Placement Empowerment Program

Cloud Computing and DevOps Centre

Setup a bastion-host with public subnet to access virtual machines inside private subnet

Name: Anumitha M Department: AML

Introduction :

A Bastion Host is a dedicated server designed to act as a secure gateway between a public subnet (accessible from the internet) and a private subnet (isolated from direct internet access). The primary role of the Bastion Host is to facilitate secure SSH or RDP connections from the internet to instances in the private subnet, which would otherwise be unreachable. Typically, the Bastion Host is deployed in a public subnet where it has a public IP address and can be accessed directly from the internet. Once an administrator or user connects to the Bastion Host, they can then securely access other instances in the private subnet using protocols like SSH (for Linux instances) or RDP (for Windows instances). This setup ensures that the private instances remain shielded from the outside world, reducing the attack surface. To enhance security, access to the Bastion Host is strictly controlled, often limited to specific IP addresses or ranges, and it's important to harden the Bastion Host itself by ensuring minimal software installation, applying security patches, using strong authentication methods (like SSH keys), and enabling monitoring and logging for auditing purposes. The Bastion Host serves as a controlled and auditable point of entry into a private network, maintaining a balance between secure access and network isolation.

Overview :

*A **Bastion Host** is a secure server deployed in a **public subnet** that acts as a gateway for accessing instances in a **private subnet**, which are not directly accessible from the internet. It allows administrators to securely connect to private instances via SSH or RDP, ensuring the private subnet remains protected from direct exposure. The Bastion Host typically has a public IP, but access is tightly controlled, often limited to specific IP addresses, and it should be hardened with strong authentication, monitoring, and logging to minimize security risks. This setup enables secure access to private resources while maintaining isolation and reducing the attack surface.*

Objective :

The objective of this task is to:

***Secure Access**: Provide a controlled entry point for accessing instances in a private subnet.*

***Isolation of Private Resources**: Ensure instances in the private subnet remain shielded from direct internet access.*

***Centralized Gateway**: Serve as the only access point for administrative SSH or RDP connections to private instances.*

***Access Control**: Restrict access to the Bastion Host, typically by IP address or VPN, to ensure only authorized users can connect.*

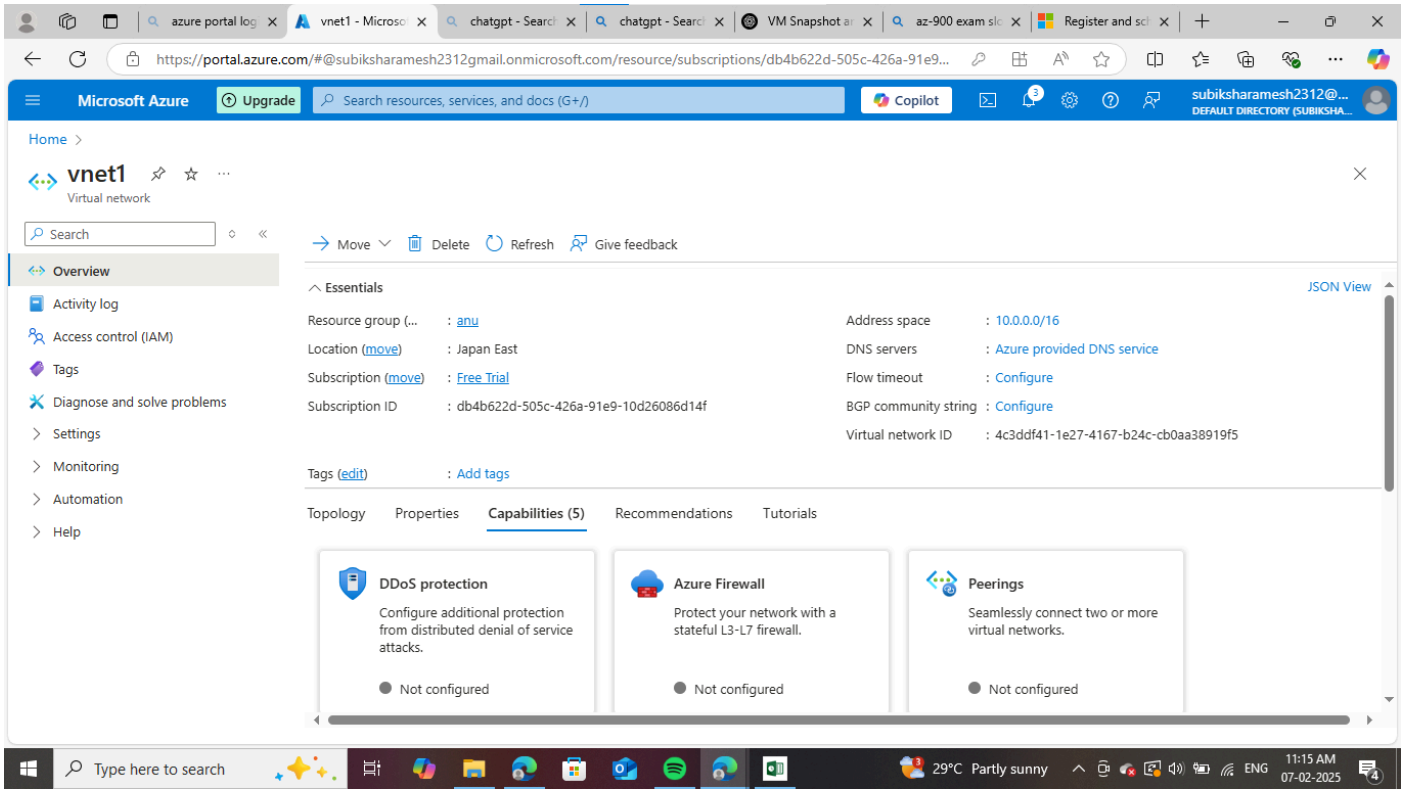
***Minimize Attack Surface**: Reduce exposure of the internal network by limiting external entry to a single, hardened point.*

***Auditing and Monitoring**: Enable logging and monitoring to track access and detect potential security issues.*

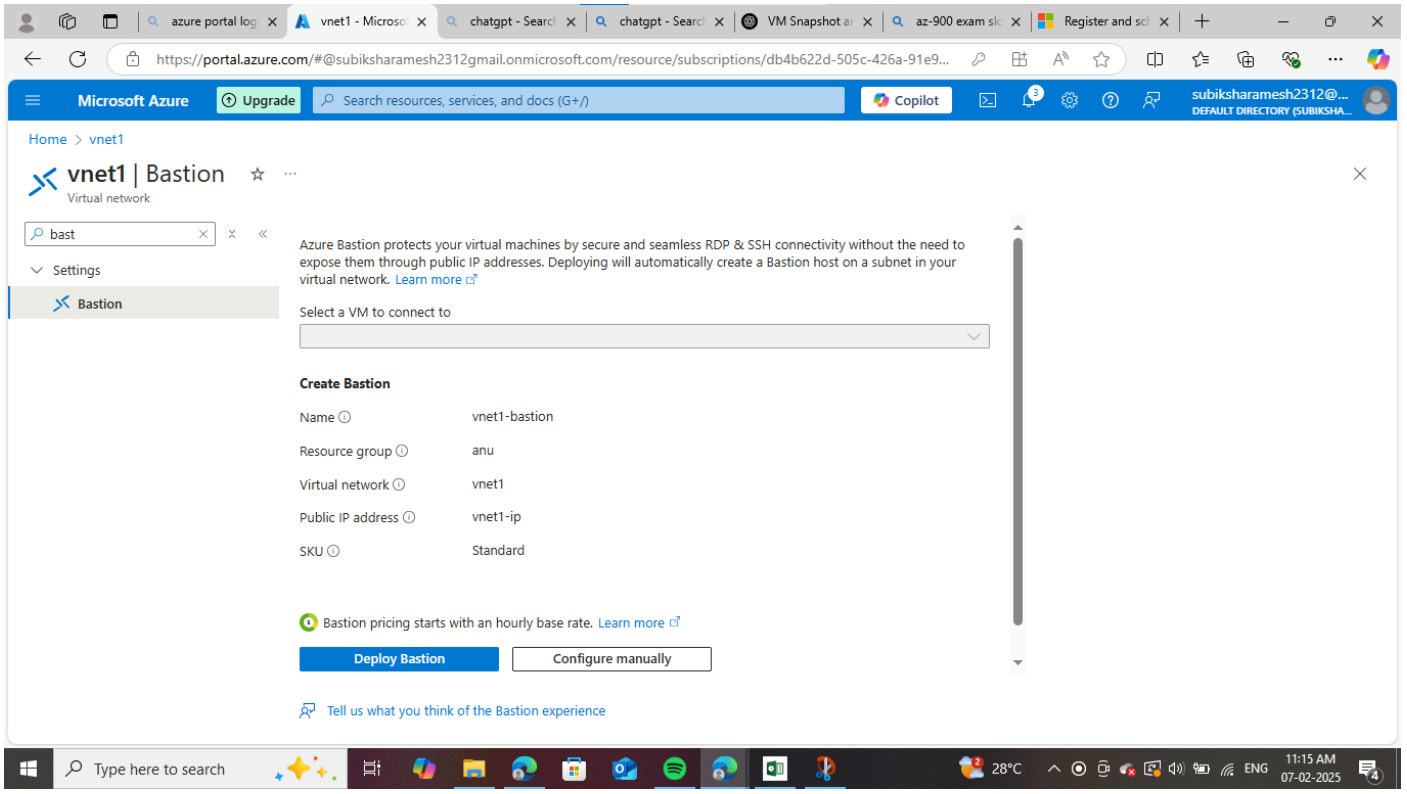
***Security Hardening**: Implement strong security measures such as multi-factor authentication, SSH key-based login, and patching to protect the Bastion Host itself.*

Step-by-Step procedure :

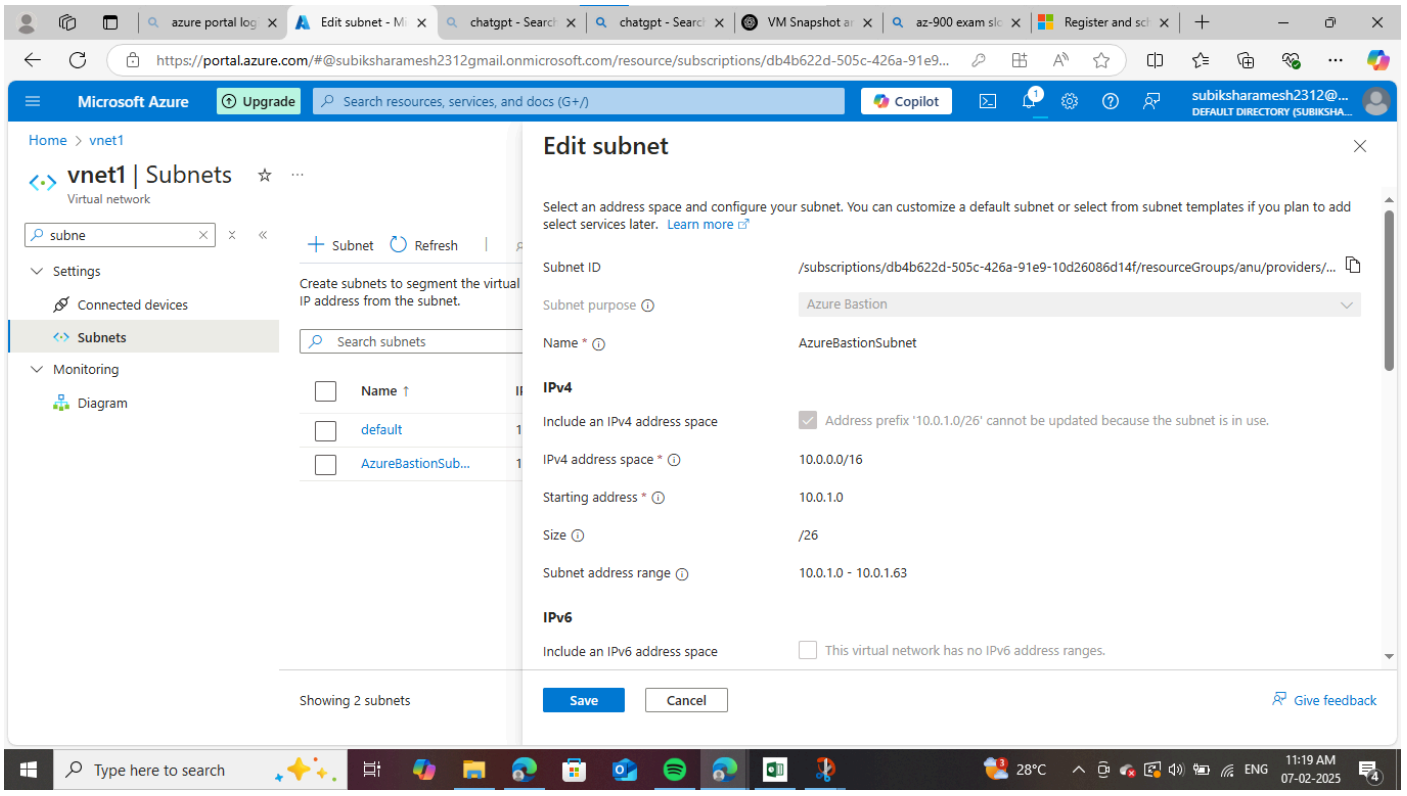
STEP 1 *:Create a vnet*



STEP 2:under vnet go to bastion,deploy the bastion with public ip,create if it doesn't already exists

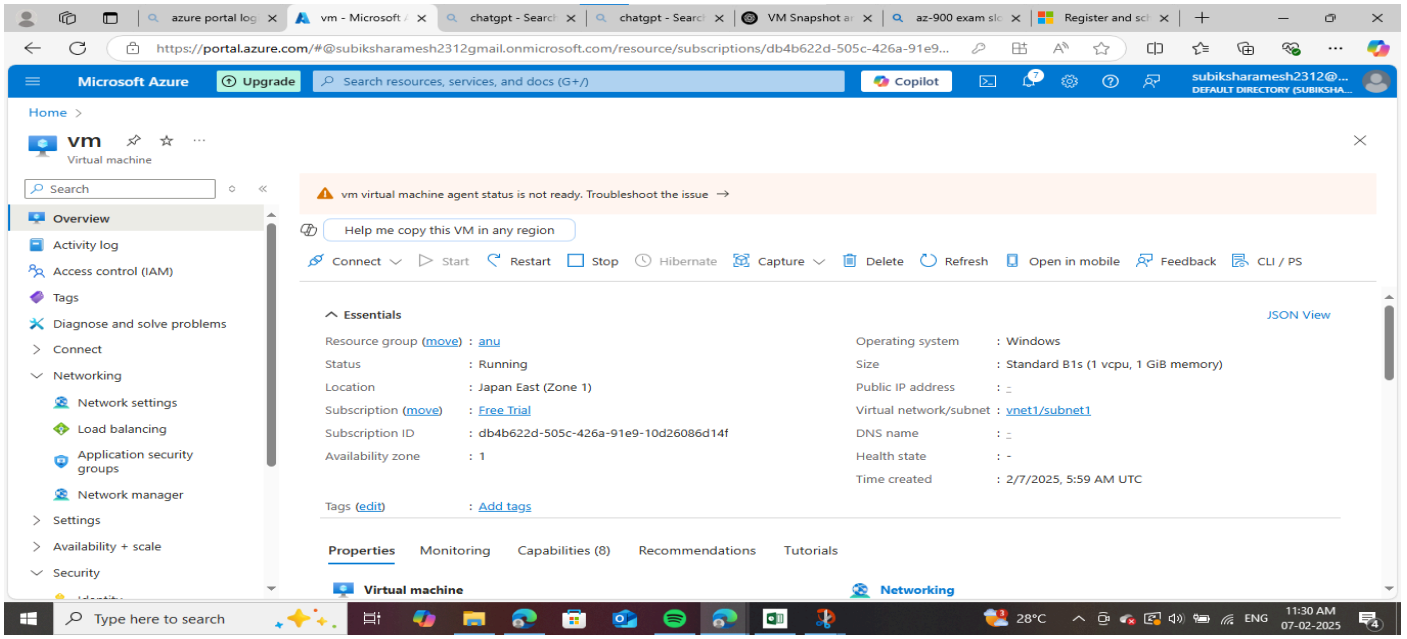


STEP 3:thus the bastion subnet will be created,now create a private subnet for virtual machine to avoid public access to internet

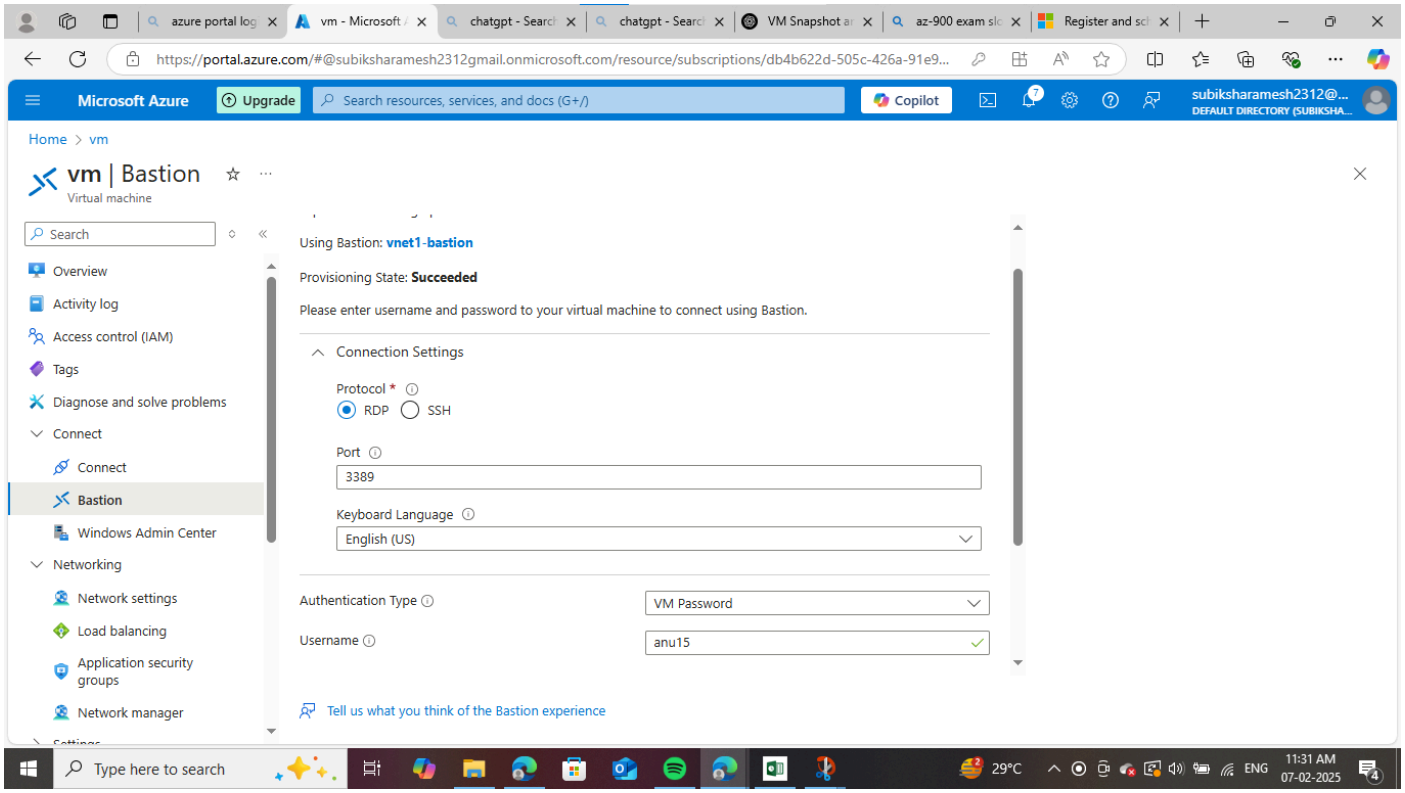


STEP 4:create a virtual machine under created private subnet

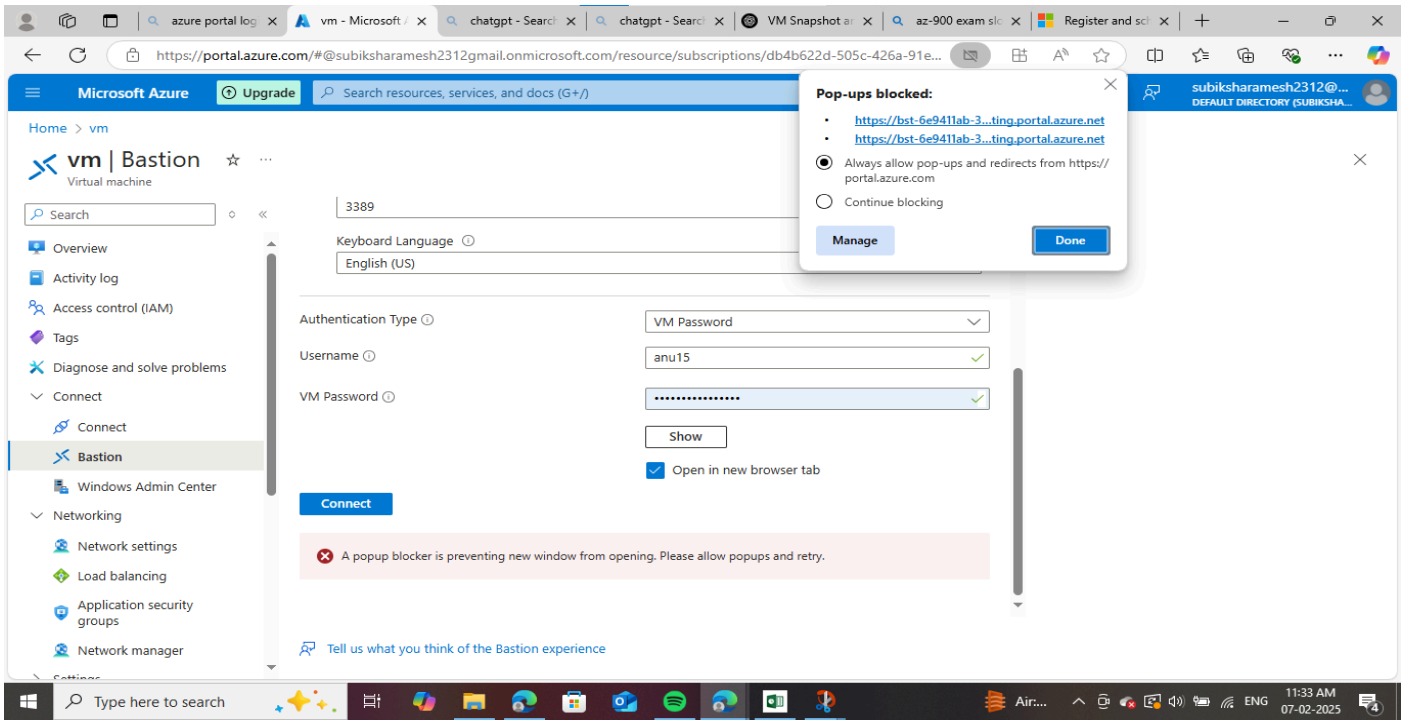
- ***disable the public-ip***



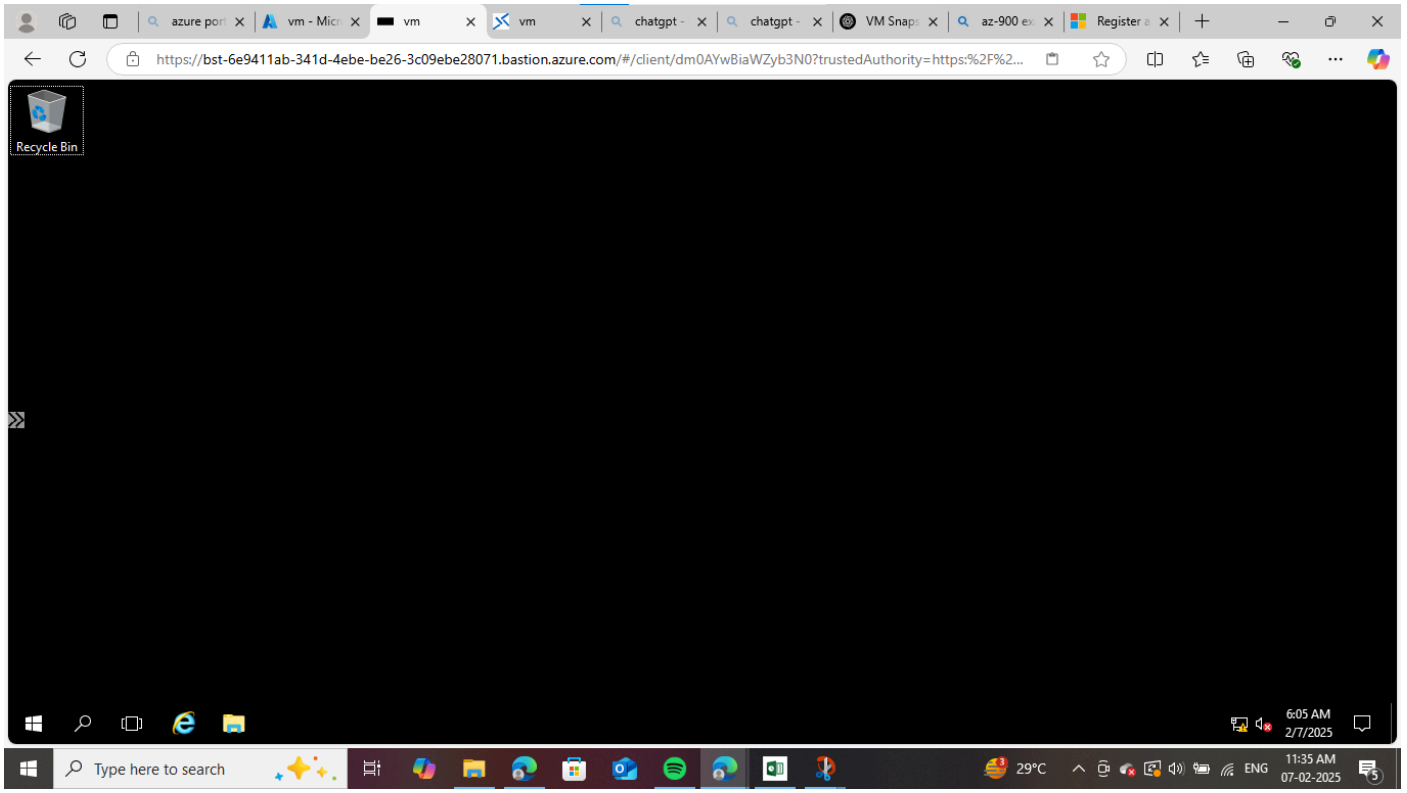
STEP 5:under created virtual machine,go to bastion authenticate it by username and password

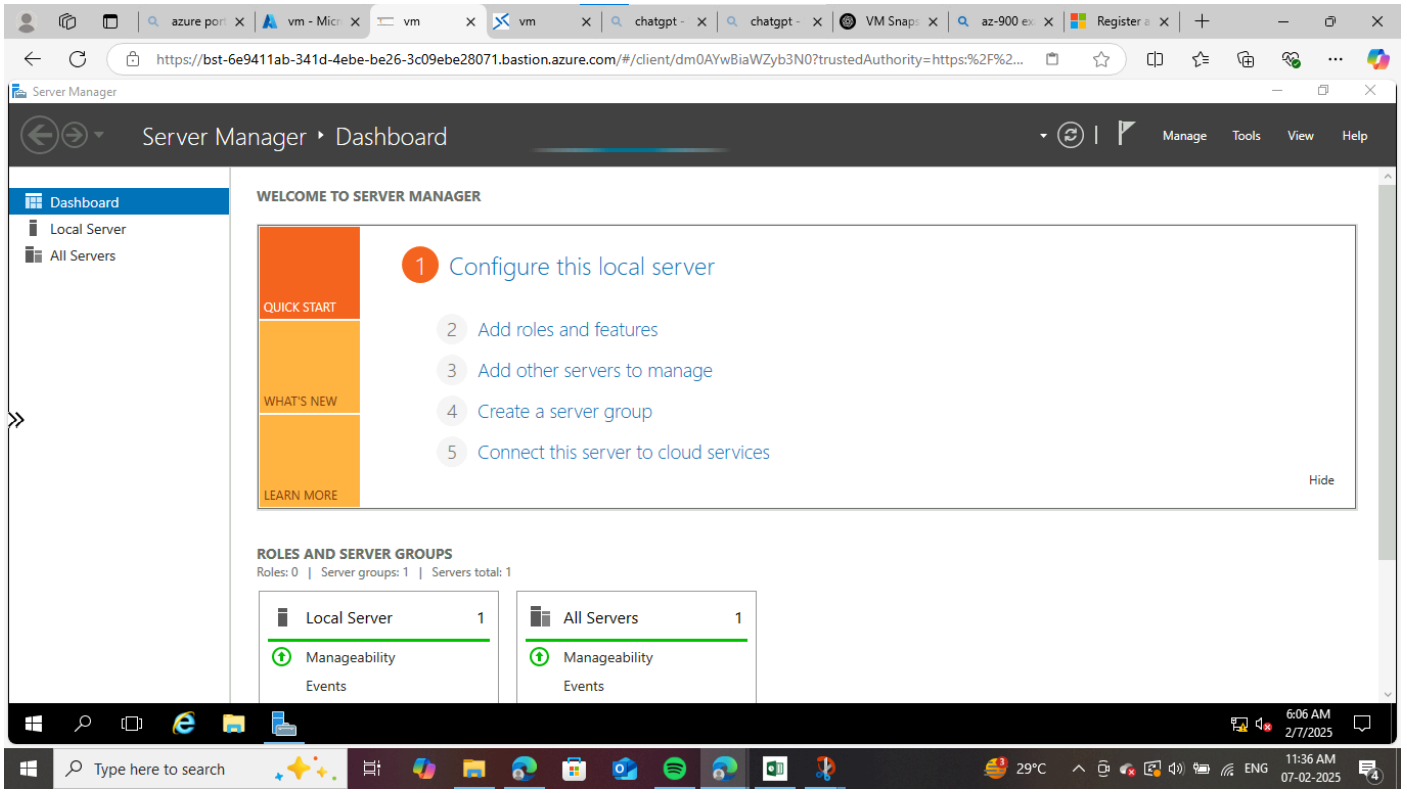


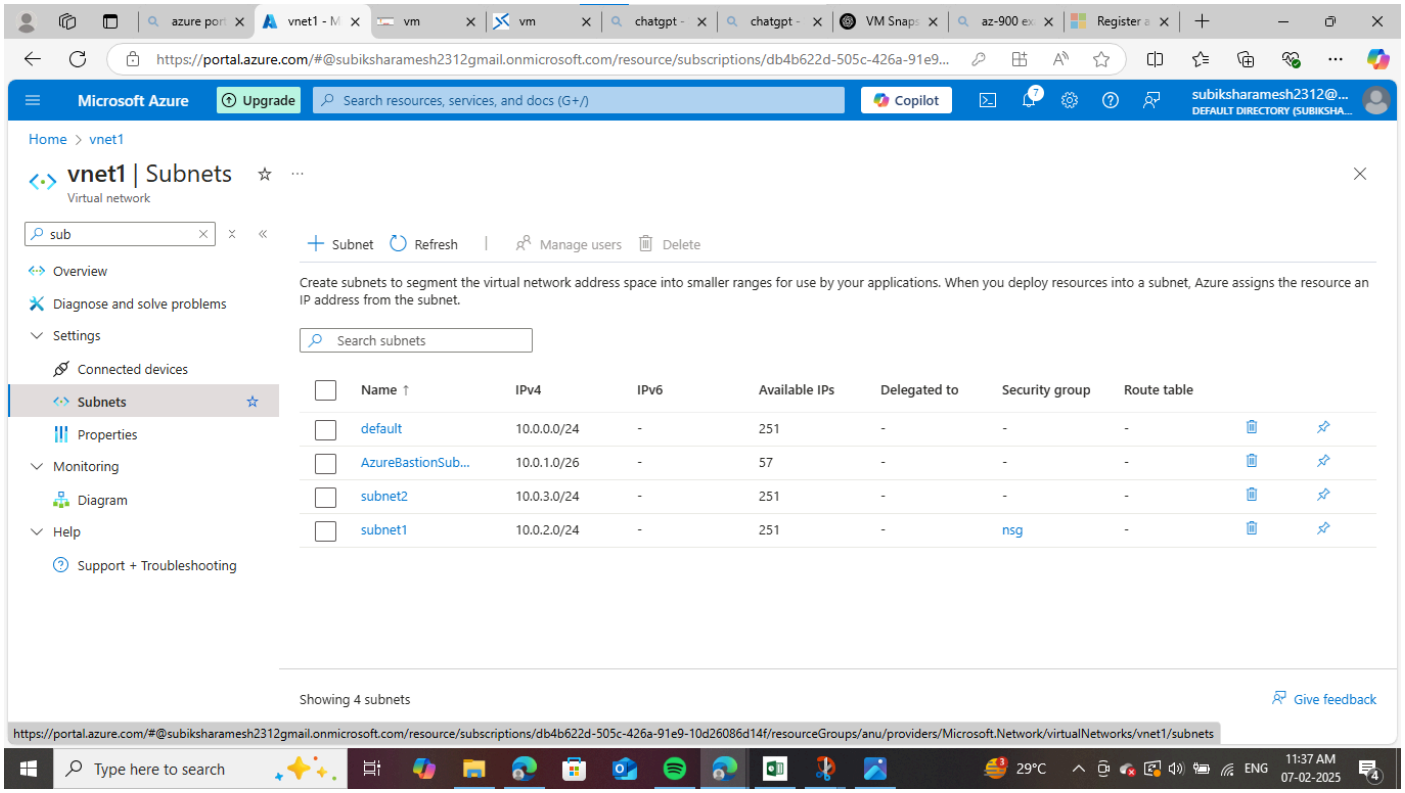
STEP 7:go to the side address bar of the window to enable the blocked pop-up



STEP 8:Hence,the virtual machine will open under the privately created bastion host







Outcome :

Creating a bastion host for a virtual machine (VM) provides a secure entry point for accessing VMs in a private subnet, reducing the need to expose them directly to the internet. The bastion host acts as a gateway, allowing authorized users to access private VMs via SSH or RDP while maintaining tighter security by isolating access to only the bastion host. This setup helps in improving security by ensuring that only one machine is publicly accessible, while all others remain protected. Additionally, it enables centralized logging and monitoring of all access, making it easier to track activity and manage security policies. With access control policies, including options like Multi-Factor Authentication (MFA), and the ability to implement strict firewall rules, the bastion host ensures that only authorized users can connect. VMs in the private subnet no longer require public IP addresses, minimizing their exposure to external threats. Furthermore, using a bastion host simplifies access management, and by opting for high availability, you can ensure uninterrupted access to the network.