Automated IT Monitoring With Logs

Agenda

01

Overview

We will discuss the project's overview, scope and architecture

02

Live Demo

We will perform a live demo of the project

03

Key Technologies

We will discuss the technologies we will be using in the project

04

Conclusion

We will discuss what was accomplished and next steps

05

Q & A

We will give the audience time to ask questions

Automated IT Infrastructure Monitoring Benefits

- Proactive Anomaly Detection
- Compliance and Security
- Enhanced Reliability
- Cost Efficiency
- Performance Optimization

01

Project Overview

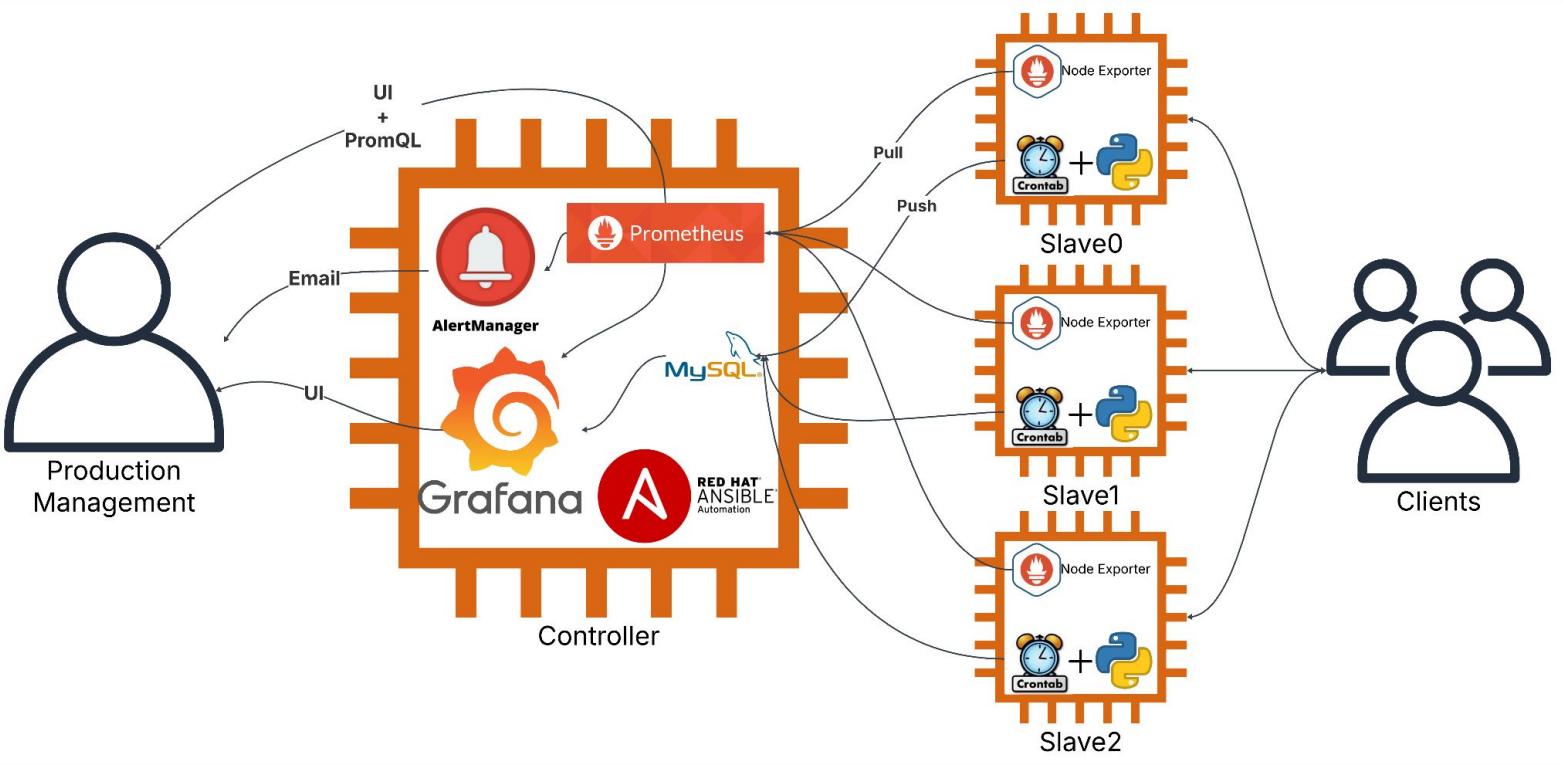
Objective

Implement an automated IT infrastructure monitoring and log management system that utilizes AWS EC2, Ansible, Prometheus, Grafana, Python, and MySQL. This system will ensure proactive monitoring, real-time visualization of server metrics, log collection, storage, and automated alerting for system anomalies.

Scope

- Automate deployment of Prometheus, Node Exporter, and Grafana using Ansible.
- Install Python and MySQL using Ansible.
- Install Node Exporter on target servers using Ansible.
- Collect system metrics such as CPU, memory, disk usage, and network activity.
- Use Grafana for real-time visualization of metrics.
- Implement Prometheus Alertmanager to send notifications based on predefined thresholds.
- Use a Python script to scrape logs and store them in a MySQL database.

Project Architecture



02

Live Demo

03

Key Technologies

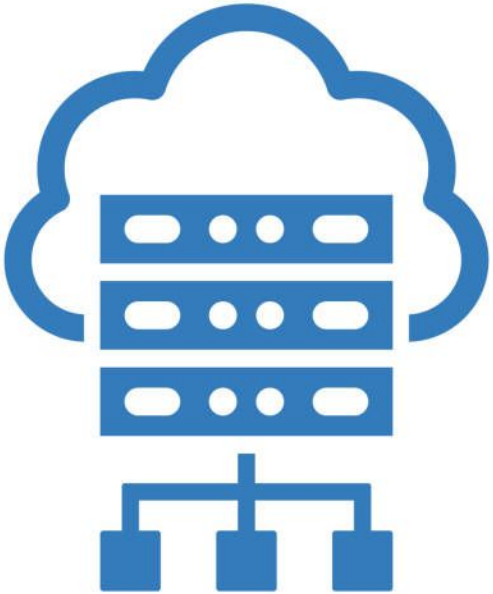
AWS EC2 & SSH

What is AWS EC2?

- Scalable virtual cloud servers
- Key Features
  - Scalable Resources
  - On-Demand Pricing
  - Flexible Instance Types
- Use Cases
  - Web Hosting
  - Application Servers
  - Databases

How it works?

- **Core Functionality:**
  - Virtual Servers
  - Customizable Resources
  - Cloud-Based Instances
- **How It Works:**
  - Choose Instance
  - Launch Instance
  - SSH Access
  - Scale Resources



What is SSH?

- Secure remote access
- **Key Features:**
  - Encryption
  - Authentication
  - Remote Access
- **Use Cases:**
  - Server Management
  - File Transfers

How it works?

- **Core Functionality:**
  - Remote Server Access
  - Secure Communication
- **Authentication Methods:**
  - Password
  - Key-Based
- **Typical Use:**
  - Administer Servers
  - Execute Commands

AWS EC2 and SSH in this Project?

- **AWS EC2 in the Project:**
  - Hosts Monitoring Stack
  - Scalable Infrastructure
- **SSH in the Project:**
  - Secure Setup & Configuration
  - Remote Management
- **Together in the Project:**
  - EC2 + SSH = Secure Automation

Ansible

What is Ansible?

- Open-source IT automation tool
- Simplifies process of managing and configuring multiple servers

How Does It Work?

- Control Node
- Playbooks
- Inventory
- Modules

Why Use Ansible?

- Agentless
- Declarative
- Idempotent
- Scalability
- Integration

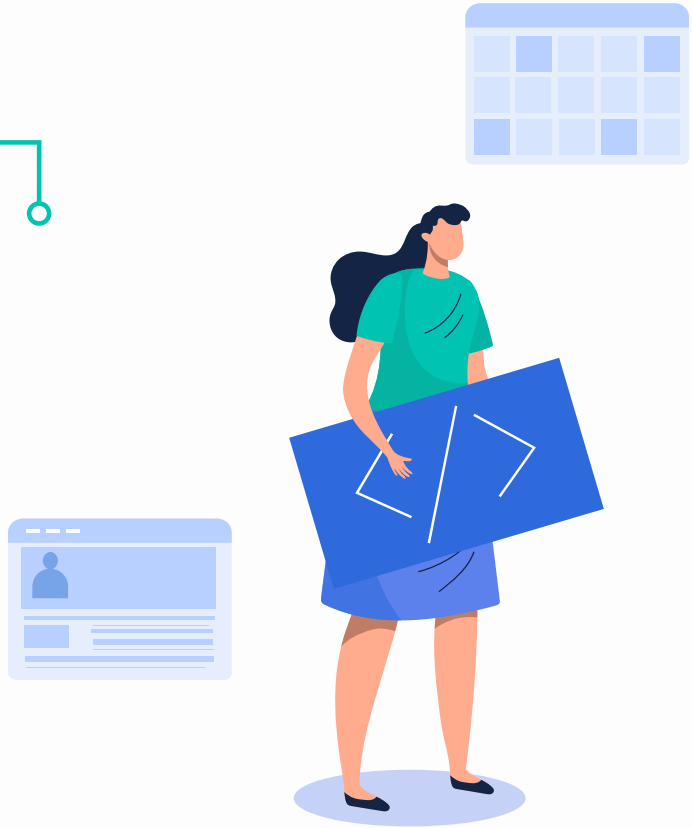
Ansible in this Project

Automates Installation

Ensures efficient and error-free deployment

Simplifies Configurations

MySQL



What is SQL

- Structured Query Language
- It’s a programming language used for querying, manipulating, and managing databases.

MySQL

- Open Source RDBMS
- Uses SQL to manage and organize data

MySQL in this project

- Store logs collected by the Python script
- Structured log storage, easy querying, and efficient log analysis to help identify patterns and troubleshoot system issues

Python

Python

- A widely-used open-source programming language
  - Object oriented, and thus can perform on the ‘4 Pillars of OOP’.
  - Interpreted line-by-line, which means Python script can be modified as needed as it’s running.
  - Multi-platform.
  - Hundreds of libraries and frameworks.

Python in the Project

- In our project, we use Python to collect metrics data and send logs of that data to a MySQL database.
- Script activated on each worker using an Ansible playbook.

Prometheus

What is Prometheus

- Open-source systems monitoring and alerting toolkit
- Records real-time metrics in a time series database
- Built using a HTTP pull model
    - Times series data identified by metric name and key/value pairs

How Does Prometheus Work

- Exposes metrics via HTTP
- Discovers targets via service discovery or static configuration
- Has a multi-dimensional data model
- PromQL
    - Flexible query language is used to leverage this dimensionality

Prometheus Use Cases

- Measures application runtimes
- Monitors and measures the stability of your services
- Alerts you to errors

How did we use Prometheus?

- Automatically collecting system metrics
- Detecting issues using predefined alerting rules
- Storing performance data for analysis
- Providing real-time monitoring

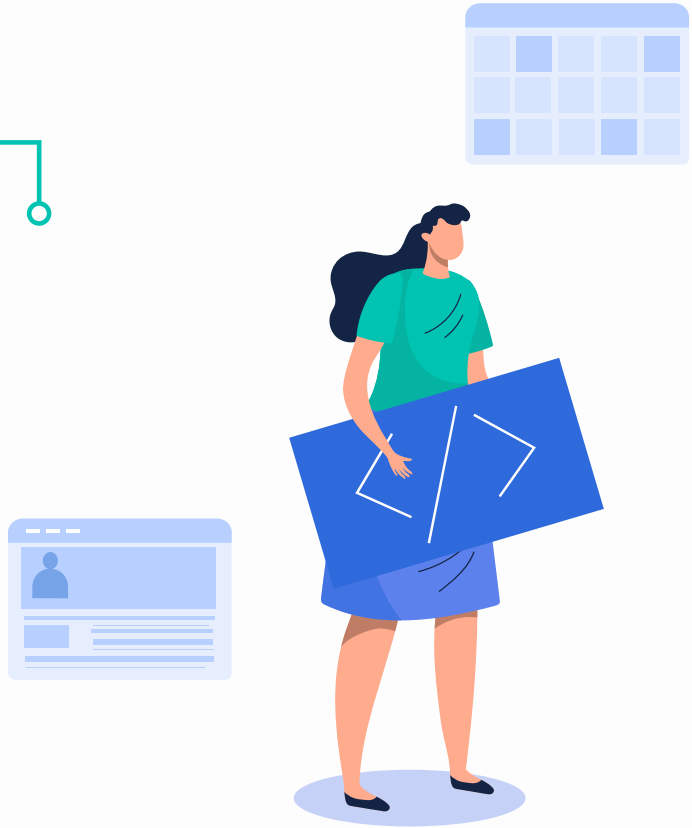
Analysis and Visualization

- **Queries(PromQL) for insights:**
- CPU and memory trends over time
- **Alerts Handling**
- Prometheus → Alertmanager
- **Dashboards:**
- Grafana for visualization

Node Exporter

What is Node Exporter

- A Prometheus Exporter for hardware and OS-level metrics.
- Collects system metrics from Linux based systems and exposes them in a format that Prometheus can scrape for monitoring and alerting.



Node Exporter Metrics

- CPU Usage
- Memory Usage
- Disk I/O
- Network Statistics
- System Load

Key Features of Node Exporter

- System Metrics Collection
- Multi-Module Support
- Exporter for Prometheus
- Text-Based Metrics Endpoint
- Minimal Resource Usage

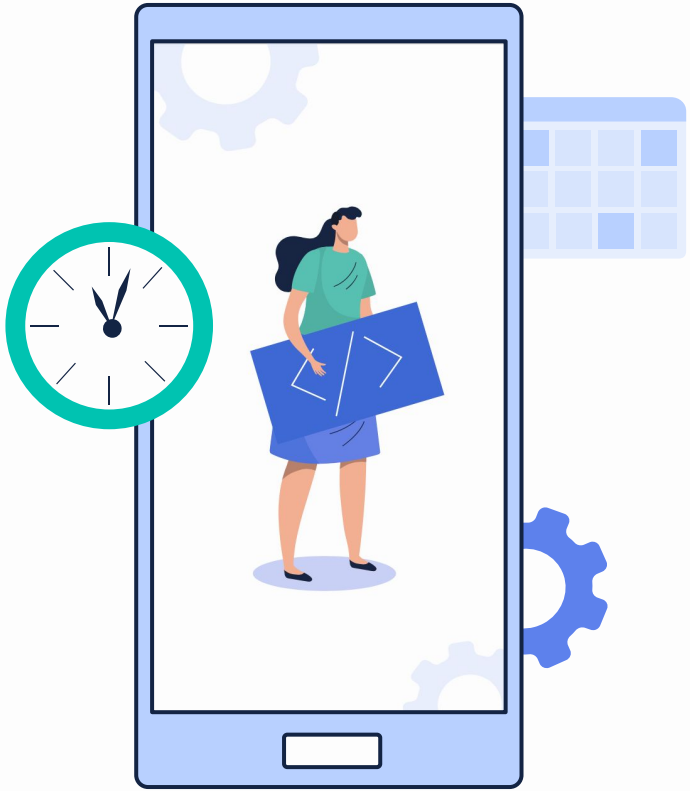
How we used Node Exporter

- Deployed Node Exporter on workstations.
- Collected workstation metrics using Prometheus.
- Integrated with Alertmanager for alerts.
- Integrated with Grafana for visualizations.

AlertManager

What is AlertManager?

AlertManager is a component of Prometheus that handles alerts generated while Prometheus is monitoring a system.



Key Features of AlertManager

Deduplication

Will merge duplicate alerts to prevent excessive notifications

Silencing

Temporary suppression of alerts based on set conditions

Grouping

Combines related alerts for easier management

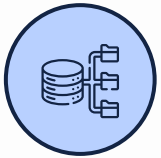
Inhibition

Prevent low-priority alerts triggering when high-priority alerts are active

Routing

Direct alerts to appropriate receivers with predefined rules

How are we using AlertManager?



Instance Monitoring

If metrics are not received from an instance, Prometheus triggers alert

Alerting Logic

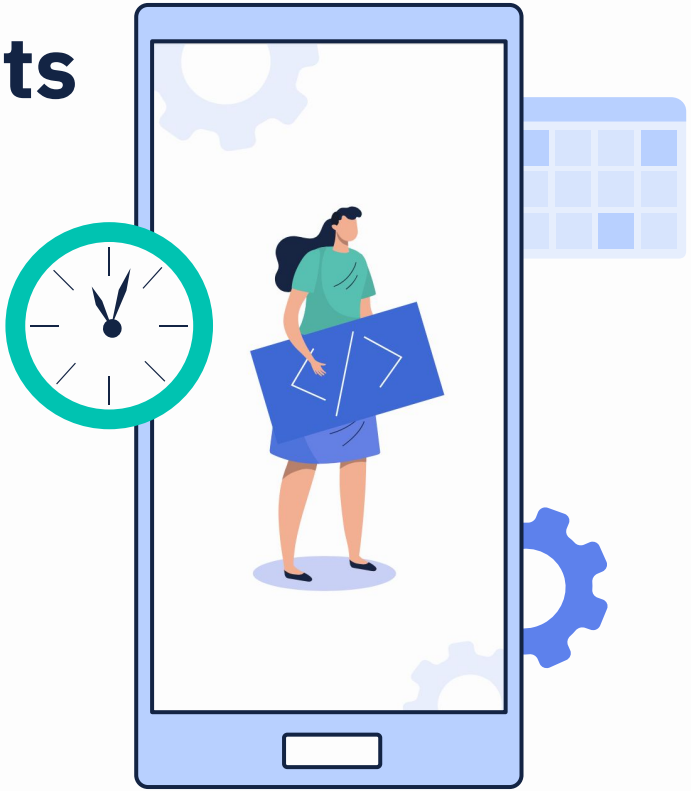
AlertManager routes alerts from Prometheus to appropriate destinations

Email Notifications

When AlertManager receives an alert, send a warning email

AlertManager Benefits

- Proactive Monitoring
  - Detecting instance downtime as soon as possible enables faster issue resolution
- Automated Notifications
  - Reduces manual effort required for monitoring and alerting
- Customizable Alerts
  - Alerts can be tailored to specific levels of severity and routed appropriately



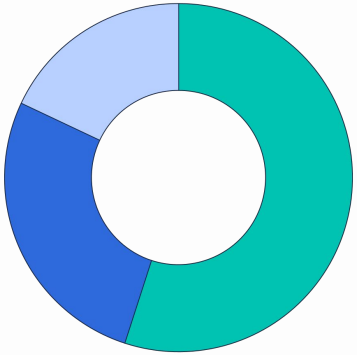
Grafana

What is Grafana?

- open-source analytics and visualization platform
- monitoring and observation

How it works?

- Infrastructure Monitoring
- Application Performance
- Business metrics



04
Conclusion

What was Accomplished?

- Automated Deployment
- Real-Time Monitoring
- Log Scraping
- Alerting

Next Steps

- Enhance Monitoring
- Testing & Validation
- Scale Infrastructure
- Automation Improvements

Project Relevance to Production Management

- Proactive Monitoring
- Operational Efficiency
- Scalability
- Data-Driven Decisions

05

Questions?

Thank You!