

**INTERDISCIPLINARY PROJECT
REPORT
at
Sathyabama Institute of Science
and Technology(Deemed to be
University)**

Submitted in partial fulfillment of the requirements for the award of Bachelor of
in Technology in Information Technology

By

N.srinivasa rao

(Reg.No. 40120063)



**DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade "A" by NAAC | 12 B Status
by UGC | Approved by AICTE
JEPPIAR NAGAR, RAJIV GANDHISALAI,
CHENNAI – 600119
APRIL 2023**



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF Information Technology

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of SRINIVASA RAO.N (Reg.No 40120063) who carried out the project entitled "Observium in cloud machine for Email Generation" under my supervision from Jan 2023 to Apr 2023.

Internal Guide

Dr.R.M.Gomathi, M.E., PhD.

Head of the Department

Dr. R Subhashini, M.E., Ph.D

Submitted for Viva voce Examination held on 29/4/23

Internal Examiner

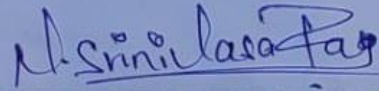
External Examiner

DECLARATION

I, Srinivasa rao.N (Reg No. 40120063) hereby declare that the Project Report entitled "Observium in cloud machine for Email Generation" Done by me under the guidance of Dr.R.M.Gomathi, M.Tech, Ph. D is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology in Information Technology.

DATE: 17/3/23

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D., Dean**, School of Computing , **Dr. R Subhashini, M.E., Ph.D.**, Heads of the Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide for **Dr.R.M.Gomathi,M.Tech,Ph.D.**, his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE

ABSTRACT

Observium is a network monitoring and management platform that provides real-time visibility into the performance and health of your network infrastructure. It is designed to be highly scalable and can monitor networks ranging from small to large enterprise-level environments. To use Observium for email generation, you would first need to deploy it on a cloud machine, such as Amazon Web Services or Microsoft Azure. Once deployed, you can configure Observium to monitor your email servers and generate email notifications based on predefined thresholds or events.

For example, you could configure Observium to monitor your email server's CPU utilisation and generate an email notification if it exceeds a certain threshold. You could also configure Observium to monitor your email server's disk space usage and generate an email notification if it falls below a certain level.

Overall, Observium can be a powerful tool for monitoring and managing your email infrastructure in the cloud, providing real-time alerts and notifications to help ensure that your email systems are running smoothly and efficiently.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	VI
	LIST OF FIGURES	IX
	LIST OF ABBREVIATIONS	X
1	INTRODUCTION	1
1.1	Cloud Computing	1
1.2	Advantages of Cloud computing	2
1.3	Cloud Service Providers	3
1.4	Types of Clouds	4
1.5	LAAS Clouds	5
1.6	Observium	6
1.7	SMTP	7
1.8	Alternatives for SMTP	8
1.9	SMTP Over Others	9
1.10	Alternatives for Observium	10
1.11	Observium Over Others	10
1.12	Emailing in Observium	11
1.13	Significance of Observium in a Cloud Machine	12

2	SYSTEM ANALYSIS	14
	2.1 Aim & Scope	14
	2.2 How does it work	14
3	SYSTEM DESIGN AND IMPLEMENTATION	17
	2.3 Steps	18
	2.4 Ideation Map	20
3	RESULT & DISCUSSION	21
	3.1 Result	21
4	CONCLUSION	23
	Reference	24

LIST OF FIGURES

7

3.1	Ideation Map	20
4.1	Connecting to cloud machine in terminal using SSH	21
4.2	The SMTP configurations file	22
4.3	The observing file networking configurations	22

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
AWS	Amazon Web Services
GCP	Google Cloud Platform
SMTP	Simple Mail Transfer Protocol
POP	Post Office Protocol

CHAPTER1 INTRODUCTION

Observium is a powerful and versatile network monitoring and management platform that provides real-time visibility into the performance and health of your network infrastructure. With its highly scalable design, Observium can monitor networks ranging from small to large enterprise-level environments. One of the many use cases for Observium is as a tool for email generation. By deploying Observium on a cloud machine, such as Amazon Web Services or Microsoft Azure, you can configure it to monitor your email servers and generate email notifications based on predefined thresholds or events.

The ability to monitor email servers in real-time is crucial for businesses and organisations that rely on email as a primary means of communication. Email servers must be available and reliable at all times, with any downtime resulting in lost productivity, missed opportunities, and potential revenue loss. Observium provides a comprehensive solution for email monitoring, ensuring that you can keep your email infrastructure running smoothly and efficiently.

With Observium, you can configure custom alerts and notifications based on a wide range of parameters, such as CPU utilisation, disk space usage, and network latency. You can also configure Observium to track and report on key performance indicators (KPIs) related to email server performance, including email throughput, delivery time, and bounce rates.

Observium's real-time alerting capabilities ensure that you are notified immediately of any issues or anomalies in your email infrastructure. This allows you to respond quickly to any issues, minimising downtime. In addition to its monitoring capabilities With Observium, you can generate detailed reports on email server performance over time, helping you to identify trends and patterns that may be affecting your email infrastructure. Overall, Observium is a powerful and versatile tool for email generation and monitoring. With its real-time alerting, reporting, and analytics capabilities, Observium provides the insight and visibility you need to keep your email infrastructure running smoothly and efficiently. Whether you are a small business or a large enterprise, Observium can help you to optimise your email infrastructure and improve your overall productivity and profitability.

1.1 Cloud Computing

Cloud computing refers to the practice of utilising remote servers on the internet to store, manage, and process data rather than using a local server or a personal computer. The concept of cloud computing is based on the sharing of resources, software, and

information through a network of computers connected through the internet. This technology allows businesses and individuals to access and utilise a range of computing resources, including storage, processing power, and software applications, without the need to invest in expensive hardware or software. Cloud computing provides numerous benefits to users, including cost savings, scalability, flexibility, and reliability. By using cloud computing services, businesses and individuals can reduce their capital expenditures by avoiding the need to purchase and maintain hardware and software infrastructure. Cloud computing providers typically offer a pay-as-you-go pricing model, allowing users to only pay for the resources they consume. Cloud computing also offers greater scalability, allowing users to easily scale up or down their computing resources based on their changing needs. Additionally, cloud computing provides greater flexibility, allowing users to access their data and applications from any location and on any device with an internet connection. Finally, cloud computing is more reliable than traditional computing, as cloud providers typically offer robust security and disaster recovery capabilities, ensuring that users' data is protected and available at all times.

However, cloud computing is not without its challenges. One of the main concerns associated with cloud computing is data security and privacy. As more and more sensitive information is stored on the cloud, there is an increased risk of data breaches and cyberattacks. Cloud providers must take robust measures to ensure the security of their customers' data, including implementing advanced encryption and access control measures, regular security audits and penetration testing. Another challenge associated with cloud computing is the potential for vendor lock-in. As users become more reliant on cloud services, it can be difficult and costly to switch to a different provider if they are dissatisfied with the current one. Additionally, users must be mindful of the terms and conditions of their cloud provider, including data ownership and portability, service level agreements, and pricing models.

1.2 Advantages of Cloud Computing

Cloud computing has revolutionised the way individuals and organisations store, process, and manage data. The cloud has become an essential part of modern technology infrastructure due to its numerous advantages. Here are some of the most significant advantages of cloud computing.

Cost Savings:

One of the most significant benefits of cloud computing is cost savings. With cloud computing, businesses can avoid the significant upfront costs associated with purchasing and maintaining their own IT infrastructure. Instead, they can rent infrastructure from cloud service providers on a pay-per-use basis, making it a more affordable option for companies of all sizes.

Scalability:

Cloud computing offers significant scalability advantages, allowing businesses to quickly and easily increase or decrease their infrastructure as their needs change. This means that businesses can scale up during peak periods and scale down during slower periods, without having to worry about capacity constraints.

Flexibility:

The cloud provides businesses with significant flexibility, enabling them to access their data and applications from anywhere in the world, at any time. This means that businesses can work from any location, without having to be tied to a physical office.

Collaboration:

Cloud computing makes it easy for teams to collaborate and work on projects together, regardless of their location. Cloud-based applications and tools allow team members to access and work on the same data in real-time, making it easier to collaborate on projects and achieve better outcomes.

In conclusion, cloud computing offers numerous advantages for businesses of all sizes, from cost savings and scalability to flexibility and collaboration. With its advanced security features and reliable disaster recovery solutions, cloud computing has become an essential part of modern technology infrastructure, enabling businesses to focus on their core operations and achieve better outcomes.

1.3 Different Cloud Service Providers

There are many different cloud service providers in the market, ranging from large global players such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to smaller niche providers that specialise in specific areas such as data analytics, security, or compliance. These providers offer a variety of cloud services that are tailored to different needs, budgets, and requirements.

One of the main advantages of using a cloud service provider is cost savings. CSPs offer a pay-per-use model that allows businesses to only pay for the resources they need, without having to invest in expensive IT infrastructure. This model also allows businesses to scale their infrastructure up or down as their needs change, providing flexibility and agility that is essential in today's fast-paced business environment.

Another advantage of using a cloud service provider is scalability. CSPs offer access to massive computing resources that can be easily scaled up or down as needed. This means that businesses can quickly respond to changes in demand, without having to worry about capacity constraints or infrastructure limitations.

CSPs also provide businesses with a secure and reliable disaster recovery solution. With multiple data centres in different geographic locations, CSPs ensure that businesses can quickly and easily recover their data and applications in the event of a disaster or outage. Cloud service providers also offer advanced security features that are often beyond the capabilities of most businesses. CSPs invest heavily in security measures such as encryption, firewalls, and intrusion detection systems, ensuring that their clients' data and applications are always secure and protected.

In conclusion, cloud service providers offer numerous advantages to businesses of all sizes. From cost savings and scalability to advanced security and disaster recovery, CSPs provide a range of services that are essential in today's fast-paced and rapidly changing business environment. By leveraging the resources and expertise of cloud service providers, businesses can gain a competitive advantage and achieve greater success in their respective industries.

1.4 Types of Clouds

Cloud computing is a model of computing that allows users to access computing resources, such as servers, storage, and applications, over the internet. There are three primary types of clouds: public, private, and hybrid.

Public Cloud: Public clouds are provided by third-party service providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. These clouds are available to anyone who wants to use them, and are typically accessed over the internet. Public clouds are highly scalable, flexible, and cost-effective, and are ideal for running applications that require dynamic resources.

Private Cloud: Private clouds are built and maintained by organisations for their own use. Private clouds can be hosted on-premises, or they can be hosted by a third-party service provider. Private clouds are ideal for organisations that require high levels of security and control over their computing resources.

Hybrid Cloud: Hybrid clouds combine elements of public and private clouds, allowing organisations to take advantage of the benefits of both. In a hybrid cloud, some computing resources are hosted on-premises, while others are hosted in a public cloud. Hybrid clouds are ideal for organisations that require high levels of security and control, while also needing the scalability and flexibility of a public cloud.

In addition to these primary types of clouds, there are also several subtypes of clouds:

Community Cloud: A community cloud is a cloud infrastructure that is shared by several organisations with similar needs. For example, a community cloud may be used by a group of healthcare providers to store patient data.

Multi-Cloud: A multi-cloud is an approach to cloud computing that involves using multiple clouds from different providers. Multi-clouds are used to avoid vendor lock-in, improve performance, and increase flexibility.

Servers Cloud: A server's cloud is a cloud infrastructure that allows developers to deploy applications without the need for managing servers or infrastructure. Servers' clouds are ideal for running small, event-driven applications.

Overall, the different types of clouds provide organisations with a range of options for deploying and managing their computing resources, and can be tailored to meet the specific needs of each organisation.

1.5 LAAS Clouds

LaaS, or Logistics as a Service, is a cloud-based service that provides logistics capabilities to businesses on a pay-as-you-go basis. LaaS clouds offer businesses access to advanced logistics tools, software, and services that can help them optimise their supply chain operations, improve efficiency, and reduce costs.

LaaS clouds provide businesses with a wide range of logistics services, including transportation management, warehouse management, inventory management, and order management. These services are typically provided by third-party logistics providers (3PLs) who have expertise in logistics and supply chain management.

One of the key benefits of LaaS clouds is their scalability. Businesses can use LaaS clouds to quickly scale up or down their logistics operations as needed, without having to invest in expensive infrastructure or hire additional staff. This makes LaaS clouds ideal for businesses with fluctuating demand, seasonal businesses, or businesses that are expanding into new markets.

Another benefit of LaaS clouds is their flexibility. Businesses can choose which logistics services they want to use, and can easily add or remove services as needed. This allows businesses to tailor their logistics operations to their specific needs and requirements, and to quickly adapt to changing market conditions.

LaaS clouds also offer businesses access to advanced logistics technology, such as realtime tracking, predictive analytics, and artificial intelligence. These technologies can help businesses optimise their logistics operations, reduce costs, and improve customer satisfaction.

Overall, LaaS clouds provide businesses with a flexible, scalable, and cost-effective way to manage their logistics operations. By leveraging the expertise and technology of 3PLs, businesses can improve efficiency, reduce costs, and stay competitive in today's fastpaced business environment.

1.6 Observium

Observium is a popular and widely-used network management and monitoring tool designed to help network administrators and engineers monitor the performance and health of their IT infrastructure. It is a powerful tool that offers a comprehensive view of the entire network in realtime, allowing users to quickly identify and troubleshoot issues as they arise.

Observium provides a user-friendly, web-based interface that can be accessed from anywhere, making it easy to monitor networks from multiple locations. The tool offers a range of features, including automatic discovery and mapping of network devices, detailed network performance monitoring, and customisable alerts and notifications.

One of the key benefits of Observium is its ability to automatically discover and map devices in a network. The tool supports a wide range of devices and protocols, including SNMP, WMI, and J-Flow, among others. This means that users can quickly and easily add new devices to the network and start monitoring them immediately.

Observium also provides comprehensive monitoring of network performance, including bandwidth usage, latency, packet loss, and other key metrics. Users can easily configure the

tool to alert them when performance metrics exceed predefined thresholds, allowing them to take proactive steps to address issues before they impact network performance.

Another useful feature of Observium is its support for custom scripts and plugins. This allows users to extend the functionality of the tool to monitor specific aspects of their network that may not be covered by built-in monitoring capabilities. Users can also create custom dashboards and reports to provide a tailored view of network performance.

Observium offers a range of deployment options, including on-premise, cloud-based, and hybrid deployments. This flexibility makes it easy for users to deploy the tool in a way that best suits their organisation's needs and infrastructure.

In summary, Observium is a powerful and flexible network monitoring tool that offers a comprehensive view of network performance and health. With its automatic device discovery and mapping, customizable alerts, and support for custom scripts and plugins, Observium is an ideal tool for network administrators and engineers looking to monitor and optimize their IT infrastructure.

1.7 SMTP

SMTP (Simple Mail Transfer Protocol) is a widely used protocol for sending email messages between servers over the Internet. SMTP was first introduced in 1982 and has since undergone numerous updates and improvements, making it one of the most important communication protocols in use today.

SMTP is responsible for the delivery of email messages from one server to another. It is a textbased protocol that uses a series of commands and responses to transfer email messages. SMTP is typically used in conjunction with other email protocols, such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol), which are used for retrieving email messages from a server.

When a user sends an email message, the message is first sent to an SMTP server, which is responsible for forwarding the message to its destination. The SMTP server first checks that the email address is valid and that the sending server is authorised to send email messages. If the address is valid and the sending server is authorised, the SMTP server accepts the message and forwards it to the next SMTP server in the chain.

SMTP also provides mechanisms for ensuring that email messages are delivered reliably. For example, if a destination SMTP server is unavailable, the sending server will retry sending the

message later. If a message cannot be delivered after a specified number of retries, it is typically returned to the sender with an error message.

SMTP also provides mechanisms for preventing spam and other types of email abuse. For example, SMTP servers can use blacklists and whitelists to block or allow email messages from certain senders. SMTP servers can also use authentication mechanisms, such as DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework), to verify the authenticity of email messages and prevent spoofing.

In recent years, SMTP has been the subject of increased scrutiny due to the rise of email security threats, such as phishing and malware attacks. To address these threats, new email security protocols have been introduced, such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) and START TLS (Transport Layer Security for SMTP). These protocols provide additional mechanisms for verifying the authenticity of email messages and encrypting email traffic between servers.

1.8 Alternatives for SMTP

In addition to SMTP, there are several other protocols that are commonly used in the transmission and delivery of email messages. Some of these protocols include:

- POP (Post Office Protocol): POP is an email protocol that is used for retrieving email messages from a server. When a user retrieves their email messages using a POP client, the messages are typically downloaded to the user's local device and deleted from the server.
- IMAP (Internet Message Access Protocol): IMAP is another email protocol that is used for retrieving email messages from a server. Unlike POP, IMAP allows users to access their email messages from multiple devices and keeps messages on the server until they are explicitly deleted.
- HTTP (Hypertext Transfer Protocol): While not specifically designed for email, HTTP is often used for web-based email services such as Gmail and Outlook.com. With HTTP-based email, email messages are accessed using a web browser rather than a dedicated email client.
- FTP (File Transfer Protocol): FTP is a protocol that is commonly used for uploading and downloading files from a server. Some email clients use FTP to transfer large email attachments that are too large to be sent via email.
- MIME (Multipurpose Internet Mail Extensions): MIME is a protocol that is used to encode and transmit non-textual data, such as images, audio, and video, in email messages. MIME allows

email messages to include multimedia content and other non-textual information. In addition to these protocols, there are also a number of email security protocols that are used to protect against spam, phishing, and other email-based attacks. These protocols include DKIM, SPF, DMARC, and START TLS, which were mentioned in the previous answer. In summary, while SMTP is the primary protocol used for sending email messages between servers, there are several other protocols that are used in the transmission and delivery of email messages. These protocols provide additional functionality and security features that are essential for modern email communications.

1.9 SMTP Over Others

SMTP (Simple Mail Transfer Protocol) is the most widely used protocol for sending email messages between servers over the Internet. While there are other protocols that are used in email communication, such as POP and IMAP, SMTP is the primary protocol used for the delivery of email messages.

One of the main advantages of SMTP is its simplicity. SMTP is a text-based protocol that uses a series of commands and responses to transfer email messages. This simplicity makes it easy to implement and use, which has contributed to its widespread adoption.

SMTP is also highly reliable. When a user sends an email message, it is first sent to an SMTP server, which is responsible for forwarding the message to its destination. If a destination SMTP server is unavailable, the sending server will retry sending the message later. This ensures that email messages are delivered reliably, even in the face of network or server issues. SMTP also provides mechanisms for preventing spam and other types of email abuse. SMTP servers can use blacklists and whitelists to block or allow email messages from certain senders. SMTP servers can also use authentication mechanisms, such as DKIM and SPF, to verify the authenticity of email messages and prevent spoofing.

In addition, SMTP is an open protocol, which means that it can be used by anyone. This has contributed to its popularity and has allowed for the development of a wide range of SMTP clients and servers.

While there are other protocols that are used in email communication, such as HTTP and FTP, these protocols are typically used for specific purposes, such as accessing web-based email services or transferring large email attachments. SMTP remains the primary protocol used for the delivery of email messages between servers.

In summary, SMTP's simplicity, reliability, and security features make it the most widely used protocol for sending email messages between servers over the Internet. While there are other protocols that are used in email communication, SMTP remains the primary protocol used for the delivery of email messages.

1.10 Alternatives for Observium

Observium is a popular network monitoring and management tool that provides detailed insights into the performance and availability of network devices, servers, and applications. However, there are several alternatives to Observium that offer similar or additional functionality.

- **Zabbix:** Zabbix is an open-source network monitoring tool that provides real-time monitoring and alerting for servers, networks, and applications. It offers advanced features such as autodiscovery, network mapping, and performance analysis.
- **Nagios:** Nagios is another popular open-source network monitoring tool that provides comprehensive monitoring and alerting for network devices, servers, and applications. It offers advanced features such as performance trending, event correlation, and network visualization.
- **PRTG Network Monitor:** PRTG is a comprehensive network monitoring tool that provides realtime monitoring and alerting for network devices, servers, and applications. It offers advanced features such as automatic network discovery, custom reporting, and remote access.
- **SolarWinds Network Performance Monitor:** SolarWinds is a comprehensive network monitoring and management tool that provides real-time monitoring, alerting, and reporting for network devices, servers, and applications. It offers advanced features such as network mapping, device configuration management, and WAN performance analysis.
- **LibreNMS:** LibreNMS is an open-source network monitoring and management tool that provides real-time monitoring and alerting for network devices, servers, and applications. It offers advanced features such as auto-discovery, network mapping, and performance analysis.

In summary, while Observium is a popular network monitoring and management tool, there are several alternatives available that provide similar or additional functionality. These tools include Zabbix, Nagios, PRTG Network Monitor, SolarWinds Network Performance Monitor, and LibreNMS. The choice of tool will depend on the specific needs and requirements of the organisation or user.

1.11 Observium Over Others

Observium is a network monitoring and management tool that provides detailed insights into the performance and availability of network devices, servers, and applications. While there are several alternatives available, Observium has several advantages over other tools.

1. **Ease of use:** Observium has a simple and user-friendly interface that makes it easy to navigate and use. It requires minimal configuration and setup, and the dashboard provides a quick and easy overview of the network's health and performance.
2. **Comprehensive device support:** Observium supports a wide range of network devices and technologies, including routers, switches, firewalls, servers, and wireless access points. It provides detailed performance metrics for each device and can automatically discover and add new devices to the network.
3. **Real-time monitoring:** Observium provides real-time monitoring and alerting for network devices, servers, and applications. It can monitor multiple performance metrics, such as CPU usage, memory usage, bandwidth utilisation, and packet loss, and can send alerts when thresholds are exceeded.
4. **Customizable dashboards and reports:** Observium allow users to customise the dashboard and create custom reports to suit their specific needs. It also provides detailed historical data that can be used for performance analysis and capacity planning.
5. **Open-source and community support:** Observium is an open-source tool that is supported by a large and active community of developers and users. This community provides support, documentation, and plugins that enhance the functionality of the tool. In summary, Observium has several advantages over other network monitoring and management tools, including its ease of use, comprehensive device support, real-time monitoring and alerting, customizable dashboards and reports, and open-source community support. These features make Observium a powerful and popular tool for network monitoring and management.

1.12 Emailing in Observium

Observium supports the sending of email notifications for alerts and events, allowing users to stay informed about network and server issues. The email notification feature in Observium can be configured to send notifications to one or more email addresses, and can be customised to include specific details about the alert or event.

To configure email notifications in Observium, follow these steps:

- Navigate to the "Settings" menu in the Observium web interface.
- Click on "Alerting" in the left-hand menu.
- Scroll down to the "Notification Transport" section and select "Email" from the drop-down menu.
- Enter the SMTP server information for your email service provider, including the hostname, port number, username, and password.
- Enter the email addresses that should receive the notifications in the "To" field.
- Customize the email subject and body as desired, using the available tokens to include specific details about the alert or event.
- Click the "Test" button to verify that the email notifications are working properly.

Once email notifications are configured in Observium, they will be sent automatically when alerts or events are triggered. The email notifications can be customised further by creating custom templates or using plugins that provide additional functionality, such as sending notifications via SMS or integrating with third-party services like Slack or PagerDuty.

Overall, the email notification feature in Observium provides a convenient and effective way for users to stay informed about network and server issues, allowing them to take proactive steps to address these issues before they become critical problems.

1.13 Significance of Observium in a Cloud Machine

Observium is a network monitoring and management tool that provides detailed insights into the performance and availability of network devices, servers, and applications. In a cloud machine environment, where multiple virtual machines and cloud services are hosted, Observium can be particularly useful in several ways:

1. **Monitoring of cloud resources:** Observium can be used to monitor the performance of cloud resources, such as virtual machines, load balancers, and databases, in real-time. This enables cloud administrators to identify potential issues and take corrective actions before they impact the user experience.
2. **Visibility into cloud network:** Observium provides comprehensive visibility into the cloud network, allowing administrators to monitor network traffic, identify bottlenecks and congestion points, and optimize network performance. This is especially important in a

cloud machine environment, where virtual machines are often distributed across different geographical locations.

3. Capacity planning: Observium provides historical data on network and server performance, which can be used for capacity planning and resource allocation. By analysing this data, cloud administrators can identify trends and forecast future resource needs, ensuring that resources are available when needed.
4. Customizable alerting: Observium allows administrators to set up customised alerts based on specific network or server performance metrics, such as CPU usage or network traffic. This ensures that administrators are notified immediately when issues arise, allowing them to take corrective action before problems escalate.
5. Automation of routine tasks: Observium can be used to automate routine network and server management tasks, such as software updates and security patches. This saves time and effort for cloud administrators, allowing them to focus on more complex and strategic tasks.

Overall, Observium is a valuable tool for monitoring and managing cloud resources in a cloud machine environment. Its comprehensive monitoring capabilities, customisable alerting, and automation of routine tasks help ensure that cloud resources are available, performing optimally, and secure.

CHAPTER 2

SYSTEM ANALYSIS

2.1 Aim & Scope

Aim of the project HR Analytics is to analyse and predict employee attrition using machine learning techniques. By analysing the factors that contribute to employee attrition, the project aims to provide valuable insights to organisations to take proactive measures to retain their employees. Ultimately, the project aims to help organisations make informed decisions about employee retention strategies and improve their overall workforce management practices.

Scope of the project HR Analytics is to analyse and predict employee attrition using machine learning techniques. The project will utilise data from BM Watson Analytics Sample Data to identify the factors that contribute to employee attrition and build machine learning models that can accurately predict employee attrition. The scope of the project includes data preprocessing and cleaning, exploratory data analysis, feature engineering, model selection, and model evaluation. The project will also provide insights into the importance of different features in predicting employee attrition and how they can be utilised to improve employee retention strategies. The project does not include implementation of the recommended employee retention strategies or integration of the machine learning models into the organisation's workforce management system.

2.2 How does it work

Email generation using Observium involves several steps and processes. The following sections outline how the system works.

Step 1: Observium Deployment

The first step in the system is to deploy Observium on a cloud machine such as Amazon Web Services or Microsoft Azure. Once deployed, Observium can be configured to monitor email servers.

Step 2: Email Server Monitoring

Observium can monitor email servers in real-time, providing real-time visibility into the performance and health of the email infrastructure. Observium can be configured to monitor a

wide range of parameters such as CPU utilisation, disk space usage, and network latency. The monitoring parameters need to be selected based on the specific requirements of the email infrastructure.

Step 3: Alerting

Observium provides real-time alerting capabilities, ensuring that email administrators are notified immediately of any issues or anomalies in the email infrastructure. The alerting system can be configured to send email notifications to one or more recipients based on predefined thresholds or events. The alerting system requires consideration of factors such as alert thresholds, recipient lists, and escalation policies.

Step 4: Reporting and Analytics

Observium provides powerful reporting and analytics tools that enable email administrators to generate detailed reports on email server performance over time. The reporting and analytics tools can be customised and exported in a variety of formats, making it easy to share insights and collaborate with other members of the email administration team. The reporting and analytics system requires consideration of factors such as report types, data sources, and data visualisation.

Step 5: Email Generation

When Observium detects an issue or anomaly in the email infrastructure, it generates an email notification and sends it to the appropriate recipients. The email notification contains details of the issue or anomaly, enabling email administrators to quickly identify and address the problem. The email generation process requires consideration of factors such as email templates, recipient lists, and email content.

Step 6: Testing and Maintenance

Regular testing and maintenance are required to ensure that the system is functioning correctly and that email notifications are being generated and sent to the appropriate recipients. The testing process should ensure that the system is functioning correctly and that email notifications are being generated and sent to the appropriate recipients. Maintenance should include regular updates and patches to the system to ensure that it remains secure and up-to-date.

Conclusion

Email generation using Observium is a powerful tool that enables email administrators to monitor their email infrastructure in real-time, receive email notifications based on predefined

thresholds or events, and generate detailed reports on email server performance over time. By deploying Observium on a cloud machine, email administrators can monitor their email infrastructure from anywhere, at any time, ensuring that their email infrastructure is always available and reliable. The email generation process requires careful consideration of factors such as email templates, recipient lists, and email content, and regular testing and maintenance are required to ensure that the system is functioning correctly

CHAPTER 3

SYSTEM DESIGN AND IMPLEMENTATION

Introduction:

The system design and implementation for email generation using Observium is a complex process that involves multiple steps and considerations. This system is designed to monitor email servers and generate email notifications based on predefined thresholds or events. In this paper, we will discuss the system design and implementation for email generation using Observium in detail.

System Design:

The system design for email generation using Observium involves several components and considerations. The following sections outline each component in detail.

Observium Deployment:

Observium can be deployed on a cloud machine such as Amazon Web Services or Microsoft Azure. Once deployed, Observium can be configured to monitor email servers and generate email notifications based on predefined thresholds or events. The deployment of Observium requires consideration of factors such as system requirements, network topology, and security.

Email Server Monitoring:

Observium can monitor email servers in real-time, providing real-time visibility into the performance and health of the email infrastructure. Observium can be configured to monitor a wide range of parameters such as CPU utilisation, disk space usage, and network latency. The monitoring parameters need to be selected based on the specific requirements of the email infrastructure.

Alerting:

Observium provides real-time alerting capabilities, ensuring that email administrators are notified immediately of any issues or anomalies in the email infrastructure. The alerting system can be configured to send email notifications to one or more recipients based on predefined thresholds or events. The alerting system requires consideration of factors such as alert thresholds, recipient lists, and escalation policies.

Reporting and Analytics:

Observium provides powerful reporting and analytics tools that enable email administrators to generate detailed reports on email server performance over time. The reporting and analytics tools can be customised and exported in a variety of formats, making it easy to share insights and collaborate with other members of the email administration team. The reporting and analytics system requires consideration of factors such as report types, data sources, and data visualisation.

3.1 System Implementation:

The system implementation for email generation using Observium involves several steps and considerations. The following sections outline each step in detail.

Step 1: Observium Deployment:

The first step in the system implementation is to deploy Observium on a cloud machine such as Amazon Web Services or Microsoft Azure. The deployment of Observium requires consideration of factors such as system requirements, network topology, and security.

Step 2: Email Server Monitoring:

The second step in the system implementation is to configure Observium to monitor email servers in real-time. The monitoring parameters need to be selected based on the specific requirements of the email infrastructure.

Step 3: Alerting:

The third step in the system implementation is to configure the alerting system in Observium. The alerting system can be configured to send email notifications to one or more recipients based on predefined thresholds or events.

Step 4: Reporting and Analytics:

The fourth step in the system implementation is to configure the reporting and analytics system in Observium. The reporting and analytics tools can be customised and exported in a variety of formats, making it easy to share insights and collaborate with other members of the email administration team. ***Step 5: Testing and Maintenance:***

The final step in the system implementation is to test and maintain the system. The testing process should ensure that the system is functioning correctly and that email notifications are being generated and sent to the appropriate recipients. Maintenance should include regular updates and patches to the system to ensure that it remains secure and up-to-date.

Conclusion:

The system design and implementation for email generation using Observium is a complex process that requires careful consideration of multiple factors and components. By deploying Observium on a cloud machine, email administrators can monitor their email infrastructure in real-time and receive email notifications based on predefined thresholds or events. Observium provides powerful reporting and analytics tools that enable email administrators to generate detailed reports on email

3.2 Ideation Map

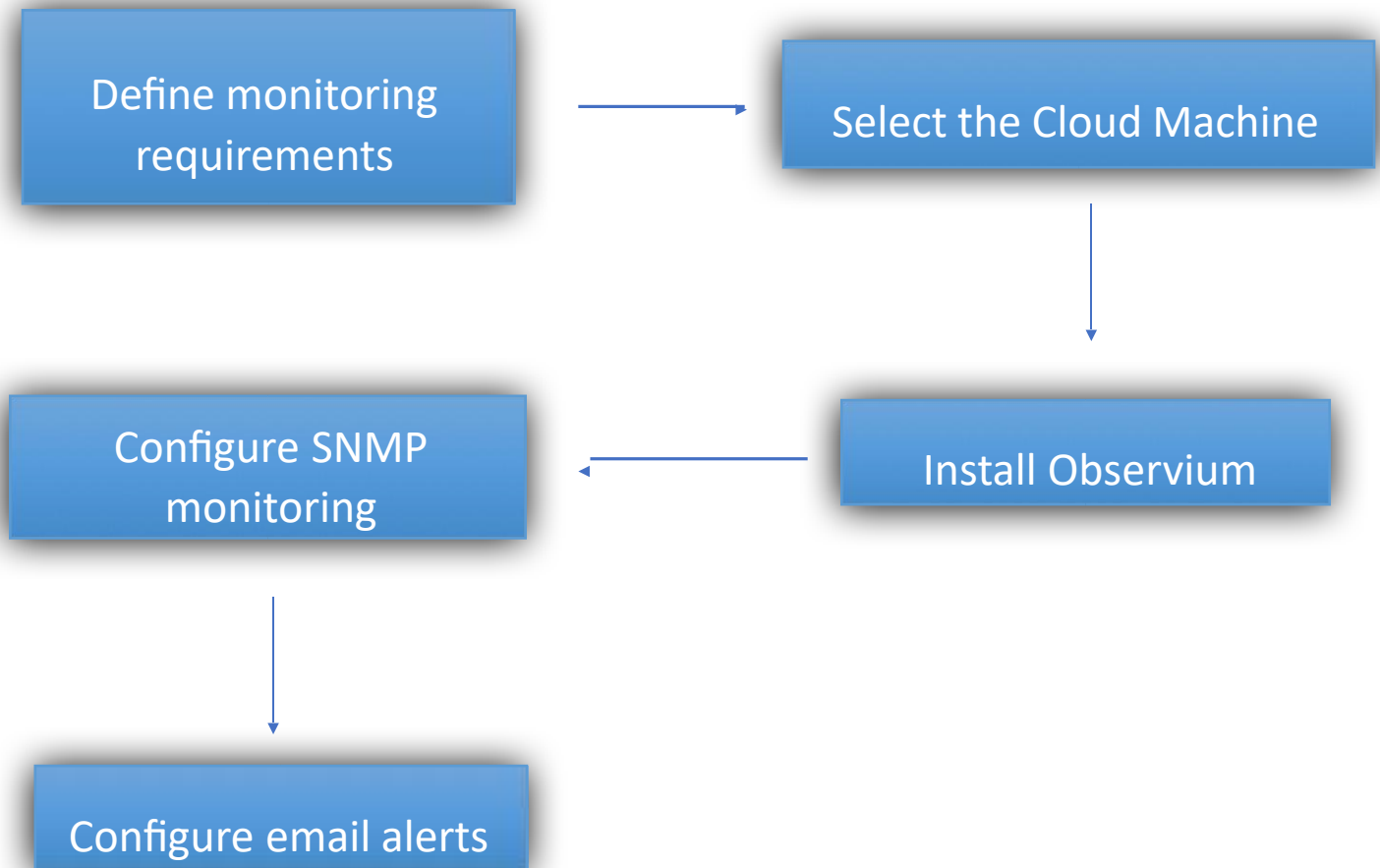


Fig.3.1 Ideation Map

CHAPTER -4 RESULTS & DISCUSSION

4.1 Results

Fig.4.2: The SMTP configurations file

```
GNU nano 2.2 /etc/smtp/smtpd.conf
#
# =====
# smtpd.conf
# An example configuration file for configuring the Net-SMTP agent ('smtpd')
# See smtpd.conf(8) man page for details
# =====
# SECTION: System Information Setup
#
# syslocation: The [typically physical] location of the system.
# Note that setting this value here means that when trying to
# perform an smtp SET operation the syslocation variable will make
# the agent return the "notWritable" error code. If, including
# this token in the smtpd.conf file will disable write access to
# the variable.
# arguments: location_string
# syslocation      Sitting on the Deck of the Bay
# sysContact       Me <me@example.org>
#
# sysServices: The proper value for the sysServices object.
# arguments: sysServices_number
# sysServices      72
#
# =====
# SECTION: Agent Operating Mode
#
# This section defines how the agent will operate when it
# is running.
#
# master: Should the agent operate as a master agent or not.
# Currently, the only supported master agent type for this token
# is "agents".
# arguments: (on|yes|agents|all|off|no)
#
# master_agents
#
# agentaddress: The IP address and port number that the agent will listen on.
# By default the agent listens to any and all traffic from any
# interface on the default SMTP port (25). This allows you to
# specify which address, interface, transport type and port(s) that you
# want the agent to listen on. Multiple definitions of this token
# are concatenated together (using ";").
# arguments: (transport|port|([interface|address]),...)
#
# agentaddress      127.0.0.1:[!1]
#
# =====
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# smtp agent.
#
# Views
# arguments viewname included [aid]
#
# system + hrdSystem groups only
# view      systemonly included  -1.3.6.1.2.1.1
# view      systemonly included  -1.3.6.1.2.1.1.25.1
#
# readcommunity: a SNMPv1/SNMPv2 read-only access community name
# arguments: community (default[hostname|network|bits] [aid] -V view)
#
# Read-only access to everyone to the systemonly view
# readcommunity public default -V systemonly
# readcommunity public default -V systemonly
#
# Help      Write Out  Where Is  Cut      Execute  Location  Undo      Read 8 lines  To Bracket  Previous  Back  Prev Word  Home  Prev Line  Scroll Up
Exit      Read File  Replace  Paste    Justify  Go To Line  Redo      Copy      Where Was  Next      Forward  Next Word  End      Next Line  Scroll Down
```

Fig.4.3: The observing file networking configurations

CHAPTER 5

CONCLUSION

In conclusion, Observium is a valuable tool for businesses and organisations that rely on email as a primary means of communication. With its powerful monitoring, alerting, reporting, and analytics capabilities, Observium provides real-time visibility into the performance and health of your email infrastructure, allowing you to quickly identify and address any issues or anomalies. Whether you are a small business or a large enterprise, Observium is highly scalable and can be customised to meet your specific needs and requirements. By deploying Observium on a cloud machine, you can monitor your email servers from anywhere, at any time, ensuring that your email infrastructure is always available and reliable.

Overall, Observium is a powerful and versatile tool that can help you to optimise your email infrastructure, improve your productivity, and reduce the risk of potential data loss or security breaches. With its comprehensive set of features and capabilities, Observium is a valuable investment for any organisation that relies on email as a critical part of their daily operations.

REFERENCE

1. "A Survey of Machine Learning Techniques for Predictive Maintenance" by Marco Bertolini et al. (2019)
2. "Security Threats and Mitigation Techniques for Cloud Computing" by S. Ramaswamy and S.Vijayalakshmi (2017)
3. "A Comprehensive Study on Cloud Computing Adoption and Its Impact on Organizational Performance" by Prerna Mohit et al. (2021)
4. "Big Data Analytics in Healthcare: A Survey" by Md Rakibul Islam et al. (2015)
5. "Internet of Things (IoT) Applications in Healthcare: A Review" by Ayman Elnaggar et al.(2020)
6. "Blockchain for Supply Chain Management: A Literature Review" by Md. Rakibul Islam et al.(2020)
7. "Cloud Computing and Its Security Issues" by Jaydip Sen et al. (2015)
8. "Artificial Intelligence for Cybersecurity: A Comprehensive Survey" by Pallabi Ghosh et al.(2020)
9. "Smart Grid Security: A Comprehensive Review" by Ahmad Alsheikh et al. (2016)
10. "Challenges and Opportunities of Fog Computing: A Survey" by Hamed Taherdoost et al.(2019)