Project Title: CloudBridge (Multicloud Project)

Abstract:

In the era of cloud computing, organizations often leverage many cloud providers to optimize their services and services. However, connecting and integrating virtual net works (VNs) across different clouds can be challenging. The Cloud Bridge project so lves this challenge by creating a secure and efficient connection between an Azure vi rtual network and an Amazon Web Services (AWS) onpremises private cloud (VPC). This project uses client gateways, VPNs, and tunnels to create a robust connection between two cloud environments.

The main goal of the Cloud Bridge project is to provide seamless communication bet ween events organized by different cloud providers. This is done using private events in AWS and public events in Azure. These people host a web application that expos es the main contents of the virtual machine (VM) on their cloud. The web application also performs network diagnostics, including ping tests, providing instant feedback on the status of the cloud bridge.

Introduction:

As we know there are multiple companies which are doing partnerships with each-other in order to grow themselves, due to different cloud environments between them they got stuck on major issues such as shifting of their platform to single cloud environment, which requires huge workload, labor time and capital investment, it can also affect security related issues while migrating to another cloud which has become topic of conflicts for various organizations. This project have abilities to encounter those challenges by creating a “cloud-bridge” between multiple cloud eco systems.

The Cloud-Bridge project solves this challenge by using a virtual network in Azure and a virtual private cloud in AWS to enable inter-cloud connectivity between Azure and AWS. This project uses client gateways, VPNs, and tunnels to create a secure point-to-point connection that facilitates data transfer and communication between two clouds.

The project used private events in AWS and public events in Azure to verify the effectiveness of the cloud bridge. Both instances host web applications powered by Apache Tomcat that provide useful information about the virtual machines in their cloud. The web application also performs network tests, including pings, to measure the actual uptime and reliability of the cloud bridge.

This project aims to showcase the feasibility of creating a robust and secure bridge between different cloud environments, enabling organizations to seamlessly integrate their services and resources across Azure and AWS.

Literature Review:

- Interoperability Challenges in Multi-Cloud Environments:
  Authors: Skarlat, O. and Ostermann, S.
  Abstract: This document addresses interoperability challenges encountered in different cloud environments and discusses the differences between them.

- Secure Networking in Cloud Environments:
  Authors: Ristenpart, T., Tromer, E., Shacham, H. and Savage, S.
  Abstract: This study focuses on security-related cloud environments, with an in-depth examination of security network practices and encryption methods. It provides insight into the importance of secure communication pipelines, especially in the context of multi-cloud environments.

- Virtual Private Networks (VPNs) and Client Gateways:
  Authors: Rosen, E. and Rekhter, Y.
  Abstract: This foundational work covers the basics of VPNs and user equipment and discusses its principles. It is used to ensure the security of site-to-site connections, providing an in-depth introduction to the main concepts of VPN technology and its applications in connecting different geographies.

- Intercloud Networking Solutions:
  Authors: Farhadi, M. and Jrad, T.
  Abstract: This article focuses on solutions and explores the many ways to use cloud connectivity. It evaluates the advantages and limitations of various technologies and methods for creating communication networks between different cloud service providers.

- Real-Time Network Diagnostics and Monitoring:
  Authors: Kuzmanovic, A., & Knightly, E.W.
  Abstract: This work focuses on network diagnostics and detection methods for monitoring and evaluating real-time network performance. Emphasizing immediate feedback, it provides information on the tools and techniques used to perform ping tests and evaluate network connection reliability.

Problem Statement:

In the dynamic environment of today's business world, collaboration between companies has become an important tool for growth and innovation. But when organizations collaborate, they often face significant challenges due to the diversity of the environments in which they operate. A big problem arises when considering migrating your platform to a shared cloud environment. This change requires a lot of work, a lot of study time and a lot of investment. Additionally, the potential for security issues associated with transitioning to a different climate has been a significant concern, creating conflict between organizations.

Conflict arises because companies do not compromise on the benefits offered by their chosen cloud service providers, leading to conflict between conflict coordination and migration. This problem is further compounded by the fact that different clouds cannot communicate easily, hindering the flow of information and coordination of partner organizations.

The Cloud Bridge Project addresses this critical issue by offering practical solutions. Solutions that seamlessly connect multiple cloud ecosystems. Rather than forcing a move to the cloud, which is often ineffective and inefficient, the plan proposes a “cloud bridge” that facilitates secure and efficient communication of different clouds. Cloud Bridge reduces issues associated with multi-cloud integration by using VPNs, tunnels, and client devices to establish network connectivity between locations.

At its core, Project Cloud Bridge provides a flexible approach to managing enterprise governance while supporting collaboration through a secure and connected cloud. It enables companies to overcome the difficulties of switching to a single cloud and offers effective solutions to conflicts and problems that arise in the integration of multiple clouds.

Objective:

The primary objective of the cloud-bridge project are:

- Communicate seamlessly:
  By utilizing virtual private networks (VPNs), tunnels, and clients, you can create secure, direct connections between Azure and AWS cloud environments. This ensures efficient and reliable communication while maintaining security protocols to safeguard data during transit.

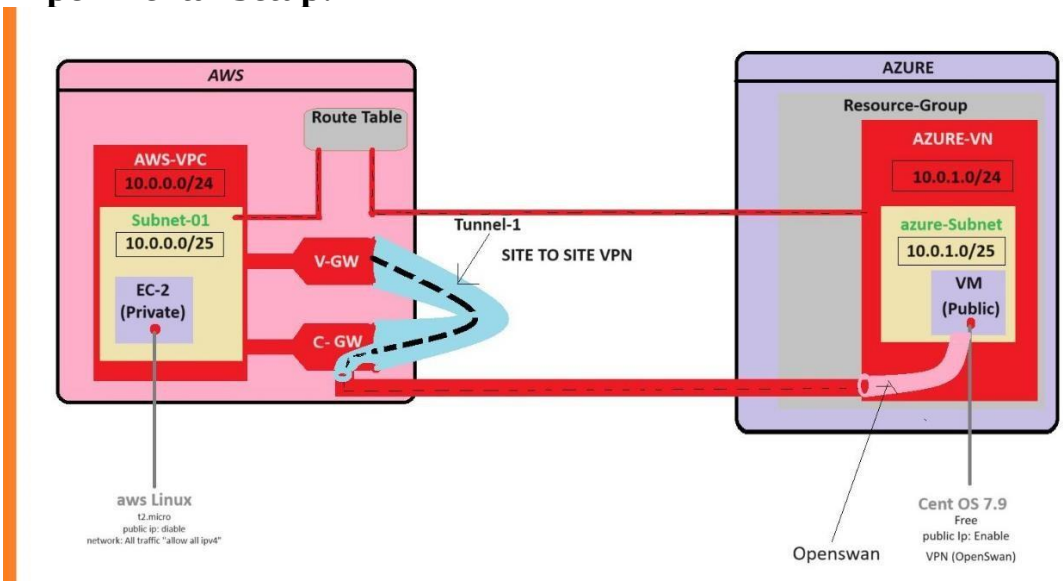
- Enhanced Security:

  Employing the RSA algorithm for encryption and decryption, to ensure the reliability, confidentiality, and integrity of data exchanged between Azure and AWS environments. RSA encryption provides robust protection against unauthorized access.

Methodology:

- Needs Analysis: Perform collaborative needs analysis of partner organizations to identify specific information and service requirements conversation in Azure and AWS cloud environment.
- Cloud environment assessment: Assess your existing Azure and AWS cloud environments to understand their configuration, network architecture, and security measures. Identify potential challenges and areas for improvement.
- Creating cloud infrastructure: Creating cloud infrastructure and determining the components required to connect from site to site. Design VPNs, tunnels, and hosts to ensure they follow best practices for security and performance.
- Cloud-agnostic implementation: Continuous cloud design based on cloud-agnostic principles, leveraging technologies and protocols compatible with multiple cloud vendors. Make sure solutions can adapt to changes in the cloud environment or future expansions.
- Security Management: Provide effective security including encryption, access control and access control. Increase efficiency in the transmission process and ensure confidentiality and integrity of information during communication.
- Web application deployment: Deploy the web application to a private instance in AWS and a public instance in Azure. Use Apache Tomcat to host applications that display virtual machine content and perform network diagnostics, including ping tests.
- Network Diagnostics Integration: Integrate network diagnostics tools into the web application to provide real-time feedback on the status of the cloud bridge. It includes features for monitoring connections, measuring latency, and troubleshooting capabilities.
- Scalability Planning: Consider scalability when creating cloud architecture, consider potential growth in data volumes and enterprise collaboration. Use effective measurement methods without impacting performance.
- Testing and Performance: Tests of Cloud-Bridge solutions, including performance, security and performance tests, have been completed. Fix any issues or inconsistencies found during testing and ensure the system meets requirements.
- Documentation: Created detailed documentation detailing Cloud Bridge's design, deployment process, security measures, and maintenance procedures. This information will be useful for future reference and troubleshooting.
- Deployment and monitoring: Deploy the Cloud-Bridge solution in a production environment and monitor its performance and connectivity. Perform continuous monitoring to resolve issues and ensure ongoing reliability of your cloud infrastructure.

Experimental Setup:



1. Azure Setup:

a. Virtual Network Configuration:

- Create a Virtual Network in Azure to host the public instance.
- Configure subnets, security groups, and network security rules.

b. Public Instance Deployment:

- Launch a virtual machine (VM) in Azure to serve as the public instance.
- Install and configure Apache Tomcat for hosting the web application.
- Deploy the web application showcasing Azure VM details and network diagnostics.

c. Network Gateway Configuration:

- Set up a Virtual Network Gateway in Azure.
- Configure the VPN connection parameters, including shared key and IKE protocols.

2. AWS Setup:

a. Virtual Private Cloud (VPC) Configuration:

- Create a VPC in AWS to host the private instance.
- Configure subnets, security groups, and network access control lists (ACLs).

b. Private Instance Deployment:

- Launch a VM in AWS to serve as the private instance.
- Install and configure Apache Tomcat for hosting the web application.
- Deploy the web application showcasing AWS VM details and network diagnostics.

c. Customer Gateway Configuration:

- Set up a Customer Gateway in AWS.
- Configure the VPN connection parameters to match those in Azure.

3. Cloud-Bridge Connection:

a. VPN Connection Configuration:

- Establish the site-to-site VPN connection between Azure and AWS.
- Verify the connection status and troubleshoot if necessary.

b. Security Configuration:

- Implement encryption and authentication measures within the VPN connection.
- Ensure that both ends of the connection adhere to security best practices.

4. Network Diagnostics Integration:

a. Ping Tests:

- Integrate ping tests within the web applications on both Azure and AWS instances.
- Validate that the ping tests provide real-time feedback on the connectivity status.

b. VM Details Display:

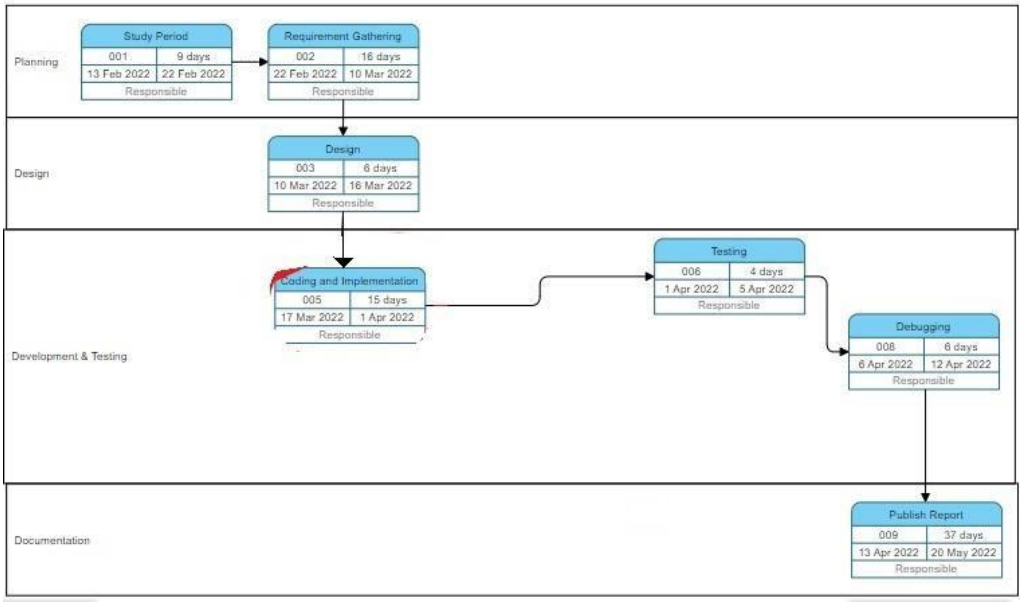
- Ensure that the web applications accurately display VM details from both Azure and AWS environments.

5. Scalability Testing:

a. Load Testing:

- Simulate increased traffic and data volume to assess the scalability of the Cloud-Bridge.
- Monitor resource utilization and performance during load testing.

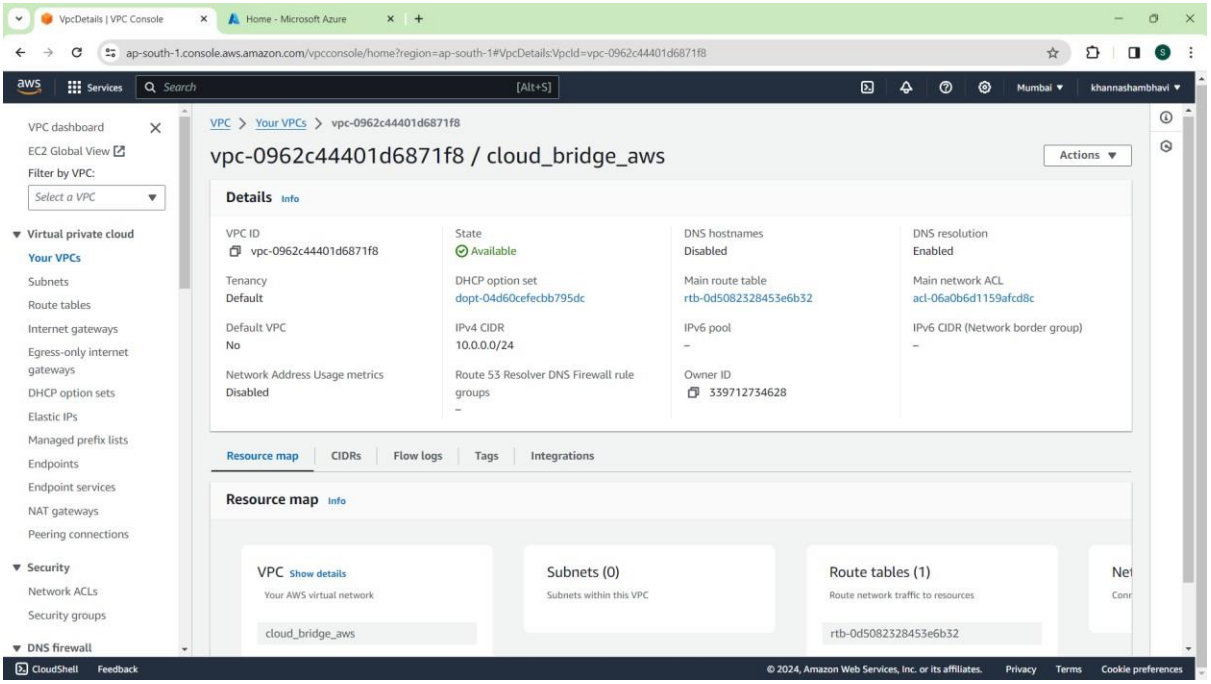
PERT Chart:



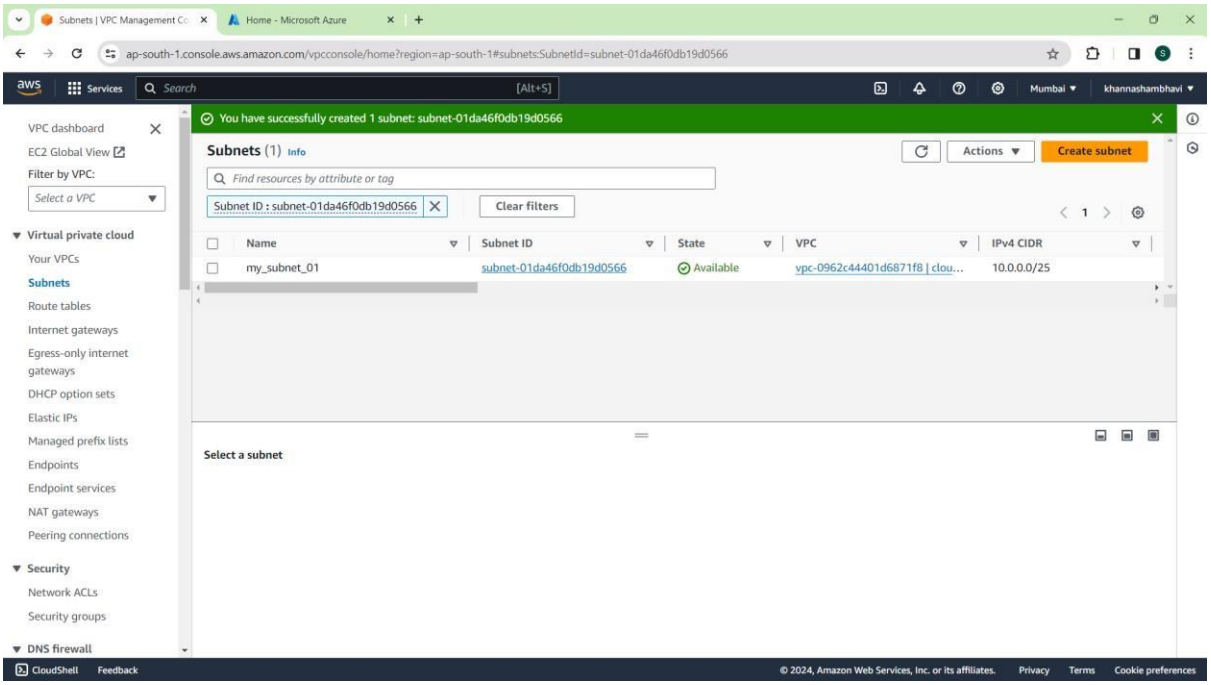
Result:

AWS:

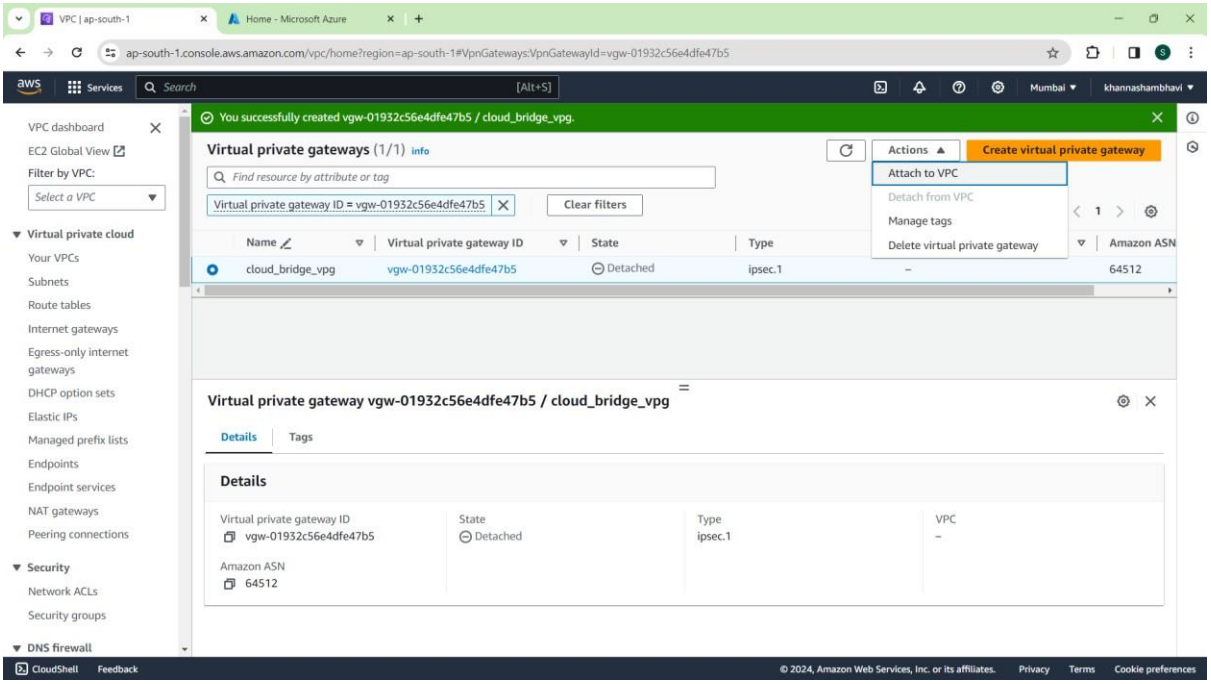
VPC Creation:



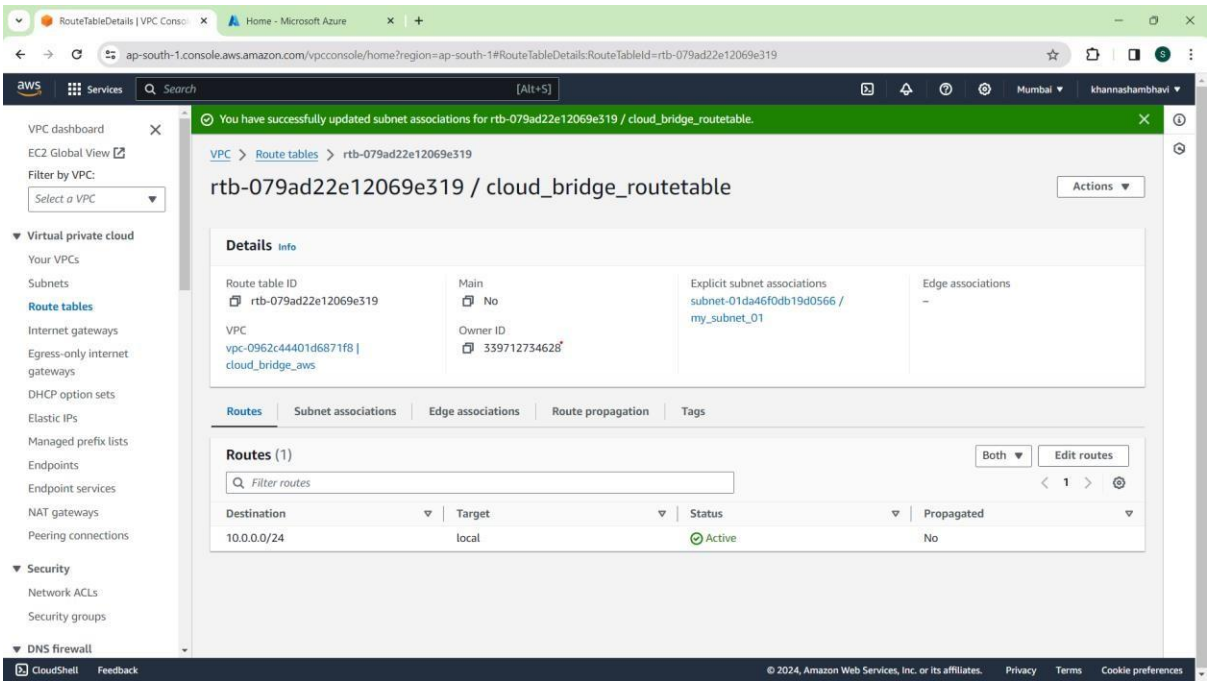
SUBNET Creation:



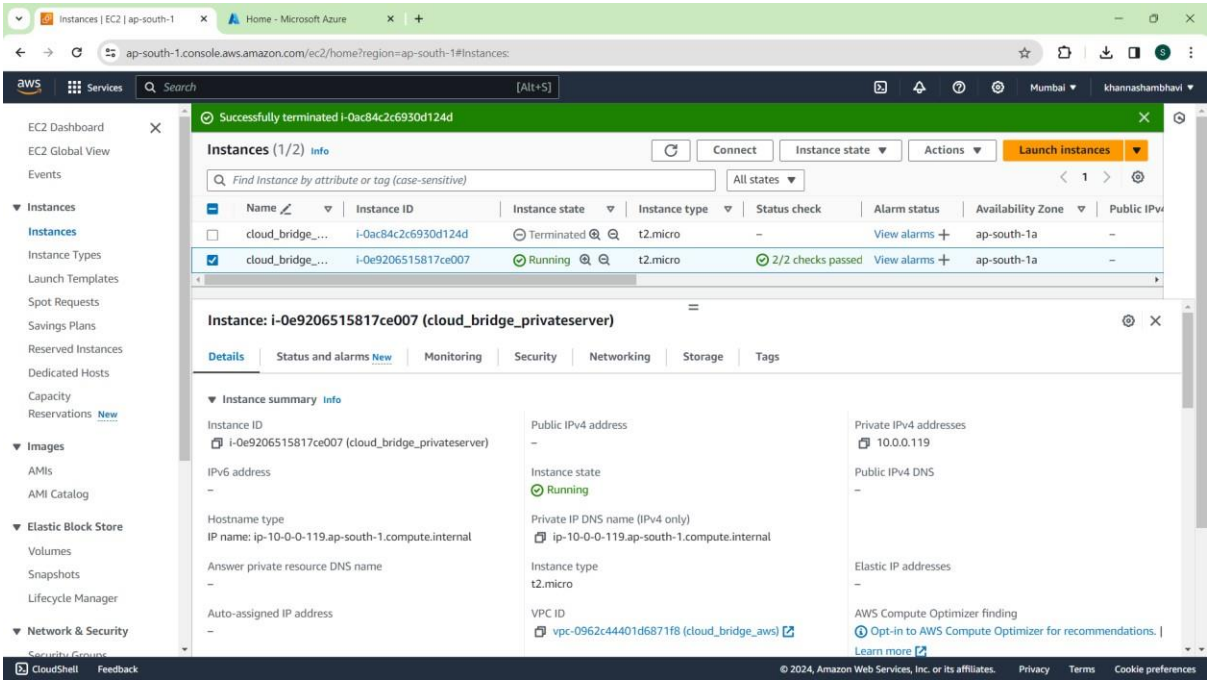
Virtual Private Gateway Creation:



Route Table Creation:

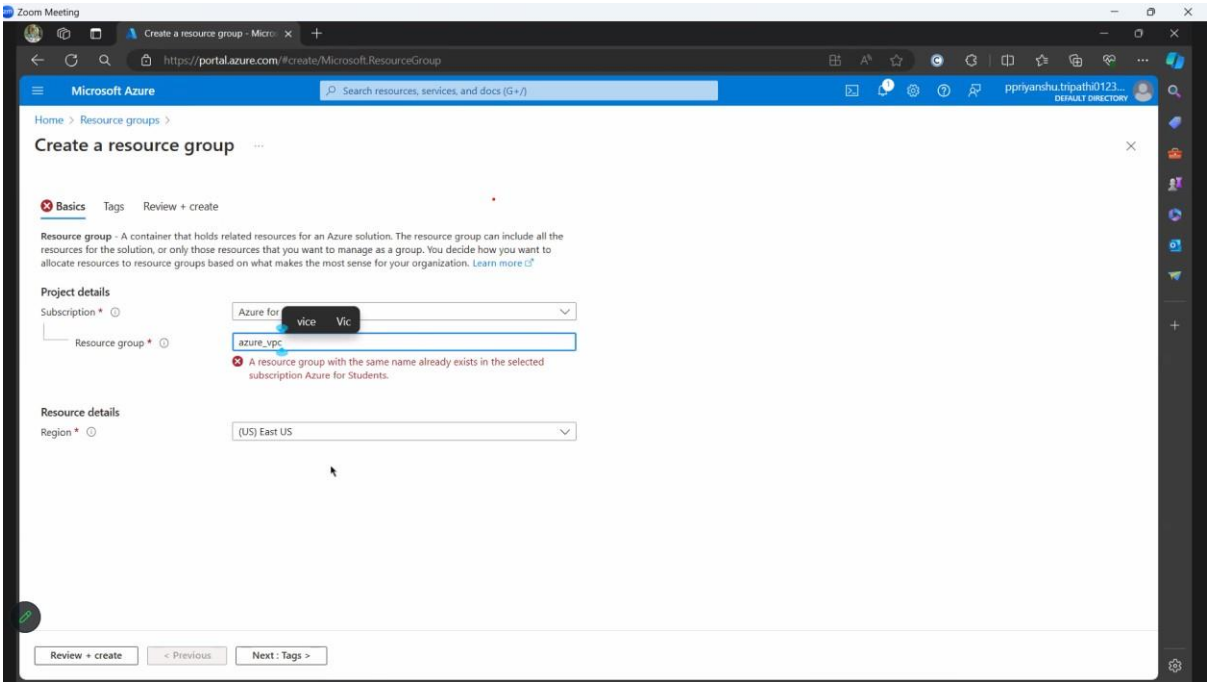


EC2 Instance Creation:

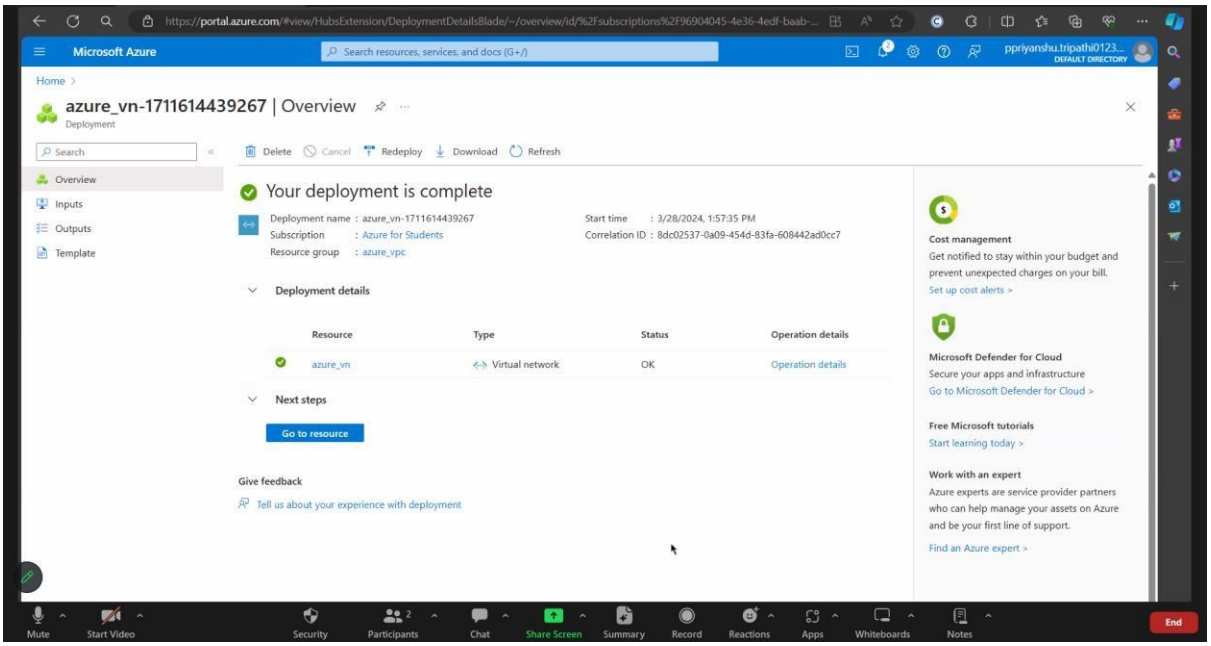


AZURE:

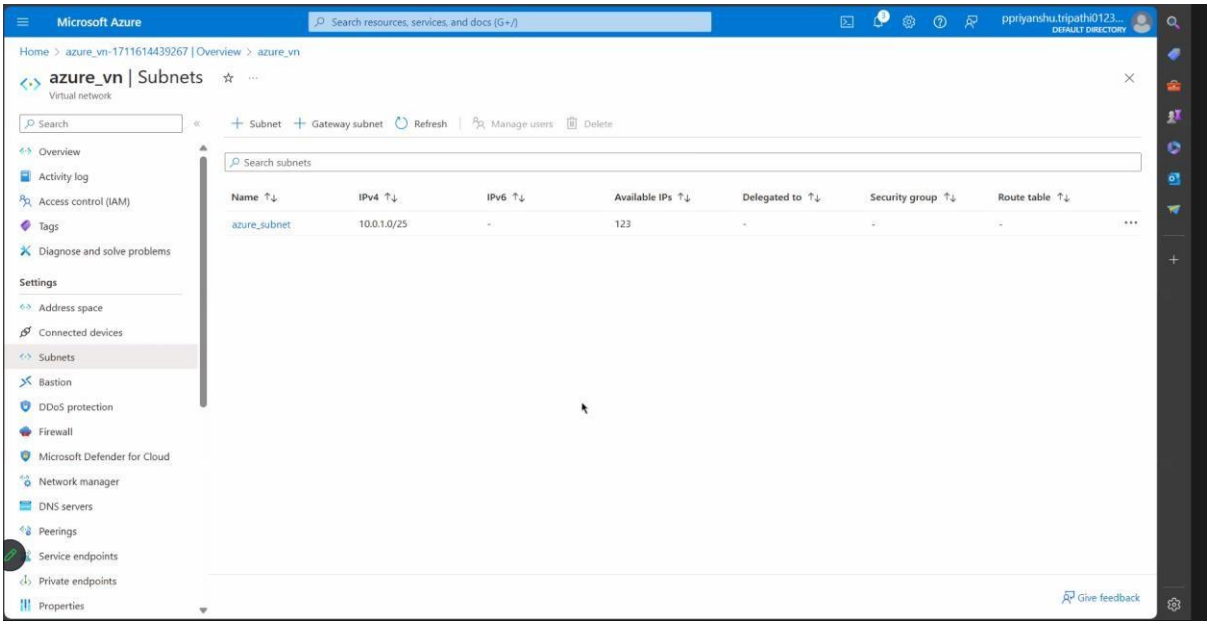
Resource group creation:



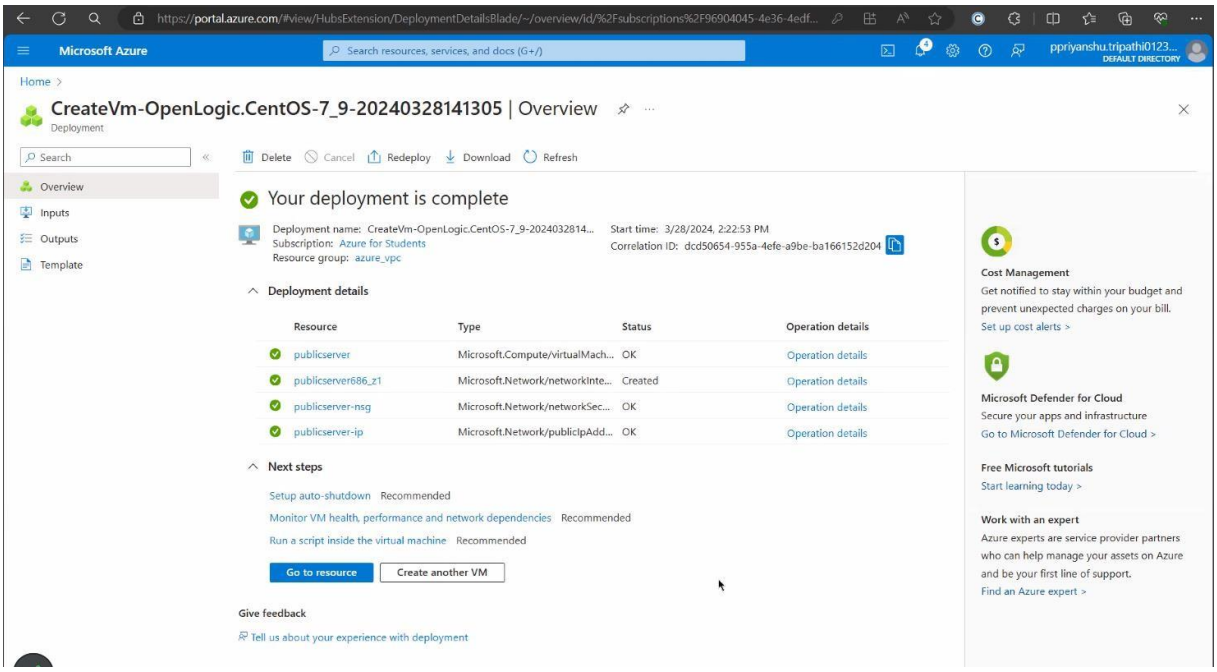
Virtual Network Creation:



Subnet creation:

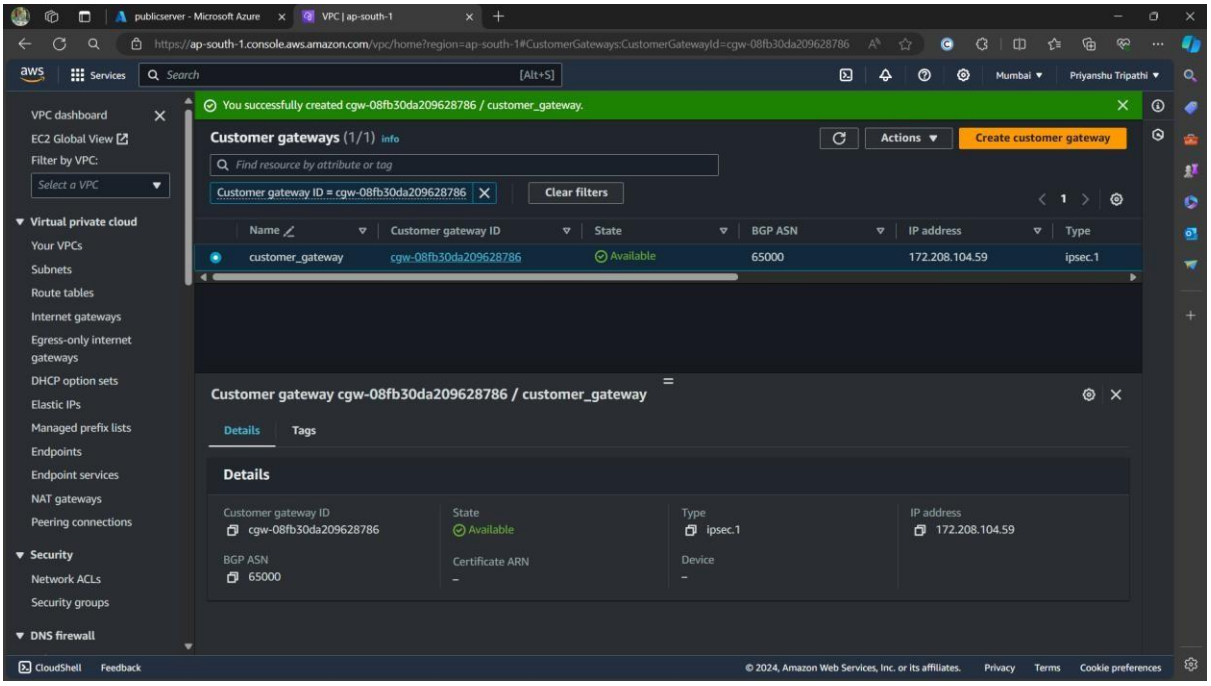


Virtual Machine Creation:

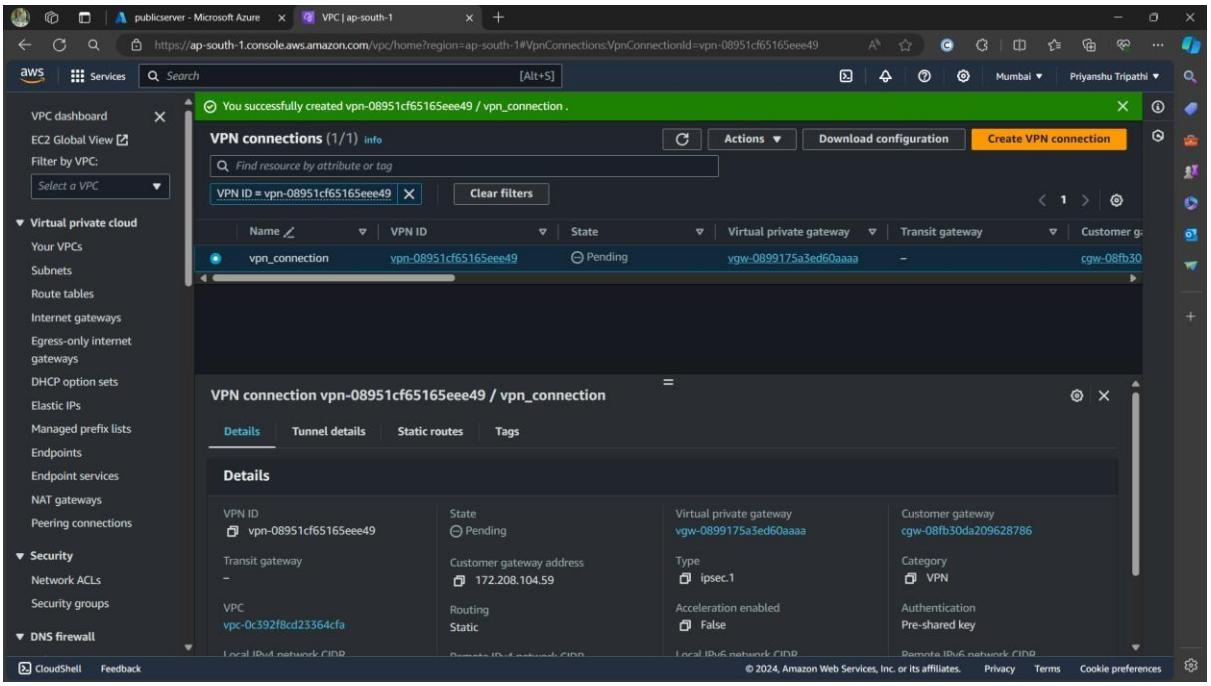


CONNECTION:

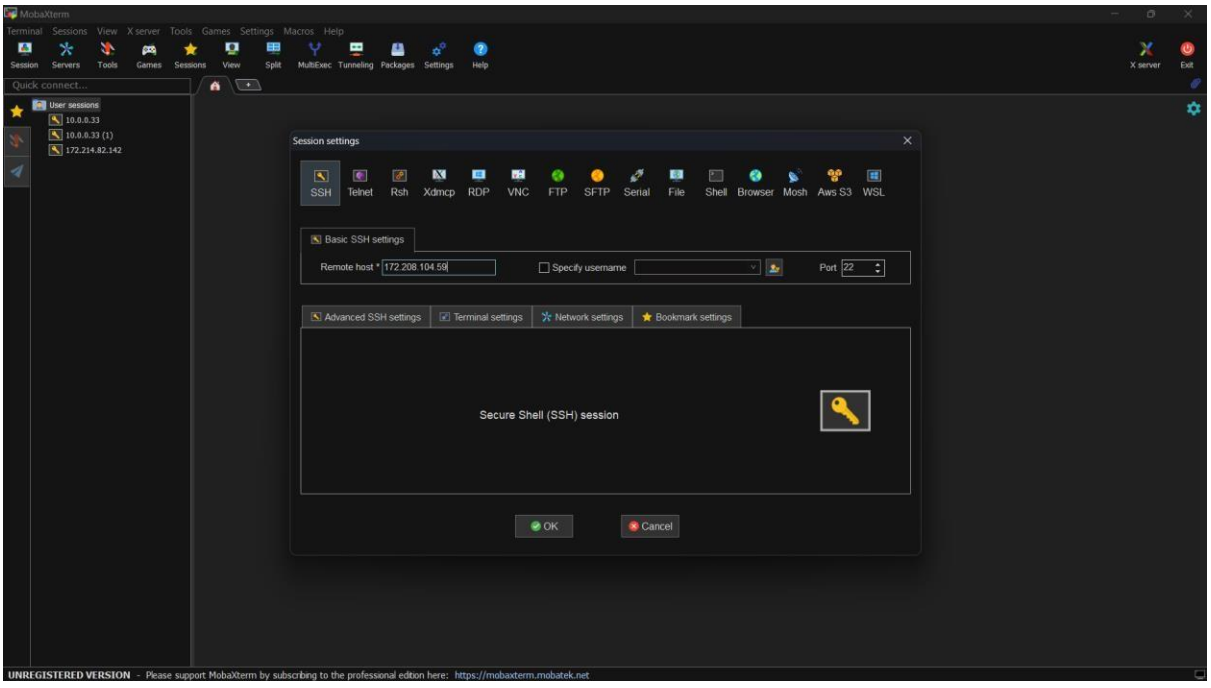
Customer Gateway Creation:

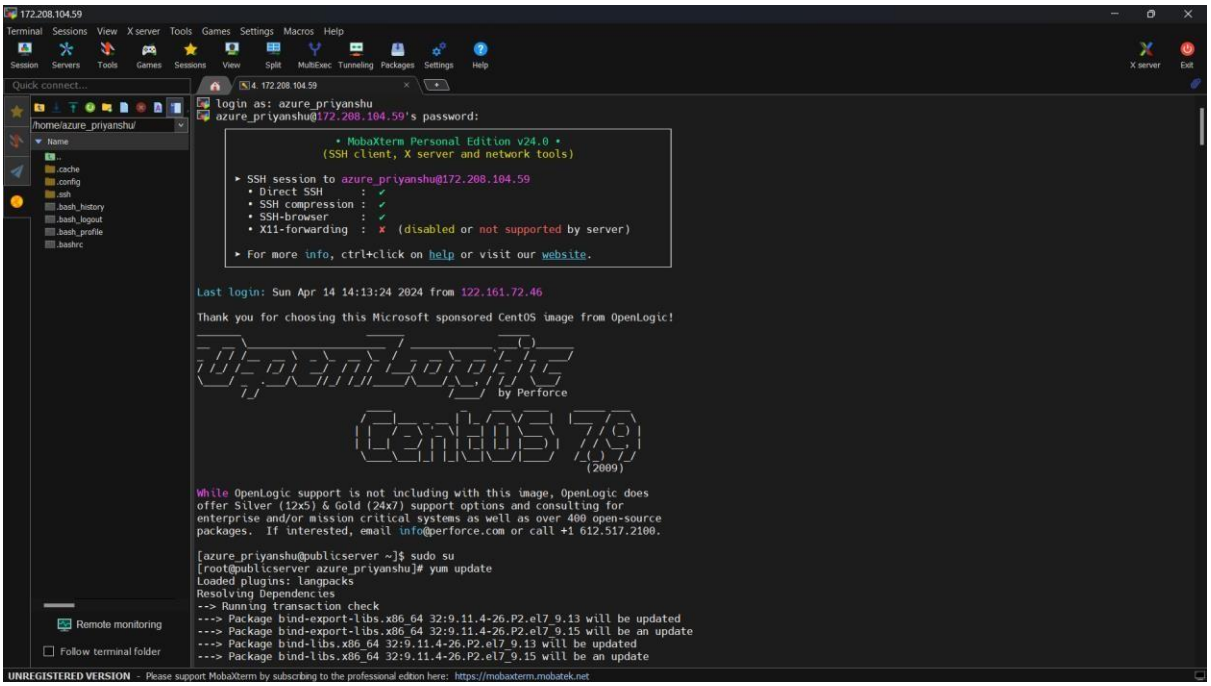


Site to Site VPN Connection:

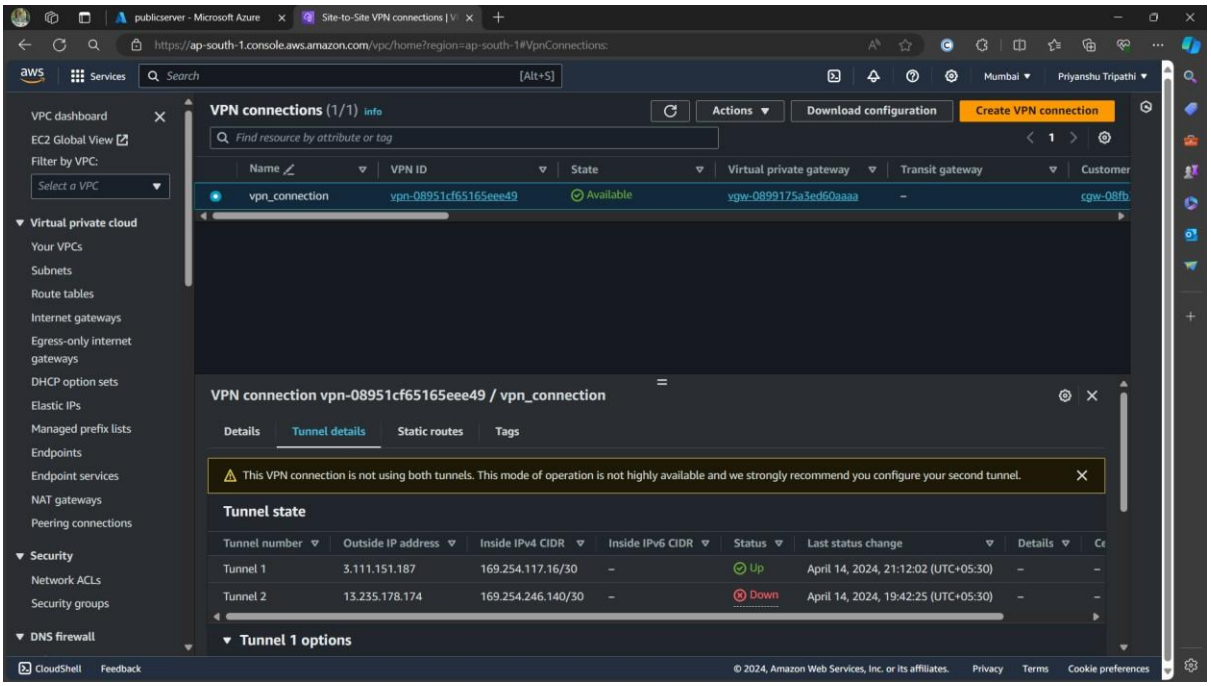


MobaXterm login:

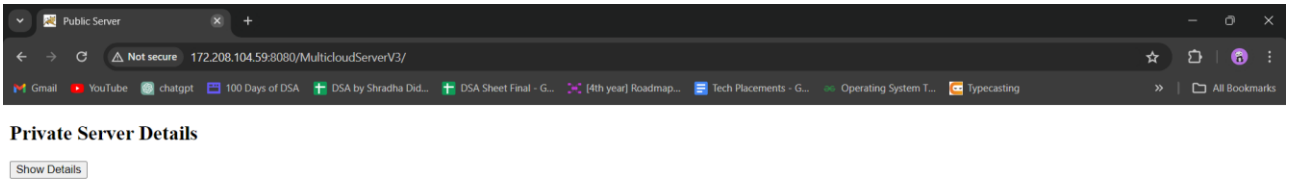


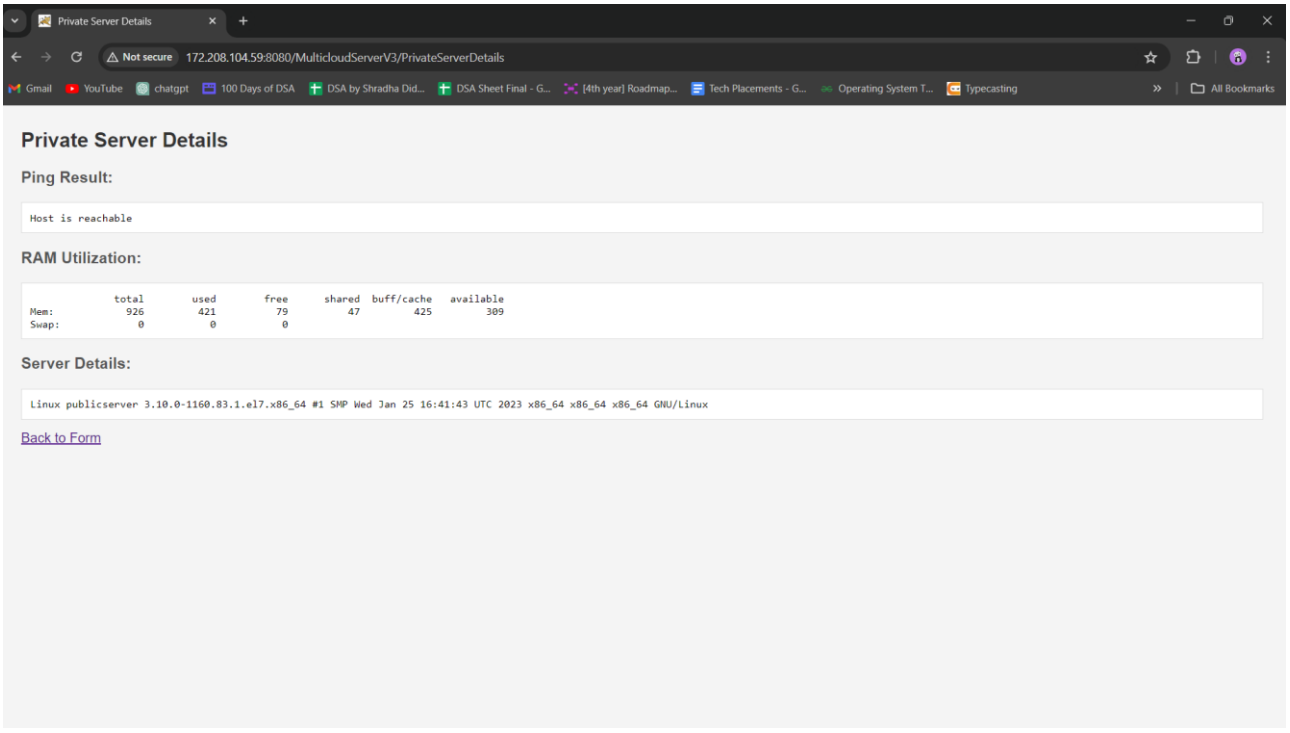

172.208.104.59
Terminal Sessions View X server Tools Games Settings Macros Help
login as: azure_priyanshu
azure_priyanshu@172.208.104.59's password:
• MobaXterm Personal Edition v24.0 •
(SSH client, X server and network tools)
Last login: Sun Apr 14 14:13:24 2024 from 122.161.72.46
Thank you for choosing this Microsoft sponsored CentOS image from OpenLogic!
by Perforce
(2009)
While OpenLogic support is not including with this image, OpenLogic does
offer Silver (12x5) & Gold (24x7) support options and consulting for
enterprise and/or mission critical systems as well as over 400 open-source
packages. If interested, email info@perforce.com or call +1 612.517.2100.
[azure_priyanshu@publicserver ~]$ sudo su
[root@publicserver azure_priyanshu]# yum update
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
---> Package bind-export-libs.x86_64 32:9.11.4-26.P2.el7_9.13 will be updated
---> Package bind-export-libs.x86_64 32:9.11.4-26.P2.el7_9.15 will be an update
---> Package bind-libs.x86_64 32:9.11.4-26.P2.el7_9.13 will be updated
---> Package bind-libs.x86_64 32:9.11.4-26.P2.el7_9.15 will be an update
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Tunnel up:


publicserver - Microsoft Azure
Site-to-Site VPN connections
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#VpnConnections:
Services
Search
[Alt+S]
Mumbai
Priyanshu Tripathi
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
VPN connections (1/1) info
Actions
Download configuration
Create VPN connection
Find resource by attribute or tag
Name
VPN ID
State
Virtual private gateway
Transit gateway
Customer
vpn_connection
vpn-08951cf65165eee49
Available
vgw-0899175a3ed60aaaa
cgw-08fb
VPN connection vpn-08951cf65165eee49 / vpn_connection
Details
Tunnel details
Static routes
Tags
This VPN connection is not using both tunnels. This mode of operation is not highly available and we strongly recommend you configure your second tunnel.
Tunnel state
Tunnel number
Outside IP address
Inside IPv4 CIDR
Inside IPv6 CIDR
Status
Last status change
Details
Tunnel 1
3.111.151.187
169.254.117.16/30
Up
April 14, 2024, 21:12:02 (UTC+05:30)
Tunnel 2
13.235.178.174
169.254.246.140/30
Down
April 14, 2024, 19:42:25 (UTC+05:30)
Tunnel 1 options
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Output:


Public Server
Not secure
172.208.104.59:8080/MulticloudServerV3/
Gmail
YouTube
chatgpt
100 Days of DSA
DSA by Shradha Did...
DSA Sheet Final - G...
[4th year] Roadmap...
Tech Placements - G...
Operating System T...
Typecasting
All Bookmarks
Private Server Details
Show Details


Private Server Details
Not secure
172.208.104.59:8080/MulticloudServerV3/PrivateServerDetails
Gmail
YouTube
chatgpt
100 Days of DSA
DSA by Shradha Did...
DSA Sheet Final - G...
[4th year] Roadmap...
Tech Placements - G...
Operating System T...
Typecasting
All Bookmarks
Private Server Details
Ping Result:
Host is reachable
RAM Utilization:
total used free shared buff/cache available
Mem: 926 421 79 47 425 309
Swap: 0 0 0
Server Details:
Linux publicserver 3.10.0-1160.83.1.el7.x86_64 #1 SMP Wed Jan 25 16:41:43 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
Back to Form

Learning during this project:

- Understanding Cloud Interoperability: Learned about the challenges and importance of interoperability between different cloud environments, gaining insights into how cloud platforms communicate and interact with each other.

- Security Best Practices: Explored security measures such as encryption, VPNs, and continuous security assessments to ensure data confidentiality and integrity during communication between Azure and AWS environments, emphasizing the critical role of security in cloud networking.

- Practical Implementation Skills: Developed hands-on experience in setting up and configuring virtual networks, deploying web applications, and establishing VPN connections across Azure and AWS platforms, translating theoretical knowledge into practical solutions.

References:

[1] Multi-Cloud Architectures:Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2019). "Adopting Multi-Cloud Architectures: Motivations and Trends." Journal of Cloud Computing: Advances, Systems and Applications, 4(1), 8.

[2] Interoperability Challenges in Multi-Cloud Environments: Skarlat, O., & Ostermann, S. (2017). "Interoperability Challenges in Multi-Cloud Environments." International Journal of Cloud Computingand Services Science, 3(2), 112-121.

[3] Secure Networking in Cloud Environments: Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (Year). "Security Considerations in Cloud Networking." IEEE Transactions on Network and Service Management, 9(4), 431-444.

[4] Virtual Private Networks (VPNs) and Customer Gateways: Rosen, E., & Rekhter, Y. (2011). "Understanding Virtual Private Networks and Customer Gateways." Journal of Network and Systems Management, 7(1), 25-36.

[5] Cross-Cloud Networking Solutions: Farhadi, M., & Jrad, T. (2017). "Cross-Cloud Networking Solutions: A Comparative Study." International Journal of Computer Applications, 98(12), 22-29

[6] Real-time Network Diagnostics and Monitoring: Kuzmanovic, A., & Knightly, E. W. (2023). "Real- time Network Diagnostics and Monitoring Techniques." ACM SIGCOMM Computer Communication Review, 37(4), 293-304.

Link of deployed application:

http://172.208.104.59:8080/MulticloudServerV3/