

## Table of Contents

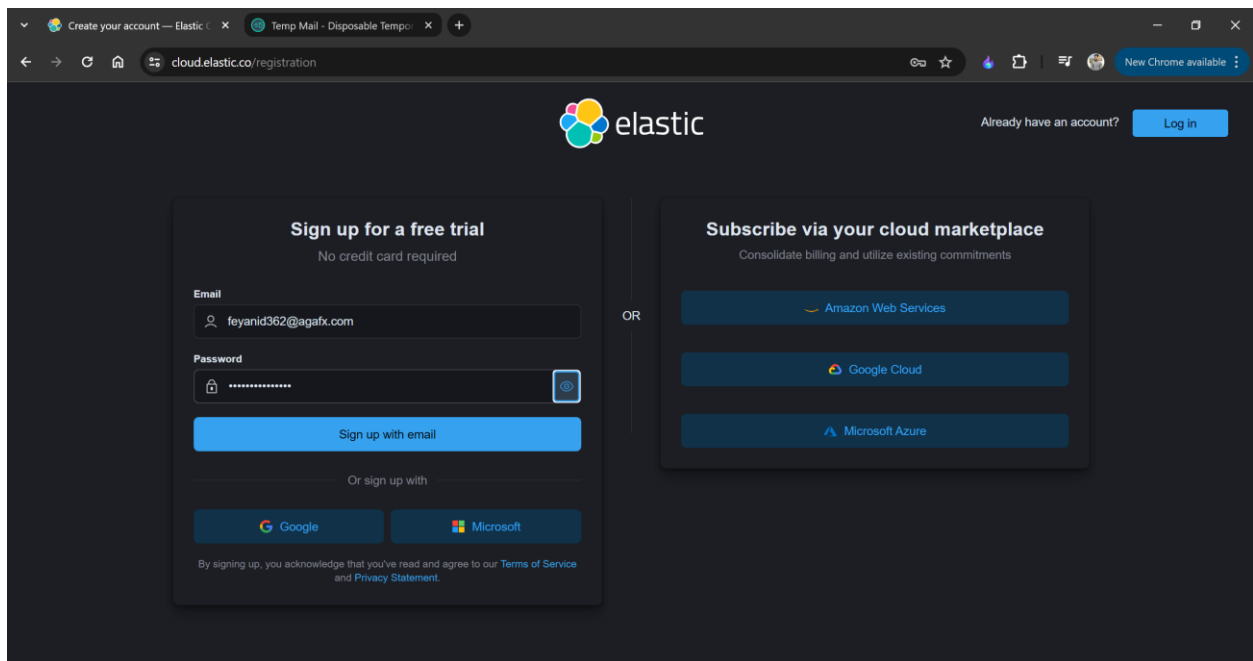
1. Introduction .....	1
1.1. Signup for Elastic Cloud .....	1
1.2. Deployment of Cloud .....	1
1.3. Access Dashboard .....	2
1.4. ELK Ready for Monitoring .....	2
2. Setting up Ubuntu Server .....	3
2.1. Ubuntu Server Host Secure .....	3
3. Adding Fleet Agent .....	4
3.1. Adding Agent on Ubuntu Server .....	4
3.2. Confirming Enrollment .....	4
3.3. Data Agent on Dashboard .....	5
4. Installing Metricbeat for Logs Demonstration .....	6
4.1. Confirming Logs .....	6
5. Overall Agent Information .....	7
6. Centralized Log Management .....	8
6.1. Sudo Commands Execution Logs .....	8
6.2. SSH Attempts Logs .....	9
6.3. Detailed Logs for Failed Attempts .....	10
7. Mitigations for Sudo Command Execution .....	11
7.1. Mitigations for SSH Attempts .....	12
8. Conclusions .....	12
9. References .....	12

## **Introduction of Scenario:**

In this scenario, we are going to installation a tracking machine using Elastic Cloud, or ELK. First, we will sign on for ELK and set up it inside the cloud. Then, we'll make certain our Ubuntu Server is stable via including Fleet Agents to it. After that, we will install Metricbeat to reveal how logs are managed. We'll reveal such things as sudo instructions and SSH login attempts to preserve our machine safe. Finally, we're going to suggest methods to address any safety troubles and provide a few references for extra records

## **Signup for Elastic Cloud:**

To sign up for Elastic Cloud trial model, go to the Elastic Cloud internet site, click at the "Sign Up" button, and comply with the prompts to create an account. Once registered, you will benefit get admission to a tribulation version with restrained capabilities to explore Elastic Cloud's talents.



**Figure-1 Sign up for ELK**

## **Deployment of Cloud:**

Following that, customers continue with the aid of coming into their information and choosing deployment alternatives inclusive of cloud provider, area, and cluster size. Once showed, Elastic Cloud initiates the deployment procedure, provisioning sources and setting up the ELK stack

infrastructure as a consequence.

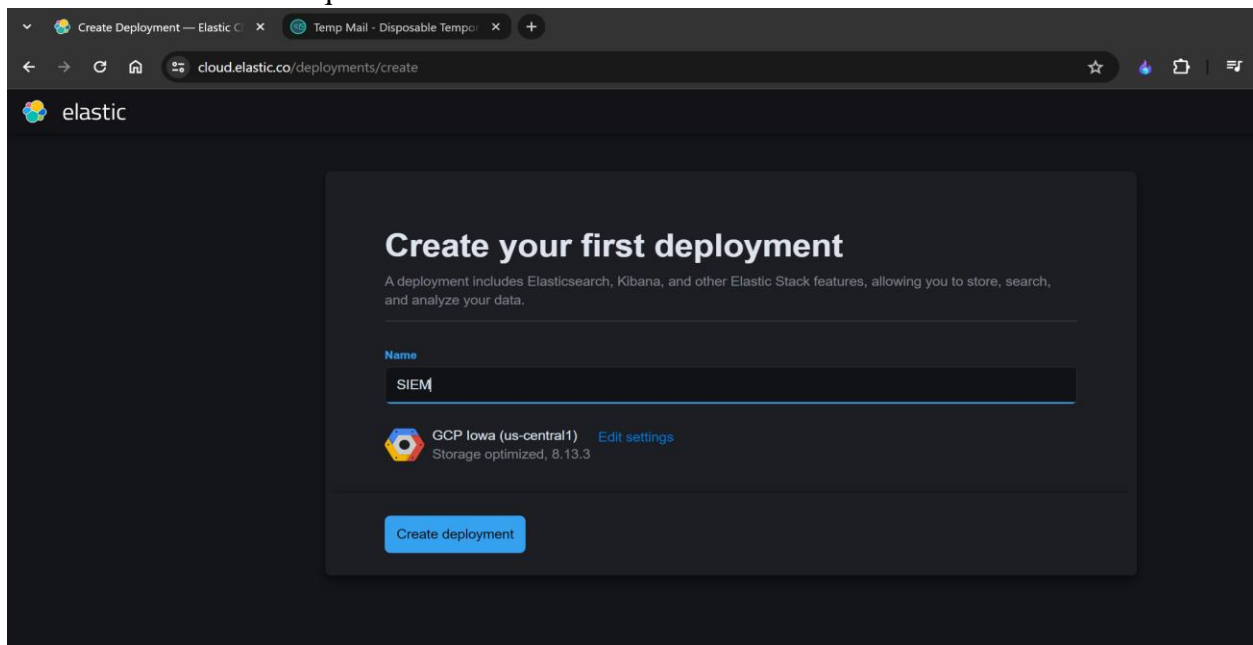


Figure-2 Create Deployment

### Access Dash Board:

After completing the deployment system, customers can get right of entry to the dashboard by using logging into the Elastic Cloud console the use of their credentials. Upon successful login, they are provided with a person-friendly interface wherein they are able to view and manage their ELK stack deployment, including tracking, configuration, and analysis features.

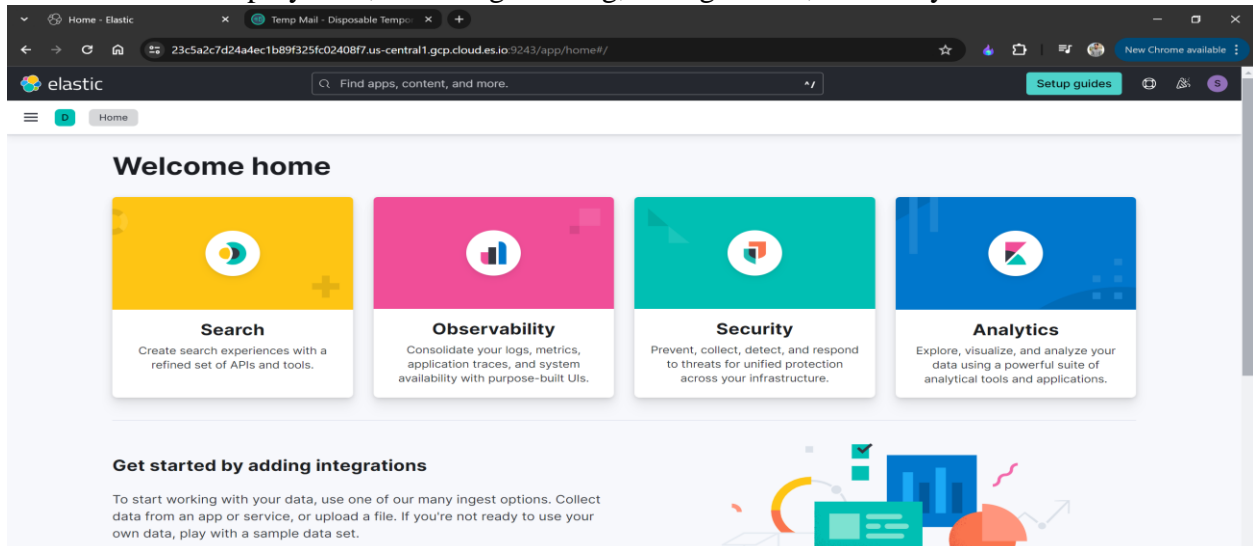


Figure-3 ELK Ready for Monitoring

## Setting up Ubuntu Server:

Setting up the Ubuntu Server includes putting in the operating gadget on a chosen device, configuring network settings, and ensuring primary security features including firewall setup and user authentication. Additionally, important applications and dependencies may need to be mounted to help subsequent duties and packages.

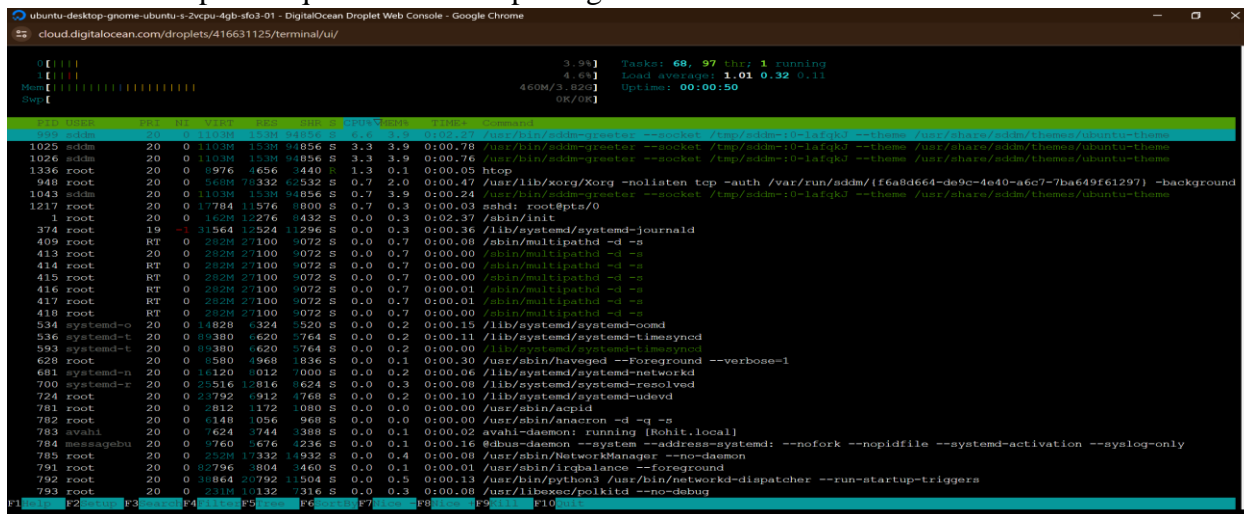


Figure-4 Ubuntu Server Host to secure.

## Adding Fleet Agent:

To setup a Fleet Agent, first, make sure that the Elastic Stack is well configured. Then, navigate to the Fleet section inside the Elastic Cloud console and follow the activates to add a brand new agent. Finally, deploy the agent to the desired hosts for tracking and control.

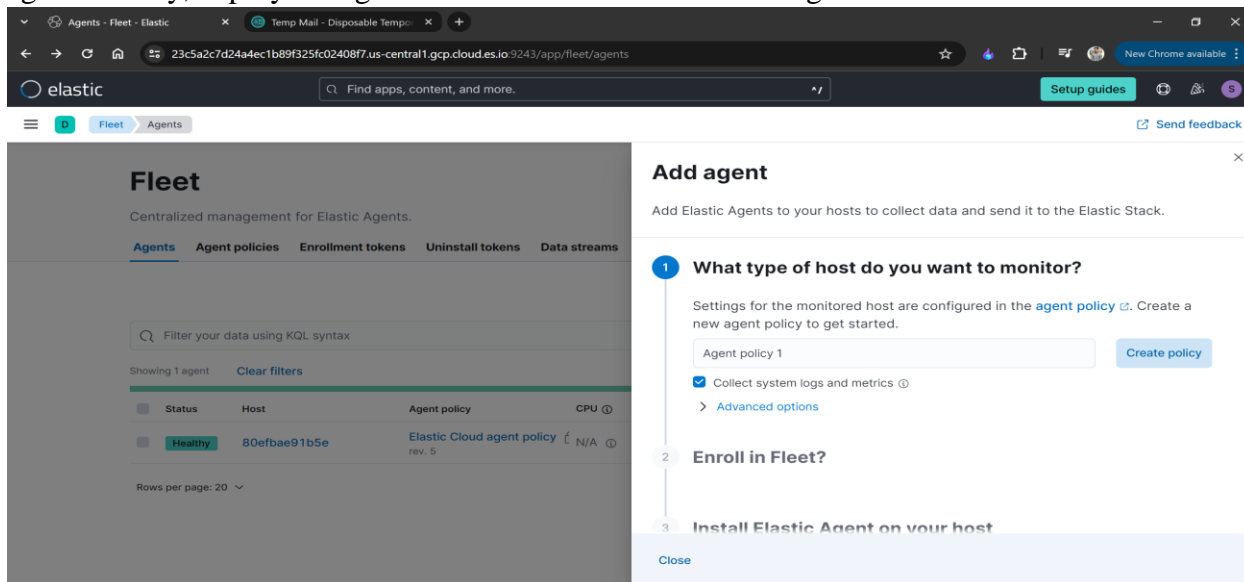


Figure-5 Fleet Agent adding

## Adding Agent on Ubuntu Server

"Adding an agent on Ubuntu Server includes downloading the agent package deal, installing it with dpkg, and configuring its settings through the YAML configuration file. Once configured, the agent provider may be started using a carrier control command like 'service' or 'systemctl'."

Figure-6 Installing on agent

## Confirming Enrolment:

To Confirm enrollment, navigate to the Fleet segment inside the Elastic Cloud console. Locate the newly brought agent and affirm its reputation to ensure a hit enrollment. Additionally, evaluate any enrollment logs or reputation messages for in addition validation.

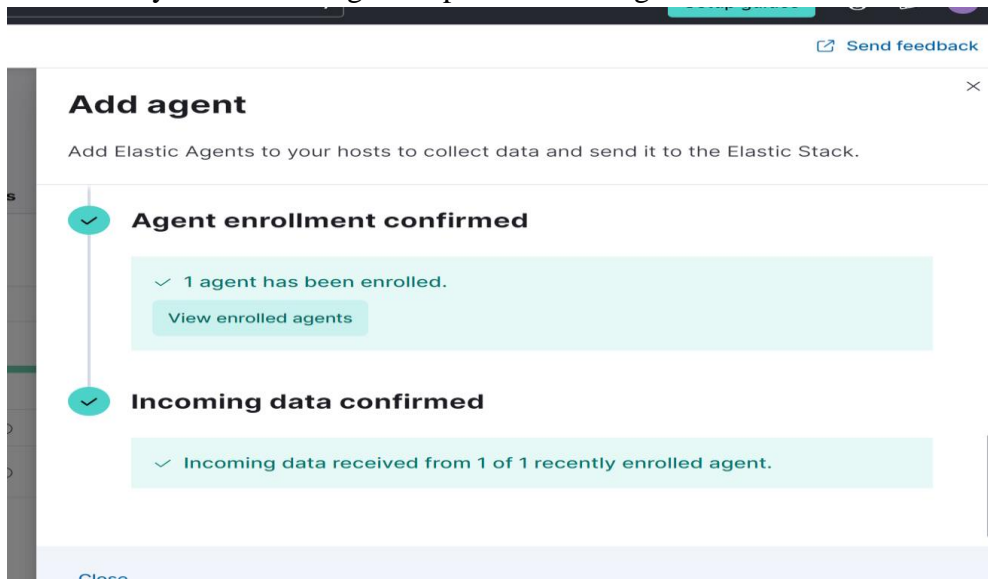


Figure-7 Agent Enrollment Confirmation.

## Data Agent on Dashboard:

On the dashboard, get entry to the "Agents" or "Fleet" section to view data from the newly introduced agent. Here, you may display metrics, logs, and different applicable information supplied via the agent, facilitating real-time insights into device overall performance and hobby. Utilize filtering and visualization equipment to customize the show and higher recognize the records.

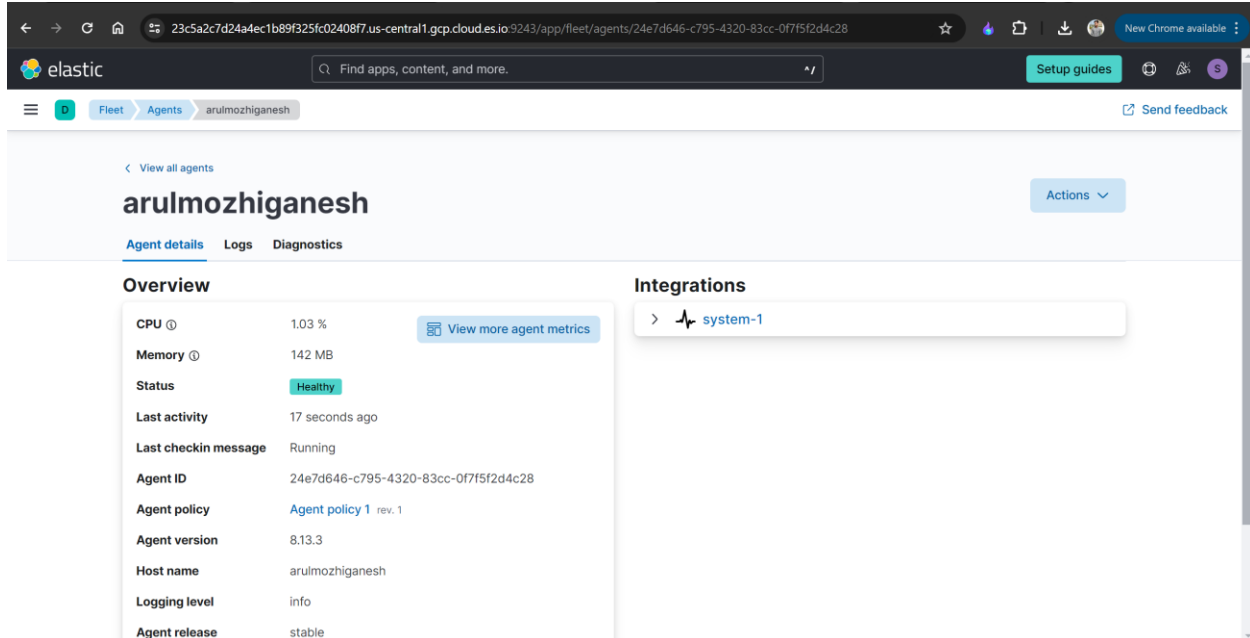


Figure-8 Agent Data on Dashboard

### **Installing Metricbeat for Logs Demonstration:**

To install Metricbeat for demonstrating logs, first, download the Metricbeat package suitable for your system. Then, install it using the appropriate package manager or by manually extracting and configuring it. Finally, start the Metricbeat service to begin collecting system metrics and logs for visualization and analysis.

```
cloud.digitalocean.com/droplets/416631125/terminal/ui/
root@Rohit:~/Rohit/elastic-agent-8.13.3-linux-x86_64# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
sudo apt-get update && sudo apt-get install metricbeat
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  apt-transport-https
1 upgraded, 0 newly installed, 0 to remove and 184 not upgraded.
Need to get 1510 B of archives.
After this operation, 0 B of additional disk space will be used.
```

Figure-9 Installing Metricbeat for Logs Demonstration

### **Confiming Logs:**

To confirm logs, navigate to the certain log storage place or use the Elastic Stack interface to view incoming log facts. Verify that logs from Metricbeat or other assets are being indexed and displayed successfully. Additionally, carry out searches or practice filters to make sure unique log events are being captured as it should be. Agent's status, ID, and utterance time are all retrievable. Thus, it enables the right choices, giving out details about the performance of the

agents and the system itself.

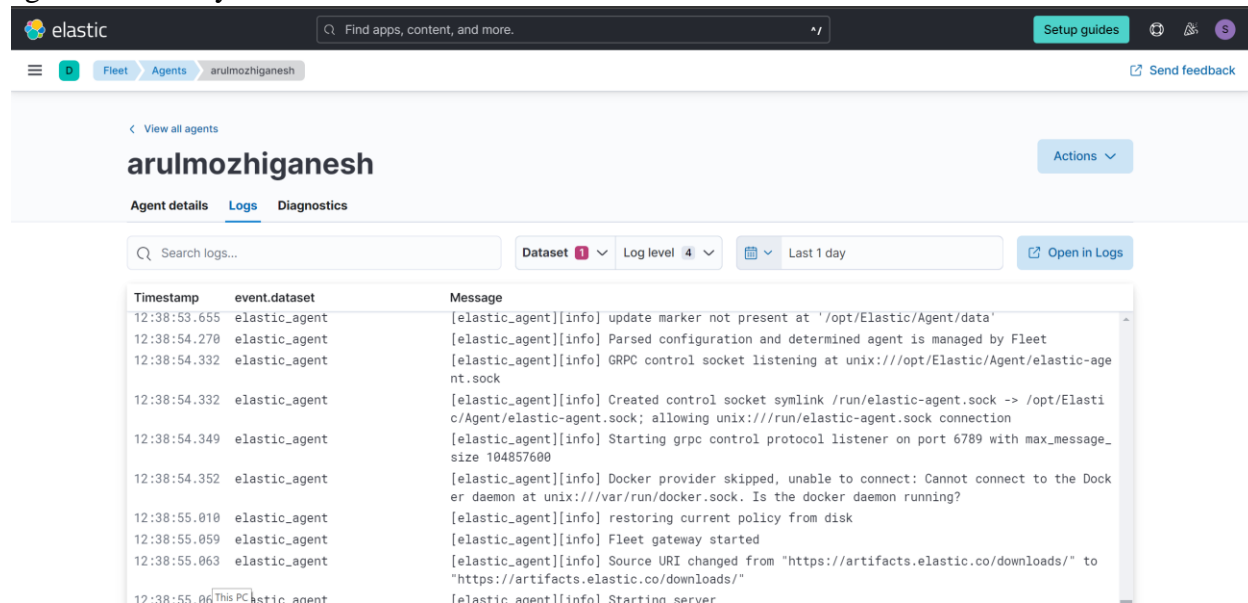


Figure-10 Logs from Arulmoz Agent

## Overall Agent Information:

Back in the Elastic Cloud main menu, the fleets or agents section stores the extensive agent information. This is where users can see things like, say, agent status, version, when was the last communication on that agent, and any errors or warnings that might have been set. This generalized return gives information about the health and performance conditions in all the agents that are implanted in the system.

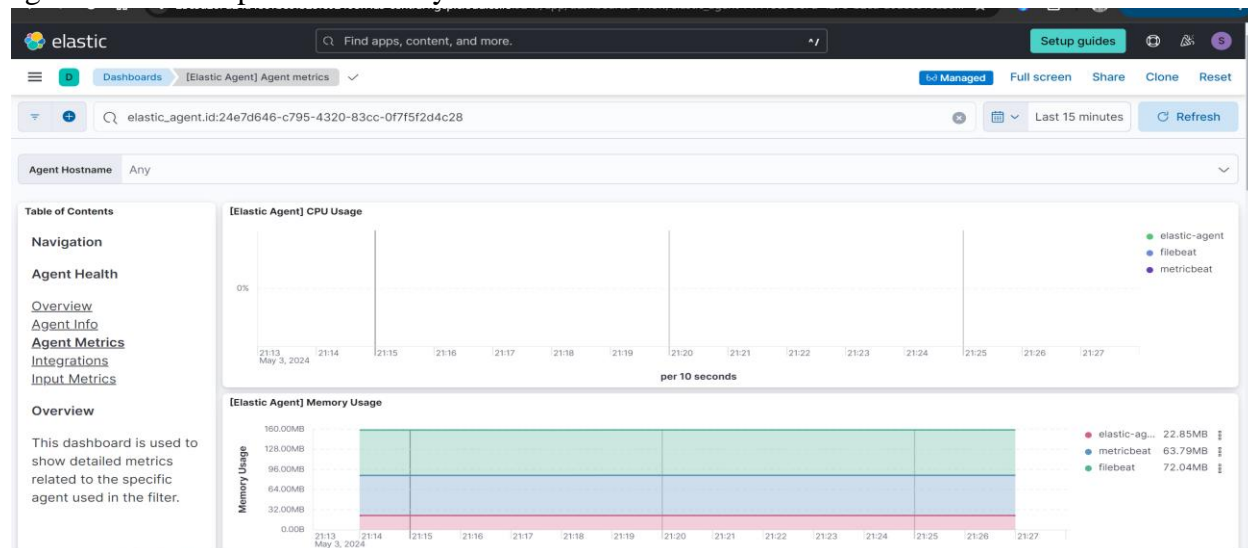


Figure-11 Agent Information

## Centralized Log Management

Centralized log management fundamentally means to put log records generated from multiple resources into a central place to be analyzed and processed, say, with the help of Elastic search. logs are collect, indexed and saved in the one place which is easily searchable, analyzable and visualize songs are stored on the cloud and every move of the user is continuously tracked This approach coexists with visibility, eases troubleshooting, and through granting a general view in the device operation activity provides a holistic view of technological developments across living environments.

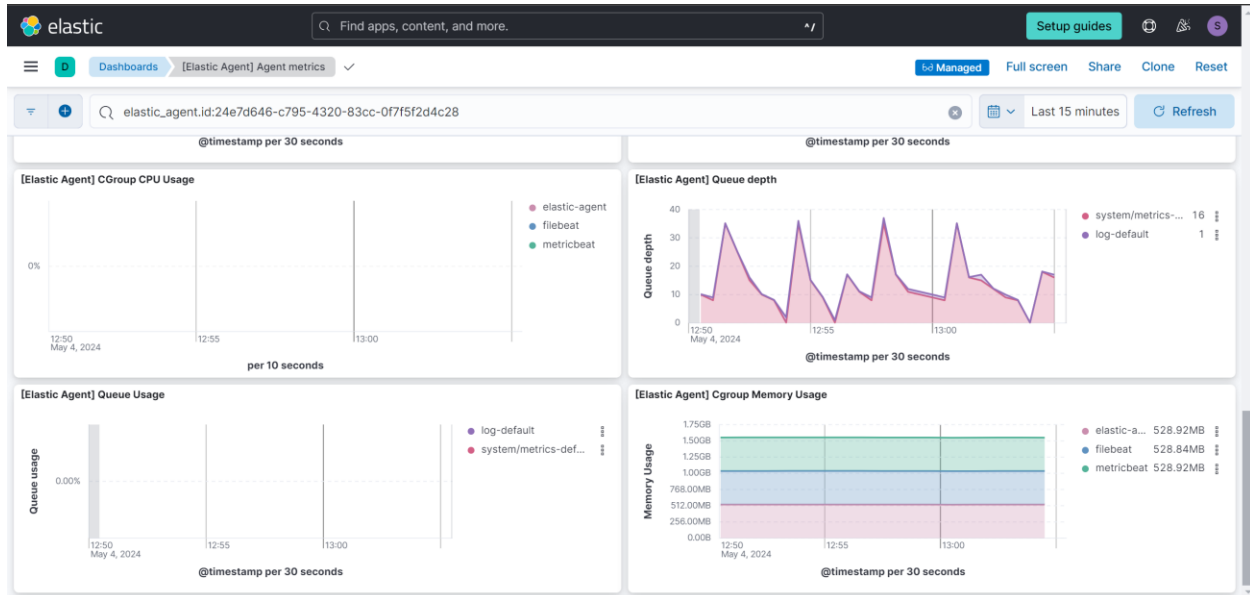


Figure-12 Dashboard to Monitor all

### Advantages of Centralized Log Management:

Centralized log management entails records centralization, addressing the issue of visibility, as it does this by consolidating log records from the multiple systems, enabling administrators to have effective monitoring of the systems for both security incidents and operational troubles. It provides with methods to solve problems remotely that is man powerful that the cloud itself because remember is it can provide on-demand service for more than one request. Moreover, it helps to ensure compliance and managing activities by gathering and storing all the relevant logs in order to carry out the tasks of audit functions and compliance with regulatory requirements from assembling. Through real-time analysis of logs for traces of malicious habits or anomalies, this process delivers advanced danger recognition. By doing this, it upgrades standard security features. However, details address scalability and performance. They are able to process thousands of log data points for a sample of time and recognize that these performance needs are dynamic, adapting as the organizational requirements evolve.

### Sudo Commands Execution Logs:

Command execution log rooted in sudo registers details of completed commands with higher privileges upon a sudo application. Every record is typically composed by a log consisting of facts such as person who made the command, timestamp, the command itself, and result (success



or failure). Keeping track of the routing of the sudo command logs are essential for the audit of automation, tracing the breaches, and being sure that the system is in compliance with the security regulations.

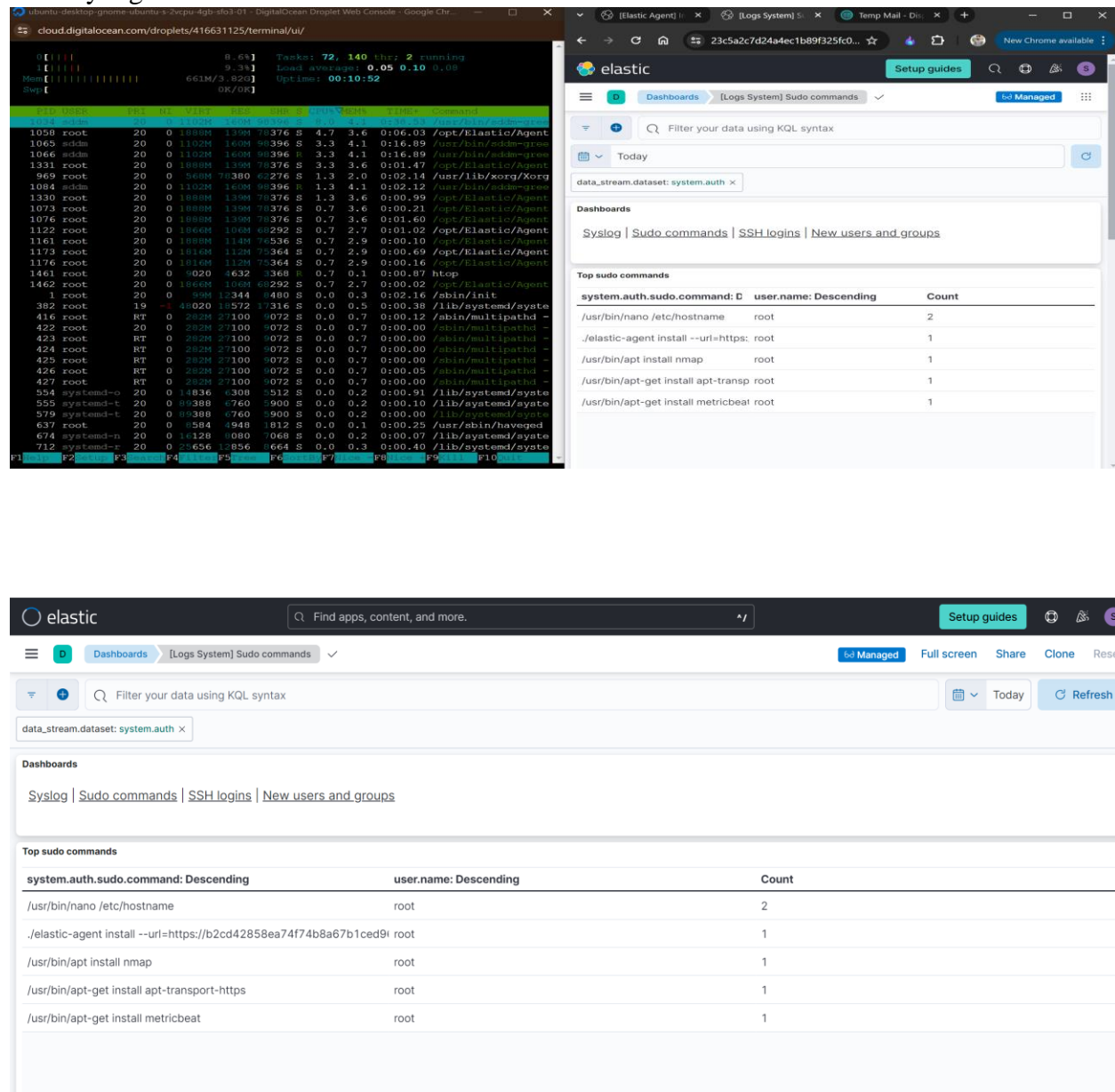


Figure-13 Sudo Commands Execution Logs

## Ssh attempts logs:

SSH designed the log file according to which it recorded all login attempts done through SSH protocol, including notified success and unsuccessful attempts. these logs are the instances of these data, such as the source IP address, the user name, the login timestamp, and the authentication status. Watching incoming SSH session log, especially failed attempts, is paramount for detection of unauthorized access attempts and then setting crucial security features

like preventive measures to block malicious attacks.

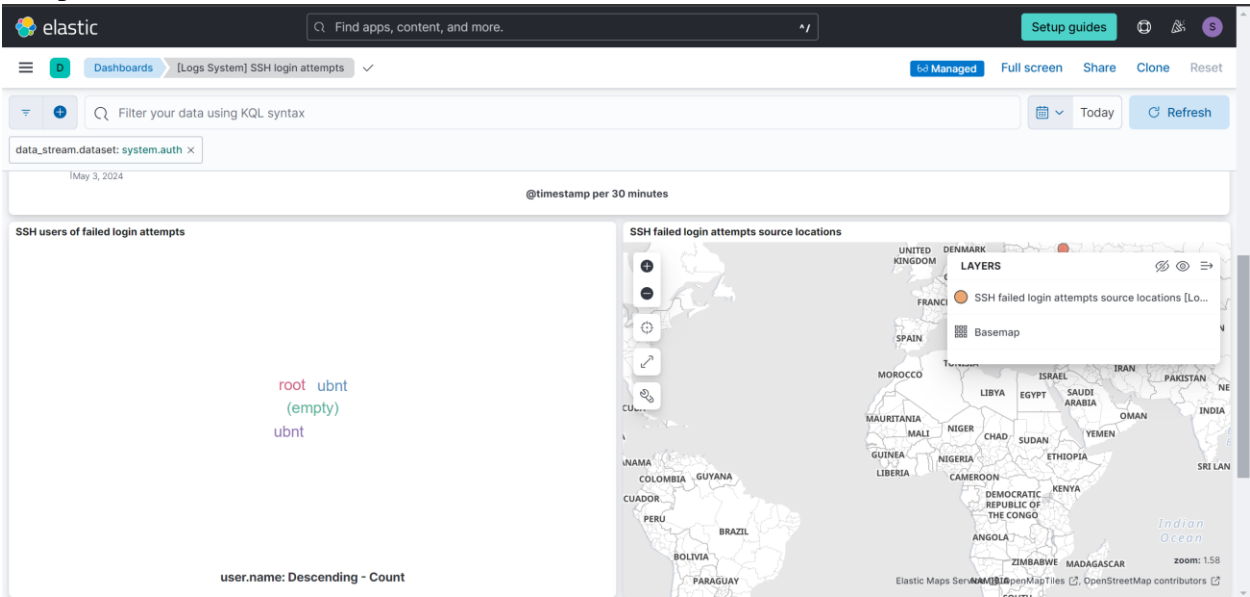


Figure-14 Failed and Passed Login attempts

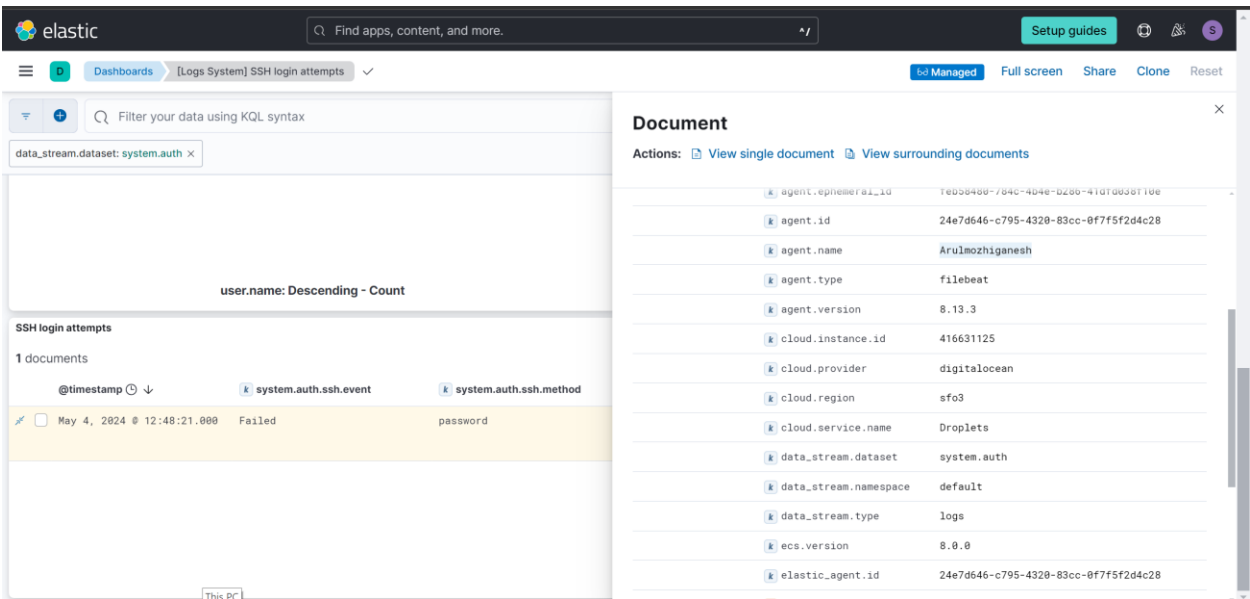


Figure-15 Detailed Logs for Failed Attempts

### Global attacks Identification:

Embedding GeoIP place data into ELK to deliver specialized logs of unsuccessful login attempts directly provides out - standing comprehension of our cyber environment security weaknesses. Through contrasting the geographical and climatic regulation of supply IP deal, such as country, region, and city, directors will be able to estimate the places and derive useful information on attack attempts origin. Integration makes this task easier since it allows to include the contextual information necessary to spot any potential risk and prevent its increasing. Every log item with

GeoIP place data enables a view of the global picture, which as a result decreases the possibilities for unwanted intrusion into the infrastructure maintenance system. Consequently, through heightening area nearest a dangerousness of abnormal activities and improve usual cybersecurity defenses they spending their tools and their resources.

### **Mitigations for Sudo Command Execution:**

On Linux, security risks involving the execution of sudo can be mitigated by putting in stricter access rules, limiting roles that are allowed to run sudo commands, and confining the privileges given out to essential users and commands. Data logging is most necessary for the record of privileged activities eventually it helps jo making the response to incidents easier. Introduce 2FA (two factor authentication) for the sudo access to make sure the authentication is being protected on that level. One of the sudo configuration opinion we have on a standard basis under the supervision of security is to quickly pick out and rectify any unauthorized access which has been part of our system by mistake or not.

### **Mitigations for ssh attempts:**

As a measure of countering SSH threats, a sound security system should be developed. Coordinate firewalls regulations to allow SSH access only from trusted IP addresses, thus, lowering potential threat of hackers. Use strong authentication methods such as SSH key-based logins to help protect your remotely by deploying Intrusion Detection Systems (IDS) that can catch and quell suspicious SSH acts in real time advancing security position of all participants.

### **Conclusions:**

To conclude, this scenario described how ELK stack could be deployed for visibility and to analyze the consolidated events that are generated by devices. The process consisted of several other aspects which were creating much ELK account, deploying on the cloud, safe Ubuntu Server with Fleet Agents, and adding Metricbeat for log collection. Minimization approaches for protection hazards such as sudo command execution and others have been mentioned as well, stressing the greatness of access controls and tracking. Subsequently the main target is to make a holistic approach for machines tracking, safety.

### **References:**

- 1- Lahmadi, A. and Beck, F., 2015, June. Powering monitoring analytics with elk stack. In 9th international conference on autonomous infrastructure, management and security (aims 2015).
- 2- Detken, K.O., Rix, T., Kleiner, C., Hellmann, B. and Renners, L., 2015, September. SIEM approach for a higher level of IT security in enterprise networks. In 2015 IEEE 8th

International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 322-327). IEEE.

- 3- Mahmoud, R.V., Anagnostopoulos, M. and Pedersen, J.M., 2022. Detecting cyber-attacks through measurements: learnings from a cyber-range. IEEE Instrumentation & Measurement Magazine, 25(6), pp.31-36.
- 4- Martín-Pérez, M., Parella, J.M., Fernández, J., de Juan Fidalgo, P., Casadamente, J., Romero, A.Á. and Diaz-Rodriguez, R., 2023, June. A testbed for a nearby-context aware: Threat detection and mitigation system for connected vehicles. In 2023 JNIC Cybersecurity Conference (JNIC) (pp. 1-8). IEEE.