Data view', and 'Alerts'.
- Rule Details:**
 - Title:** Auth-Successful-logon
 - Status:** Enabled (toggle switch)
 - Created by:** elastic on Mar 27, 2025 @ 18:37:30.136
 - Updated by:** elastic on Mar 27, 2025 @ 18:37:30.136
 - Last response:** succeeded at Mar 27, 2025 @ 18:37:30.956
 - Notify when alerts generated:** (toggle switch)
- About Section:**
 - Description:** Credential are valid. Successful Logon by user.
 - Severity:** Low
 - Risk score:** 21
 - Max alerts per run:** 100
- Definition Section:**
 - Index patterns:** logs-* winlogbeat-*
 - Custom query:** event.code: "4624" AND winlog.event_data.LogonType : (2 OR 10)
 - Custom query language:** KQL
 - Rule type:** Query
 - Timeline template:** None

At the bottom of the interface, there are buttons for 'Show Applications', 'Timeline', and 'Unsaved'.

Rule Enabled

localhost:9200/

Detection rules (SIEM) - K X

+

localhost:5601/app/security/rules/management?rulesTable=(enc

elastic

Find apps, content, and more.

AI Assistant

Security

Rules

Detection rules (SIEM)

ML job settings

Add integrations

Rules

Add Elastic rules 1348

Manage value lists

Import rules

Create new rule

Installed Rules 1

Rule Monitoring 1

Chat

Rule name, index pattern (e.g. ...)

Tags 0

Last response 3

Elastic rules (0)

Custom rules (1)

Enabled rules

Disabled rules

Showing 1-1 of 1 rule

Selected 1 rule

Select all 1 rule

Bulk actions

Refresh

Clear filters

Updated 7 seconds ago

Off

☒

Rule

Risk s...

21

2...

4...

Notify

Enabled

☒

Auth-Suc...

21

2...

4...

Notify

☒

Rows per page: 20

< 1 >

Untitled timeline

Unsaved

Input to this VM, move the mouse pointer inside or press Ctrl+G.

Rule: 2 Failed login

Rule Created

localhost:9200/

Detection rules (SIEM) - K X

+

localhost:5601/app/security/rules/id/9b8a5988-fc03-4392-bbe8-

elastic

Find apps, content, and more.

AI Assistant

Sec... R... Auth-Failed-... AI... ML job settings Add integrations Data view Alerts

Filter your data using KQL syntax Today

Auth-Failed-Logon

Created by: elastic on Mar 27, 2025 @ 18:44:26.618
Updated by: elastic on Mar 27, 2025 @ 18:44:26.618

Last response: succeeded at Mar 27, 2025 @ 18:44:28.194 Notify when alerts generated

About

Invalid Credential.

Severity	Medium
Risk score	47
Max alerts per run	100

Definition

Index patterns	logs-* winlogbeat-* -*elastic-cloud-logs-*
Custom query	event.code : "4625"
Custom query language	KQL
Rule type	Query
Timeline template	None

Show Applicationsed timelineUnsaved

Rule Enabled

localhost:9200/

Detection rules (SIEM) - K X

+

localhost:5601/app/security/rules/management?rulesTable=(ena

elastic

Find apps, content, and more.

AI Assistant

E

SecurityRulesDetection rules (SIEM)

ML job settingsAdd integrations

Rules

Add Elastic rules1348

Manage value lists

Import rules

Create new rule

Installed Rules2

Rule Monitoring2

Chat

Rule name, index pattern (e.g.

Tags0

Last response3

Elastic rules (0)

Custom rules (2)

Enabled rules

Disabled rules

Showing 1-2 of 2 rules

Selected 1 rule

Select all 2 rules

Bulk actions

Refresh

Clear filters

Updated 9 seconds ago

Off

Rule	Risk s...		I	I	L	Notify	Enabled
<input checked="" type="checkbox"/> Auth-Fail...	47	1...	1...	1...		<input checked="" type="checkbox"/>	
<input type="checkbox"/> Auth-Suc...	21	1...	8...			<input checked="" type="checkbox"/>	

Rows per page: 20

< 1 >

Floppy Disk

Untitled timeline

Unsaved