A Project-II
Report
on

EFFICIENT LOG DATA MANAGEMENT WITH KQL: WRITING AZURE QUERIES FOR LOG ANALYTICS WORKSPACE

A Project Report submitted to JNTUK Partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

BY

PADUCHURI DEEPTHI	19JU1A0513
GOLAMARI KAVYA	19JU1A0533
KONGANI HARI PRIYA YADAV	19JU1A0526
ULAPU KIRAN KUMAR	19JU1A0538
DUDEKULA MEERAVALI	19JU1A0553

Under the Esteemed Guidance of
Mrs.A.AMRUTAVALLI M.Tech,(Ph.D)
Assoc. Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES
(Approved by A.I.C.T.E & Affiliated to JNTU, KAKINADA Accredited by NAAC)
DEVARAJUGATTU, PEDDARAVEEDU MANDAL, PRAKASAM (DIST), A.P.

2019-2023

KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY&SCIENCES

(Approved by A.L.C.T.E & Affiliated to JNTU, KAKINADA Accredited by NACC)

DEVARAJUGATTU, PEDDARAVEEDU MANDAL, PRAKASAM (Dist), A.P.

2019-2023

CERTIFICATE

This is to certify that the project-II entitle "EFFICIENT LOG DATA MANAGEMENT WITH KQL:WRITING AZURE QUERIES FOR LOG ANALYTICS WORKSPACE"**, is the confide work done by Paduchuri Deepthi**[19JU1A0513]**, Golamari Kavya**[19JU1A0533]**, Kongani Hari Priya Yadav**[19JU1A0526]**, Ulapu Kiran Kumar**[19JU1A0538]**, Dudekula Meeravali**[19JU1A0553] **under the guidance of Mrs.A.Amrutavalli M.TECH,(Ph.D) in partial fulfillment of the requirements for the award of** BACHELOR OF TECHNOLOGY **in the department of** COMPUTER SCIENCE AND ENGINEERING **in KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES affiliated to** JNTU Kakinada **during the academic year 2022-2023.**

PROJECT GUIDE
Mrs.A.AMRUTAVALLI M.Tech,(Ph.D
Assoc. Professor
Dept of CSE

HEAD OF THE DEPARTMENT
Dr.J.V.ANIL KUMAR M.Tech,Ph.D
HOD & Professor,
Dept of CSE

External Viva voce conducted on _____

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We wish to express our thanks to various personalities who are responsible for the completion of the project. we express our beloved chairman **Sri A.V.RAMBABU GARU** and secretary and correspondent **Dr.A.KRISHNA CHAITANYA GARU, Krishna Chaitanya Institute of Technology and Sciences,** for providing support and stimulate environment for developing the project.

We express our deep sense of reverence and profound gratitude **Dr.V.KRISHNA REDDY,** Principal, **Krishna Chaitanya Institute of Technology and Sciences,** for providing us the great support on completing our resource for carrying out project.

Our sincere thanks to **Dr.J.V.ANIL KUMAR** MTech,Ph.D Professor and HOD , Dept.of CSE Who has encouraged us and his moral support throughout the project.

Our sincere thanks to **Mrs.A.AMRUTAVALLI** MTech,(Ph.D) Assoc. professor. Our guide who has encouraged us and gave her moral support throughtout the project.

A lot thanks to other faculty members of the department who gave them valuable suggestion at various stage of our project.

We take this Opportunity to thank to Teaching and Non-Teaching staff of the department , without those support the project would not have been successful.

We have no words to acknowledgement the warm affection, constant inspiration and encouragement that we received.

Project Associates

PADUCHURI DEEPTHI	19JU1A0513
GOLAMARI KAVYA	19JU1A0533
KONGANI HARI PRIYAYADAV	19JU1A0526
ULAPU KIRAN KUMAR	19JU1A0538
DUDEKULA MEERAVALI	19JU1A0553

DECLARATION

We hereby declare that the project-II entitled "EFFICIENT LOG DATA MANAGEMENT WITH KQL : WRITING AZURE QUERIES FOR LOG ANALYTICS WORKSPACE", **submitted for the B.Tech Degree is our original work and the project has not formed the basis for the award of any degree, associate ship, fellowship or any other similarities.**

PADUCHURI DEEPTHI	19JU1A0513
GOLAMARI KAVYA	19JU1A0533
KONGANI HARI PRIYAYADAV	19JU1A0526
ULAPU KIRAN KUMAR	19JU1A0538
DUDEKULA MEERAVALI	19JU1A0553

ABSTRACT

Efficient Log Data Management with KQL: Writing Azure Queries for Log Analytics Workspace is a project that focuses on using the Kusto Query Language (KQL) for efficient log data management in Azure Log Analytics Workspace. This project explores the importance of log data management, the challenges faced in managing log data, and how KQL can be leveraged to write queries for efficient log data analysis.

The project provides a step-by-step guide on how to write Azure queries using KQL for log data management. It covers topics such as data ingestion, creating custom logs, and data visualization using KQL queries. The project also explores how to use KQL to identify and resolve issues in real-time, set up alerts, and create dashboards for effective log data management.

By the end of this project, readers will have a better understanding of the importance of log data management, how to use KQL for log data analysis, and how to optimize log data management using Azure Log Analytics Workspace. The project will be beneficial to IT professionals, cloud administrators, and anyone interested in learning how to effectively manage log data using KQL in Azure Log Analytics Workspace.

KEYWORDS:

Virtual Machine, Azure Log Analytics Workspace, Kusto Query Language (KQL), Agents.

TABLE OF CONTENTS

1.INRODUCTION

CHAPTER-1

INTRODUCTION

With the growing number of applications, systems, and devices in use today, it has become essential to monitor and manage log data effectively. Azure Log Analytics Workspace is a cloud-based log management solution that provides a centralized platform for collecting, analyzing, and visualizing log data from various sources. It offers advanced features such as log search, log analytics, and custom queries, which can help organizations gain insights into their log data and identify potential issues.

The objective of this project is to explore and analyze Azure Log Analytics Workspace and develop efficient queries for log data management. The project will start with an in-depth study of the Azure Log Analytics Workspace and its capabilities, including log ingestion, data retention, data visualization, and data querying. The project will also explore various log sources, including application logs, system logs, and security logs.

The project will then focus on developing efficient queries for log data management. This will involve identifying common log data patterns, creating custom queries using Azure Log Analytics Workspace query language, and analyzing query results to identify potential issues. The project will also investigate the use of machine learning algorithms for log data analysis and anomaly detection.

The success of this project will be evaluated based on the efficiency and effectiveness of the developed queries for log data management. The project will also be evaluated based on its ability to provide insights into log data and identify potential issues. Overall, this project aims to provide a valuable contribution to the field of log data management by demonstrating practical solutions for log data analysis using Azure Log Analytics Workspace.

2.LITERATURE REVIEW

CHAPTER-2

LITERATURE SURVEY

There are several advantages to deploying resources in the Azure cloud compared to on-premises infrastructure. The following literature review summarizes some of the key advantages of Azure cloud deployment with references to support these claims:

1. **Scalability and Flexibility:** One of the most significant advantages of Azure cloud deployment is scalability and flexibility. Azure allows organizations to quickly scale up or down their resources based on demand without having to invest in additional hardware. According to ***Kumar et al. (2020),*** Azure's ability to scale on demand and offer flexible pricing models provides significant benefits for businesses.
2. **Security and Compliance:** Azure offers a high level of security and compliance with various regulatory frameworks, including HIPAA, PCI, and GDPR. This provides peace of mind for businesses that deal with sensitive information. According to a study by ***Canalys (2020),*** security was the top reason why organizations chose to deploy resources in Azure.
3. **Cost Savings:** Deploying resources in Azure can lead to significant cost savings compared to on-premises infrastructure. This is due to several factors, including lower hardware and maintenance costs, flexible pricing models, and pay-as-you-go options. According to a study by ***Forrester (2020),*** organizations that deployed their resources in Azure achieved an ROI of 466% over three years.
4. **Disaster Recovery and Business Continuity:** Azure cloud deployment provides businesses with robust disaster recovery and business continuity capabilities. According to a study by ***Synergy Research Group (2021),*** Azure has one of the highest uptime rates among cloud providers, offering businesses reliable access to their resources and applications.

In conclusion, deploying resources in the Azure cloud offers several advantages, including scalability and flexibility, security and compliance, cost savings, improved business agility, and disaster recovery and business continuity capabilities. These advantages make Azure an attractive option for businesses looking to move away from on-premises infrastructure and towards cloud deployment.

3.SYSTEM ANALYSIS

CHAPTER-3

SYSTEM ANALYSIS

3.1 FEASIBILITY STUDY

A feasibility study for virtual network peering would involve an analysis of the technical, financial, and operational considerations involved in establishing such a network. Here are some of the key factors that would need to be examined:

3.1.1 Technical Feasibility:

Compatibility: Azure Log Analytics provides significant benefits, including scalability, cost savings, security, a powerful query language in KQL, and built-in integration with other Azure services. As a result, more and more organizations are turning to Azure cloud for their log data management needs.

Security: On-premises log analytics solutions require the user to manage security measures, including firewalls, access controls, and intrusion detection. In contrast, Azure cloud provides a secure infrastructure with built-in security features such as identity and access management, encryption, and compliance certifications. This can help organizations ensure their log data is safe from potential breaches.

KQL Query Language: KQL (Kusto Query Language) is a powerful query language used for log analytics in Azure. While on-premises log analytics solutions may offer their own query languages, KQL has a robust set of features that can help users quickly analyze log data, suchas time-based functions, machine learning capabilities, and easy-to-use syntax.

3.1.2 Economical Feasibility:

Costs: On-premises log analytics solutions can have high upfront costs due to hardware and software purchases, and ongoing costs for maintenance and upgrades. In contrast, Azure cloud offers a pay-as-you-go model, where users pay only for the resources they use, and there are no upfront costs. This can result in significant cost savings for organizations with varying log data management needs.

3.1.3 Social feasibility:

Integration: On-premises log analytics solutions may require manual integration with other tools or platforms, while Azure Log Analytics has built-in integration with other Azure services, including Azure Monitor, Azure Sentinel, and Azure Data Factory. This makes it easier for organizations to streamline their log data management workflows and gain insights across their entire infrastructure.

Scalability: On-premises log analytics solutions can be limited in terms of scalability due to hardware and space constraints. In contrast, Azure cloud offers scalable resources where users can easily increase or decrease their resources as needed. This means that Azure Log Analytics can handle more significant amounts of data and provide faster query results.

3.2 EXISITING SYSTEM

KQL (Kusto Query Language) is a query language developed by Microsoft for analyzing large volumes of data in real-time. KQL is the language used by Azure Data Explorer, which is a fast and scalable data analytics service provided by Microsoft.

Azure Data Explorer provides a fully managed service for ingesting, storing, and querying large amounts of data. It supports data from a variety of sources, including logs, telemetry data, and other structured data. KQL is used to query this data and extract insights.

Some of the key features of the existing system of KQL include:

1. **Cloud-Based Service:** Azure Data Explorer is a fully managed cloud-based service provided by Microsoft. It is designed to be scalable and highly available, with automaticscaling and replication built-in.

2. **Columnar Storage:** Azure Data Explorer uses a columnar storage format, which provides efficient storage and query performance. This format is optimized for handling large amountsof data and allows for fast queries on large datasets.

3. **Real-time Data Analysis:** KQL is optimized for real-time data analysis and can be used toanalyze data as it is generated. This makes it ideal for monitoring and alerting systems.

4. **Integration:** KQL integrates seamlessly with other Microsoft tools and services, such asAzure Stream Analytics, Azure Functions, and Power BI. This allows users to easily buildend-to-end data pipelines and dashboards.

5. **Security:** Azure Data Explorer provides advanced security features, such as encryption ofdata at rest and in transit, role-based access control, and auditing.

Overall, the existing system of KQL and Azure Data Explorer provides a powerful and flexible platform for data analysis and management. Its cloud-based architecture, real-time data analysis capabilities, and integration with other Microsoft tools make it a popular choice for data-driven organizations.

3.3 DISADVANTAGES

While KQL (Kusto Query Language) has several advantages, there are also some potential disadvantages that users should be aware of. Here are some potential disadvantages of KQL:

1. **Learning Curve:** While KQL has a relatively simple syntax, users who are not familiarwith SQL or other query languages may still face a learning curve when getting started with KQL.
2. **Limited Functionality:** KQL has a limited set of functions and capabilities compared to other query languages like SQL. For example, KQL does not support some common SQLoperations such as subqueries or join operations.
3. **Requires Internet Access:** KQL is a cloud-based service, which means that users musthave internet access to use it. This could be an issue for users who need to work with data offline or in areas with limited internet connectivity.
4. **Vendor Lock-In:** KQL is a proprietary language developed by Microsoft, which means that users who rely on KQL may be locked into using Microsoft's products and services.
5. **Cost:** KQL is a paid service, and users must pay for the amount of data they store and the number of queries they run. This could be a concern for users with large datasets or limited budgets.

Overall, while KQL has several advantages, it also has some potential disadvantages that users should consider before deciding to use it. It is important to evaluate the trade-offs between KQL's strengths and limitations before committing to using it for data analysis.

3.4 PROPOSED SYSTEM

As far as I know, KQL (Kusto Query Language) is a mature and established query language used in Azure Data Explorer, which is a fast and scalable data analytics service provided by Microsoft. As such, there may not be a specific "proposed system" for KQL. However, there are ongoing efforts to enhance the capabilities and features of KQL to better serve the needs of users.

Some possible directions for future development of KQL could include:

1. **Enhanced Query Capabilities:** As with any query language, there is always room for improvement in terms of query performance and functionality. Future versions of KQL could incorporate additional query functions and operators to support more complex analysis.
2. **Machine Learning Integration:** As machine learning and AI become increasingly important in data analysis, it is possible that KQL could be enhanced to better support machine learning models and algorithms.
3. **Improved Data Visualization:** While KQL already supports data visualization throughintegrations with tools like Power BI, there is always room for improvement in terms of making data visualization more intuitive and user-friendly.
4. **Improved Security:** As data privacy and security become increasingly important, future versions of KQL could include enhanced security features to better protect data andensure compliance with regulations.
5. **More Flexible Deployment Options:** While Azure Data Explorer is a powerful cloud-based service, some users may prefer to deploy KQL in other environments, such as on- premises or in hybrid cloud environments. Future versions of KQL could be designed to be more flexible in terms of deployment options.

Overall, the future development of KQL will likely focus on enhancing its capabilities and features to better serve the needs of users and keep up with changing trends in data analysis and management.

3.5 ADVANTAGES

KQL (Kusto Query Language) is a query language used for analyzing large amounts of data in real-time. Here are some advantages of KQL:

1. **Simple Syntax:** KQL uses a simple syntax that is easy to learn and use. Its syntax issimilar to SQL, which makes it familiar to users who have experience with SQL.
2. **Query Performance:** KQL is designed to be highly performant and can handle largedatasets. It uses a columnar data store that allows for efficient processing of data.
3. **Real-time Data Analysis:** KQL is optimized for real-time data analysis and can be used to analyze data as it is generated. This makes it ideal for monitoring and alerting systems.
4. **Flexibility:** KQL is a versatile language that can be used to query a wide range of datasources. It can be used to query data stored in Azure Data Explorer, Azure Log Analytics, Azure Monitor, and other data sources.
5. **Integration:** KQL integrates seamlessly with other Microsoft tools and services. It canbe used with Azure Data Factory, Azure Stream Analytics, Azure Functions, and other Azureservices.

Overall, KQL is a powerful query language that is easy to learn and use, highly performant, and optimized for real-time data analysis. Its flexibility and integration with other Microsoft services make it an excellent choice for data analysis and monitoring.

4.SYSTEM REQUIREMENTS

CHAPTER 4

SYSTEM REQUIREMENTS

4.1 HARDWARE REQUIREMENTS

- RAM: minimum 4 GB
- Space on Hard Disk: minimum 256 GB
- Processor: Core i3 or i5
- High speed internet(min-50Mbps per second)

4.2 OPERATING SYSTEMS SUPPORTED

- Windows 7 or above

4.3 SOFTWARE REQUIREMENTS

- Microsoft Azure in cloud

5.SYSTEM DESIGN

CHAPTER-5

SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE

We did this virtual network peering based on the cloud architecture provided below. Each virtual network, including a peered virtual network, can have its own subnet.

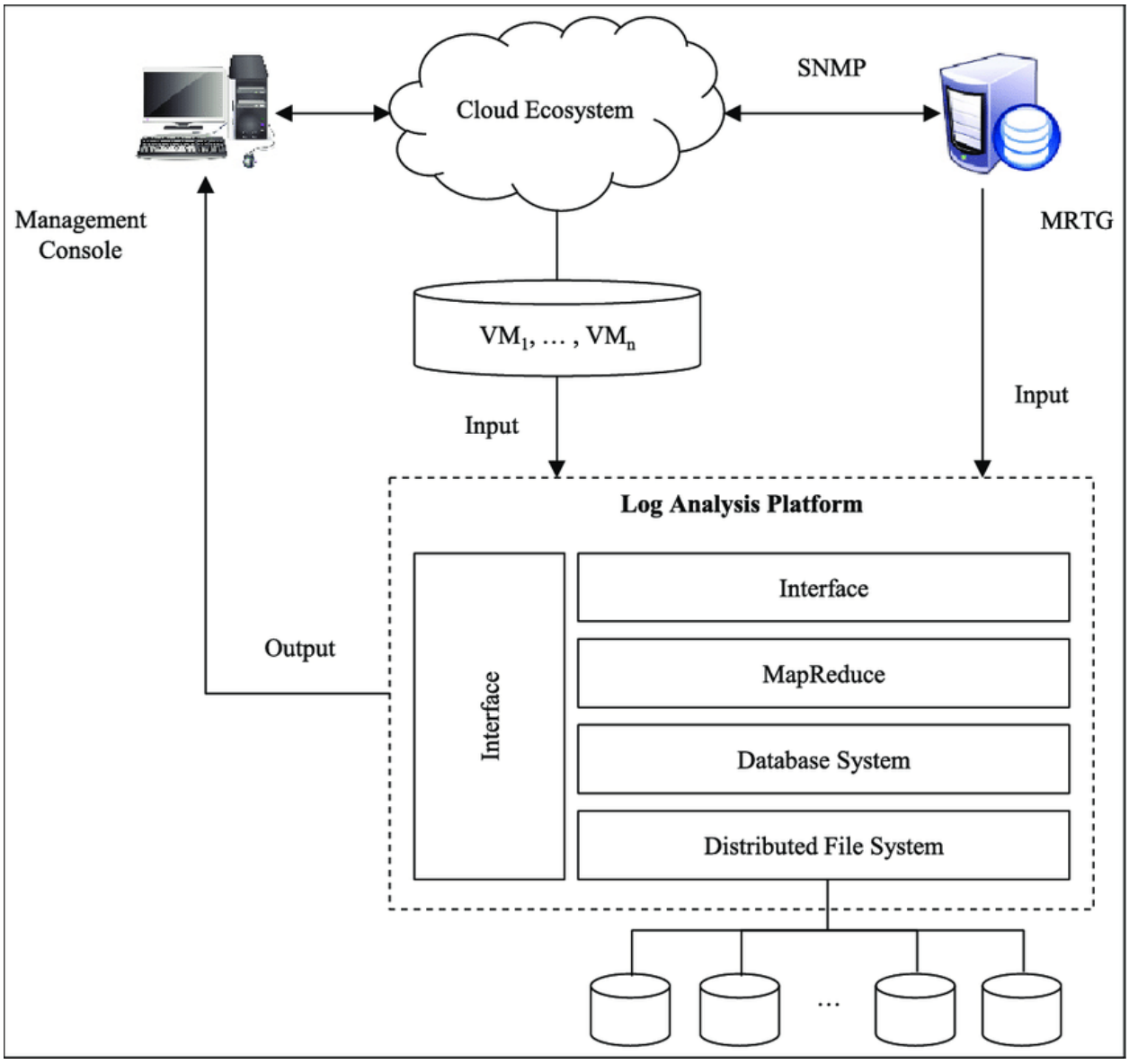


Fig: System architecture

DATA FLOW DIAGRAM

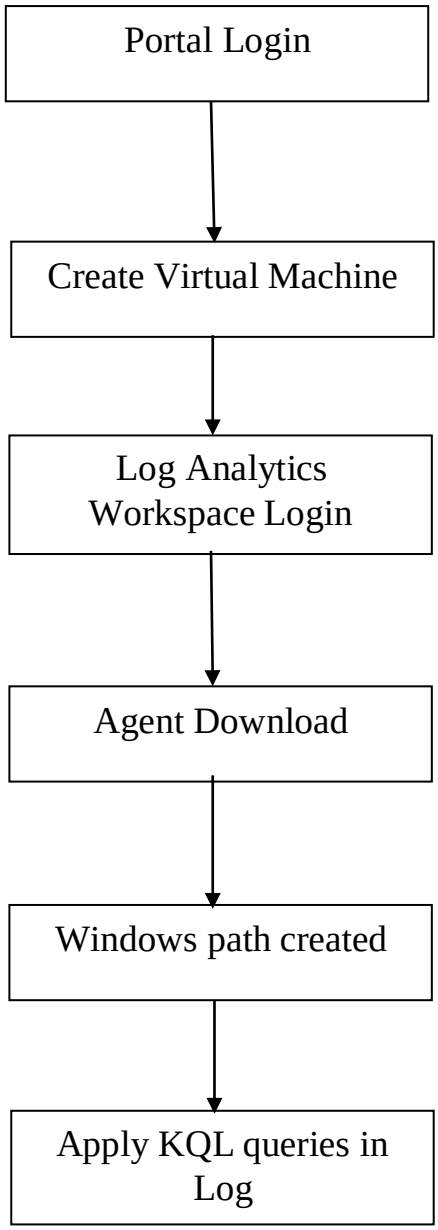


Fig: Data Flow for KQL

5.2 UML DIAGRAMS

UML stands for Unified Modelling Language. It is a generic developmental modelling language used for analysis, design and implementation of software systems. The purpose of UML is to provide a simple and common method to visualise a software system's inherent architectural properties. Over time, UML has become the de-facto standard of building Object-Oriented Software. UML blueprints are used by business users, developers and anybody who need data modelling. UML is not a development method or a programming language.

5.2.1 Goals

The primary goal of UML is to define some general-purpose simple modelinglanguage so that all modelers can use and understand.

- UML is not a development method rather it accompanies with processes to make asuccessful system.
- UML diagrams are the representation of object-oriented concepts only.
- Thus, before learning UML, it becomes important to understand OO concept indetail.
- UML can be described as the successor of object-oriented analysis and design.
- UML diagrams are not only made for developers but also for business users, common people, and anybody interested to understand the system.
- The system can be a software or non-software system. Thus it must be clear that UML is not a development method rather it accompanies with processes to make it a successful system.
- In conclusion, the goal of UML can be defined as a simple modeling mechanism to model all possible practical systems in today's complex environment.

5.2.2 Use Case Diagrams:

A Use case diagrams can be used to represent the functional requirements of log data management with KQL by showing the interactions between the system and its actors, such as the user or the log data source.

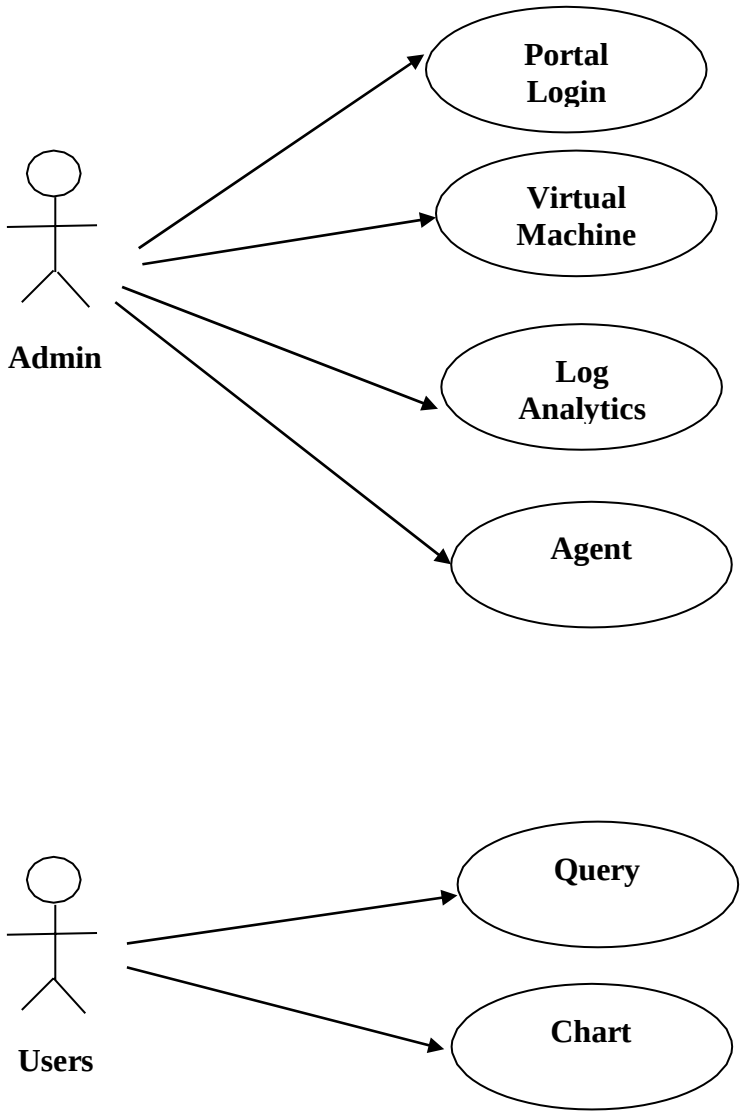


Fig: Use case for LAW

5.2.3 Class Diagram:

Class diagrams can be used to represent the structure of the log data with KQL by showing the classes, their attributes, and relationships, such as the classes that represent log messages, fields, and operators.

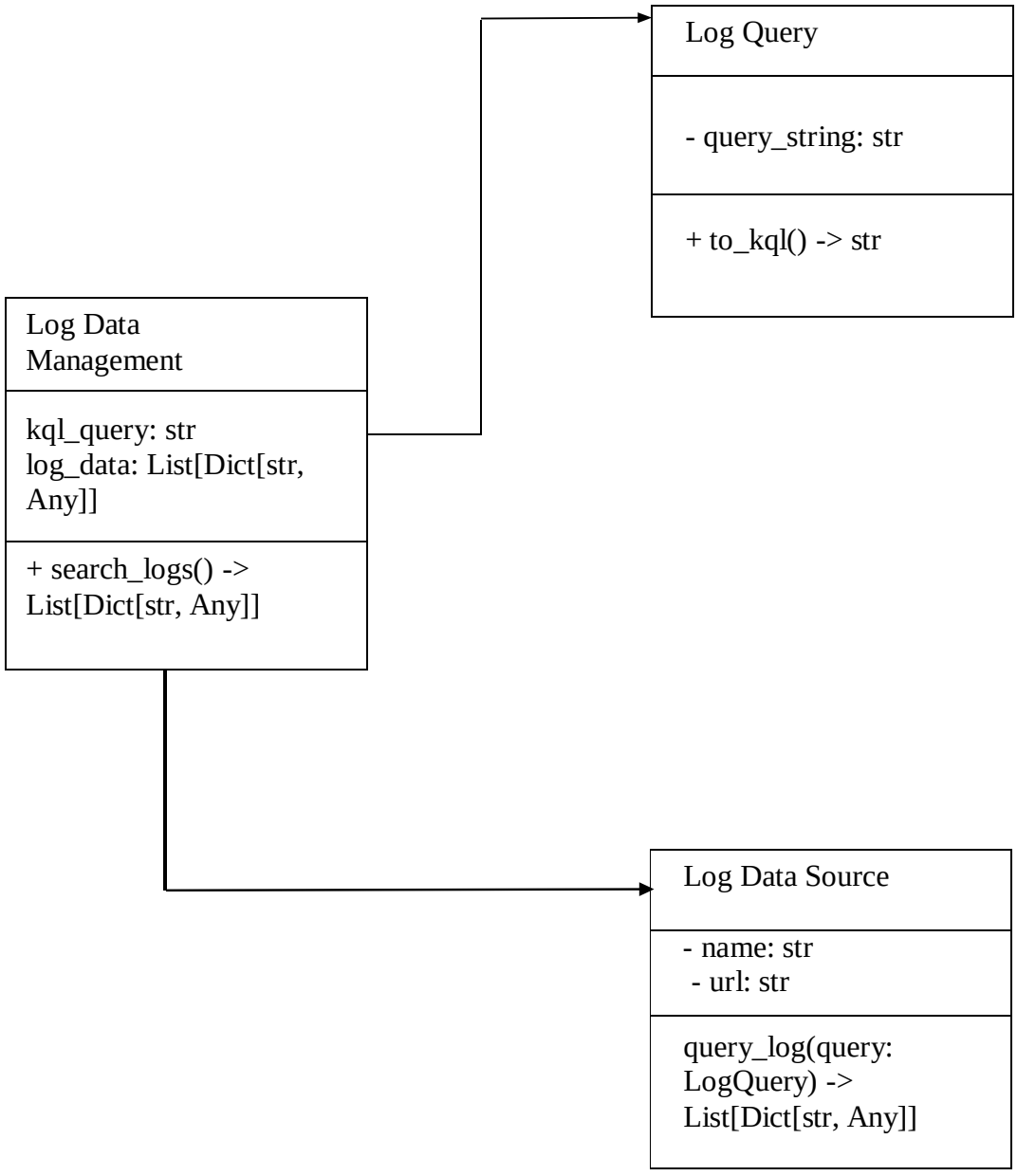


Fig: Class diagram for LAW

5.2.4 Sequence Diagram:

Sequence diagrams can be used to represent the dynamic behavior of the log data management process with KQL by showing the interactions between the system components and the log data source, such as the sequence of events that occur when a query is executed.

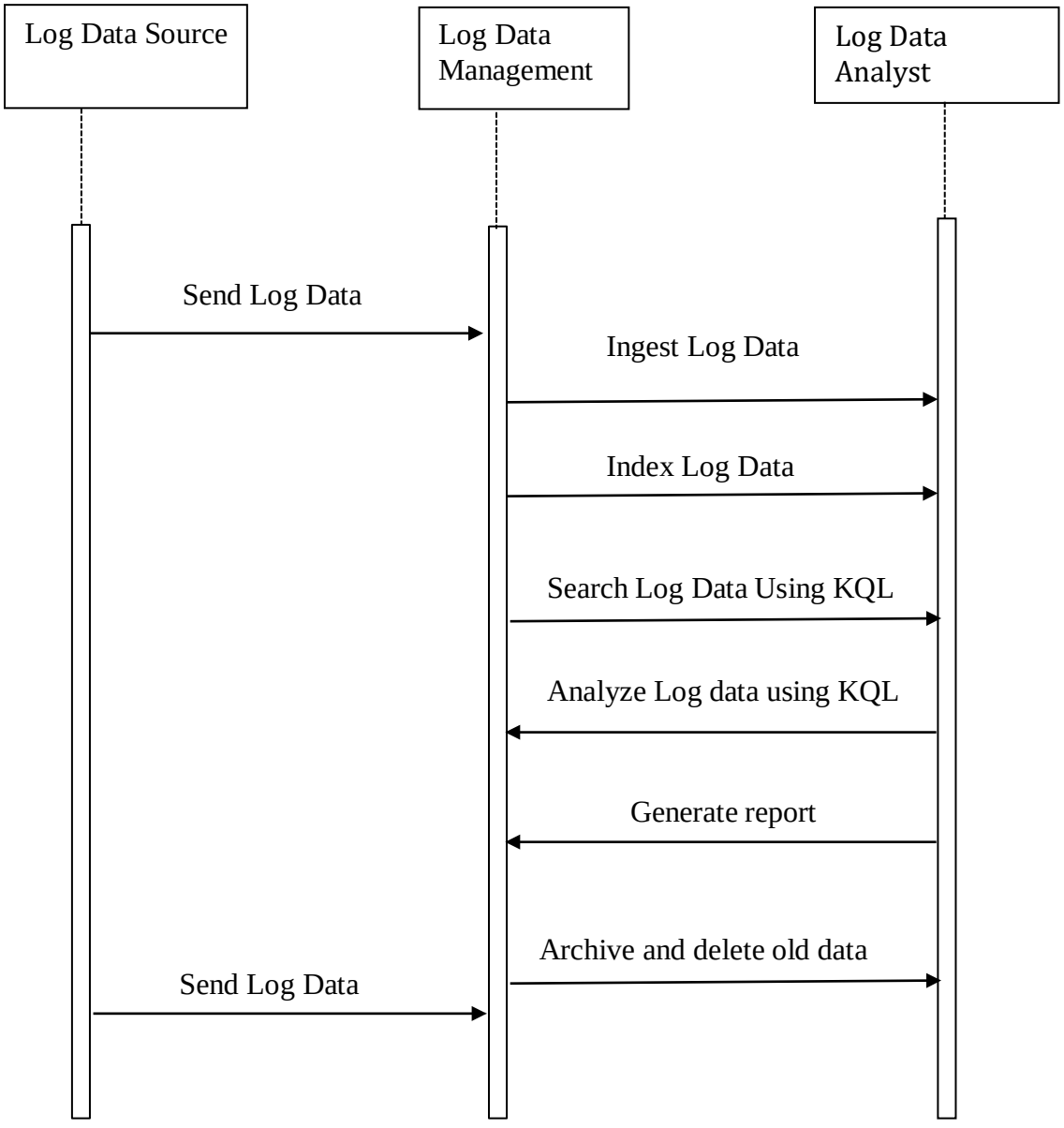


Fig: Sequence diagram for LAW

6.SOFTWARE ENVIRONMENT

CHAPTER 6
SOFTWARE ENVIRONMENT

6.1 What is CLOUD?

The word "CLOUD" often refers to the Internet, which more precisely means data centres full of servers connected to the Internet performing services such as website hosting, email, video calling and streaming Communications network.

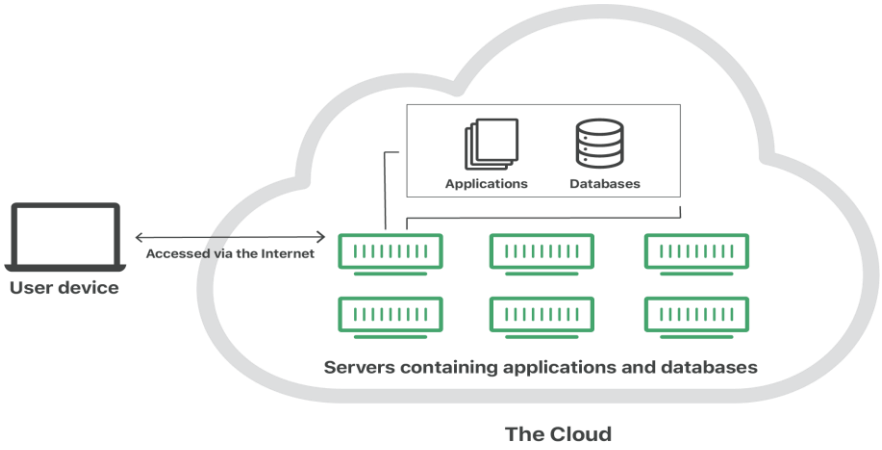


Fig: Cloud

The definition for the cloud can seem murky, but essentially, it's a term used to describe a global network of servers, each with a unique function. The cloud is not a physical entity, but instead is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem. These servers are designed to either store and manage data, run applications, or deliver content or a service such as streaming videos, web mail, office productivity software, or social media. Instead of accessing files and data from a local or personal computer, you are accessing them online from any Internet-capable device—the information will be available anywhere you go and anytime you need it.

Some of the main reasons to use the are cloud convenience and **reliability**. For example, if you've ever used a **web-based email service**, such as **Gmail** or **Yahoo! Mail**, you've already

used the cloud. All of the emails in a web-based service are stored on servers rather than on your computer's hard drive. This means you can access your email from any computer with an Internet connection. It also means you'll be able to recover your emails if something happens to your computer.

6.1.2 What is Cloud Computing

Cloud computing is on-demand access, via the internet, to computing resources applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more hosted at a remote data centre managed by a cloud services provider (or CSP). The CSP makes these resources available for a monthly subscription fee or bills them according to usage.

Cloud computing service models are based on the concept of sharing on-demand computing resources, software, and information over the internet. Companies or individuals pay to access a virtual pool of shared resources, including compute, storage, and networking services, which are located on remote servers that are owned and managed by service providers.

The term ‘cloud computing’ also refers to the technology that makes cloud work. This includes some form of *virtualized IT infrastructure*- servers, operating system software, networking, and other infrastructure that’s abstracted, using special software, so that it can be pooled and divided irrespective of physical hardware boundaries. For example, a single hardware server can be divided into multiple virtual servers.

Virtualization enables cloud providers to make maximum use of their data centre resources. Not surprisingly, many corporations have adopted the cloud delivery model for their on-premises infrastructure so they can realize maximum utilization and cost savings vs. traditional IT infrastructure and offer the same self-service and agility to their end-users.

Fig: Cloud Computing

In simpler terms, cloud computing uses a network (most often, the internet) to connect users to a cloud platform where they request and access rented computing services. A central server handles all the communication between client devices and servers to facilitate the exchange of data. Security and privacy features are common components to keep this information secure and safe.

When adopting cloud computing architecture, there is no one-size-fits-all. What works for another company may not suit you and your business needs. In fact, this flexibility and versatility is one of the hallmarks of cloud, allowing enterprises to quickly adapt to changing markets or metrics.

6.1.3 Cloud Computing Architecture

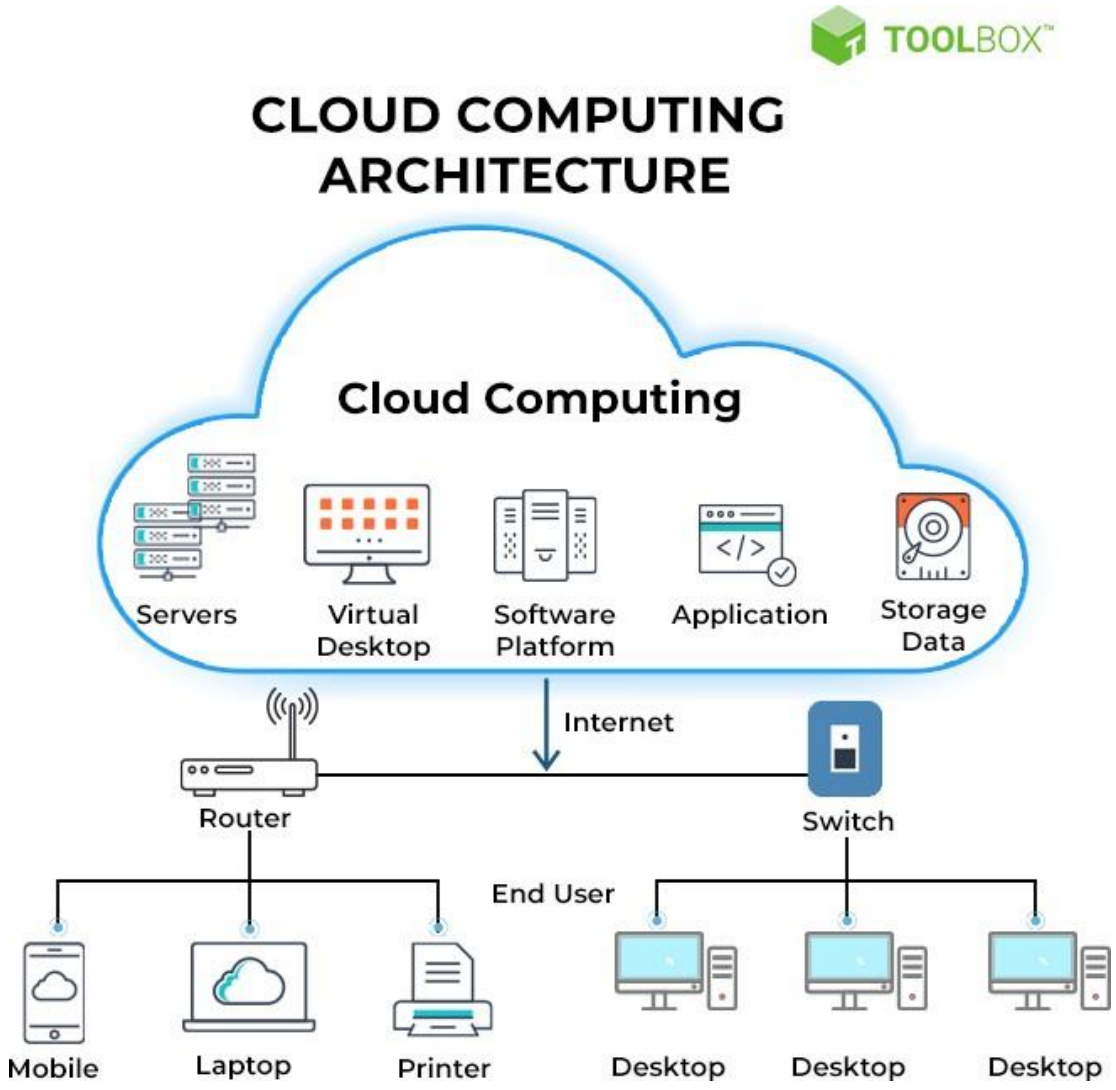


Fig: Cloud Computing Architecture

Cloud Architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over application programming interfaces, usually web services.

6.1.4 Basic Concepts

There are certain services and models working behind the scene making the cloud computing feasible and accessible to the end users. Following
are the working models for cloud computing:

1. Deployment Models
2. Service Models

6.1.4.1 Deployment Models:

The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's nature and purpose. The location of the servers you're utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types.

Different types of cloud computing deployment models are:

A. Public cloud
B. Private cloud
C. Hybrid cloud
D. Community cloud

A. Public Cloud: A public cloud is an IT model where public cloud service providers make computing services—including compute and storage, develop-and-deploy environments, and applications—available on-demand to organizations and individuals over the public internet.

B. Private Cloud : A **Private Cloud** is a model cloud computing where the infrastructure is dedicated to a single user organization.

C. Hybrid Cloud : A hybrid cloud is a mixed computing environment where applications are run using a combination of computing, storage, and services in different environments- public clouds and private clouds, including on-premises data centres or "edge" locations.

D. Community Cloud : Community cloud computing refers to a shared cloud computing service environment that is targeted to a limited set of organizations or employees (such as banks or heads of trading firms).

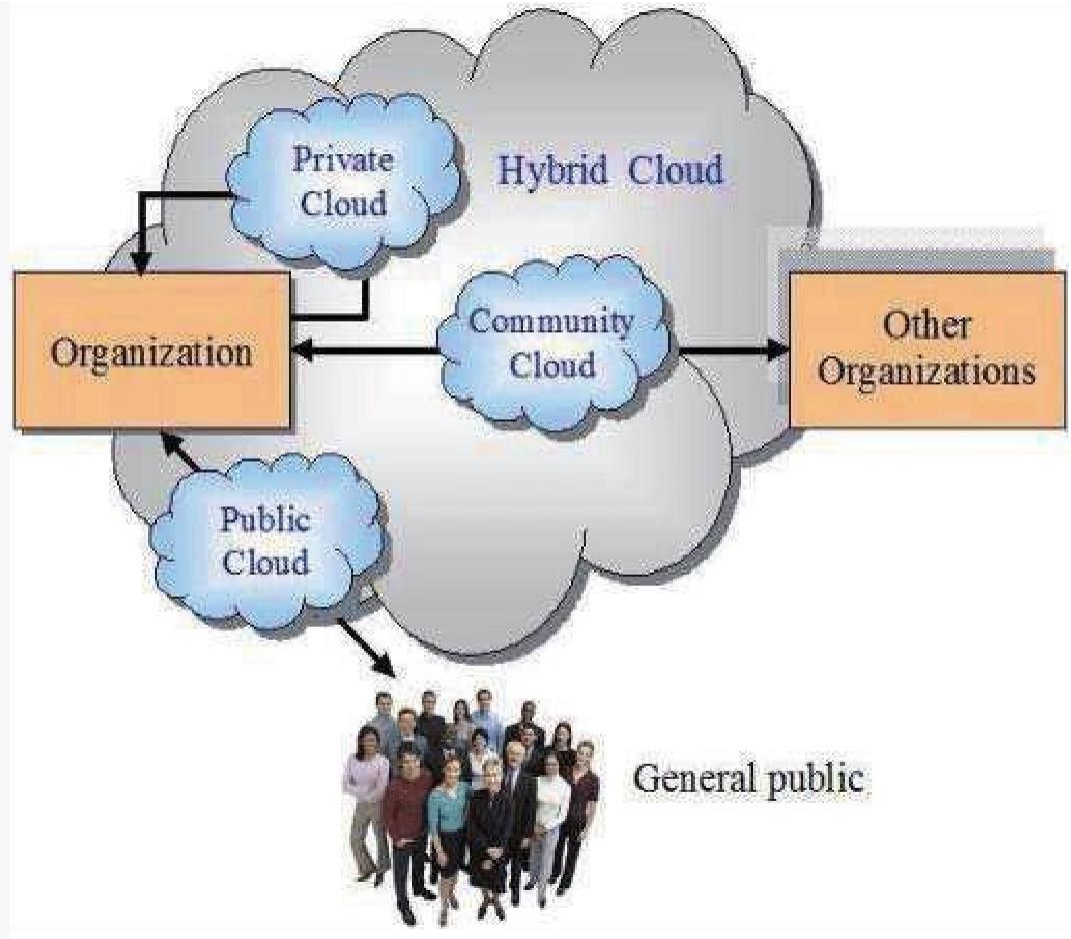


Fig: Deployment Models

6.1.4.2 Service Models :

Cloud Computing can be defined as the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Companies offering such kinds of Cloud computing services are called *cloud providers* and typically charge for cloud computing services based on usage. Grids and clusters are the foundations for cloud computing.

Most cloud computing services fall into three broad categories:

A. Software as a service (SaaS)
B. Platform as a service (PaaS)
C. Infrastructure as a service (IaaS)

A. Software as a service (SaaS) : It is a way of delivering application over the

Internet- as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.

B. Platform as a service (PaaS) : It is a complete development environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications.

C. Infrastructure as a service (IaaS) : Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis. IaaS is one of the four types of cloud services, along with software as a service (SaaS), platform as a service (PaaS), and serverless.

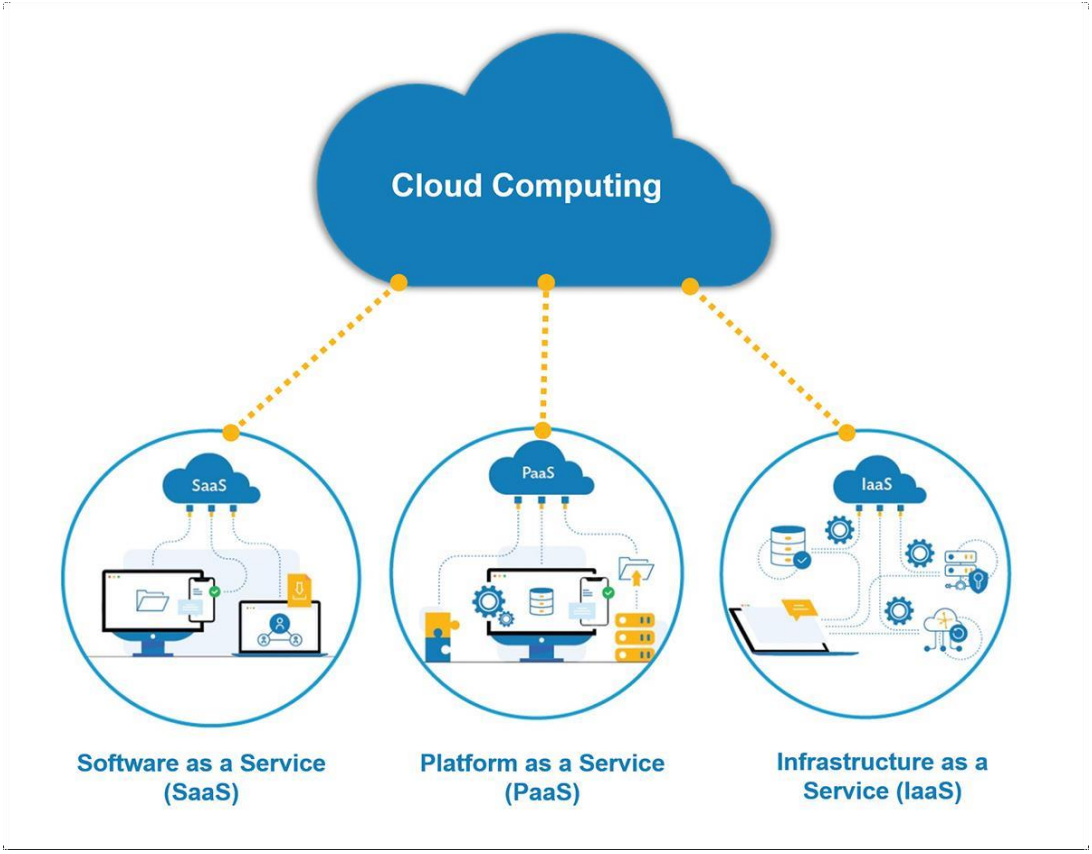


Fig: Service Models

6.1.5 Cloud Service Providers

Cloud computing is computing that provides shared resources, software, and information to computers and other devices on demand. It is a flexible model from which customers can access various types of services and applications with the help of the internet. Cloud service providers provide cloud services to customers over the internet.

Fig: Cloud Service Providers

There are so many cloud services these days that it can be challenging to figure out which ones are best. But deciding which one best fits your needs is important. This article lists the top globally available cloud service providers in 2023.

6.2 MICROSOFT AZURE

6.2.1 Introduction to Microsoft Azure

Microsoft Azure, often referred to as **Azure** is a cloud computing platform operated by Microsoft that provides access, management, and development of applications and services via around the world-distributed data centres. Microsoft Azure has multiple capabilities such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) and supports many different programming languages, tools, and frameworks, including both Microsoft-specific and third-party software and systems.

Microsoft Azure

Developer(s)	Microsoft
Initial release	October 27, 2008; 14 years ago[1]
Operating system	Linux, Microsoft Windows, iOS, Android
Type	Web service, cloud computing
License	Proprietary for platform, MIT License for client SDKs
Website	azure.microsoft.com

Fig: Azure

6.2.2 History :

Microsoft unveiled Windows Azure in early October 2008 but it went to live after February 2010. Later in 2014, Microsoft changed its name from Windows Azure to Microsoft Azure. Azure provided a service platform for .NET services, SQL Services, and many Live Services. Many people were still very skeptical about "the cloud". As an industry, we were entering a brave new world with many possibilities. Microsoft Azure is getting bigger and better in coming days. More tools and more functionalities are getting added. It has two releases as of now. It's famous version **Microsoft Azure v1** and later **Microsoft Azure v2**. Microsoft Azure v1 was more like JSON script driven then the new version v2, which has interactive UI for simplification and easy learning. Microsoft Azure v2 is still in the preview version.

6.2.3 Why Azure?

Microsoft Azure is a cloud computing services provided by internet giant Microsoft. It allows users to build, test, host or manage web applications and data.

Microsoft has its own data center infrastructure across the world which provides over 600 kind of cloud services.

The direct and major competitor of Microsoft Azure is Amazon Web Services, commonly called as AWS. Apart from that it does compete with Google Cloud and Alibaba Cloud which are quite behind.

Microsoft Corporation's Intelligent Cloud segment contains Azure, the second largest cloud service provider globally. Through Microsoft Azure, the company delivers a consistent hybrid cloud experience, developer productivity, artificial intelligence (AI) capabilities, and security & compliance.

Microsoft Cloud revenue, which includes revenue from Azure and other cloud services, Office 365 Commercial, the commercial portion of LinkedIn, and Dynamics 365, reached $23.4 billion for the latest quarter, an increase of 32% year-over-year. As such, on an annualized basis, Microsoft Cloud revenue currently stands at $93.6 billion. However,

Microsoft does not explicitly disclose Azure revenues, meaning that Azure is only a subset of total Microsoft Cloud revenue.

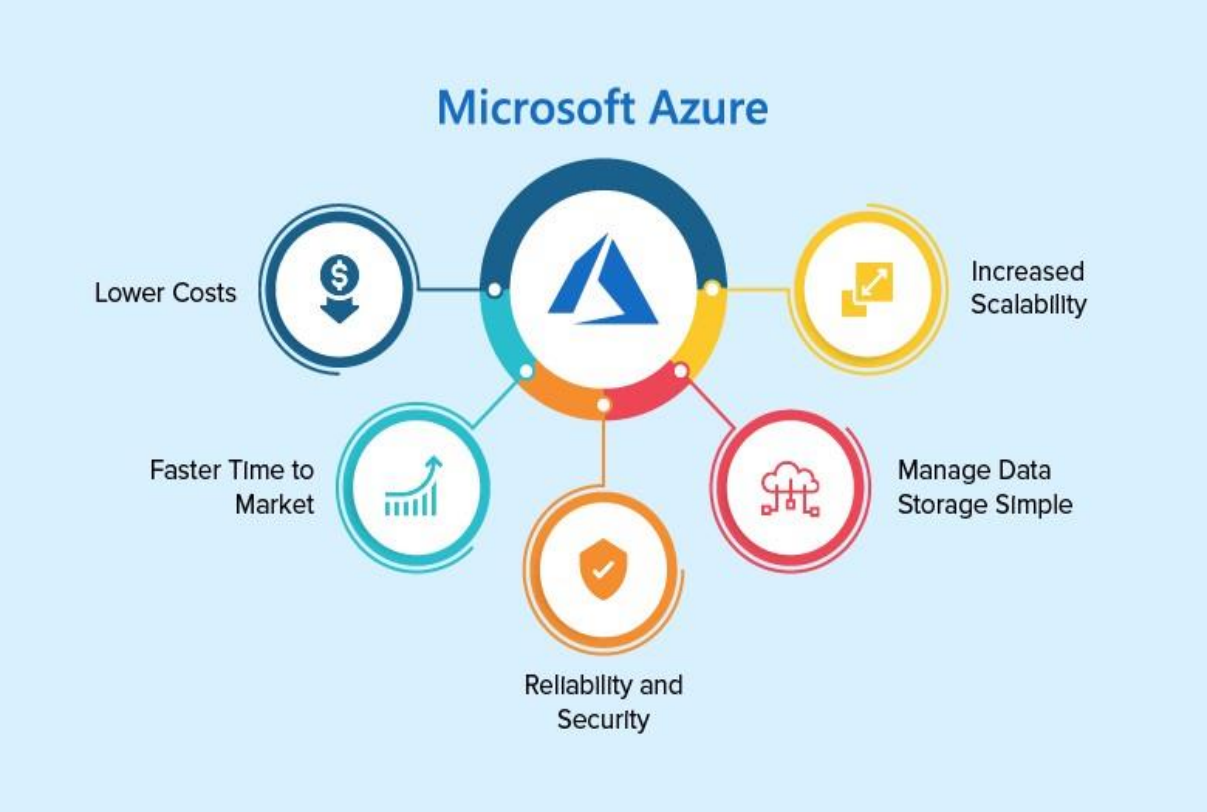


Fig: Microsoft Azure

6.2.4 DATACENTERS

Microsoft Azure currently has 59 regions in operation and a further 19 under development, meaning that the company will have a **total** of 78 regions available in the near-term. Within each Azure **region** are 1 to 3 unique physical locations, known as **availability zones**, which offer high uptime to protect data and applications from data centre failures.

Presently, Microsoft Azure has 113 availability zones in operation and a further 51 under development, meaning that the company will have a **total** of 164 availability zones existing in the near-term.

Microsoft Azure has similar way of classifying the location as that to AWS. Mainly, it uses Geographies (mostly countries, continents as well), Regions (cities) and availability zones. In

fact, almost all of the major cloud infrastructure providers these days follow this pattern to describe their data center locations.

Fig: Data Centers

6.2.5 Microsoft Azure has data centre regions in following maingeographies:

Since Microsoft has used both continents and countries as geographies, for your convenience, we have separated out each such geographies on the basis of continents in our world political map.

6.2.5.1 Microsoft Azure Geographies in Asia & Oceania:

- Asia Pacific
- Australia
- China
- India

- Israel
- Japan
- Korea
- New Zealand
- Qatar
- United Arab Emirates

6.2.5.2 Microsoft Azure Geographies in Africa:

- Africa

6.2.5.3 Microsoft Azure Geographies in Europe:

- Europe
- France
- Germany
- Italy
- Norway
- Poland
- Spain
- Switzerland
- United Kingdom

6.2.5.4 Microsoft Azure Geographies in North America:

- Azure Government
- Canada
- United States

6.2.5.5 Microsoft Azure Geographies in South America:

- Brazil
- Mexico

6.2.6 Where Are Microsoft Azure Data Centres Located?

6.2.6.1 United States :

In the United States, Microsoft Azure operates or is planning 10 regions and 26 availability

zones. Specifically, Azure is available or will be opening in the following markets: Des Moines, Iowa; Richmond, Virginia; Atlanta, Georgia; Chicago, Illinois; San Antonio, Texas; Cheyenne, Wyoming; San Francisco, California; Moses Lake (Quincy), Washington; and Phoenix, Arizona.

United States – Regions and Availability Zones

Regions	# of Zones	City	State	Opened
Central US	3	Des Moines	Iowa	2014
East US	3	Richmond	Virginia	2012
East US 2	3	Richmond	Virginia	2014
East US 3	3	Atlanta	Georgia	*Future*
North Central US	1	Chicago	Illinois	2009
South Central US	3	San Antonio	Texas	2008
West Central US	3	Cheyenne	Wyoming	2016
West US	1	San Francisco	California	2012
West US 2	3	Moses Lake	Washington	2007
West US 3	3	Phoenix	Arizona	2021
Total	**26**	–	–	–

Fig: United States

6.2.6.2 Azure Government

Azure Government is a cloud service built to meet government security and compliance requirements for classified and unclassified U.S. Government data. For example, agencies and organizations that Azure Government targets are the Department of Defense (DoD), the U.S. Intelligence Community – which includes the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) – federal civilians, and state & local governments.

Through the Azure Government service, Microsoft Azure operates or is planning 8 regions and 12 availability zones. Presently, Azure Government is available in the following markets: Des Moines, Iowa; Richmond, Virginia; Phoenix, Arizona; Austin, Texas; Washington, D.C.; and San Francisco, California.

Azure Government – Regions and Availability Zones

Regions	# of Zones	City	State	Opened
US DoD Central	1	Des Moines	Iowa	2017
US DoD East	1	Richmond	Virginia	2017
US Gov Arizona	1	Phoenix	Arizona	2017
US Gov Texas	1	Austin	Texas	2017
US Gov Virginia	3	Washington	D.C.	2014
US Sec East	1	Richmond	Virginia	2020
US Sec West	1	San Francisco	California	2020
US Sec West Central	3	Des Moines	Iowa	*Future*
Total	**12**	—	—	—

Fig: Azure Government

6.2.6.3 Americas

In the Americas, Microsoft Azure operates or is planning 6 regions and 16 availability zones. Specifically, Azure is available or will be opening in the following markets: Campinas (São Paulo), Brazil; Rio de Janeiro, Brazil; Toronto, Canada; Quebec City, Canada; Santiago, Chile; and Querétaro State, Mexico.

Americas – Regions and Availability Zones

Regions	# of Zones	Location	Country	Opened
Brazil South	3	Campinas	Brazil	2014
Brazil Southeast*	3	Rio de Janeiro	Brazil	2020
Canada Central	3	Toronto	Canada	2016
Canada East	1	Quebec City	Canada	2016
Chile Central	3	Santiago	Chile	*Future*
Mexico Central	3	Querétaro State	Mexico	*Future*
Total	**16**	—	—	—

Fig: Americas

6.2.6.4 Middle East and Africa

In the Middle East and Africa, Microsoft Azure operates or is planning 6 regions and 12 availability zones. Particularly, Azure is available or will be opening in the following markets: Tel Aviv, Israel; Doha, Qatar; Johannesburg, South Africa; Cape Town, South Africa; Abu Dhabi, United Arab Emirates (UAE); and Dubai, United Arab Emirates (UAE)

Middle East and Africa – Regions and Availability Zones

Regions	# of Zones	Location	Country	Opened
Israel Central	3	Tel Aviv	Israel	*Future*
Qatar Central	3	Doha	Qatar	*Future*
South Africa North	3	Johannesburg	South Africa	2019
South Africa West*	1	Cape Town	South Africa	2019
UAE Central*	1	Abu Dhabi	UAE	2019
UAE North	1	Dubai	UAE	2019
Total	**12**	—	—	—

Fig: Middle East and Africa

6.2.6.5 Europe

In Europe, Microsoft Azure operates or is planning 24 regions and 52 availability zones. Particularly, Azure is available or will be opening in the following markets: Vienna, Austria; Brussels, Belgium; Copenhagen, Denmark; Helsinki, Finland; Paris, France; Marseille, France; Frankfurt, Germany; Berlin, Germany; Magdeburg, Germany; Athens, Greece; Dublin, Ireland; Milan, Italy; Amsterdam, Netherlands; Oslo, Norway; Stavanger, Norway; Warsaw, Poland; Madrid, Spain; Gävle, Sweden; Staffanstorp (Malmö), Sweden; Zürich, Switzerland; Geneva, Switzerland; London, United Kingdom; and Cardiff, United Kingdom.

Europe – Regions and Availability Zones

Regions	# of Zones	Location	Country	Opened
Austria East	3	Vienna	Austria	*Future*
Belgium Central	1	Brussels	Belgium	*Future*
Denmark East	3	Copenhagen	Denmark	*Future*
Finland Central	1	Helsinki	Finland	*Future*
France Central	3	Paris	France	2018
France South*	1	Marseille	France	2018
Germany Central (Sovereign)	1	Frankfurt	Germany	2016
Germany North*	1	Berlin	Germany	2019
Germany Northeast (Sovereign)	1	Magdeburg	Germany	2016
Germany West Central	3	Frankfurt	Germany	2019
Greece Central	3	Athens	Greece	*Future*
North Europe	3	Dublin	Ireland	2009
Italy North	3	Milan	Italy	*Future*
West Europe	3	Amsterdam	Netherlands	2010
Norway East	3	Oslo	Norway	2019
Norway West*	1	Stavanger	Norway	2019
Poland Central	3	Warsaw	Poland	*Future*
Spain Central	3	Madrid	Spain	*Future*
Sweden Central	3	Gävle	Sweden	2021
Sweden South*	3	Staffanstorp	Sweden	2021
Switzerland North	1	Zürich	Switzerland	2019
Switzerland West*	1	Geneva	Switzerland	2019
UK South	3	London	UK	2016
UK West	1	Cardiff	UK	2016
Total	**52**	—	—	—

Fig: Europe

Asia Pacific – Regions and Availability Zones

Regions	# of Zones	Location	Country	Opened
Australia Central	1	Canberra	Australia	2018
Australia Central 2*	1	Canberra	Australia	2018
Australia East	3	Sydney	Australia	2014
Australia Southeast	1	Melbourne	Australia	2014
China East	1	Shanghai	China	2014
China East 2	1	Shanghai	China	2018
China East 3*	1	Nanjing	China	2022
China North	1	Beijing	China	2014
China North 2	1	Beijing	China	2018
China North 3	3	Langfang	China	2022
East Asia	3	Hong Kong	SAR	2010
Central India	3	Pune	India	2015
South India	1	Chennai	India	2015
Southcentral India	1	Hyderabad	India	*Future*
West India	1	Mumbai	India	2015
Indonesia Central	3	Jakarta	Indonesia	*Future*
Japan East	3	Tokyo, Saitama	Japan	2014
Japan West	1	Osaka	Japan	2014
Korea Central	3	Seoul	South Korea	2017
Korea South*	1	Busan	South Korea	2017
Malaysia West	3	Kuala Lumpur	Malaysia	*Future*
New Zealand North	3	Auckland	New Zealand	*Future*
Southeast Asia	3	Singapore	Singapore	2010
Taiwan North	3	Taipei	Taiwan	*Future*
Total	**46**	**—**	**—**	**—**

6.2.7 Microsoft Datacentres Present in the World :

Fig: Data Centers

6.2.8 HOW TO CREATE MICROSOFT AZURE ACCOUNT

Click on the **Start free** button.

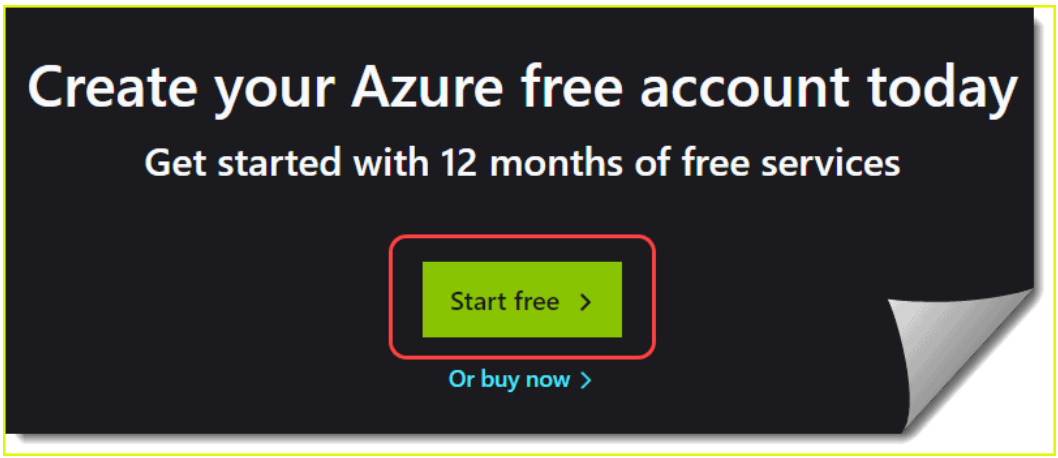
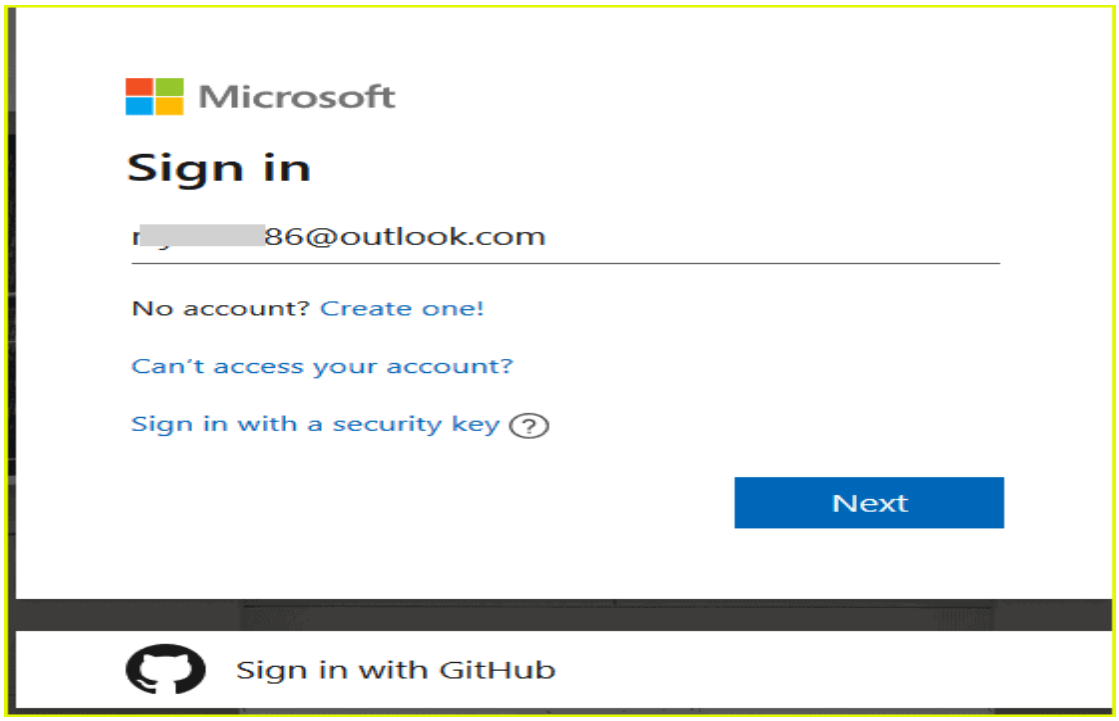


Fig: Creation of Microsoft Azure

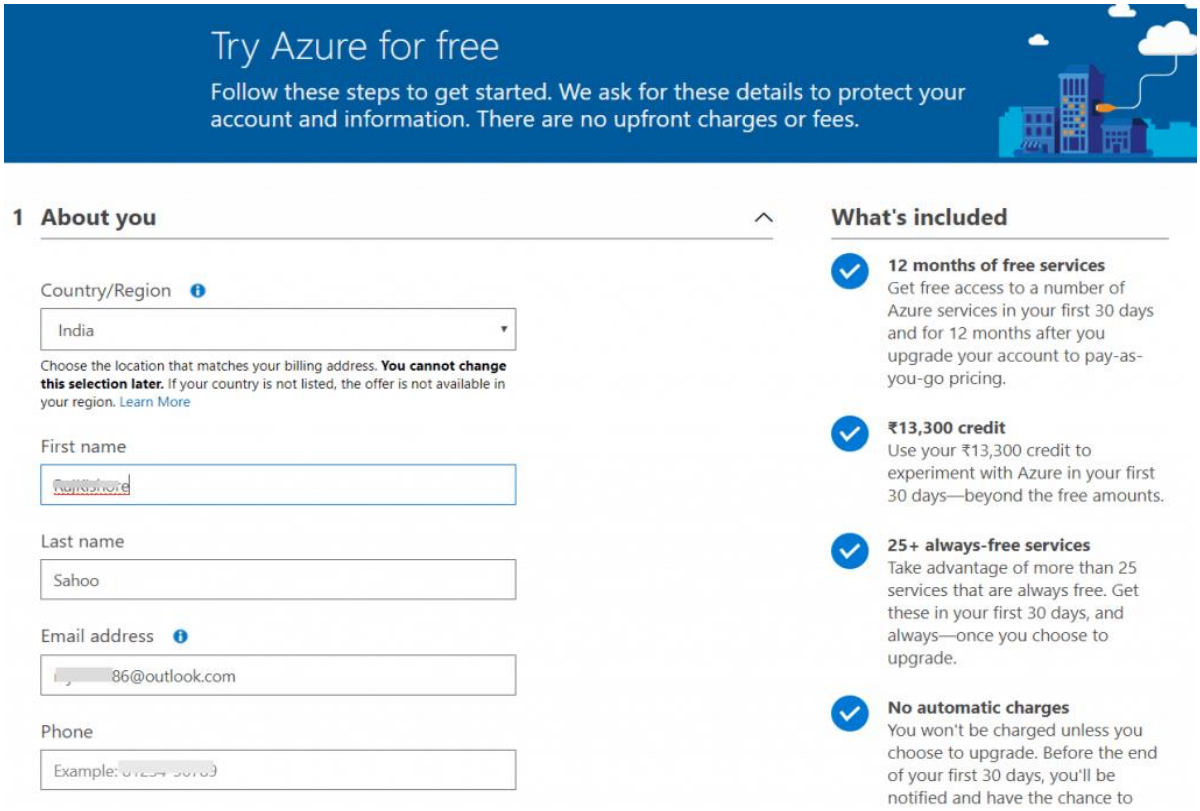
On the next screen, you can enter your email (Microsoft account), Phone or Skype.

Also, you can sign in with your GitHub account.

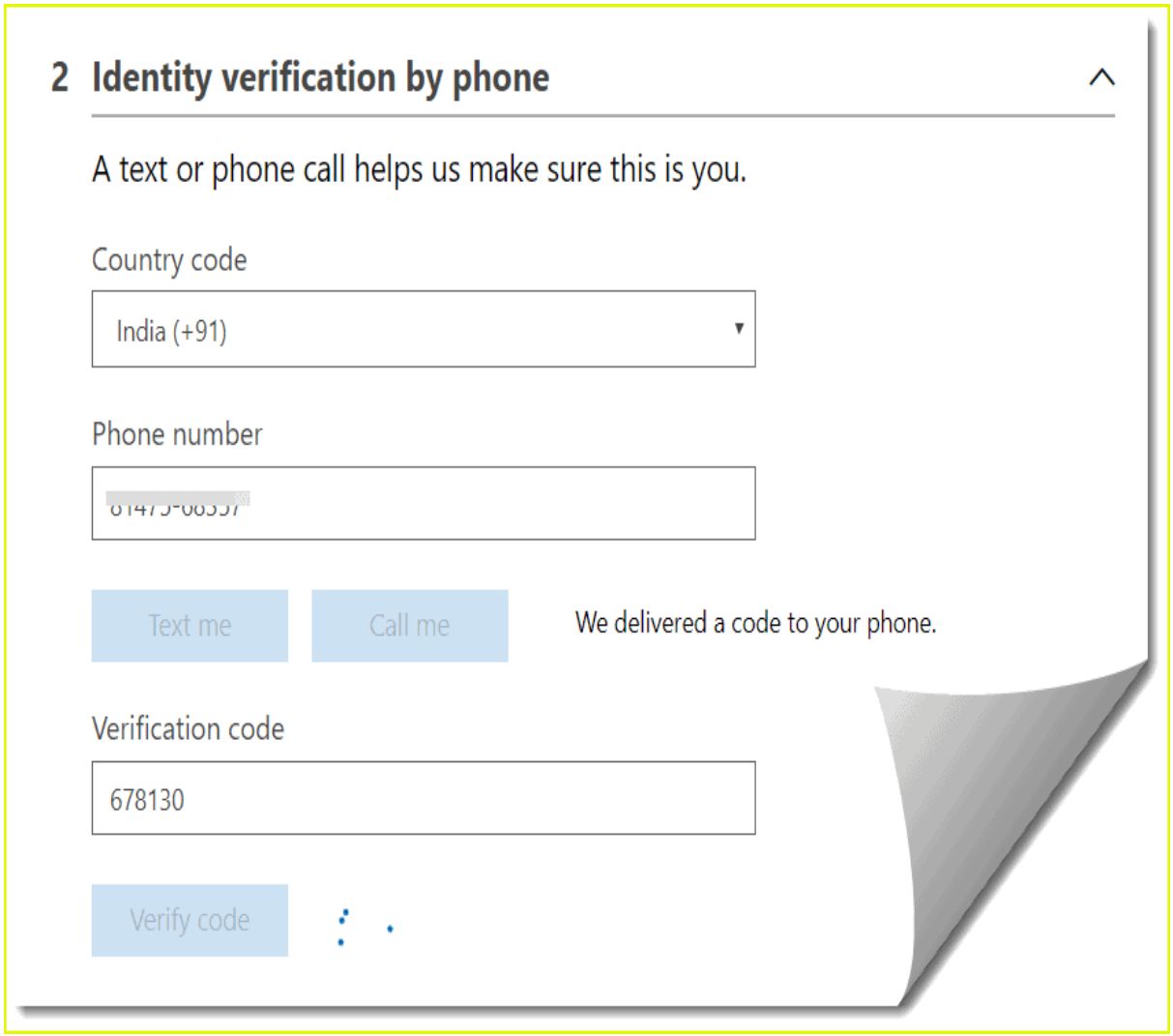


Then it will ask you to enter personal details like Country/Region, First name, last name, Email Address, Phone, City, etc.

Fill in all the details and click on **Next**.



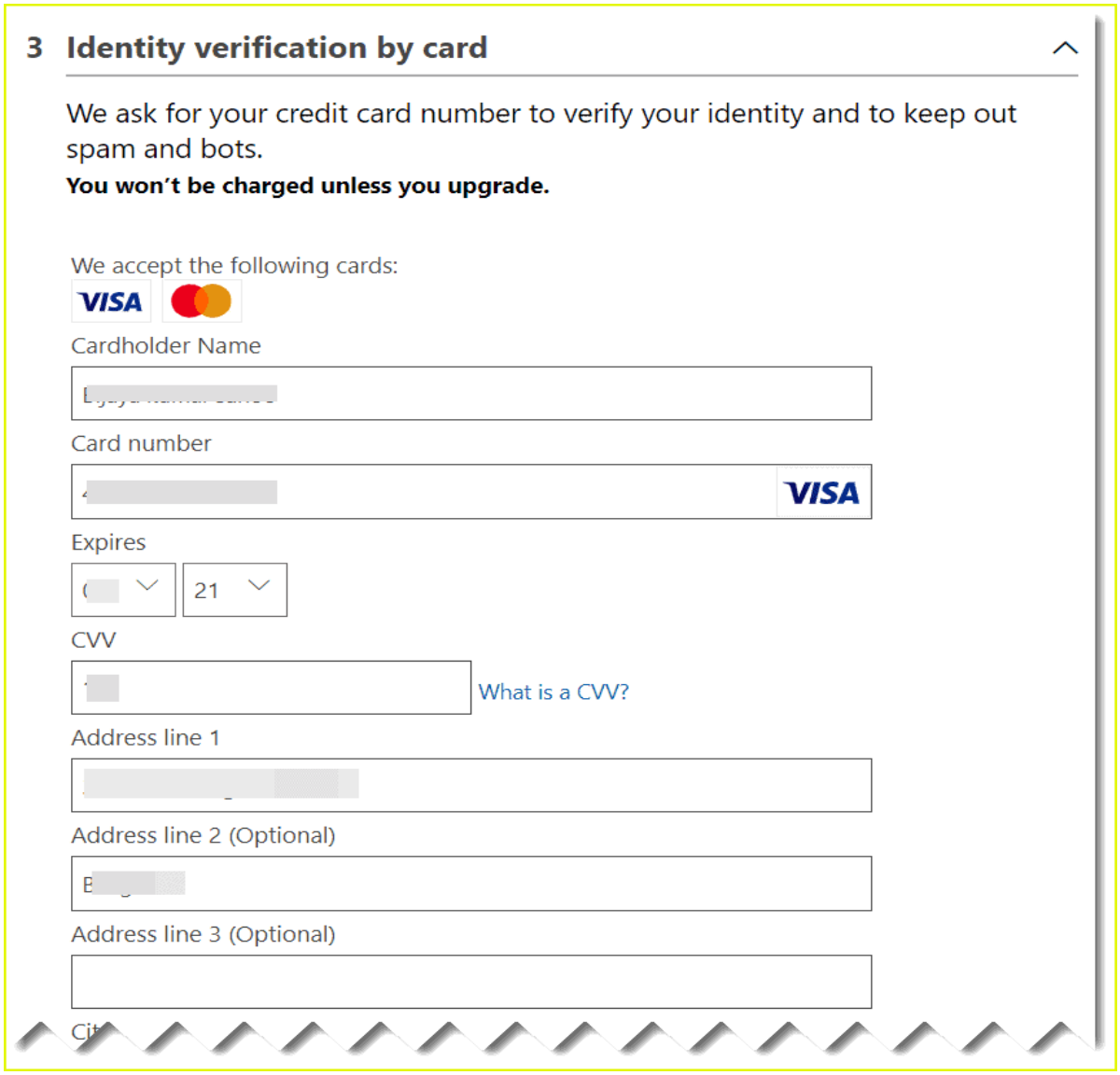
Then it will ask you to provide the Phone number details, make sure to provide a valid phone number. Because you need to confirm by a text message or by a call.



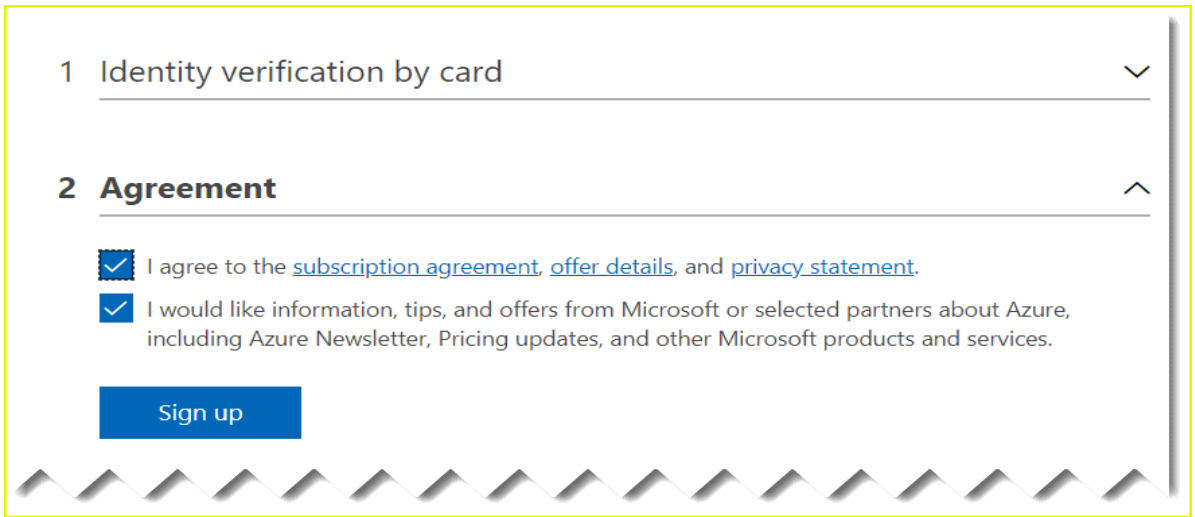
Once verification is done, click on **Next**,

Now, you need to provide the credit card details. Provide everything correctly here. Because it is going to deduct a little amount of money

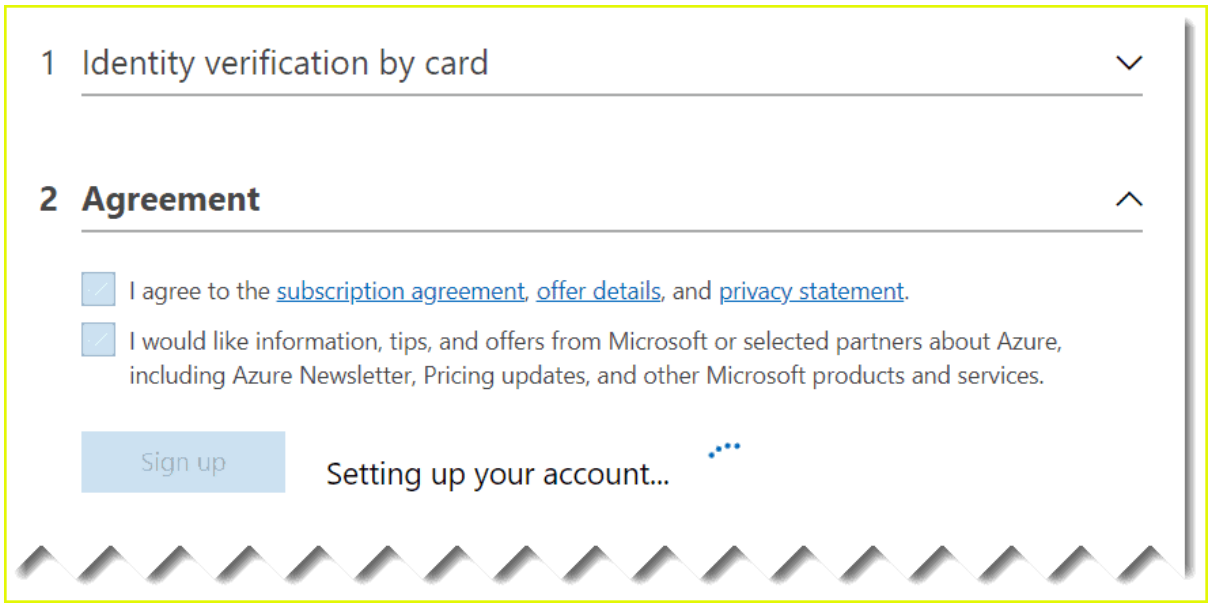
from your account.



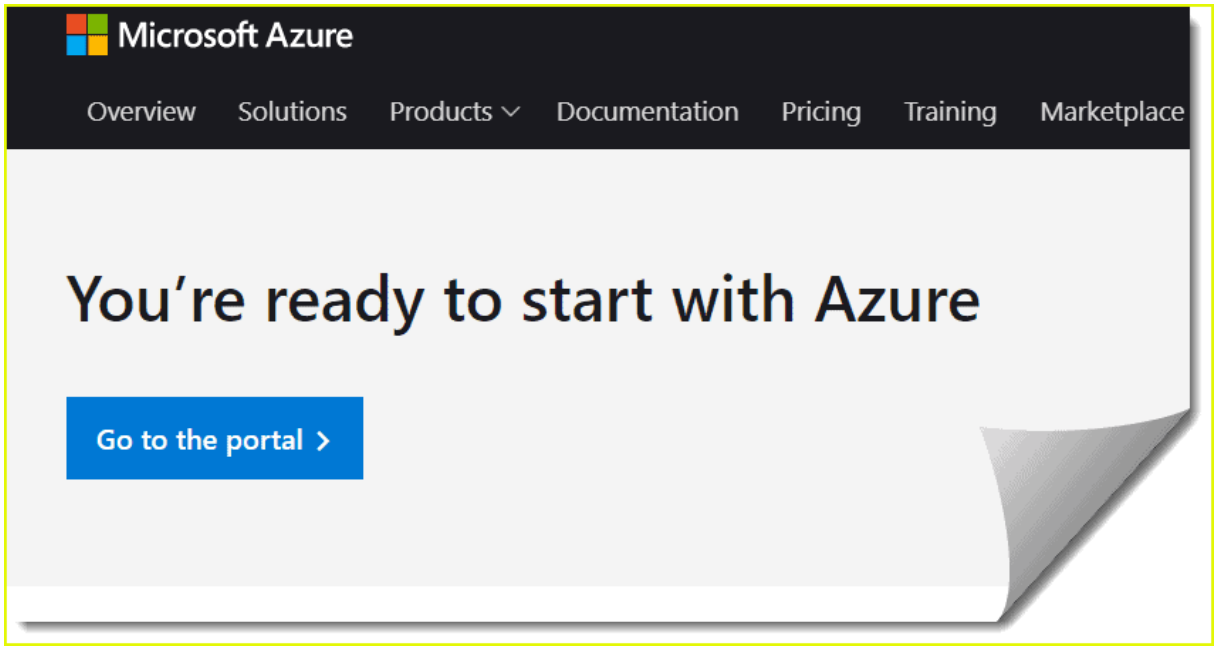
Then check the Agreement checkbox like below :



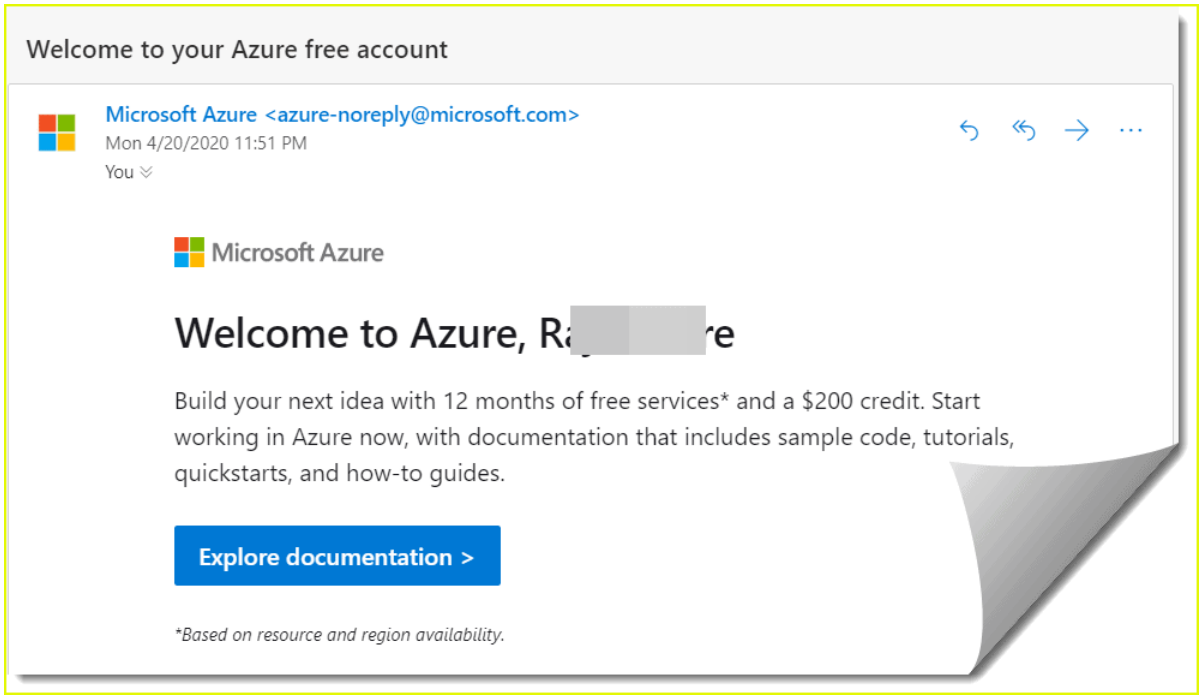
It will take some time and setup your account like the below :



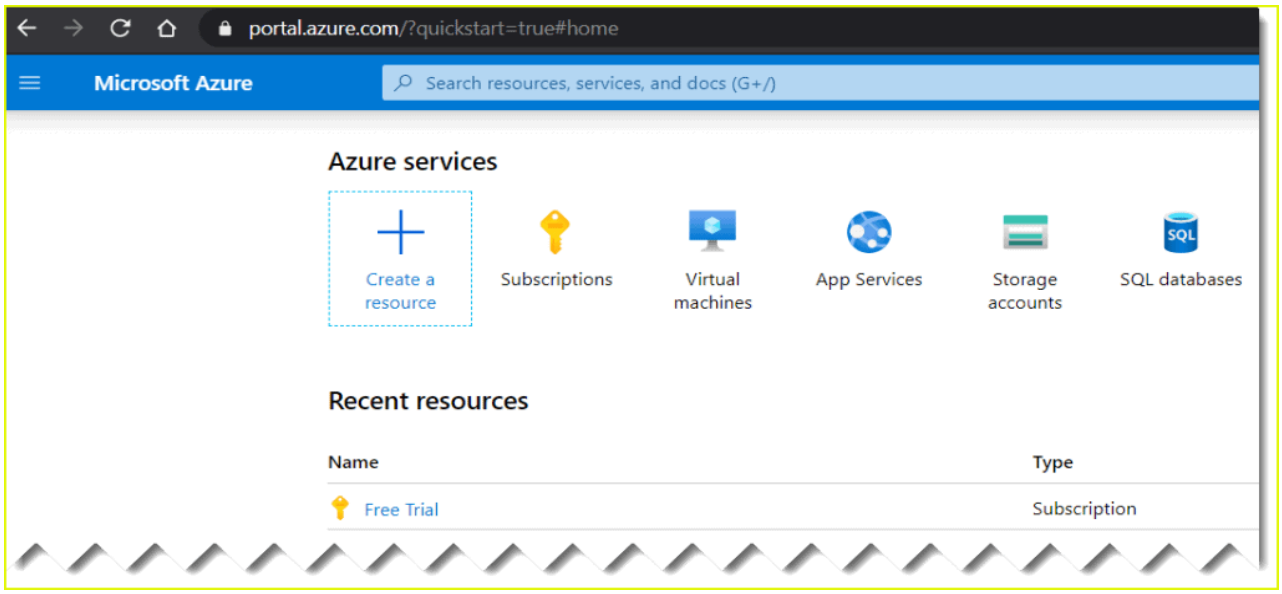
After some time, you can see Our Azure portal is ready and we can access the Azure portal.



Also, you will receive an email to the email id which you have provided while setting up free azure account.



Then you can go to **Portal.Azure.com** and you can see the Azure portal.



This way we can **sign up for a free Azure subscription** and can access Microsoft Azure for 12 months.

7.IMPLEMENTATION

CHAPTER-7

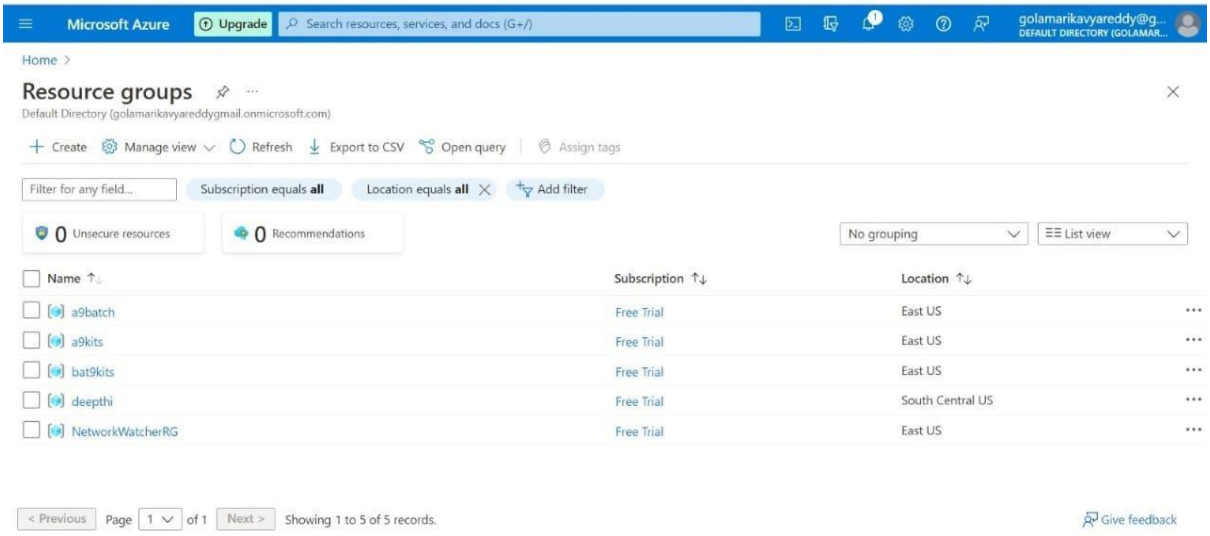
IMPLEMENTATION

A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Generally, add resources that share the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.

7.1.1 Create resource groups

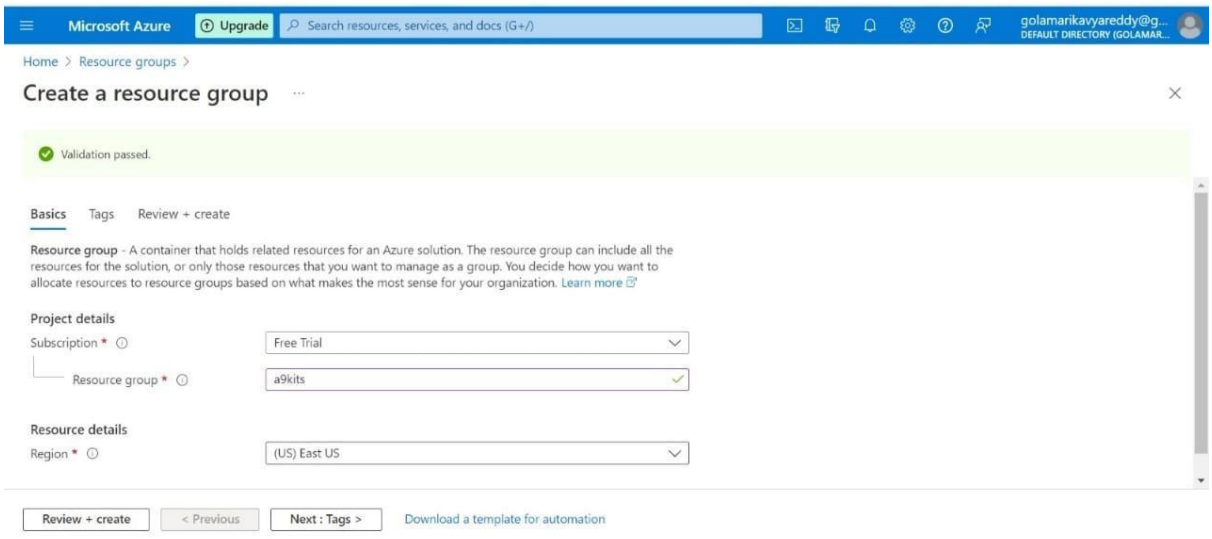
1. Sign in to the Azure portal.

2. Select **Resource groups**



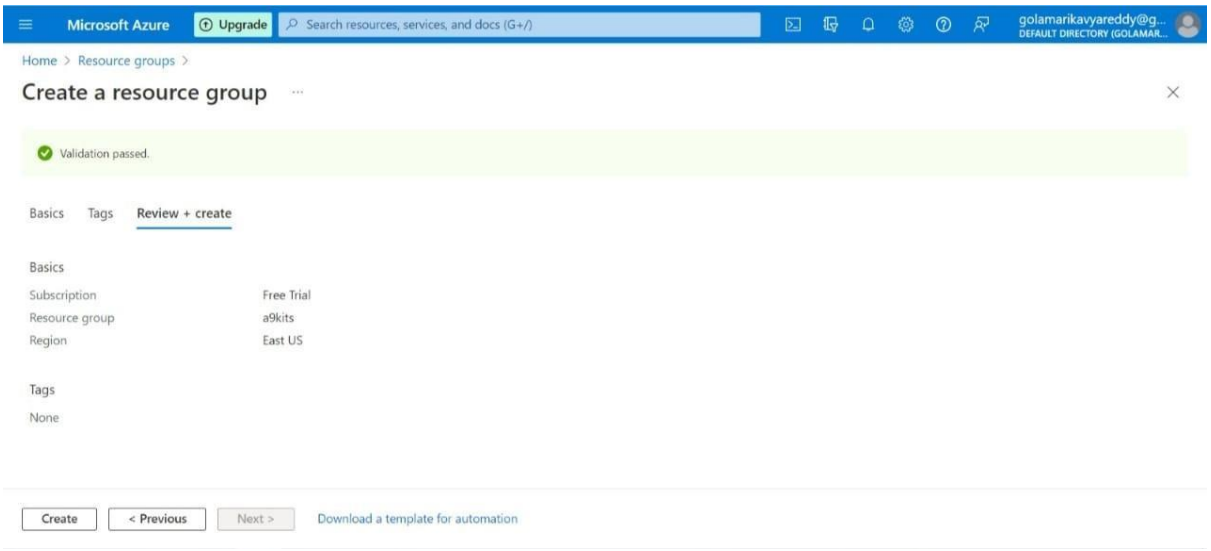
3. Select **Add**.
4. Enter the following values

   - **Subscription**: Select your Azure subscription.
   - **Resource group**: Enter a new resource group name.
   - **Region**: Select an Azure location, such as **Central US**.



5. Select **Review + Create.**

6. Select **Create**. It takes a few seconds to create a resource group.



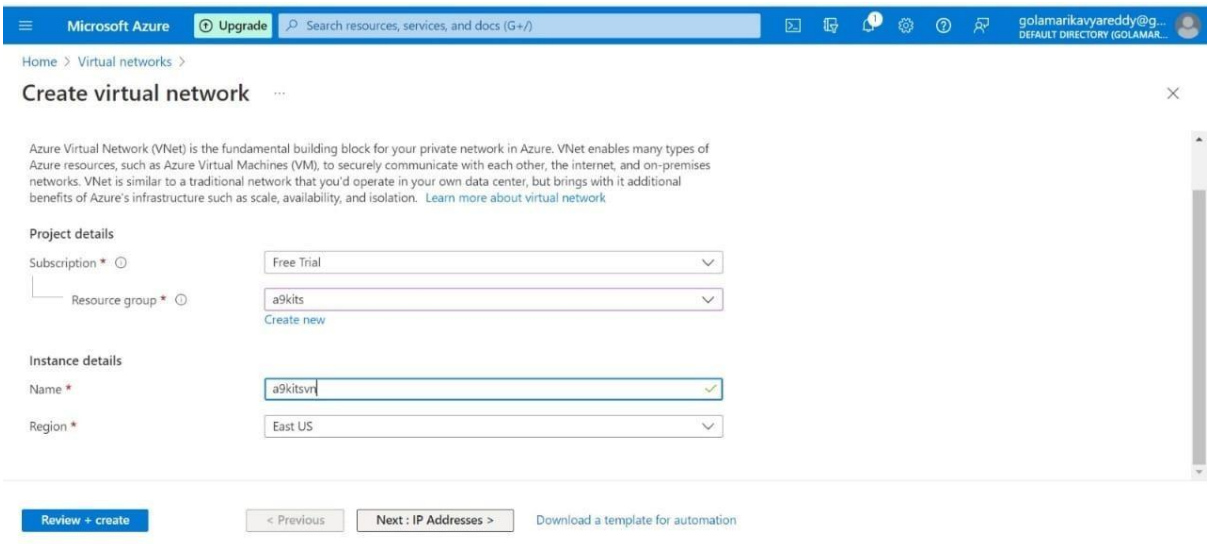
7. Select **Refresh** from the top menu to refresh the resource group list, and then select the newly created resource group to open it. Or select **Notification**(the bell icon) from the top, and then select **Go to resource group** to open the newly created resource group.

7.2 VIRTUAL NETWORK

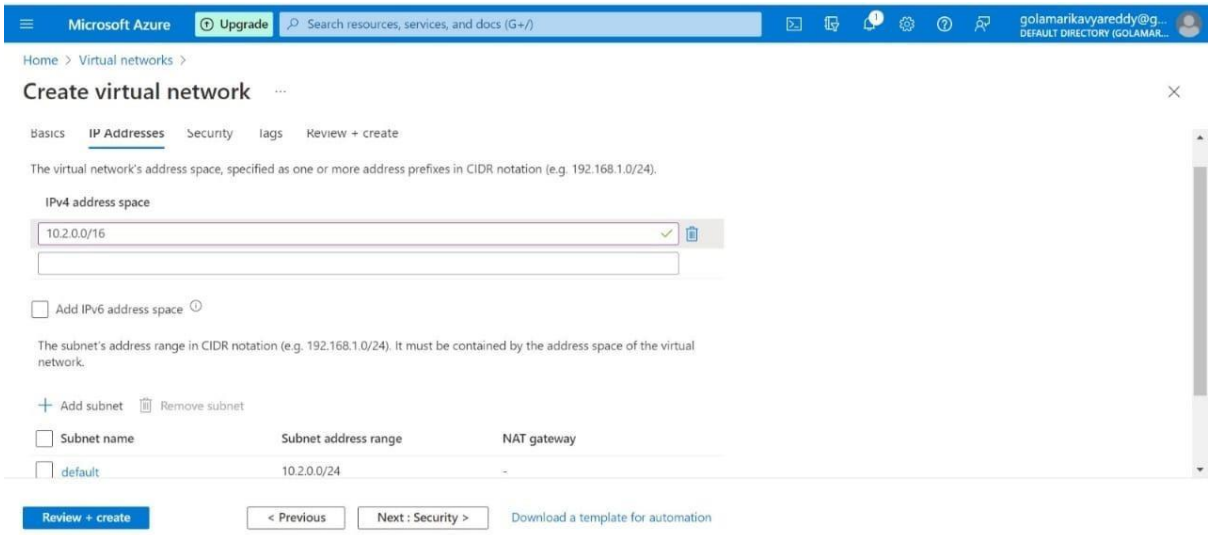
Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

7.2.1 Create a virtual network

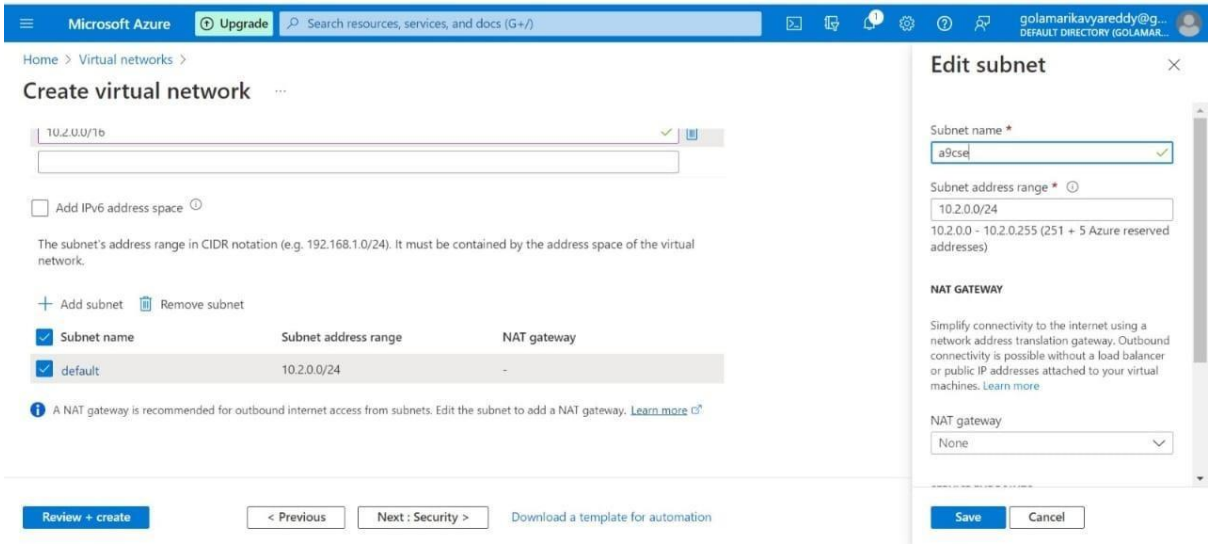
1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.



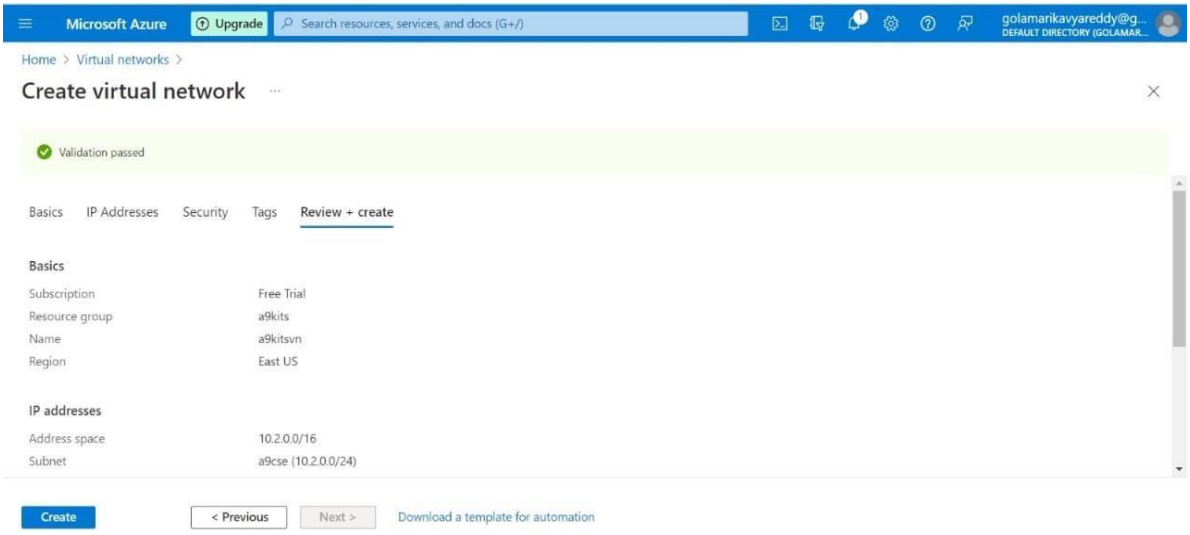
4. In **Create virtual network**, enter or select this information in the **Basics** tab:
5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom of the page and enter in the following information then select **Add**:



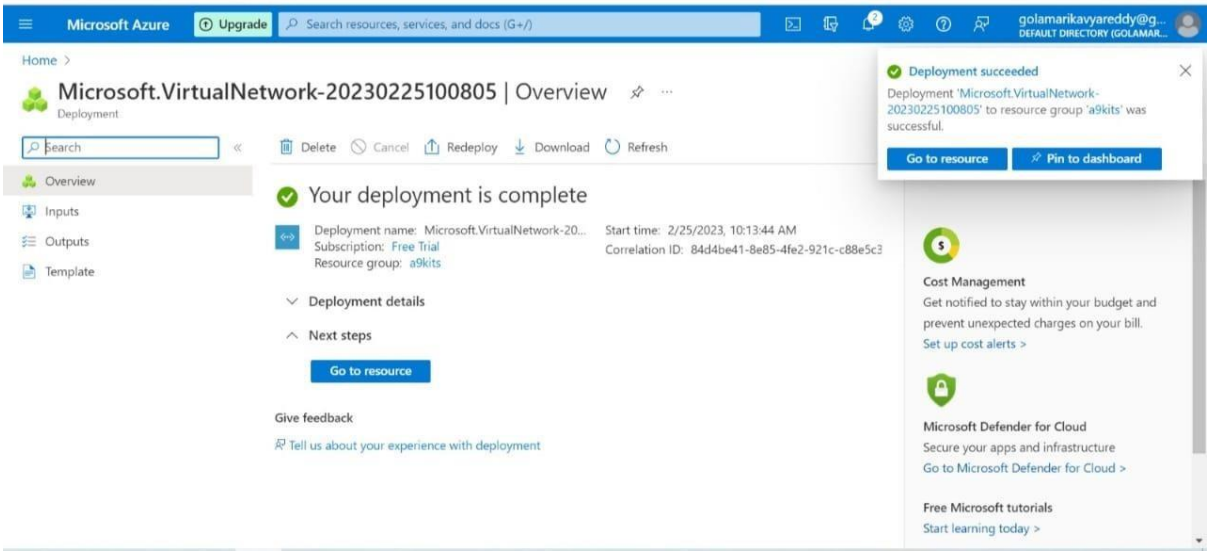
6. Select the **Security** tab, or select the **Next: Security** button at the bottom of the page.

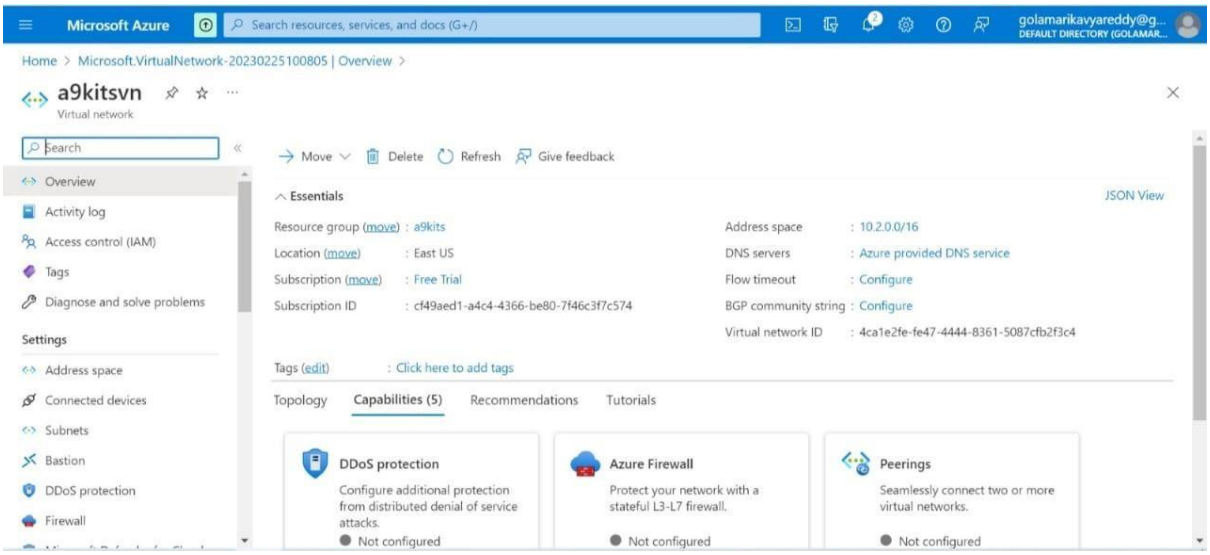


7. Select the **Review + create** tab or select the **Review + create** button.



8. Select **Create**.




Microsoft Azure
Search resources, services, and docs (G+/)
golamarikavyareddy@g...
DEFAULT DIRECTORY (GOLAMAR...
Home > Microsoft.VirtualNetwork-20230225100805 | Overview >
a9kitsvn
Virtual network
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move) : a9kits
Location (move) : East US
Subscription (move) : Free Trial
Subscription ID : cf49aed1-a4c4-4366-be80-7f46c3f7c574
Address space : 10.2.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : 4ca1e2fe-fe47-4444-8361-5087cfb2f3c4
Tags (edit) : Click here to add tags
Topology
Capabilities (5)
Recommendations
Tutorials
DDoS protection
Configure additional protection from distributed denial of service attacks.
Not configured
Azure Firewall
Protect your network with a stateful L3-L7 firewall.
Not configured
Peerings
Seamlessly connect two or more virtual networks.
Not configured

7.3 VIRTUAL MACHINE

Azure virtual machines (VMs) can be created through the Azure portal. This method provides a browser-based user interface to create VMs and their associated resources. This quickstart shows you how to use the Azure portal to deploy a virtual machine (VM) in Azure that runs Windows Server 2019. To see your VM in action, you then RDP to the VM and install the IIS web server.

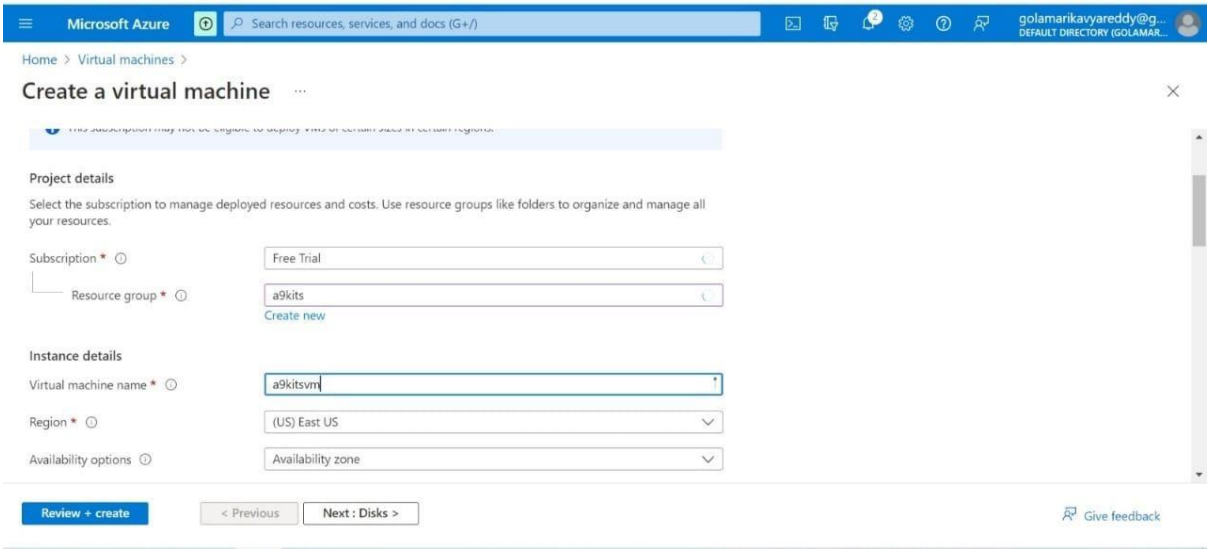
If you don't have an Azure subscription, create a free account before you begin.

7.3.1 Sign in to Azure

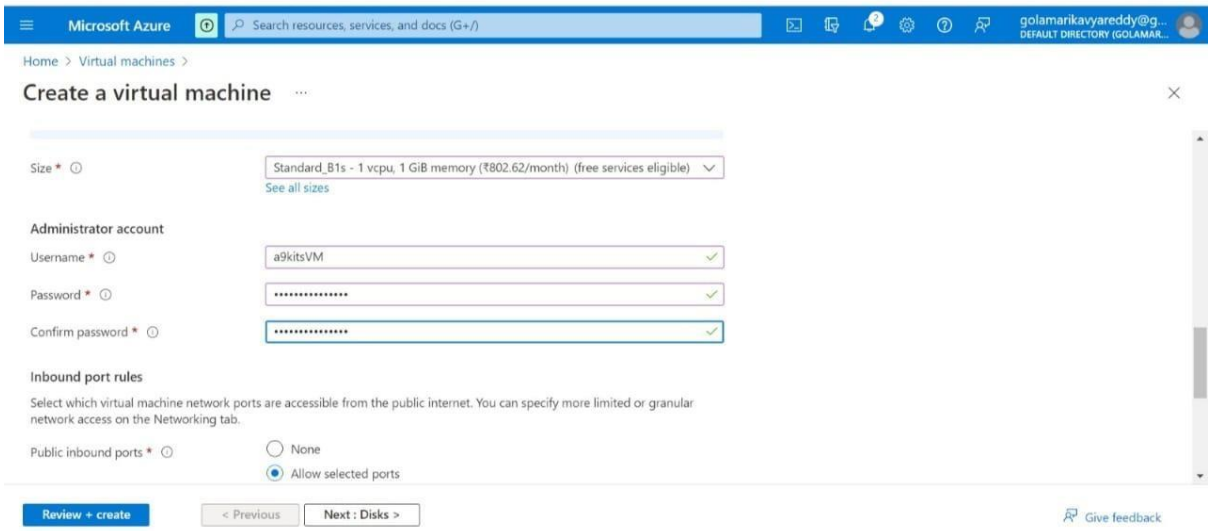
Sign in to the Azure portal at https://portal.azure.com.

7.3.2 Create virtual machine

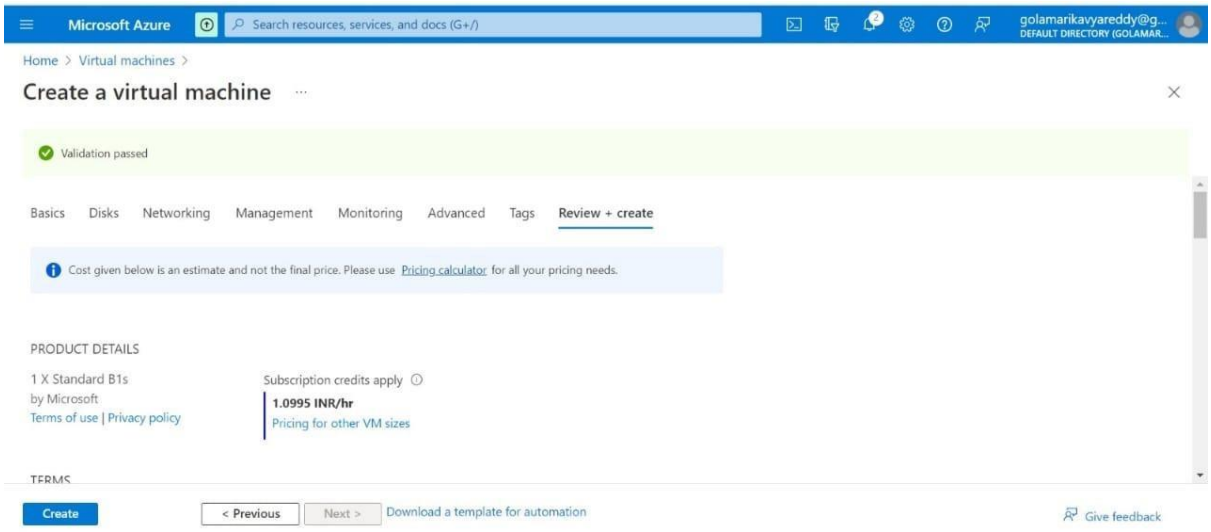
1. Enter *virtual machines* in the search.Under **Services**, select **Virtual machines**.
2. In the **Virtual machines** page, select **Create** and then **Azure virtual machine**. The **Create a virtual machine** page opens.
3. Under **Instance details**, enter *a9kits* for the **Virtual machine name** and choose *Windows Server 2019 Datacenter - Gen 2* for the **Image**. Leave the other defaults.



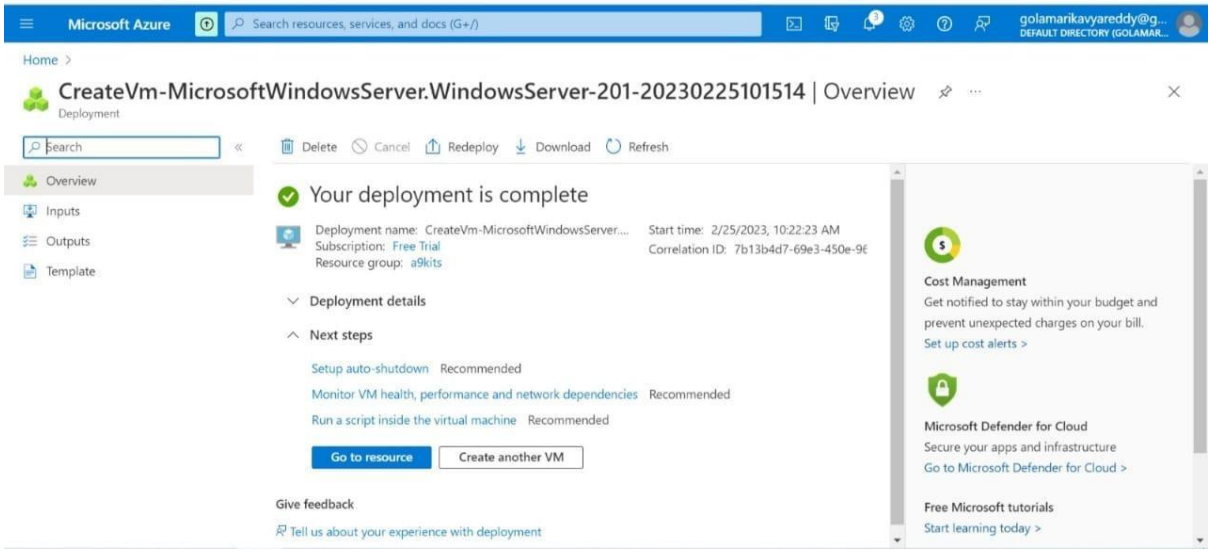
4. Under **Administrator account**, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long and meet the defined complexity requirements.



5. Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP (80)** from the drop-down.
6. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.
7. After validation runs, select the **Create** button at the bottom of the page.



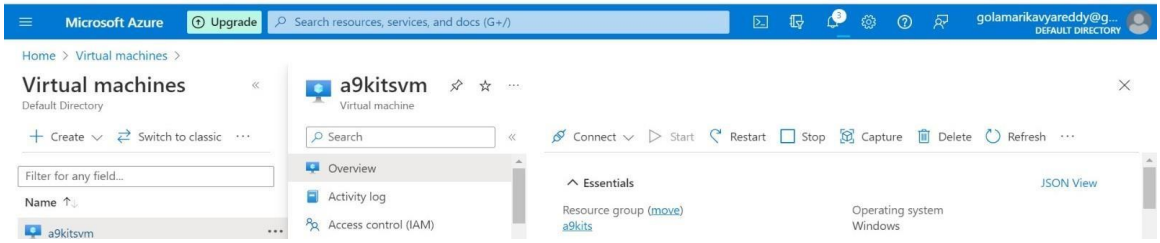
8. After deployment is complete, select **Go to resource**.



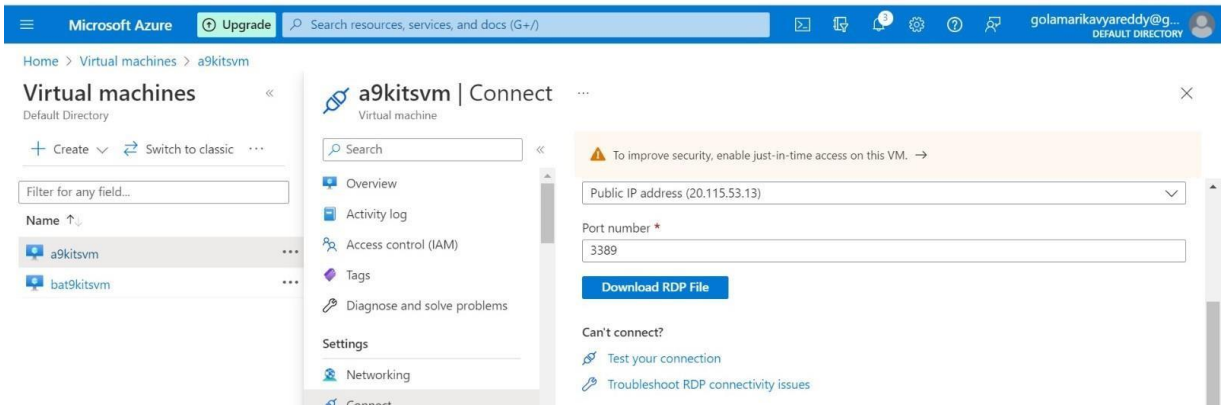
7.3.3 Connect to virtual machine

Create a remote desktop connection to the virtual machine. These directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store.

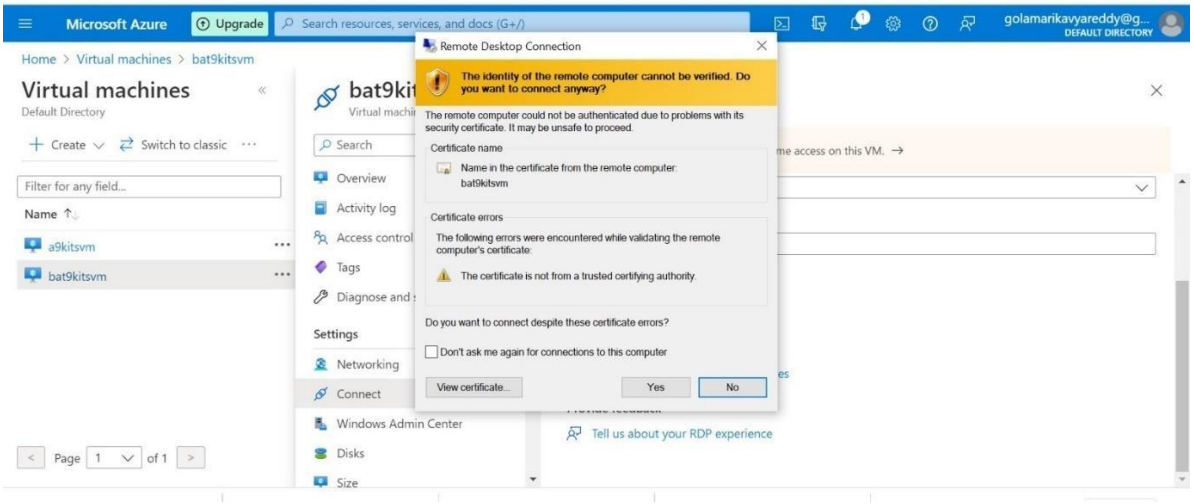
1. On the overview page for your virtual machine, select the **Connect** > **RDp.**



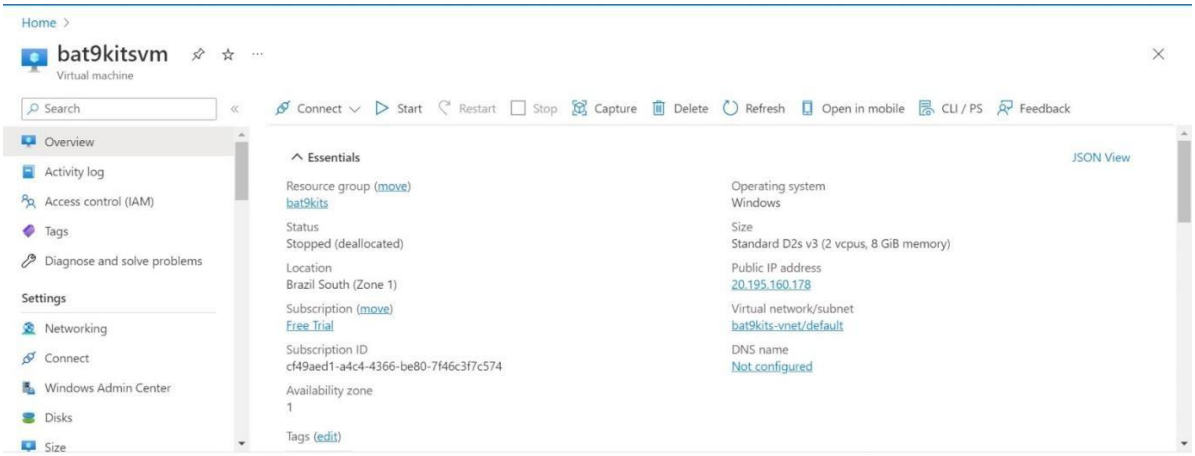
2. In the **Connect with RDP** tab, keep the default options to connect by IP address, over port 3389, and click **Download RDP file**.



3. Open the downloaded RDP file and click **Connect** when prompted.



4. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as **localhost***username*, enter the password you created for the virtual machine, and then click **OK**.



8.TESTING AND VALIDATION

CHAPTER-8

TESTING AND VALIDATION

8.1 Log Analytics Workspace

This article shows you how to create a Log Analytics workspace. When you collect logs and data, the information is stored in a workspace. A workspace has a unique workspace ID and resource ID. The workspace name must be unique for a given resource group. After you've created a workspace, configure data sources and solutions to store their data there.

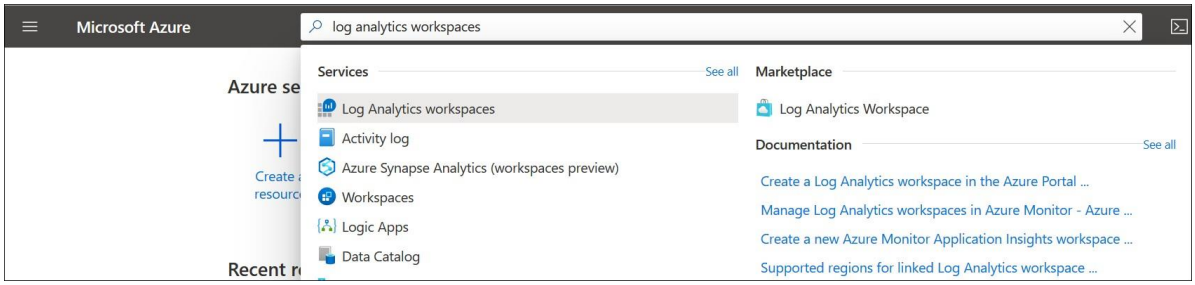
You need a Log Analytics workspace if you collect data from:

- Azure resources in your subscription.
- On-premises computers monitored by System Center Operations Manager.
- Device collections from Configuration Manager.
- Diagnostics or log data from Azure Storage.

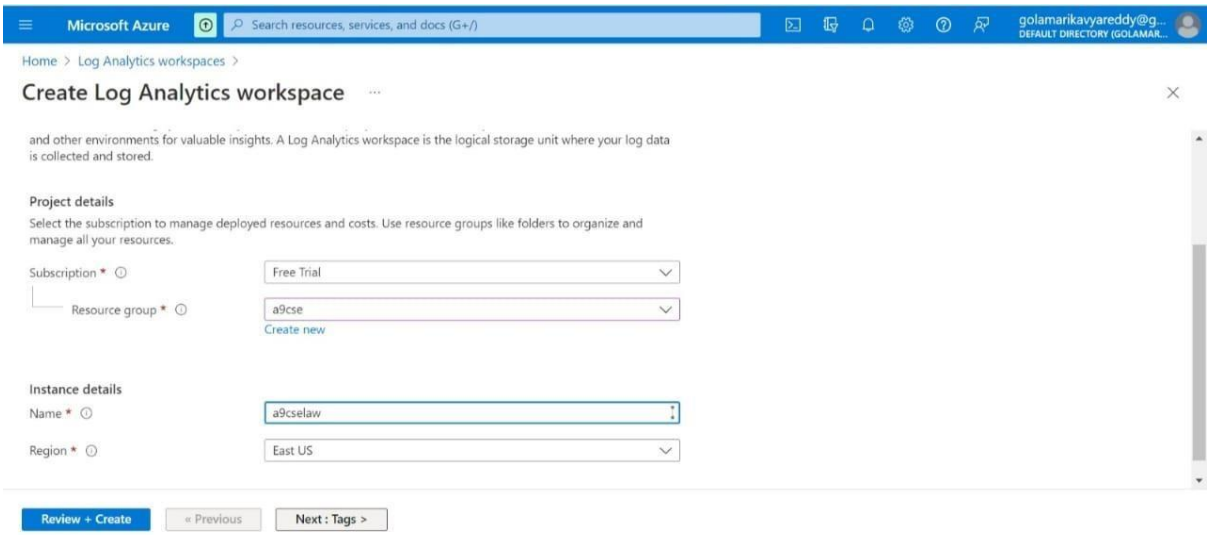
8.1.1 Create a workspace

Use the **Log Analytics workspaces** menu to create a workspace.

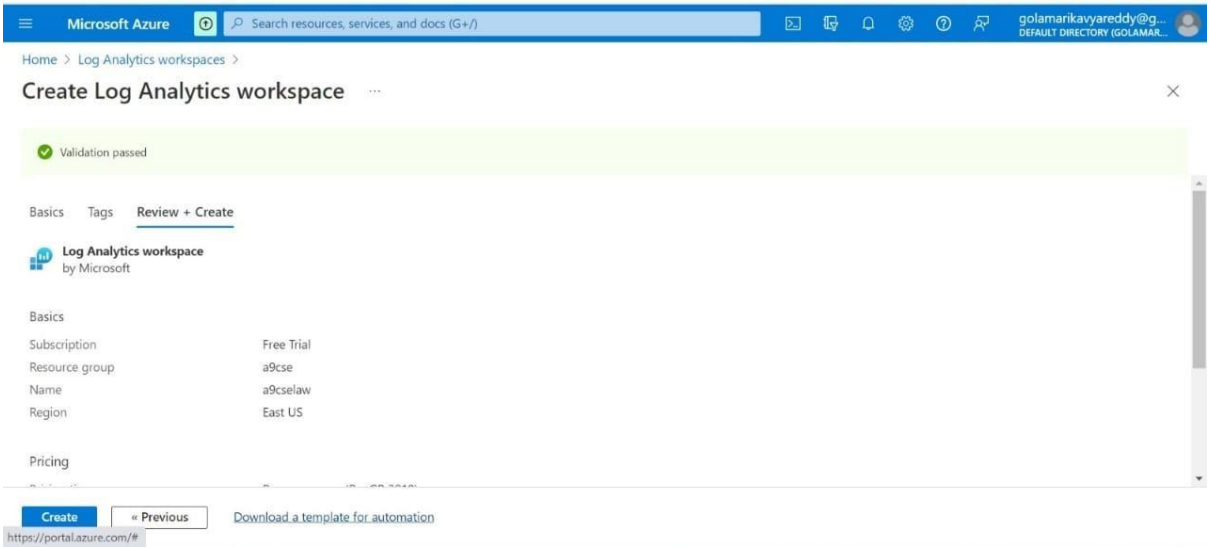
1. In the Azure portal, enter **Log Analytics** in the search box. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.



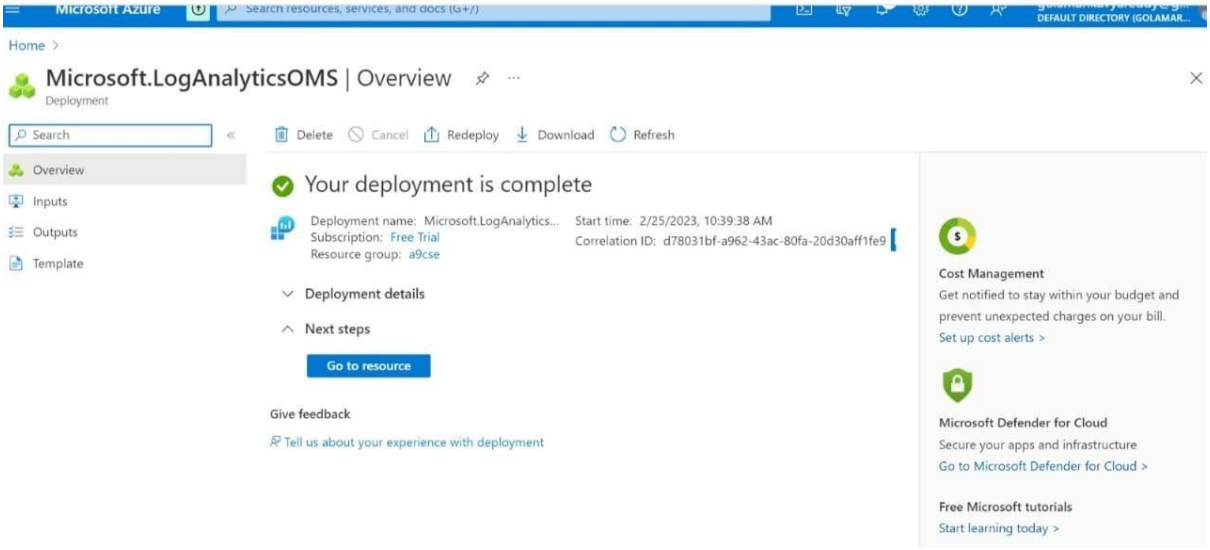
2. Select **Add**.
3. Use an existing **Resource Group** or create a new one.
4. Provide a name for the new **Log Analytics workspace**, such as *DefaultLAWorkspace*. This name must be unique per resource group.



5. Select an available **Region**. For more information, see which regions Log Analytics is available in. Search for Azure Monitor in the **Search for a product** box.



6. Select **Review + Create** to review the settings. Then select **Create** to create the workspace. A default pricing tier of pay-as-you-go is applied. No charges will be incurred until you start collecting enough data. For more information about other pricing tiers, see Log Analytics pricing details.



8.2 Installation of Log Analytics Agent

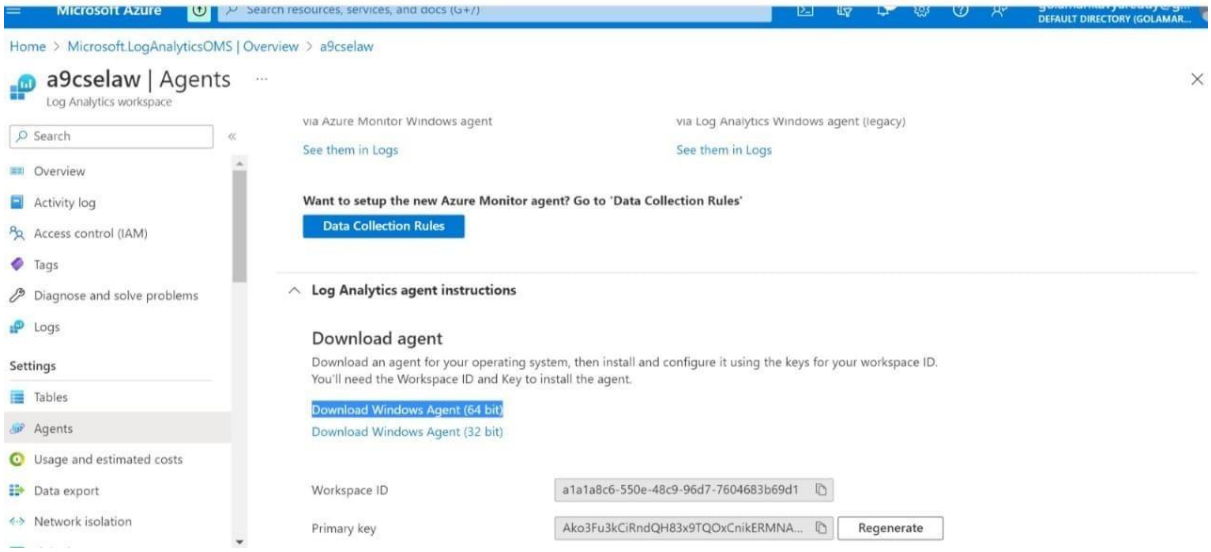
This article provides information on how to install the Log Analytics agent on Windows computers by using the following methods:

- Manual installation using the setup wizard or command line.
- Azure Automation Desired State Configuration (DSC).

The installation methods described in this article are typically used for virtual machines on-premises or in other clouds.

8.2.1 Workspace ID and key

Regardless of the installation method used, you'll require the workspace ID and key for the Log Analytics workspace that the agent will connect to. Select the workspace from the **Log Analytics workspaces** menu in the Azure portal. Then in the **Settings** section, select **Agents**.

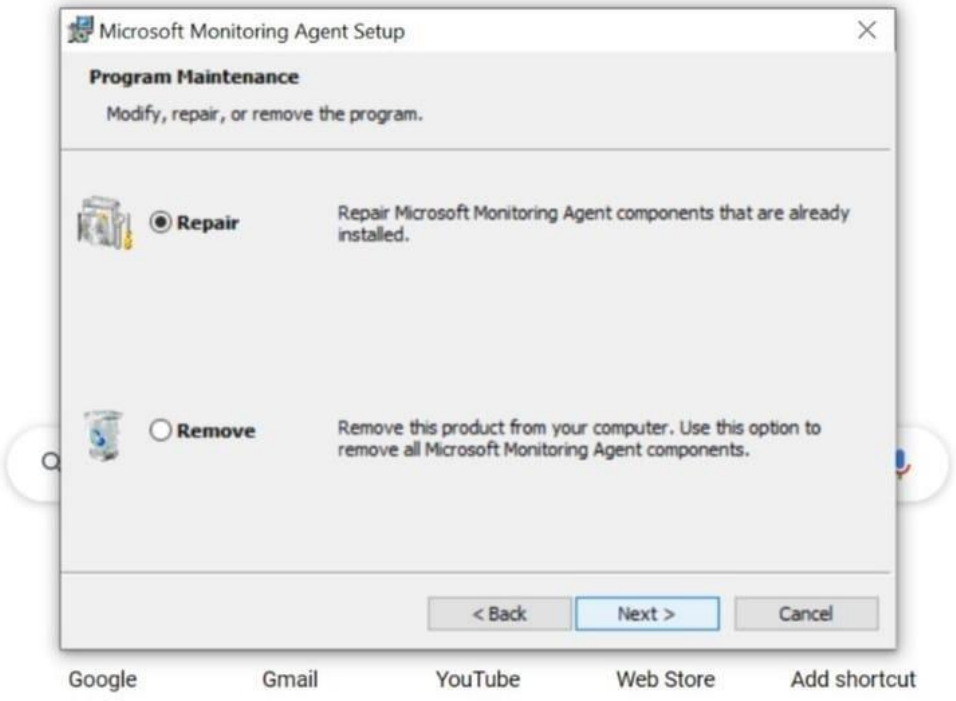


8.2.2 Install the agent

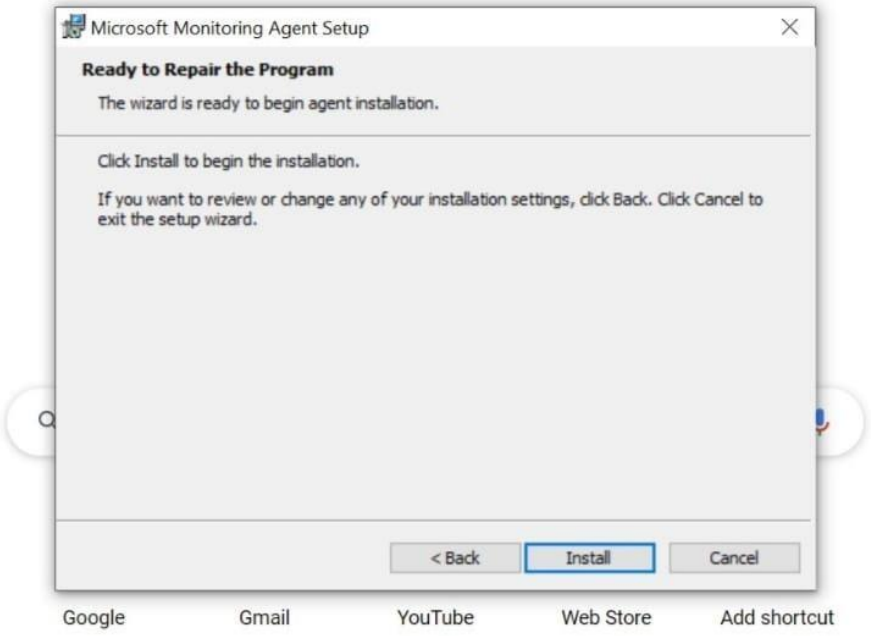
The following steps install and configure the Log Analytics agent in Azure and Azure Government cloud by using the setup wizard for the agent on your computer..

1. In your Log Analytics workspace, from the **Windows Servers** page you navigated to earlier, select the appropriate **Download Windows Agent** version to download depending on the processor architecture of the Windows operating system.

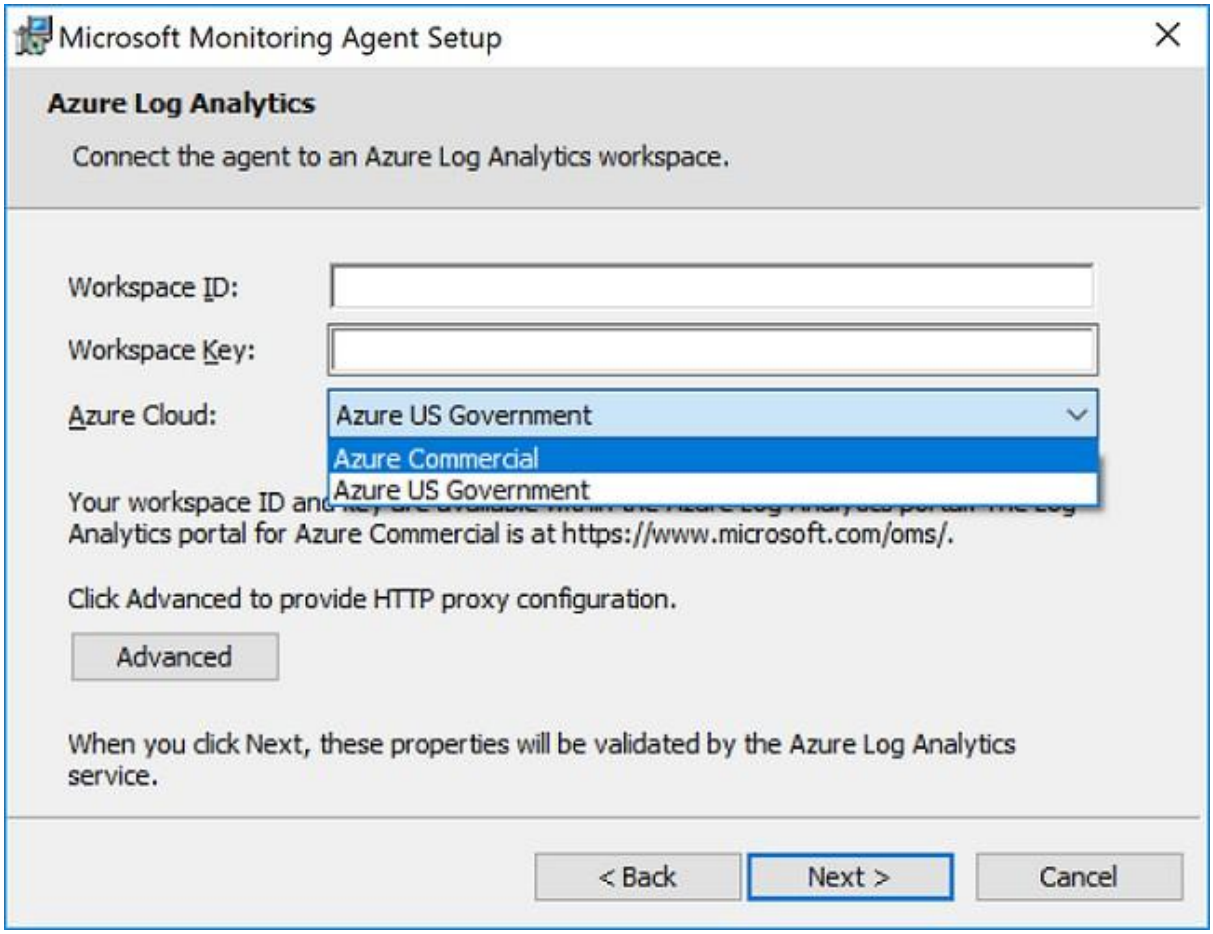
2. Run Setup to install the agent on your computer.
3. On the **Welcome** page, click **Next**.



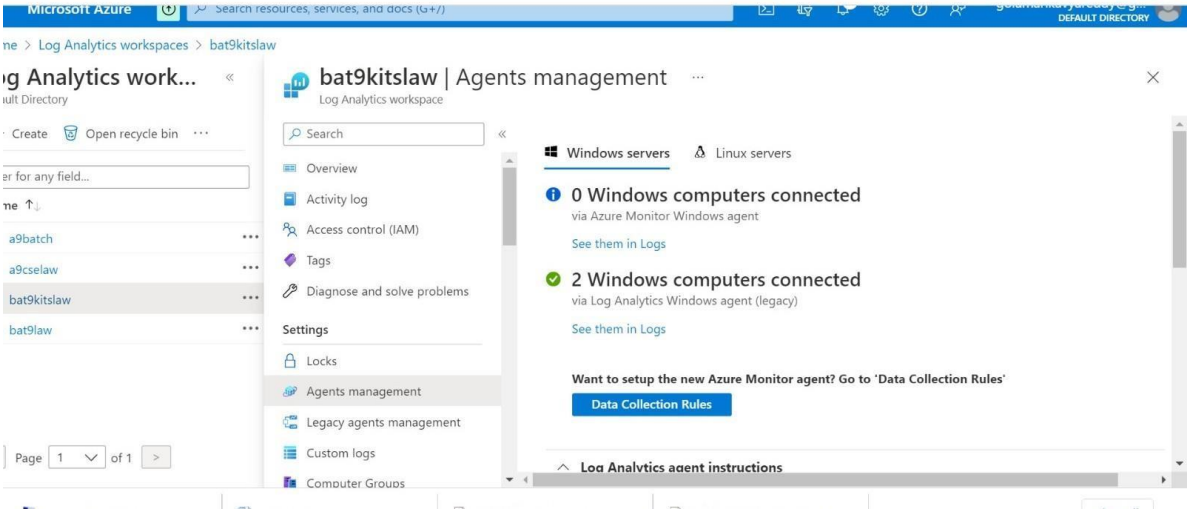
4. On the **Destination Folder** page, change or keep the default installation folder and then click **Next**.



5. On the **Agent Setup Options** page, choose to connect the agent to Azure Log Analytics and then click **Next**.
6. On the **Azure Log Analytics** page, perform the following:
    1. Paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied earlier. If the computer should report to a Log Analytics workspace in Azure Government cloud, select **Azure US Government** from the **Azure Cloud** drop-down list.
    2. If the computer needs to communicate through a proxy server to the Log Analytics service, click **Advanced** and provide the URL and port number of the proxy server. If your proxy server requires authentication, type the username and password to authenticate with the proxy server and then click **Next**.

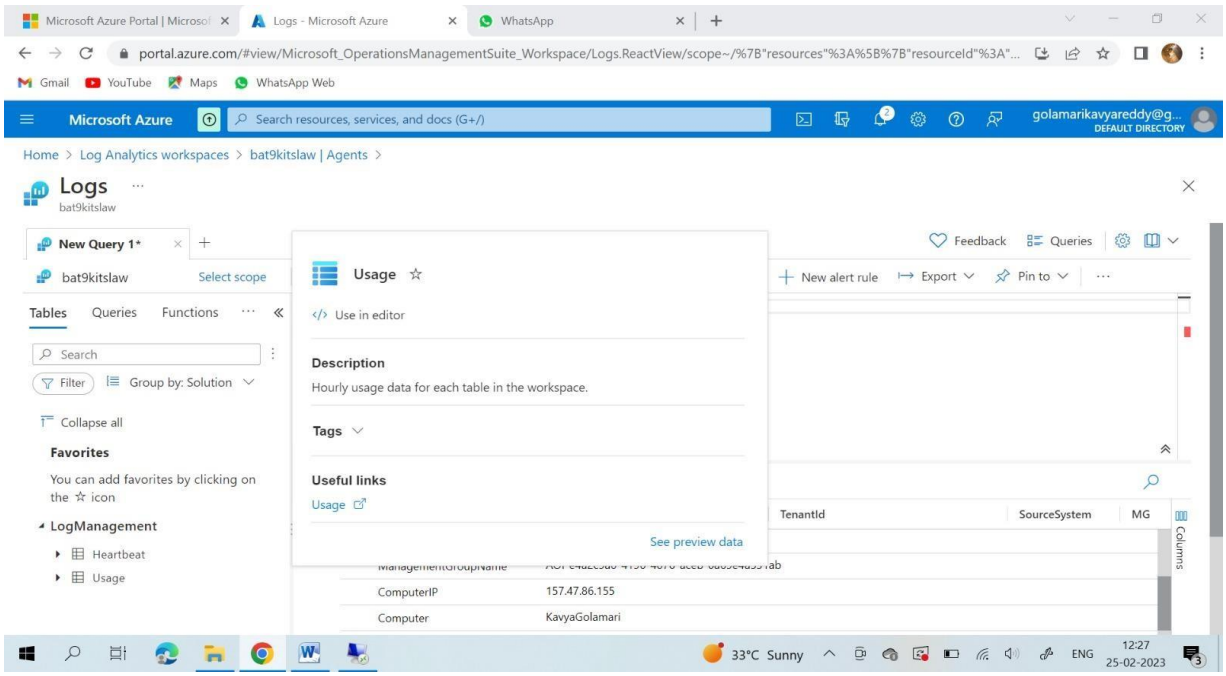


7. Click **Next** once you have completed providing the necessary configuration settings.



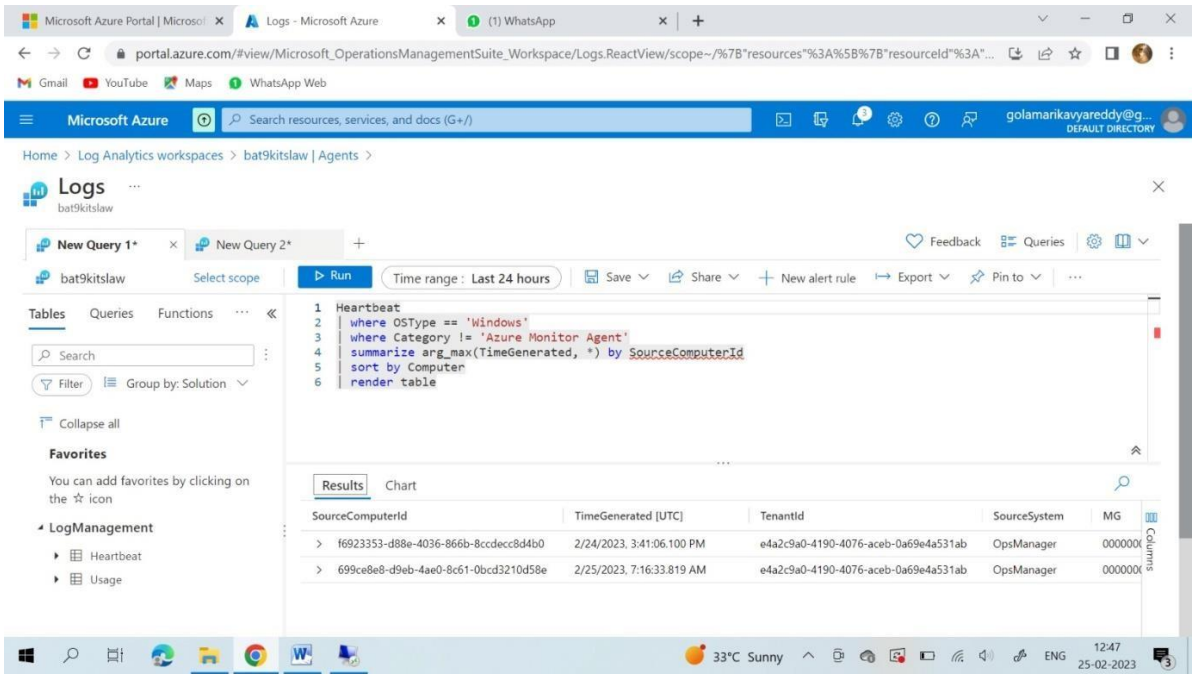
8.2.3 Agent Query:

1. Select the logs in query.



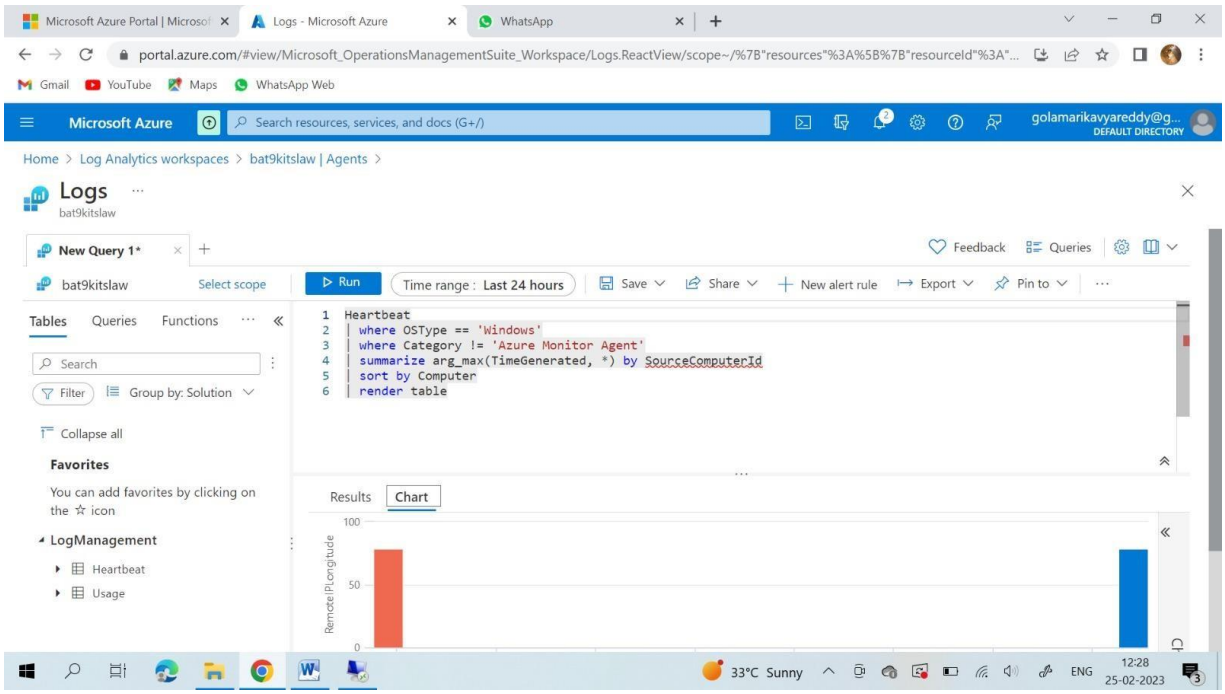
2. Go to heartbeat.

3. Select the new query in the logs.

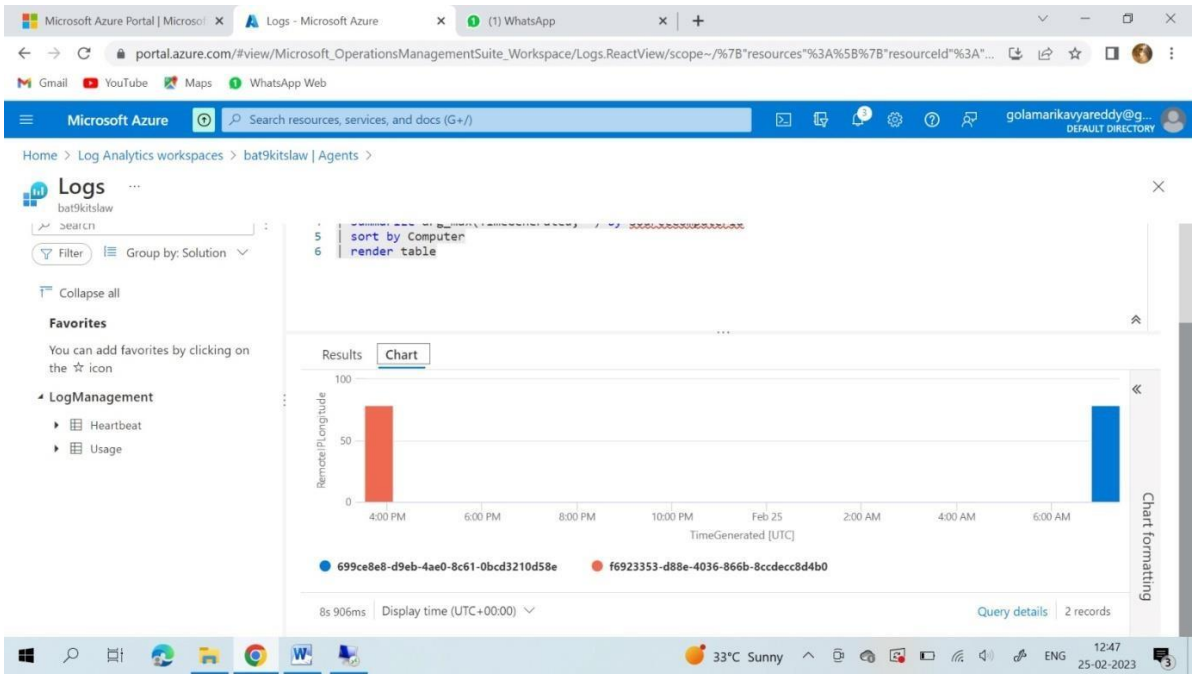


4. Query will be display in the right side then click run option.

5. Source computer id will be display in the results format.



6. Then output will be display in the chart format.



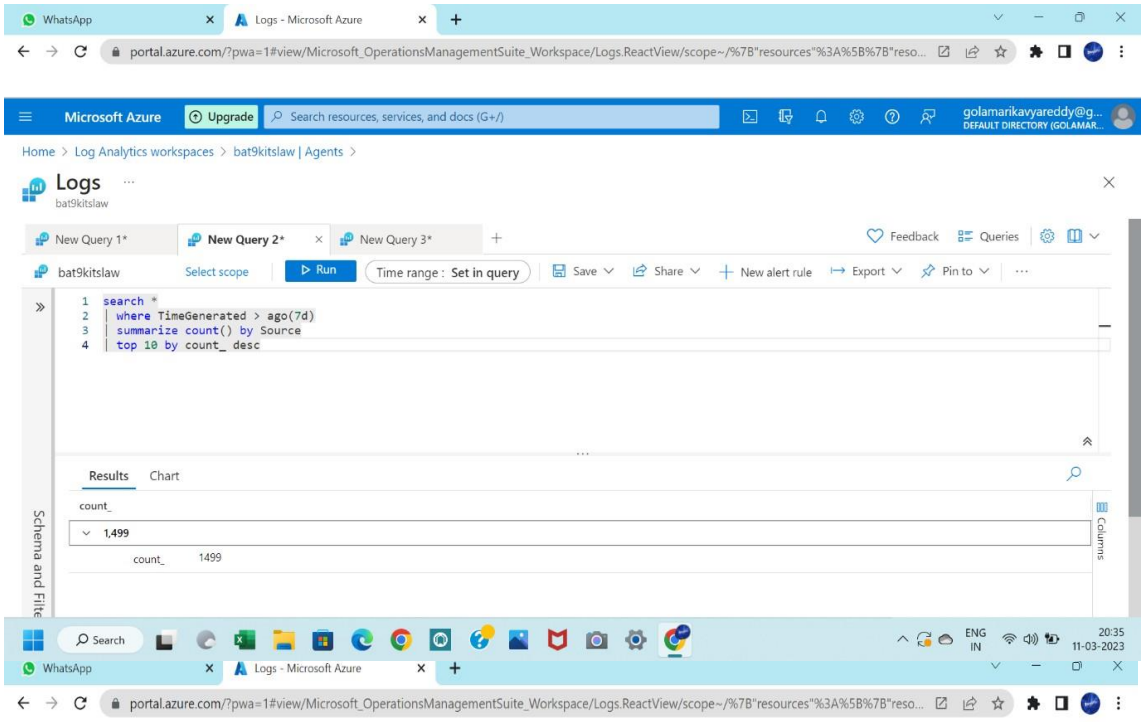
9.SCREENSHOTS

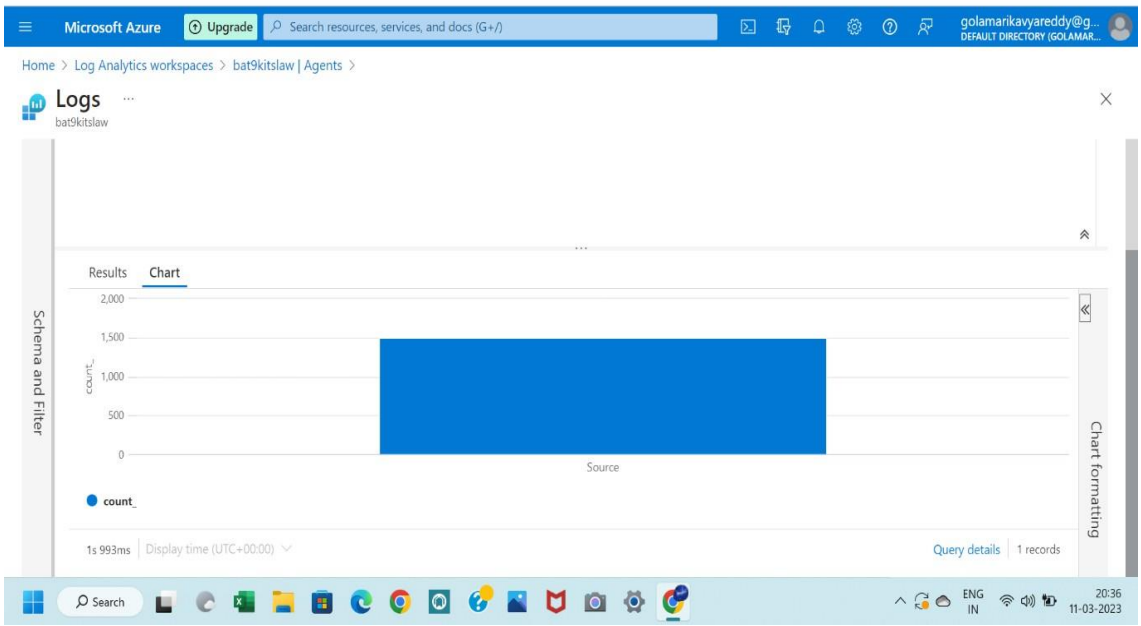
CHAPTER-9

SCREENSHOTS

KQL Query -1:

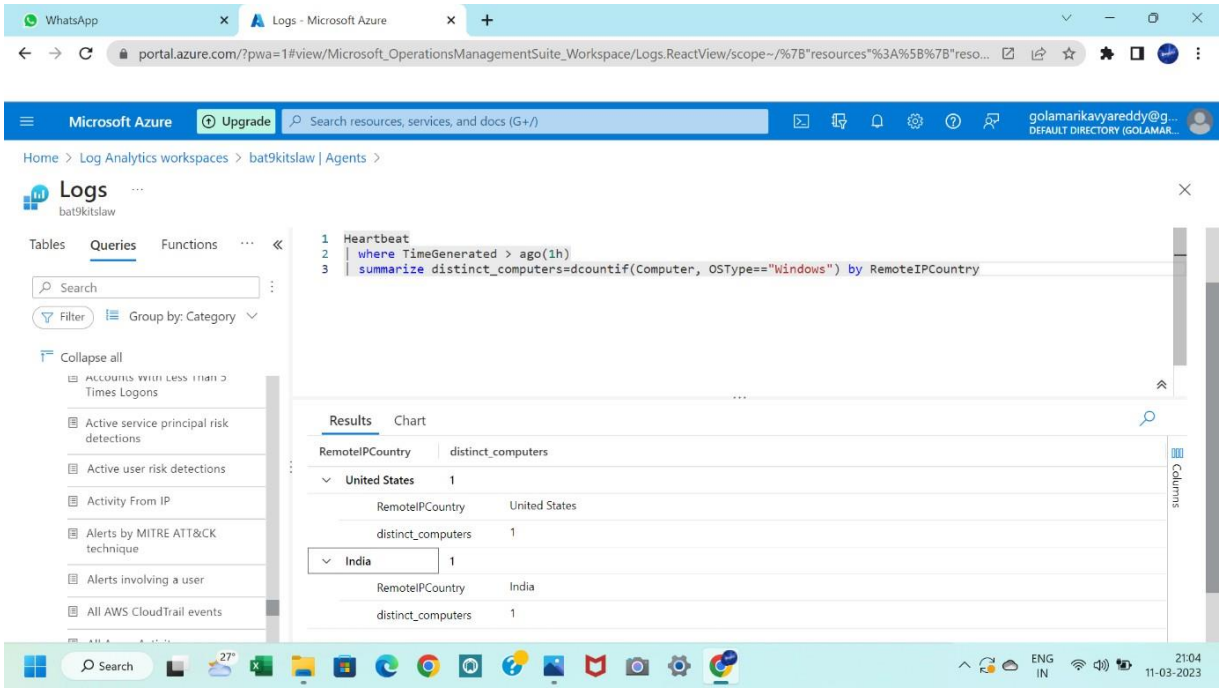
```
search*
| where TimeGenerated > ago(7d)
| summarize count() by Source
| top 10 by count_ desc
```

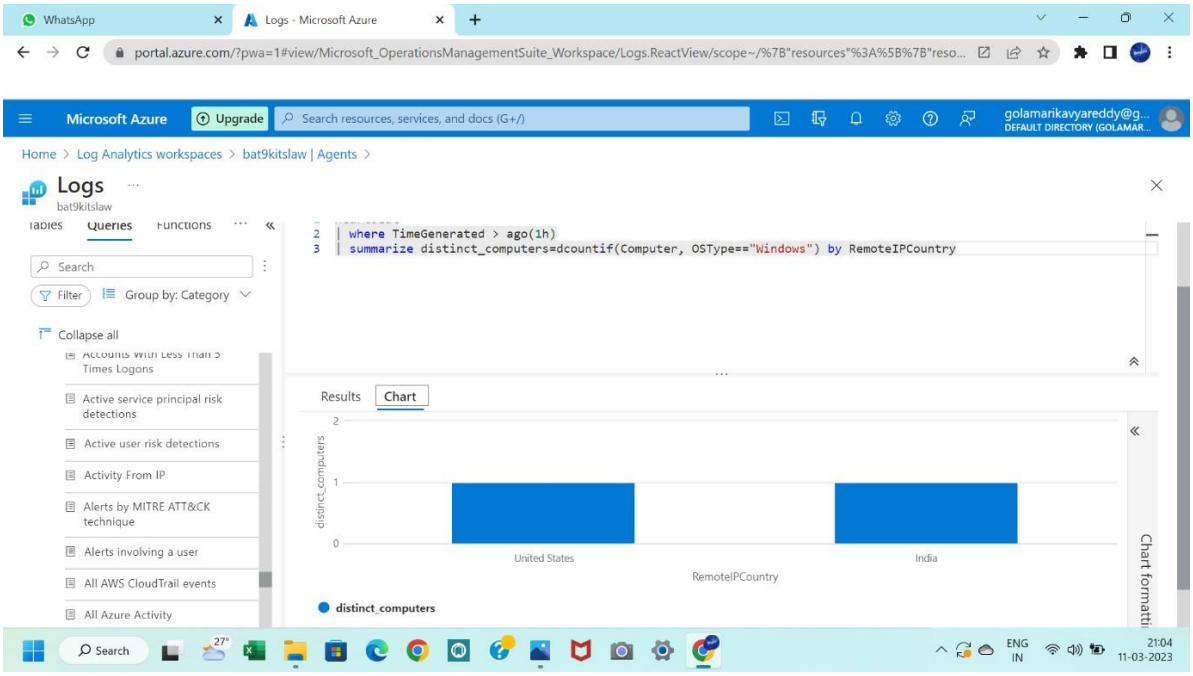




KQL Query -2:

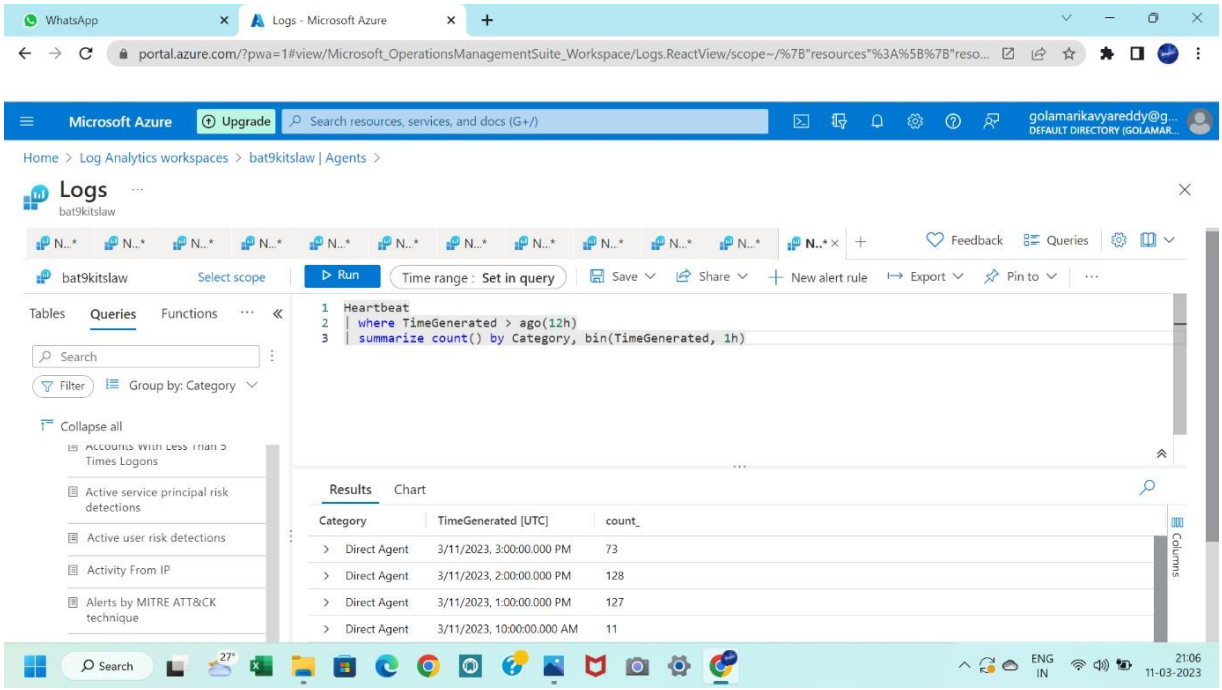
```
 Heartbeat
| where TimeGenerated > ago(1h)
| summarize distinct_computers=dcountif(Computer, OSType=="Windows")by
RemoteIPCountry
```

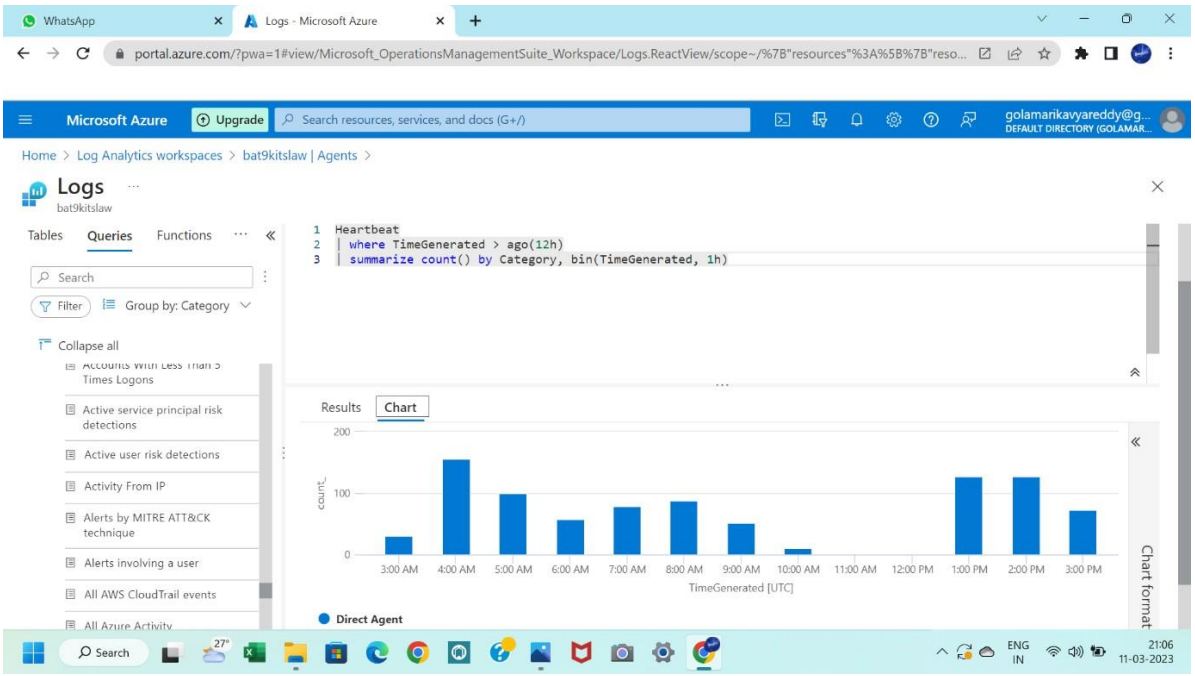




KQL Query -3:

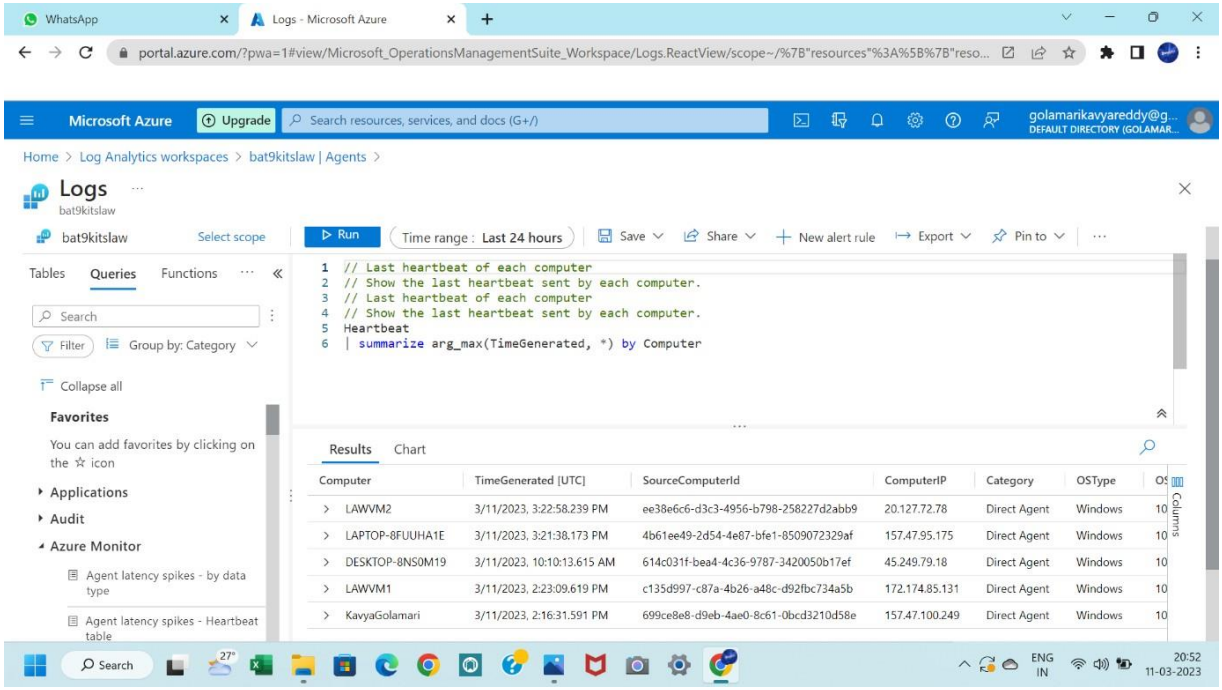
```
Heartbeat
| where TimeGenerated > ago(12h)
| summarize count() by Category,bin(TimeGenerated,1h)
```

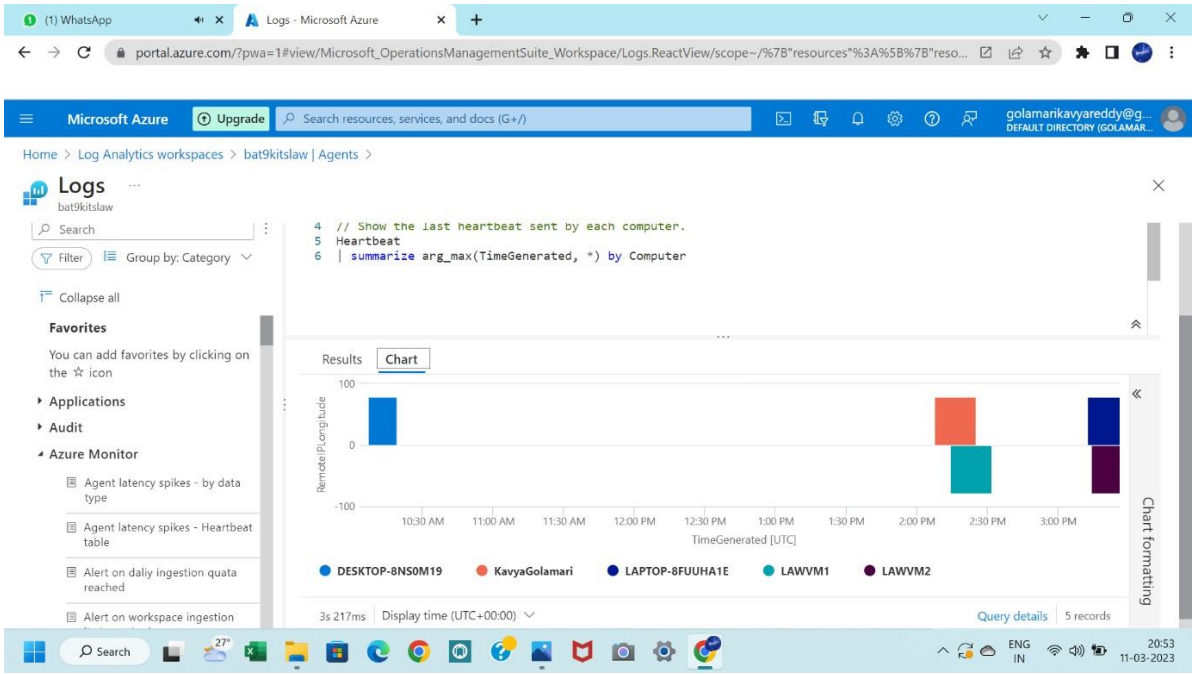




KQL Query -4:

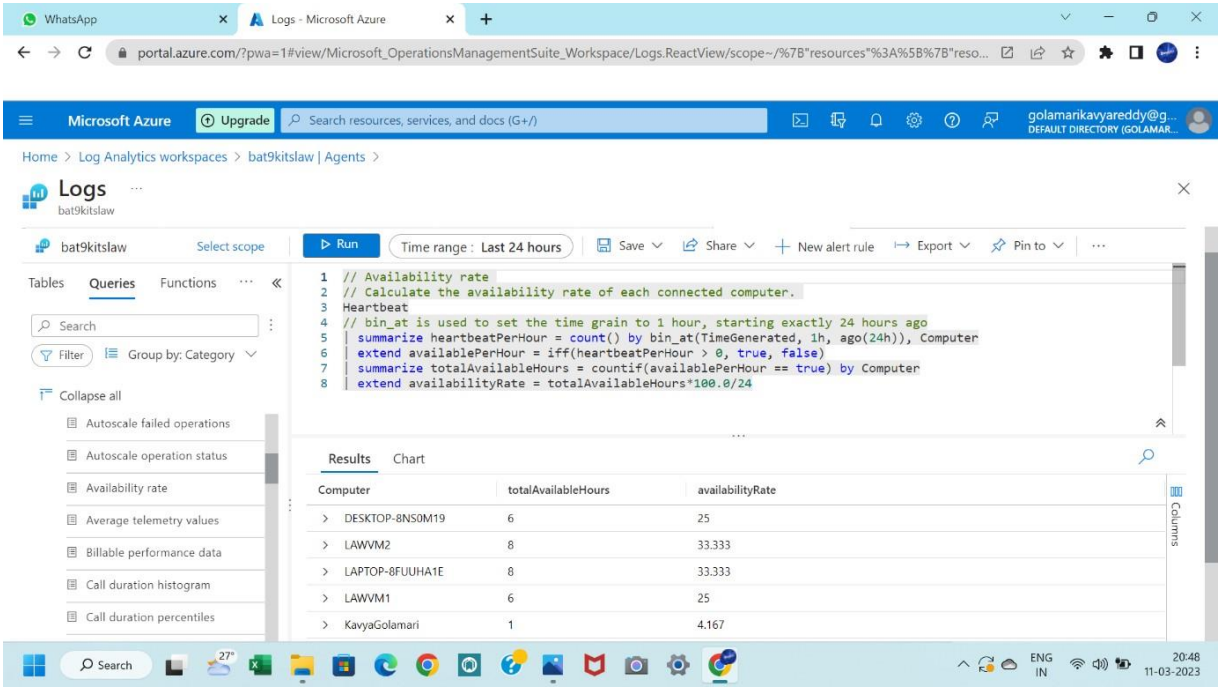
```
Heartbeat
| summarize arg_max(TimeGenerated, *) by Computer
```

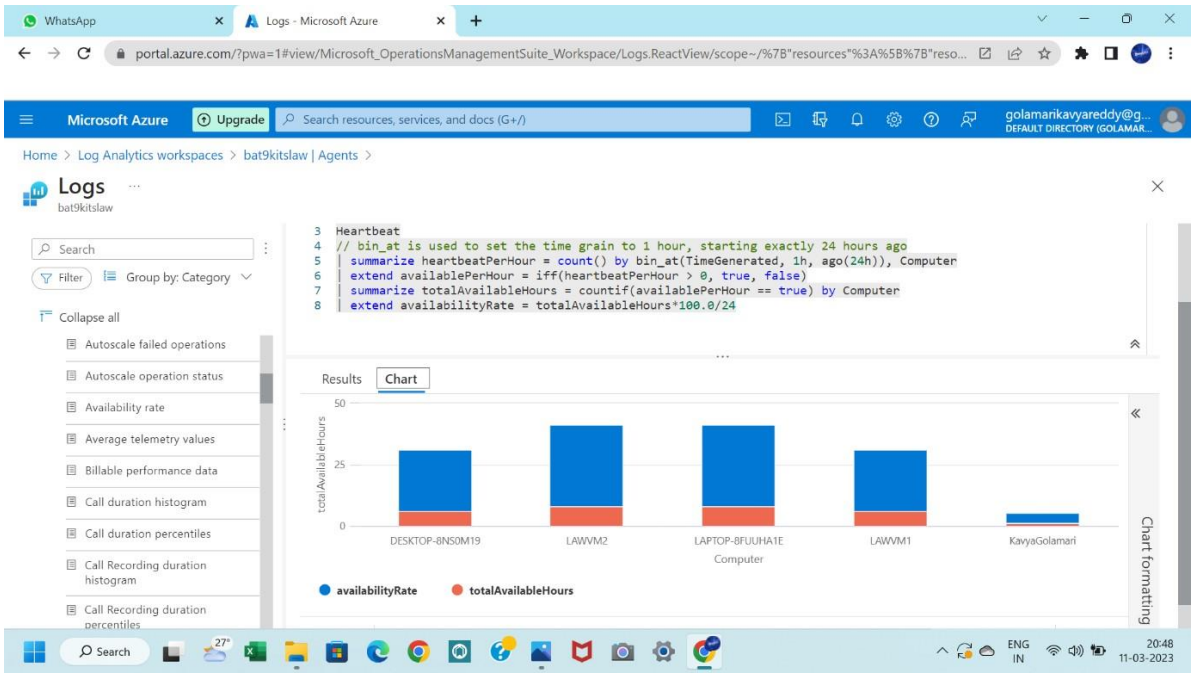




KQL Query -5:

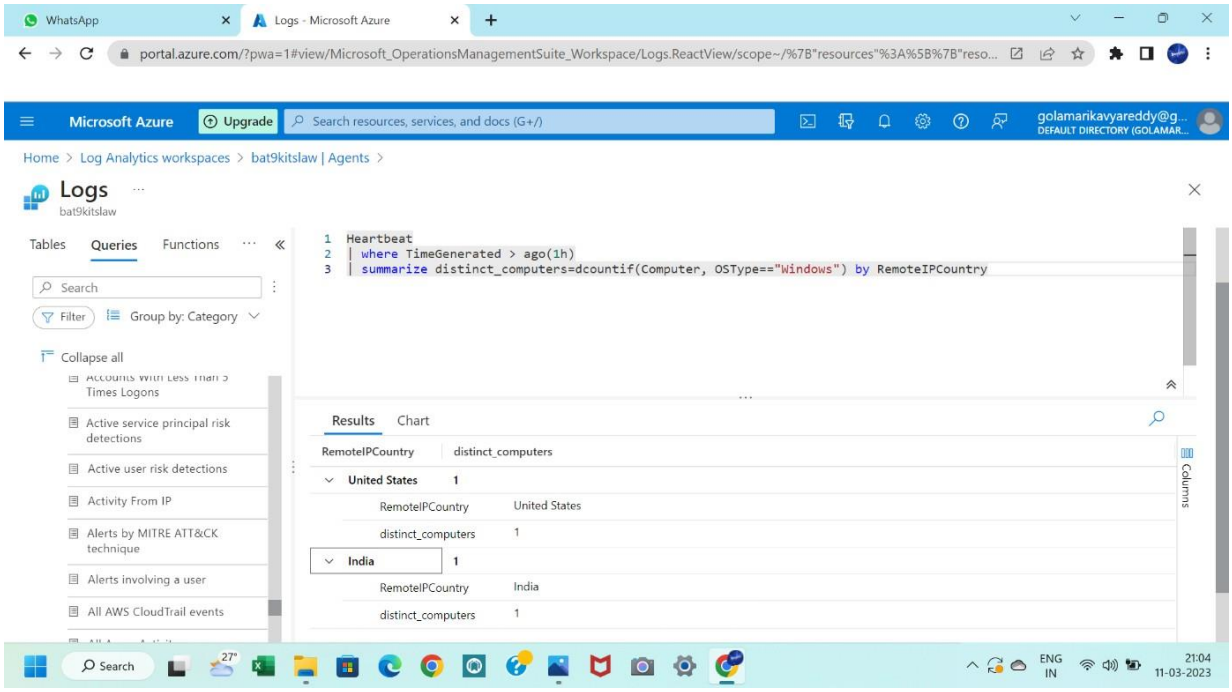
```
Hearbeat
| summarize heartbeatPerHour = count() by bin_at(TimeGenerated, 1h, ago(24h)), Computer
| extend availabilityRate = iff(heartbeatPerHour == true) by Computer
| summerize totalAvailableHours = countif(availableHour == true) by Computer
| extend availabilityRate = totalAvailableHours*100.0/24
```

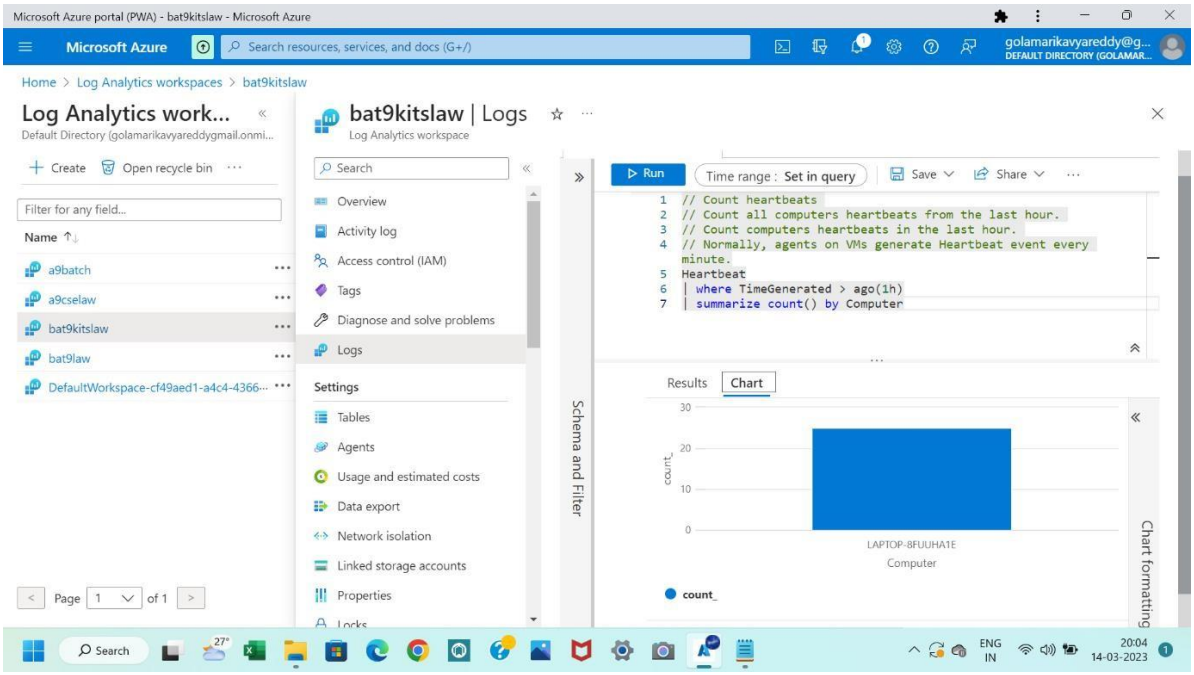




KQL Query -6:

```
Heartbeat
| where TimeGenerated > ago(1h)
| summarize count() by Computer
```





10.CONCLUSION

CHAPTER-10
CONCLUSION

In conclusion, the exploration and analysis of Azure Log Analytics Workspace for developing efficient queries for log data management is a critical step in achieving effective IT infrastructure management. This project has demonstrated the importance of log analytics and the role it plays in monitoring and troubleshooting IT infrastructure. By leveraging the capabilities of Azure Log Analytics Workspace, organizations can gain valuable insights into their log data and take proactive steps to optimize their IT infrastructure.

Through this project, we have explored the various tools and technologies involved in using Azure Log Analytics Workspace, including log queries, data visualization, and custom alerts. We have also discussed best practices for log data management, such as identifying key performance indicators (KPIs), monitoring resource utilization, and maintaining service availability.

Overall, this project provides a practical guide and valuable insights into how organizations can efficiently use Azure Log Analytics Workspace for log data management. By utilizing the strategies and techniques outlined in this project, organizations can enhance the efficiency and effectiveness of their IT infrastructure management and deliver better business outcomes. With Azure Log Analytics Workspace, organizations can easily manage and analyze their log data, monitor the health of their IT infrastructure, and troubleshoot issues in real-time, thereby reducing downtime and improving overall operational efficiency.

11.FUTURE WORK

CHAPTER-11
FUTURE SCOPE

The project "Efficient Log Data Management with KQL: Writing Azure Queries for Log Analytics Workspace" has a promising future scope in the field of cloud computing and data analytics. As more and more organizations move their workloads to the cloud, the need for efficient log data management and analysis is increasing.

Here are some potential future scope of the project:

a. Integration with other cloud platforms: The project can be extended to support log data management and analysis in other cloud platforms such as AWS and Google Cloud.
b. Support for additional data sources: Currently, the project supports log data from Azure services. It can be extended to support other data sources such as on-premises servers, IoT devices, and applications.
c. Advanced analytics capabilities: The project can be enhanced to support more advanced analytics capabilities such as machine learning and predictive analytics.
d. Real-time log data analysis: Real-time log data analysis is becoming increasingly important in today's fast-paced business environment. The project can be extended to support real-time log data analysis.
e. Integration with DevOps tools: The project can be integrated with DevOps tools such as Azure DevOps and GitHub to provide a seamless experience for developers and IT professionals.
f. Improved visualization: The project can be improved to provide more advanced visualization capabilities to help users better understand their log data.

12.REFERENCES

CHAPTER-12

REFERENCE

1. Forrester. (2020). The Total Economic Impact™ Of Microsoft Azure. Retrieved from https://www.forrester.com/report/The+Total+Economic+Impact+Of+Microsoft+Azure/-/E-RES156568
2. Synergy Research Group. (2021). Microsoft Azure achieves high uptime rate in Q4. Retrieved from https://www.srgresearch.com/articles/microsoft-azure-achieves-high-uptime-rate-q4
3. *(NIST), Author: Karen Kent; (NIST), Author: Murugiah Souppaya (2006). "SP 800-92, Guide to Computer Security Log Management" (PDF). csrc.nist.gov. doi:10.6028/NIST.SP.800-92. S2CID 221183642.* {{cite journal}}: |first1= has generic name (help)
4. *^ "Leveraging Log Data for Better Security". EventTracker SIEM, IT Security, Compliance, Log Management. Archived from the original on 28 December 2014. Retrieved 12 August 2015.*
5. *^ "Top 5 Log Mistakes - Second Edition". Docstoc.com. Retrieved 12 August 2015.*
6. Chris MacKinnon: "LMI In The Enterprise". *Processor* November 18, 2005, Vol.27 Issue 46, page 33. Online at http://www.processor.com/editorial/article.asp?article=articles%2Fp2746%2F09p46%2F09p46.asp, retrieved 2007-09-10
7. MITRE: Common Event Expression (CEE) Proposed Log Standard. Online at http://cee.mitre.org, retrieved 2010-03-03
8. NIST 800-92: Guide to Security Log Management. Online at http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, retrieved 2010-03-03
9. Canalys. (2020). Cloud security is the top reason businesses choose Azure. Retrieved from https://www.canalys.com/newsroom/cloud-security-is-top-reason-businesses-choose-azure.

10. IDC. (2020). Cloud Infrastructure Services Market Share Q2 2020. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS46947320

11. Kumar, A., Singh, S., & Agarwal, A. (2020). Cloud Computing – A Review of Advantages and Disadvantages of Cloud Deployment Models. International Journal of Computer Sciences and Engineering, 8(10), 96-101. doi: 10.26438/ijcse/v8i10.96101.