Cybersecurity Home Lab Project using Microsoft Sentinel 2025

Name: Phanindhar Reddy Karnati

Date: 06/14/2025

Table of Contents

Introduction

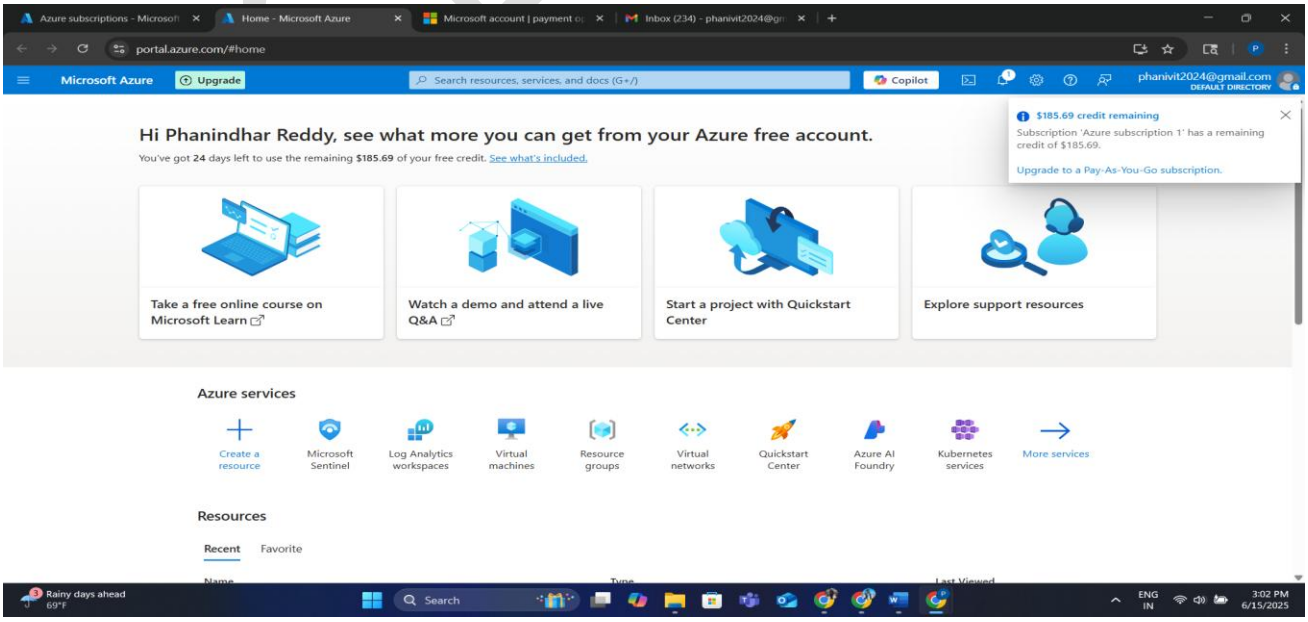
This project outlines the creation and deployment of a cloud-based home Security Operations Center (SOC) using Microsoft Azure and Microsoft Sentinel. The lab provides real-world simulation experience by configuring a honeypot virtual machine (VM) to receive actual malicious traffic from the internet. Through this setup, we demonstrate how to monitor, analyze, and visualize attack patterns using security event logs, Kusto Query Language (KQL), and geographic enrichment via a custom IP-to-location watchlist. This lab is suitable for beginners, professionals, and cybersecurity students seeking hands-on SIEM experience that can be highlighted on resumes.

1. Azure Account Creation and Access

Before deploying any infrastructure, a free Azure subscription is created. Microsoft requires a credit card to verify the user. If a free account is unavailable, users may opt for:

- A pay-as-you-go Azure model (billed like a utility)
- Accessing Azure through the paid "Cyber Range" platform which includes other cybersecurity tools like Tenable

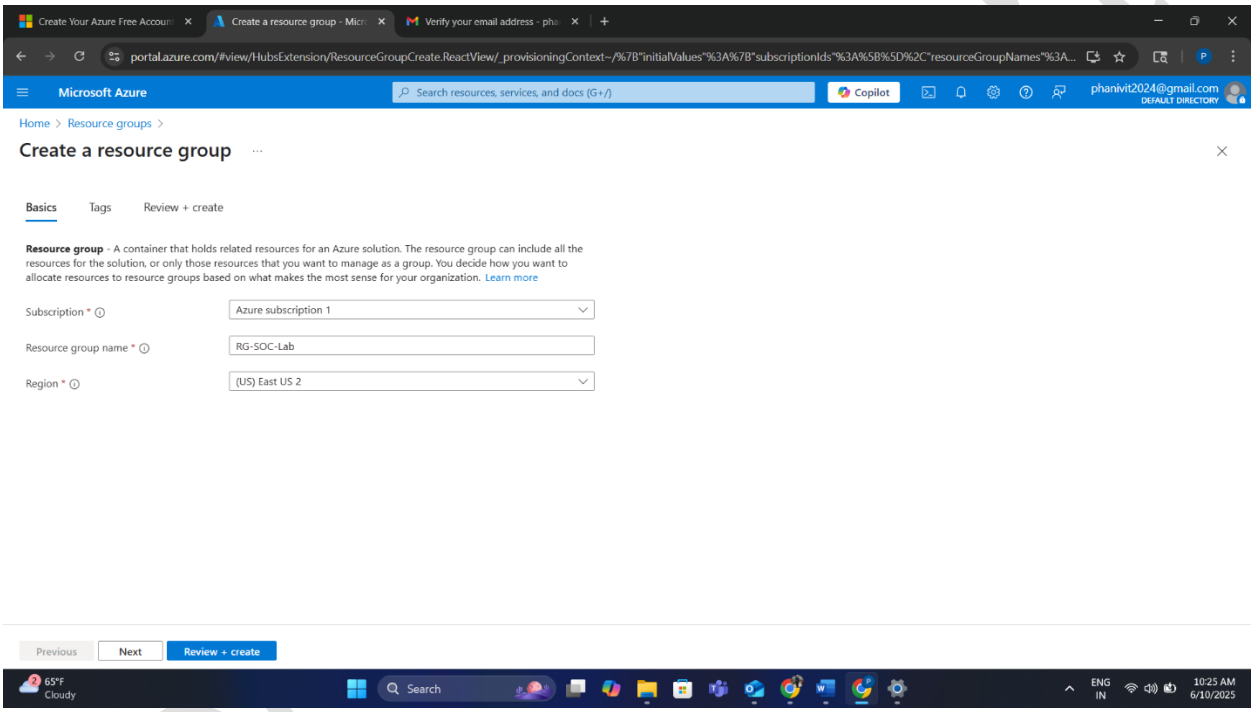
Once an account is active, users can access the Azure dashboard through portal.azure.com.



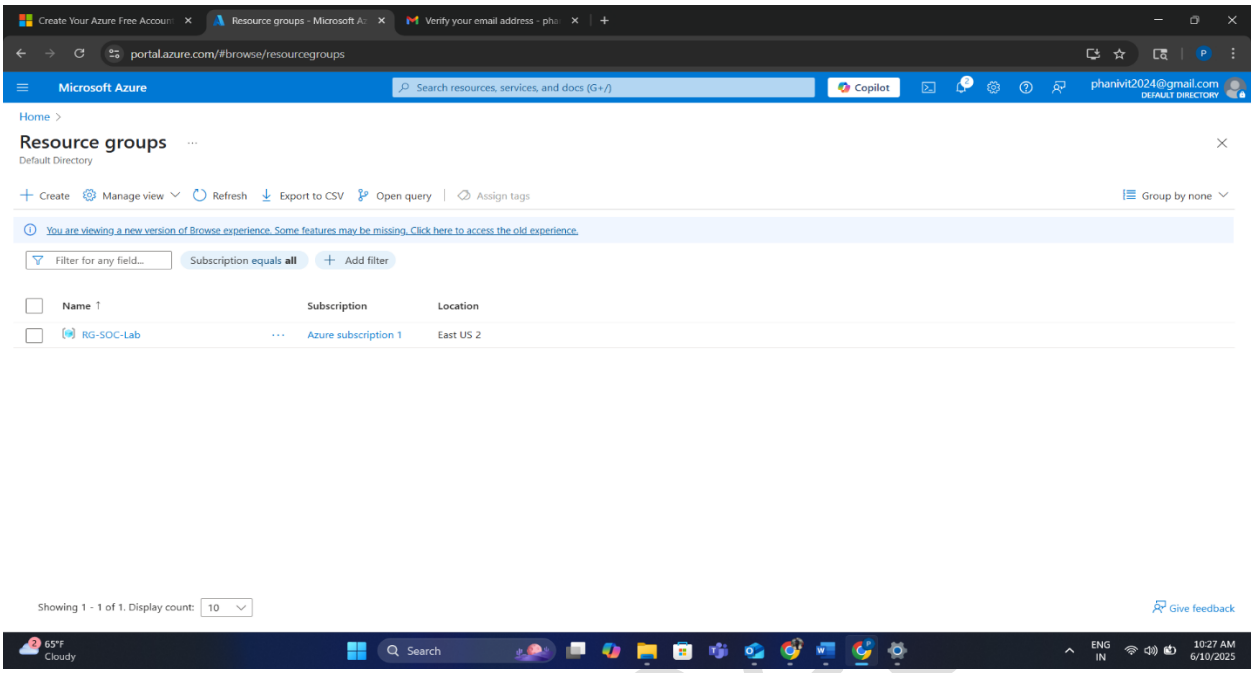
2. Resource Group Setup

Resource groups in Azure serve as containers for related resources.

- They allow easier management, deletion, and auditing of associated services.



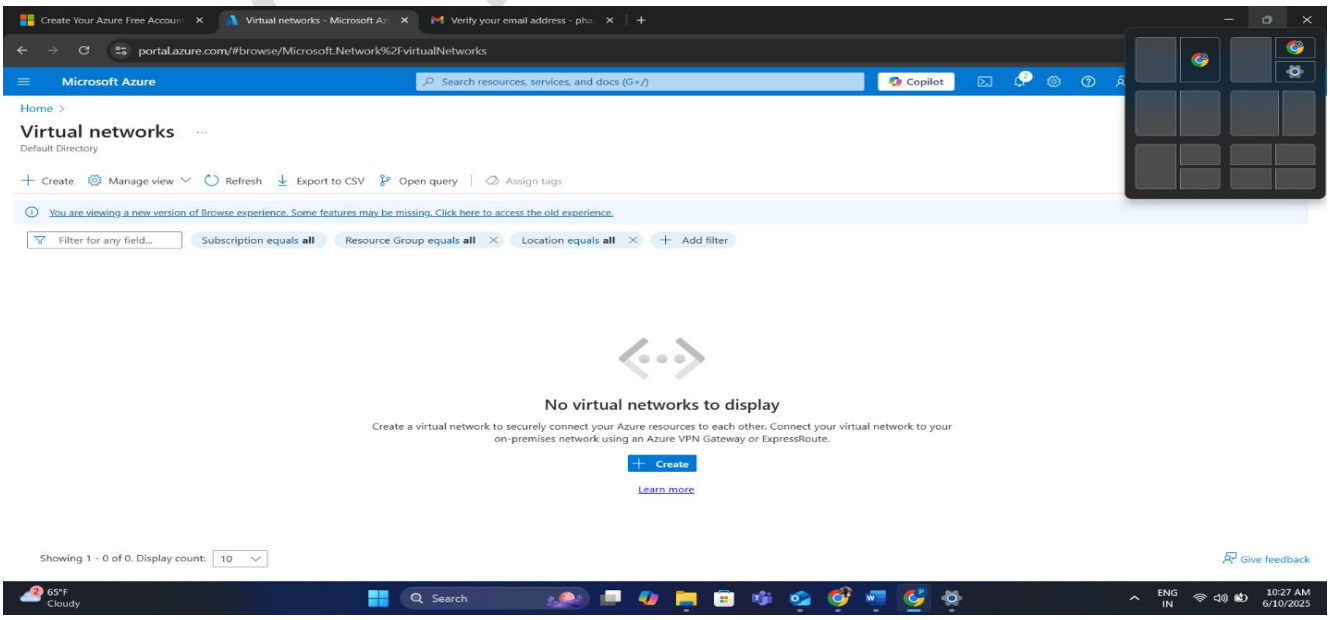
- We created a resource group named rg-socklab in the "East US 2" region to ensure data locality for our VMs and networking resources.

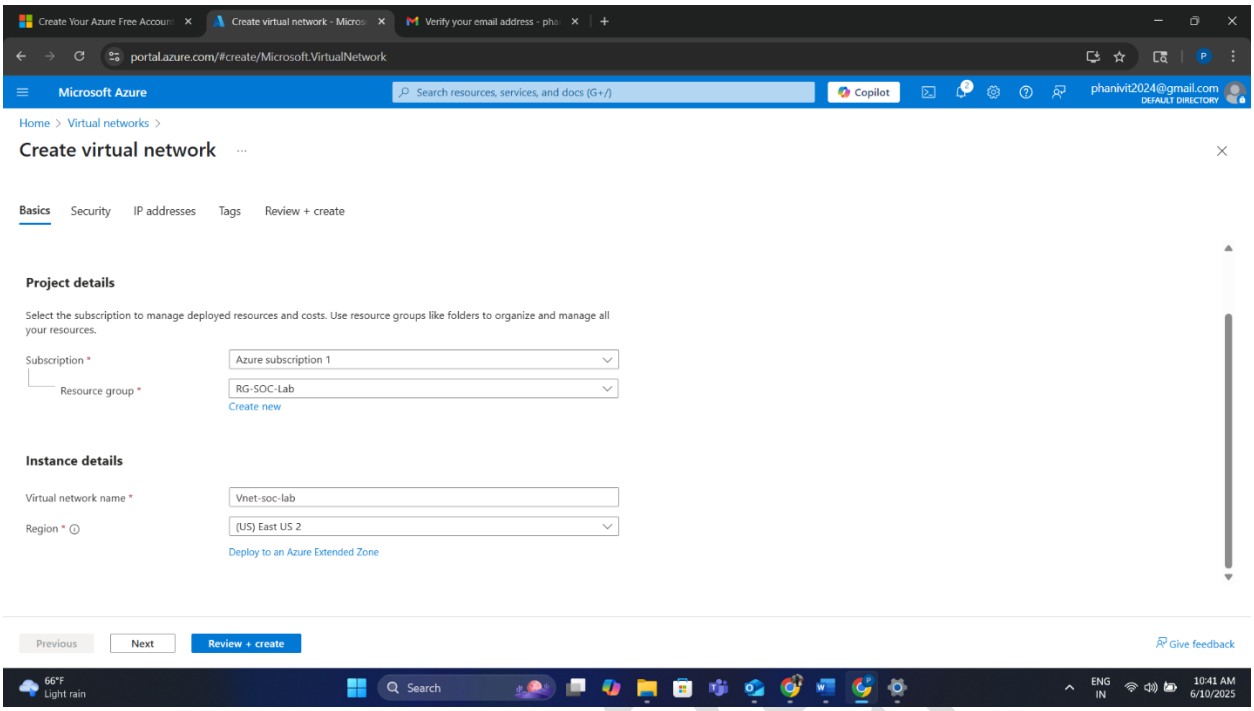


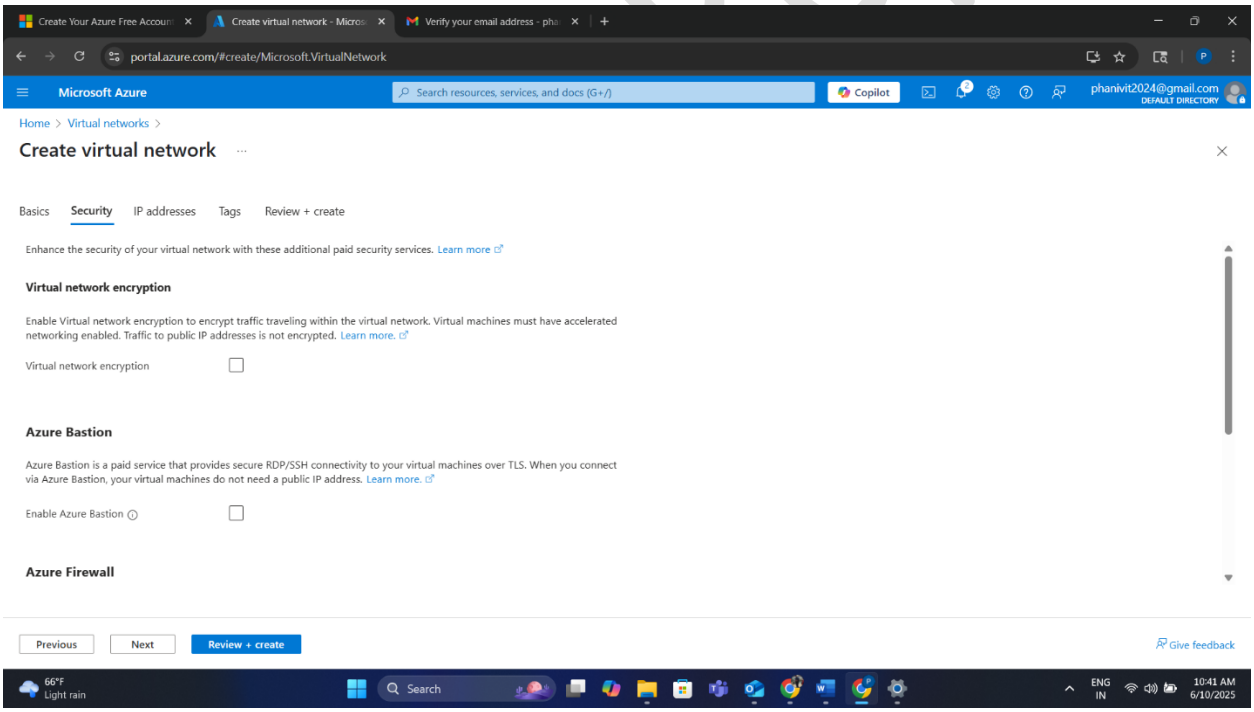
3. Virtual Network and Subnet Configuration

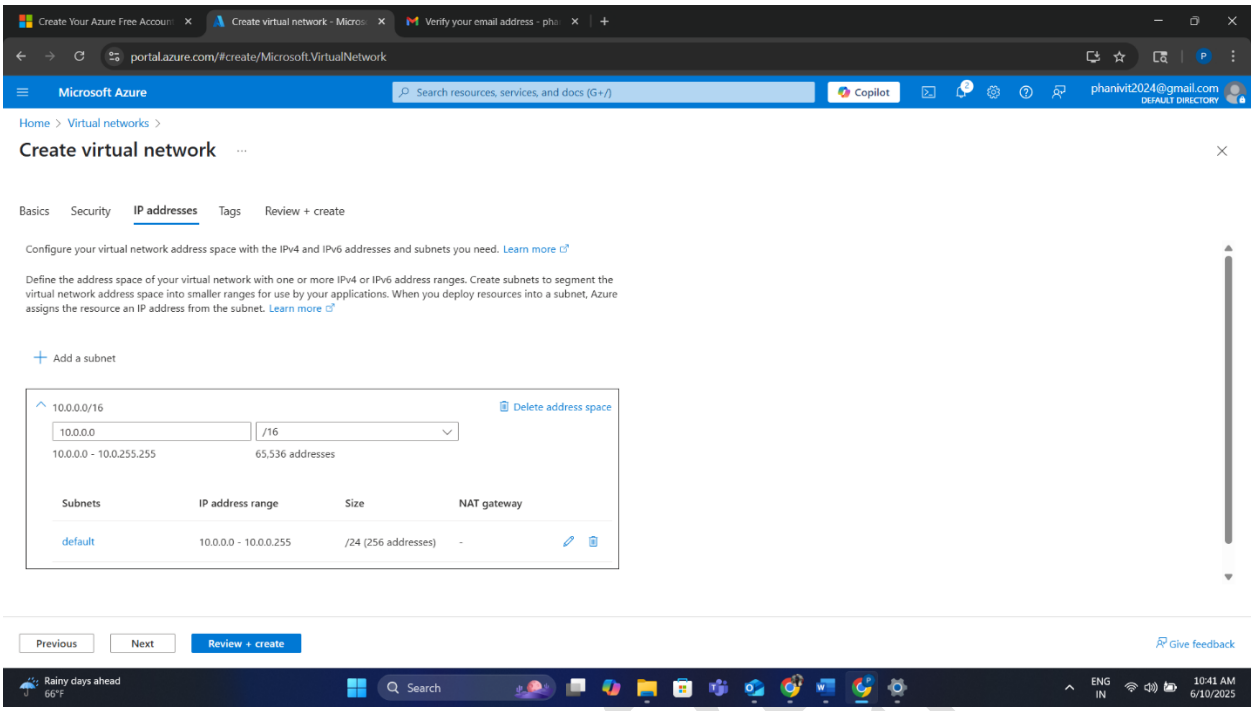
A Virtual Network (VNet) simulates a traditional networking environment in the cloud. It functions like a router at home, enabling internal communication and internet exposure:

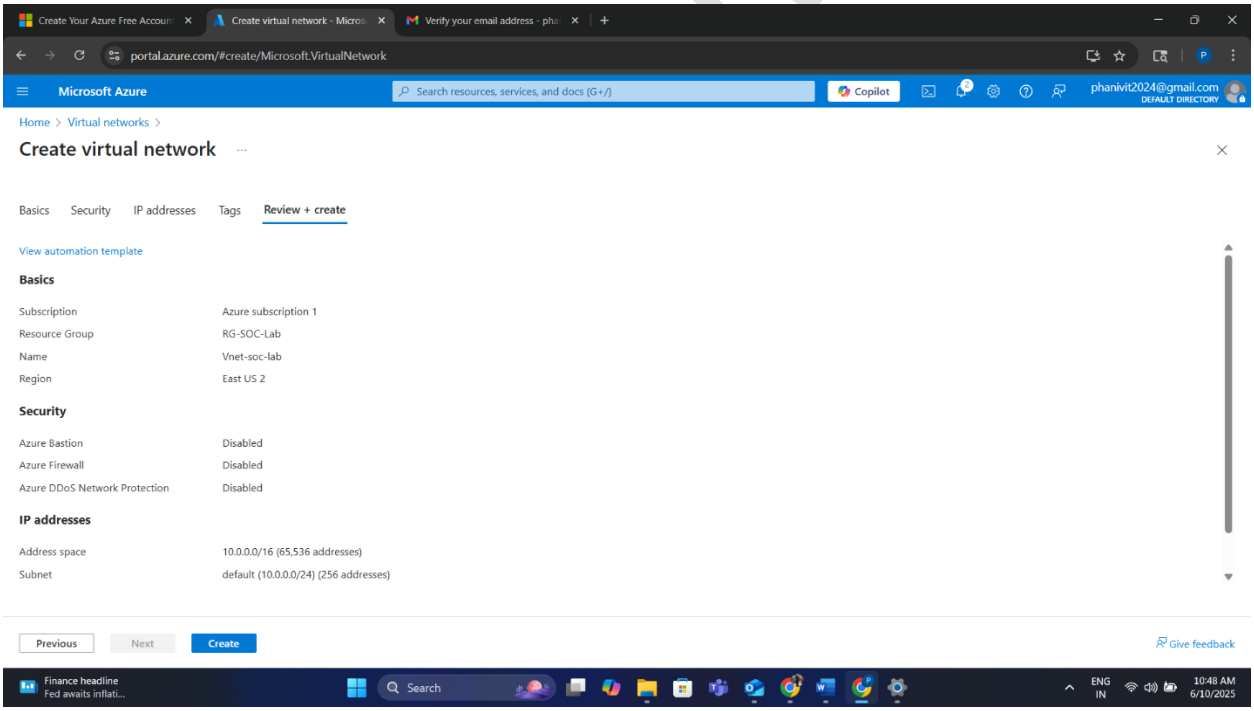
- A VNet named vnet-socklab was created in the same resource group.
- A default subnet was automatically created within the VNet, enabling internal VM traffic.

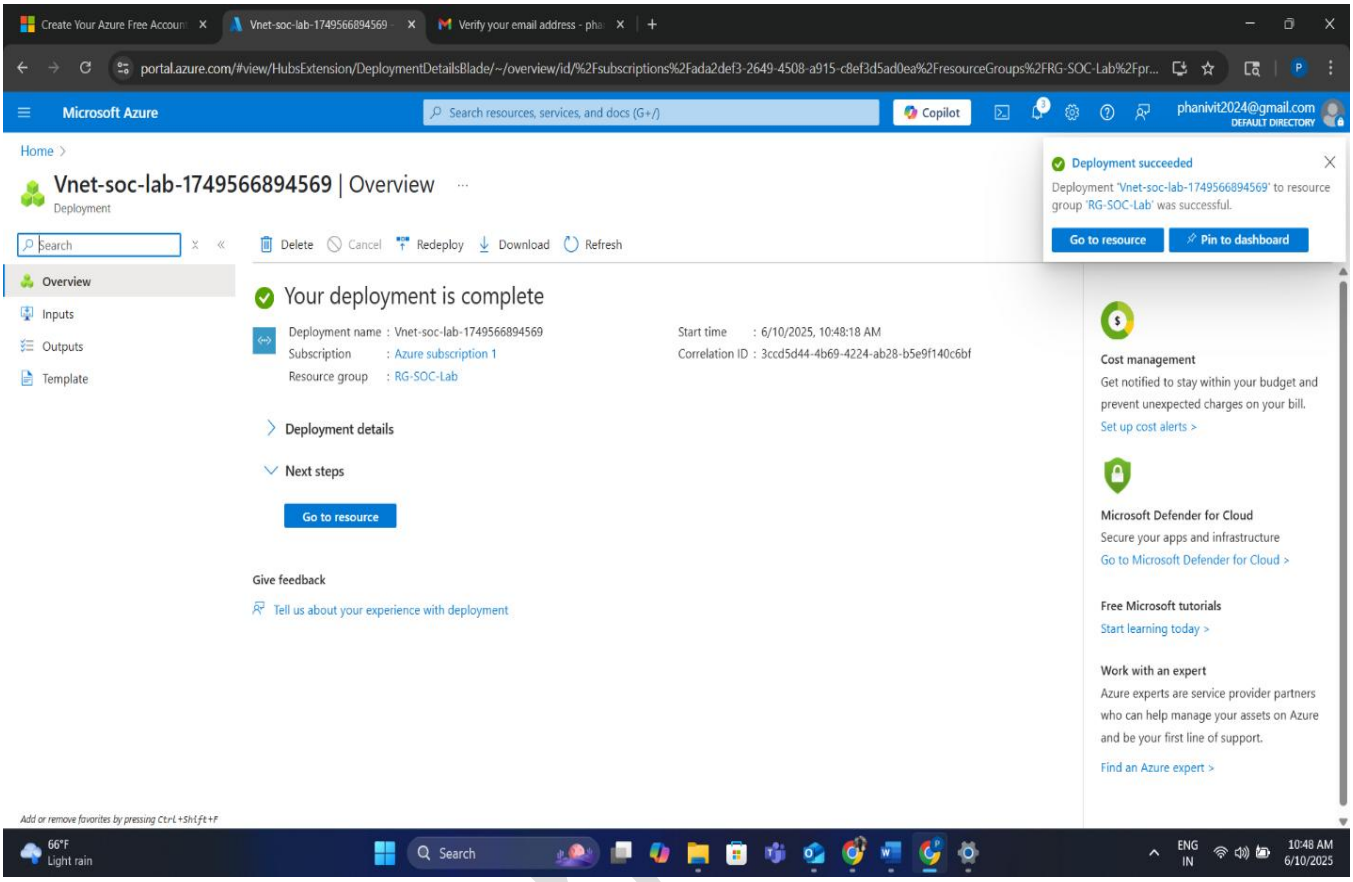



Create Your Azure Free Accoun
Create virtual network - Micros
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualNetwork
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home > Virtual networks >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure subscription 1
Resource group *
RG-SOC-Lab
Create new
Instance details
Virtual network name *
Vnet-soc-lab
Region *
(US) East US 2
Deploy to an Azure Extended Zone
Previous
Next
Review + create
Give feedback
66°F
Light rain
Search
ENG
IN
10:41 AM
6/10/2025


Create Your Azure Free Accoun
Create virtual network - Micros
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualNetwork
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home > Virtual networks >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Enhance the security of your virtual network with these additional paid security services. Learn more
Virtual network encryption
Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. Learn more.
Virtual network encryption
Azure Bastion
Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. Learn more.
Enable Azure Bastion
Azure Firewall
Previous
Next
Review + create
Give feedback
66°F
Light rain
Search
ENG
IN
10:41 AM
6/10/2025

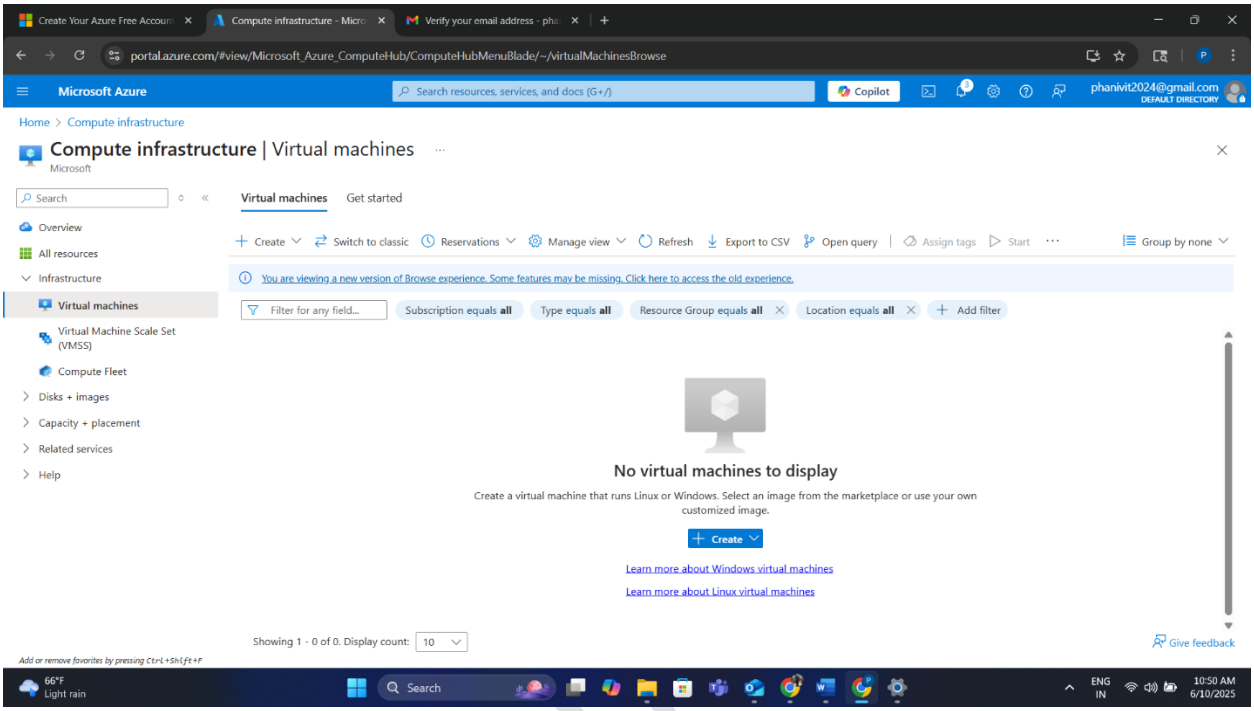

Create Your Azure Free Account
Create virtual network - Micros
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualNetwork
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home > Virtual networks >
Create virtual network
Basics Security IP addresses Tags Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more
Add a subnet
10.0.0.0/16
Delete address space
10.0.0.0
/16
10.0.0.0 - 10.0.255.255
65,536 addresses
Subnets
IP address range
Size
NAT gateway
default
10.0.0.0 - 10.0.0.255
/24 (256 addresses)
-
Previous
Next
Review + create
Give feedback
Rainy days ahead
66°F
Search
ENG
IN
10:41 AM
6/10/2025

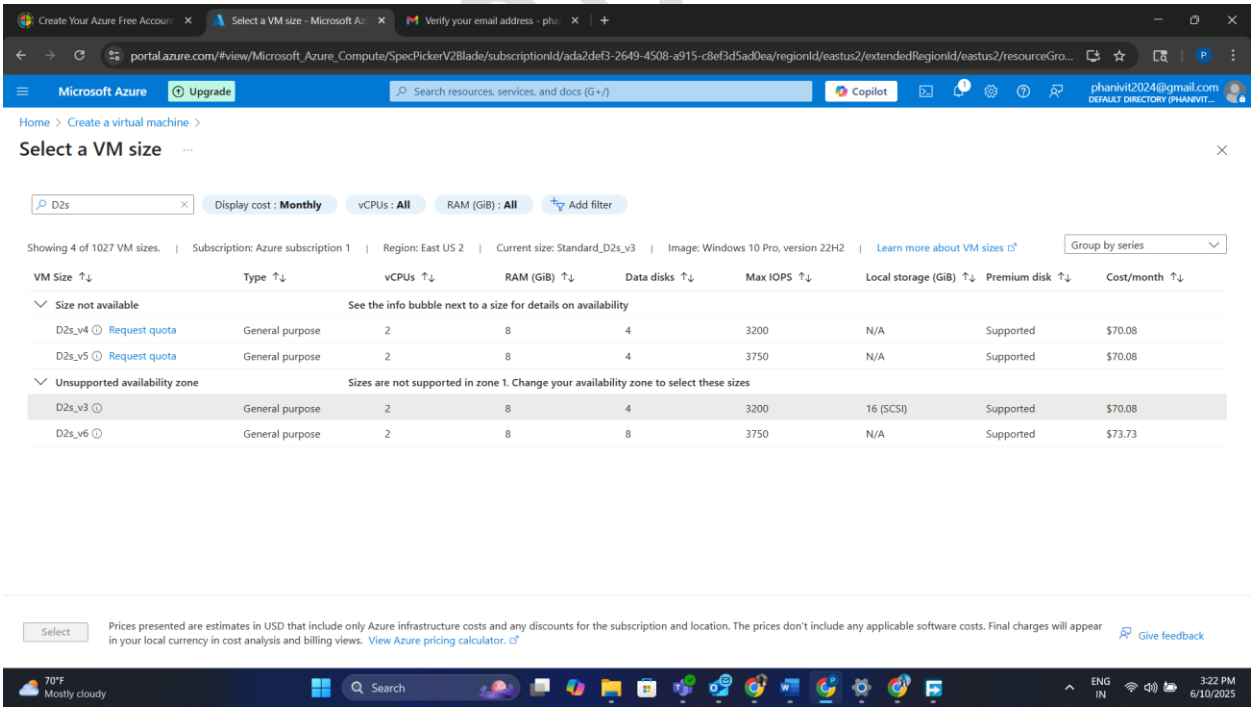

Create Your Azure Free Account
Create virtual network - Micros
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualNetwork
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home > Virtual networks >
Create virtual network
Basics Security IP addresses Tags Review + create
View automation template
Basics
Subscription
Azure subscription 1
Resource Group
RG-SOC-Lab
Name
Vnet-soc-lab
Region
East US 2
Security
Azure Bastion
Disabled
Azure Firewall
Disabled
Azure DDoS Network Protection
Disabled
IP addresses
Address space
10.0.0.0/16 (65,536 addresses)
Subnet
default (10.0.0.0/24) (256 addresses)
Previous
Next
Create
Give feedback
Finance headline
Fed awaits inflati...
Search
ENG
IN
10:48 AM
6/10/2025

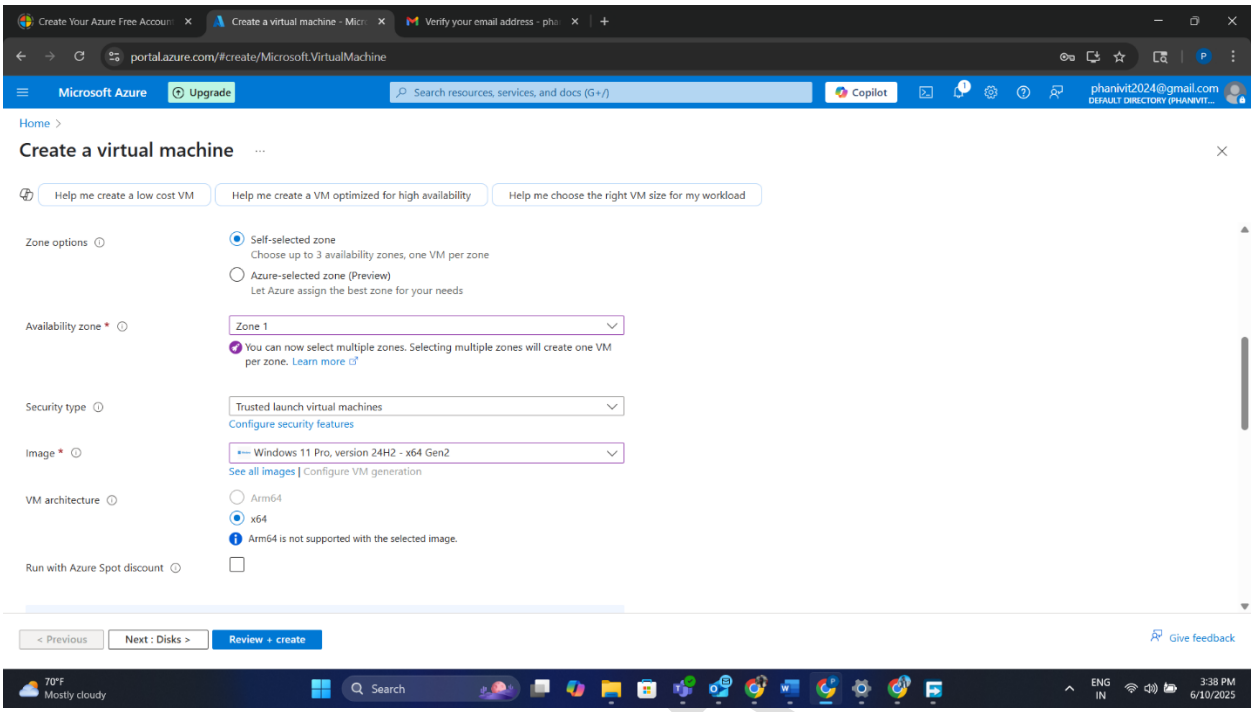

Create Your Azure Free Accoun
Vnet-soc-lab-1749566894569
Verify your email address - pha
portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2Fada2def3-2649-4508-a915-c8ef3d5ad0ea%2FresourceGroups%2FRG-SOC-Lab%2Fpr...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home
Vnet-soc-lab-1749566894569 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : Vnet-soc-lab-1749566894569
Subscription : Azure subscription 1
Resource group : RG-SOC-Lab
Start time : 6/10/2025, 10:48:18 AM
Correlation ID : 3ccd5d44-4b69-4224-ab28-b5e9f140c6bf
Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
Deployment succeeded
Deployment 'Vnet-soc-lab-1749566894569' to resource group 'RG-SOC-Lab' was successful.
Go to resource
Pin to dashboard
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Add or remove favorites by pressing Ctrl+Shift+F
66°F
Light rain
Search
ENG
IN
10:48 AM
6/10/2025

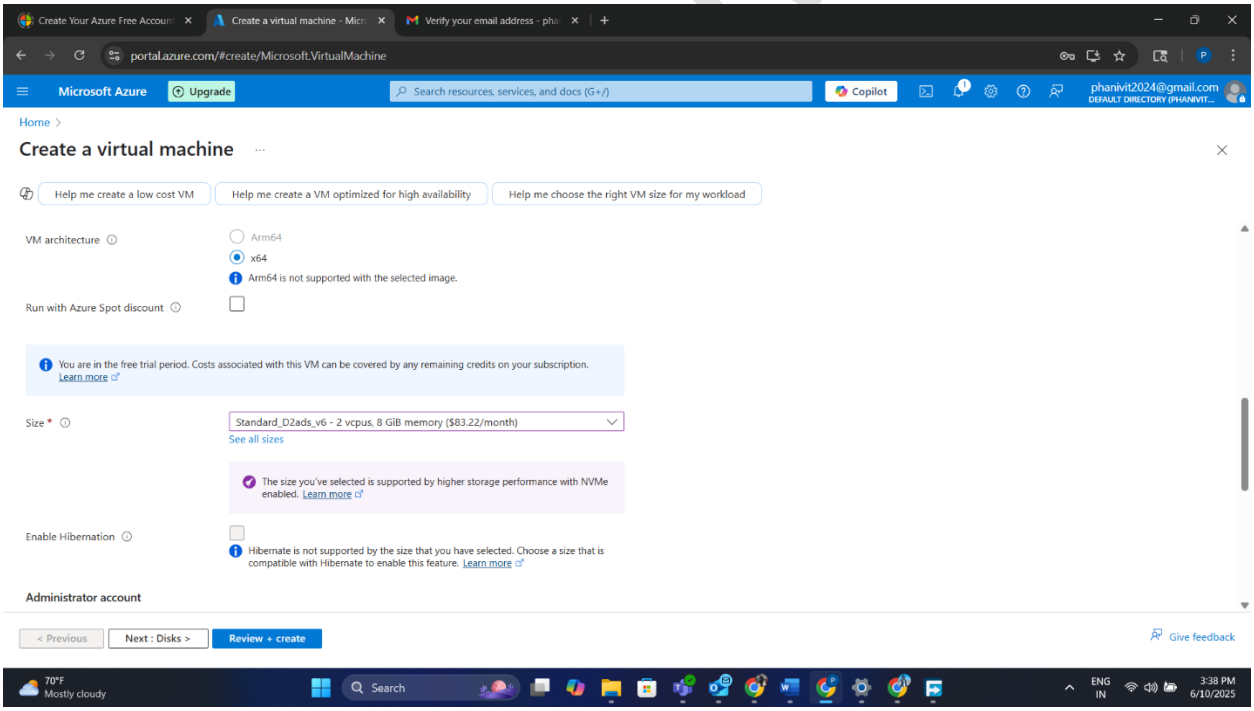
4. Deploying the Windows Virtual Machine (Honeypot)

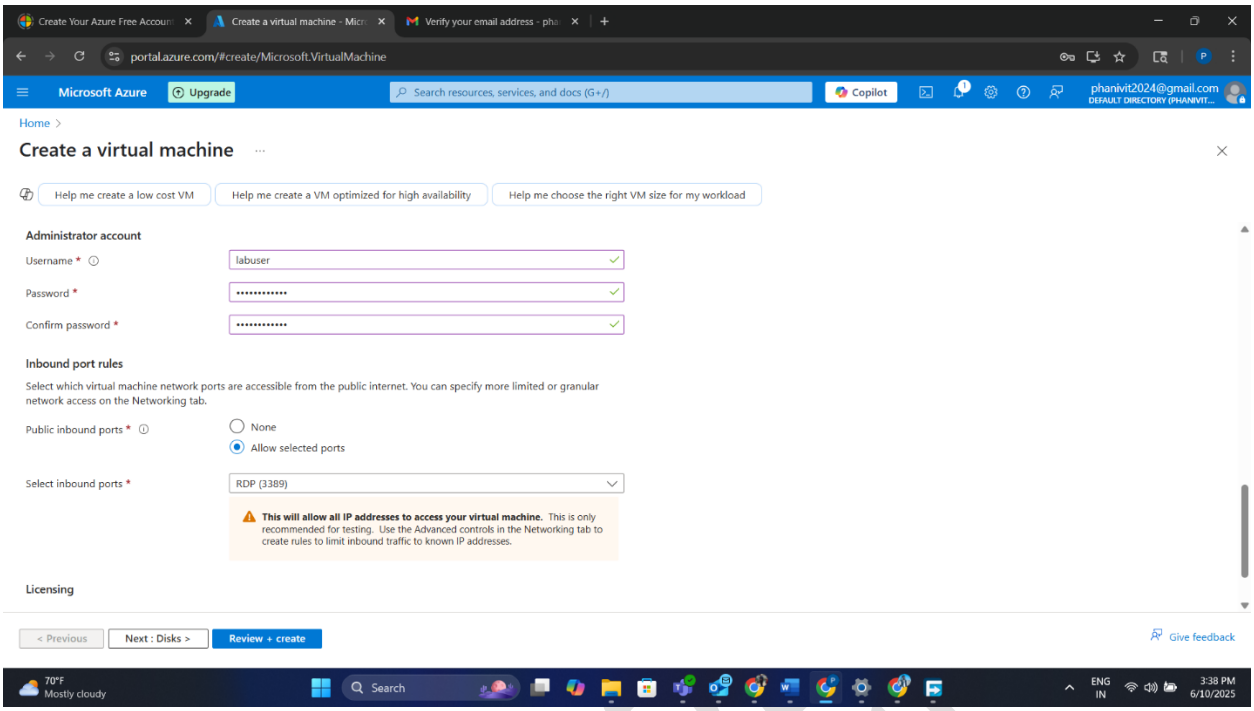
The core of the honeypot lab is a Windows 10 VM deployed to attract unauthorized access attempts:

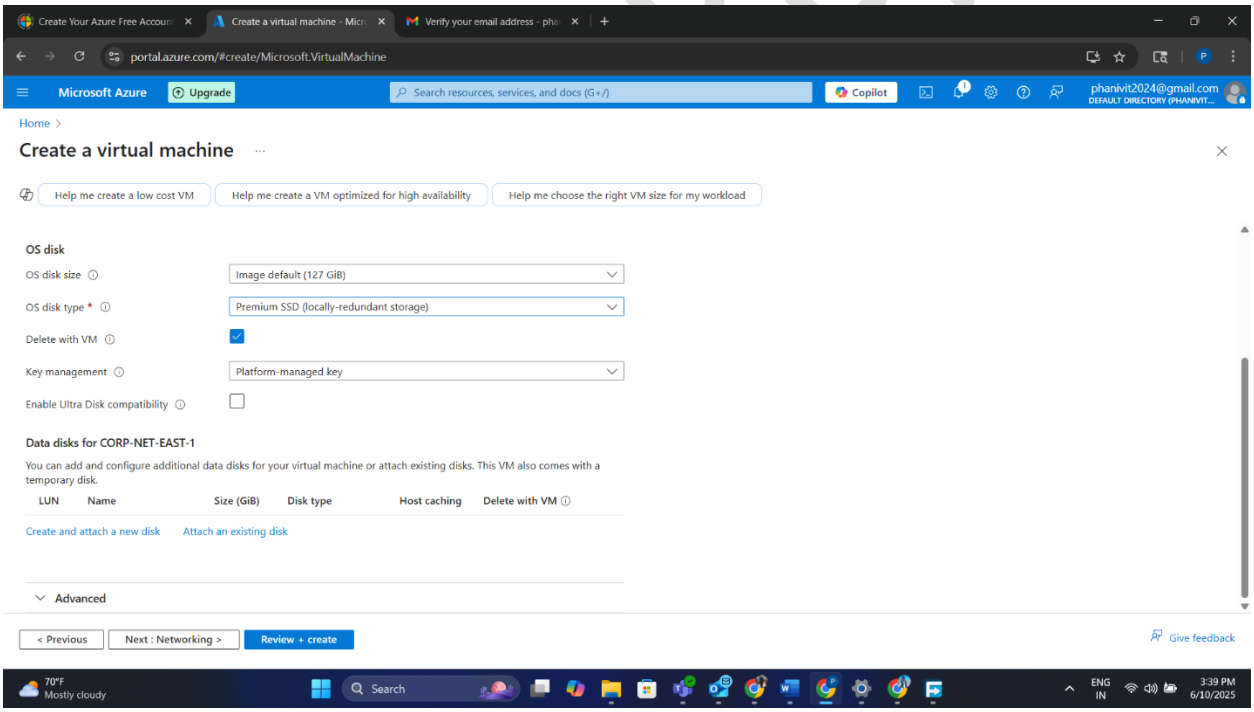


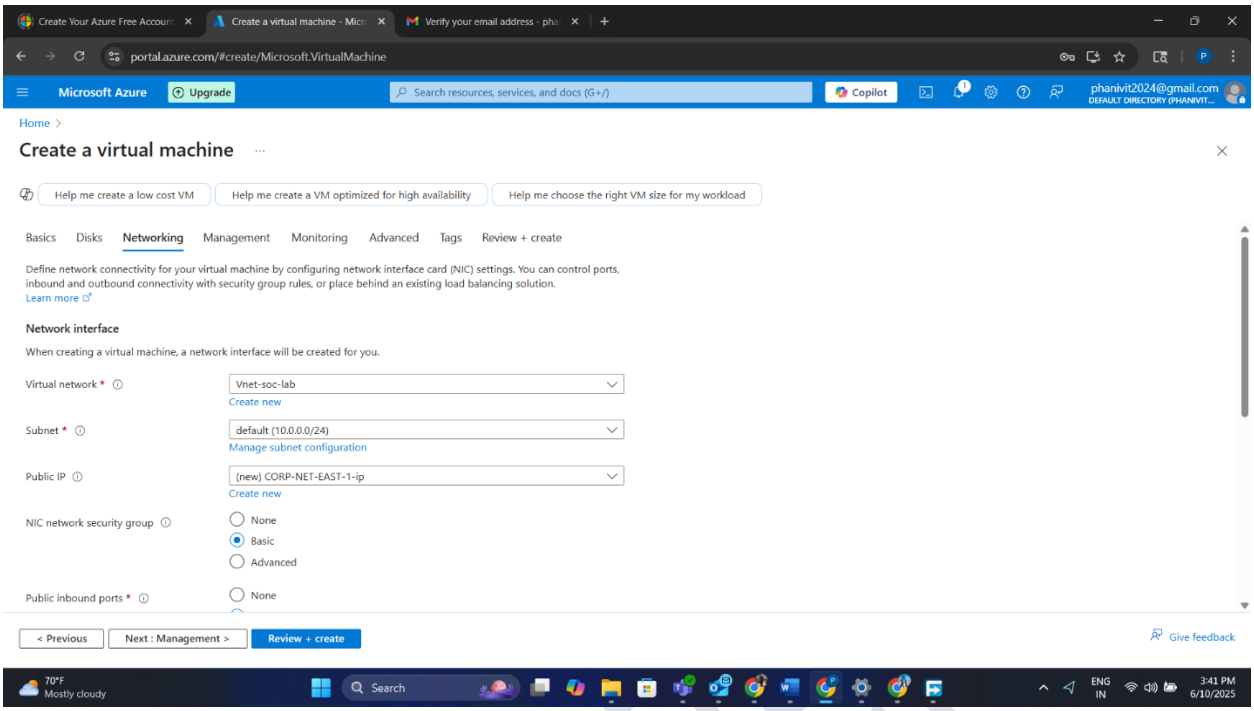


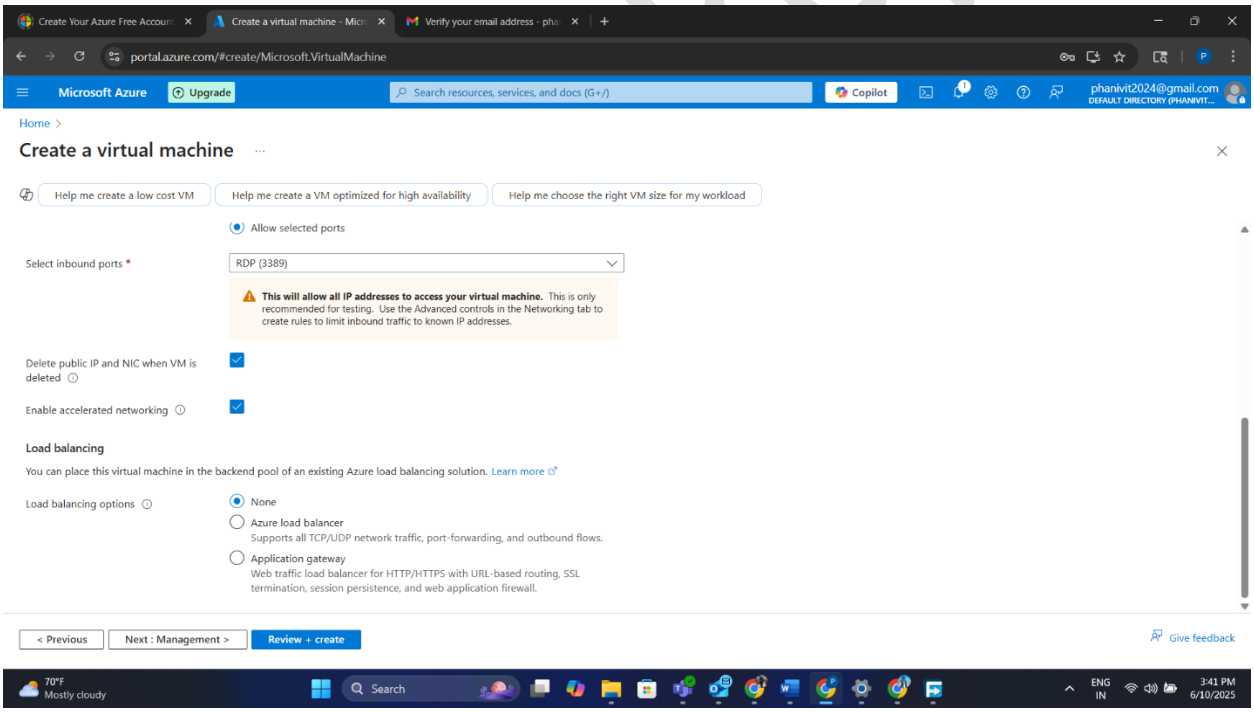

Create Your Azure Free Account
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Zone options
Self-selected zone
Choose up to 3 availability zones, one VM per zone
Azure-selected zone (Preview)
Let Azure assign the best zone for your needs
Availability zone *
Zone 1
You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more
Security type
Trusted launch virtual machines
Configure security features
Image *
Windows 11 Pro, version 24H2 - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount
< Previous
Next : Disks >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:38 PM
6/10/2025

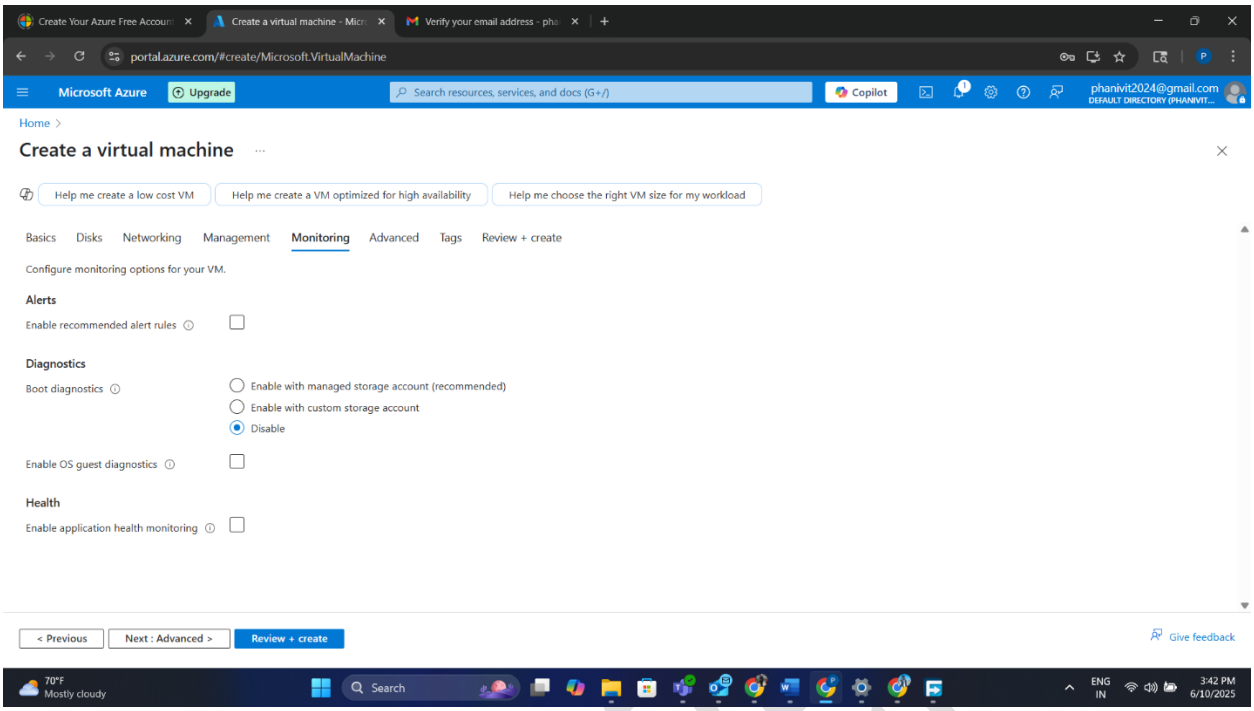

Create Your Azure Free Account
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount
You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription.
Learn more
Size *
Standard_D2ads_v6 - 2 vcpus, 8 GiB memory ($83.22/month)
See all sizes
The size you've selected is supported by higher storage performance with NVMe enabled. Learn more
Enable Hibernation
Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more
Administrator account
< Previous
Next : Disks >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:38 PM
6/10/2025

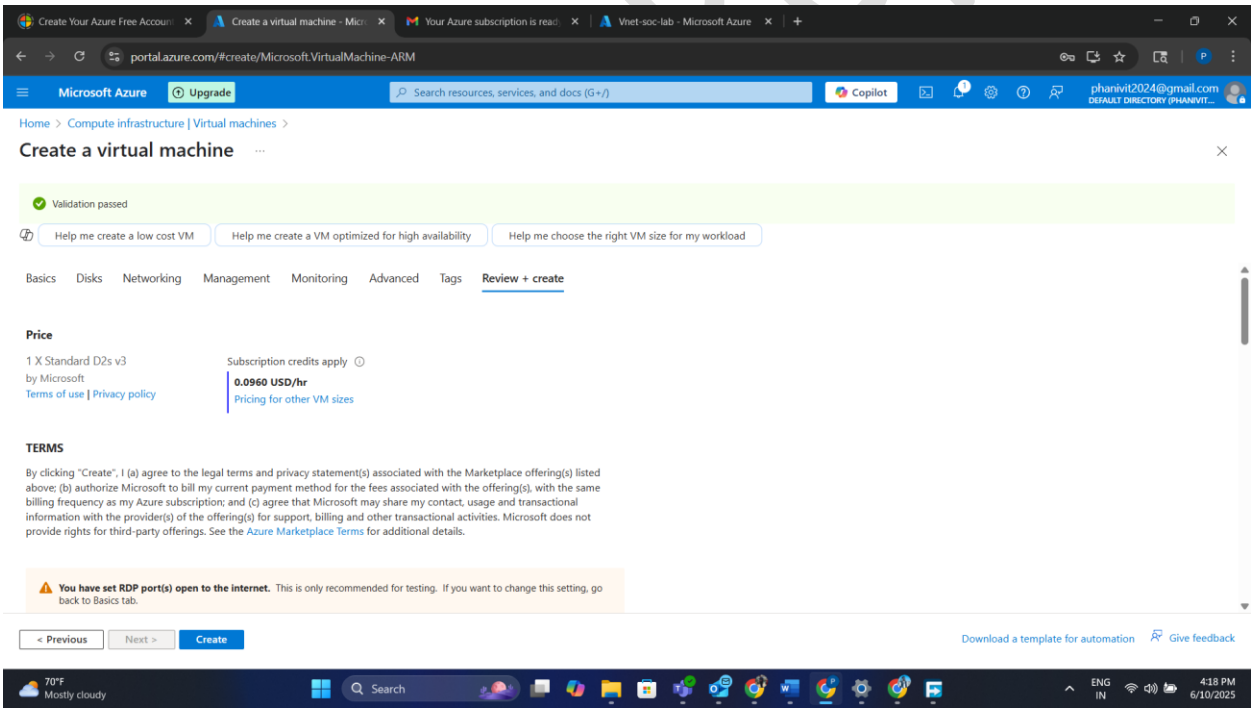

Create Your Azure Free Accoun
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Administrator account
Username *
labuser
Password *
Confirm password *
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
Select inbound ports *
RDP (3389)
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.
Licensing
< Previous
Next : Disks >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:38 PM
6/10/2025

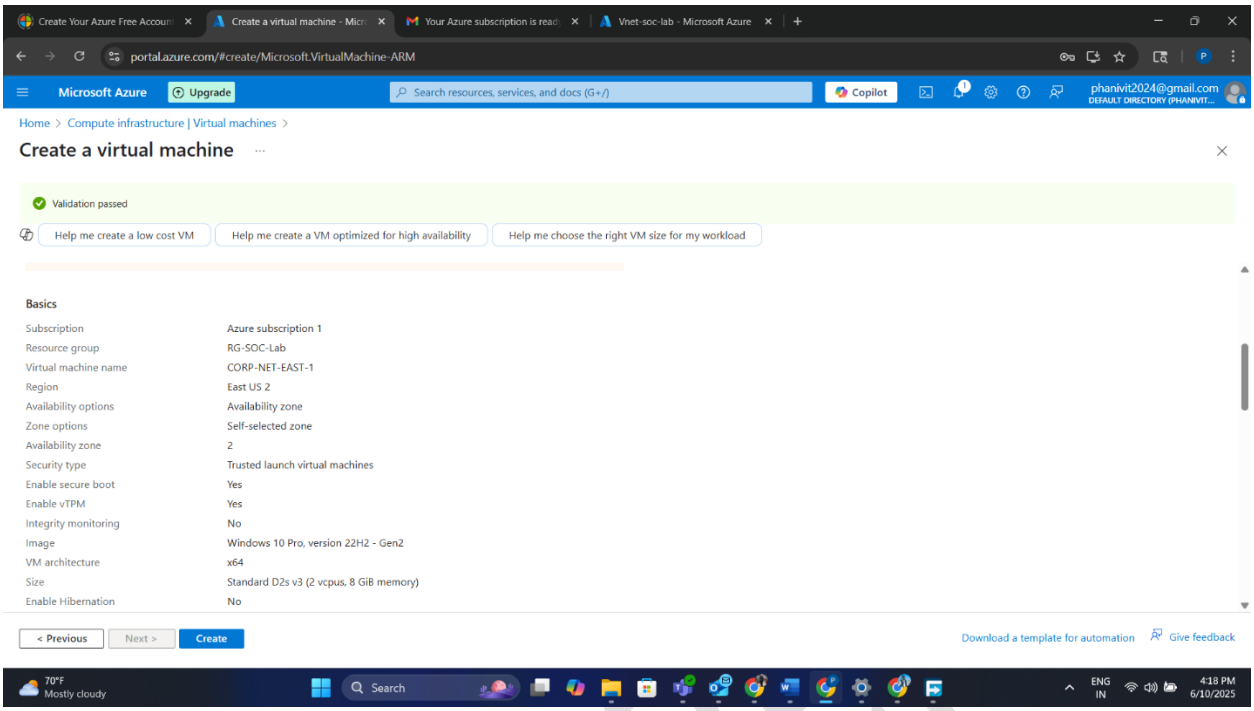

Create Your Azure Free Accoun
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
OS disk
OS disk size
Image default (127 GiB)
OS disk type *
Premium SSD (locally-redundant storage)
Delete with VM
Key management
Platform-managed key
Enable Ultra Disk compatibility
Data disks for CORP-NET-EAST-1
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.
LUN
Name
Size (GiB)
Disk type
Host caching
Delete with VM
Create and attach a new disk
Attach an existing disk
Advanced
< Previous
Next : Networking >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:39 PM
6/10/2025

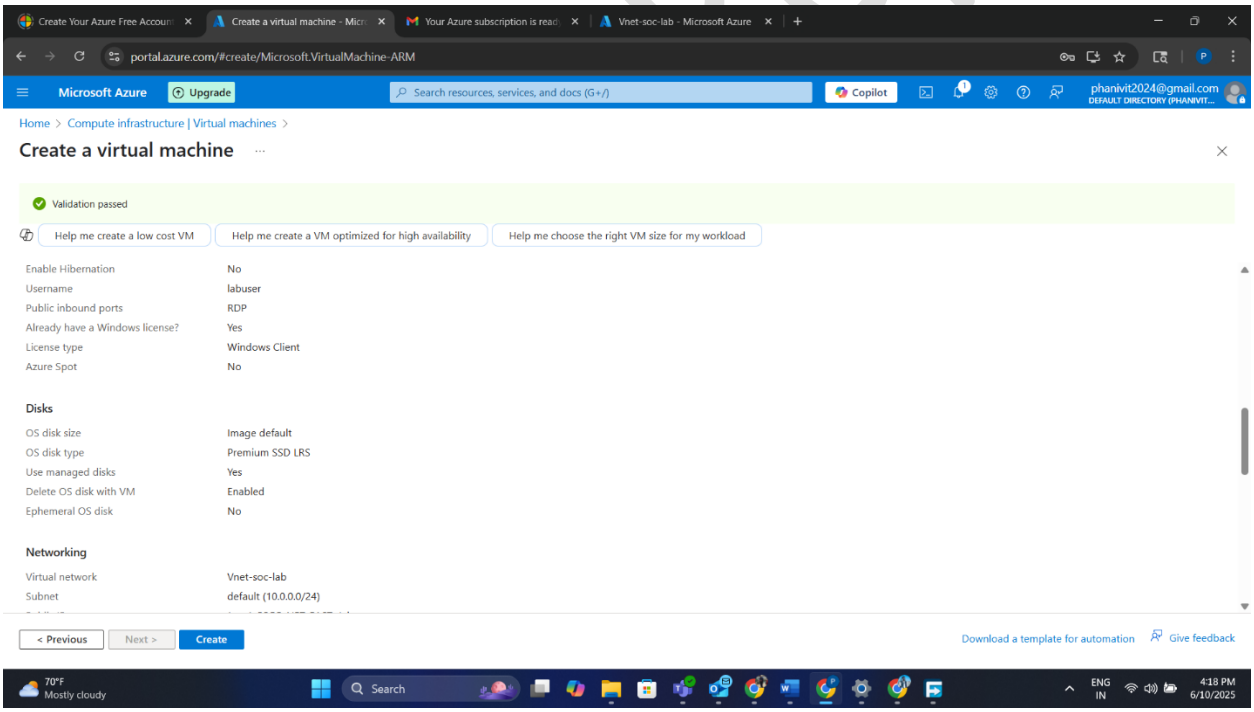

Create Your Azure Free Accoun
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
Vnet-soc-lab
Create new
Subnet *
default (10.0.0.0/24)
Manage subnet configuration
Public IP
(new) CORP-NET-EAST-1-ip
Create new
NIC network security group
None
Basic
Advanced
Public inbound ports *
None
< Previous
Next : Management >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:41 PM
6/10/2025

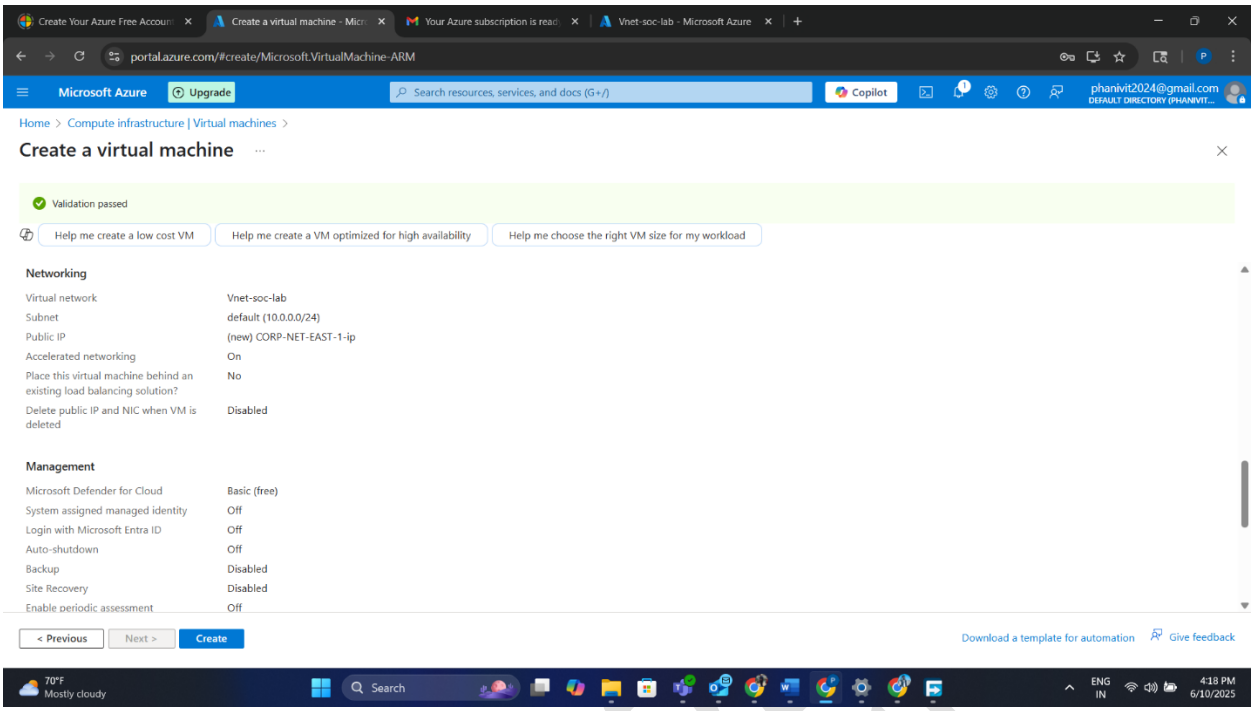

Create Your Azure Free Accoun
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Allow selected ports
Select inbound ports *
RDP (3389)
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.
Delete public IP and NIC when VM is deleted
Enable accelerated networking
Load balancing
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more
Load balancing options
None
Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.
< Previous
Next : Management >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:41 PM
6/10/2025

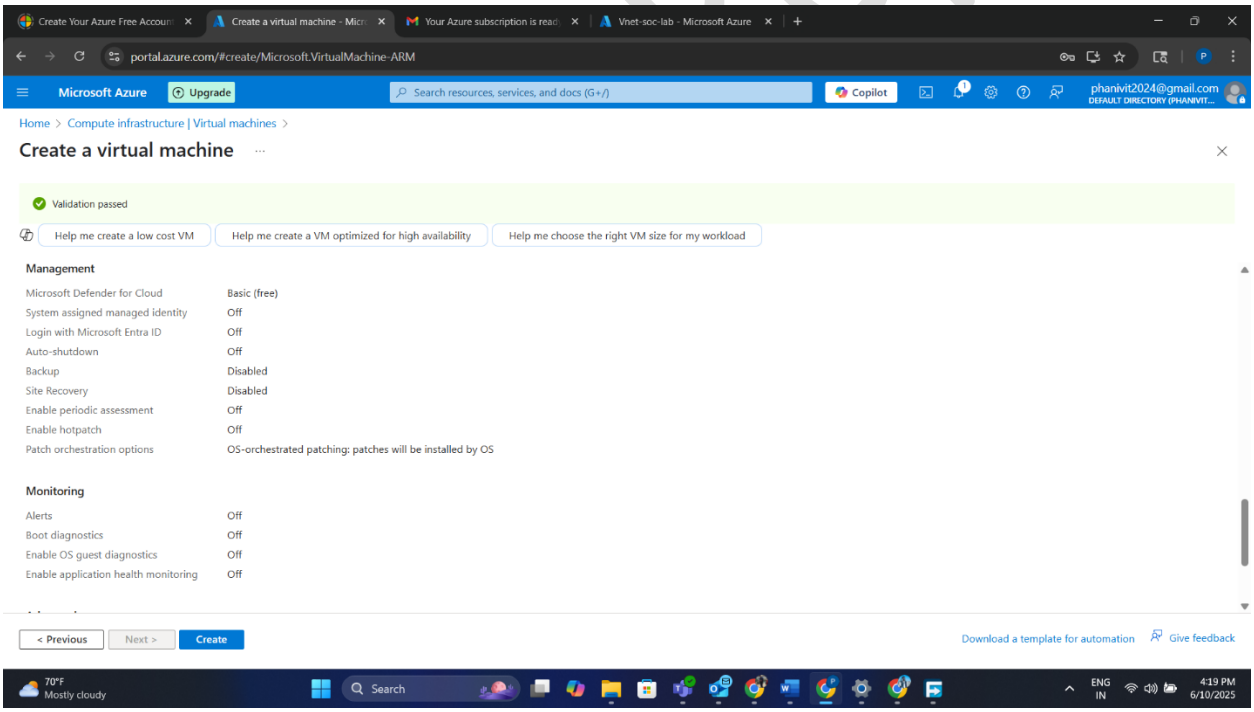

Create Your Azure Free Accoun
Create a virtual machine - Micr
Verify your email address - pha
portal.azure.com/#create/Microsoft.VirtualMachine
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics Disks Networking Management Monitoring Advanced Tags Review + create
Configure monitoring options for your VM.
Alerts
Enable recommended alert rules
Diagnostics
Boot diagnostics
Enable with managed storage account (recommended)
Enable with custom storage account
Disable
Enable OS guest diagnostics
Health
Enable application health monitoring
< Previous
Next : Advanced >
Review + create
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
3:42 PM
6/10/2025

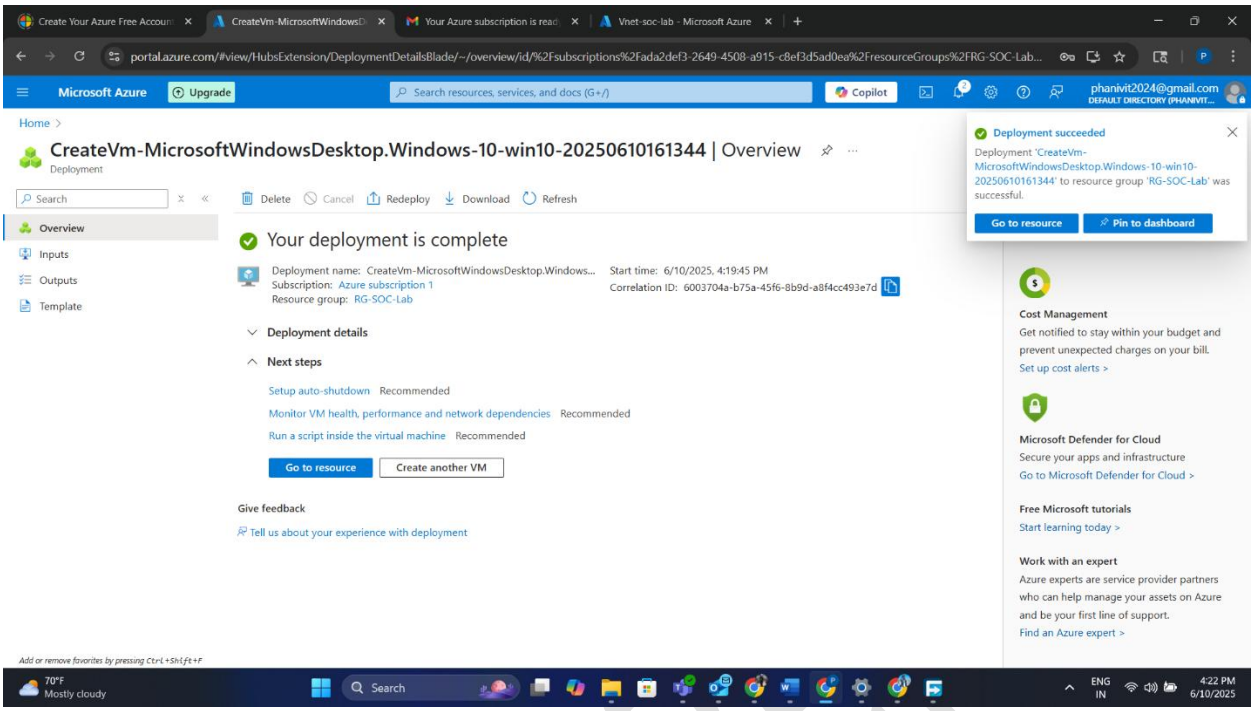

Create Your Azure Free Accoun
Create a virtual machine - Micr
Your Azure subscription is read
Vnet-soc-lab - Microsoft Azure
portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics Disks Networking Management Monitoring Advanced Tags Review + create
Price
1 X Standard D2s v3
by Microsoft
Terms of use | Privacy policy
Subscription credits apply
0.0960 USD/hr
Pricing for other VM sizes
TERMS
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.
You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.
< Previous
Next >
Create
Download a template for automation
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
4:18 PM
6/10/2025

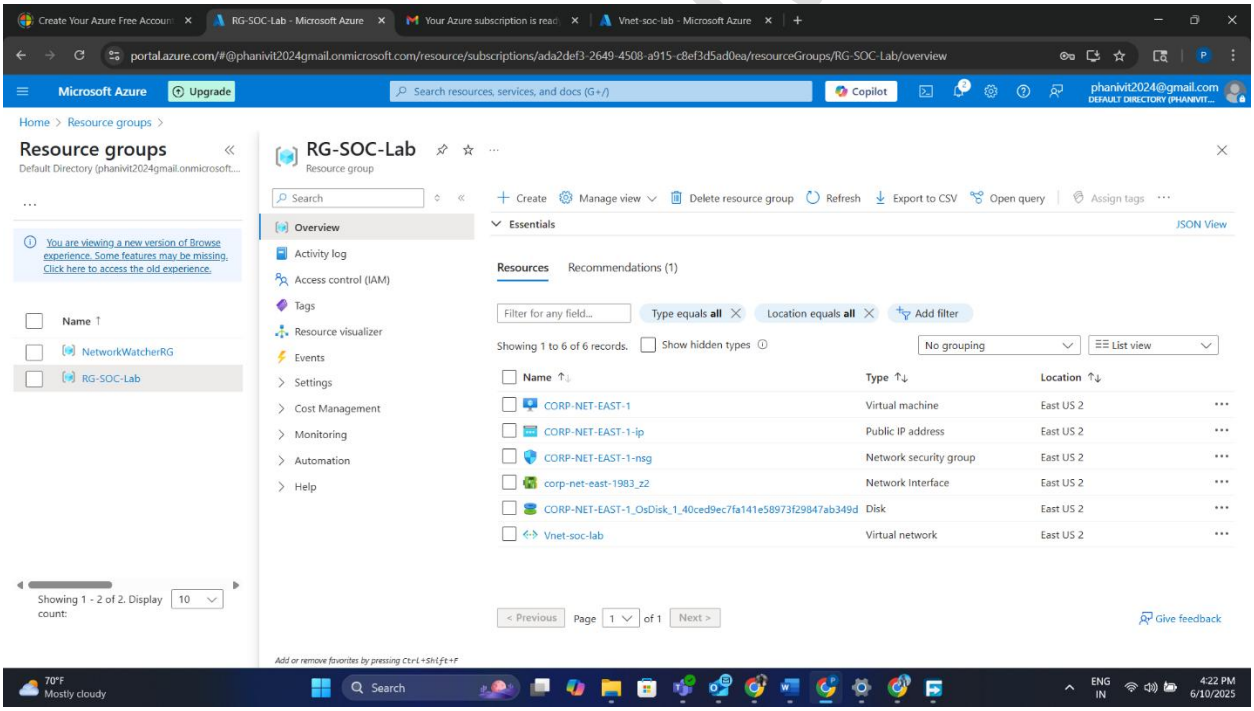

Create Your Azure Free Accoun
Create a virtual machine - Micr
Your Azure subscription is read
Vnet-soc-lab - Microsoft Azure
portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Subscription Azure subscription 1
Resource group RG-SOC-Lab
Virtual machine name CORP-NET-EAST-1
Region East US 2
Availability options Availability zone
Zone options Self-selected zone
Availability zone 2
Security type Trusted launch virtual machines
Enable secure boot Yes
Enable vTPM Yes
Integrity monitoring No
Image Windows 10 Pro, version 22H2 - Gen2
VM architecture x64
Size Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation No
< Previous
Next >
Create
Download a template for automation
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
4:18 PM
6/10/2025

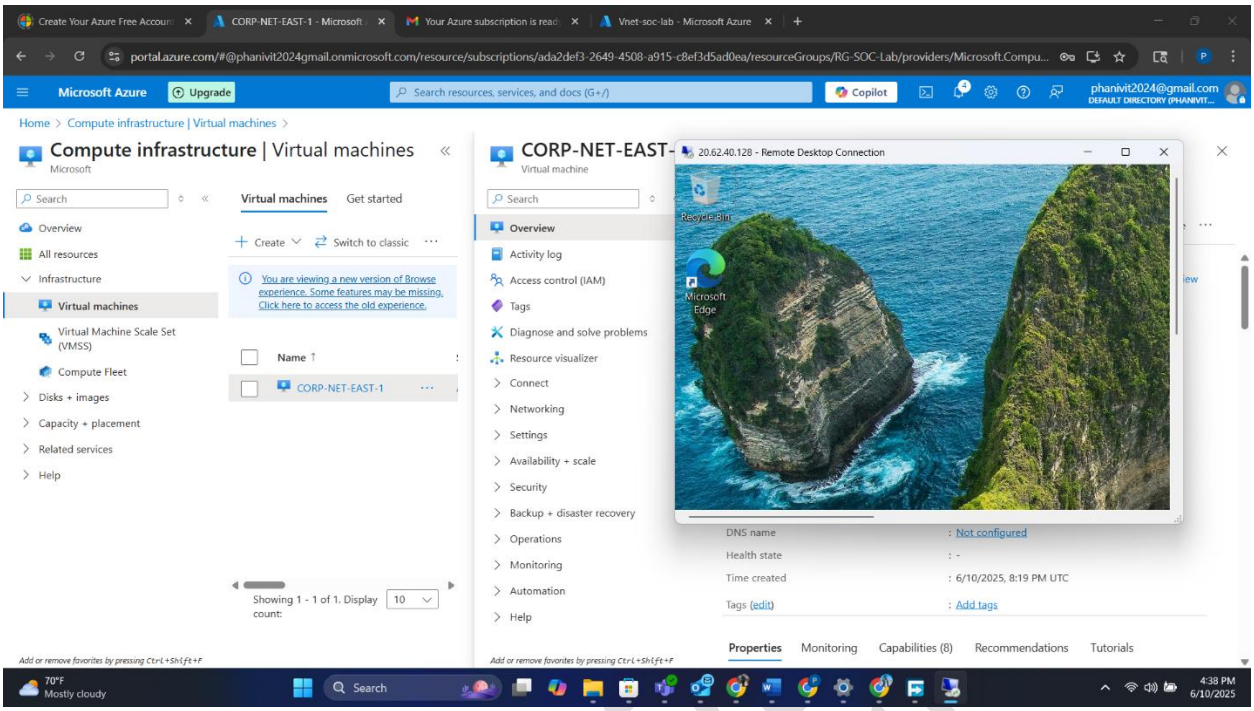

Create Your Azure Free Accoun
Create a virtual machine - Micr
Your Azure subscription is read
Vnet-soc-lab - Microsoft Azure
portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Enable Hibernation No
Username labuser
Public inbound ports RDP
Already have a Windows license? Yes
License type Windows Client
Azure Spot No
Disks
OS disk size Image default
OS disk type Premium SSD LRS
Use managed disks Yes
Delete OS disk with VM Enabled
Ephemeral OS disk No
Networking
Virtual network Vnet-soc-lab
Subnet default (10.0.0.0/24)
< Previous
Next >
Create
Download a template for automation
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
4:18 PM
6/10/2025

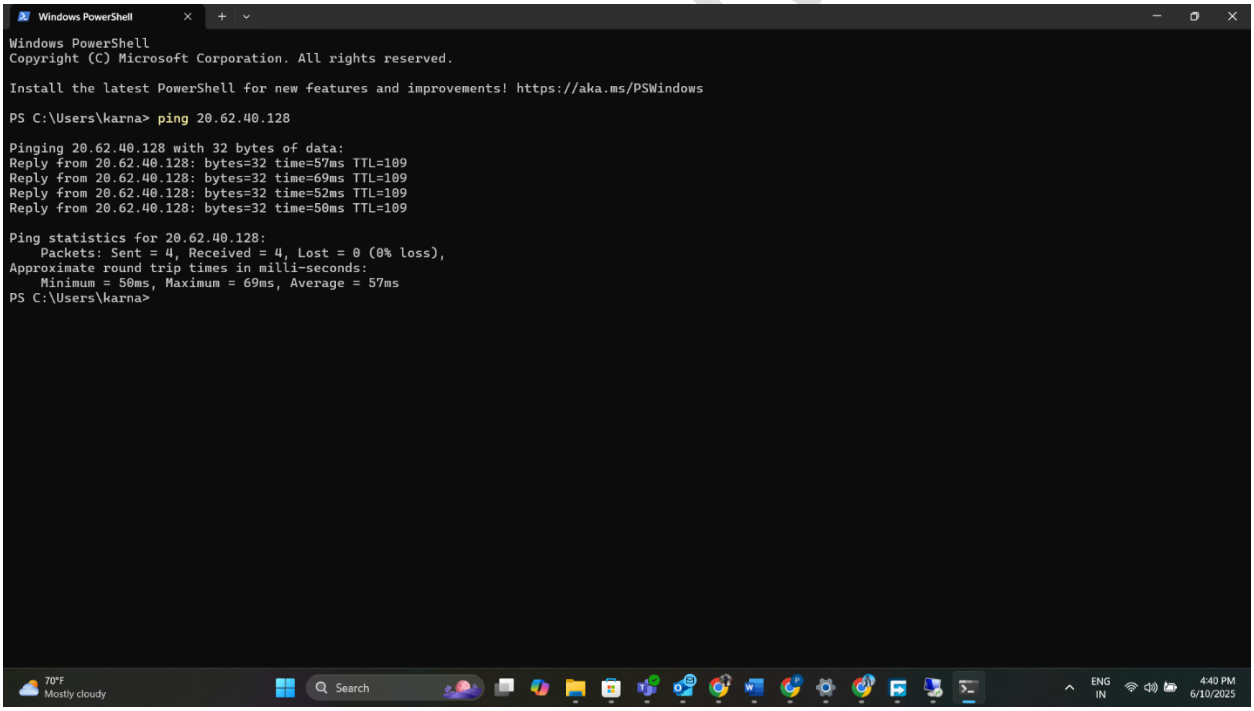

Create Your Azure Free Accoun
Create a virtual machine - Micr
Your Azure subscription is read
Vnet-soc-lab - Microsoft Azure
portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Networking
Virtual network Vnet-soc-lab
Subnet default (10.0.0.0/24)
Public IP (new) CORP-NET-EAST-1-ip
Accelerated networking On
Place this virtual machine behind an existing load balancing solution? No
Delete public IP and NIC when VM is deleted Disabled
Management
Microsoft Defender for Cloud Basic (free)
System assigned managed identity Off
Login with Microsoft Entra ID Off
Auto-shutdown Off
Backup Disabled
Site Recovery Disabled
Enable periodic assessment Off
< Previous
Next >
Create
Download a template for automation
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
4:18 PM
6/10/2025


Create Your Azure Free Accoun
Create a virtual machine - Micr
Your Azure subscription is read
Vnet-soc-lab - Microsoft Azure
portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Management
Microsoft Defender for Cloud Basic (free)
System assigned managed identity Off
Login with Microsoft Entra ID Off
Auto-shutdown Off
Backup Disabled
Site Recovery Disabled
Enable periodic assessment Off
Enable hotpatch Off
Patch orchestration options OS-orchestrated patching: patches will be installed by OS
Monitoring
Alerts Off
Boot diagnostics Off
Enable OS guest diagnostics Off
Enable application health monitoring Off
< Previous
Next >
Create
Download a template for automation
Give feedback
70°F
Mostly cloudy
Search
ENG
IN
4:19 PM
6/10/2025


Create Your Azure Free Account
CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20250610161344 | Overview
Deployment
Your deployment is complete
Deployment succeeded
Deployment 'CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20250610161344' to resource group 'RG-SOC-Lab' was successful.
Go to resource
Pin to dashboard
Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows...
Subscription: Azure subscription 1
Resource group: RG-SOC-Lab
Start time: 6/10/2025, 4:19:45 PM
Correlation ID: 6003704a-b75a-45f6-8b9d-a8f4cc493e7d
Deployment details
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM
Give feedback
Tell us about your experience with deployment
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
70°F
Mostly cloudy
4:22 PM
6/10/2025


RG-SOC-Lab - Microsoft Azure
Resource groups
RG-SOC-Lab
Resource group
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Essentials
JSON View
Resources
Recommendations (1)
Showing 1 to 6 of 6 records.
Name
Type
Location
CORP-NET-EAST-1
Virtual machine
East US 2
CORP-NET-EAST-1-ip
Public IP address
CORP-NET-EAST-1-nsg
Network security group
corp-net-east-1983_z2
Network Interface
CORP-NET-EAST-1_OsDisk_1_40ced9ec7fa141e58973f29847ab349d
Disk
Vnet-soc-lab
Virtual network
Give feedback
70°F
Mostly cloudy
4:22 PM
6/10/2025


Microsoft Azure
Upgrade
Copilot
Home > Compute infrastructure | Virtual machines
Compute infrastructure | Virtual machines
Microsoft
Search
Overview
All resources
Infrastructure
Virtual machines
Virtual Machine Scale Set (VMSS)
Compute Fleet
Disks + images
Capacity + placement
Related services
Help
Virtual machines
Get started
Create
Switch to classic
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
CORP-NET-EAST-1
Showing 1 - 1 of 1. Display count: 10
CORP-NET-EAST-
Virtual machine
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
20.62.40.128 - Remote Desktop Connection
Recycle Bin
Microsoft Edge
DNS name : Not configured
Health state : -
Time created : 6/10/2025, 8:19 PM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
70°F
Mostly cloudy
Search
4:38 PM
6/10/2025

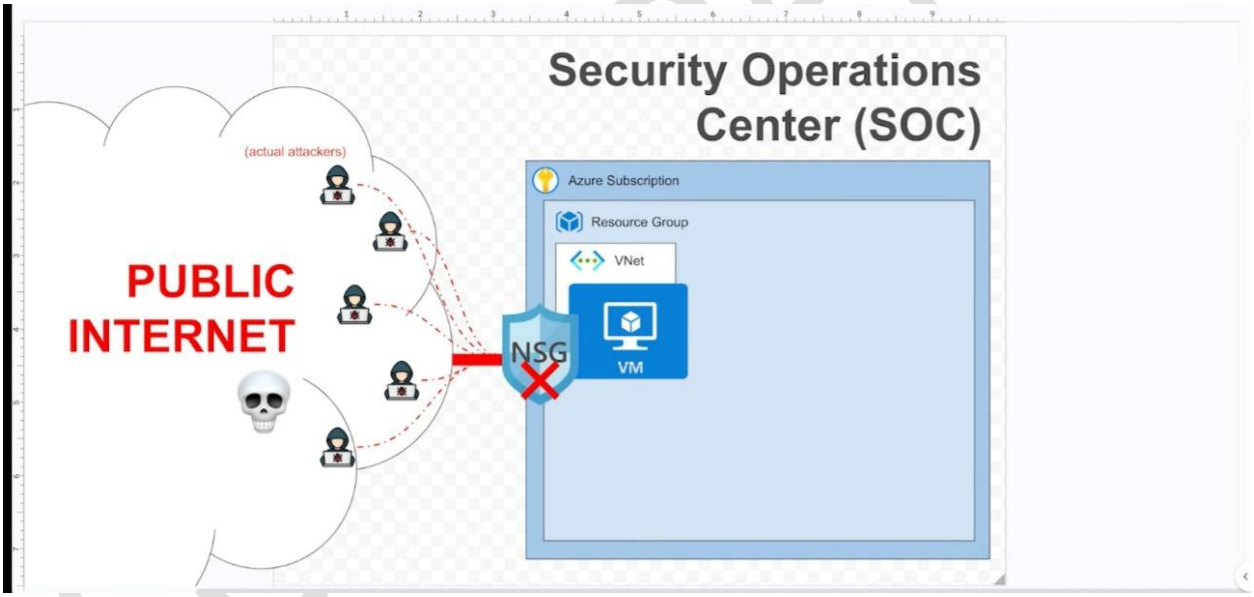

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\karna> ping 20.62.40.128
Pinging 20.62.40.128 with 32 bytes of data:
Reply from 20.62.40.128: bytes=32 time=57ms TTL=109
Reply from 20.62.40.128: bytes=32 time=69ms TTL=109
Reply from 20.62.40.128: bytes=32 time=52ms TTL=109
Reply from 20.62.40.128: bytes=32 time=50ms TTL=109
Ping statistics for 20.62.40.128:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 69ms, Average = 57ms
PS C:\Users\karna>
70°F
Mostly cloudy
Search
ENG
IN
4:40 PM
6/10/2025

5. Configuring Network Security Group (NSG)

To allow attacker interaction:

- The default RDP-only inbound rule was deleted.
- A new inbound rule was added:
    - Source: Any
    - Destination: Any
    - Protocol: Any
    - Port Range: *
    - Action: Allow

This effectively opens the VM to all inbound traffic, simulating an exposed public system.

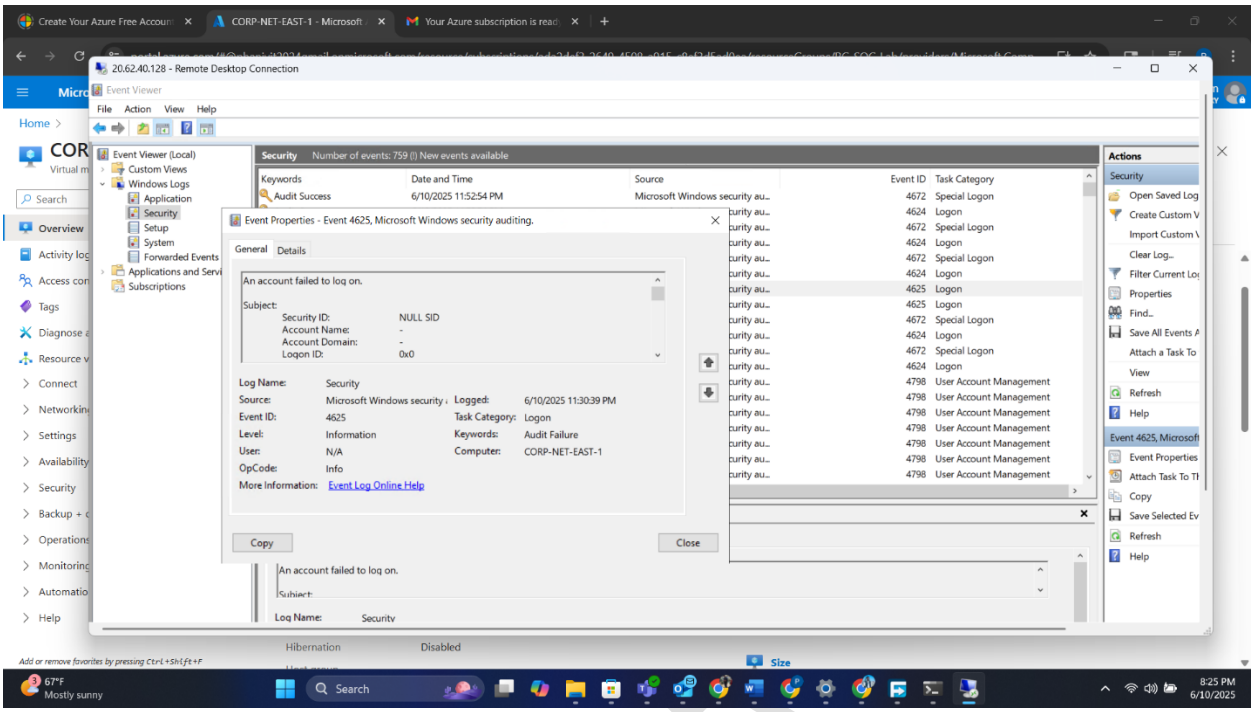


6. Disabling Windows Defender Firewall

To ensure all incoming traffic is logged:

- Remote Desktop Protocol (RDP) was used to log into the VM.
- Windows Firewall was accessed via wf.msc.
- The firewall was turned off for Domain, Private, and Public profiles.

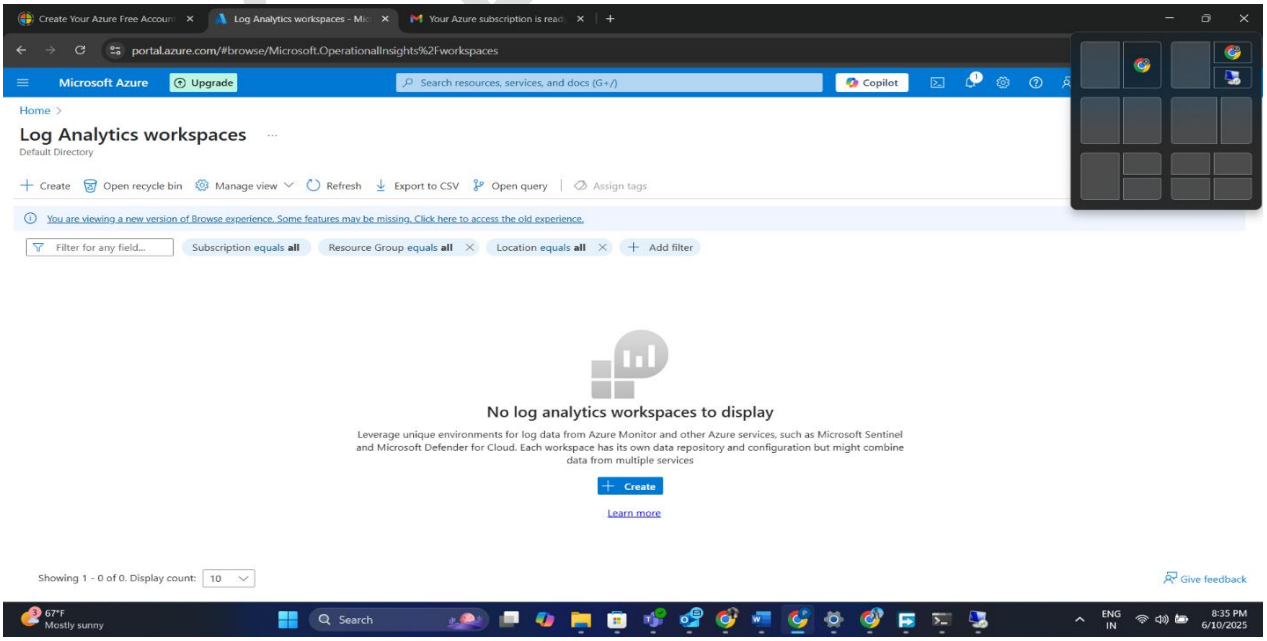
This further simulates a vulnerable system and guarantees event logging.



7. Generating Simulated Attack Logs

To simulate brute-force attempts:

- Several failed login attempts were made using fake usernames like employee.
- These actions triggered Windows Security Event ID 4625 (failed logon attempt).

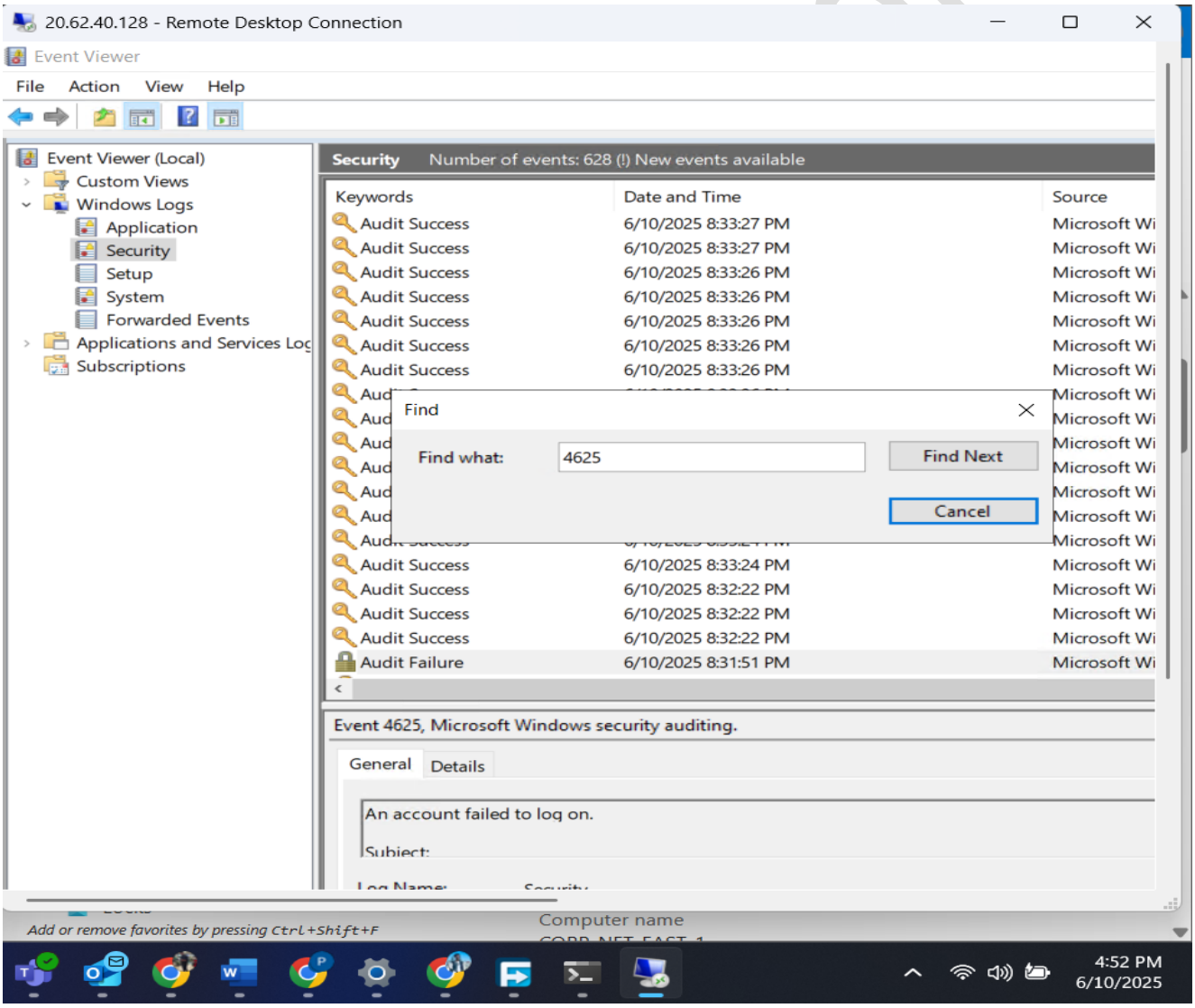


8. Verifying Logs Using Event Viewer

Within the VM:

- Event Viewer was opened.
- Navigated to: Windows Logs > Security
- Filtered logs by Event ID 4625.

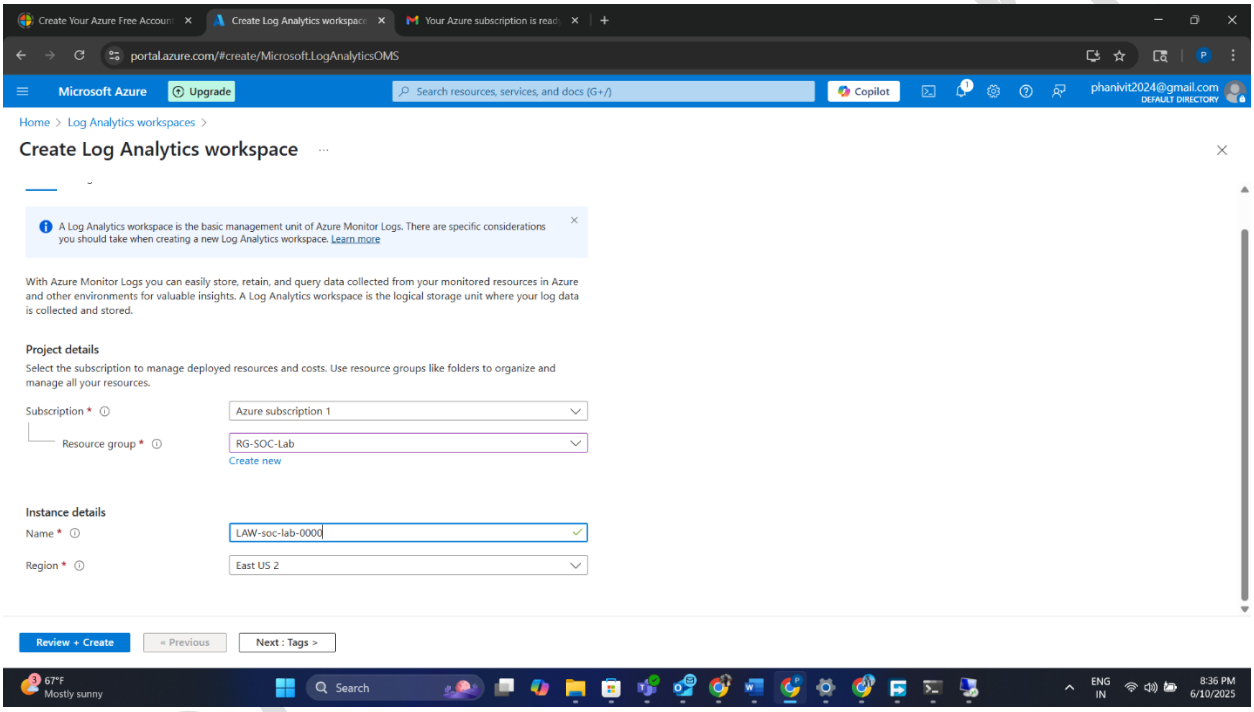
Details such as the attempted username, source IP, and failure reasons were verified.

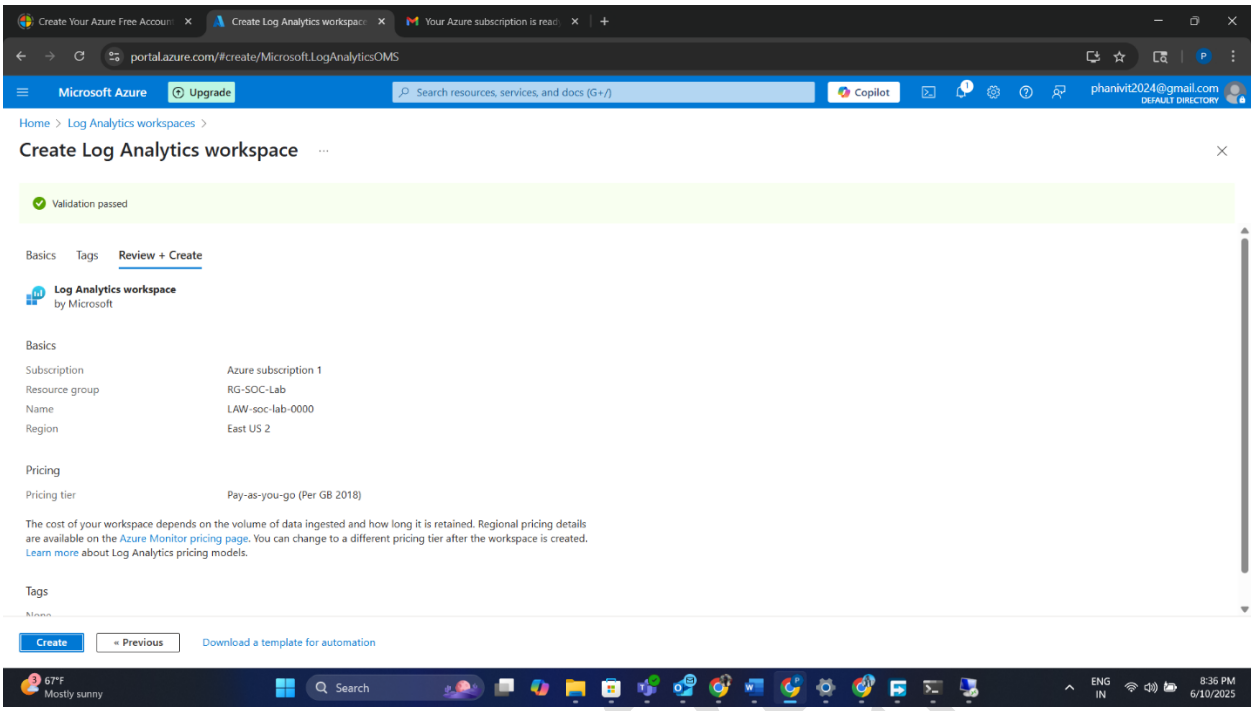


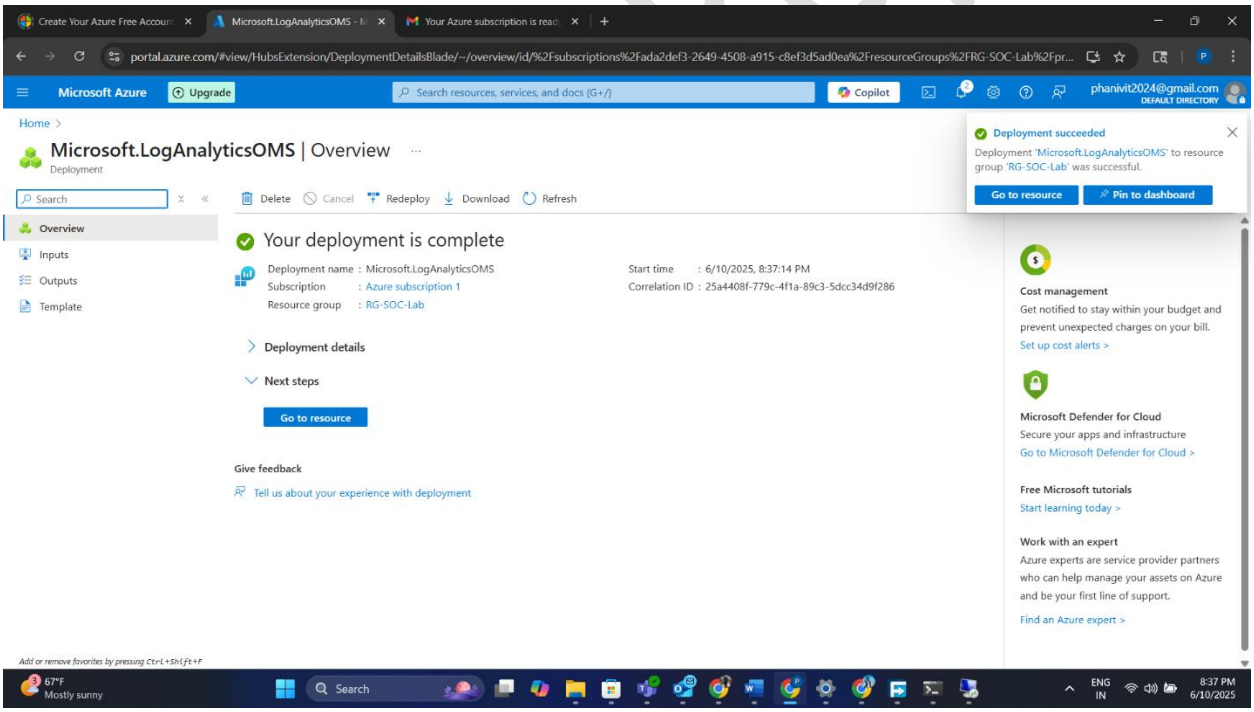
9. Creating Log Analytics Workspace (LAW)

A Log Analytics Workspace acts as a centralized repository:

- Created within **rg-socklab**
- Named **law-socklab-east2**
- Used to ingest logs forwarded from Azure resources, including VMs.



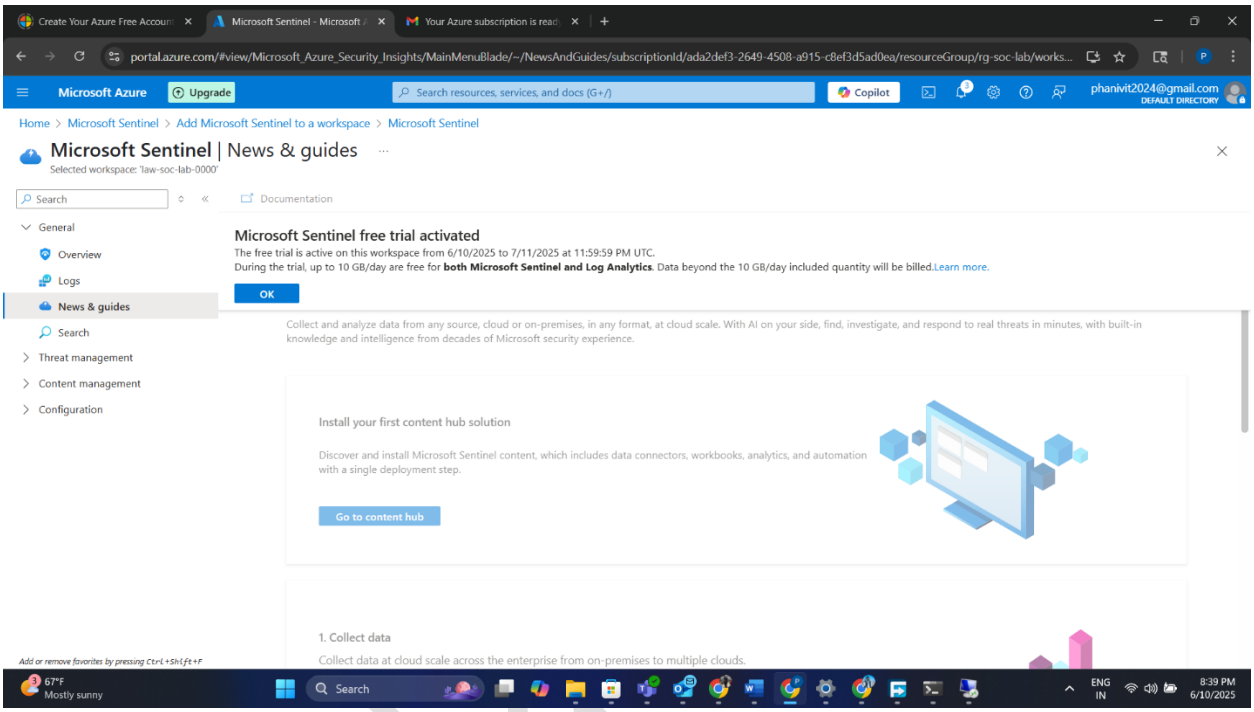

Create Your Azure Free Accoun
Create Log Analytics workspac
Your Azure subscription is read
portal.azure.com/#create/Microsoft.LogAnalyticsOMS
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home > Log Analytics workspaces >
Create Log Analytics workspace
Validation passed
Basics
Tags
Review + Create
Log Analytics workspace
by Microsoft
Basics
Subscription
Azure subscription 1
Resource group
RG-SOC-Lab
Name
LAW-soc-lab-0000
Region
East US 2
Pricing
Pricing tier
Pay-as-you-go (Per GB 2018)
The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created.
Learn more about Log Analytics pricing models.
Tags
Create
« Previous
Download a template for automation
67°F
Mostly sunny
Search
ENG
IN
8:36 PM
6/10/2025


Create Your Azure Free Accoun
Microsoft.LogAnalyticsOMS - M
Your Azure subscription is read
portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2Fada2def3-2649-4508-a915-c8ef3d5ad0ea%2FresourceGroups%2FRG-SOC-Lab%2Fpr...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY
Home >
Microsoft.LogAnalyticsOMS | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : Microsoft.LogAnalyticsOMS
Subscription : Azure subscription 1
Resource group : RG-SOC-Lab
Start time : 6/10/2025, 8:37:14 PM
Correlation ID : 25a4408f-779c-4f1a-89c3-5dcc34d9f286
Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
Deployment succeeded
Deployment 'Microsoft.LogAnalyticsOMS' to resource group 'RG-SOC-Lab' was successful.
Go to resource
Pin to dashboard
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Add or remove favorites by pressing Ctrl+Shift+F
67°F
Mostly sunny
Search
ENG
IN
8:37 PM
6/10/2025

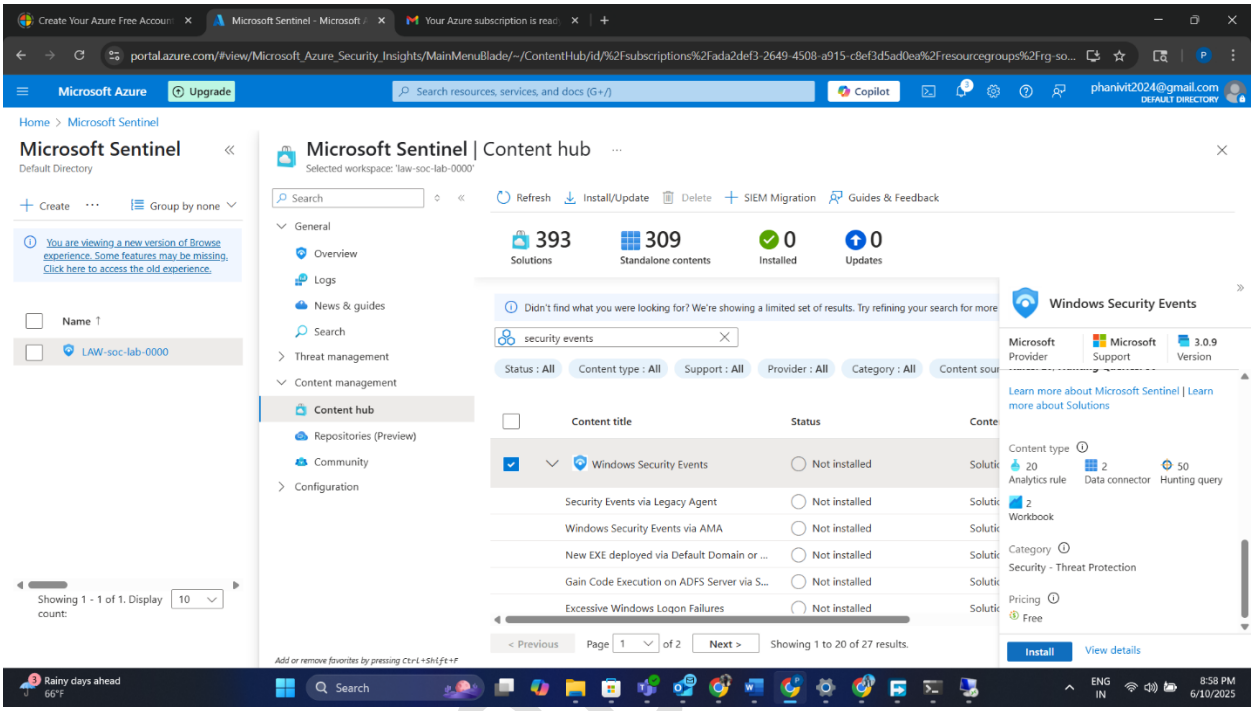
10. Deploying Microsoft Sentinel Instance

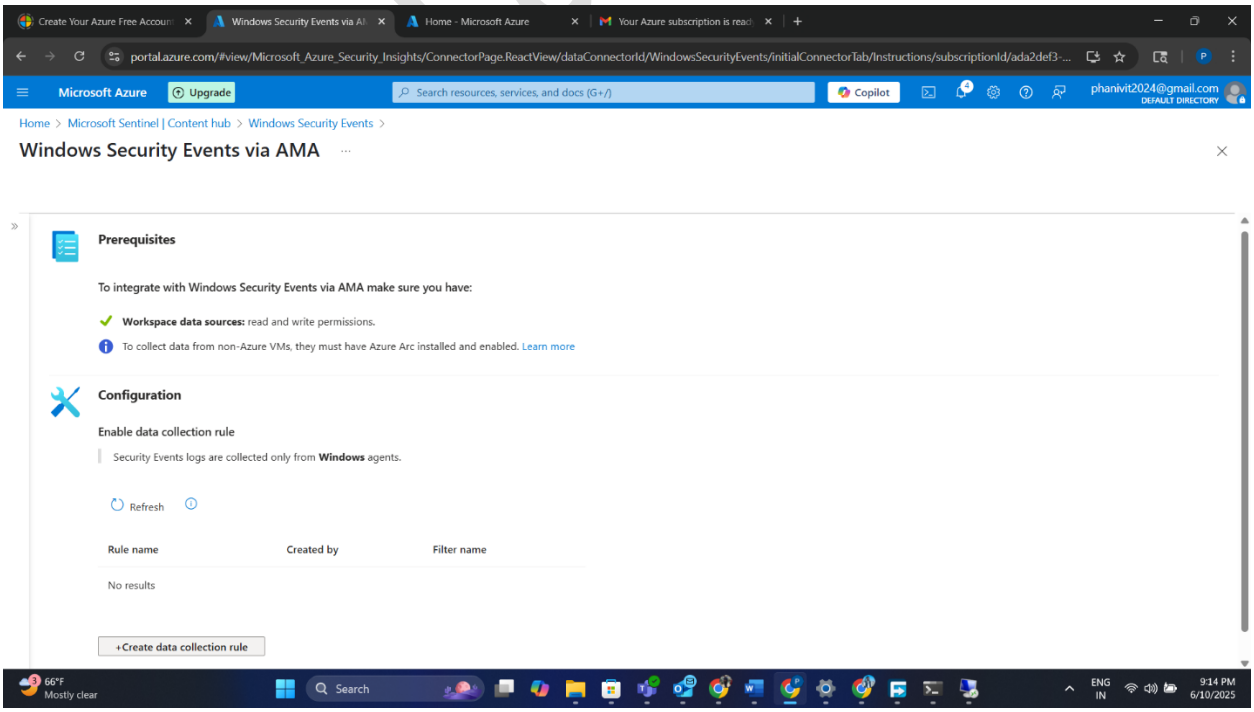
Microsoft Sentinel, a cloud-native SIEM/SOAR platform, was added to the LAW:

- The LAW created earlier was selected.
- Sentinel connects to LAW to run detection queries, dashboards, and incidents.



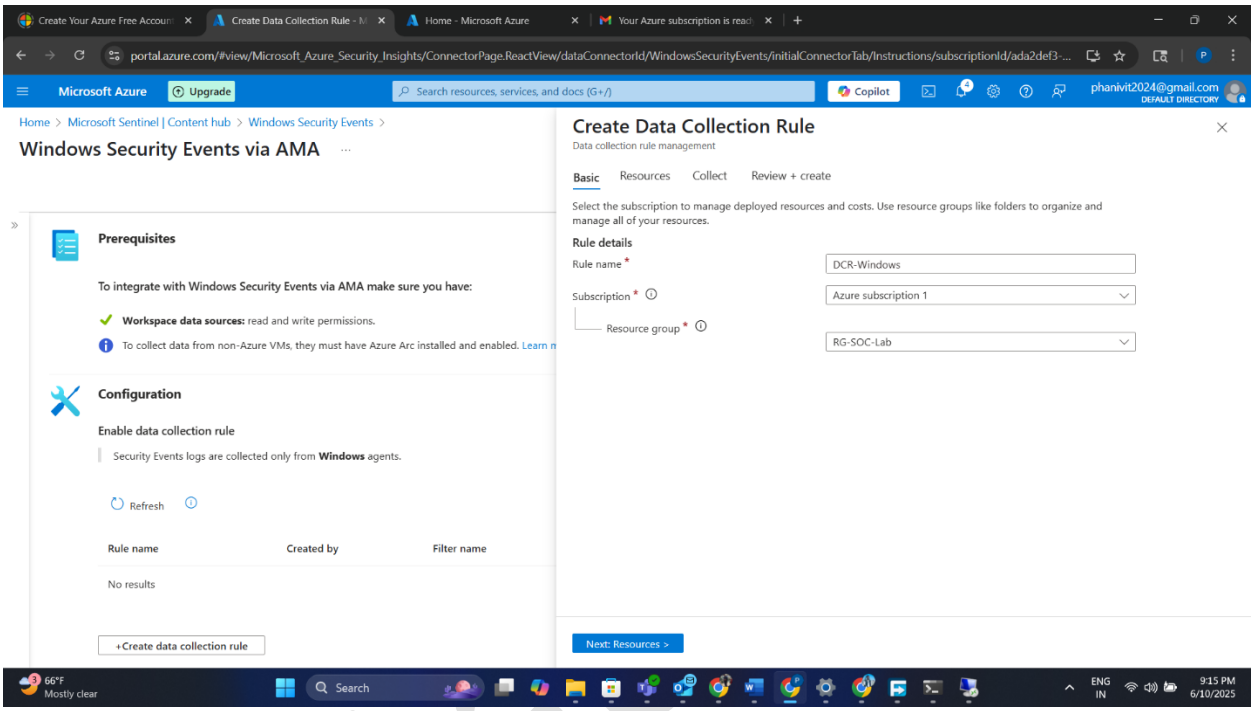
11. Enabling Log Forwarding with Azure Monitoring Agent (AMA)

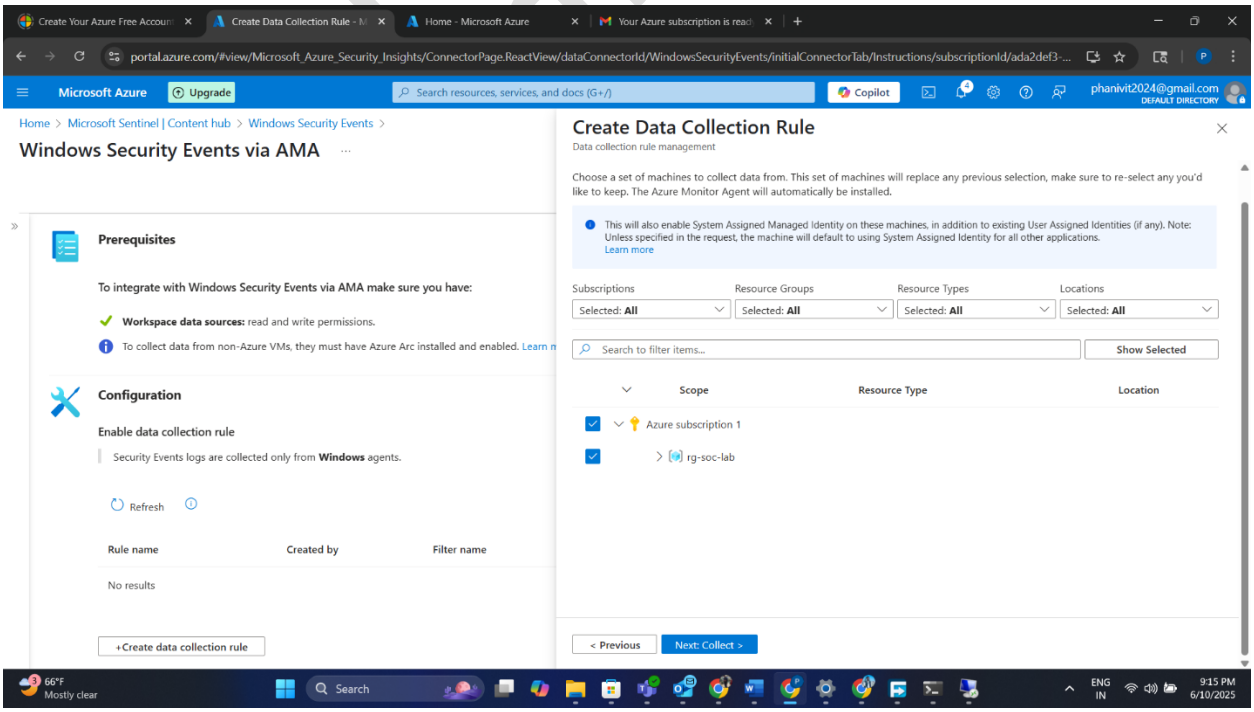


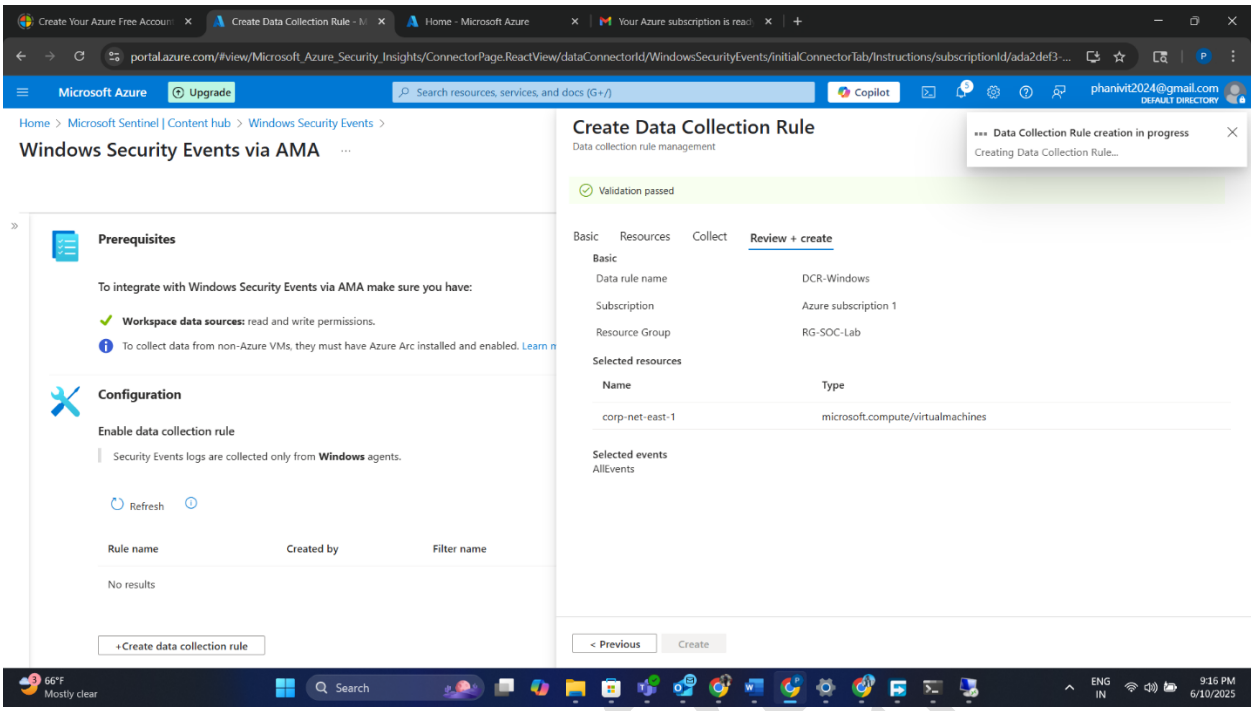


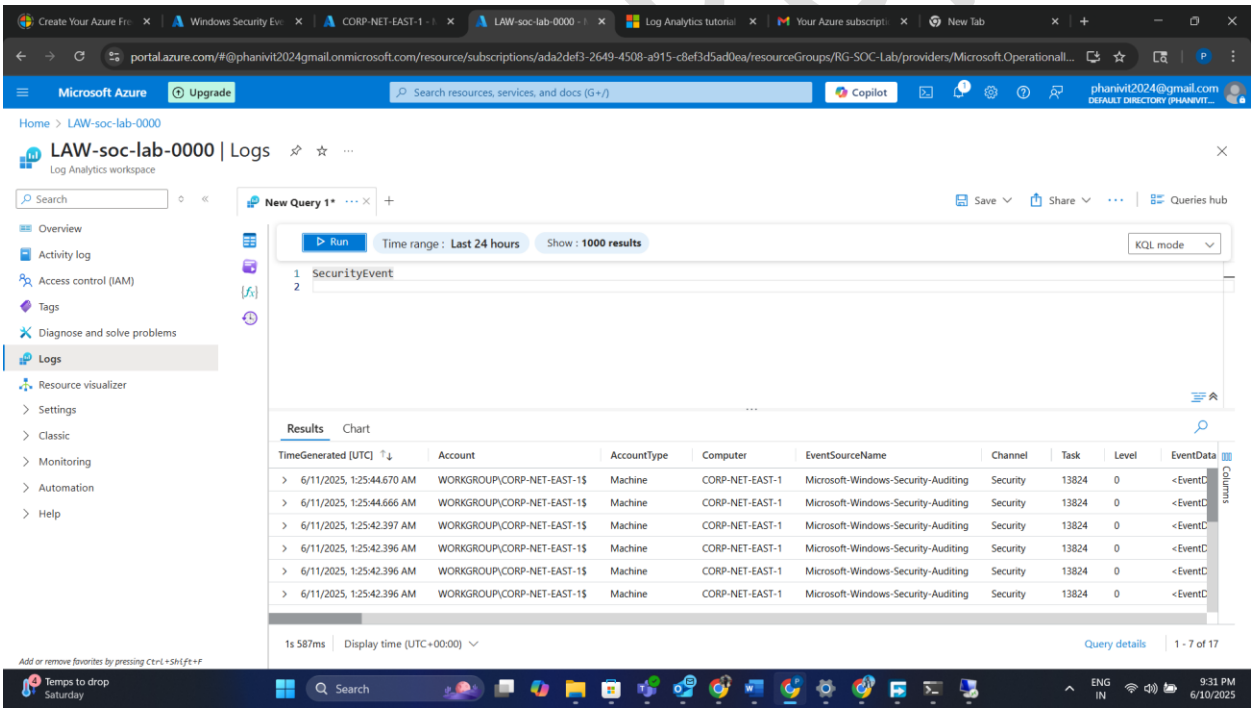
To connect VM logs to LAW:

- Windows Security Events Data Connector (Windows Security Events via AMA) was installed.



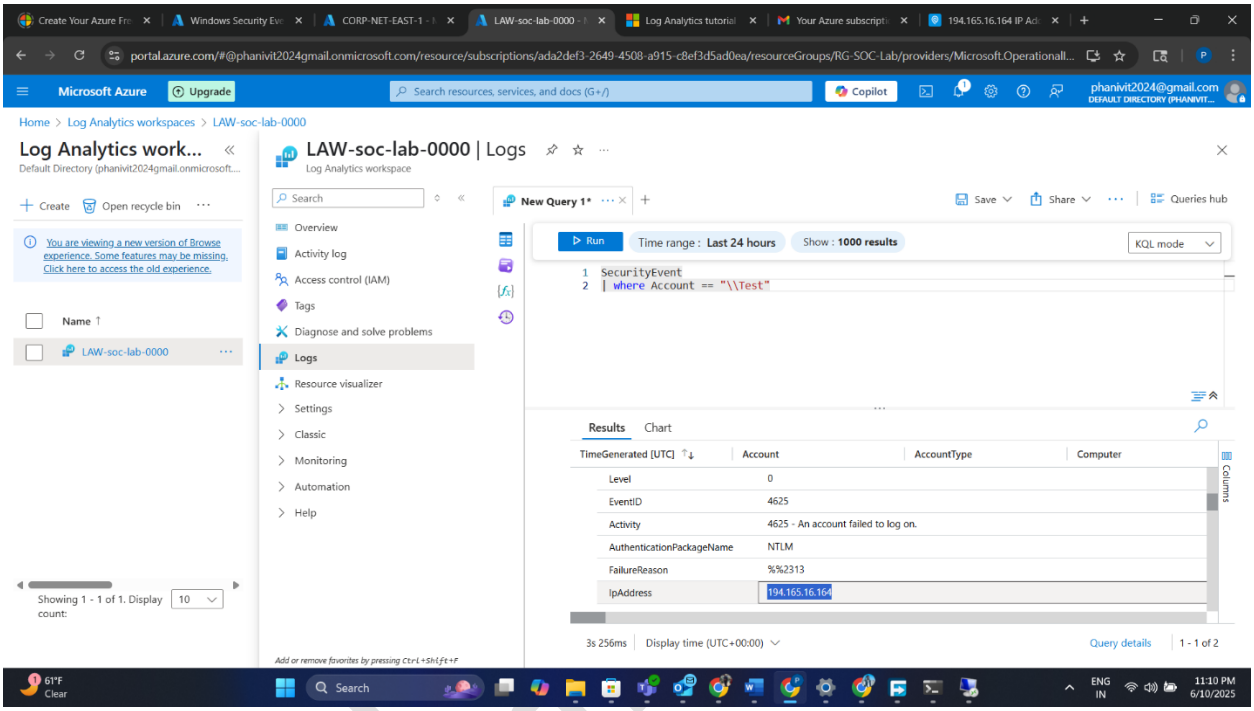


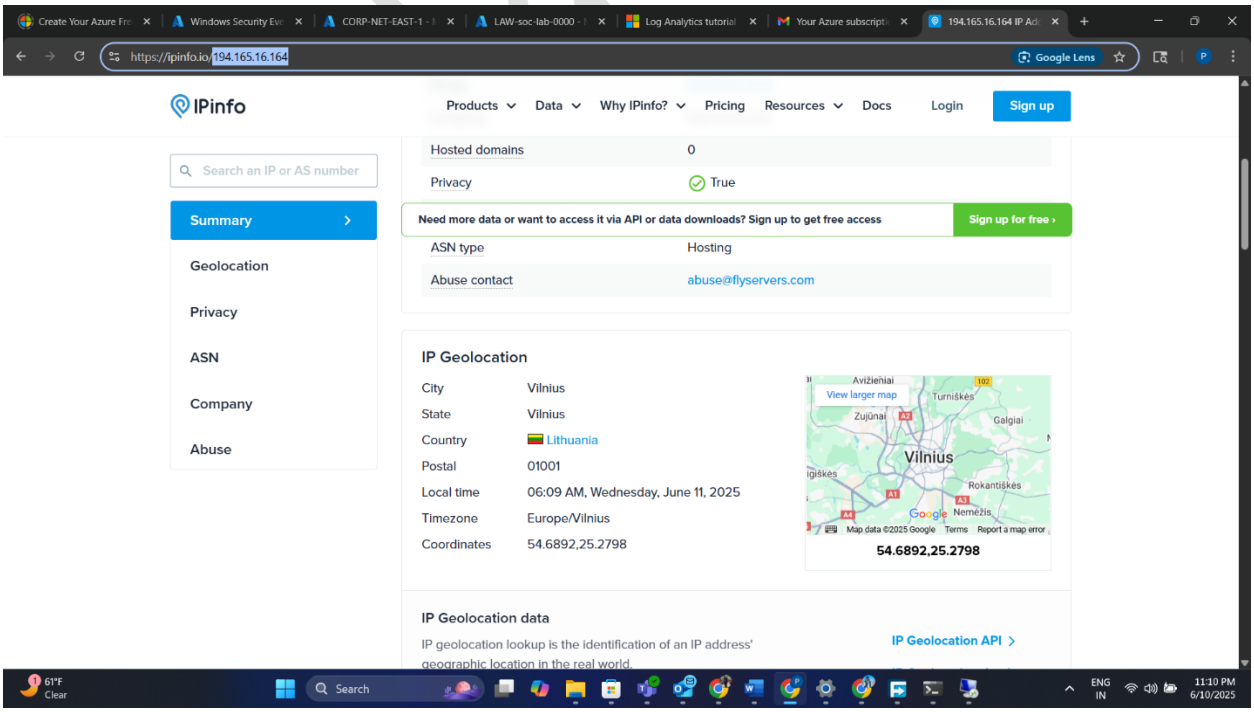

Create Data Collection Rule
Windows Security Events via AMA
Prerequisites
To integrate with Windows Security Events via AMA make sure you have:
Workspace data sources: read and write permissions.
Configuration
Enable data collection rule
Security Events logs are collected only from Windows agents.
Refresh
Rule name
Created by
Filter name
No results
+Create data collection rule
Data Collection Rule creation in progress
Creating Data Collection Rule...
Validation passed
Basic
Resources
Collect
Review + create
Data rule name
DCR-Windows
Subscription
Azure subscription 1
Resource Group
RG-SOC-Lab
Selected resources
Name
Type
corp-net-east-1
microsoft.compute/virtualmachines
Selected events
AllEvents
< Previous
Create


LAW-soc-lab-0000 | Logs
Log Analytics workspace
New Query 1*
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
SecurityEvent
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Results
Chart
TimeGenerated [UTC]
Account
AccountType
Computer
EventSourceName
Channel
Task
Level
EventData
6/11/2025, 1:25:44.670 AM
WORKGROUP\CORP-NET-EAST-1$
Machine
CORP-NET-EAST-1
Microsoft-Windows-Security-Auditing
Security
13824
0
6/11/2025, 1:25:44.666 AM
6/11/2025, 1:25:42.397 AM
6/11/2025, 1:25:42.396 AM
6/11/2025, 1:25:42.396 AM
6/11/2025, 1:25:42.396 AM
1s 587ms
Display time (UTC+00:00)
Query details
1 - 7 of 17

- A Data Collection Rule (**DCR**) was created to:
    - Link the VM to the LAW
    - Forward all security events

Confirmation of success was verified in the VM's Extensions tab.





12. Confirming Log Ingestion via KQL Queries

In the LAW > Logs tab:

- Queried SecurityEvent table using KQL
- Verified presence of Event ID **4625**

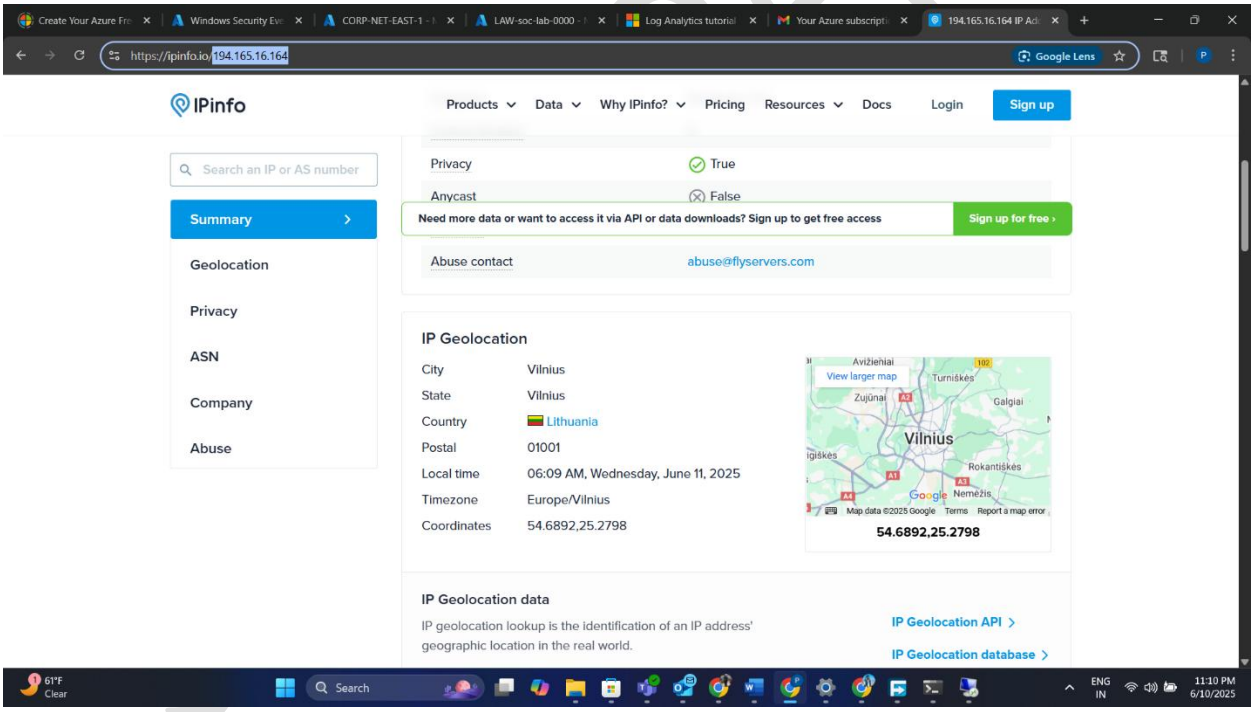
Example query:

SecurityEvent

| where EventID == 4625

| project TimeGenerated, Account, Computer, IPAddress #

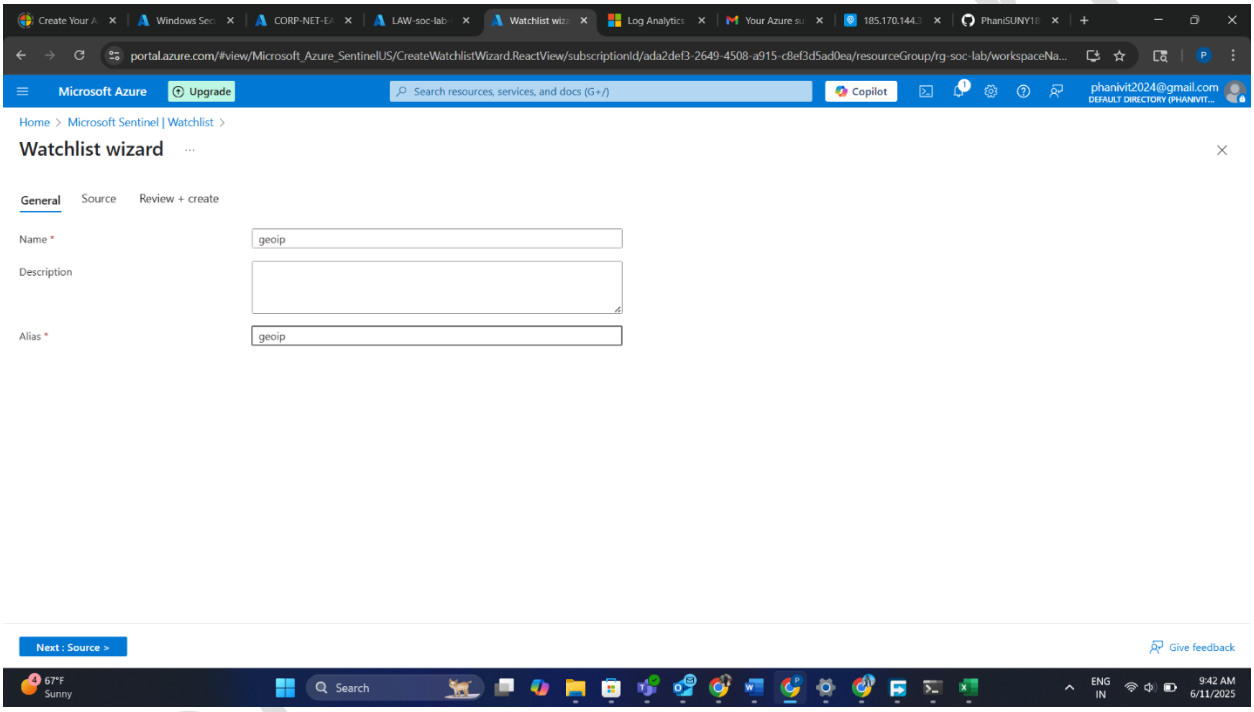
Thousands of failed login attempts from global IPs appeared within minutes.

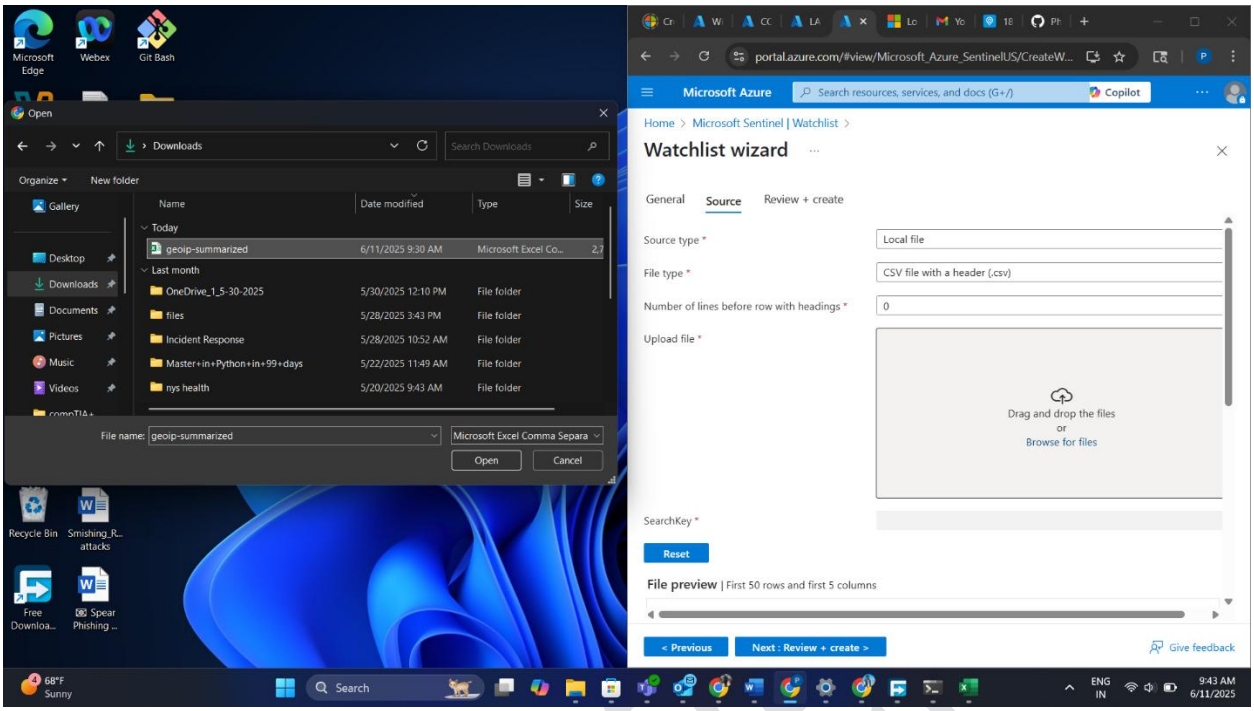


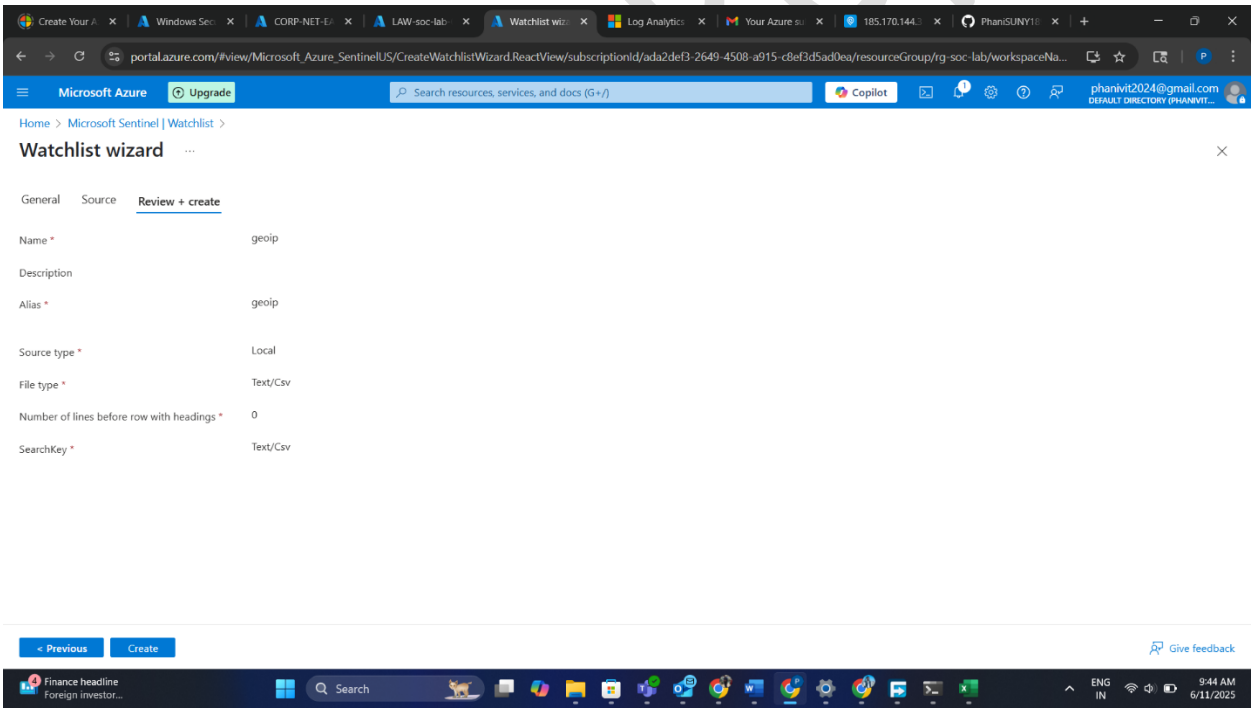
13. Uploading GeoIP Watchlist to Sentinel

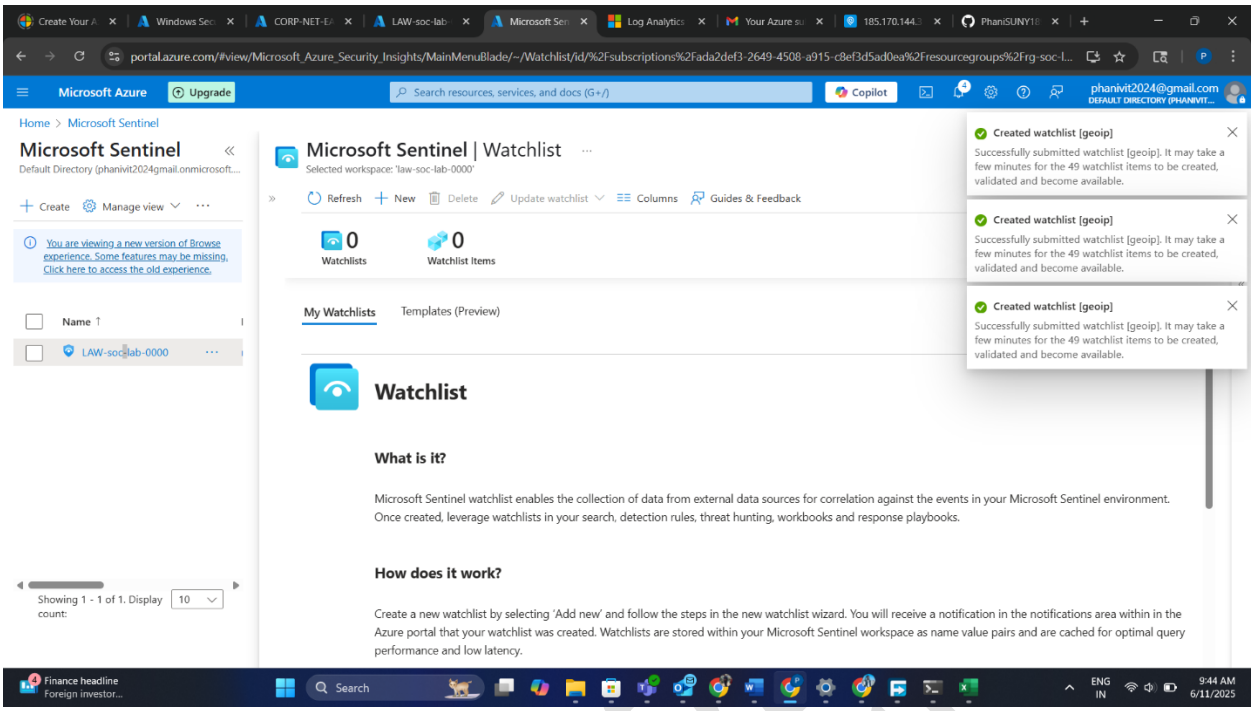
To enrich IPs with location data:

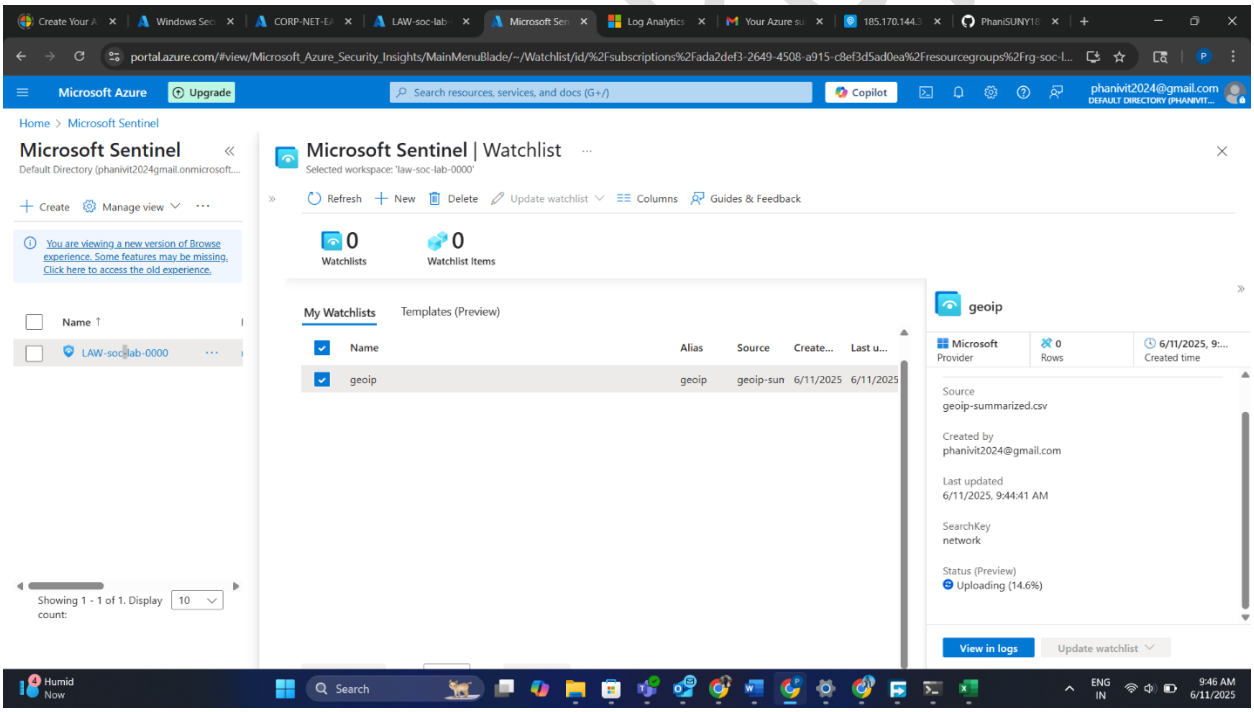
- A CSV file (geoip-summarized.csv) was uploaded as a Watchlist in Sentinel
- Watchlist fields included: IP range, latitude, longitude, city, country
- Name and alias: GeoIP and geoip




Microsoft Edge
Webex
Git Bash
Open
Downloads
Search Downloads
Organize
New folder
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
Name
Date modified
Type
Size
Today
geoip-summarized
6/11/2025 9:30 AM
Microsoft Excel Co...
Last month
OneDrive_1_5-30-2025
5/30/2025 12:10 PM
File folder
files
5/28/2025 3:43 PM
Incident Response
5/28/2025 10:52 AM
Master+in+Python+in+99+days
5/22/2025 11:49 AM
nys health
5/20/2025 9:43 AM
File name: geoip-summarized
Microsoft Excel Comma Separa
Open
Cancel
Recycle Bin
Smishing_R... attacks
Free Downloa...
Spear Phishing ...
portal.azure.com/#view/Microsoft_Azure_SentinelUS/CreateW...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel | Watchlist >
Watchlist wizard
General
Source
Review + create
Source type *
Local file
File type *
CSV file with a header (.csv)
Number of lines before row with headings *
0
Upload file *
Drag and drop the files
or
Browse for files
SearchKey *
Reset
File preview | First 50 rows and first 5 columns
< Previous
Next : Review + create >
Give feedback
68°F
Sunny
Search
ENG
IN
9:43 AM
6/11/2025


portal.azure.com/#view/Microsoft_Azure_SentinelUS/CreateWatchlistWizard.ReactView/subscriptionId/ada2def3-2649-4508-a915-c8ef3d5ad0ea/resourceGroup/rg-soc-lab/workspaceNa...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Microsoft Sentinel | Watchlist >
Watchlist wizard
General
Source
Review + create
Name *
geoip
Description
Alias *
geoip
Source type *
Local
File type *
Text/Csv
Number of lines before row with headings *
0
SearchKey *
Text/Csv
< Previous
Create
Give feedback
Finance headline
Foreign investor...
Search
ENG
IN
9:44 AM
6/11/2025


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Microsoft Sentinel
Microsoft Sentinel
Default Directory (phanivit2024gmail.onmicrosoft....
Create
Manage view
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-soc-lab-0000
Showing 1 - 1 of 1. Display count:
10
Microsoft Sentinel | Watchlist
Selected workspace: 'law-soc-lab-0000'
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
0
Watchlists
0
Watchlist Items
My Watchlists
Templates (Preview)
Created watchlist [geoip]
Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.
Created watchlist [geoip]
Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.
Created watchlist [geoip]
Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.
Watchlist
What is it?
Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.
How does it work?
Create a new watchlist by selecting 'Add new' and follow the steps in the new watchlist wizard. You will receive a notification in the notifications area within in the Azure portal that your watchlist was created. Watchlists are stored within your Microsoft Sentinel workspace as name value pairs and are cached for optimal query performance and low latency.
Search
ENG
IN
9:44 AM
6/11/2025


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Microsoft Sentinel
Microsoft Sentinel
Default Directory (phanivit2024gmail.onmicrosoft....
Create
Manage view
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-soc-lab-0000
Showing 1 - 1 of 1. Display count:
10
Microsoft Sentinel | Watchlist
Selected workspace: 'law-soc-lab-0000'
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
0
Watchlists
0
Watchlist Items
My Watchlists
Templates (Preview)
Name
Alias
Source
Create...
Last u...
geoip
geoip
geoip-sun
6/11/2025
6/11/2025
geoip
Microsoft
Provider
0
Rows
6/11/2025, 9:...
Created time
Source
geoip-summarized.csv
Created by
phanivit2024@gmail.com
Last updated
6/11/2025, 9:44:41 AM
SearchKey
network
Status (Preview)
Uploading (14.6%)
View in logs
Update watchlist
Search
ENG
IN
9:46 AM
6/11/2025

14. Joining Security Logs with GeoIP Data

Using KQL, logs were joined with the Watchlist to extract attacker locations:

let geo = _GetWatchlist("geoip");

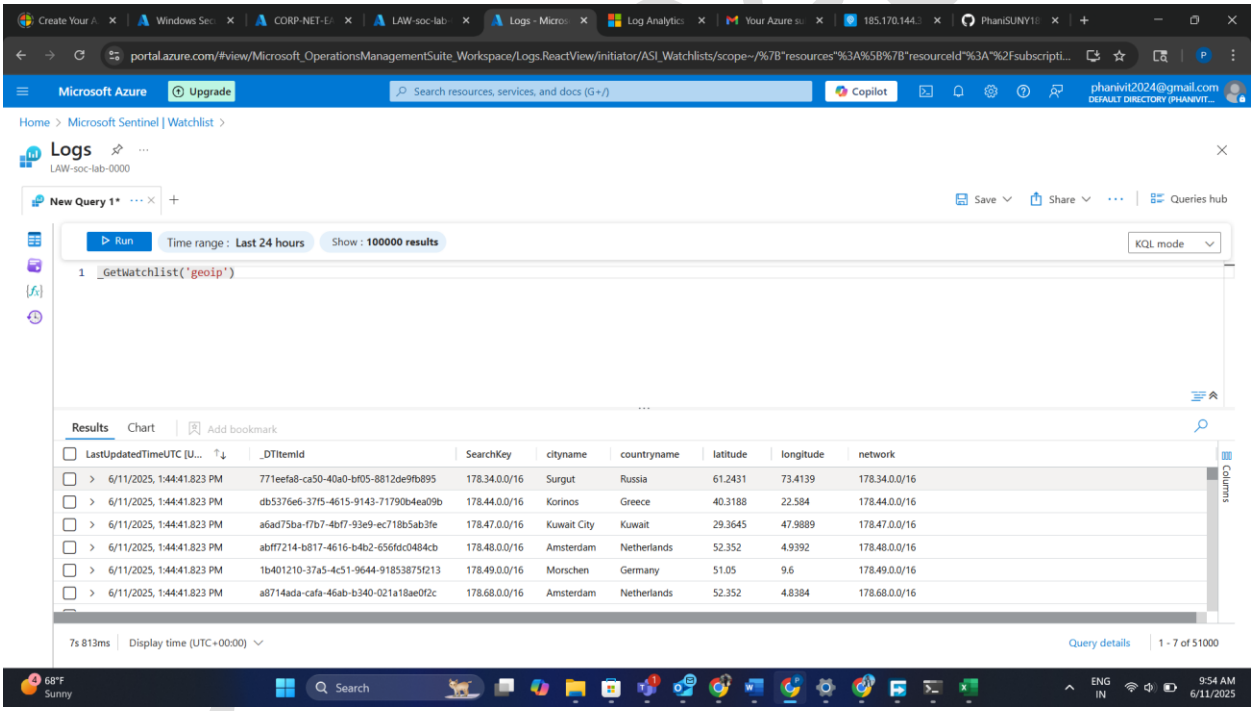
SecurityEvent

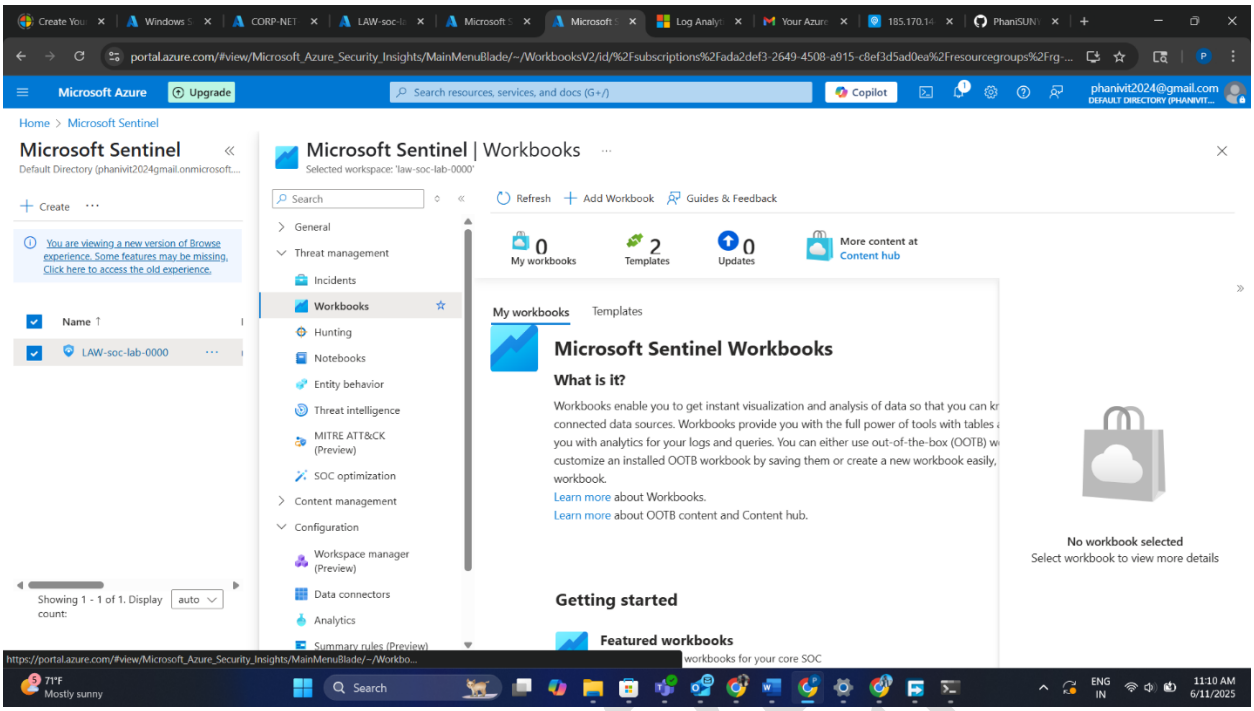
| where EventID == 4625

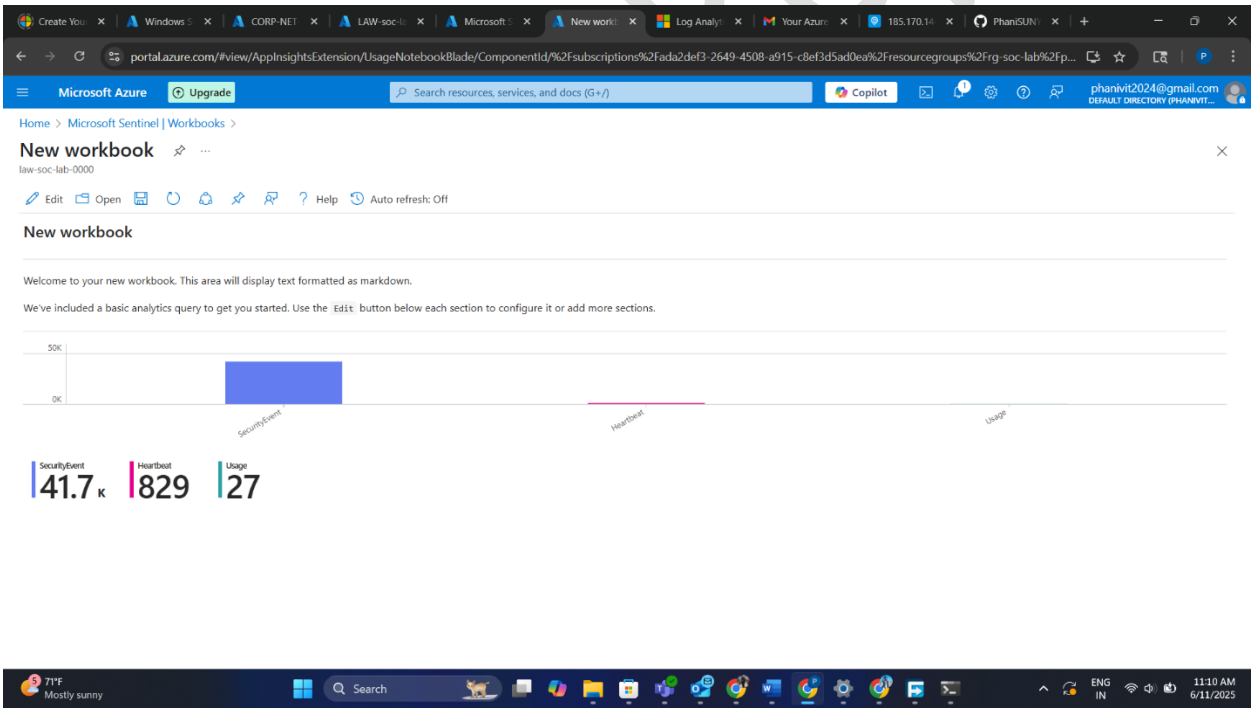
| lookup kind=leftouter geo on $left.IPAddress == $right.Network

| project TimeGenerated, Account, IPAddress, CityName, CountryName, Latitude, Longitude

---



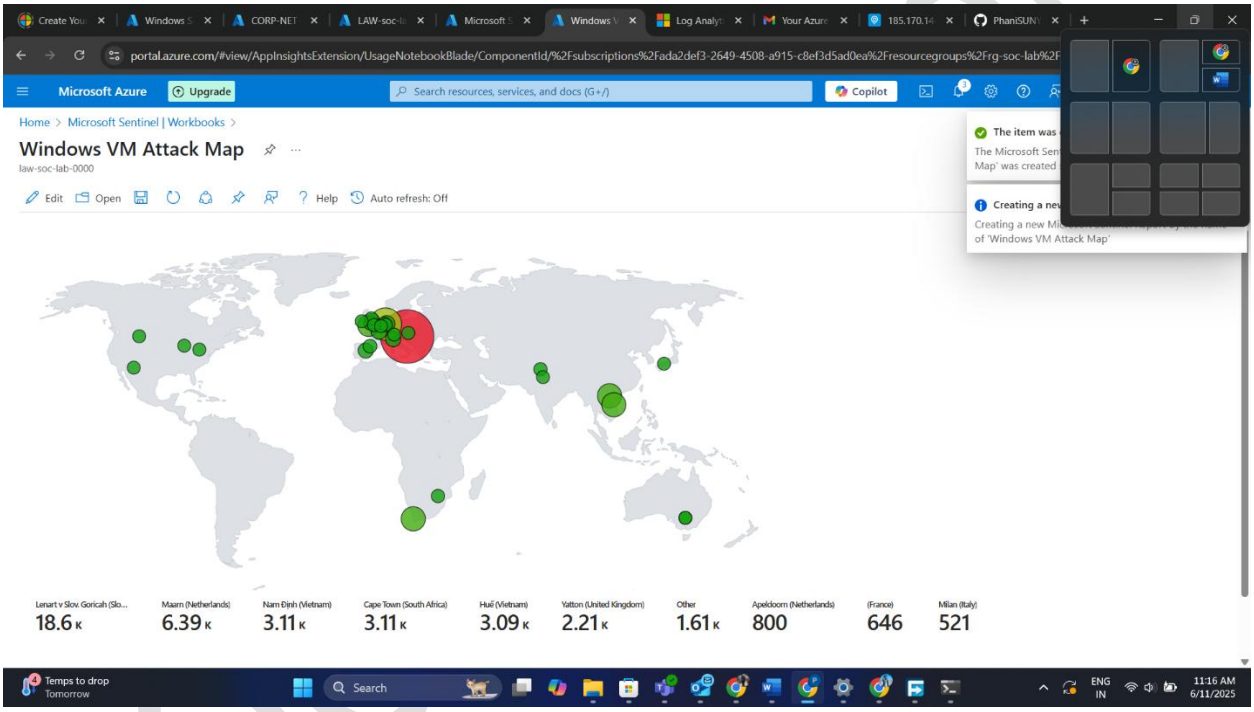

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Microsoft Sentinel
Microsoft Sentinel
Default Directory (phanivit2024gmail.onmicrosoft....
Create
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-soc-lab-0000
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Workbooks
Selected workspace: 'law-soc-lab-0000'
Search
Refresh
Add Workbook
Guides & Feedback
General
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
0
My workbooks
2
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
Microsoft Sentinel Workbooks
What is it?
Workbooks enable you to get instant visualization and analysis of data so that you can kr
connected data sources. Workbooks provide you with the full power of tools with tables
you with analytics for your logs and queries. You can either use out-of-the-box (OOTB) w
customize an installed OOTB workbook by saving them or create a new workbook easily,
workbook.
Learn more about Workbooks.
Learn more about OOTB content and Content hub.
Getting started
Featured workbooks
workbooks for your core SOC
No workbook selected
Select workbook to view more details
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/Workbo...
71°F
Mostly sunny
Search
ENG
IN
11:10 AM
6/11/2025

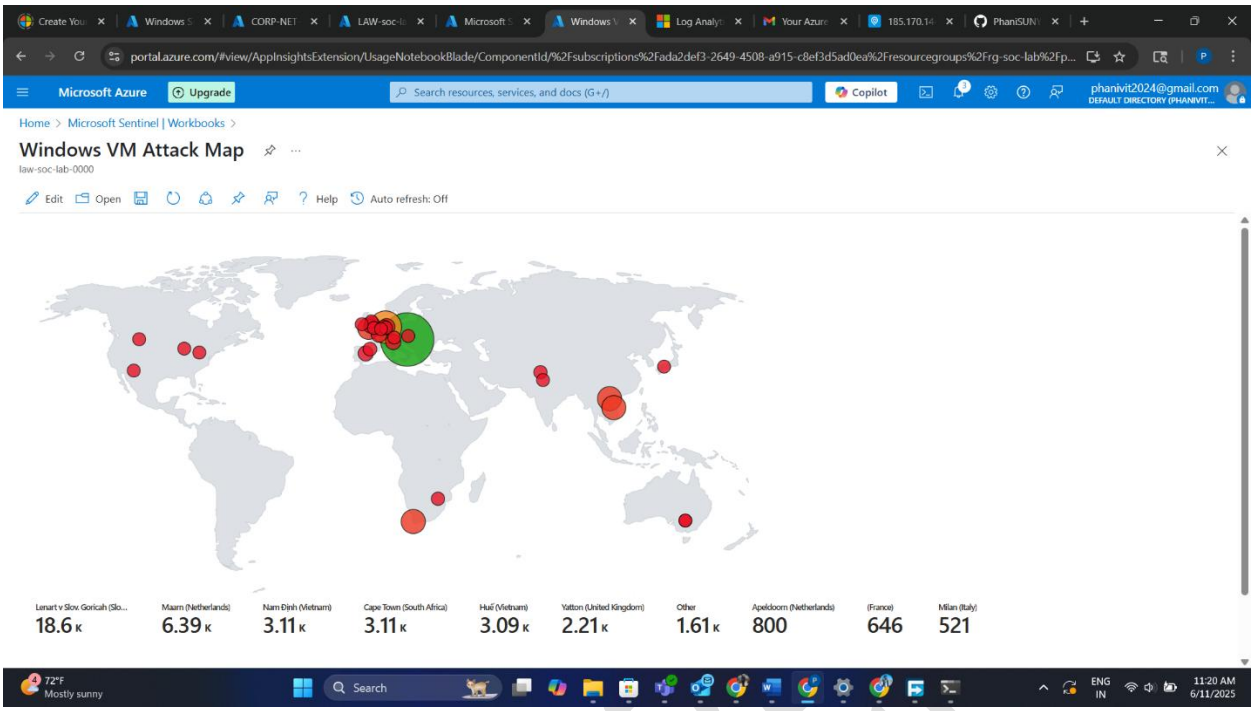

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Microsoft Sentinel | Workbooks >
New workbook
law-soc-lab-0000
Edit
Open
Help
Auto refresh: Off
New workbook
Welcome to your new workbook. This area will display text formatted as markdown.
We've included a basic analytics query to get you started. Use the Edit button below each section to configure it or add more sections.
50K
0K
SecurityEvent
Heartbeat
Usage
SecurityEvent
41.7 K
Heartbeat
829
Usage
27
71°F
Mostly sunny
Search
ENG
IN
11:10 AM
6/11/2025

15. Visualizing Attacks on World Map (Attack Map Workbook)

A custom Sentinel Workbook was created:

- Visualized attacker locations using a heatmap
- JSON template from the lab was imported
- Map labeled by city + country
- Updated in real time as logs increased




portal.azure.com/#view/AppInsightsExtension/UsageNotebookBlade/ComponentId/%2Fsubscriptions%2Fada2def3-2649-4508-a915-c8ef3d5ad0ea%2Fresourcegroups%2Frg-soc-lab%2Fp...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
phanivit2024@gmail.com
DEFAULT DIRECTORY (PHANIVIT...
Home > Microsoft Sentinel | Workbooks >
Windows VM Attack Map
law-soc-lab-0000
Edit
Open
Help
Auto refresh: Off
Lenart v Slov. Goricah (Slo...
18.6 K
Maarn (Netherlands)
6.39 K
Nam Dinh (Vietnam)
3.11 K
Cape Town (South Africa)
3.11 K
Huế (Vietnam)
3.09 K
Yatton (United Kingdom)
2.21 K
Other
1.61 K
Apeldoorn (Netherlands)
800
(France)
646
Milan (Italy)
521
72°F
Mostly sunny
Search
ENG
IN
11:20 AM
6/11/2025

Conclusion

This lab simulates how real-world systems are probed and attacked almost instantly when exposed online. It teaches:

- Cloud infrastructure setup
- Vulnerability simulation
- Log ingestion and enrichment
- Security analytics with KQL
- Building geographic visualizations

Completing this lab is a strong portfolio item for aspiring SOC analysts, threat hunters, and cybersecurity engineers.