Predictive Infrastructure Monitoring Dashboard Using Zabbix

NICHOLAS TSILIMIDOS

RACHAEL OYENOLA

REDDY SAI MANIKANTA

What is Zabbix

- Open-source IT monitoring tool used for servers, networks, applications, and websites.
- Collects real-time performance metrics such as CPU, RAM, disk usage, and network traffic
- Provides automated alerts and notifications when issues or failures occur.
- Supports multiple monitoring methods: agent-based, agentless, SNMP, API, and website checks.
- Offers dashboards, graphs, and reports for easy visualization and analysis of system health.

Why Zabbix?

- Free, open-source solution with enterprise-level monitoring capabilities.
- Supports a wide range of devices, servers, cloud services, and websites.
- Highly customizable alerts help detect issues early and reduce downtime
- Scalable for small setups to large enterprise environments
- Provides detailed dashboards,graphs,and reports for clear visibility of system performance
- Strong community support and extensive documentation make it easy to learn and troubleshoot.
- Integrates easily with automation tools, APIs, and third-party systems.

Introduction

- This project focuses on real-time monitoring using the open-source Zabbix platform.
- Zabbix provides the ability to track system health, service uptime, and network performance.
- Monitoring is a critical cybersecurity function that help detect issues early before they become incidents
- The goal was to simulate a real-world monitoring setup in a controlled virtual environment.

Project Objectives

- Install and configure Zabbix Server and Zabbix Frontend on an ubuntu VM
- Enable website monitoring using Zabbix web scenarios to track availability and response times
- Deploy and configure the Zabbix Agent to collect system metrics from the Ubuntu host.
- Analyze monitoring data using graphs, dashboards, and triggers to identify system behavior.
- Gain hands-on experience with infrastructure monitoring and cybersecurity tools.

Project Relevance

- Monitoring tools like Zabbix are essential in cybersecurity operations and incident response.
- They help detect suspicious activity, system failures, performance issues, and downtime.
- Skills gained include Linux administration,server setup,network monitoring,and alert configuration.
- Zabbix is commonly used in soc's,IT operations,and digital forensics for evidence collection
- This project builds foundational Knowledge required for cybersecurity roles

Setup & Environment

- VirtualBox used to host the ubuntu virtual machine where Zabbix was installed.
- Ubuntu OS updated with necessary packages, repositories, and dependencies
- Apache,MYSQL,php installed to support the Zabbix frontend.
- Network configuration ensured the VM had full internet access for external monitoring.
- Browser access allowed connection to the Zabbix web UI from the host machine
- Monitored the UAlbany website and created triggers in case of website is unavailable.it will trigger the alert so that the appropriate team can handle the error

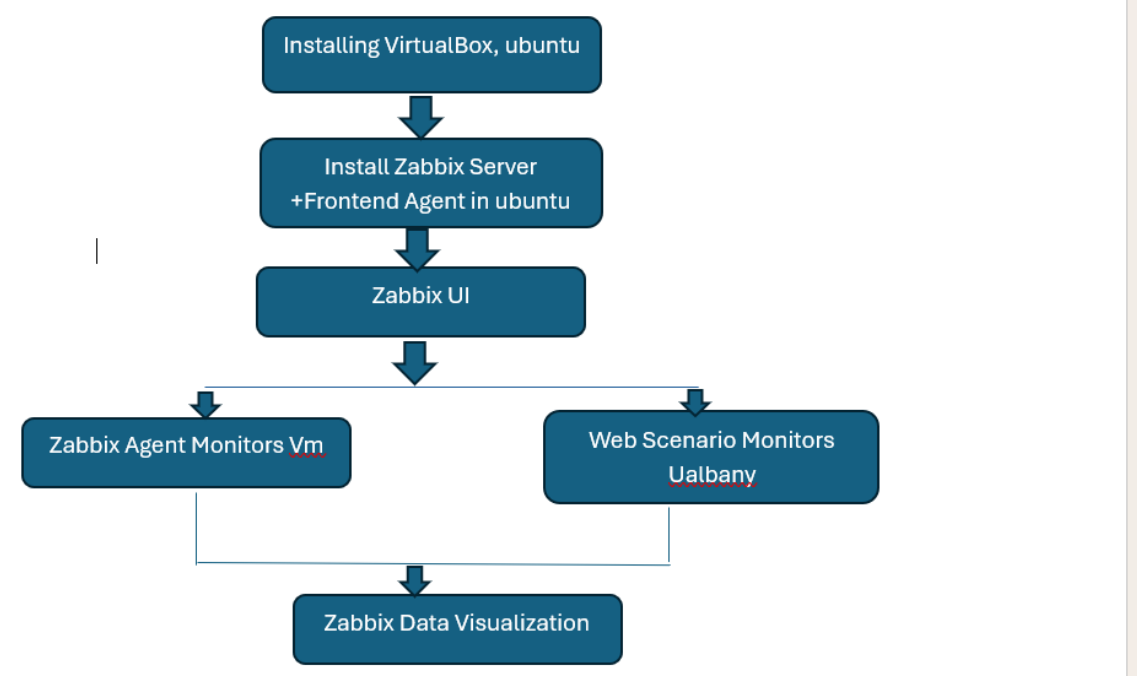
Tools Used

- **VirtualBox:** Virtualization platform used to create and run the Ubuntu VM.
- **Ubuntu Linux:** Operating system hosting Zabbix Server, Frontend, and Agent.
- **Zabbix Server:** Processes monitoring data and manages triggers and events.
- **Zabbix Frontend:** Web interface used to configure hosts, view dashboards, and analyze metrics.
- **Zabbix Agent:** Installed on the Ubuntu host to collect CPU, memory, disk, and network metrics.
- **Web Scenario:** Built-in Zabbix feature for website monitoring and HTTP checks.

Architecture Overview

- Zabbix Server is the central component that stores and processes all monitoring data.
- Zabbix Frontend allows the user to interact with the server via a browser interface.
- Zabbix Agent collects detailed system metrics directly from the Ubuntu host.
- Web scenarios allow Zabbix to monitor external websites such as UAlbany.
- All data flows into the Zabbix database and is displayed through dashboards and graphs.

Workflow



Summary:

- Installed Ubnutu on virtual box and configured Mysql,php,apache2 services
- Installed Zabbix Server,Agent,and Frontend using official repositories
- Accessed the Zabbix dashboard and performed initial configuration
- Added ualbany website as a monitored target using web Scenario checks and created triggers
- Created Ubuntu hosts and monitored the host using zabbix

Monitoring UAlbany website

- Configured a web scenario to monitor the official UAlbany website.
- Zabbix sent periodic HTTP/HTTPS requests to measure website response time.
- Added steps to check status codes and validate page availability.
- Configured triggers to alert if the website becomes unreachable or responds too slowly.
- Useful for identifying downtime, slow performance, or connection issues.

Monitoring Ubuntu Host

Installed and enabled the Zabbix Agent on the Ubuntu VM.

Agent collected CPU load, memory usage, disk space, network traffic, and system uptime.

Linked the host with the “Template OS Linux” for automatic monitoring items

Results displayed through graphs, latest data logs, and real-time charts

Helps detect hardware stress, resource issues, or Unusual activity

Results & Observations

Zabbix successfully monitored both the UAlbany website and the Ubuntu host.

Dashboard showed consistent updates to performance metrics and website status.

CPU, memory, and network usage were accurately tracked on the VM

Website monitoring confirmed the uptime and response stability of the Ualbany Site

No major errors encountered, configuration was stable and functional

Conclusion

- The project successfully demonstrated the installation and use of Zabbix for monitoring.
- Monitoring both internal (Ubuntu host) and external (UAlbany website) systems provided practical insight.
- Gained valuable Cybersecurity Skills including server setup, monitoring, configuration, and data analysis
- Zabbix proved to be a powerful tool for identifying performance issues and ensuring system reliability
- This hands-on experience contributes directly to real-word cybersecurity and system administration practice.

THANK YOU