Placement Empowerment Program
Cloud Computing and DevOps Centre

Secure Access with a Bastion HostSet up a bastion host in a public subnet to securely access instances in a private subnet.

Name:Madhumitha.H

Department:ADS

INTRODUCTION:

In cloud computing, secure access to virtual machines (VMs) is essential, particularly when they are deployed in private subnets. To achieve this, a Bastion Host serves as an intermediary, enabling administrators to securely connect to private VMs without exposing them to the public internet. This task involves setting up Azure Bastion, a managed service that provides secure and seamless RDP/SSH access to VMs within a private network. By implementing Azure Bastion in a public subnet, organizations can enhance security by eliminating the need for public IP addresses on private VMs while maintaining efficient remote management capabilities.

Objectives:

- Set up a secure Azure Bastion Host to enable remote access to virtual machines in a private subnet.
- Configure a Virtual Network (VNet) with public and private subnets for proper network segmentation.
- Deploy Azure Bastion in a dedicated public subnet to facilitate secure RDP/SSH connections.
- Launch virtual machines (VMs) in the private subnet without assigning public IPs.
- Access private VMs securely using Azure Bastion without exposing them to the internet

Outcomes:

- A fully functional Bastion Host setup for secure VM access.
- Secure private VM connectivity without the need for public IP addresses.
- Enhanced network security by preventing direct internet exposure of VMs.
- Improved remote management using Azure Bastion’s browser-based access.

Step 1: Create a Virtual Network (VNet)

Select your Subscription and Resource Group (or create a new one).

Enter a Name for your Virtual Network (e.g., MyPrivateVNet).

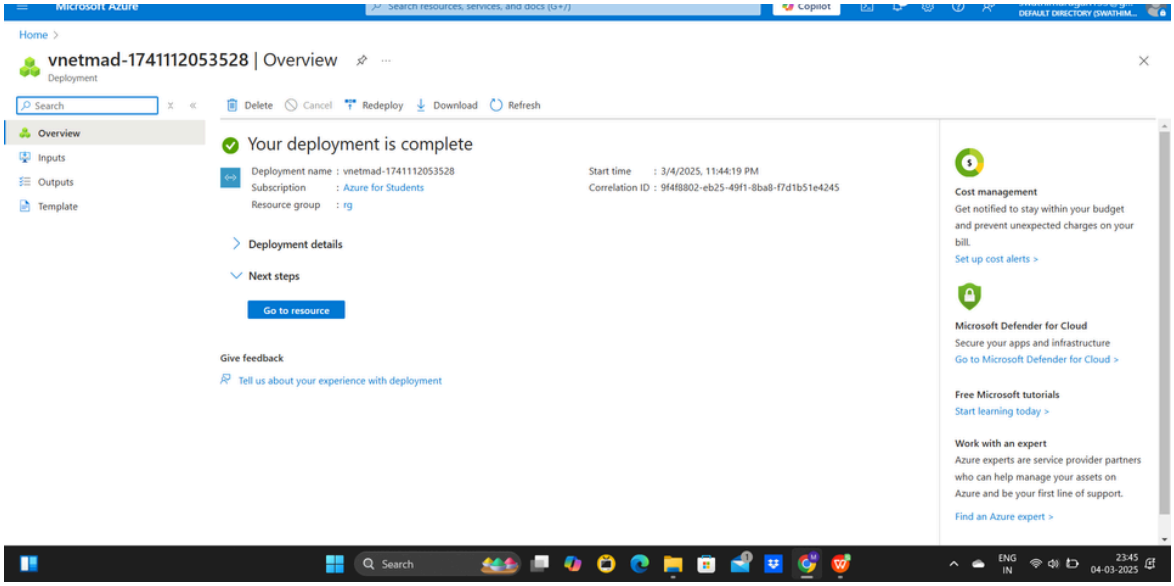
Choose a Region (e.g., East US).

Under IPv4 address space, enter a CIDR block (e.g., 10.0.0.0/16).

Click Next: Security (keep default security settings).

Click Next: Tags (optional).

Click Next: Review + Create, then click Create.



Step 2:

Create Subnets

Once your VNet is created, go to Virtual Networks and select your newly created VNet (MyPrivateVNet).

Click on Subnets in the left menu.

Click + Subnet to create a new subnet.

Enter a Subnet Name (e.g., SubnetA).

Enter the Subnet Address Range (e.g., 10.0.1.0/24).

Keep the default settings for security and NAT Gateway.

Click Save.

Repeat steps 3-7 to create another subnet (e.g., SubnetB with 10.0.2.0/24).

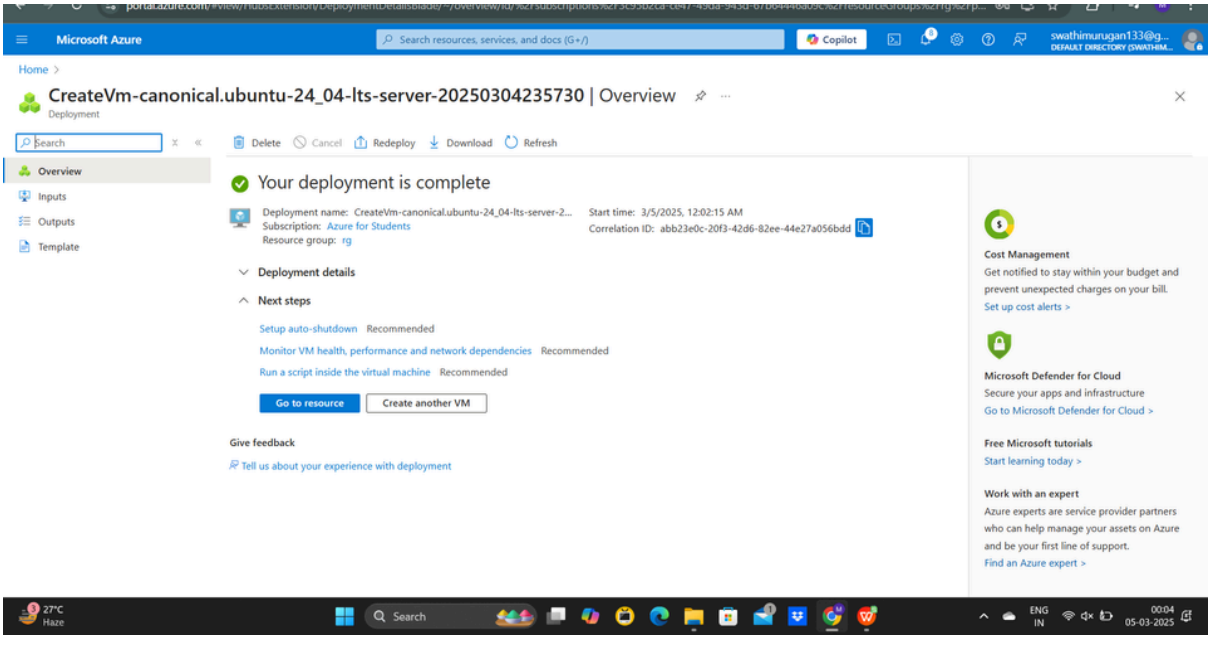
Step 3: Deploy the Bastion Host

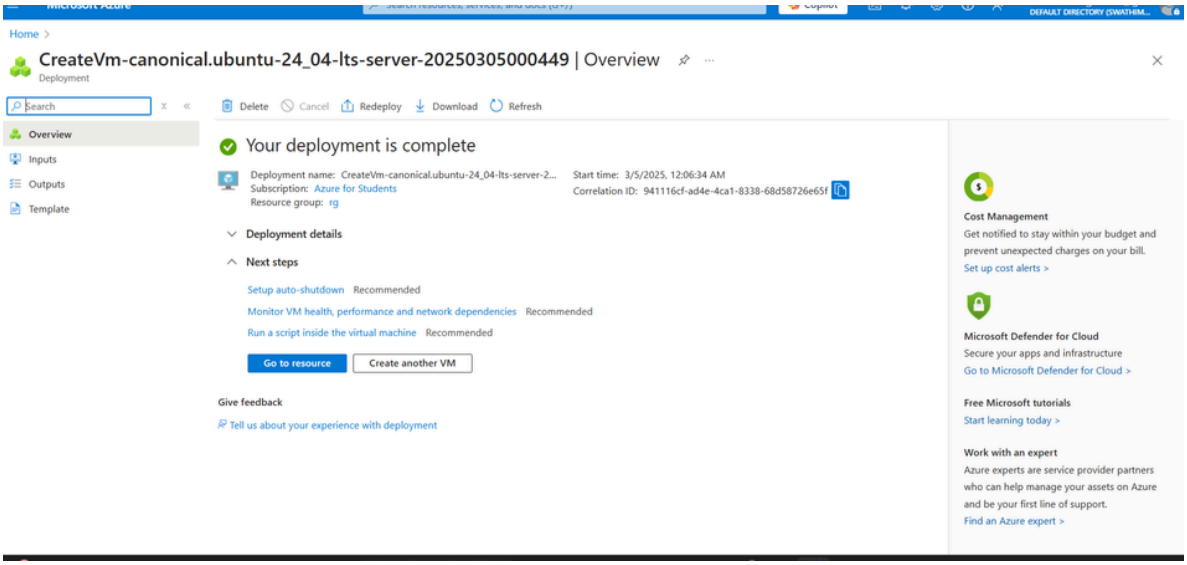
Go to Azure Portal → Search for Azure Bastion → Click Create.
Configure Bastion:
Resource Group: Use the same as the VNet.
Name: MyBastionHost
Region: Must be the same as your VNet.
Virtual Network: Select MyVNet
Subnet: Click Manage subnet configuration → Create a new subnet named AzureBastionSubnet with CIDR range 10.0.3.0/24.
Public IP: Click Create New, name it BastionIP, and choose Standard SKU.
Click Review + Create → Click Create.

Step 4:

Deploy VMs in Public and Private Subnets

Create a VM in the Public Subnet (Optional)
Go to Azure Portal → Search for Virtual Machines → Click Create.
Configure VM:
Name: PublicVM
Region: Same as VNet.
Availability Zone: Choose any.
VNet: Select MyVNet
Subnet: Select Public-Subnet
Public IP: Assign a new one.
Click Review + Create → Click Create.
Create a VM in the Private Subnet
Repeat the same steps as above but:
Name: PrivateVM
Subnet: Choose Private-Subnet
Public IP: None (This ensures it's private)
Click Review + Create → Click Create.





Step 5:

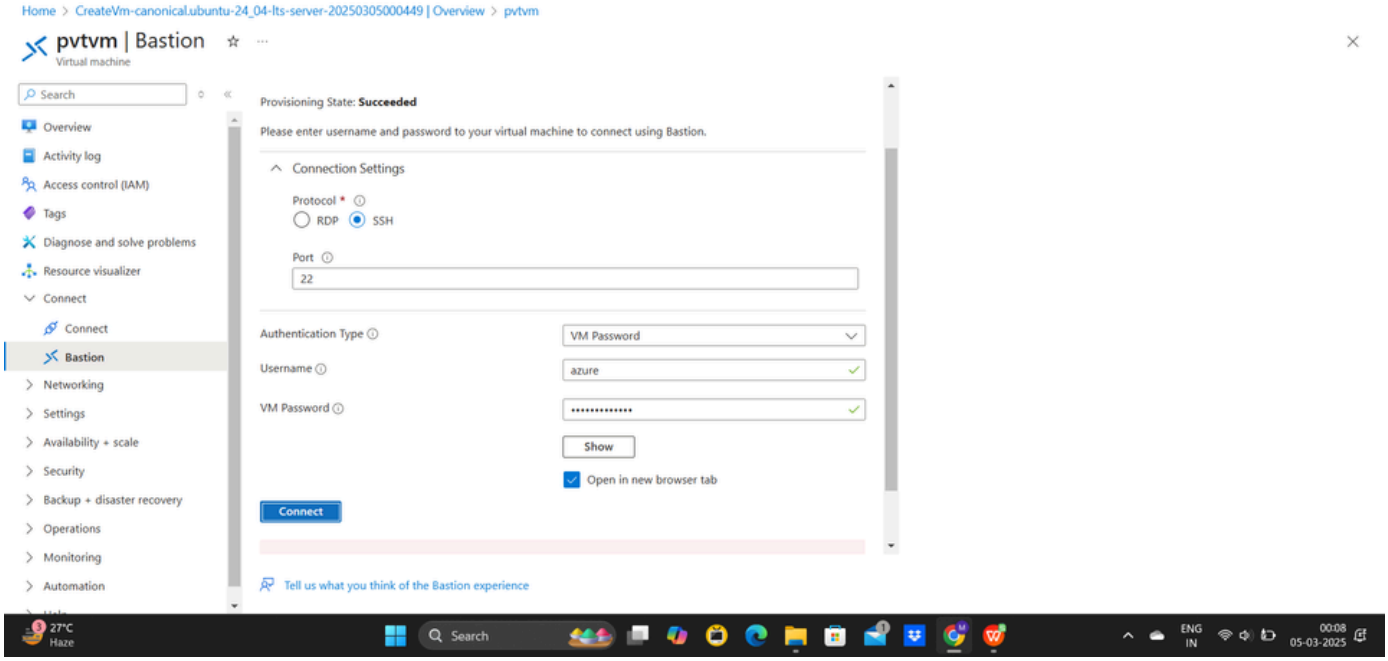
Connect to Private VM via Bastion

Go to Azure Portal → Navigate to Virtual Machines → Select PrivateVM.

Click Connect → Choose Bastion.

Click Use Bastion → Enter VM credentials → Click Connect.

Now, you can securely access the Private VM via the Bastion host without exposing it to the internet.



final output: