Document Name	Design Document of Prometheus & Grafana
Version	1.3
Prepared by	Harishvar M
Validated by	Guru Raghav
Approved by	Mahavishnu
Date	24.06.2024

Version No.	Date	Revised by	Description of Changes
1.0	05.01.2024	Harishvar M	First Version
1.2	10.03.2024	Harishvar M	Second Version
1.4	03.06.2024	Harishvar M	Third Version

1CloudHub

Table Of Contents

Introduction 3

Architecture Diagram 3

Security Considerations 4

Design considerations 5

User & Access management 5

Dashboards 6

Alerts & Event Co-relation 7

Alerts Acknowledgement & Downtime 7

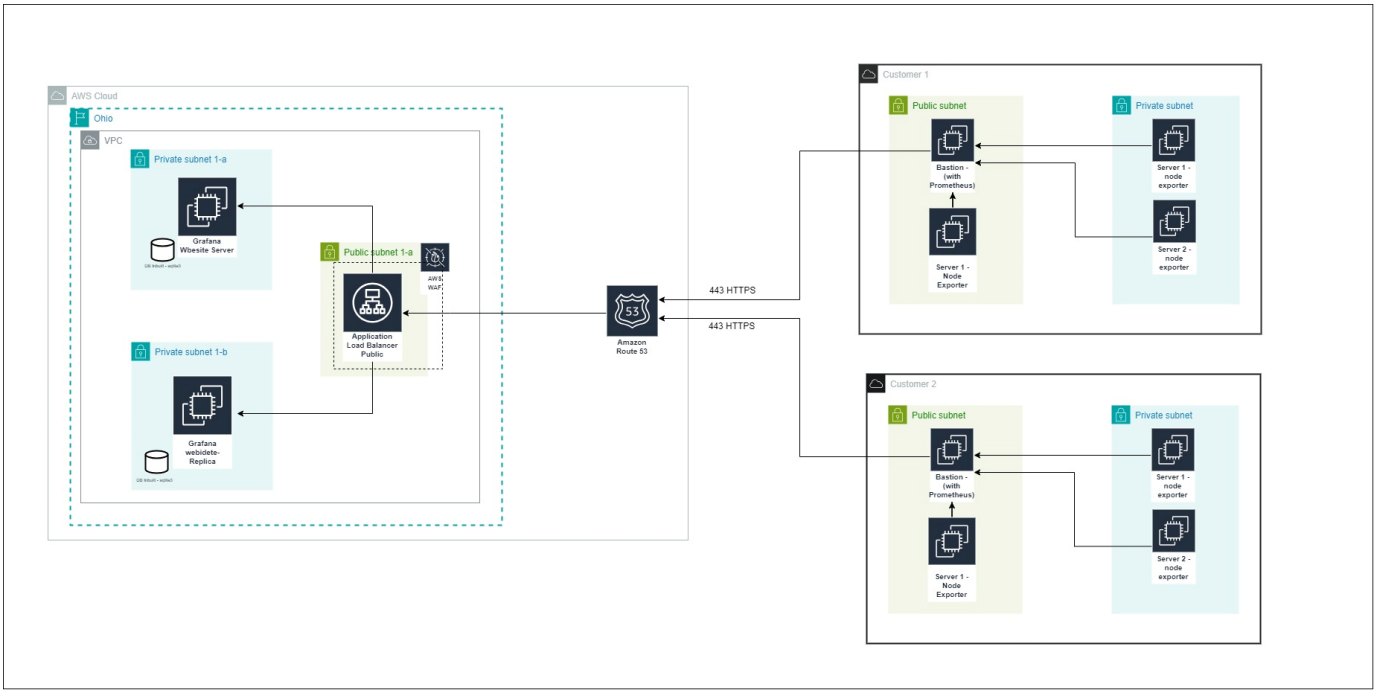
Implementation 8

Prerequisites 9

Conclusion 9

Introduction

Prometheus is an open-source monitoring system and time-series database designed to collect and display metrics from various systems. It offers powerful querying, alerting, and visualization capabilities. It is well-suited for dynamic service discovery and recording rules. Highly customizable and highly scalable. Grafana's flexible and customizable interface makes it suitable for building comprehensive monitoring solutions.



Architecture Diagram

Security Considerations

Authentication and Authorization

1. **User Authentication**: Implement strong user authentication mechanisms, such as LDAP, OAuth, or integration with single sign-on (SSO) solutions.
2. **Role-Based Access Control (RBAC)**: Use RBAC to define and enforce who can access specific resources and perform certain actions within Grafana.

Network Security

1. **Encryption**: Use TLS/SSL to encrypt data in transit between, Grafana, and any other systems or users accessing them.
2. **Firewall Rules**: Configure firewall rules to restrict access to Grafana servers to only trusted IP addresses and networks.
3. **Network Segmentation**: Place Grafana servers in a dedicated, secure network segment to minimize exposure to potential threats.
4. **Load Balancer:** The backend connections are TLS encrypted.

Data Security

Data Storage Encryption: Encrypt sensitive data at rest, including time-series data and configuration files. All the volumes of Grafana is encrypted by KMS key encryption.

Application Security

1. **Regular Updates**: The Grafana servers will be patched on monthly basics with security patches.
2. **Input Validation**: Ensure proper input validation to prevent injection attacks, especially in user-provided data or query parameters.
3. **Security Audits**: Conduct regular security audits and vulnerability assessments to identify and address potential security issues.

Logging and Monitoring

1. **Access Logs**: Applications load balancer logs are maintained for access logs.
2. **Audit Logs**: Maintain audit logs of configuration changes, user actions, and other critical events.
3. **Intrusion Detection**: Implement intrusion detection systems (IDS) and monitoring tools to detect and respond to potential security incidents. (AWS Guard Duty is enabled for IDS).

Design considerations

High Availability for Grafana

HA Grafana Setup: Deploy multiple Grafana instances in different AZs and use a load balancer to handle incoming requests. Ensure that Grafana instances are stateless and share a common backend database.

Scalability

Horizontal Scaling - Server are scaled based on the utilization of the past 3 months.

Backup and Recovery

Automated Backups: AWS backup is enabled with daily backup with retention of one month. Yearly AMI for audit purpose.

Disaster Recovery Plan: backup restore method using AWS backup.

User & Access management

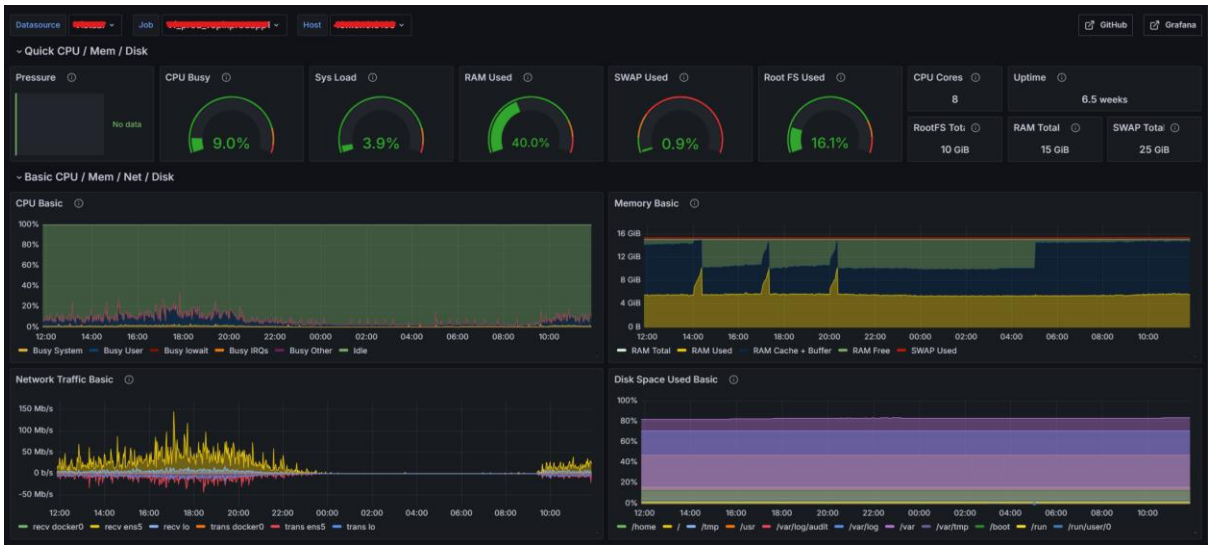
- The user access for Grafana is provided with inbuilt role-based access.
- For customers, a user can be created in Grafana, and access can be given to the specific dashboard.
- The Admin Access is with Tech Manager (1CH) & ASDL (1CH).

Dashboards

The dashboards are predefined for both Windows and Linux, Additional dashboards can be added upon approval from SDL & Tech Manager. Additionally, a resource overview a dashboard is set for all Linux servers.

Windows,

Linux,

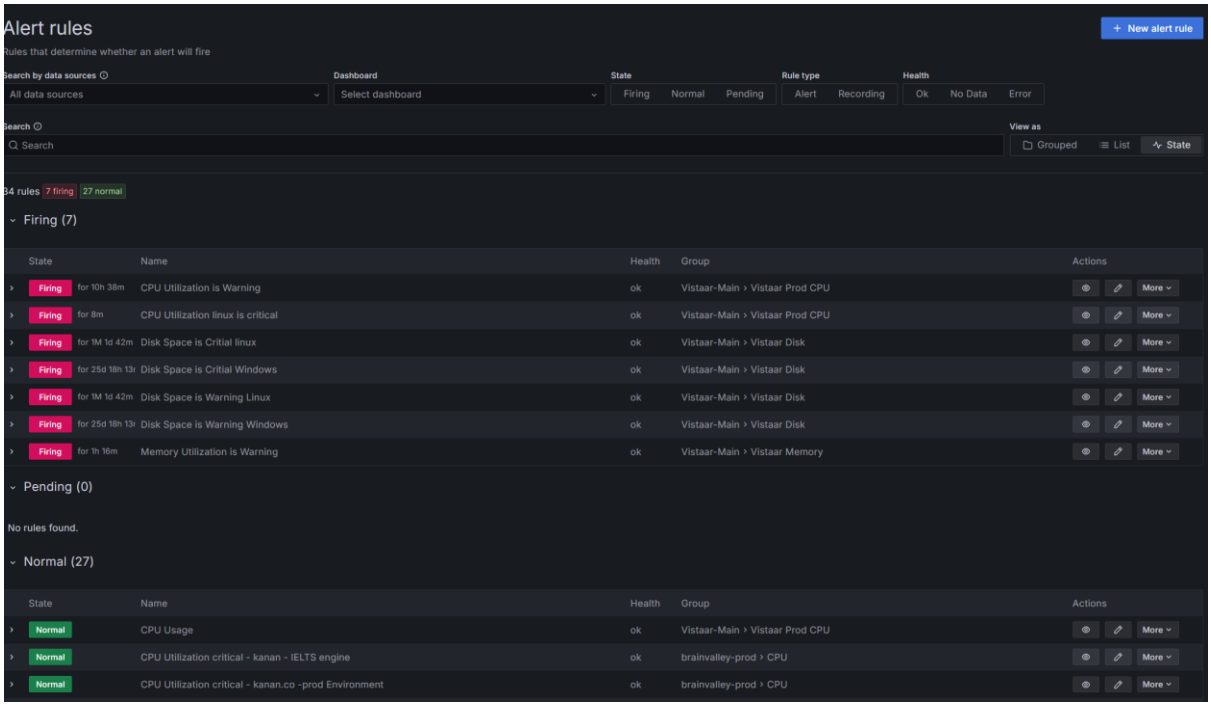


Alerts & Event Co-relation

The alerts set via Grafana predefined contact points & notifications. Event Co-relation is set for linux & windows servers separately,

- CPU – Pending Period 5m and Memory/RAM – 10m.
- The default Evaluation period is 1m for all services.

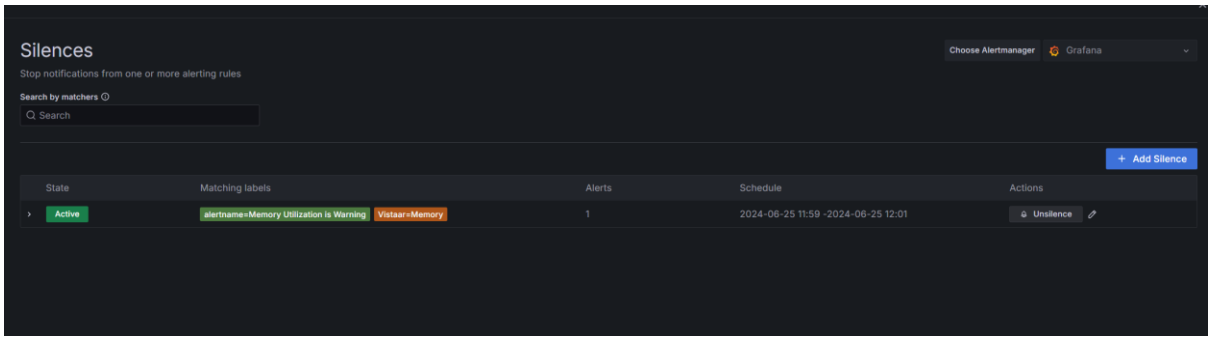
Alerts Overview:



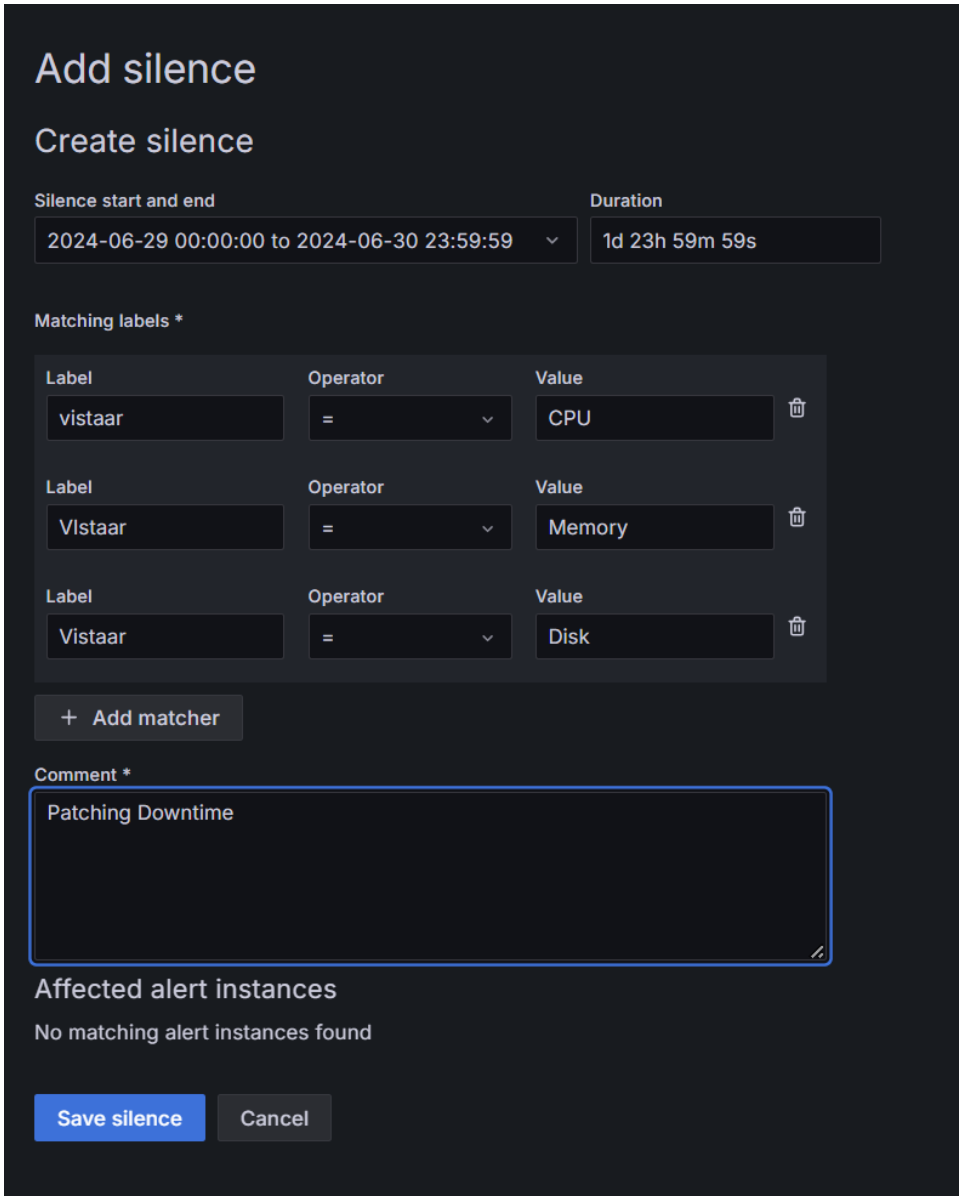
Alerts Acknowledgement & Downtime

The alerts can acknowledged & downtime via silences, You can create an silence either for one service or group of severs or all servers with the same services.

Acknowledgement



Scheduled Downtime



Implementation

On the Bastion server, the Prometheus agent is installed, and data is collected from the server using the Node Exporter agent. The servers communicate with each other using custom ports: 9182 for Windows and 9100 for Linux, via private IP addresses.

Grafana is hosted in the 1CH internal account, with the server positioned behind an Application Load Balancer (ALB) and managed via Route 53. Alerts are configured in Grafana and are currently forwarded to the ServiceAssurance Mailbox.

Prerequisites

The below prerequisites are required to implement Prometheus and Grafana in customer environment.

- Bastion server (public Access) with access to all the servers.
- Installation Access or Execution access in servers.
- VPN Access if applicable.

Proof Of Concept

One of the new accounts has been identified and was configured and run parallelly with the existing monitoring tool (CheckMK). The results as follows,

Range	23-06-2024 Till 28-06-2024

Date	From Grafana	From CheckMK
6/23/2024	76	159
6/24/2024	82	163
6/25/2024	41	162
6/26/2024	121	142
6/27/2024	43	144
6/28/2024	63	167
Total	**426**	**937**

The above is the naked comparison of alerts i.e. the alerts are without acknowledgement and downtime of alerts. Using the above alerts comparison and dashboard comparison the migrations of alerts were approved.

Conclusion

Prometheus and Grafana offer a robust, scalable monitoring solution with powerful querying, alerting, and customizable dashboards. They excel in alert acknowledgment, downtime scheduling, and visualization flexibility. Implementing Prometheus on the Bastion server and setting up Grafana behind an ALB with Route 53 ensures a reliable infrastructure. Regular backups and firewall are being checked for maintaining system integrity.