Networks and Cyber Security II

PROJECT:SIEM WAZUH WITH GRAFANA

MEMBERS:-

Asad Khursheed 22i-1585

Syed Inshal Yousaf 22i-7439

Ehtisham ul-Hasan 22i-1777

Contents

Introduction:- 3
Wazuh indexer cluster installation 3
Credentials are stores in Wazuh-install-files that are used to login to the dashboards. 4
Command line based agent is installed on ubuntu 5
Grafana Installation: 6
Grafana dashboard: 7
Filebeat Installation: 7
Filebeat.yml configuration: 8
Elastic Search Installation: 9
Adding data source on grafana 10
Conclusion:- 11

Introduction:-

Security Information and Event Management (SIEM) systems play a vital role in enhancing an organization's security posture. This report focuses on deploying and configuring the Wazuh SIEM solution integrated with Grafana for comprehensive monitoring and analysis. The integration allows for centralized log management, real-time event monitoring, and interactive dashboards to visualize security data effectively. This guide covers the installation, configuration, and usage of Wazuh and Grafana in a systematic manner, ensuring a robust SIEM setup.

Wazuh indexer cluster installation

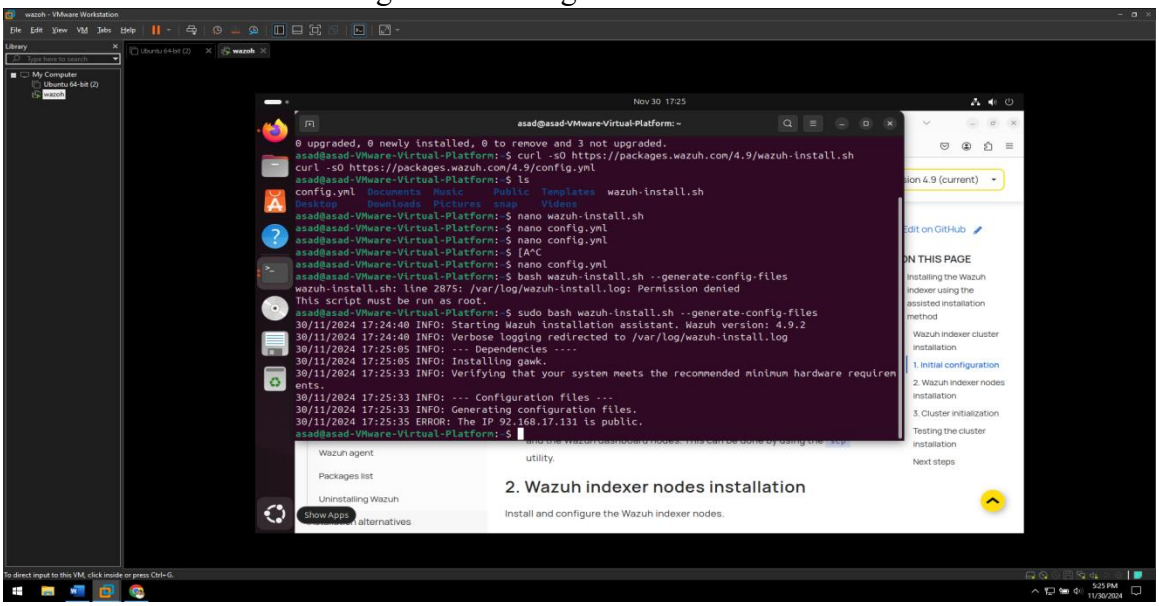
- **Initial configuration**

Indicate your deployment configuration, create the SSL certificates to encrypt communications between the Wazuh components, and generate random passwords to secure your installation.

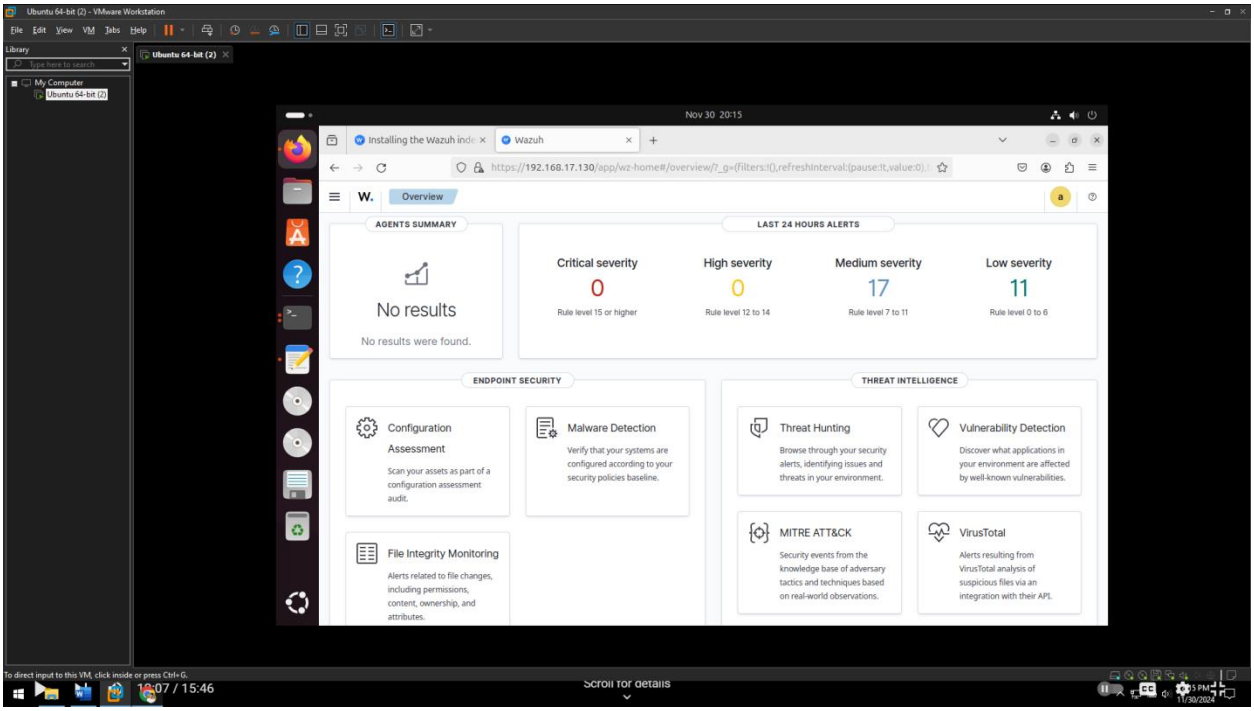
1. Download the Wazuh installation assistant and the configuration file.
2. # curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh

curl -sO https://packages.wazuh.com/4.9/config.yml

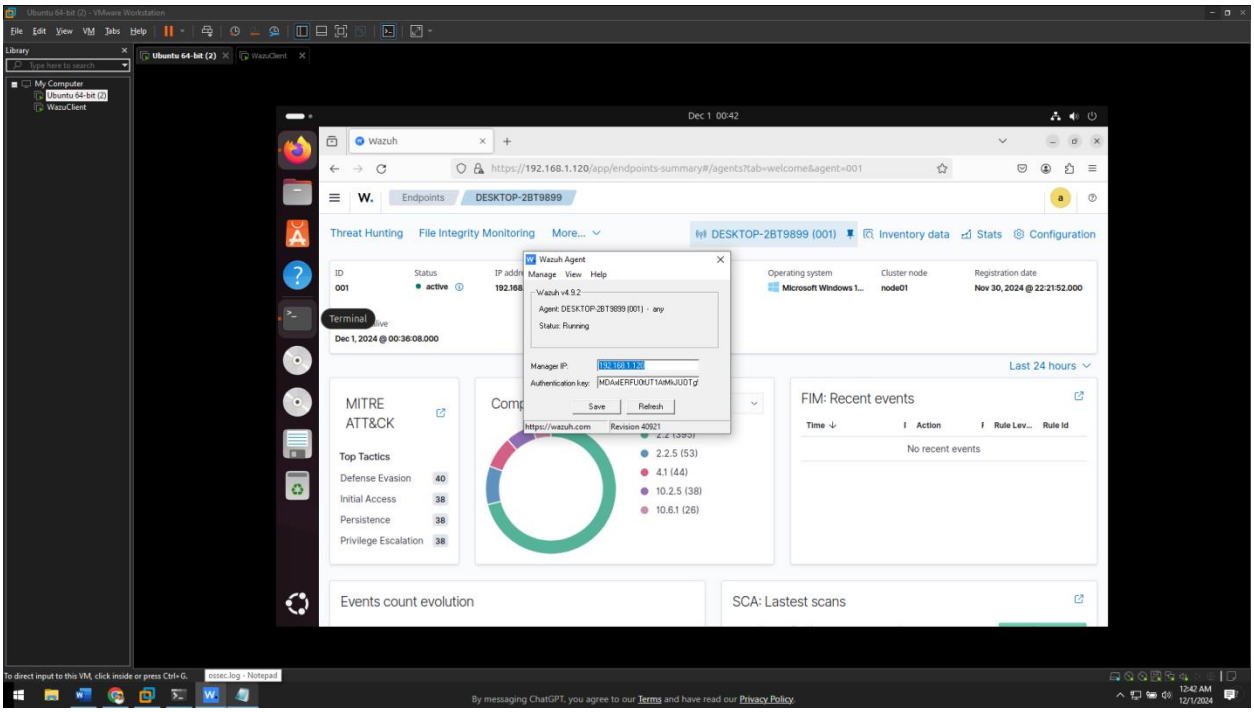
- Edit ./config.yml and replace the node names and IP values with the corresponding names and IP addresses. You need to do this for all Wazuh server, Wazuh indexer, and Wazuh dashboard nodes. Add as many node fields as needed.
- Run the Wazuh installation assistant with the option --generate-config-files
  sudo bash wazuh-install.sh --generate-config-files



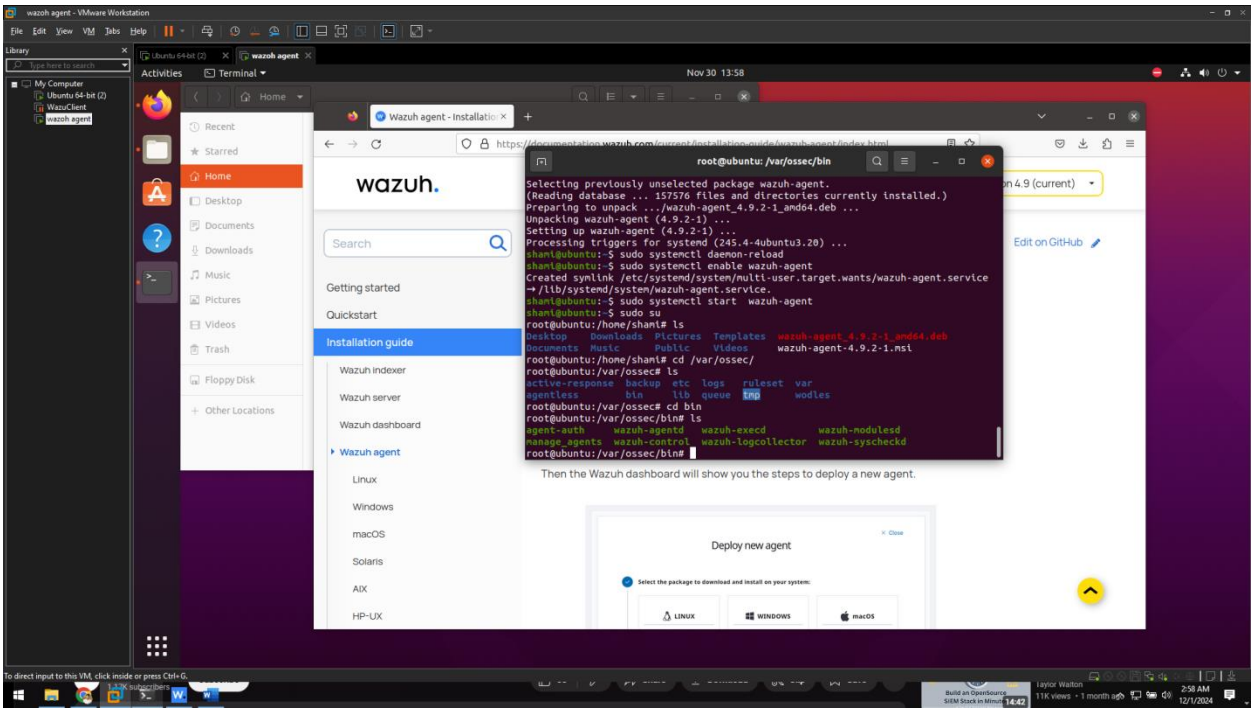
Credentials are stores in Wazuh-install-files that are used to login to the dashboards.



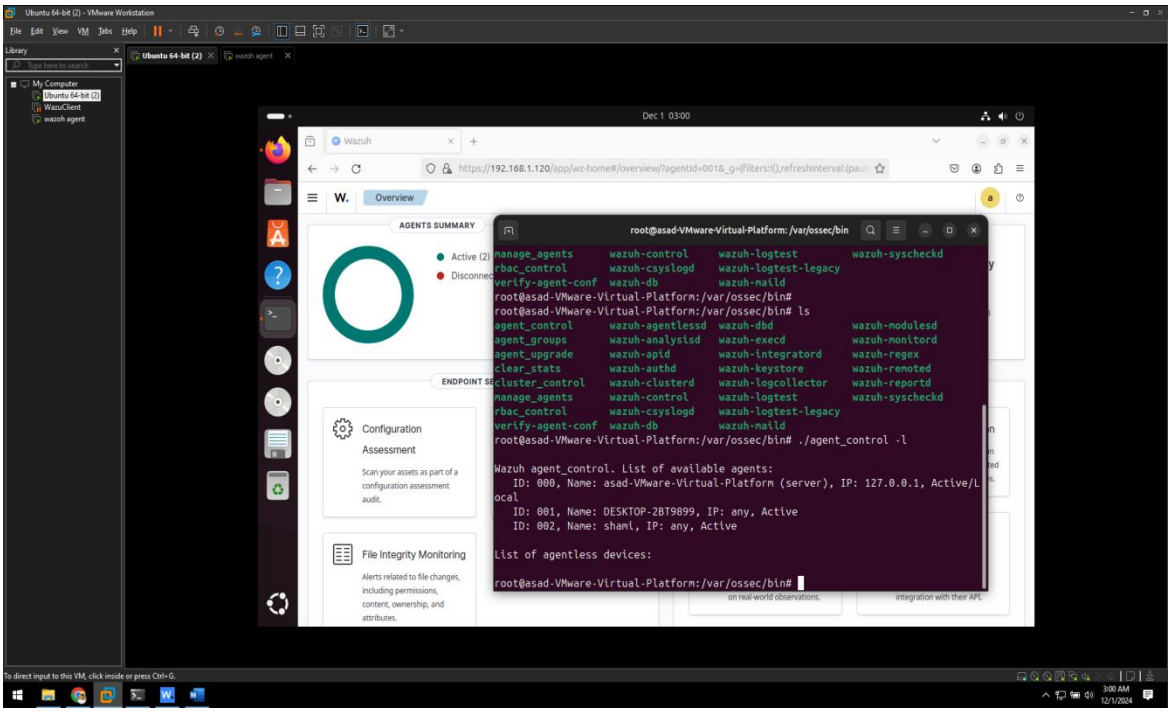
Agent installation:



Command line based agent is installed on ubuntu



Listed agents are shown on server side

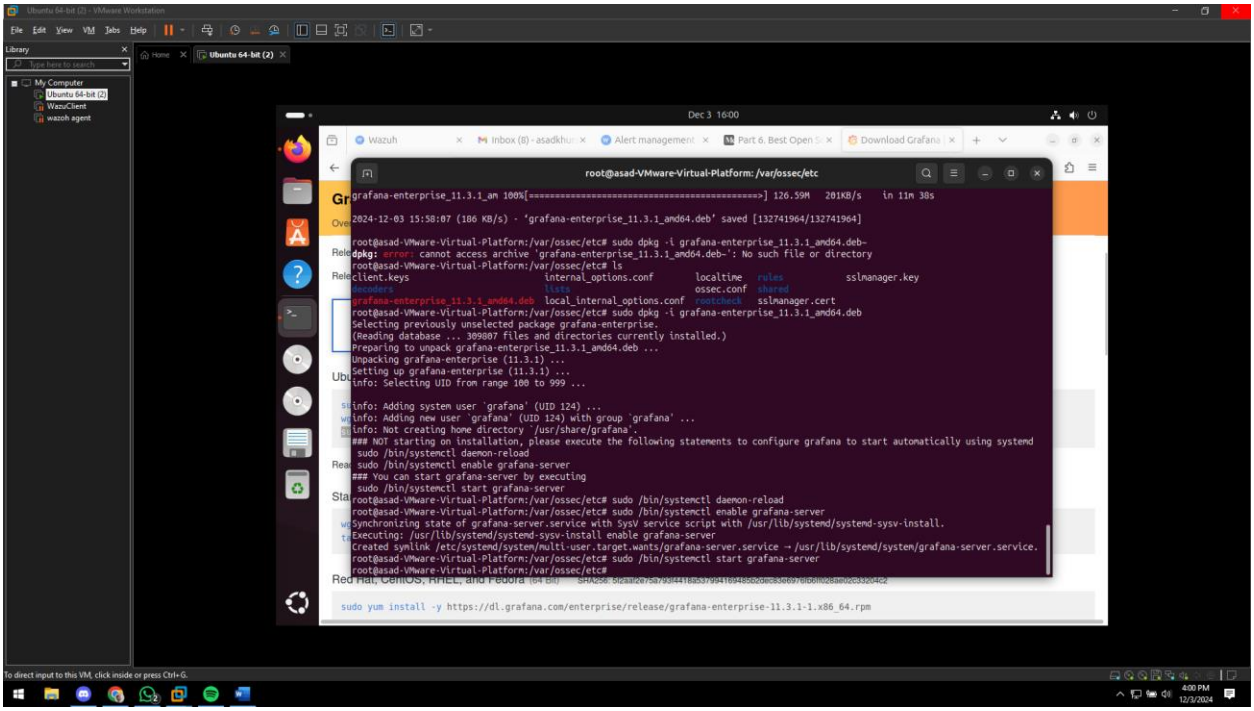


Grafana Installation:

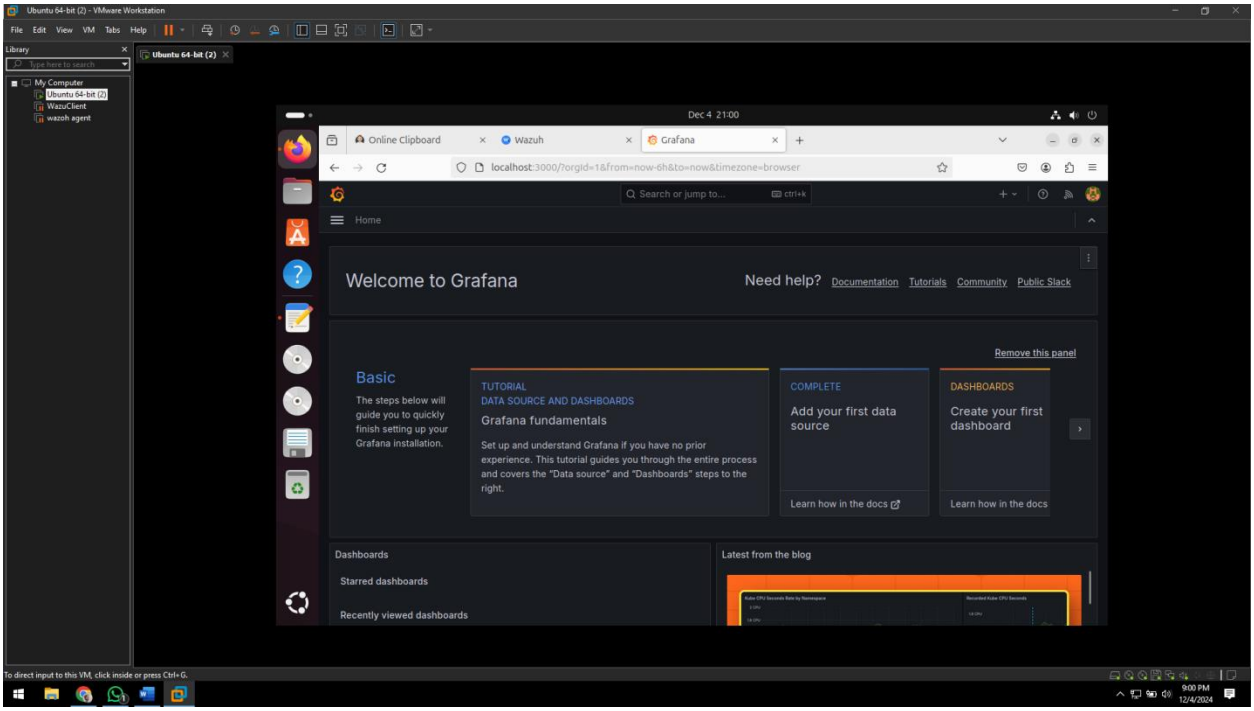
Grafana is installed to provide an interactive visualization interface for monitoring Wazuh SIEM data. Its integration with Elasticsearch allows users to create customized dashboards and analyze security events in real-time.

Steps:

1. Install Grafana on the server.
2. Configure Grafana to connect with Elasticsearch as a data source.
3. Create dashboards to visualize Wazuh metrics and logs for better insights.



Grafana dashboard:

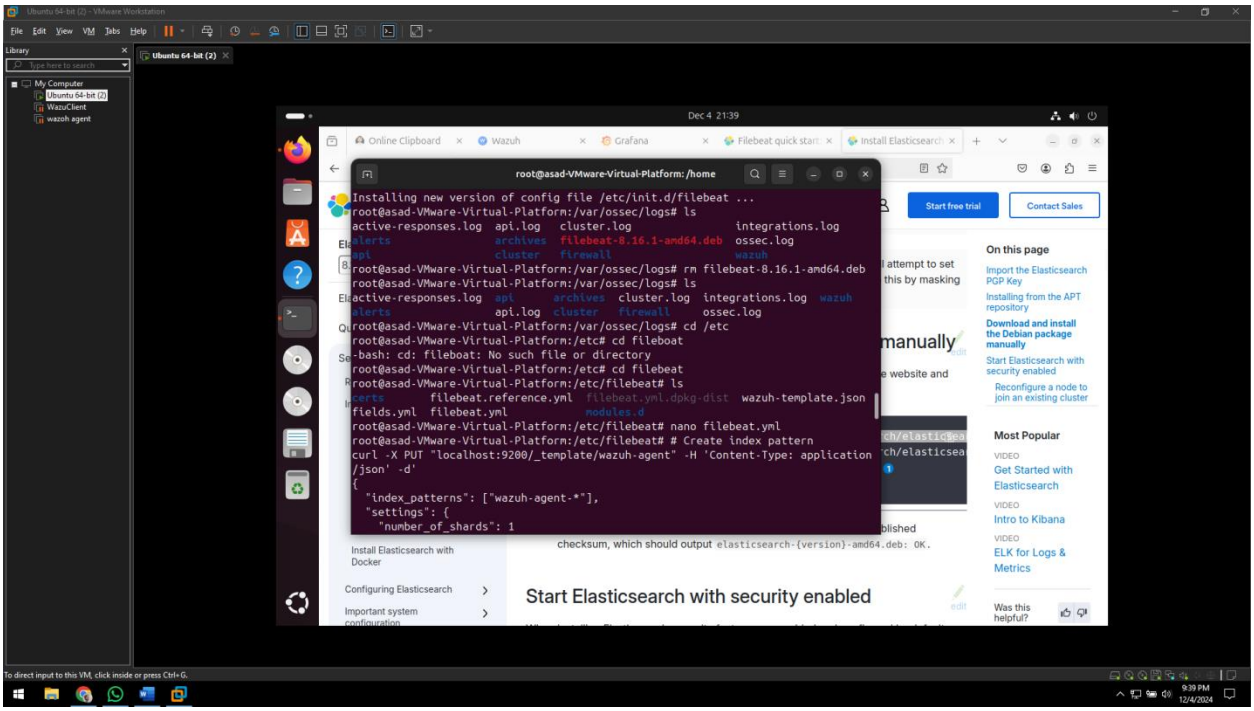


Filebeat Installation:

Filebeat, a lightweight log shipper, is installed to collect and forward Wazuh logs for analysis. It is configured using the filebeat.yml file to define log paths, processing logic, and the Elasticsearch output.

Steps:

1. Install Filebeat.
2. Configure filebeat.yml for Wazuh log processing and Elasticsearch integration.



Filebeat.yml configuration:

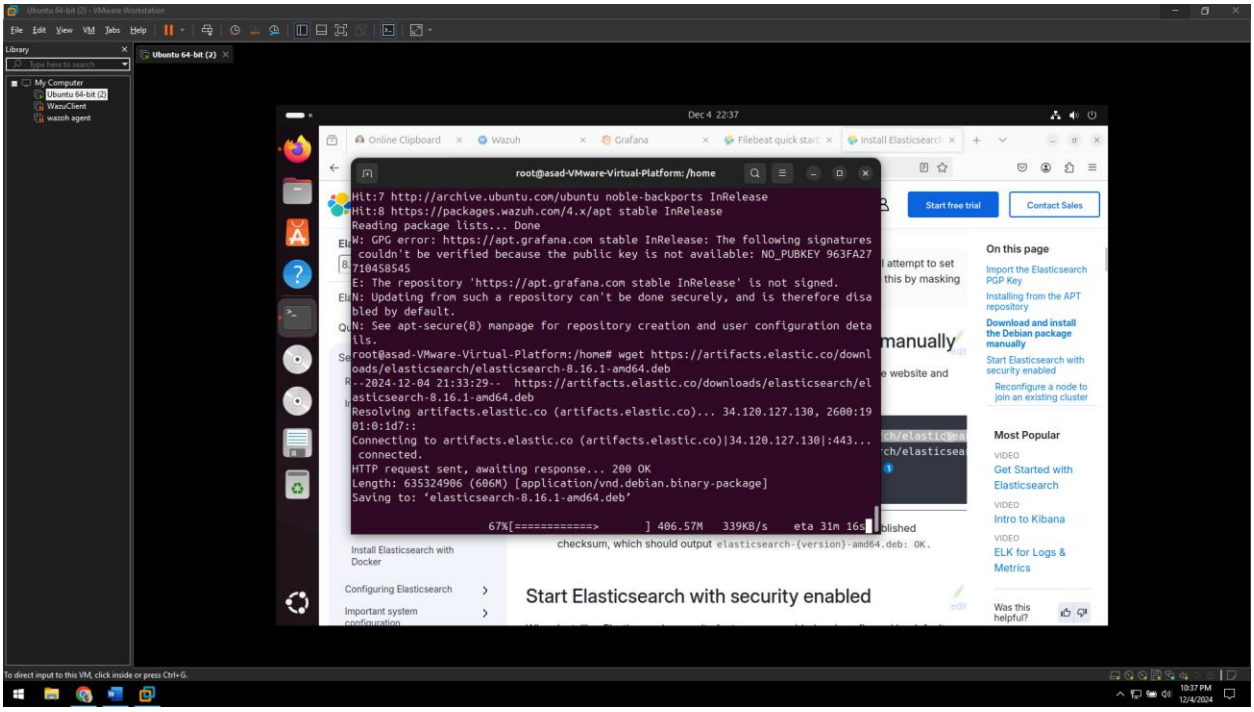
```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/ossec/logs/ossec.log
  fields:
    log_type: wazuh_agent
  fields_under_root: true
  json.keys_under_root: true

  # Custom processing to parse Wazuh log format
  processors:
    - dissect:
        tokenizer: "%{timestamp} %{log_level}: %{message}"
        field: "message"
        target_prefix: "wazuh"
    - timestamp:
        field: "timestamp"
        layouts:
          - "2006/01/02 15:04:05"
        target_field: "@timestamp"
    - drop_fields:
        fields: ["timestamp"]
```

```
output.elasticsearch:
  hosts: ["localhost:9200"]
  index: "wazuh-agent-%{+yyyy.MM.dd}"

setup.template.name: "wazuh-agent"
setup.template.pattern: "wazuh-agent-*"
setup.ilm.enabled: true
```

Elastic Search Installation:

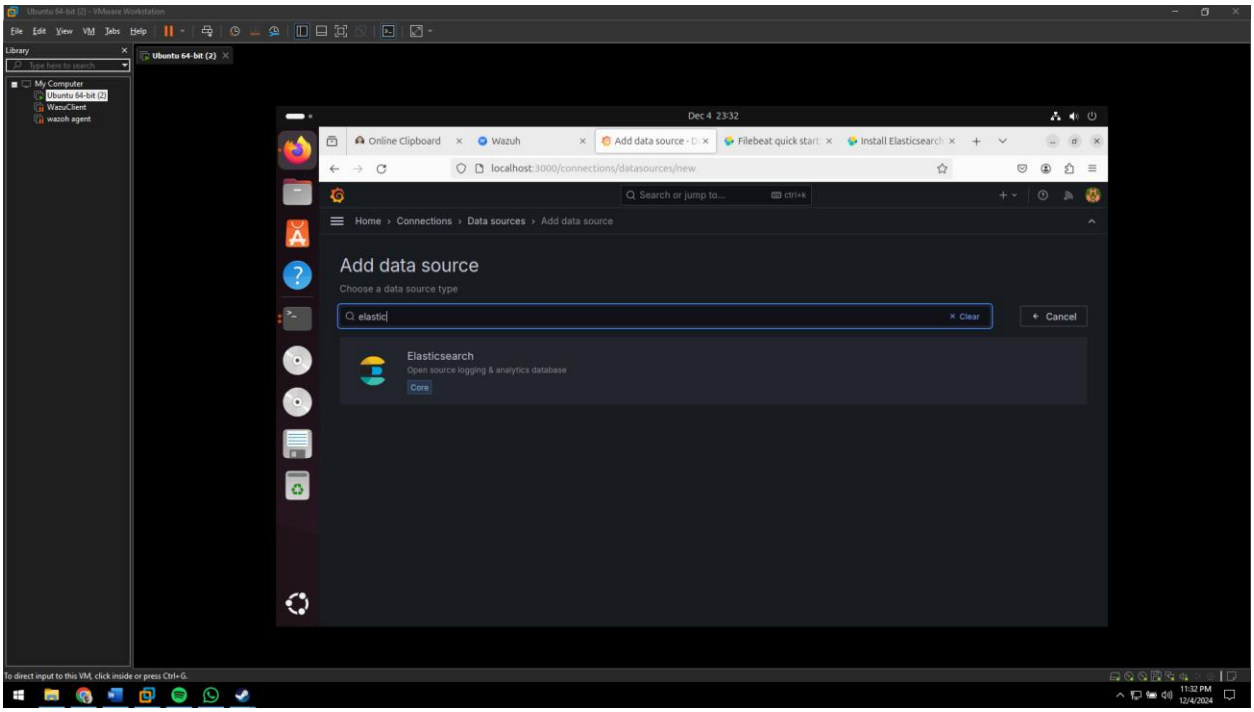


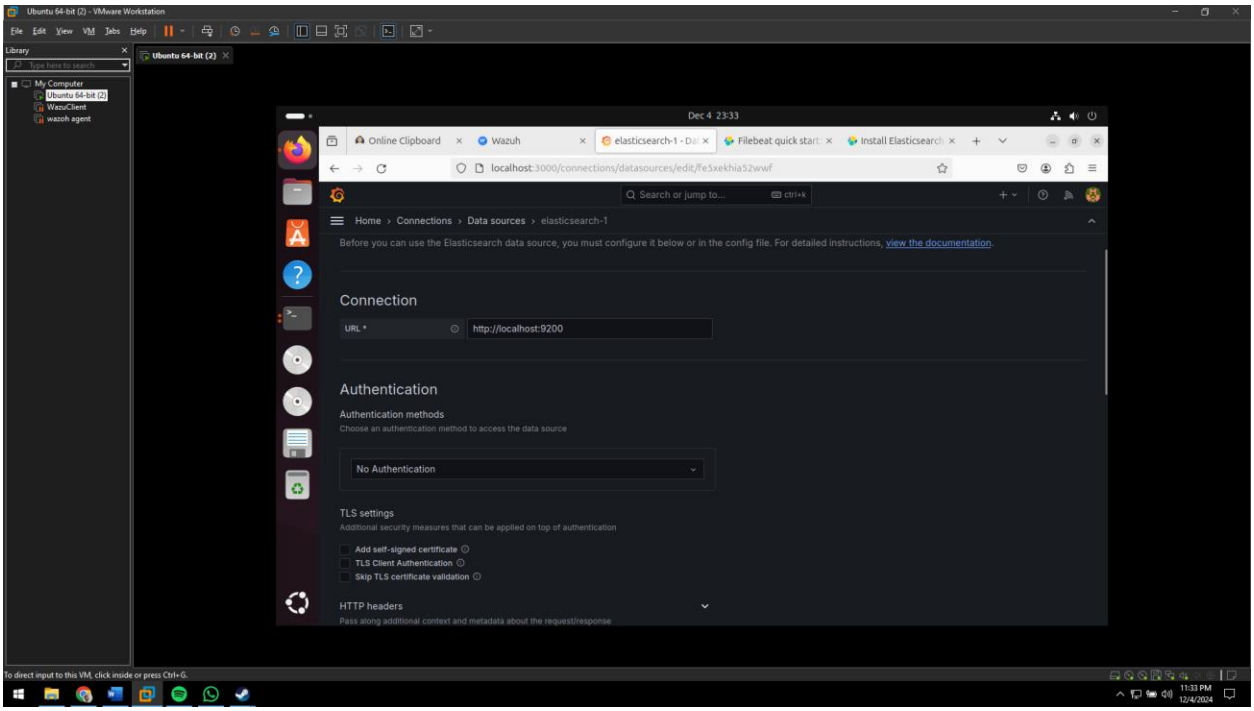
Elastic Search bash script for configuration:

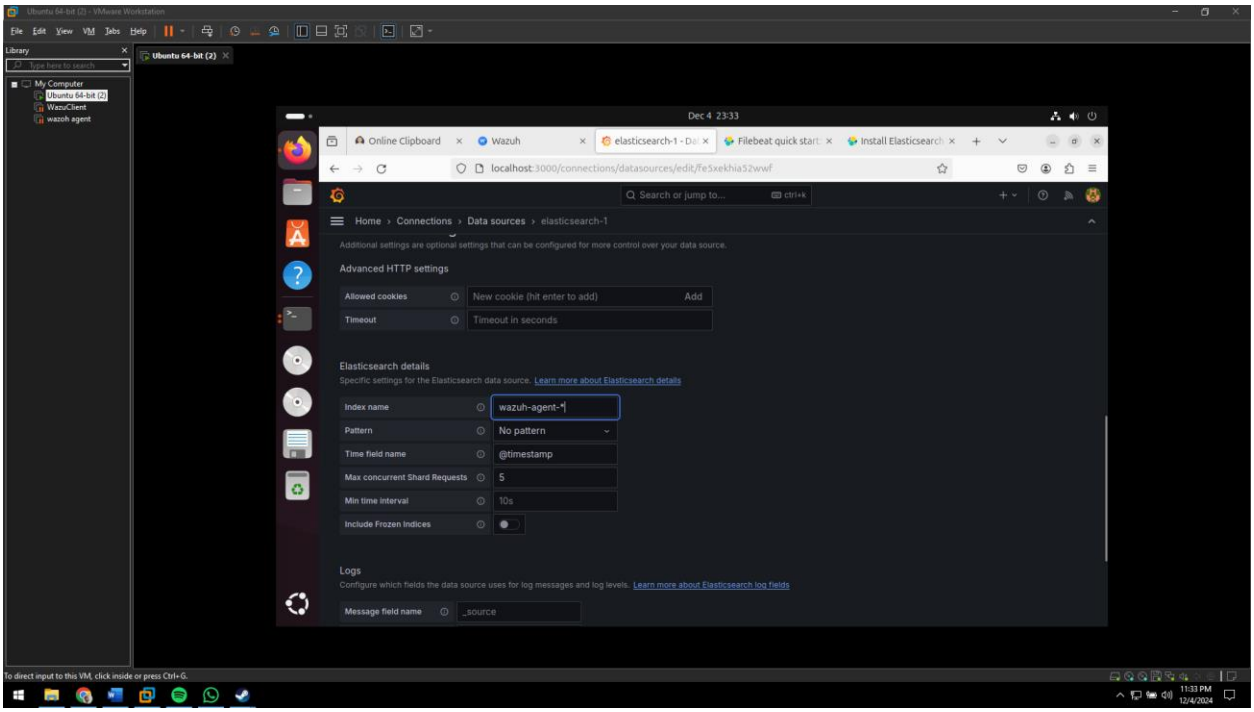
```
# Create index pattern
curl -X PUT "localhost:9200/_template/wazuh-agent" -H 'Content-Type: application/json' -d'
{
  "index_patterns": ["wazuh-agent-*"],
  "settings": {
    "number_of_shards": 1
  },
  "mappings": {
    "properties": {
      "@timestamp": {
        "type": "date"
      },
      "wazuh.log_level": {
        "type": "keyword"
```

```
    },
    "wazuh.message": {
      "type": "text"
    }
  }
 }
}'
```

Adding data source on grafana







Conclusion:-

Integrating Wazuh with Grafana provides a powerful SIEM solution that enhances security monitoring and log analysis capabilities. This setup leverages Wazuh's efficient data collection and event detection with Grafana's interactive dashboards to provide real-time visibility into

system performance and security events. By combining these tools, organizations can streamline their incident response process, identify threats more effectively, and ensure compliance with security standards.

The implementation process outlined in this report demonstrates a step-by-step approach to establishing a secure, scalable, and user-friendly SIEM environment. From configuring Wazuh components and agents to setting up Grafana dashboards and Elasticsearch indices, each step ensures the seamless integration of these technologies. The resulting system not only simplifies the management of security events but also provides actionable insights for proactive threat mitigation. By following this guide, organizations can significantly enhance their cybersecurity posture and maintain robust operational resilience.