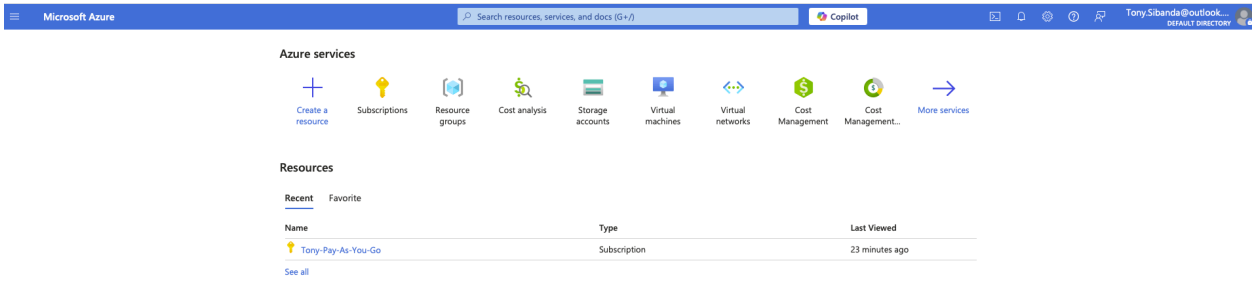
Creating Windows and Linux Virtual Machines on Microsoft Azure

---

- A Windows 11 VM
- An Ubuntu Linux VM

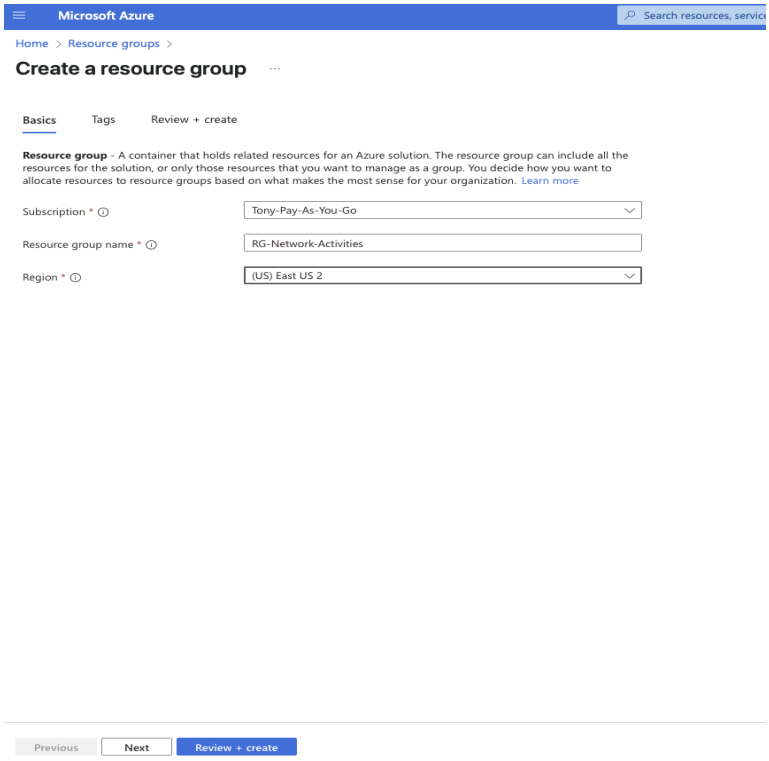
Open the Azure Portal

1. Go to https://portal.azure.com
2. From the dashboard, click Virtual Machines or Create a resource



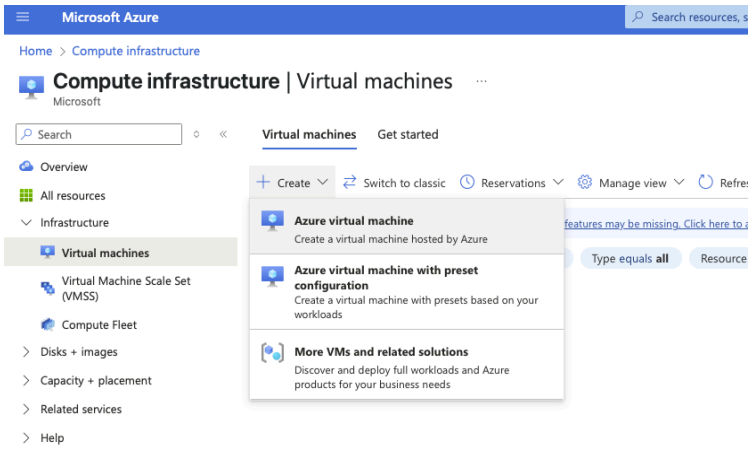
Create a Resource Group

1. Click Resource groups in the left menu
2. Click + Create
3. Name the group RG-Network-Activities (any name that you want)
4. Set Region to (US) East US 2
5. Click Review + create, then click Create



Create a Windows Virtual Machine

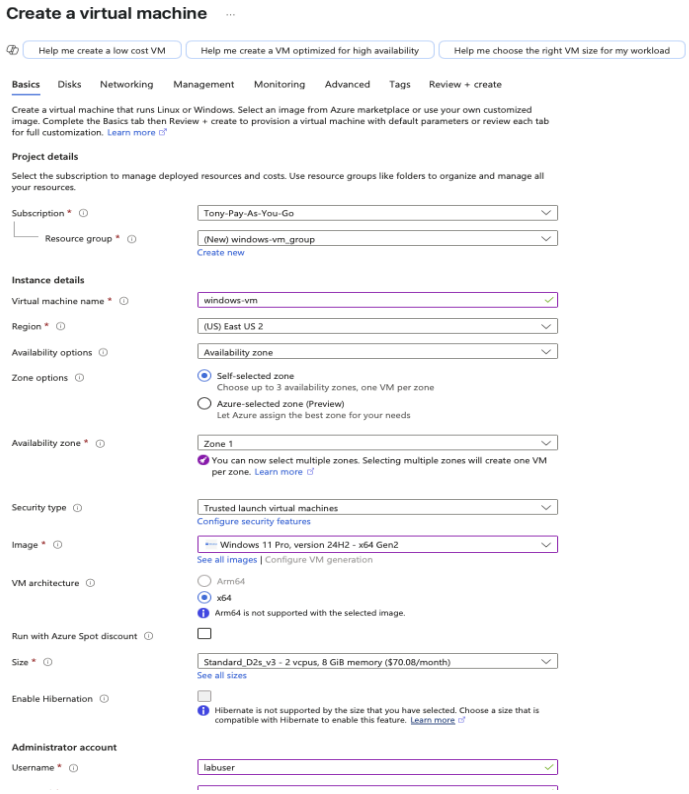
1. Go to Virtual Machines
2. Click + Create → Azure virtual machine
3. Select the Resource Group RG-Network-Activities

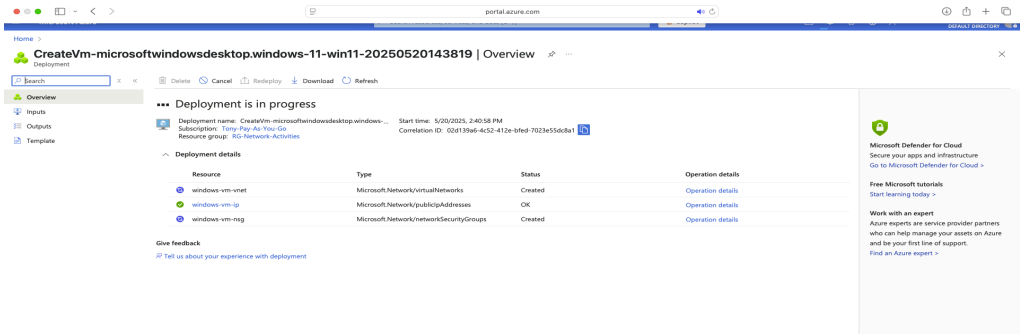


Configure the Windows VM

Basic Tab Setup:

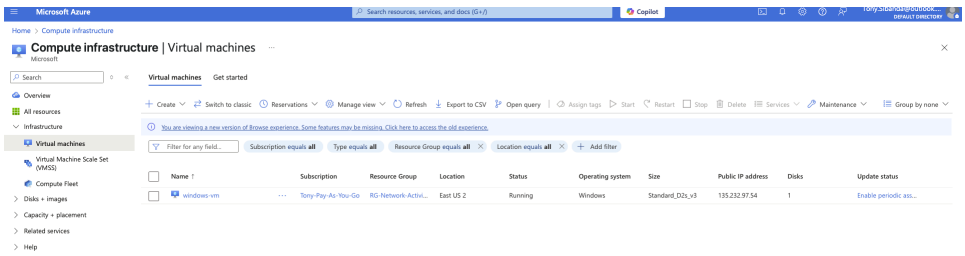
- VM Name: windows-vm (any name that you want).
- Region: East US 2 (same region as the Resource Group for purposes of this exercise)
- Availability Zone: Zone 1
- Image: Windows 11 Pro, version 24H2 - x64 Gen2
- Size: Standard_D2s_v3
- Security Type: Trusted launch virtual machines
- Username: labuser
- Password: Your secure password
- Public inbound ports: Allow RDP (3389)
- Be sure to click the confirm that you have eligible Windows 10/11 license with multi-tenant hosting rights at the bottom of the screen
- Disk, Networking, Management, Monitoring, Advanced & Tags (for purposes of this exercise we'll skip these steps, we don't need to change or add anything here)
- Click Review & Create and start the deployment process
- After clicking review and create and after the Validation Test has passed





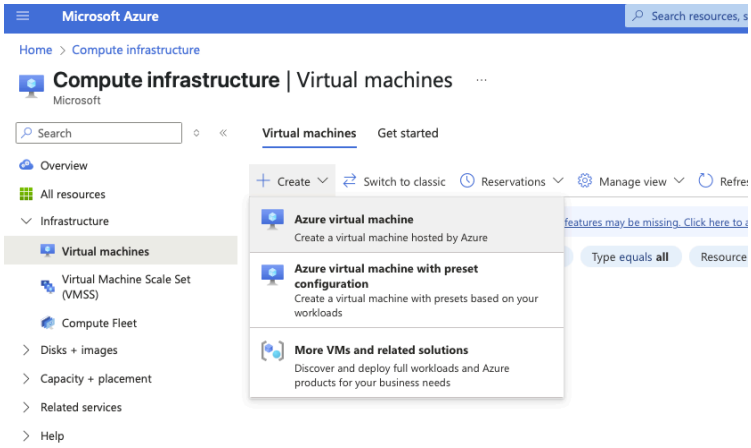
Deployment Configuration Completion

- It is good practice to go back to the Virtual Machines and double check the VM is running



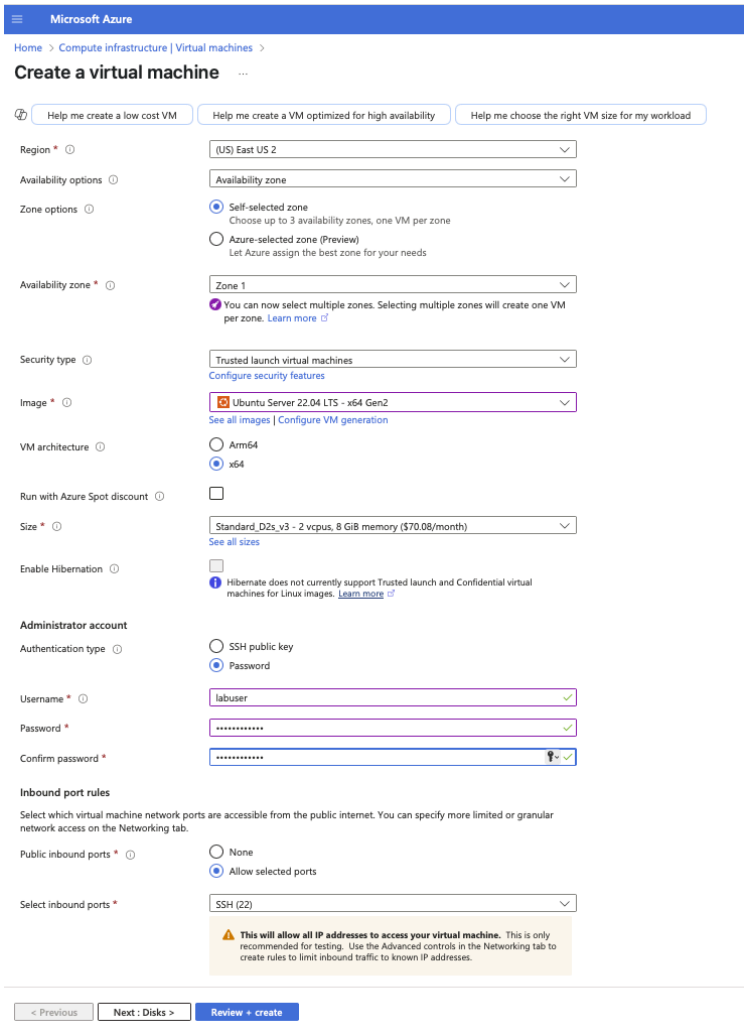
Create a Linux Virtual Machine

4. Go to Virtual Machines
5. Click + Create → Azure virtual machine
6. Select the Resource Group RG-Network-Activities



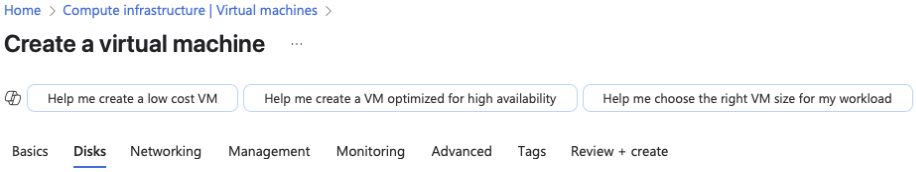
Basic Tab Setup:

- VM Name: linux-vm
- Image: Ubuntu Server 22.04 or 24.04 LTS
- Authentication Type: Password
- Username: labuser
- Password: Your secure password
- Public inbound ports: Allow SSH (22)
- Keep the other settings consistent with the Windows VM



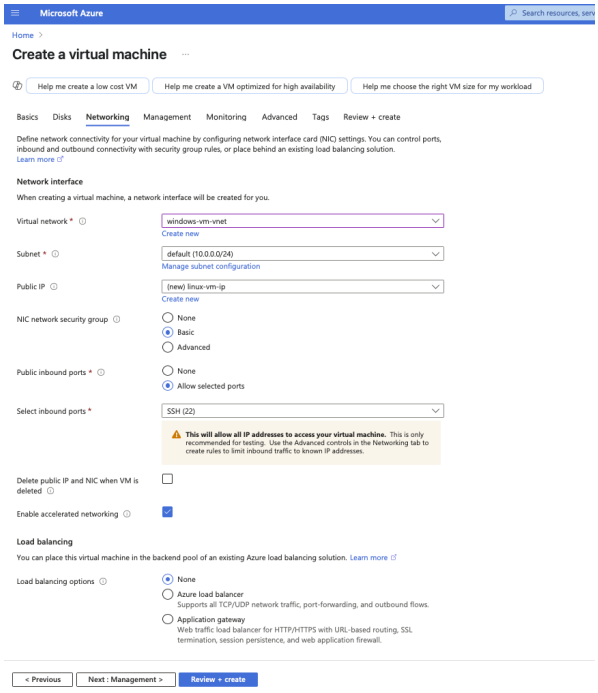
Configure Disks

- Disk Type: Premium SSD
- Leave default size and redundancy (locally-redundant)
- Check the option to Delete disk when VM is deleted



Configure Networking

- Virtual Network: We'll use the windows-vm network that we just created
- Public IP: Automatically assigned
- NIC Security Group: Basic
- Public inbound ports:
    - Windows VM: RDP (3389)
    - Linux VM: SSH (22)
- Leave Accelerated Networking enabled



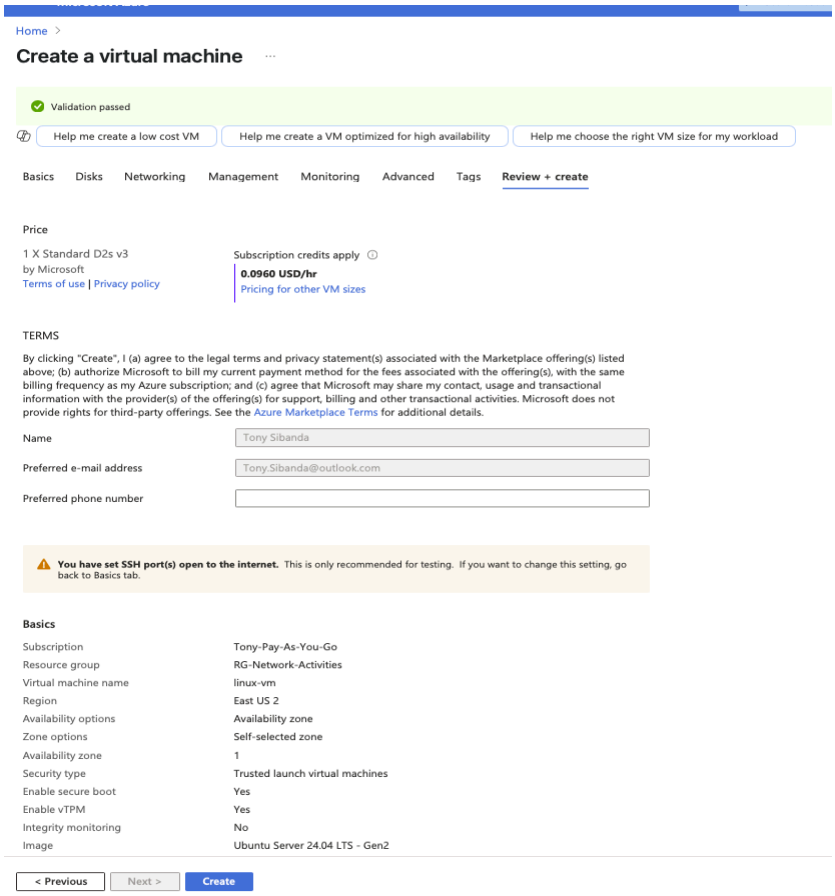
Why We Skip the Remaining Tabs (Management, Monitoring, Advanced, Tags)

These tabs are optional and not necessary for basic setups or practice labs:

- Management: Enables auto-shutdown, backup, and diagnostics, useful later but not needed for testing.
- Monitoring: You can configure insights and metrics later if desired.
- Advanced: Not required unless you need VM extensions or custom scripts.
- Tags: Useful in enterprise environments for cost tracking, optional for personal use.

Review and Create

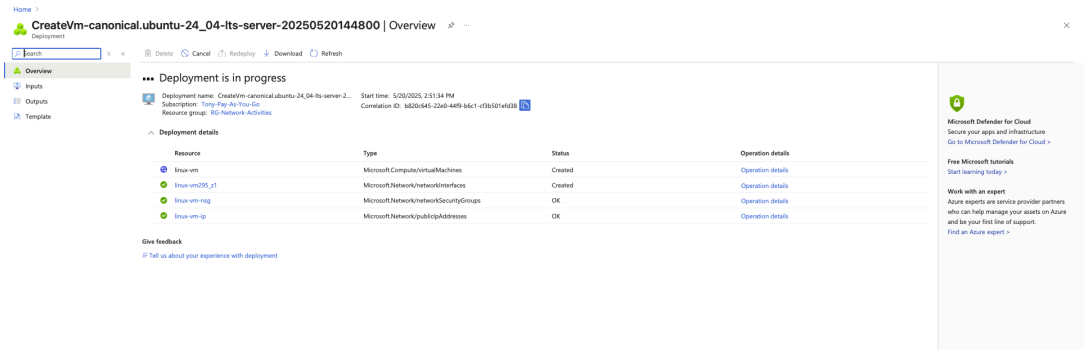
- Azure runs a validation check.
- If successful, click Create to begin deployment.



Deployment Progress

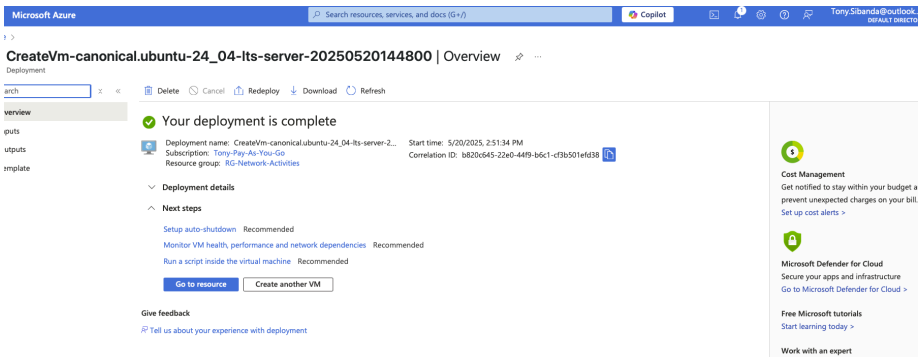
Azure will begin provisioning resources:

- Virtual Network
- Subnet
- NSG (Network Security Group)
- Public IP
- Disk and NIC



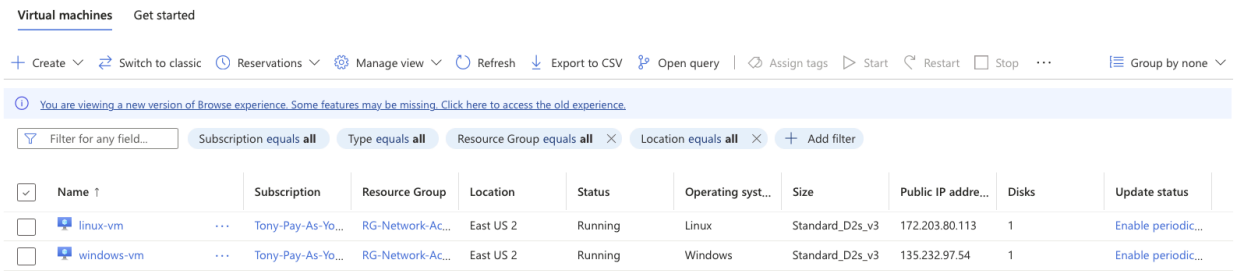
Deployment Complete

After a few minutes, you'll see Deployment Succeeded.
Click Go to resource to view your new virtual machine.



Verify Virtual Machines

Go back to the Virtual Machines panel.
Confirm both windows-vm and linux-vm show status as Running and have public IP addresses assigned.



Best Practices

- Shutdown unused VMs to avoid charges
- Use NSG rules to secure access (don’t allow all IPs in production)
- Consider Azure Bastion or VPN for secure remote access
- Use Tags when working with multiple environments or users
