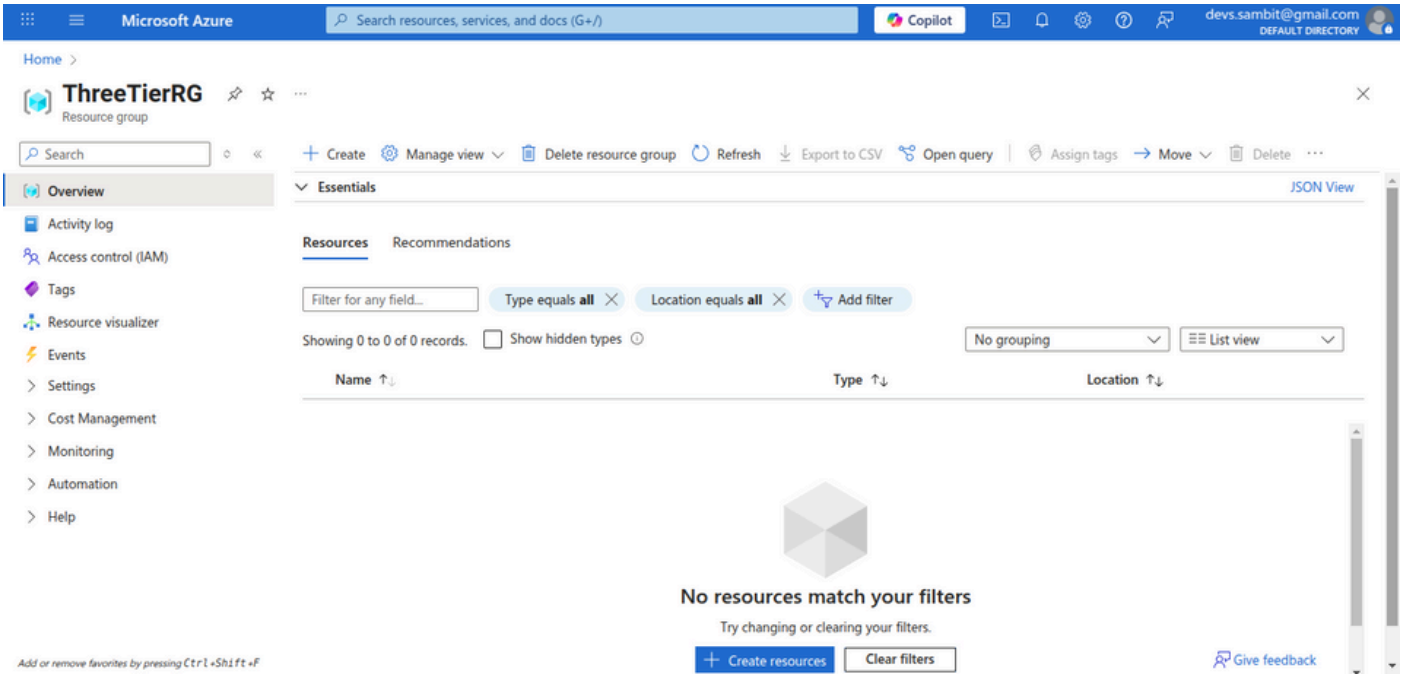
THREE TIER ARCHITECTURE

1. Create a Resource Group :

- Open your web browser and go to the Azure portal.
- In the search bar at the top, type Resource groups and select it from the results.
- Click the + Create button.
- On the "Create a resource group" page:
  - Subscription: Select your Azure subscription.
  - Resource group name: Enter ThreeTierRG.
  - Region: Choose a region geographically close to you (e.g., Central India).
- Click Review + create, then click Create.

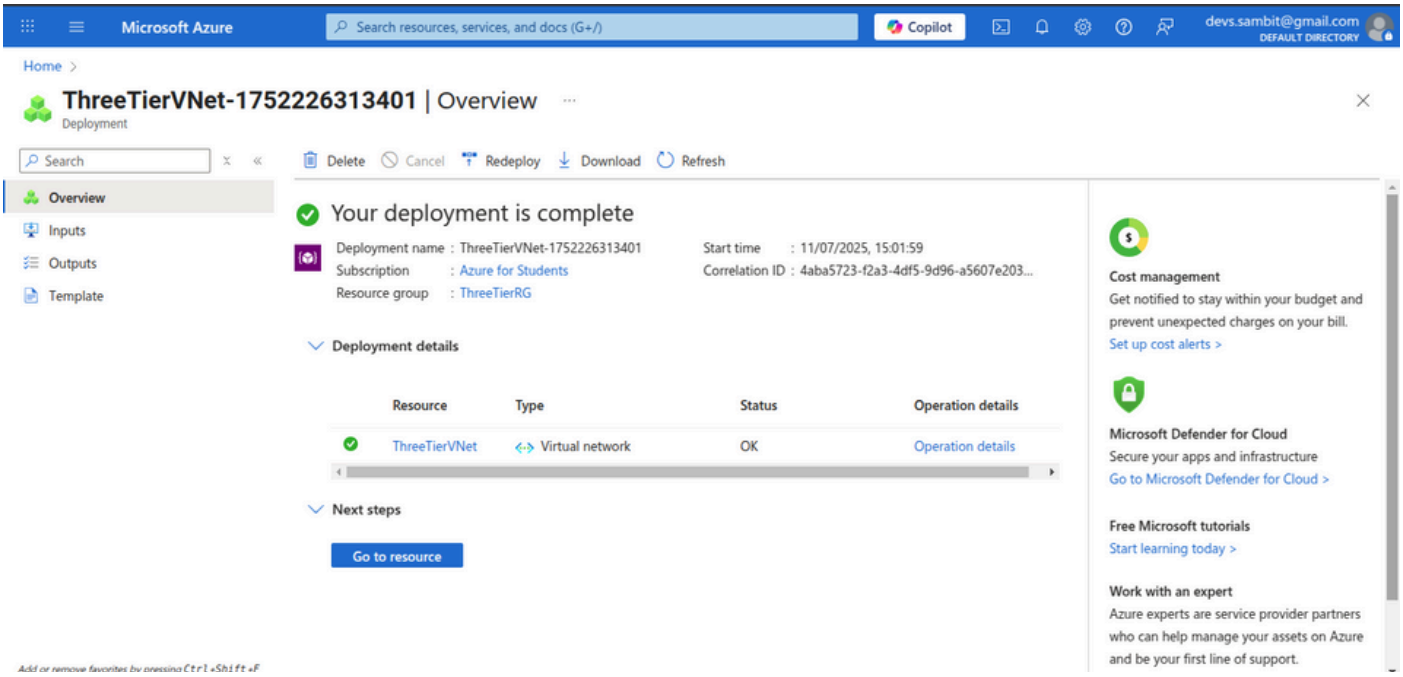


RESOURCE GROUP : THREETIERRG

2. Create a Virtual Network (VNet) :

This VNet will serve as the private network for your entire architecture.

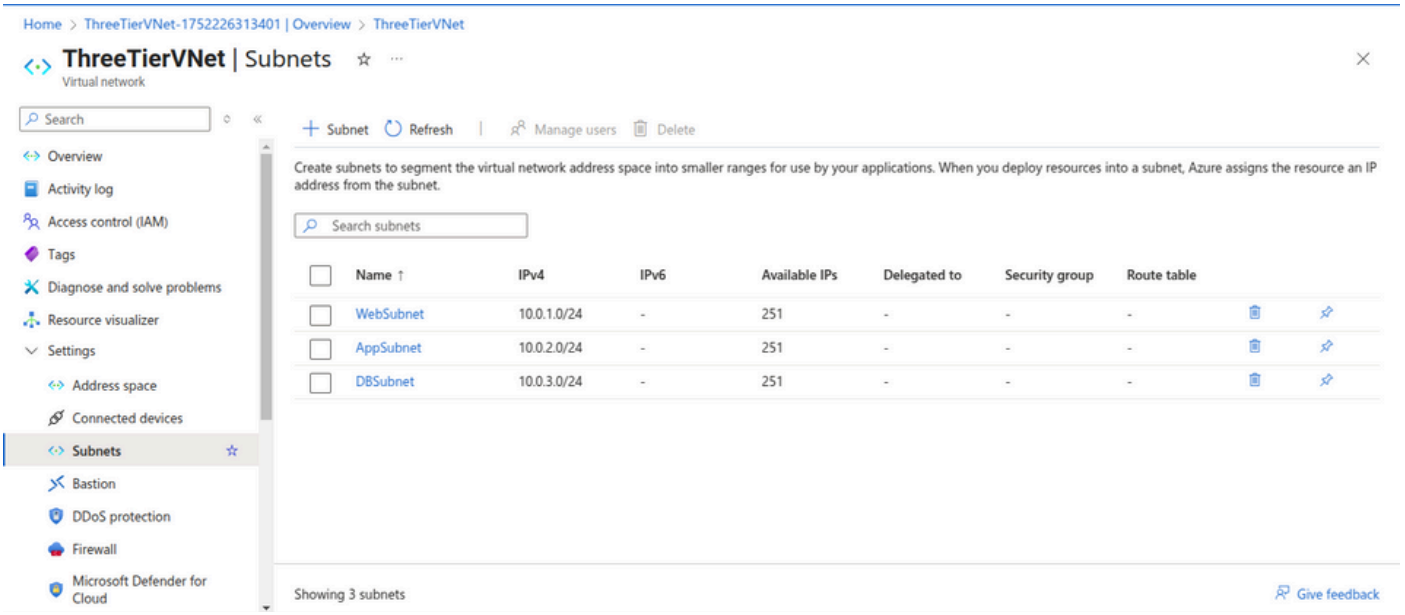
- On the "Create virtual network" page:
  - Basics Tab:
    - Subscription: Ensure your subscription is selected.
    - Resource Group: Select ThreeTierRG.
    - Name: Enter ThreeTierVNet.
  - IP Addresses Tab:
    - For IPv4 address space, ensure it's set to 10.0.0.0/16. This provides a large enough range.
    - Under Subnets, you'll see a default subnet listed. Click on the three dots ... next to it and select Remove subnet. We will create our specific subnets.
  - Click Review + create, then click Create.



VIRTUAL NETWORK : THREETIERVNET

3. Create Subnets :

- In the Azure portal search bar, type Virtual networks and select ThreeTierVNet.
- In the left-hand menu, under Settings, click on Subnets.
- Click the + Subnet button.
- For Web Tier Subnet:
  - Name: Enter WebSubnet.
  - IPv4 address range: Enter 10.0.1.0/24.
- Click + Subnet again.
- For App Tier Subnet:
  - Name: Enter AppSubnet.
  - IPv4 address range: Enter 10.0.2.0/24.
- Click + Subnet again.
- For DB Tier Subnet:
  - Name: Enter DBSubnet.
  - IPv4 address range: Enter 10.0.3.0/24.

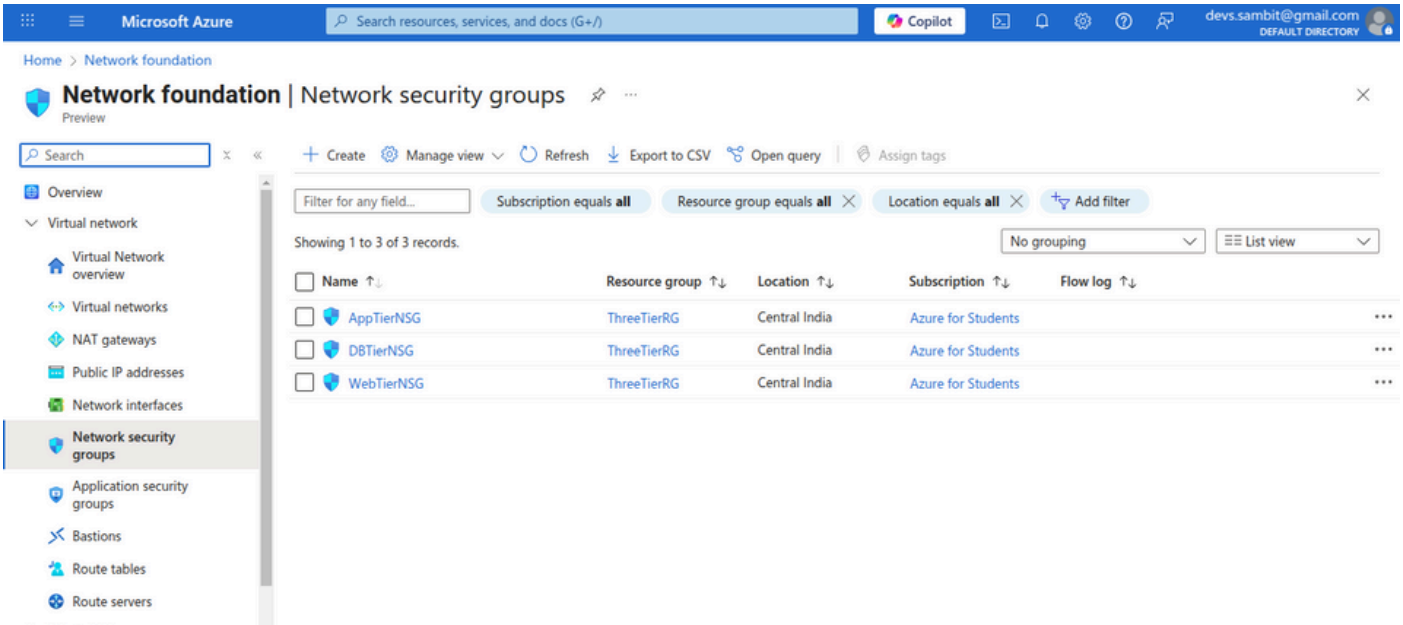


SUBNETS : APP, DB, WEB

4. Create Network Security Groups (NSGs)

You'll create one NSG for each tier to control network traffic.

1. In the Azure portal search bar, type Network security groups and select it.
2. Click the + Create button.
3. For Web Tier NSG:
    - Subscription: Select your subscription.
    - Resource Group: Select ThreeTierRG.
    - Name: Enter WebTierNSG.
    - Region: Select the same region as your VNet and Resource Group.
    - Click Review + create, then click Create.
4. Repeat the above steps to create the following NSGs, ensuring they are in ThreeTierRG and the same region:
    - Name: AppTierNSG
    - Name: DBTierNSG



NSG : APP, DB, WEB

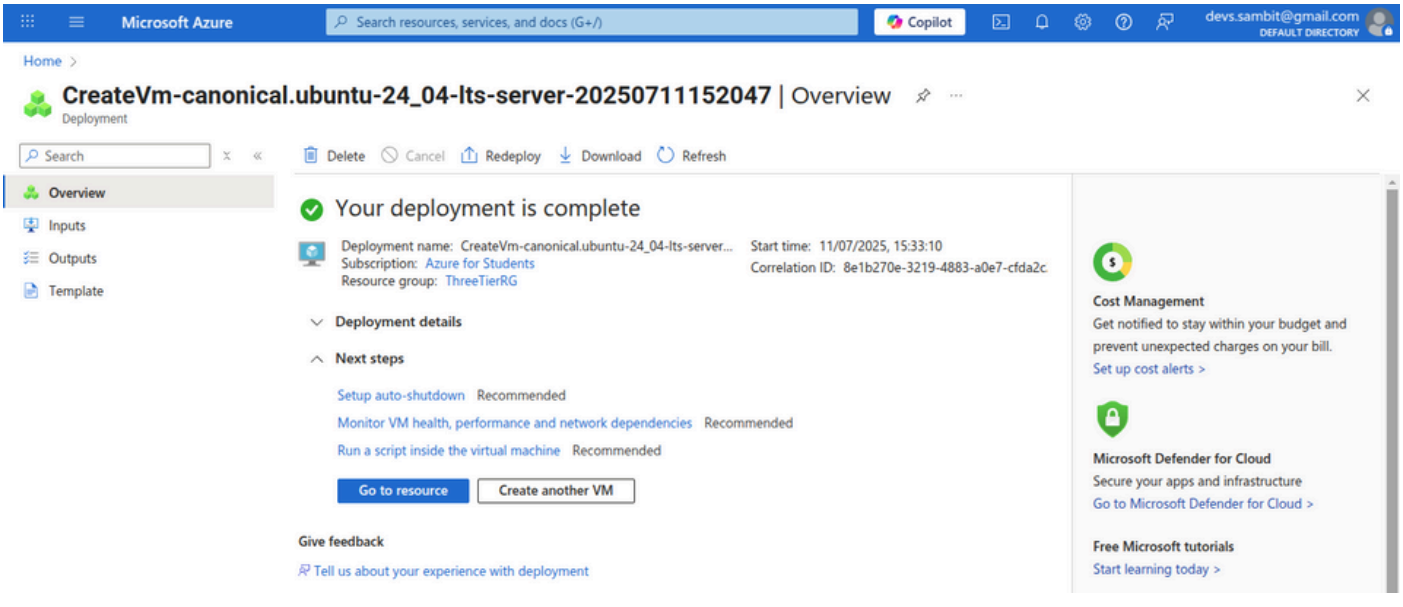
5. Deploy Virtual Machines (VMs)

You will deploy two VMs in each subnet: one Linux and one Windows. Crucial: Pay close attention to the Public IP setting for each VM to ensure only the Web Tier VMs are internet-facing.

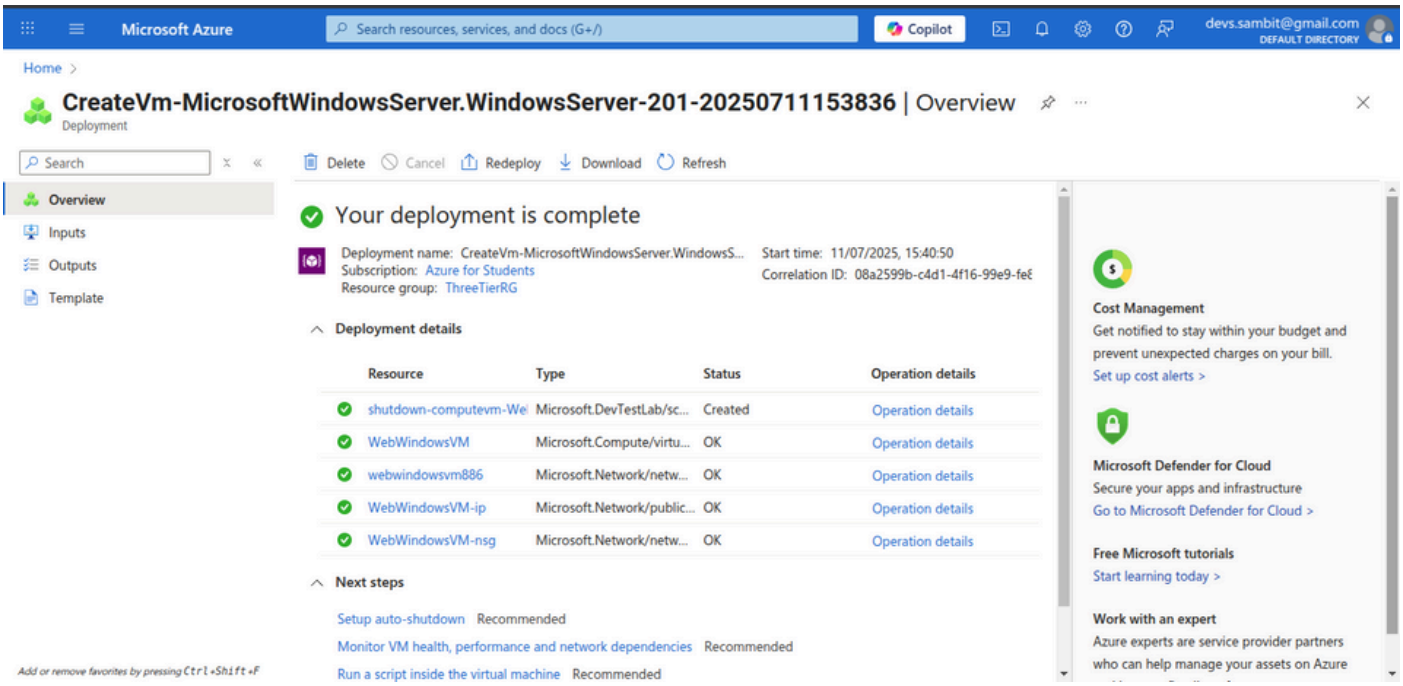
5.1. Deploy Web Tier VMs (WebSubnet) :

Click the + Create button, then select Azure virtual machine.

- **Web Tier - Linux VM (Apache):**
  - Basics Tab:
    - Virtual machine name: WebLinuxVM
    - Image: Select Ubuntu Server 24.04 LTS.
    - Size: Choose a suitable size.
    - Authentication type: Select SSH public key.
  - Networking Tab:
    - Subnet: Select WebSubnet.
    - Public IP: Select (New).
    - NIC network security group: Select Basic.
    - Public inbound ports: Select Allow selected ports.
    - Select inbound ports: Check HTTP (80), HTTPS (443), and SSH (22).



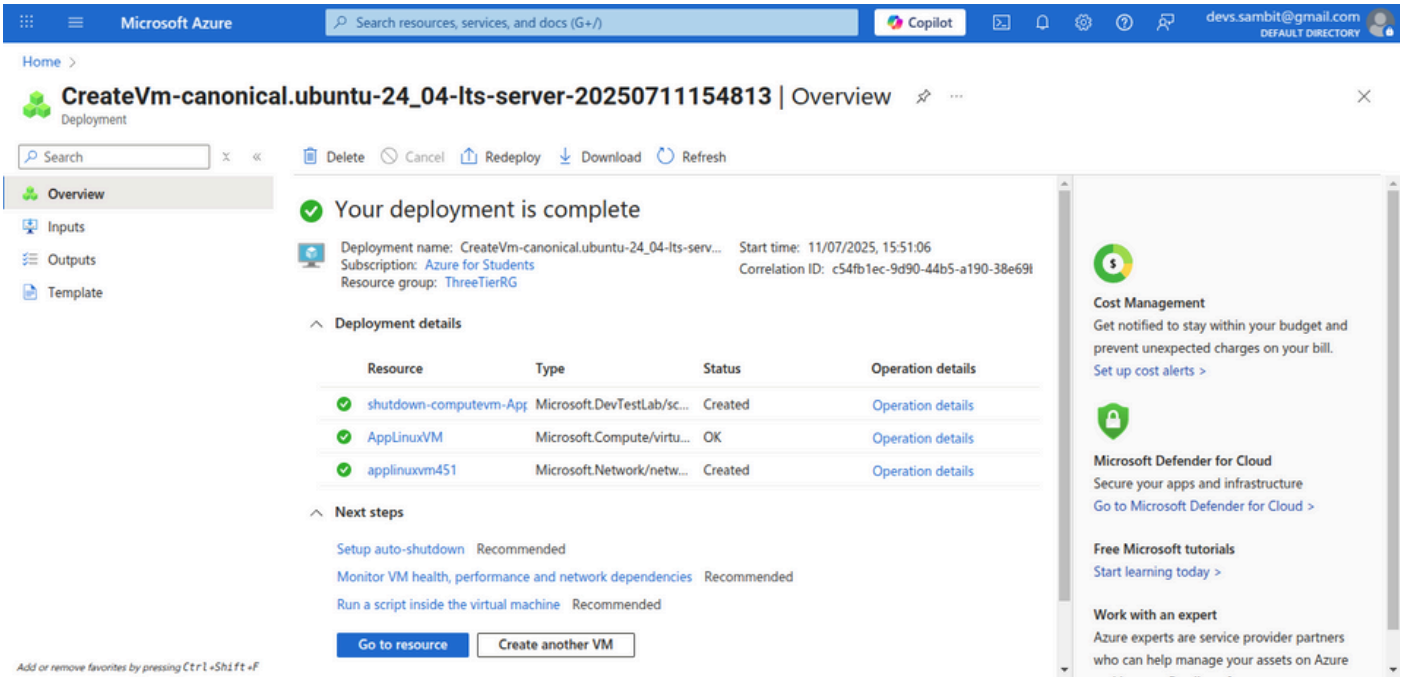
- **Web Tier - Windows VM (IIS):**
- Basics Tab:
  - Virtual machine name: WebWindowsVM
  - Image: Select Windows Server 2019 Datacenter.
  - Size: Choose a suitable size.
  - Administrator account: Create a username and password.
- Networking Tab:
  - Subnet: Select WebSubnet.
  - Public IP: Select (New).
  - NIC network security group: Select Basic.
  - Public inbound ports: Select Allow selected ports.
  - Select inbound ports: Check HTTP (80), HTTPS (443), and RDP (3389).



5.2. Deploy App Tier VMs (AppSubnet) :

1. Repeat the VM creation process : App Tier - Linux VM
    - Basics Tab: Virtual machine name: AppLinuxVM.
    - Select appropriate Image, Size, and credentials.

- Networking Tab:
    - Subnet: Select AppSubnet.
    - Public IP: Select None. (This is critical: App and DB tiers should not have direct internet access).
    - NIC network security group: Select None.
    - Click Review + create, then click Create.

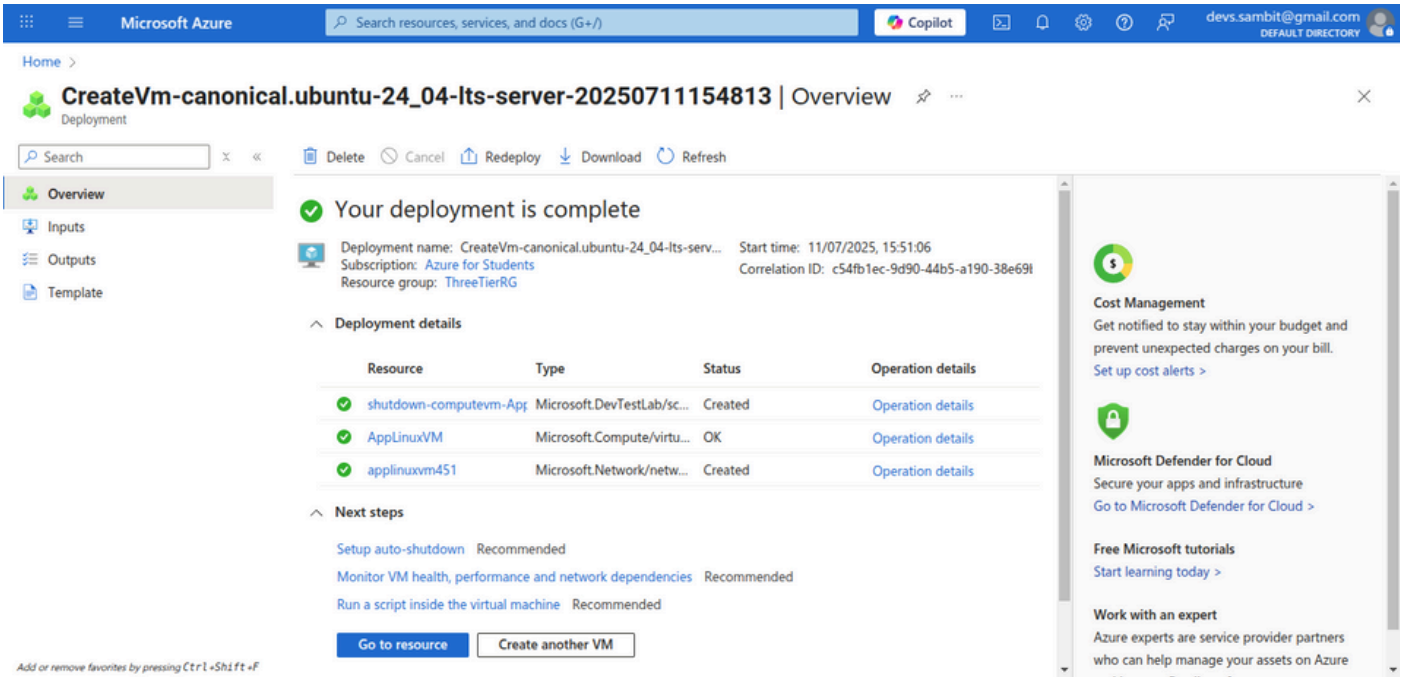


- **App Tier - Windows VM:**
    - Basics Tab: Virtual machine name: AppWindowsVM. Select appropriate Image, Size, and credentials.
    - Networking Tab:
        - Subnet: Select AppSubnet.
        - Public IP: Select None.
        - NIC network security group: Select None.

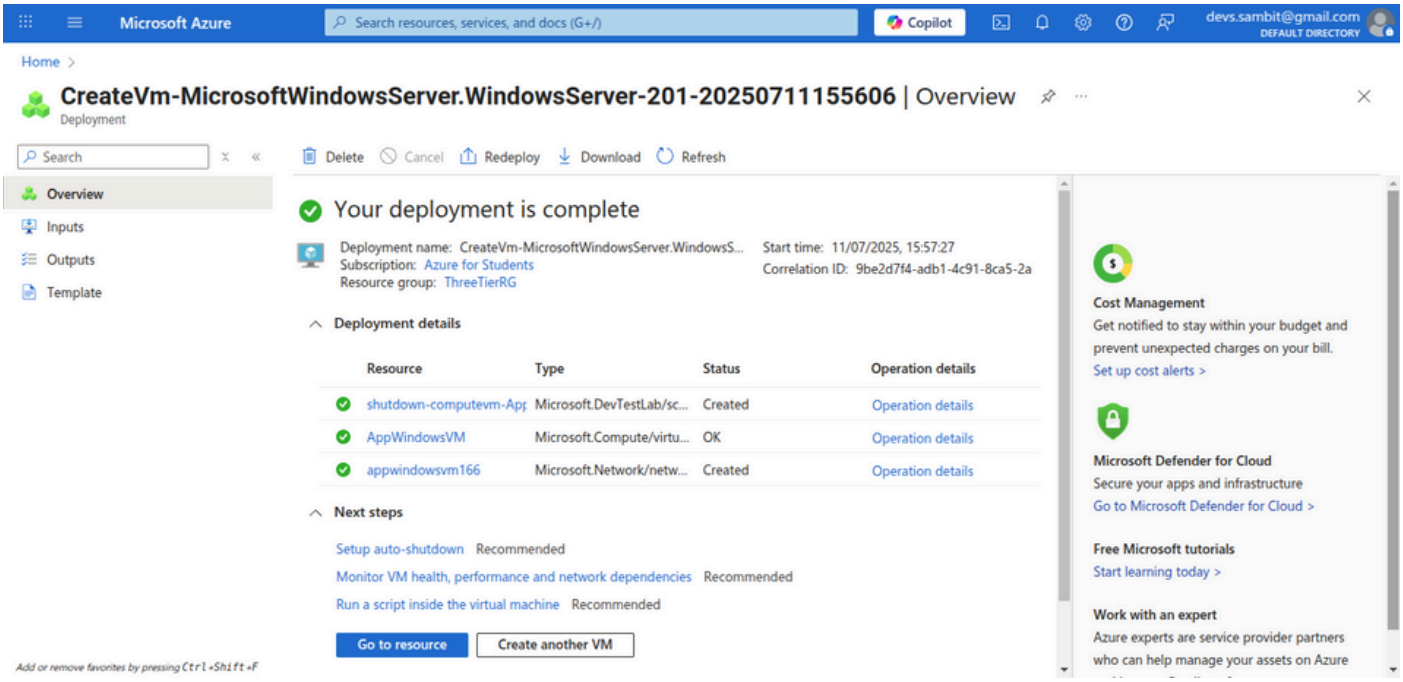
5.2. Deploy App Tier VMs (AppSubnet) :

1. Repeat the VM creation process : App Tier - Linux VM
    - Basics Tab: Virtual machine name: AppLinuxVM.
    - Select appropriate Image, Size, and credentials.

- Networking Tab:
    - Subnet: Select AppSubnet.
    - Public IP: Select None. (This is critical: App and DB tiers should not have direct internet access).
    - NIC network security group: Select None.
    - Click Review + create, then click Create.

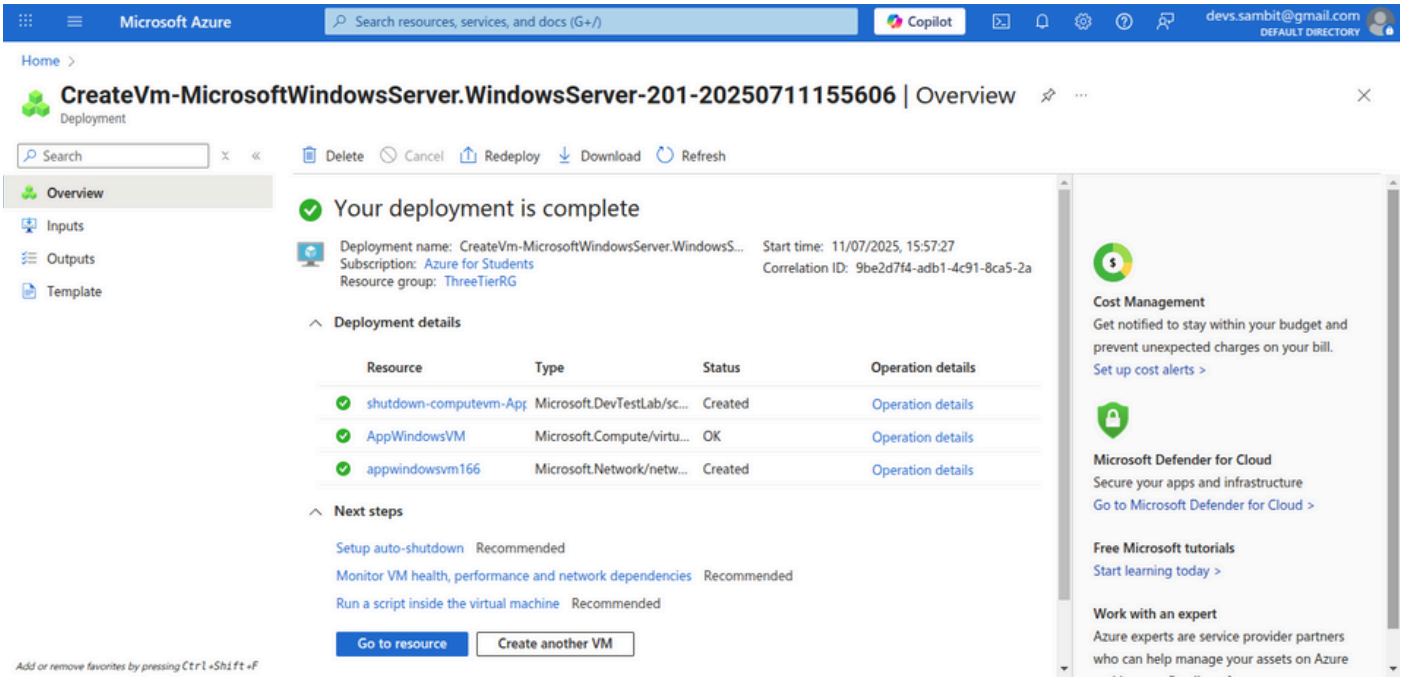


- **App Tier - Windows VM:**
    - Basics Tab: Virtual machine name: AppWindowsVM. Select appropriate Image, Size, and credentials.
    - Networking Tab:
        - Subnet: Select AppSubnet.
        - Public IP: Select None.
        - NIC network security group: Select None.



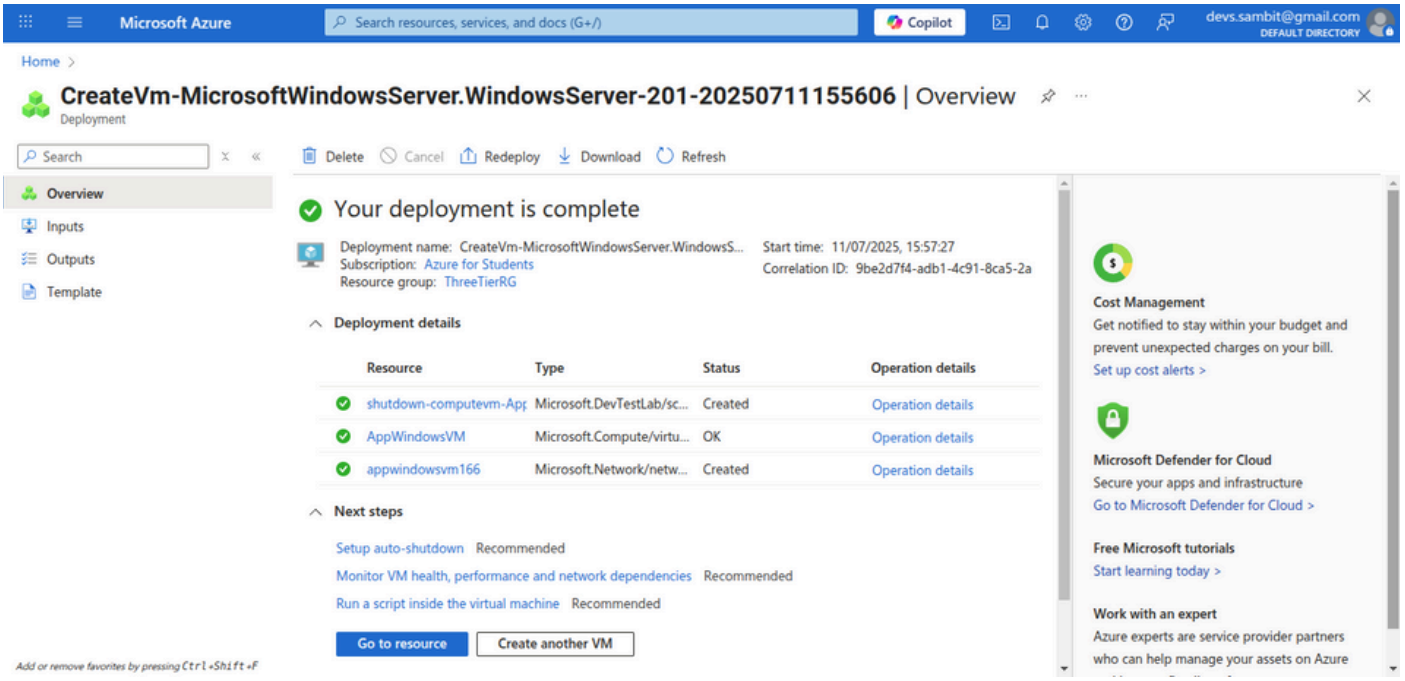
5.3. Deploy DB Tier VMs (DBSubnet) :

1. Repeat the VM creation process. DB Tier - Linux VM:
    - Basics Tab: Virtual machine name: DBLinuxVM. Select appropriate Image, Size, and credentials.
    - Networking Tab:
        - Subnet: Select DBSubnet.
        - Public IP: Select None.
        - NIC network security group: Select None.



DB Tier - Windows VM :

- Basics Tab: Virtual machine name: DBWindowsVM. Select appropriate Image, Size, and credentials.
- Networking Tab:
  - Virtual network: ThreeTierVNet.
  - Subnet: Select DBSubnet.
  - Public IP: Select None.
  - NIC network security group: Select None.



6. Associate NSGs with Subnets

Now, link each NSG you created to its respective subnet.

1. Type Virtual networks and select it. Click on ThreeTierVNet.
2. Click on Subnets, Click on the WebSubnet.
3. Under NSG, select WebTierNSG from the dropdown list. Click Save.
4. Repeat this process for the other subnets:
   - Click on AppSubnet, then associate AppTierNSG. Click Save.
   - Click on DBSubnet, then associate DBTierNSG. Click Save.

7. Configure NSG Rules :

This is the most critical part, defining exactly how traffic flows between your tiers and to/from the internet.

7.1. Configure Web Tier NSG (WebTierNSG) Rules

This NSG allows inbound internet traffic (HTTP/HTTPS) and outbound traffic to the App Tier and the internet, Click on WebTierNSG

Inbound Security Rules:

- Click + Add.
    - Allow HTTP from Internet:
        - Source: Any
        - Source port ranges: *
        - Destination: Any
        - Destination port ranges: 80
        - Protocol: TCP
        - Action: Allow
        - Priority: 100 (Lower number = higher priority)
        - Name: Allow_HTTP_Internet
        - Click Add.
    - Allow HTTPS from Internet:
        - Same as above...
        - Destination port ranges: 443
        - Priority: 110
        - Name: Allow_HTTPS_Internet
        - Click Add.

- Allow SSH/RDP from your IP (for management):
  - Source: My IP address
  - Destination port ranges: 22, 3389
  - Protocol: Any
  - Priority: 120
  - Name: Allow_Mgmt_Internet
  - Click Add.

Outbound Security Rules:

- Click + Add.
  - Allow Outbound to App Tier:
    - Source: Any
    - Source port ranges: *
    - Destination: IP Addresses
    - Destination IP addresses/CIDR ranges: 10.0.2.0/24 (This is the AppSubnet CIDR)
    - Destination port ranges: 8080, 443 (Common application ports. Adjust if your app uses different ports).
    - Protocol: TCP
    - Action: Allow
    - Priority: 100
    - Name: Allow_Web_to_App
    - Click Add.
  -

- Allow Outbound to Internet: (This is often a default rule, but confirm or add if missing).
  - Destination: Service Tag -> Internet
  - Destination port ranges: *
  - Protocol: Any
  - Action: Allow
  - Priority: 110 (Ensure this priority is lower than any potential deny rules you might add later).
  - Name: Allow_Outbound_Internet
  - Click Add.

7.2. Configure App Tier NSG (AppTierNSG) Rules :

This NSG allows inbound from the Web Tier, outbound to the DB Tier, and denies direct internet access, navigate to AppTierNSG.

Inbound Security Rules:

- Allow Inbound from Web Tier:
  - Source: IP Addresses
  - Source IP addresses: 10.0.1.0/24 (This is the WebSubnet CIDR)
  - Source port ranges: *
  - Destination: Any
  - Destination port ranges: 8080, 443
  - Protocol: TCP
  - Action: Allow
  - Priority: 100
  - Name: Allow_Web_to_App

- Allow RDP/SSH from Web Tier (for management traversal):
  - Destination port ranges: 22, 3389
  - Protocol: Any
  - Priority: 110
  - Name: Allow_Web_to_App_Mgmt

Outbound Security Rules:

- Allow Outbound to DB Tier:
  - Destination IP addresses: 10.0.3.0/24 (This is the DBSubnet CIDR)
  - Destination port ranges: 3306 (for MySQL), 1433 (for SQL Server), 5432 (for PostgreSQL) - choose the port relevant to your database.
  - Protocol: TCP
  - Action: Allow
  - Priority: 100
  - Name: Allow_App_to_DB
- Deny Outbound to Internet:
  - Source: Any
  - Source port ranges: *
  - Destination: Service Tag -> Internet
  - Destination port ranges: *
  - Protocol: Any
  - Action: Deny
  - Priority: 1000 (Make this a high number so it's evaluated last, catching anything not explicitly allowed).
  - Name: Deny_App_to_Internet

7.3. Configure DB Tier NSG (DBTierNSG) Rules :

This NSG allows inbound only from the App Tier and denies all outbound traffic to Web/App tiers and the internet, navigate to DBTierNSG.

Inbound Security Rules:

- Allow Inbound from App Tier:
  - Source: IP Addresses
  - Source IP addresses/CIDR: 10.0.2.0/24 (This is the AppSubnet CIDR)
  - Source port ranges: *
  - Destination: Any
  - Destination port ranges: 3306 (for MySQL), 1433 (for SQL Server), 5432 (for PostgreSQL) - choose the port relevant to your database.
  - Protocol: TCP
  - Action: Allow
  - Priority: 100
  - Name: Allow_App_to_DB
- Allow RDP/SSH from App Tier (for management traversal):
  - Source: IP Addresses
  - Source IP addresses/CIDR ranges: 10.0.2.0/24
  - Source port ranges: *
  - Destination: Any
  - Destination port ranges: 22, 3389
  - Protocol: Any
  - Action: Allow
  - Priority: 110
  - Name: Allow_App_to_DB_Mgmt

Outbound Security Rules:

- Deny Outbound to Web Tier:
  - Source: Any
  - Source port ranges: *
  - Destination: IP Addresses
  - Destination IP addresses/CIDR ranges: 10.0.1.0/24 (WebSubnet CIDR)
  - Destination port ranges: *
  - Protocol: Any
  - Action: Deny
  - Priority: 100
  - Name: Deny_DB_to_Web
- Deny Outbound to App Tier:
  - Destination IP addresses/CIDR ranges: 10.0.2.0/24 (AppSubnet CIDR)
  - Priority: 110
  - Name: Deny_DB_to_App
- Deny Outbound to Internet:
  - Source: Any
  - Source port ranges: *
  - Destination: Service Tag -> Internet
  - Destination port ranges: *
  - Protocol: Any
  - Action: Deny
  - Priority: 120
  - Name: Deny_DB_to_Internet

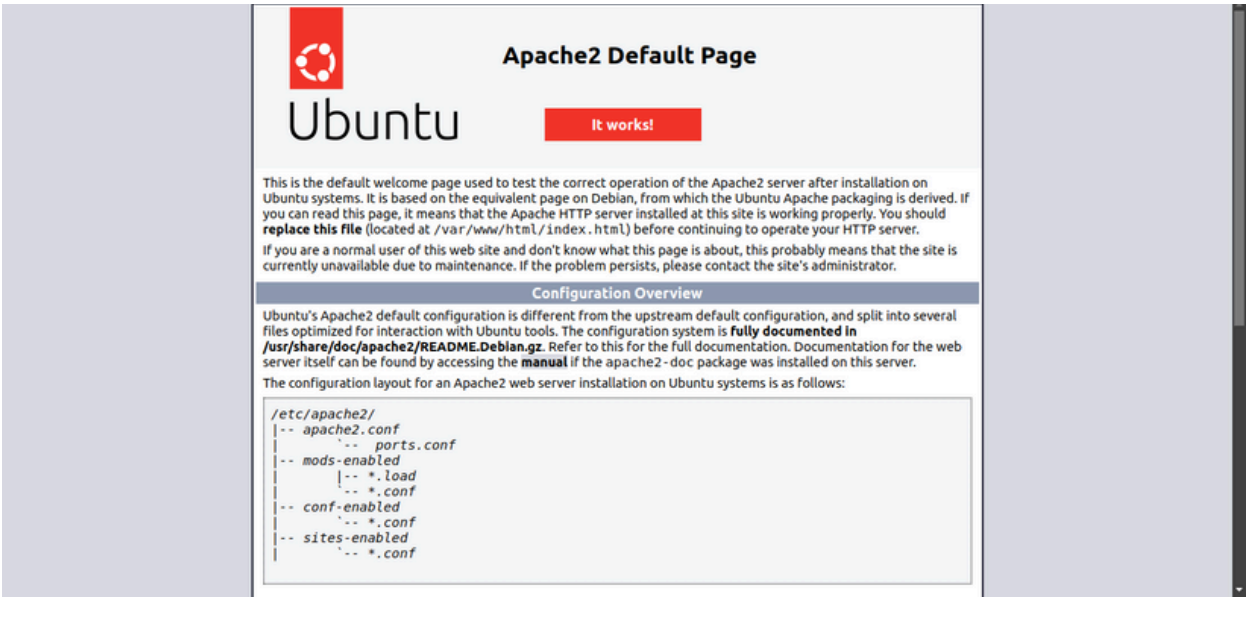
8. Configure Apache and IIS Servers :

After all networking is in place, configure the web servers on your Web Tier VMs.

8.1. Configure Apache on WebLinuxVM :

1. Get Public IP: WebLinuxVM. Note its Public IP address.
2. Connect via SSH: ssh your_username@<WebLinuxVM_Public_IP>
3. Update packages:sudo apt update
4. Install Apache: sudo apt install apache2 -y
5. Verify Apache status: sudo systemctl status apache2
6. You should see "active (running)".
7. Test: Open a web browser on your local machine and navigate to the Public IP of WebLinuxVM. You should see the default Apache welcome page.
8. **The process of setup is same for all Linux VMs.**

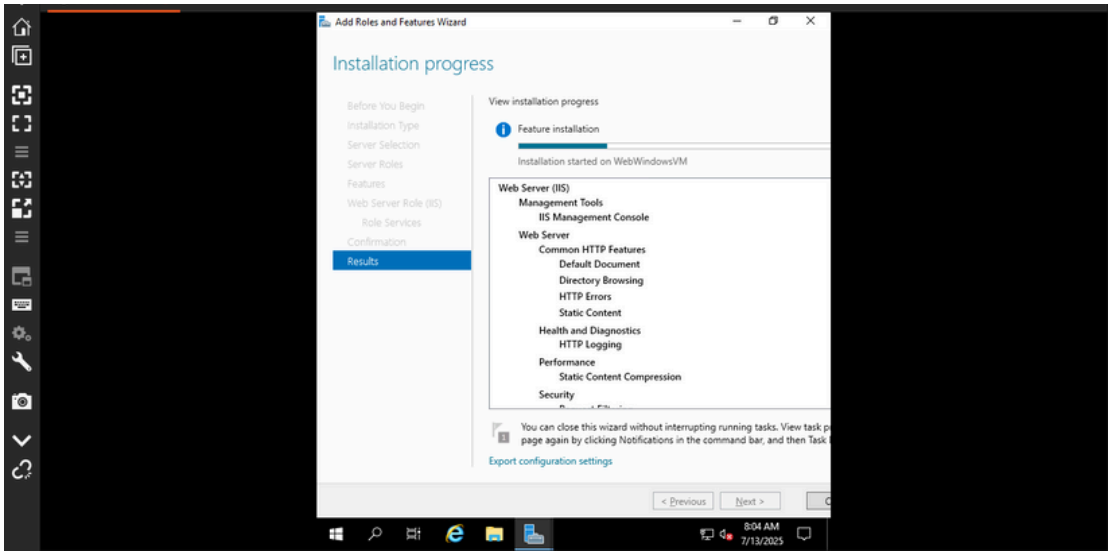
```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-07-13 07:43:14 UTC; 18s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2237 (apache2)
      Tasks: 55 (limit: 1056)
     Memory: 5.3M (peak: 5.6M)
        CPU: 33ms
     CGroup: /system.slice/apache2.service
             ├─2237 /usr/sbin/apache2 -k start
             ├─2240 /usr/sbin/apache2 -k start
             └─2241 /usr/sbin/apache2 -k start

Jul 13 07:43:14 WebLinuxVM systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jul 13 07:43:14 WebLinuxVM systemd[1]: Started apache2.service - The Apache HTTP Server.
```



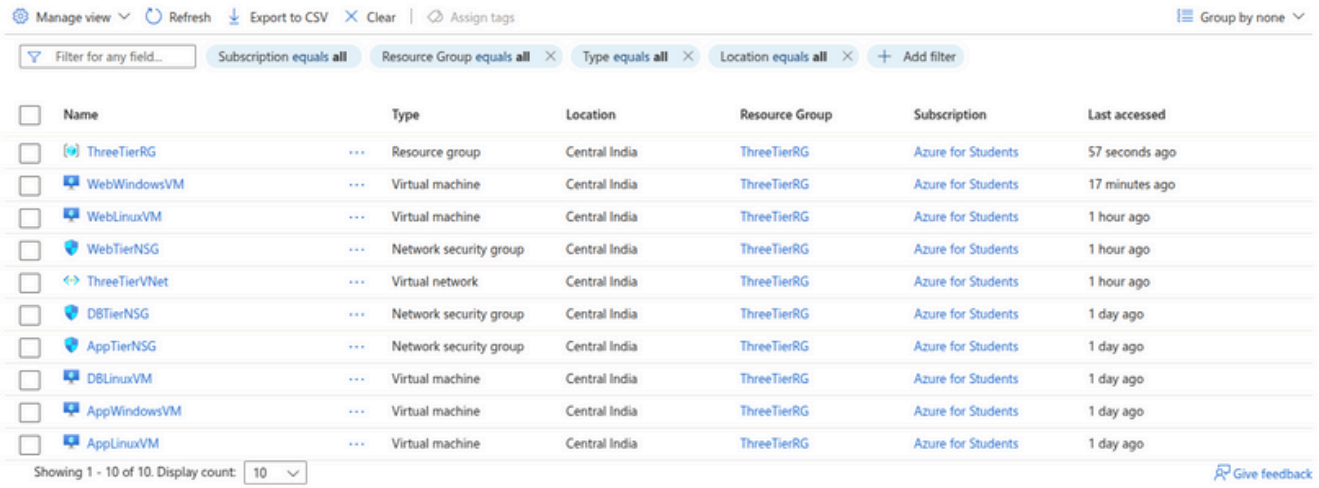
8.2. Configure IIS on WebWindowsVM :

1. Get Public IP: WebWindowsVM. Note its Public IP address.
2. Connect via RDP: Use a Remote Desktop client on your local machine to connect using the Public IP and the admin credentials you set up.
3. Install IIS:
    - Once logged into the VM, open Server Manager and add roles and features.
    - On the Server Selection page, ensure WebWindowsVM is selected.
    - On the Server Roles page, check the box next to Web Server (IIS).
    - A dialog will appear asking to add features required for IIS. Click Add.
    - Click Next until you reach the Confirmation page and click Install.
4. Verify IIS status: Once the installation completes, open a web browser on the VM itself and navigate to http://localhost. You should see the default IIS welcome page.
5. Test from outside: Open a web browser on your local machine and navigate to the Public IP of WebWindowsVM. You should see the default IIS welcome page.
6. **The process of setup is same for all Windows VMs.**

You have now successfully set up your three-tier architecture in Azure with the specified network segmentation and server configurations.



CONCLUSION



- Successfully deployed a robust three-tier application architecture in Azure.
- **Network Segmentation:** Effectively isolating application components into distinct subnets (Web, App, DB tiers) for enhanced security and organization.
- Traffic Control: Implementing NSGs to precisely manage inbound and outbound traffic, ensuring only authorized communication paths exist.
- Virtual Machine Deployment: Provisioning and configuring both Linux (Apache) and Windows (IIS) virtual machines to serve specific roles.
- Secure Connectivity: Establishing controlled access for management while limiting public exposure to only the necessary web services.

Submitted by:

Sambit Kumar Panda

References:

https://www.google.com/search?q=https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview%23resource-groups
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet
https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview
https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-machines/overview
https://learn.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows
https://learn.microsoft.com/en-us/azure/virtual-machines/windows/connect-rdp