

Project Report on SIEM

Submitted in partial fulfillment of the Requirement of the degree
Bachelor of Computer Application

By:

S. MANIKANTHAN	220714100106
B.RITTIKA RAO	220714100015
BISWA RANJAN MALIK	220714100082
SAMREEN KAUSHAR	220714100102
SAKSHI PRIYA	220714100045

Academic Year-2022-25

Under the esteemed guidance of

PUSHKAR KISHORE

Prof of BCA department



Centurion
UNIVERSITY

Department of Computer Science

**Centurion University of Technology and
Management**

(Bhubaneswar, Jatani, Khurda, Odisha-752050)

Department of Bachelor's in Computer Application
Centurion University, Bhubaneswar.

BONAFIDE CERTIFICATE

Certified that this project report “**SIEM**” is the Bonafide work of **S.MANIKANTHAN** who carried out the project work under my supervision. This is to further certify to the best knowledge, that this project has not been carried out earlier in this institute and the university.

SIGNATURE

Pushkar Kishore

Certified that the above-mentioned project has been duly carried out as per the norms of the college and statutes of the university.

SIGNATURE

Mr. Rakesh Ku. Ray

HEAD OF THE DEPARTMENT

CANDIDATE'S DECLARATION

I, hereby declare that the project report entitled “**SIEM**” is an original work, and the data provided in the study is authentic. This report has not been submitted to any other Institute for the award of any other degree by me.

Name of the Student: S.MANIKANTHAN

Signature of the Student:

Registration No: 220714100106

Place: Centurion University of Technology and Management, Jatni

Date:

ACKNOWLEDGEMENT

It is my pleasure to be indebted to various people, who directly or indirectly contributed in the development of this work and who influenced our thinking, behavior and acts during the course of study.

We also extend our sincere appreciation to **Mr. Rakesh Ray** who provided his valuable suggestions and precious time in accomplishing our project report.

We express our sincere gratitude to Prof. (Dr.) **Prof. Sujata Chakrabarti**, Dean Academics for providing academic support & opportunities.

We express our sincere gratitude to **Pushkar Kishore**, Project guide for providing academic support & opportunities.

Lastly, we would like to thank the almighty and our parents for their moral support and friends with whom we shared my day-to day experiences and received lots of suggestions those improved the quality of work.

Name of the Student: S.MANIKANTHAN

Signature of the Student :

Registration No: 220714100106

Place: Centurion University of Technology and Management, Jatni

Date:

INDEX

- 1. Certificate**
- 2. Declaration**
- 3. Acknowledgements**
- 4. Contents**
- 5. Abstract**
- 6. Chapters**
 - Chapter: 1 Introduction to Project**
 - Chapter: 2 Project Overview**
 - Chapter: 3 System Requirements**
 - Chapter: 4 Project Discussions**
 - 4.1 Key Features
 - 4.2 Key Designing Goals
 - Chapter:5 Implementation**
 - Chapter:6 Snapshot**
- 7. Conclusion**
- 8. Future Scope**
- 9. References**
- 10. Assessment**
- 11. Course Outcome Attainment**

ABSTRACT

This project focuses on the design and implementation of a Security Information and Event Management (SIEM) solution using Wazuh within an Active Directory (AD) environment. The increasing complexity of cyber threats demands robust security measures that can effectively monitor, detect, and respond to potential incidents. This project aims to showcase the capabilities of Wazuh as a comprehensive open-source SIEM tool tailored for real-time security monitoring and analysis.

The core components of this project include the setup and configuration of the Wazuh SIEM platform, log onboarding from various sources within the AD environment, and the development of customized use cases for detecting suspicious activities. Key features such as alerting mechanisms, dashboard creation, KPI monitoring, and incident response are implemented to enhance the visibility and security posture of the network. The project also incorporates threat hunting and threat intelligence, enabling proactive identification of potential threats before they escalate.

Through this implementation, the project demonstrates how Wazuh can be leveraged to build a scalable and efficient security monitoring solution. The report provides a detailed walkthrough of the configuration process, highlighting the integration of log sources, the setup of detection rules, and the creation of actionable alerts. This work serves as a practical guide for cybersecurity professionals seeking to enhance their skills in SIEM deployment and security operations, paving the way for further exploration into advanced topics like automated threat detection, compliance management, and continuous security improvement.

CHAPTER – 1

INTRODUCTION TO THE PROJECT

The project on **SIEM Implementation Using Wazuh in an Active Directory Environment** explores the development of a robust security monitoring solution tailored to the needs of a modern IT infrastructure. In today's rapidly evolving threat landscape, organizations require comprehensive tools to monitor, detect, and respond to a wide array of security incidents. Security Information and Event Management (SIEM) systems have become critical in this regard, offering centralized logging, real-time analysis, and enhanced incident response capabilities. This project leverages Wazuh, an open-source SIEM tool, to build a scalable and efficient security solution within an Active Directory (AD) environment, providing a practical setup for detecting and mitigating potential threats.

The implementation involves configuring the Wazuh SIEM platform, integrating it with an AD environment, and onboarding logs from various sources such as domain controllers, servers, and endpoints. Key components of the project include log collection and analysis, the development of use cases to detect suspicious activities, and the configuration of alerts for proactive monitoring. Additionally, dashboards are created to visualize key performance indicators (KPIs), while incident response mechanisms and threat intelligence capabilities are set up to enhance the overall security posture.

This project not only demonstrates the practical application of SIEM tools but also emphasizes advanced security practices such as threat hunting, KPI monitoring, and automated alerting. Through this implementation, participants gain hands-on experience in setting up a comprehensive security monitoring solution, managing logs and alerts, and responding to potential incidents. The hands-on nature of the project bridges the gap between theoretical learning and real-world security operations, equipping students and professionals with the skills necessary to safeguard organizational assets against cyber threats.

By completing this project, participants gain valuable insights into the complexities of SIEM implementation, the importance of continuous monitoring, and the integration of threat intelligence to enhance an organization's ability to detect and respond to security incidents effectively.

CHAPTER -2

Overview

This project centers on the **implementation of a Security Information and Event Management (SIEM) solution** using Wazuh within a simulated Active Directory (AD) environment. It offers a comprehensive, hands-on learning experience by allowing users to design, configure, and test a robust security monitoring framework without the need for extensive physical infrastructure. The setup replicates real-world scenarios where organizations deploy SIEM systems to enhance visibility, detect threats, and streamline incident response across their IT landscape.

Key learning objectives include:

- Deploying Wazuh as an integrated SIEM platform in an AD environment, incorporating various log sources for comprehensive monitoring.
- Configuring log collection from critical components such as domain controllers, servers, and endpoints to ensure extensive visibility.
- Developing tailored use cases for threat detection and implementing automated alert mechanisms for timely response to security incidents.
- Building interactive dashboards to visualize key performance indicators (KPIs) and monitor the overall security posture of the network.
- Enhancing capabilities for incident response, threat hunting, and leveraging threat intelligence for proactive security management.

CHAPTER – 3

SYSTEM REQUIREMENT

The requirements of the program are very basic. This program will run in most of the current computers and laptops. Still the basic requirements are: -

3.1 Hardware Requirements

Minimum Specifications:

- **Processor:** Dual-core CPU (Intel or equivalent)
- **RAM:** At least 4 GB for basic performance
- **Storage:** 35 GB or more to accommodate project files and software

Recommended Specifications:

- **Processor:** Octa-core CPU (Intel or Ryzen) for optimal performance
- **RAM:** 16 GB or higher for smooth multitasking
- **Storage:** 60 GB or more for enhanced storage capacity

3.2 Software Requirements

- **Wazuh Version:** 4.9.0 or the most current release version.

CHAPTER – 4

BRIEF DISCUSSION ABOUT OUR PROJECT

4.1 Key Features

- **SIEM Integration with AD Environment:**
Implements Wazuh as the SIEM tool within an Active Directory environment, providing centralized security monitoring and enhanced identity management.
- **Comprehensive Log Management:**
Collects and analyzes logs from various systems and applications to ensure robust security monitoring and compliance.
- **Dynamic Alerts and Visual Dashboards:**
Configures real-time alerts for critical security events and provides intuitive dashboards for monitoring system performance.
- **Incident Response Automation:**
Streamlines the incident response process for rapid detection, containment, and resolution of security threats.
- **Advanced Threat Hunting Capabilities:**
Proactively explores security data to identify hidden threats and vulnerabilities within the network.

4.2 Key Design Goals

- **Efficient Security Event Monitoring:**
Ensure real-time and reliable monitoring of security events across the network, minimizing false positives and providing accurate threat detection for seamless operations.
- **Optimized System Performance:**
Configure the network and SIEM tool to ensure low latency and efficient processing of logs and alerts, simulating real-world enterprise environments.
- **User-Friendly Dashboards and Interfaces:**
Design intuitive dashboards and interfaces in Wazuh, enabling easy access to critical insights and simplifying the analysis of security data.

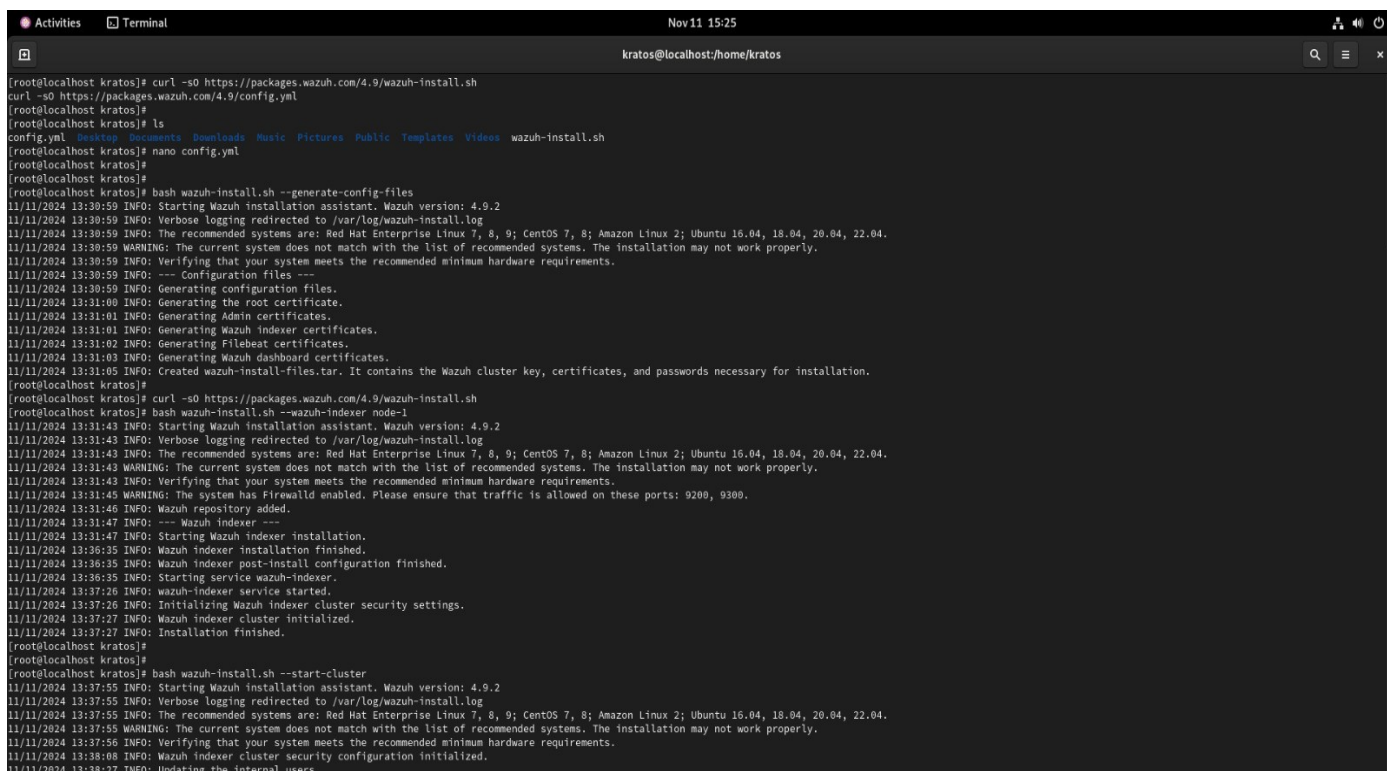
CHAPTER – 5

IMPLEMENTATION

The implementation of Wazuh involves setting up the server, deploying agents, integrating with Active Directory, configuring log collection, and customizing dashboards. It also includes creating use cases, setting up alerts, monitoring KPIs, and implementing incident response and threat hunting to ensure a robust security monitoring system.

1. Installing the Wazuh indexer using the assisted installation method:

- Download the Wazuh installation script and configuration files.
- Run the script to generate the necessary certificates and cluster configuration.
- Install Wazuh indexer.
- Start the Wazuh cluster.



```
[root@localhost kratos]# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
[root@localhost kratos]# curl -sO https://packages.wazuh.com/4.9/config.yml
[root@localhost kratos]# ls
config.yml  Downloads  Music  Pictures  Public  Templates  Videos  wazuh-install.sh
[root@localhost kratos]# nano config.yml
[root@localhost kratos]#
[root@localhost kratos]# bash wazuh-install.sh --generate-config-files
11/11/2024 13:30:59 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
11/11/2024 13:30:59 INFO: Verbose Logging redirected to /var/log/wazuh-install.log
11/11/2024 13:30:59 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
11/11/2024 13:30:59 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
11/11/2024 13:30:59 INFO: Verifying that your system meets the recommended minimum hardware requirements.
11/11/2024 13:30:59 INFO: --- Configuration files ---
11/11/2024 13:30:59 INFO: Generating configuration files.
11/11/2024 13:31:00 INFO: Generating the root certificate.
11/11/2024 13:31:01 INFO: Generating Admin certificates.
11/11/2024 13:31:01 INFO: Generating Wazuh indexer certificates.
11/11/2024 13:31:02 INFO: Generating Filebeat certificates.
11/11/2024 13:31:03 INFO: Generating Wazuh dashboard certificates.
11/11/2024 13:31:05 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
[root@localhost kratos]# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
[root@localhost kratos]# bash wazuh-install.sh --wazuh-indexer node-1
11/11/2024 13:31:43 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
11/11/2024 13:31:43 INFO: Verbose Logging redirected to /var/log/wazuh-install.log
11/11/2024 13:31:43 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
11/11/2024 13:31:43 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
11/11/2024 13:31:43 INFO: Verifying that your system meets the recommended minimum hardware requirements.
11/11/2024 13:31:45 WARNING: The system has Firewall enabled. Please ensure that traffic is allowed on these ports: 9200, 9300.
11/11/2024 13:31:46 INFO: Wazuh repository added.
11/11/2024 13:31:47 INFO: --- Wazuh indexer ---
11/11/2024 13:31:47 INFO: Starting Wazuh indexer installation.
11/11/2024 13:36:35 INFO: Wazuh indexer installation finished.
11/11/2024 13:36:35 INFO: Wazuh indexer post-install configuration finished.
11/11/2024 13:36:35 INFO: Starting service wazuh-indexer.
11/11/2024 13:37:26 INFO: wazuh-indexer service started.
11/11/2024 13:37:26 INFO: Initializing Wazuh indexer cluster security settings.
11/11/2024 13:37:27 INFO: Wazuh indexer cluster initialized.
11/11/2024 13:37:27 INFO: Installation finished.
[root@localhost kratos]#
[root@localhost kratos]#
[root@localhost kratos]# bash wazuh-install.sh --start-cluster
11/11/2024 13:37:55 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
11/11/2024 13:37:55 INFO: Verbose Logging redirected to /var/log/wazuh-install.log
11/11/2024 13:37:55 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
11/11/2024 13:37:55 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
11/11/2024 13:37:56 INFO: Verifying that your system meets the recommended minimum hardware requirements.
11/11/2024 13:38:08 INFO: Wazuh indexer cluster security configuration initialized.
11/11/2024 13:38:27 INFO: Updating the internal users.
```

A. IMPORTANT NOTE:-

- **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 IP "192.168.79.144".

2. Wazuh server cluster installation:

- Extract the wazuh-install-files.tar to retrieve admin credentials for cluster management.
- Use curl commands to verify the Wazuh indexer status and configuration details.
- Check cluster nodes and roles to ensure all components are properly configured.
- Download the Wazuh installation script from the official repository.
- Copy the wazuh-install-files.tar to the appropriate target directory.
- Ensure file paths and permissions are correctly set for seamless execution.

```
Nov 11 15:25
kratos@localhost/home/kratos

11/11/2024 13:38:27 INFO: Updating the internal users.
11/11/2024 13:38:35 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
11/11/2024 13:39:05 INFO: Wazuh indexer cluster started.
[root@localhost kratos]#
[root@localhost kratos]# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\admin\\"" -A 1
indexer_username: "admin"
indexer_password: "378ljn8sUdL7JvF7KM8SzgYngkS+8qJN"
[root@localhost kratos]#
[root@localhost kratos]# curl -k -u admin:378ljn8sUdL7JvF7KM8SzgYngkS+8qJN https://192.168.79.144:9200
bash: 378ljn8sUdL7JvF7KM8SzgYngkS+8qJN: No such file or directory
[root@localhost kratos]# curl -k -u admin:378ljn8sUdL7JvF7KM8SzgYngkS+8qJN https://192.168.79.144:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "5dJf936aRA2j1l4cUZ1sKA",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "0aa3533d9a82a2a9acf03285cc47dfe264c5a15b",
    "build_date" : "2024-10-28T15:29:00.446834Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
[root@localhost kratos]# curl -k -u admin:378ljn8sUdL7JvF7KM8SzgYngkS+8qJN https://192.168.79.144:9200/_cat/nodes?v
ip heap.percent ram.percent cpu load_1m load_5m load_15m node.role node.roles cluster_manager name
192.168.79.144 48 59 10 0.26 0.40 0.50 dimr data,ingest,master,remote_cluster_client * node-1
[root@localhost kratos]#
[root@localhost kratos]#
[root@localhost kratos]# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
[root@localhost kratos]# ls
Desktop Documents Downloads Music Pictures Public Templates Videos wazuh-install-files.tar wazuh-install.sh
[root@localhost kratos]# pwd
/home/kratos
[root@localhost kratos]# cp /path/to/original_file.tar /path/to/destination/directory/
bash: cp: command not found...
[root@localhost kratos]# cp /path/to/original_file.tar /path/to/destination/directory/
bash: /root: Is a directory
[root@localhost kratos]#
[root@localhost kratos]# cp /home/kratos/wazuh-install-files.tar /home/kratos/Document
[root@localhost kratos]# ls
Desktop Documents Music Public Videos wazuh-install-files.tar wazuh-install.sh
Document Downloads Pictures Templates wazuh-install-files.tar
```

• **IMPORTANT NOTE:**

If you want a Wazuh server single-node cluster, everything is set and you can proceed directly with [Installing the Wazuh dashboard using the assisted installation method](#).

3. Wazuh dashboard installation

- Copy and Extract Files:-

Moved wazuh-install-files.tar to the Documents directory and extracted the contents.

- Install Wazuh Manager:-

Ran `bash wazuh-install.sh --wazuh-server wazuh-1` to set up the Wazuh Manager, vulnerability detection, and Filebeat.

- Configure System Requirements:-

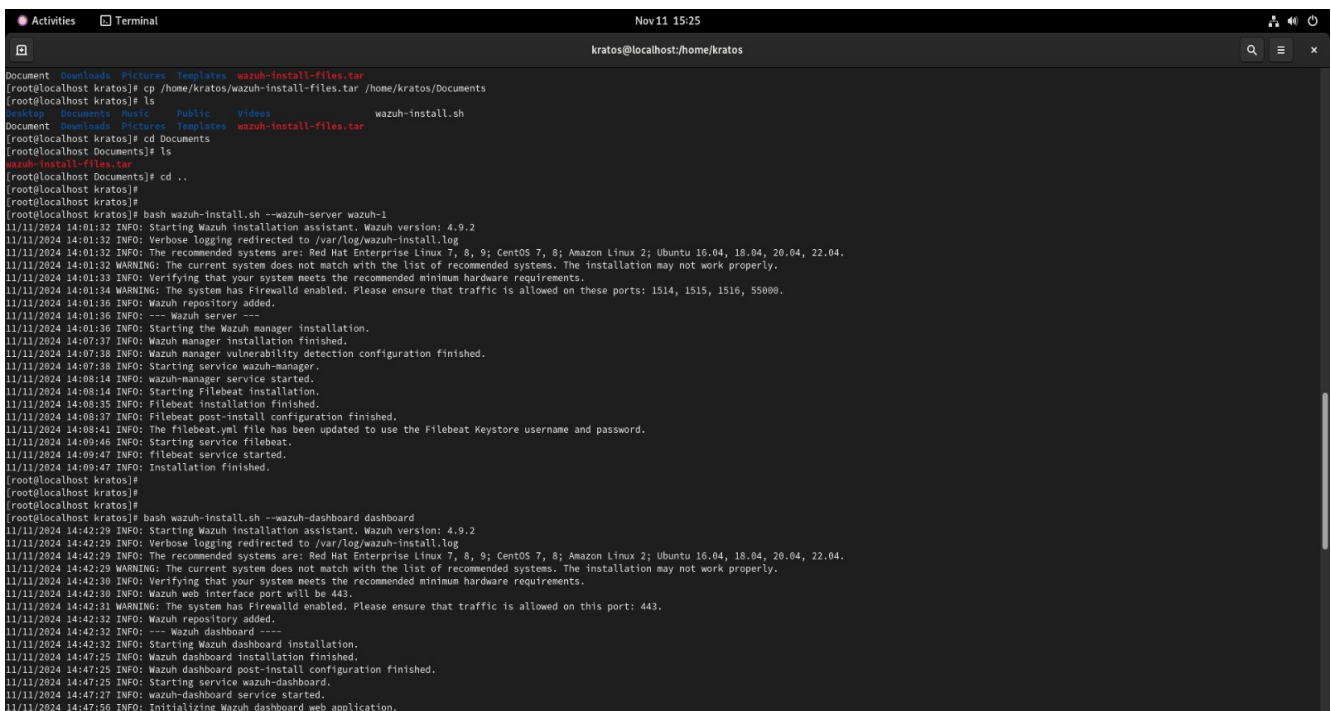
Addressed warnings about unsupported systems and ensured required firewall ports (1514, 1515, 1516, 55000) were open.

- Install Wazuh Dashboard:-

Executed `bash wazuh-install.sh --wazuh-dashboard dashboard` to set up the dashboard, ensuring port 443 was open.

- Verify Installations:-

Confirmed that all services (Manager, Filebeat, and Dashboard) were running properly.

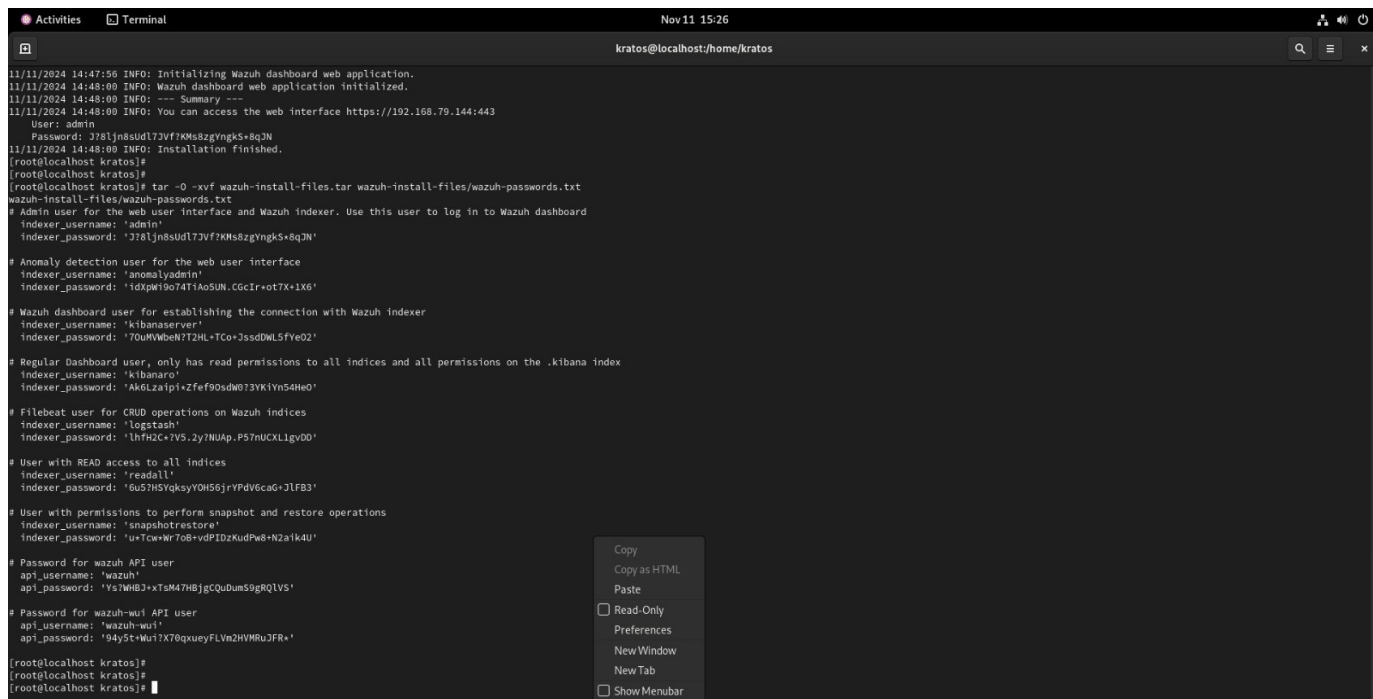


```
Nov 11 15:25
kratos@localhost/home/kratos

Document Downloads Pictures Templates wazuh-install-files.tar
[root@localhost kratos]# cp /home/kratos/wazuh-install-files.tar /home/kratos/Documents
[root@localhost kratos]# ls
Desktop Documents Music Public Videos wazuh-install.sh
Document Downloads Pictures Templates wazuh-install-files.tar
[root@localhost kratos]# cd Documents
[root@localhost Documents]# ls
wazuh-install-files.tar
[root@localhost Documents]# cd ..
[root@localhost kratos]#
[root@localhost kratos]#
[root@localhost kratos]# bash wazuh-install.sh --wazuh-server wazuh-1
11/11/2024 14:01:32 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
11/11/2024 14:01:32 INFO: Verbose logging redirected to /var/log/wazuh-install.log
11/11/2024 14:01:32 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
11/11/2024 14:01:32 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
11/11/2024 14:01:33 INFO: Verifying that your system meets the recommended minimum hardware requirements.
11/11/2024 14:01:34 WARNING: The system has FirewallD enabled. Please ensure that traffic is allowed on these ports: 1514, 1515, 1516, 55000.
11/11/2024 14:01:36 INFO: Wazuh repository added.
11/11/2024 14:01:36 INFO: --- Wazuh server ---
11/11/2024 14:01:36 INFO: Starting the Wazuh manager installation.
11/11/2024 14:07:37 INFO: Wazuh manager installation finished.
11/11/2024 14:07:38 INFO: Wazuh manager vulnerability detection configuration finished.
11/11/2024 14:07:38 INFO: Starting service wazuh-manager.
11/11/2024 14:08:14 INFO: wazuh-manager service started.
11/11/2024 14:08:14 INFO: Starting Filebeat installation.
11/11/2024 14:08:35 INFO: Filebeat installation finished.
11/11/2024 14:08:37 INFO: Filebeat post-install configuration finished.
11/11/2024 14:08:41 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
11/11/2024 14:09:46 INFO: Starting service filebeat.
11/11/2024 14:09:47 INFO: filebeat service started.
11/11/2024 14:09:47 INFO: Installation finished.
[root@localhost kratos]#
[root@localhost kratos]#
[root@localhost kratos]# bash wazuh-install.sh --wazuh-dashboard dashboard
11/11/2024 14:42:29 INFO: Starting Wazuh dashboard installation assistant. Wazuh version: 4.9.2
11/11/2024 14:42:29 INFO: Verbose logging redirected to /var/log/wazuh-install.log
11/11/2024 14:42:29 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
11/11/2024 14:42:29 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
11/11/2024 14:42:30 INFO: Verifying that your system meets the recommended minimum hardware requirements.
11/11/2024 14:42:30 INFO: Wazuh web interface port will be 443.
11/11/2024 14:42:31 WARNING: The system has FirewallD enabled. Please ensure that traffic is allowed on this port: 443.
11/11/2024 14:42:32 INFO: Wazuh repository added.
11/11/2024 14:42:32 INFO: --- Wazuh dashboard ---
11/11/2024 14:42:32 INFO: Starting Wazuh dashboard installation.
11/11/2024 14:47:25 INFO: Wazuh dashboard installation finished.
11/11/2024 14:47:25 INFO: Wazuh dashboard post-install configuration finished.
11/11/2024 14:47:25 INFO: Starting service wazuh-dashboard.
11/11/2024 14:47:27 INFO: wazuh-dashboard service started.
11/11/2024 14:47:56 INFO: Initializing Wazuh dashboard web application.
```

4. Find all the passwords

- Find all passwords that the Wazuh installation assistant generated in the wazuh-passwords.txt file inside the wazuh-install-files.tar archive.
- Extract the Wazuh installation files:
- View generated credentials for Wazuh and Kibana users.



```
11/11/2024 14:47:56 INFO: Initializing Wazuh dashboard web application.
11/11/2024 14:48:00 INFO: Wazuh dashboard web application initialized.
11/11/2024 14:48:00 INFO: --- Summary ---
11/11/2024 14:48:00 INFO: You can access the web interface https://192.168.79.144:443
User: admin
Password: J781jn8sUdL7JvF?KMs8zgYngkS+8qJN
11/11/2024 14:48:00 INFO: Installation finished.
[root@localhost kratos]#
[root@localhost kratos]#
[root@localhost kratos]# tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh Indexer. Use this user to log in to Wazuh dashboard
indexer_username: 'admin'
indexer_password: 'J781jn8sUdL7JvF?KMs8zgYngkS+8qJN'

# Anomaly detection user for the web user interface
indexer_username: 'anomalydetection'
indexer_password: 'idXpW19074TiAoSUN.CGCiR+oT7X+1X6'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username: 'kibanaserver'
indexer_password: '70uWVbeN7T2HL+TC0+JssdDWLSfy02'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
indexer_username: 'kibanaro'
indexer_password: 'Ak6LzaiPiZf99sdW0?3YK1Yn54He0'

# Filebeat user for CRUD operations on Wazuh indices
indexer_username: 'logstash'
indexer_password: 'lhfh2C+7VS.2y7NUAp.P57nUcXLIgv00'

# User with READ access to all indices
indexer_username: 'readall'
indexer_password: '6u57HSVqksyYOH56jrYPdV6cag+JLF83'

# User with permissions to perform snapshot and restore operations
indexer_username: 'snapshotrestore'
indexer_password: 'u+Tcw+Wr70B+vdPID2KudPw8+N2a1k4U'

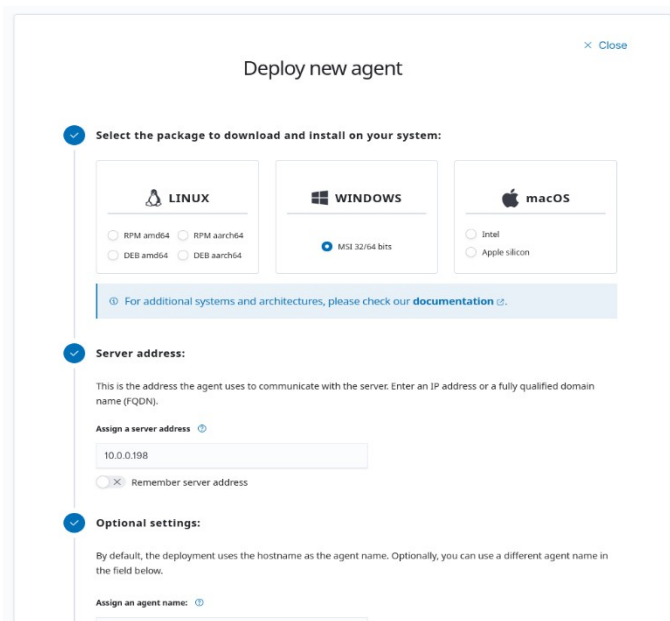
# Password for wazuh API user
api_username: 'wazuh'
api_password: 'Ys7WHB3+xTsm47HBjgQQuDumS9gRQlVS'

# Password for wazuh-wui API user
api_username: 'wazuh-wui'
api_password: '94y5t+Wu1?X70quxyFLVn2HVmRuJFR+'

[root@localhost kratos]#
[root@localhost kratos]#
[root@localhost kratos]#
```

5. Agent installation

- You can also deploy a new agent following the instructions in the Wazuh dashboard. Go to **Endpoints Summary**, and click on **Deploy new agents**.



Deploy new agent

Select the package to download and install on your system:

LINUX

☐ RPM amd64 ☐ RPM aarch64

☐ DEB amd64 ☐ DEB aarch64

WINDOWS

☒ MSI 32/64 bits

macOS

☐ Intel

☐ Apple silicon

For additional systems and architectures, please check our [documentation](#).

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

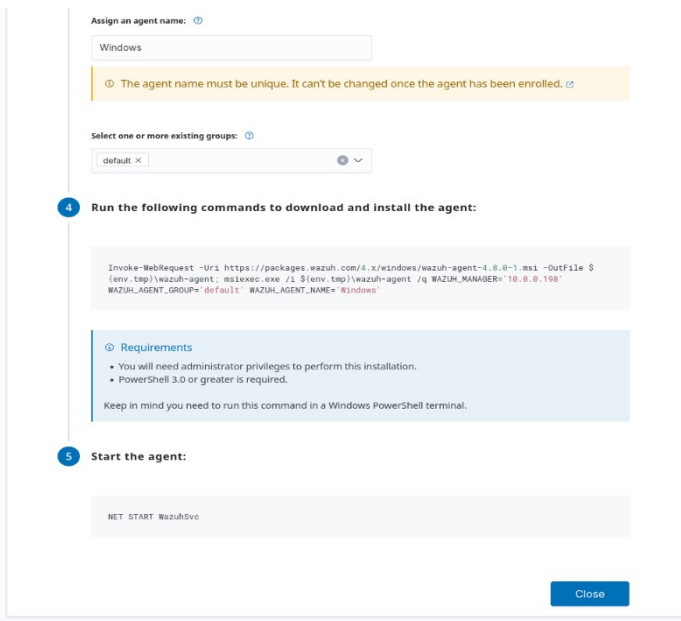
10.0.0.198

☐ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:



Assign an agent name:

Windows

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

default

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.0-1.msi -OutFile $
(env.tmp)\wazuh-agent.msi; msexec.exe /i $(env.tmp)\wazuh-agent.msi /q WAZUH_MANAGER="10.0.0.198"
WAZUH_AGENT_GROUP="default" WAZUH_AGENT_NAME="Windows"
```

Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

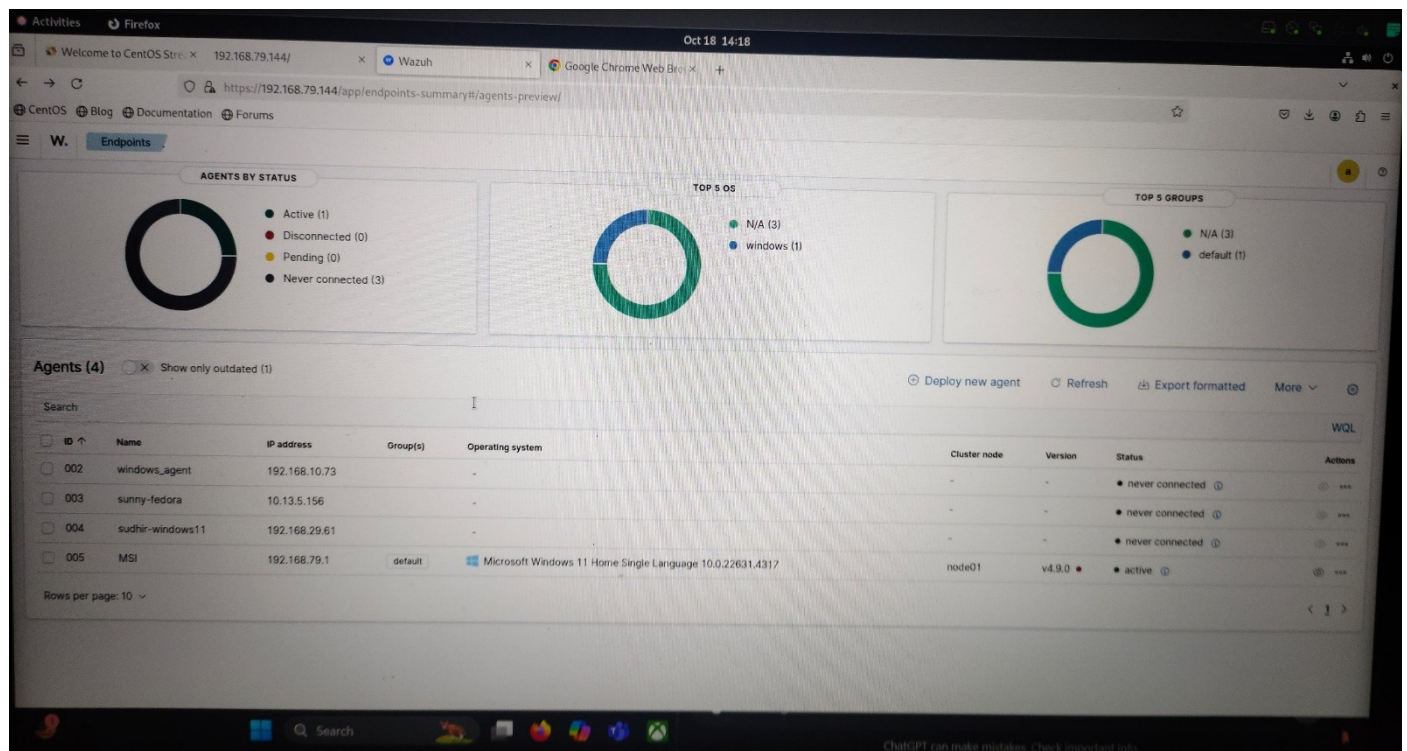
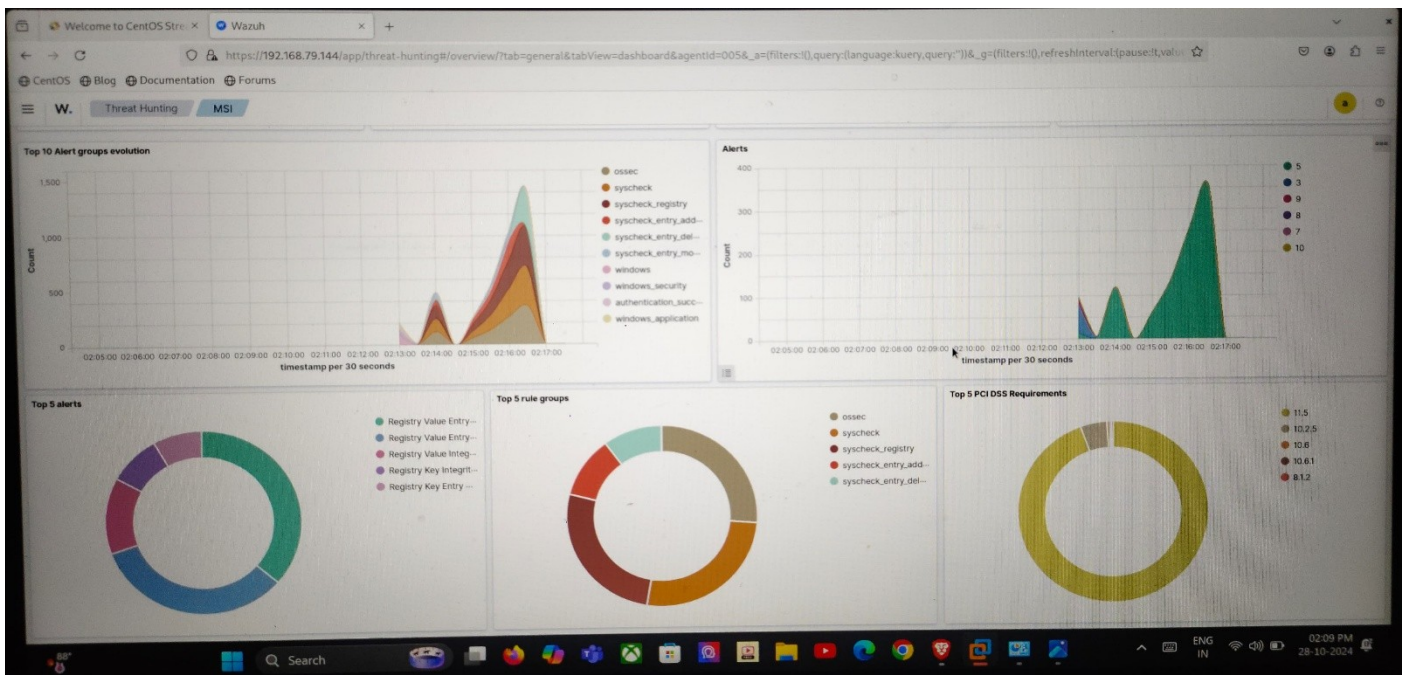
Start the agent:

NET START WazuhSvc

Close

CHAPTER -6

Snapshot



Conclusion

The successful implementation of a Wazuh-based SIEM solution highlights the critical importance of centralized security monitoring in modern IT ecosystems. By leveraging Wazuh agents, Elasticsearch, and Kibana dashboards, the project enables real-time threat detection, log analysis, and incident management across a diverse network infrastructure.

This deployment underscores the value of comprehensive log collection, tailored use case development, and proactive threat hunting to strengthen an organization's security posture. The integration of the Wazuh server with endpoint agents showcases the solution's scalability and flexibility for various environments.

Additionally, the project emphasizes the importance of KPI tracking, alerting systems, and threat intelligence in building a robust cybersecurity framework. By providing actionable insights and ensuring adherence to security policies, the Wazuh-based SIEM platform empowers organizations to effectively mitigate risks and respond to evolving threats. This hands-on experience has been instrumental in gaining expertise in SIEM deployment and cybersecurity best practices.

Future Scope

The implementation of the Wazuh-based SIEM solution lays a strong foundation for future advancements in cybersecurity monitoring and threat management. As cybersecurity threats continue to evolve, there are several potential areas for further development and enhancement:

1. **Integration with Advanced Threat Intelligence Platforms**

Future iterations can integrate Wazuh with advanced threat intelligence platforms like MISP (Malware Information Sharing Platform) or ThreatConnect. This integration will provide enhanced data feeds, allowing for more comprehensive threat detection and proactive defense strategies.

2. **Machine Learning and AI Integration:**

Incorporating machine learning and AI algorithms into the Wazuh platform can enable automated anomaly detection and more accurate threat classification. These technologies can assist in identifying sophisticated threats, reducing the time required for incident response.

3. **Scalability and Cloud Integration:**

The Wazuh solution can be expanded to scale across larger, distributed environments, supporting hybrid and multi-cloud setups. Moving the SIEM infrastructure to the cloud can also improve flexibility, resource management, and disaster recovery capabilities.

4. **Enhanced Log Analytics and Correlation:**

Future development can focus on improving log analytics and correlation rules to identify complex attack patterns and provide deeper insights into system behavior. By fine-tuning these capabilities, organizations can achieve faster threat detection and response times.

5. **Automated Incident Response:**

Introducing automation tools for incident response will allow the Wazuh platform to take predefined actions upon detecting specific types of security incidents. This automation could include isolating affected systems, blocking malicious IP addresses, or triggering alerts to relevant stakeholders.

Reference

- Wazuh Documentation: Comprehensive guides and official resources available on the Wazuh website for assisted setup and configuration.
- YouTube Tutorials on Wazuh: Assisted method tutorials, providing insights into Wazuh deployment, log monitoring, and threat detection.

Appendix

The appendix should contain computer programming (if any), the sample, calculations, explanation of theory (if any) etc which will be used as reference.

ASSESSMENT

Internal:

SL NO	RUBRICS	FULL MARK	MARKS OBTAINED	REMARKS
1	Understanding the relevance, scope and dimension of the project	10		
2	Methodology	10		
3	Quality of Analysis and Results	10		
4	Interpretations and Conclusions	10		
5	Report	10		
	Total	50		

Date:

Signature of the Faculty

COURSE OUTCOME (COs) ATTAINMENT

> Expected Course Outcomes (COs):

(Refer to COs Statement in the Syllabus)

> Course Outcome Attained:

How would you rate your learning of the subject based on the specified COs?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10

LOW

HIGH

> Learning Gap (if any):

➤ **Books / Manuals Referred:**

Date:

Signature of the Student

➤ **Suggestions / Recommendations:**

(By the Course Faculty)

Date:

Signature of the Faculty